UNIVERSITA KARLOVA V PRAZE
PRÁVNICKÁ FAKULTA
KATEDRA TRESTNÍHO PRÁVA

Trestněprávní a kriminologické aspekty internetové kriminality

DISERTAČNÍ PRÁCE
30.8.2012

Autor disertační práce: JUDr. Jiří Krupička

Adresa: náměstí Svatopluka Čecha 1358/10
Praha 10 - Vršovice
101 00

Obor: Veřejné právo III **2012**

Rád bych touto cestou vyjádřil poděkování panu prof. JUDr. Jiřímu Jelínkovi, CSc. za jeho cenné rady, trpělivost, vstřícnost a pomoc při mé cestě za vyšším poznáním.

Prohlášení o původnosti disertační práce

Prohlašuji, že jsem tuto disertační práci zpracoval samostatně, všechny v ní použité prameny a literatura byly řádně citovány a tato práce nebyla využita k získání jiného nebo stejného titulu.

V Praze dne 30.8.2012

_____

JUDr. Jiří Krupička

Obsah

Seznam použitých zkratek:

tr.ř.	zákon č. 141/1961 Sb., trestní řád v aktuálním znění
tr.zák.	zákon č. 40/2009 Sb., trestní zákoník
AutZ	zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon)
ObčZ	zákon č. 40/1964 Sb., občanský zákoník
ObchZ	zákon č. 513/1991 Sb., obchodní zákoník
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 jej známe dnes, je starý přibližně 20 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[1] 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 2012, je tímto médiem disk DVD (odhlédneme-li od různých druhů paměťových karet) 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 zmnohonásobila) 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 a není to ani ve stanoveném rozsahu dost dobře možné. 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.

[1] Autor této práce se rozhodl v textu psát slovo „internet" s malým písmenem a nerozlišovat tak mezi „Internetem" jakožto konkrétním celosvětovým systémem pracujícím na protokolu TCP/IP a „internetem" jakožto obecným pojmem pro jakékoliv a jakkoliv propojené sítě.

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, analýzu důvodů rozmachu a latence internetové kriminality, obecnou charakteristiku pachatele kyberkriminality a výklad o vybraných trestněprávních aspektech internetové kriminality.

Druhá část popisuje vybrané typy trestné činnosti páchané přímo nebo prostřednictvím internetu. V každé hlavě této části je rozbor (kriminologický a následně trestněprávní) jednoho typu internetové kriminality. 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.

Předposlední část sestává z kritické analýzy právních předpisů a jednotlivých norem postihujících internetovou kriminalitu (de lege lata), které jsou doplněny i o úvahy a návrhy potřebných změn do budoucna (de lege ferenda).

Poslední část je konečně věnována zahraničnímu srovnání právní úpravy trestných činů určených přímo k postihu kyberkriminality.

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 způsobu provedení jednotlivých kyberzločinů. V takových případech se autor snažil nezabředávat do zbytečných a s problematikou přímo nesouvisejících detailů, popř. se je pokusil ve stručnosti vysvětlit. Práce je zpracována ke dni 30.8.2012.

I Obecná část

1. Vymezení pojmů

Na rozdíl 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. Tak je tomu i v případě 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,[2] a to shodně i v zahraničních pramenech.[3,4] Další možnou definicí je trestná činnost, při které tvoří počítač nezbytnou součást této činnosti, a to jako nástroj trestného činu, předmět útoku trestného činu nebo jako pramen důkazů o trestném činu.[5]

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. Někteří autoři proto přichází s definicí, která se tomuto problému snaží vyhnout, výsledkem však často bývá její značná komplikovanost a nesrozumitelnost. Příkladem může být definice počítačové kriminality jakožto „*páchání trestné činnosti, v níž figuruje určitým způsobem*

---

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

[3] „Computer crime is most often thought of as a crime that is committed with the aid of a computer.“; Watson Business Systems Ltd: A Guide To Computer Crime - An Introduction To Computer Crime and Internet Fraud, http://legal.practitioner.com/computer-crime/, zobrazeno 10.5.2011, 16:22

[4] Vito, G., F., Maahs, J., R.,Holme, R., M.: Criminology: Theory, Research, And Policy. 2. vydání. Jones and Barlett Publisher, Sudbury 2007, s. 419

[5] Moore, R.: Cybercrime: Investigating High-Technology Computer Crime. 2. vydání. Elsevier, Oxford 2011, s. 3

počítač jako souhrn technického a programového vybavení včetně dat, nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď:

a) *jako předmět této trestné činnosti, ovšem s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité,*
b) *nebo jako nástroj trestné činnosti*."[6]

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
6) porušování průmyslových práv a práv duševního vlastnictví prostřednictvím počítače či sítí (tzv. počítačové pirátství)[7]
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 počítačové kriminality zahrnuje.

1.2. Pojem internetové kriminality

Při definici pojmu internetové kriminality[8] se nutně musíme potýkat se stejnými problémy jako u pojmu počítačové kriminality. Můžeme ji nejjednodušeji definovat jako trestnou činnost

---

[6] Smejkal, V., Sokol, T., Vlček, M.: Počítačové právo. 1. vydání. C.H.Beck, Praha 1995
[7] Dastych, J.: Počítačová kriminalita – stručný přehled in: Musil, S.: op. cit., příloha 2
[8] Smejkal a kol. v této souvislosti hovoří o „e-kriminalitě" – viz Smejkal, V. a kol.: Právo informačních a telekomunikačních systémů. 2. aktualizované a rozšířené vydání. C.H.Beck, Praha 2004, s. 694

páchanou využíváním internetu.[9,10] Podobně vyzní definice internetové kriminality jako aktivity, při nichž je užito internetu za účelem spáchání trestného činu či jiného deliktu, přičemž internet sám může být i předmětem takového útoku. 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 spojená 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. Technologicky se jedná o soustavu serverů, datových komunikací a k nim připojených počítačů[11], které mezi sebou komunikují. 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), internetová telefonie 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),[12] pravý rozmach internetu přišel až počátkem 90. let minulého století, kdy v květnu 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.[13] K 31.12.2011 byl počet uživatelů internetu již 2.267.233.742 osob,[14] přičemž tento počet neustále narůstá.

---

[9] Gottschalk, P.: Policing Cyber Crime. 1. vydání. Petter Gottschalk & Ventus Publishing ApS, 2000, s. 10

[10] Obdobně srov. Kuchta, J., Válková, H. a kol.: Základy kriminologie a trestní politiky. 1. vydání. C. H. Beck, Praha 2005, s. 515

[11] Smejkal, V. a kol.: op. cit., s. 587

[12] Poprvé představen 29.10.1969; http://en.wikipedia.org/wiki/History_of_internet; zobrazeno 15.4.2012, 18:35

[13] Více k historii internetu viz např. Mowery, D. C., Simce, T.: Is the Internet a US invention? – an economic and technological history of computer networking in: Research Policy. Vol. 31, Elsevier Science B.V., 2002, s. 1369 - 1387

[14] World Internet Usage Statistics News and Population Stats, http://www.internetworldstats.com/stats.htm, zobrazeno 20.2.2012, 13:45

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 pod č. 185. Její anglický název totiž zní „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“[15] 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.[16]

Jelikož je tento kyberprostor vytvářen zejména elektronickými sítěmi, zdá se být velice výstižná[17] definice pojmu kybernetické kriminality jako souhrnu všech kriminálních aktivit, které jsou páchány prostřednictvím komunikačních zařízení propojených v síti. Může se tak dít prostřednictvím internetu, telefonních, mobilních či jiných obdobných sítí.[18] V takovém případě by „kyberkriminalita“ netvořila podmnožinu počítačové kriminality, jelikož určitá trestná činnost by mohla být páchána prostřednictvím např. mobilního telefonu. Jednalo by se tak o dva odlišné pojmy, množiny, s některými prvky shodnými a jinými nikoliv. Naopak internetová kriminalita by pak ležela v průniku pojmů počítačové kriminality a kybernetické kriminality.

Ve většině případů (zejména v zahraniční literatuře) se však pojmy kybernetická kriminalita, internetová a počítačová kriminalita používají promiscue, některé tak např. kybernetickou kriminalitu definují jako počítačovou kriminalitu, která se týká internetu.[19] Obecný trend i v české literatuře spěje k nahrazení termínu počítačová kriminalita pojmem kybernetická kriminalita.

---

[15] Wiener, N.: Kybernetika a společnost. Academia, Praha 1963
[16] 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
[17] Pokud tedy chceme vzájemně odlišit počítačovou a kybernetickou kriminalitu
[18] Halder, D., Jaishankar, K.: Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. IGI Global, Hershey 2011, s. 13 a násl.
[19] Reid, S., T.: Crime and Criminology. Oxford University Press, New York 2009, s. 249 a násl.

2. Členění internetové kriminality

2.1. Typové členění

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 sem náležející nemají obvykle výrazně podobný ekvivalent mimo kybernetický svět. Jsou často 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, šíření pornografie, podpora a propagace hnutí směřujících k potlačení práv a svobod člověka, nebezpečné pronásledování 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. Tak je možné internetovou kriminalitu rozdělit na:[20]

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

Další členění rozděluje internetovou kriminalitu na dvě skupiny podle zištnosti:

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 často nemusí mít 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 škodlivá, mohou znamenat obrovské ztráty (vyřazení sítě, náklady na nápravu bezpečnostních mezer, ztráty na výdělku apod.).

[20] Idem

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.[21]

[21] V podrobnostech srov. Jelínek, J. a kol.: Trestní právo hmotné. 2. vydání. Leges, Praha 2010, s. 131 a s. 154 a násl.; Novotný, O., Vanduchová, M., Šámal, P. a kol.: Trestní právo hmotné. Obecná část. 6. vydání. Wolters Kluwer ČR, a.s., Praha 2010, s. 125 a s. 144 a násl.

3. Důvody rozmachu a latence internetové kriminality

3.1. Nejdůležitější faktory růstu prevalence internetových deliktů

Důvodů rozmachu internetové kriminality je bezpočet a zasloužil by samostatnou studii. Lze je nalézt napříč různými společenskými odvětvími. Jsou jak technologické, sociologické, psychologické i historické. Mezi nimi však lze najít ty, které bychom mohli považovat za stěžejní, podmiňující exponenciální růst internetových deliktů z poslední doby. Autor této práce mezi ně řadí:

1) Globalizaci – 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.[22]

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). Tomuto pokroku však neodpovídá jak vývoj prevenčních opatření, tak i právo samotné, které za ním značně zaostávají.

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. Jen u málokterého typu kriminality může pachatel dosahovat tak obrovského zisku za takřka nulové investice.

4) Nízké právní vědomí obětí a pachatelů[23] – jak bude popsáno níže ve zvláštní části této práce, u některých druhů internetové kriminality závisí úspěšnost útoku pouze na naivitě a důvěryhodnosti obětí. To je patrné zejména u různých podvodných jednání. Naopak někdy může spočívat důvod protiprávního činu v prosté nevědomosti delikventa, že jeho jednání je protiprávní. Tyto případy se objevují např. u nevědomého porušování autorských práv neoprávněným užitím softwarových programů na domácím počítači.

5) 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 apod.)? 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. Podobně velkou část své agendy převádí do

[22] O globálním působení internetu vypovídá i mapa procentní míry uživatelů internetu v populaci jednotlivých států světa v Příloze č. 1 této práce
[23] Dianiška, G. a kol.: Kriminológia. 2. vydání. Aleš Čeněk, Plzeň 2011, s. 247

elektronické podoby i státní orgány. S tímto vývojem pak ruku v ruce jde i umísťování stále více důležitých (a zneužitelných) informací na internetu. V dnešní době jsou dokonce pouze elektronicky vedeny soudní spisy v insolvenčních věcech (odhlédneme-li od značné nedokonalosti a nepropracovanosti stávajícího systému elektronického spisu). Je zřejmé, že toto prostředí pak představuje skvělé podhoubí nejrůznějších kybernetických trestných činů.

6) Absence schopných strážců – jelikož je internet ve skutečnosti decentralizovaná síť, která není vlastněna určitou osobou[24] (pouze jsou tu poskytovatelé připojení a tzv. poskytovatelé volného prostoru), neexistuje ani určitá osoba, která by využívání internetu kontrolovala. Policejní orgány jednotlivých zemí obvykle narážejí na neexistenci globálních zákonů,[25] 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.

7) Anonymita (někdy však relativní) pachatelů – internet je lákavým prostředím k páchání trestné činnosti, neboť nabízí pachatelům anonymitu, kterou by ve skutečném světě nikdy neměli.[26] 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.

8) Nízká koupěschopnost obyvatel některých zemí[27] – chudoba patří k jednomu z nejvýznamnějších kriminogenních faktorů vůbec. Řada pachatelů se uchyluje k trestným činům jednoduše z toho důvodu, že nemá dostatek finančních prostředků, aby si určitou věc či službu koupila. Takto jsou kupříkladu vysoké licenční poplatky za autorská práva významnou příčinou vysoké prevalence porušování autorských práv v zemích střední, východní a jihovýchodní Evropy.

[24] Deveci, H., A.: Personal Jurisdiction: Where Cyberspace Meets the Real World – Part 1 in: Computer Law & Security Report. Vol. 2. Elsevier Science B.V., 2005, s. 465
[25] Hunton, P.: The Growing Phenomenon of Crime and the Internet: A Cybercrime Execution and Analysis Model in: Computer Law & Security Review. Vol. 25. Elsevier Science B.V., 2009, s. 530 a 533
[26] Idem.
[27] Dianiška, G. a kol.: op. cit., s. 248

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.[28] Tento názor dokládají i statistické výzkumy, dle kterých zůstává 90 - 95 % internetové kriminality neodhaleno.[29]

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.

Jiným důvodem latence této kriminality spočívá v technické (odborné) podstatě jednotlivých útoků, které bez specifických nástrojů k jejich detekci často vůbec nelze odhalit. Samotné útoky pak obvykle probíhají na dálku, a jak již bylo poznamenáno výše, zaznamenatelné a vyhodnotitelné stopy těchto kriminálních jednání jsou s velkým časovým odstupem od zjištění útoku velice obtížně identifikovatelné.

Dalším důvodem (zde zejména u fyzických osob) je ten, že se poškození z trestné činnosti 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.

---

[28] 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
[29] Dianiška, G. a kol.: op. cit., s. 247

Posledním zde uvedeným důvodem je pak možnost přilákání spáchání dalšího internetového trestného činu na prvotní oběti. Zvyšuje se tak tzv. viktimnost, čímž se rozumí 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). Řada z obětí se může domnívat, že by přilákala další pachatele v případě, kdy by odkryla, že se stala obětí úspěšného počítačového útoku a že její zabezpečení je nedokonalé.

4. Pachatelé internetové kriminality

4.1. Fyzické osoby jako 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 sepjetí internetové kriminality s technologiemi, je možné obecně říci, že typický pachatel internetové trestné činnosti je spíše nadprůměrně inteligentní a ve velké většině mladšího (často ve věku náctiletých) až středního věku.[30] 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. V současném světě jsou počítače a internet součástí každodenního života a na rozdíl od starších osob, které si na tuto technologickou invazi musely zvykat, se mladší generace už do světa ovládaného počítači narodily či se s počítači setkaly již na školách a přijaly je za své.[31]

Většina pachatelů internetové kriminality nemá dosud záznam v rejstříku trestů.[32] Některé typy deliktů kyberkriminality (typicky hacking) vyžadují ke svému provedení značnou technickou (informatickou) znalost. Je proto pochopitelné, že osoby s vyšším inteligenčním kvocientem získají tuto znalost rychleji a často efektivněji, než osoby s podprůměrnou inteligencí. To však neplatí bezvýhradně. Jako v jiných oblastech není již kybernetická kriminalita výsadou pouze počítačových „mágů“, jako tomu bylo v 90. letech minulého století. I k prostředkům hackingu se v dnešní době lze dostat jednoduše tím, že si je potenciální pachatel prostě zakoupí či jinak obstará (paradoxně i na webu), a to včetně návodu (postupu), jak je využívat. K tomu ovšem nepotřebuje vyšší inteligenci.

Jiným aspektem, který spoluurčuje charakter pachatele internetové kriminality, je ten, že se zde prakticky nevyskytují trestné činy proti životu a zdraví[33] (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, sadistických pedofilů, kyberšikany a kyberstalkingu) jen málo „násilnických“ typů pachatele.

---

[30] Holcr, K.. a kol.: Kriminológia. 1. vydání. Wolters Kluwer, Bratislava 2008, s. 361
[31] Barlow, H., D.: Introduction to Criminology. 7. vydání. HarperCollins College Publishers, Inc., New York, 1996, s. 210
[32] Kuchta, J., Válková, H. a kol.:, op. cit., s. 507
[33] Shodně Požár, J. a kol.: Základy teorie informační bezpečnosti. 1. vydání. Policejní akademie České republiky v Praze, Praha 2007, s. 129

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,[34] ačkoliv mnoho druhů činů páchaných v internetu má charakter majetkové či hospodářské kriminality. Jako zářný příklad dobře poslouží archetyp obvyklého pachatele - „hackera“, kterého lze charakterizovat všemi možnými atributy, jen ne právě „bílým límečkem“. Je však zřejmé, že i toto „archetypální“ nahlížení na pachatele internetové kriminality je plné předsudků a nepodložené paušalizace. Ne všichni hackeři jsou nevybouření postpubertální jedinci zavření ve svém světě počítačů. Mohou jimi sice být, na druhou stranu však není neobvyklé, že hackingové aktivity páchají i osoby vyspělé, které se jednoduše uchylují ke kybernetickým útokům proto, že z nich mohou mít majetkový prospěch s poměrně malým rizikem odhalení. Tak tomu je v případech kybernetických průmyslových špionáží. Je rovněž poměrně časté, že pachateli kyberútoků jsou sami zaměstnanci poškozených společností.[35] Pachatele tak lze nalézt napříč všemi společenskými vrstvami.

Výhodou kybernetického světa, kde se internetová kriminalita odehrává, je (alespoň pro pachatele) skutečnost, že nemusí absolutně korespondovat s realitou. Pachatel se tu často cítí, a dokonce i může být, úplně jiným člověkem, než je ve skutečném světě. Kyberprostor a internetová kriminalita pak mohou sloužit jako prostředek „seberealizace“ a možnost 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.

Samotná typologie pachatelů kriminality se bude značně lišit v rámci jednotlivých druhů internetové kriminality. Obvykle se setkáme se zcela jiným pachatelem u phishingu, jiným typem pachatele u šiřitele dětské pornografie a opět jiným v případě kyberstalkera. Z hlediska kriminologického je ovšem zajímavé, že kyberkriminalita, a to prakticky jakákoliv, je vnímána jako čistě mužská (resp. klukovská) doména. Tomu odpovídají i všeobecně známé případy dopadených pachatelů internetové kriminality,[36] mezi nimiž nefiguruje jediná žena.[37]

Konečně je možné pachatele internetové (ale i obecně počítačové) kriminality rozdělit podle jejich motivace, schopností, profesionality (amatérismu) a znalostí do těchto charakteristických skupin: 1.) Novic, 2.) Kybernetický chuligán, 3.) Vnitřní nepřítel, 4.) Malý

---

[34] Mnozí autoři ji však mezi kriminalitu bílých límečků stále řadí – srov. např. Požár, J. a kol.: op. cit., s. 130

[35] Završnik, A.: Definiční problémy a kriminologická specifika kyberzločinu in: Gřivna, T., Polčák, R. (eds.): Kyberkriminalita a právo. 1. vydání. Auditorium, Praha 2008, s. 37

[36] http://en.wikipedia.org/wiki/List_of_computer_criminals

[37] K genderovým aspektům kyberkriminality srov. blíže Završnik, A.: op. cit., s. 42 a násl.

zlodějíček, 5.) Stará garda, 6.) Autor škodlivých kódů, 7.) Profesionální kriminálník, 8.) Informační bojovník.[38] Z uvedeného je zřejmé, že konkrétní pachatelé mohou náležet do dvou i více skupin. Tak například si lze představit pachatele, kterého bude vzhledem k okolnostem spáchání jeho činu možné označit za informačního bojovníka, vnitřního nepřítele i autora škodlivých kódů. Naznačené rozdělení tak spíše výstižně pojmenovává konkrétní pachatele kyberzločinů, než by jasně kladlo dělicí čáru mezi jednotlivými typy pachatelů.

4.2. Právnické osoby jako pachatelé internetové kriminality

Shora uvedené charakteristické vlastnosti pachatelů kyberkriminality platí pouze pro fyzické osoby, které donedávna mohly být jako jediné trestně odpovědny. To však změnil zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim. Ten totiž s účinností od 1.1.2012 zavádí trestní odpovědnost právnických osob, jimž může být za okolností uvedených v § 8 tohoto zákona přičtena trestní odpovědnost za protiprávní čin fyzické osoby jednající v jejich zájmu, jejich jménem nebo v rámci její činnosti, a to pokud by toto jednání naplnilo skutkovou podstatu jednoho z taxativně uvedených trestných činů v § 7 tohoto zákona.[39] Za tyto trestné činy právnické osobě hrozí tresty ukládané v trestním řízení vedeném trestními senáty obecných soudů. Deliktní odpovědnost korporací je tak založena na tzv. pravé trestní odpovědnosti právnických osob.[40]

V případě právnických osob bude „motiv“ (pokud vůbec o motivu v případě právnických osob můžeme hovořit) jejich internetové trestné činnosti obvykle majetkový, a to v zájmu zvýšení příjmů právnické osoby. Od právnických osob lze očekávat delikvenci zejména v oblasti průmyslové špionáže, jednání v rozporu s pravidly hospodářské soutěže nebo počítačové sabotáže, a to ať už hackingovými praktikami či nekalým soutěžním jednáním v elektronickém obchodu a při propagaci na internetu. Z toho důvodu lze většinově označit internetovou trestnou činnost právnických osob za kriminalitu bílých límečků.

---

[38] Holcr, K. a kol.: op. cit., s. 362

[39] Konkrétní právní aspekty trestní odpovědnosti právnických osob vybočují z tématu této práce, proto v podrobnostech viz např. Jelínek, J., Herczeg, J.: Zákon o trestní odpovědnosti právnických osob a řízení proti nim. Komentář s judikaturou. 1. vydání. Leges, Praha 2012 a Šámal, P. a kol.: Trestní odpovědnost právnických osob. Komentář. 1. vydání. C. H. Beck, Praha 2012

[40] K podrobnostem o pravé trestní odpovědnosti právnických osob a jejích rozdílech oproti jiným typům odpovědnosti korporací viz Jelínek, J.: Trestní odpovědnost právnických osob. 1. vydání. Linde Praha, a.s., Praha 2007, s. 21 a násl.

Na druhou stranu z omezenosti výčtu trestných činů, které může právnická osoba spáchat, lze konstatovat, že za mnohá trestná jednání fyzických osob, ze kterých právnické osoby budou značně profitovat, nebudou často tyto korporace nést žádnou trestní odpovědnost. Tak například chybí ve výčtu trestných činů uvedených v § 7 zákona o trestní odpovědnosti právnických osob trestný čin porušení předpisů o pravidlech hospodářské soutěže podle § 248 tr.zák., jakožto jeden z nejvýznamnějších hospodářských deliktů. Právnická osoba tak nikdy nebude trestně odpovídat např. i za nejzávažnější nekalosoutěžní jednání. Rovněž dle tohoto zákona nemůže právnická osoba spáchat trestný čin porušení tajemství listin a jiných dokumentů uchovávaných v soukromí podle § 183 tr.zák. (ačkoliv může spáchat trestný čin porušení tajemství dopravovaných zpráv), pomluvu podle § 184 tr.zák., neoprávněné nakládání s osobními údaji podle § 180 tr.zák. nebo poškození cizích práv podle § 181 tr.zák. Zcela nepochopitelně pak zákonodárce vyloučil právnické osoby i z trestní odpovědnosti za trestné činy porušení práv k ochranné známce a jiným označením podle § 268 tr.zák. a porušení chráněných průmyslových práv podle § 269 tr.zák., přestože u autorských práv trestní ochranu před porušením ze strany právnických osob umožnil. Absurdní je i vynětí právnických osob z postihu za krádež podle § 205 tr.zák či neoprávněné užívání cizí věci podle § 207 tr.zák.

Z uvedeného je tedy zřejmé, že výčet trestných činů, za které může být právnická osoba trestně odpovědná, je dosti omezený. Na tom by nebylo nic špatného, kdyby toto omezení bylo jakkoliv racionálně odůvodněno. Tak například by bylo pochopitelné, pokud by zákonodárce zavedl trestní odpovědnost právnických osob pouze pro velice omezený okruh trestných činů, kupříkladu jen majetkových. Počáteční menší počet trestných činů zakládajících trestní odpovědnost korporací by mohl být odůvodněn i určitou legislativní opatrností, kdy by (nejprve) byla zavedena trestnost jen v úzkém rozsahu, a pokud by se tato úprava osvědčila, mohl by zákonodárce výčet trestných činů dále rozšiřovat. Podobný přístup zavedlo např. Švýcarsko.

Na druhou stranu by rovněž bylo možné koncipovat trestní odpovědnost právnických osob jako neomezenou, vztahující se na všechny trestné činy. Jednak pak není nutné novelizovat výčty trestných činů a jednak tato skutečnost odpovídá i rovnému nahlížení na odpovědnost fyzických i právnických osob. Tomuto řešení by samozřejmě nevadilo, pokud by z podstaty věci právnická osoba nemohla určitý trestný čin za žádných okolností spáchat. V takovém případě by se jednoduše ohledně těchto trestných činů právnická osoba pachatelem stát nemohla. Toto řešení zavedla např. Republika Rakousko.

V České republice zavedené řešení ovšem neodpovídá ani jedné z uvedených koncepcí. Výčet trestných činů v zákoně o trestní odpovědnosti právnických osob nemá vnitřní logiku a

jednoduše se zdá, že zákonodárce určité trestné činy do výčtu zařadil a jiné nikoliv pouze z jakéhosi vnitřního rozmaru. V ustanovení § 7 zákona o trestní odpovědnosti právnických osob tak zcela chybí jakékoliv trestné činy v rámci I. hlavy zvláštní části trestního zákoníku, pročež není možné hnát k trestní odpovědnosti zdravotnická zařízení ani pro nedbalostní trestné činy proti životu a zdraví. Stejně tak v něm chybí mnoho zásadních hospodářských trestných činů, které přitom historicky byly jedním z hlavních důvodů zavádění trestní odpovědnosti právnických osob (zejména uvedené porušení předpisů o pravidlech hospodářské soutěže). Svou logickou, resp. nelogickou strukturou tak citované ustanovení připomíná stejně nepochopitelný výčet trestných činů uvedený v § 163 odst. 1 tr.ř. upravující trestní stíhání se souhlasem poškozeného, u nějž si každý musí klást otázku, proč zrovna tam uvedené trestné činy vyžadují k trestnímu stíhání souhlas poškozeného.

Takovéto nesystematické a rovnost práv zpochybňující omezení trestní odpovědnosti právnických osob lze pouze odsoudit, neboť pokud zákonodárce chtěl právnickou osobu jakožto pachatele trestného činu zavést, měl tak učinit řádně a nikoliv jen polovičatě, jak vyplývá ze stávající úpravy. Zároveň může současná úprava trestní odpovědnosti právnických osob vést ke ztrátě důvěry veřejnosti v účinnost takovéhoto institutu v boji proti závažné kriminalitě.

5. Vybrané trestněprávní aspekty internetové kriminality

5.1. Obecně k trestní odpovědnosti

Aby mohl být pachatel odpovědný ze spáchání trestného činu,[41] je vždy bezpodmínečně nutné, aby se jednalo o čin protiprávní a byly vždy naplněny všechny znaky trestného činu uvedené v trestním zákoníku[42] (naplnění všech znaků trestného činu jako *conditio sine qua non* trestní odpovědnosti). Nový trestní zákoník zavedl, na rozdíl od předchozí právní úpravy, formální pojetí TČ, které je však doplněno materiálním korektivem,[43] resp. významným interpretačním principem[44] představovaným zásadou subsidiarity trestní represe. Ta v ustanovení § 12 odst. 2 tr.zák. vyžaduje, aby trestní odpovědnost a její důsledky byly uplatňovány pouze v případě společensky škodlivých, kdy nebude postačovat odpovědnost podle jiného právního předpisu.[45] Trestný čin je v § 13 odst. 1 tr.zák definován jako protiprávní čin, který trestní zákon označuje za trestný a který vykazuje tam uvedené znaky. Jsou jimi jednak obecné znaky (příčetnost a věk[46]) a jednak znaky skutkové podstaty trestného činu (objekt, objektivní stránka, subjekt a subjektivní stránka, protiprávnost).[47]

5.2. Společenská škodlivost a internetová kriminalita

Téma společenské škodlivosti jednání pachatelů je po přijetí nového trestního zákoníku v odborných kruzích značně diskutované.[48] Samotný pojem společenské škodlivosti však není v zákoně definován. Obvykle se na ni nazírá hledisky povahy a závažnosti trestného činu, které trestní zákoník příkladmo definuje jako vodítka pro ukládání trestů v § 39 odst. 2 tr.zák. Podobná hlediska se uplatňují i pro fakultativní zastavení trestního stíhání státním zástupcem v § 172 odst. 2 tr.ř. Povaha a závažnost trestného činu podmiňující společenskou škodlivost bude tak určována např. významem objektu trestného činu, který byl činem

[41] Popř. provinění u mladistvých pachatelů, dále jen: „trestný čin“ či „TČ“
[42] Dále také „tr.zák.“
[43] Jelínek, J. a kol.: op. cit., s. 117
[44] Novotný, O., Vanduchová, M., Šámal, P. a kol.: op. cit., s. 113
[45] Trest jako *ultima ratio*
[46] K věku pak přistupuje u mladistvých rozumová a mravní vyspělost (tzv. relativní trestní odpovědnost mladistvého)
[47] Podrobněji např. Jelínek, J. a kol.: op. cit., s. 119 a násl.
[48] Viz např. Jelínek J.: K pojmu trestného činu v novém trestním zákoníku in: Jelínek, J. (ed.): O novém trestním zákoníku. Sborník z mezinárodní konference Olomoucké právnické dny. Leges, Praha 2009, s. 25 a násl.; dále viz Šámal, P.: K pojmu trestného činu a souvisejícím otázkám v novém trestním zákoníku in: Trestněprávní revue, č. 5/2009, s. 129 a násl. či Růžička, M.: K formálnímu pojetí trestného činu s materiálním korektivem z pohledu státního zástupce in: Trestněprávní revue č. 6/2011, s. 159 a násl.

dotčen, způsobem provedení činu a jeho následky, okolnostmi, za kterých byl čin spáchán, osobou pachatele, mírou jeho zavinění a jeho pohnutkou, záměrem nebo cílem. K tomuto je třeba doplnit, že se hodnotí konkrétní význam konkrétního zájmu zasaženého trestným činem, nikoliv význam typový, neboť ten již je vyjádřen ve skutkové podstatě TČ a v trestní sazbě.[49]

Praktický dopad zásady subsidiarity trestní represe na trestní odpovědnost pachatele není v praxi ještě ustálen. Původně byla tato prezentována pouze jako významná interpretační zásada, která měla být dodržována při výkladu jednotlivých ustanovení jak trestního práva hmotného, tak i procesního.[50] Tento přístup měl být projevem nově zavedeného formálního pojetí trestného činu. Posléze však praxe shledala (vzhledem k nedostatečným procesním institutům) potřebu alespoň částečně materiální korektiv ryze formálního pojetí zavést, aby tak bylo možné dovodit trestní neodpovědnost osob, které spáchaly jednání sice naplňující všechny formální znaky trestného činu, avšak vzhledem k okolnostem případu nebyl takový čin vůbec (či pouze zanedbatelně) společensky škodlivý. Jako průlomový v tomto směru lze označit nález Ústavního soudu ČR ze dne 10.2.2011, sp.zn. III.ÚS 2523/10, uveřejněný pod č. N 16/60 SbNU, s. 171, v jehož odůvodnění se uvádí, že nový trestní zákoník „*sice minimální spodní práh škodlivosti činu nevyjadřuje explicite, nicméně ze samotné povahy věci plyne, že určitá minimální kvantitativní hranice, oddělující právně tolerovatelné činy od činů trestuhodných, existuje. Zákonný prostor pro řešení takových situací poskytuje zásada subsidiarity trestní represe, výslovně zakotvená v § 12 odst. 2 nového trestního zákoníku:…*“ Podobné nazírání lze vysledovat i v některých uveřejněných rozhodnutí Nejvyššího soudu ČR z poslední doby.[51] Tento přístup tak nasměroval pojetí trestní odpovědnosti opět blíže k materiálně formální koncepci původního trestního zákona z roku 1961.

Zkoumání společenské škodlivosti a povinnosti zjišťovat, zdali v dané věci nebude postačovat odpovědnost podle práva občanského či správního, bude nabývat zvláštního rozměru i u internetové trestné činnosti. Tak například v případě porušování autorských práv prostřednictvím internetu se bude posuzovat, do jaké míry bylo zasaženo do autorských práv (jiná bude jistě škodlivost 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

[49] Přiměřeně viz Jelínek, J. a kol.: Trestní právo hmotné. Obecná část. Zvláštní část. 3. přepracované a aktualizované vydání. Linde Praha, a.s., Praha 2008, str. 146

[50] Tomu odpovídalo pojetí hlediska společenské škodlivosti jako „interpretačního principu“ – srov. pozn. č. 44

[51] Srov. Usnesení Nejvyššího soudu ČR ze dne 19.1.2011, sp.zn. 5 Tdo 17/2011, Usnesení Nejvyššího soudu ČR ze dne 16.2.2011, sp.zn. 8 Tdo 112/2011 a Usnesení Městského soudu v Praze ze dne 21.9.2011, sp.zn. 7 To 251/2011 uveřejněné v časopise Trestněprávní revue č. 4/2012, s. 97

neznámé doméně zpřístupní zkrácenou nahrávku písně své oblíbené kapely). Porušování autorských práv je v tomto směru velice specifické, neboť soukromoprávní úprava sama počítá přímo se sankčními důsledky vydání případného bezdůvodného obohacení toho, kdo autorská práva porušil, a to ve výši dvojnásobku obvyklé licenční odměny autora.[52] Pokud tedy je narušitel autorských práv již majetkově potrestán v rámci civilního práva, je třeba v konkrétních případech důsledně zvážit, zdali toto potrestání již nebylo dostatečné, zejména pokud by přicházelo v úvahu pouze uložení peněžitého trestu.

Podobně se bude hledisko subsidiarity trestní represe uplatňovat při zkoumání trestnosti vnitřní (zaměstnanecké) krádeže počítačového času, když by nebyl naplněn ani důvod okamžitého zrušení pracovního poměru. V takovém případě by jen těžko mohla být dovozena trestní odpovědnost takového zaměstnance.

Posouzení společenské škodlivosti bude rovněž zásadní i v případech šíření pornografie prostřednictvím internetu. Je totiž třeba si položit otázku, zda konkrétní jednání, např. zaslání krátkého videoklipu s animovanou dětskou pornografií e-mailem v rámci komunity pedofilů, je vůbec společensky škodlivé, zda neznamená zbytečné přepínání trestní represe.[53] Pokud totiž pro pedofily nebude z hlediska trestního postihu rozdíl mezi skutečnou a virtuální pornografií, budou samozřejmě poptávat tu skutečnou, ve které jsou děti reálně zneužívány. Pro některé pak vědomí trestnosti již samotného držení dětské pornografie může vést k tomu, že sami raději zvolí přímo zneužívání dětí před ukájením pomocí pornografie, neboť rozdíly ve výši trestních sazeb už pro mnohé nemusí hrát roli.

U způsobu provedení činu a jeho následku bude z hlediska materiálního korektivu subsidiarity trestní represe relevantní zejména rozsah škod trestnou činností způsobených, nemusí to však být jediným kritériem. Spáchání trestného činu veřejně přístupnou počítačovou sítí je považováno za společensky škodlivější, pokud tak dopadá trestná činnost na více adresátů (obětí). Rovněž bývá často okolností podmiňující použití trestní sazby.

Ohledně hodnocení okolností, za kterých byl čin spáchán, je třeba si 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) uvědomit, že v současnosti povětšinou stoupá tendence

[52] Srov. § 40 odst. 4 in fine AutZ
[53] Ohledně trestnosti držení a šíření dětské virtuální pornografie viz hlava 5. zvláštní části této práce a část III. kapitola 2.1.4.2 této práce

k páchání těchto trestných činů, a roste tedy potřeba reagovat na tento vzestup i zpřísněnou represí.

Problematické bude v případech internetové kriminality posuzování povahy a závažnosti 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 společenská škodlivost 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 ignorantia legis non excusat) a že jsou více nerozvážní a jednají impulzivněji. Zákon o soudnictví ve věcech mládeže tyto skutečnosti zohledňuje již v § 3, upravujícího základní zásady trestní odpovědnosti mladistvých a řízení proti nim, když v odst. 3 citovaného ustanovení stanoví, že uložené opatření musí přihlížet mimo jiné i k věku a rozumové a mravní vyspělosti toho, komu je ukládáno, a musí být přiměřené povaze a závažnosti spáchaného činu. 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.

Co se týká společenské škodlivosti internetové kriminality ve vztahu k pohnutce pachatelova jednání, bude obecně posuzováno jako závažnější jednání, které sledovalo určitý hospodářský nebo podnikatelský účel, tedy zda pachatel jednal, aby dosáhl zisku. Proto bude jistě pro společnost škodlivější např. neoprávněné poskytování děl „zdarma" na serverech, a to za účelem odměn z reklam tam taktéž umístěných, než zaslání většího množství skladeb kamarádovi prostřednictvím e-mailu.

5.3. Místní působnost norem trestního práva a její specifika v případech internetové kriminality

Místní působností se rozumí území, na kterém trestní zákon působí své účinky. Vymezuje tak okruh případů (společenských vztahů), na které se trestněprávní norma vztahuje se zřetelem k místu, kde byl čin spáchán.[54] Při otázce, zdali se určité jednání pachatele bude posuzovat podle trestněprávní normy České republiky, bude třeba vždy zodpovědět, zdali

[54] Jelínek, J. a kol.: Trestní právo hmotné. Obecná část. Zvláštní část. 2. aktualizované vydání. Linde Praha, a.s., Praha 2006, str. 48

konkrétní trestný čin nebo jeho pachatel má určitý (kvalifikovaný) vztah k našemu státnímu území.

Jedním ze dvou základních principů v rámci určování působnosti českého trestního zákoníku je princip teritoriality (§ 4 tr.zák.), který stanoví, že: *Podle zákona České republiky se posuzuje trestnost činu, který byl spáchán na jejím území.* (§ 4 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 (§ 4 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 (§ 4 odst. 2 písm. b) tr.zák.).

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.[55]

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, internetová kavárna atd.). I zde však nalezneme určité problémy. Pokud totiž hacker napadne a vyřadí funkci webových stránek, které mohou být zpřístupněny odkudkoliv[56] a informace na nich obsažené mohou mít esenciální význam pro adresáty, je diskutabilní, 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 alespoň v případě českého trestního práva 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.).

---

[55] V podrobnostech např. Novotný, O., Vanduchová, M., Šámal, P. a kol.: Trestní právo hmotné. Obecná část. 6. vydání. Wolters Kluwer ČR, a.s., Praha 2010, s. 99 a násl.

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

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.[57]

Jak je výše uvedeno, trestní právo v ustanoveních o místní působnosti obsahuje obvykle široké podmínky svého uplatnění. Častější proto budou případy pozitivní konkurence trestních norem různých států.[58] Ze státní suverenity a (prozatím) národního charakteru trestního práva však může vyplynout situace, která bude vznášet pochyby o legitimitě širokých pravidel místní působnosti trestních norem toho kterého státu. Tak například si lze představit případ, že pachatel, občan Spojeného Království, umístí na své stránky registrované pod britskou doménou nejvyššího řádu („co.uk“) materiál propagující xenofobní a rasistické myšlenky. Z důvodu liberálního přístupu anglického práva ke svobodě projevu by takovýto materiál nebyl v Anglii, tedy místě pobytu našeho „pachatele“ i umístění serveru stránek, trestný. Na tyto stránky je však možný přístup z jakéhokoliv místa na zemi. Bude tedy možné našeho pachatele trestně postihnout např. podle polského práva, které takto liberálně na svobodu projevu nepohlíží?

Výše uvedený případ řešený německým Spolkovým soudním dvorem, pokud bychom jej analogicky vztáhli i na tuto věc, by odpověděl kladně. Rozdíl mezi oběma případy však lze spatřovat v tom, že Australan (mimochodem narozený v roce 1944 v Německu) v německém případě nejen provozoval „závadné“ webové stránky, ale tyto stránky měly „zvláštní“ vztah k Německu hned z několika důvodů. Jednak v podstatě popíraly holocaust a propagovaly nacismus, jednak autor čtvrtletně zasílal do Německa své periodikum, kde tyto myšlenky dále šířil. Webové stránky pak byly i díky těmto aktivitám pachatele německým občanům přístupnější, a i když psané v angličtině, byly jim určeny. Dovodit následek působící na německé občany tak bylo o poznání snazší, a s rozhodnutím Spolkového soudního dvora proto lze souhlasit.

V našem případě je ovšem situace trochu jiná. Náš Angličan, zcela neznalý polského trestního práva (proč by jej také znal), by žádné aktivity směrem k polským občanům nevyvíjel, jen by měl anglicky psané stránky, na které se lze z Polska připojit a které by bylo možné s trochou úsilí a anglického jazyka pomocí internetových vyhledávačů nalézt. Je jisté, že vzhledem k obecnému využívání angličtiny jako nejpoužívanějšího světového jazyka by

[57] Viz např. rozhodnutí německého Spolkového soudního dvoru ze dne 12. prosince 2000, sp.zn.: 1 StR 184/00, jehož shrnutí lze nalézt na: http://www.itpravo.cz/index.shtml?x=61318, v německém znění na: http://www.netlaw.de/urteile/bgh_04.htm

[58] Tj. případů, kdy určité jednání pachatele může být posouzeno jako trestný čin podle trestního práva více států.

se s obsahem takovýchto webových stránek mohlo seznámit mnoho Poláků. Měl by se proto náš pachatel obávat, že když odcestuje právě např. do Polska, že vzhledem k tamní trestnosti jeho jednání by ho mohla polská policie zatknout, aniž by o tom měl jedinou potuchu?

Asi vnímáme, že legitimita takto širokých podmínek působnosti trestních norem v kombinaci s přísnou zásadou *ignoratia legis non excusat* by v tomto případě neobstála. Ještě absurdněji by vyzněl v podstatě shodný případ pouze s tou obměnou, že autor stránek by byl např. Číňan hovořící ne příliš rozšířeným čínským dialektem a v tomto jazyce by byly i stránky napsány. Mohl by být autor těchto stránek postižen např. podle maďarského trestního práva jen proto, že tyto stránky by byly z Maďarska přístupné a čirou náhodou by se v Maďarsku nacházela jedna osoba, která tomuto jazyku rozumí a stránku by otevřela? Pokud bychom dospěli ke kladnému závěru, vedlo by to k ještě absurdnějším závěrům v tom, že podle trestního práva mnoha zemí jsou orgány činné v trestním řízení vázány zásadou oficiality a legality. Byly by tedy české orgány činné v trestním řízení nuceny zahajovat úkony trestního řízení proti právě takovýmto „čínským pachatelům“ jen proto, že jediný policista v celém sboru znalý čínského jazyka náhodou při brouzdání čínských webových stránek narazí na z hlediska českého trestního práva závadné stránky? Kladná odpověď by obratem znamenala hromadné porušování zákonných povinností orgánů činných v trestním řízení prakticky po celé republice.

Tato argumentace ad absurdum vede autora této práce k závěru, že široké podmínky působnosti trestních zákonů je třeba posuzovat citlivě a vždy s ohledem ke konkrétnímu případu a jeho schopnosti následek trestného činu v alespoň racionální minimální míře způsobit.

Shora uvedené úvahy nepředstavují pouze teoretický problém. Řešení místní působnosti trestních norem v případě internetové kriminality bude rovněž v popředí při využívání evropského zatýkacího rozkazu, který omezil požadavek oboustranné trestnosti vlastní institutu vydávání. Přitom je počítačová trestná činnost a jednání spočívající v rasismu a xenofobii obsažena ve výčtu čl. 2 odst. 2 Rámcového rozhodnutí Rady o evropském zatýkacím rozkazu[59] a § 412 odst. 2 tr.ř., které vypočítává ta kriminální jednání, u kterých právě není oboustranná trestnost vyžadována. Výklad extrémně rozšiřující podmínky uplatnění národních trestních zákonů by tak ve světle institutu předání mohl vést k nadměrnému vydávání evropských zatýkacích rozkazů a ve svém důsledku až

[59] Rámcové Rozhodnutí Rady č. 2002/584/SVV ze dne 13. června 2002 o evropském zatýkacím rozkazu a postupech předávání mezi členskými státy; CELEX 32002F0584

k šikanóznímu uplatňování trestního práva, a to i vůči občanům státu, kde takové jednání není vůbec trestné. Angličan z našeho případu by se pak jednoho dne mohl velice divit, že jej na území Spojeného Království zatknou a rozhodnou kvůli obsahu jeho stránek o předání k trestnímu stíhání do Polska, aniž by vůbec (oprávněně) předtím tušil, že jeho počínání je trestné. Skutečnost, že by si případný trest odpykal zpátky ve Velké Británii, by mu zřejmě nevykompenzovala pocit nespravedlivého odsouzení.

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 se pod internetovou kriminalitu řadí, a trestné činy, jejichž základní skutkovou podstatu mohou obvykle naplňovat.[60]

	Jednání	**Trestný čin dle tr.zák.**
1.	Hacking	Neoprávněný přístup k počítačovému systému a nosiči informací dle § 230 odst. 1, 2 tr.zák., opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat dle § 231 odst. 1 tr.zák.
2.	Phishing	Podvod dle § 209 odst. 1 tr.zák.
3.	Kyberterorismus	Teroristický útok dle § 311 odst. 1, 2 tr.zák., popř. sabotáž podle § 314 odst. 1 tr.zák. či obecné ohrožení dle § 272 odst. 2 tr.zák.

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

4.	Krádež (zneužívání) počítačového času a konektivity	Neoprávněné užívání cizí věci dle § 207 odst. 1 alinea 1, 2 tr.zák., krádež dle § 205 odst. 1 písm. a) tr.zák., neoprávněný přístup k počítačovému systému a nosiči informací dle § 230 odst. 1 tr.zák., opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat dle § 231 odst. 1 tr.zák.
5.	Šíření deviantní pornografie a zpřístupňování pornografie dětem	Šíření pornografie dle § 191 odst. 1, 2 nov.tr.zák., výroba a jiné nakládání s dětskou pornografií § 192 odst. 2 tr.zák.
6.	Propagace rasismu a xenofobie	Násilí proti skupině obyvatelů a proti jednotlivci dle § 352 odst. 1, 2 tr.zák., hanobení národa, rasy, etnické nebo jiné skupiny osob dle § 355 odst. 1, tr.zák., podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod dle § 356 odst. 1 tr.zák., popř. založení, podpora a propagace hnutí směřujícího k potlačení práv a svobod člověka podle § 403 odst. 1 tr.zák., projev sympatií k hnutí směřujícímu k potlačení práv a svobod člověka dle § 404 tr.zák., popírání, zpochybňování, schvalování a ospravedlňování genocidia podle § 405 tr.zák.
7.	Internetové pirátství, neoprávněné užití děl, softwarová krádež	Porušení autorských práv, práv souvisejících s právem autorským a práv k databázi dle § 270 odst. 1 tr.zák.
8.	Neoprávněné užívání obchodního jména, označení původu, uvedením do oběhu zboží nebo služeb neoprávněně označované ochrannou	Porušení práv k ochranné známce a jiným označením dle § 268 odst. 1, 2 tr.zák.

	známkou jiného	
9.	Počítačová špionáž	Vyzvědačství dle § 316 odst. 1, 2 tr.zák., popř. ohrožení utajované informace dle § 317 odst. 1 tr.zák.
10.	Neoprávněné internetové loterie a neoprávněné provozování gamblingových serverů a kybercasin	Neoprávněné provozování loterie a podobné sázkové hry dle § 252 odst. 1 tr.zák.
11.	Pomlouvání a lživé osočování na internetových serverech a fórech	Pomluva dle § 184 odst. 1 nov.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. Internet tak slouží jako skvělé místo publikace, výměny, šíření a opatřování těchto dat, ať už zdarma či za úplatu. Je navýsost zřejmé, že při těchto činnostech dochází ke střetu s právy duševního vlastnictví. Normy obsahující úpravu práv duševního vlastnictví, zejména pak normy autorskoprávní ochrany, jsou beze sporu nejčastěji porušovanými normami v prostředí internetu a četnost těchto protiprávních jednání jistě předčí i možná více obávané a diskutované hackerství. V této části práce 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 internet), jež by v jeden okamžik umožnilo přístup k dílu stovkám miliónů lidí na celém světě (počet uživatelů internetu byl k 31.12.2012 přes 2,25 mld.)[61].

2. Rapidní technologický pokrok v hardware, který umožnil na jedné straně zvyšování kapacity disků serverů[62] při jejich současné miniaturizaci a na druhé straně růst kapacity připojení (konektivity). Ještě před zhruba deseti lety byla většina uživatelů internetu v České republice připojena pomocí vytáčeného analogového telefonního připojení s maximální rychlostí 8 kB/s,[63] avšak často s hodnotou výrazně nižší. Toto připojení umožňuje návštěvu

[61] Viz pozn. č. 12

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

[63] 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 („b“). 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)

nenáročných webových stránek, vzhledem k blokaci telefonní linky a zároveň jeho nákladnosti však neumožňuje stahování většího objemu dat. Rozmach vysokorychlostních připojení (ADSL, Ethernet, WiFi)[64] s rychlostí často přesahující 1MB/s umožnil přístup 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 mnoha 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 označovaných „save harbours“[65] s nízkou nebo mizivou ochranou práv duševního vlastnictví, jako je jihovýchodní Asie, země bývalého SSSR, oblast Karibiku, atd. Na tomto místě je však třeba poznamenat, že počet těchto bezpečných přístavů se neustále snižuje s rostoucím standardem úpravy ochrany autorských práv v některých zemích ve zmiňovaných oblastech.[66]

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 internetu chránit druhotně pomocí hmotného předmětu (nosiče), prostřednictvím něhož je vyjádřeno, tak, jako je tomu například u originálních optických 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. Tento negativní vztah v posledních letech vygradoval i s růstem autorských

---

[64] ADSL = vysokorychlostní připojení pomocí telefonních linek
Ethernet = vysokorychlostní připojení pomocí lokální sítě (nejčastěji LAN) propojené kabelem, typické pro tzv. „kabelové připojení“
WiFi = bezdrátové připojení pomocí mikrovlnného elektromagnetického záření

[65] Tzv. bezpečné přístavy

[66] Ke změnám v právních úpravách ochrany autorských práv v některých zemích jihovýchodní Asie srov. např. Woo, M., Lui, V.: New copyright Bill for Hong Kong; Hong Kong releases Copyright (Amendment) Bill 2006 in: Computer Law & Security report. Vol. 22. Elsevier Science B.V., 2006, s. 418 – 420 a Tang, G., H.: Is administrative enforcement the answer? Copyright protection in the digital era in: Computer Law & Security report. Vol. 26. Elsevier Science B.V., 2006, s. 412 a násl.

poplatků z paměťových médií[67], které spotřebitelé mohli vnímat v podstatě jako kompenzace autorů za ztráty na odměně způsobené porušováním autorských práv.[68]

I když k masivnímu porušování autorských práv[69] docházelo od samého počátku vzniku internetu (drtivá většina webových stránek, resp. jejich tvůrci, totiž určitým způsobem autorská práva porušují, když ke zvýšení atraktivity svých stránek za účelem jejich vyšší návštěvnosti a následně zisku z reklam na nich umístěných využívají cizí obrázky, ikonky, texty, zvuky, videoklipy a jiné prvky bez souhlasu jejich autora), následky tohoto porušení nebyly často natolik závažné, aby oprávněné osoby hájily svá autorská práva soukromoprávními žalobami na základě odpovědnosti delikventa, natož pak aby, vzhledem k subsidiaritě trestní represe, bylo šíře využíváno institutů trestního práva.

V poslední době se však, z důvodů výše uvedených, 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 porušení autorských práv představuje natolik společensky škodlivé jednání, že se již případná civilní odpovědnost jeví být nedostatečnou a na místě je trestní postih pachatelů tohoto porušování.

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 (její soukromoprávní aspekty) je v českém právním řádu 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 citovaného zákona definován tak, že: *Právo autorské*

---

[67] Novela prováděcí vyhlášky stanovící sazby těchto poplatků z roku 2008 sice tento nárůst opět omezila stanovením maximálních výší těchto poplatků, to však již nemohlo mít vliv na subjektivní pocit spotřebitelů, že autorům platí i za prázdné nosiče.

[68] Shodně např. Minárik, T.: Peer-to-peer sítě z hlediska trestního práva in: Gřivna, T. (ed.): Český právní řád a ochrana kyberprostoru. 1. vydání. Karolinum, Praha 2008, s. 69

[69] 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 zvukově obrazového záznamu, nakladatele, vysílatele a tvůrce databáze

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 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 uměleckého díla 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, výrobků či součástek 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 a účasti na 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

Aby mohly být vytvořeny preventivní nástroje ochrany před tímto druhem kriminality, je třeba pochopit i způsob jednání (*modus operandi*), jakým k porušení autorských práv na internetu dochází.

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 způsobem je pak sdílení 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 zpřístupněním, tedy určitá forma účastenství, a to 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.

S tímto druhem kriminality úzce souvisí téma tzv. kybersquattingu, tedy registrace internetových domén nesoucích název např. známých osobností či parazitujících na dobrém jménu (značce) úspěšných obchodníků v očekávání, že tito následně předmětnou doménu od registrující osoby velice draho odkoupí. Ačkoliv tyto aktivity rozhodně nelze nazvat společensky prospěšné a ve valné většině případů se bude jednat o jednání protiprávní, což i v našich podmínkách bylo shledáno z hlediska českého práva i ze strany soudů,[70] nebude odpovědnost za tato jednání obvykle spočívat v trestním právu. V úvahu sice přichází posoudit kybersquatting jako trestný čin porušení předpisů o pravidlech hospodářské soutěže podle § 248 odst. 1 tr.zák., event. jako trestný čin porušení práv k ochranné známce a jiným označením podle § 268 odst. 1, 2 tr. zák, ovšem v daném případě dostatečnou úpravu právní odpovědnosti poskytují ustanovení obchodního zákoníku na ochranu firmy, obchodního označení či proti nekalé soutěži a také zákona o ochranných známkách. Z hlediska požadavku subsidiarity trestní represe tak budou jako trestné posuzovány jen případy nejzávažnější, kdy bude docházet k porušování pravidel na ochranu hospodářské soutěže ve velkém rozsahu. Zejména z kapacitních důvodů se proto autor rozhodl kybersquattingem v další části práce nezaobírat a v podrobnostech o tomto fenoménu odkazuje na jiné prameny.[71]

---

[70] Jako přelomový lze označit rozsudek Krajského soudu v Brně ze dne 7.5.2003, č.j. 11 Cm 8/2003-45 o užívání doménového jména „tina.cz“, jenž je podrobně analyzován ve Smejkal, V. a kol.: Právo informačních a telekomunikačních systémů. 2. aktualizované a rozšířené vydání. C.H.Beck, Praha 2004, s. 613 a násl.

[71] Velmi podrobně o problematice kybersquattingu a konkrétních soudních případech z hlediska práva USA viz Gutierrez, O., R.: Get Off My URL!; Congress Outlaws Cybersquatting in the Wild West of the Internet in: Santa Clara Computer & High Technology Law Journal. vol. 17. Santa Clara University, Santa Clara 2000, s. 139 a násl.

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[72]), 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 citovaného ustanovení 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 závažnějším 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[73] sítích se stalo v posledních letech velice aktuálním problémem. Se sílejícím tlakem ze strany autorit a zábavního průmyslu na provozovatele centrálních serverů s obsahem porušujícím autorská práva postupně docházelo k jejich rušení nebo přesunutí do zemí s nízkou ochranou autorských práv (viz kapitola 1.1 Zvláštní části). Tento proces však nesnížil neutuchající poptávkou po získání děl zdarma či za minimální cenu bez ohledu na dodržování autorských práv. Z toho důvodu došlo k přesunu těchto „zájemců“

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

[73] 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“

k technologii peer to peer, které centrální server buď úplně postrádají, nebo plní pouze evidenční roli, a proto znesnadňují efektivnímu zakročení proti nim ze strany autorit.[74]

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[75] 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.[76]

Centrální server však byl i největší slabinou tohoto systému, když 12. června 2000 podala RIAA[77] na Napster žalobu o náhradu škody. Soud Napster shledal spoluodpovědným

[74] O masovém porušování prostřednictvím peer to peer sítí hovoří i Minárik v Minárik, T.: op. cit., s. 65
[75] Tj. zpřístupní určitý objem dat pro ostatní uživatele sítě ke stažení
[76] Wikipedia; http://en.wikipedia.org/wiki/Image:Napster_Unique_Users.svg; zobrazeno 13.7.2008, 22:18
[77] Recording Industry Association of America

(contributory copyright liability) a tzv. zástupně odpovědným (vicarious copyright liability)[78] z porušování autorského práva uživateli systému (87,1 % všech děl přístupných v této síti bylo chráněno určitým způsobem autorskými právy a cca 70 % všech děl byly zvukové záznamy vytvořené členy RIAA)[79] 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.[80]

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 pracujícího s tzv. torrenty (Bittorrent).[81] 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 pouze vyhledá soubor pod známým jménem a stáhne na svůj počítač. Původní poskytovatel tak ztrácí zcela kontrolu nad jím poskytnutým souborem a lze ho i velice obtížně vystopovat. Typickým představitelem tohoto systému je projekt Freenet.[82]

---

[78] 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., dále Wells, C.: Corporations and criminal responsibility, 2nd edition, Oxford 2001

[79] Srov. Rozhodnutí United States District Court for the Northern District of California ve věci A&M Records, Inc. et. al. v. Napster, sp.zn. CV 99-5183 MHP, C 00-0074 MHP, bod 5 odůvodnění a pozn. č. 6 tohoto rozhodnutí

[80] Wikipedia; http://en.wikipedia.org/wiki/Napster; zobrazeno 14.8.2012, 21:10

[81] Podrobné vysvětlení rozdílů těchto a dalších systému přesahuje rámec této práce, 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

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

1.3.2.3. Poskytování odkazu

Poskytování odkazu je určitou formou účasti na porušování práv způsobených 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 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, které se na těchto stránkách vyskytují. 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 minimálně srozuměni, že odkazy na jejich stránkách přímo vedou k neoprávněně poskytovaným autorským dílům.[83]

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. Při aktivaci na uživatelově obrazovce tak 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 věta prvá

[83] 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

AutZ), dochází při každém užití (sdělování díla veřejnosti) bez souhlasu autora odkazovaného díla k porušování autorských práv (§ 2 ve spojení s § 18 odst. 1, 2 AutZ).[84]

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 shodné 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[85]

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 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).[86] 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).

[84] 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)

[85] Dále v této souvislosti jen „počítačové programy“ či „programy“

[86] 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

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 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 Evropského společenství

(dnes právem Evropské unie),[87] bylo přímo do znění zákona vloženo, že se musí jednat o osobní potřebu fyzické osoby. Starší úprava toto zpřesnění neobsahovala a jurisprudence někdy rozšiřovala tento pojem i na „vnitřní potřebu právnické osoby".[88]

Obsah pojmu „osobní potřeba" lze shrnout následovně:

1. Jde o potřebu koncového uživatele internetu, nikoliv pro potřebu 3. osoby.
2. Nejedná se o komerční účel.
3. Staženým dílem není počítačový program ani elektronická databáze
4. Stažení díla nesmí být na újmu oprávněným zájmům autora
5. Dle čl. 5 odst. 2 písm. b) Informační směrnice musí nositelé práv z tohoto zákonného omezení získat spravedlivou odměnu.[89]

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

V praxi nebyl vždy jednotný názor, zdali je možné zhotovit pro osobní potřebu pouze jednu či více rozmnoženin. Ačkoliv je v ustanovení § 30 odst. 2 AutZ užit singulár, je toto připisováno pouze legislativní technice, neboť legislativní právní jazyk hovoří zásadně v jednotném čísle. Argumentací ad absurdum však lze dojít k závěru, že pokud počet rozmnoženin nepřesáhne stanovenou (rozumnou) míru, může jich být takto vyhotoveno více.[90]

1.3.4. Porušování autorských práv týkající se účinných technických prostředků ochrany.

Jelikož s rozvojem internetu dochází k 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 od jejího zavedení, viz příloha č. 2.

---

[87] Čl. 5 odst. 2 písm. b) Informační směrnice (2001/29/ES)
[88] Např. Telec, I.: Autorský zákon. Komentář. 1. vydání. C. H. Beck, Praha 1997
[89] V ČR provedeno ust. § 25 AutZ
[90] Blíže viz Telec, I., Tůma, P.: Autorský zákon, 1. vydání. C. H. Beck, Praha 2007, s. 347

Jak vznik protikopírovací ochrany a jiných účinných technických prostředků ochrany práv autorů, tak jejich překonávání mělo záhy odraz v platné právní úpravě. V českém právním 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 společností je ale někdy nutí uchýlit se až k drastickým prostředkům, jejichž použití je taktéž protiprávní, a dokonce může nabývat formy trestné činnosti. 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 nainstalovala jako rootkit.[91] 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.[92]

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

[91] Více k tomuto v hlavě 2. Hackerství
[92] Podrobně k tomuto viz např. časopis CHIP.CZ, č.2/2006, s. 16

nazvaná Trestní odpovědnost naopak popisuje, kdy jsou výše uvedená jednání postižitelná z hlediska trestní odpovědnosti.

1.4.2. Subsidiarita trestní represe v případě porušování autorských práv

O subsidiaritě trestní represe, tedy o škodlivosti činu pro společnost a zásadě trestu jako ultima ratio, 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 škodlivosti porušování autorských práv:

Při zkoumání povahy a závažnosti 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 škodlivější. Majetková újma totiž prakticky vždy může být nahrazena, v případě morální a jiné psychické újmy tomu tak být nemusí.

Dalším hlediskem společenské škodlivosti 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 toto hledisko 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.

1.4.3. Skutková podstata trestného činu podle § 270 tr.zák.

K určení trestní odpovědnosti pachatele je nutné subsumovat jednání, jakými 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 § 270 tr.zák. upravující skutkovou podstatu trestného činu porušování autorského práva, práv souvisejících s právem autorským a práv k databázi**.**

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

§ 152
Porušování autorského práva, práv souvisejících s právem autorským a práv k databázi
(1) Kdo neoprávněně zasáhne nikoliv nepatrně 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, peněžitým trestem nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán,
a) vykazuje-li čin uvedený v odstavci 1 znaky obchodní činnosti nebo jiného podnikání,
b) získá-li takovým činem pro sebe nebo pro jiného značný prospěch nebo způsobí-li tím jinému značnou škodu, nebo
c) dopustí-li se takového činu ve značném rozsahu.
(3) Odnětím svobody na tři léta až osm let bude pachatel potrestán,
a) získá-li činem uvedeným v odstavci 1 pro sebe nebo pro jiného prospěch velkého rozsahu nebo způsobí-li tím jinému škodu velkého rozsahu, nebo
b) dopustí-li se takového činu ve velkém rozsahu.

Tento trestný čin je systematicky zařazen mezi trestné činy hospodářské do hlavy šesté zvláštní části trestního zákona, konkrétněji do dílu čtvrtého – trestné činy proti průmyslovým právům a proti autorskému právu.

1.4.3.1. Základní skutková podstata TČ podle § 270 tr.zák.

Ze znění § 270 odst. 1 tr.zák. vyplývá, že zákonodárce se v případě tohoto trestného činu (podobně jako u většiny trestných činů upravených v tomto díle trestního zákoníku) rozhodl využít úpravy formou blanketní (blanketové) normy. Blanketní norma trestního práva je taková norma, která sama pravidlo chování přímo neobsahuje (popřípadě obsahuje pouze jeho část), ale ve své dispozici odkazuje obecně na normu či více norem stejného druhu obsaženou v jiném právním předpise (jiných právních předpisech), aniž by tento byl v blanketní normě samé identifikován,[93] 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.

[93] Srov. Knapp, V.: Teorie práva. 1. vydání. C. H. Beck, Praha 1995, s. 160

V komunitárním[94] právu je z hlediska pramenů autorského práva podstatná zejména Informační směrnice (2001/29/ES), Směrnice 2009/24/ES 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.[95] Vzhledem k tomu, že ochrana těchto zájmů je primárně zajištěna normami soukromého práva (AutZ, občanský zákoník, obchodní zákoník), je vždy nutné z hlediska pomocné role trestní represe vždy pečlivě uvážit, 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.

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). V dané věci však nepostačí jakýkoli zásah, ale k trestní odpovědnosti bude třeba zasáhnout do zákonem chráněných autorských práv nikoli nepatrně. Zákonodárce se tak v novém trestním zákoníku snažil promítnout do tohoto ustanovení, které chrání zájmy primárně soukromoprávní, nové formální pojetí trestního zákoníku tím, že do základní skutkové podstaty vložil oproti původnímu znění v trestním zákoně č. 140/1961 Sb. tuto minimální hranici míry zásahu do autorských práv nutnou k trestní odpovědnosti.[96]

Pachatelem může být jakákoliv fyzická i právnická 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 rozšířena 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 (§ 13 odst. 2 ve spojení s § 270 odst. 1 tr.zák., arg. a contrario).

---

[94] Od účinnosti tzv. Lisabonské smlouvy byla třípilířová struktura Evropské unie sloučena a nadále se hovoří pouze o právu Evropské unie. V dalším textu proto budou uváděny pouze termíny „právo Evropské unie“, „unijní právo“ či „právo EU“

[95] Jelínek, J. a kol.: Trestní právo hmotné. 2. vydání. Leges, Praha 2010, s. 676

[96] K tomu srov. § 152 odst. 1 trestního zákona č. 140/1961 Sb., v posledním znění

Právem autorským nejsou obecně dotčena práva s autorským právem související, jejich ochrany se uplatňují vedle sebe a jedním skutkem tak pachatel může porušovat práva jak autorů, tak výkonných umělců, výrobců zvukových a audiovizuálních záznamů i televizních vysílatelů (např. neoprávněné vysílání záznamu koncertů popové zpěvačky).[97] Jelikož teorie ani praxe obecně neuznává jednočinný souběh stejnorodý, půjde tak o trestný čin jediný, jeho společenská škodlivost však bude pochopitelně vyšší.

1.4.3.2. Kvalifikovaná skutková podstata TČ podle § 270 odst. 2 a 3 tr.zák.

Kvalifikovaná skutková podstata vyjádřená v § 270 odst. 2 tr.zák. obsahuje tři okolnosti podmiňující použití vyšší trestní sazby. První podmiňuje své použití tím, že zásah do autorských práv vykazuje znaky obchodní činnosti nebo jiného podnikání (§ 270 odst. 2 písm. a) tr.zák.). Druhá spočívá v získání tímto trestným činem značného prospěchu nebo způsobení značné škody (§ 270 odst. 2 písm. b) tr.zák.). Třetí okolností podmiňující použití vyšší trestní sazby je pak páchání této trestné činnosti ve značném rozsahu. Při naplnění této kvalifikované skutkové podstaty pachateli hrozí trest odnětí svobody v délce trvání 6 měsíců až 5 let.

V třetím odstavci § 270 tr.zák. jsou upraveny dvě zvláště přitěžující okolnosti, a to získání činem prospěchu (popř. způsobení škody) ve velkém rozsahu a spáchání takového činu ve velkém rozsahu. V tomto odstavci hrozí pachateli sazba trestu odnětí svobody od tří do osmi let.

1.4.3.2.1. Porušování vykazující znaky obchodní činnosti

Porušování autorských práv vykazující znaky obchodní činnosti nebo podnikání bylo jako okolnost podmiňující použití trestní sazby zavedeno až s novým trestním zákoníkem, původní trestní zákon z roku 1961 obdobné ustanovení ani v roce 2009 neobsahoval. Dle důvodové zprávy k trestnímu zákoníku byla tato zvláště přitěžující okolnost zavedena v návaznosti na připravovanou směrnici Evropského parlamentu a Rady o trestních opatření k prosazování práv duševního vlastnictví (2005/0127/COD),[98] která používá termín „v obchodním měřítku“, jenž měl být z hlediska českého práva zákonodárcem shledán jako vágní. Uvedené tvrzení je však typickým příkladem zastírání důvodu přijetí určité normy požadavkem práva EU či mezinárodní smlouvy. Návrh směrnice totiž žádnou povinnost

[97] Viz např. rozsudek Nejvyššího soudu ČR ze dne 13.6.2001, sp.zn. 5 Tz 75/2001 publikovaný v časopise Právní rozhledy, č. 11/2001, s. 563
[98] Důvodová zpráva k § 266 – 268 (dnes 268 – 270) vládního návrhu trestního zákoníku, Poslanecká sněmovna Parlamentu České republiky, 5. volební období, 2006-2010, sněmovní tisk č. 410/0

k zavedení přísnějšího postihu v případě porušování autorských práv v obchodním měřítku neobsahoval, pouze v čl. 3 tohoto návrhu[99] stanovil, že Členské státy musí zajistit, aby bylo za trestné jednání označeno jakékoliv úmyslné porušení práva duševního vlastnictví v obchodním měřítku a také jakýkoliv pokus o takové porušení, spolupachatelství při něm a návod k takovému porušení. Tento návrh směrnice tedy požadoval, aby členské státy zavedly trestní postih minimálně v těch případech, kdy trestná činnost bude vyvíjena v obchodním měřítku. Již původní úprava takovýto požadavek zcela splňovala, neboť jako trestné označovala v podstatě každý (při naplnění materiálního znaku společenské nebezpečnosti) neoprávněný zásah do autorských práv, nikoliv jen takový, který byl spáchán v obchodním měřítku. K tomu je potřeba poznamenat, že výše uvedený návrh se nikdy nedočkal realizace v podobě přijetí směrnice, a ani se ho nedočká, neboť byl k 18.9.2010 vzat jako bezpředmětný zpět Evropskou komisí.[100] V právním rámci EU by měl být návrh této směrnice nahrazen přijetím a ratifikací Obchodní dohody proti padělatelství (tzv. úmluvou ACTA),[101] která sice obsahuje obdobné ustanovení, avšak i zde se pouze jedná o zavedení trestnosti alespoň v případě zásahů do autorského práva v komerčním měřítku, a navíc i budoucnost úmluvy ACTA je minimálně nejistá, když v nedávné době byl návrh na její uzavření zamítnut Evropským parlamentem.[102]

Lze proto uzavřít, že zavedení této okolnosti podmiňující použití vyšší trestní sazby bylo motivováno jinými důvody než nastíněnými v důvodové zprávě. Můžeme se jen dohadovat, zda se tak nestalo na základě lobbingu např. kolektivních správců autorských děl. Na druhou stranu je možné vyšší diverzifikaci okolností podmiňujících vyšší trestní sazby u tohoto trestného činu hodnotit kladně, neboť tak lze lépe vystihnout vyšší typovou závažnost jednotlivých činů. Je přitom nesporné, že pokud zásahy do autorských práv vykazují znaky obchodní činnosti a nejedná se pouze o nahodilé porušování nekomerčních fyzických osob, jsou tyto zásahy jistě typově závažnější a zasluhují vyšší trestní postih.

---

[99] Návrh je dostupný pod CELEXovým číslem 52005PC0276(01) na EUR-Lex; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52005PC0276(01):CS:NOT, zobrazeno 15.11.2011, 18:05

[100] Sdělení Evropské komise o stažení bezpředmětných návrhů Komise ze dne 18.9.2010, č. 2010/C 252/04, CELEX: 52010XC0918(02)

[101] Návrh ROZHODNUTÍ RADY o uzavření Obchodní dohody proti padělatelství mezi Evropskou unií a jejími členskými státy, Austrálií, Kanadou, Japonskem, Korejskou republikou, Spojenými státy mexickými, Marockým královstvím, Novým Zélandem, Singapurskou republikou, Švýcarskou konfederací a Spojenými státy americkými ze dne 24.6.2011, č. KOM/2011/0380, CELEX: 52011PC0380

[102] K tomu srov. Pre Lex; Sledování rozhodovacího procesu mezi orgány EU k návrhu; http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=cs&DosId=200616, zobrazeno 10.8.2012, 20:55 a oznámení Evropského parlamentu k zamítnutí návrhu dne 14.7.2012 na http://www.europarl.europa.eu/oeil/popups/summary.do?id=1214659&t=e&l=en, zobrazeno 10.8.2012, 21:05

1.4.3.2.2. Určování výše neoprávněného prospěchu a škody

Pro určení výše prospěchu v ustanovení § 270 odst. 2 písm. b) a c) tr.ř. se dle výkladového ustanovení § 138 odst. 2 užije obdobně odst. 1 téhož ustanovení týkající se výše škod. Z toho důvodu se získáním značného prospěchu rozumí zisku částky nejméně 500.000,- Kč a u prospěchu velkého rozsahu částky nejméně 5.000.000,- Kč. Složitější je však výklad pojmu „značný rozsah" a „velký rozsah", neboť tento pojem tr.zák. nevykládá a nelze bez dalšího říci, že se analogicky užijí hodnoty pro výši škody (už jen proto, že v trestním právu hmotném je analogie *in malam partem*[103] 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 § 138 odst. 1 tr.zák.[104]

V případě porušování autorských práv v síti internetu ovšem často nastává základní problém aplikace těchto okolností podmiňujících použití vyšší trestní sazby, a to určení konkrétní výše prospěchu a škody. To je způsobeno poměrně specifickou úpravou náhrady škody a vydání bezdůvodného obohacení v autorském zákoně, která vyvolává otázky i mezi vědeckými autoritami soukromého práva.

Náhrada škody a bezdůvodného obohacení je v autorském zákoně uvedena v § 40 odst. 4, ve kterém je ohledně úpravy náhrady škody a bezdůvodného obohacení odkazováno na zvláštní právní předpisy, zejména tedy občanský zákoník (§ 420 a násl.). V následující části za středníkem tohoto ustanovení je stanoven způsob určení výše škody a bezdůvodného obohacení.[105] Škoda se obecně skládá ze dvou složek, a to skutečné škody (*damnum emergens*) a ušlého zisku (*lucrum cessans)*. Z povahy autorského práva bude prakticky vyloučeno, aby zásahem do autorského práva došlo ke vzniku skutečné škody, tedy snížení hodnoty tohoto práva (jeho zničení či poškození). S tím ostatně i autorský zákon počítá, když obsahuje pouze ustanovení o způsobu určení výše ušlého zisku, nikoliv skutečné škody. Ten, komu bylo do autorského práva zasaženo, se tak bude moci domáhat jak ušlého zisku, tak bezdůvodného obohacení na straně toho, kdo dílo neoprávněně užíval (popř. jinak zasáhl do práva autora). Vyvstává proto otázka vzájemného vztahu ušlého zisku a bezdůvodného obohacení.

---

[103] V neprospěch pachatele

[104] Jelínek, J. a kol.: Trestní právo hmotné. 2. vydání. Leges, Praha 2010, s. 174

[105] *„Místo skutečně ušlého zisku se autor může domáhat náhrady ušlého zisku ve výši odměny, která by byla obvyklá za získání takové licence v době neoprávněného nakládání s dílem. Výše bezdůvodného obohacení vzniklého na straně toho, kdo neoprávněně nakládal s dílem, aniž by k tomu získal potřebnou licenci, činí dvojnásobek odměny, která by byla za získání takové licence obvyklá v době neoprávněného nakládání s dílem.*"

Komentář k autorskému zákonu[106] poměrně striktně zastává názor, „že náhrada autorské odměny ušlé neoprávněným užitím díla je nárokem z odpovědnosti za bezdůvodné obohacení, a nikoli odpovědnosti za škodu.“ Náhrada ušlého zisku pak bude přicházet v úvahu jen v ojedinělých případech, kdy neoprávněným zásahem do autorského práva nevznikne na straně narušitele obohacení. Telec a Tůma uvádí příklad, kdy třetí osoba v důsledku neoprávněného prvního vydání díla autora škůdcem ztratí zájem o vlastní vydání tohoto díla, pročež tak autor přijde o zisk – odměnu za toto první vydání.[107] V takovém případě by podle obou autorů došlo k jednočinnému souběhu náhrady škody (ušlý zisk za první vydání třetí osobou) a bezdůvodnému obohacení škůdce v podobě prospěchu z neoprávněného prvního vydání. Tento názor opírají jednak o to, že bezdůvodné obohacení obsahuje krom společných znaků bezdůvodnosti a úkoru oproti náhradě škody znak obohacení (otázku zavinění nechejme stranou), a proto je na něj třeba pohlížet jako na speciální právní institut vůči náhradě škody. Druhou oporu k uvedenému závěru shledává Telec a Tůma ve dvou rozhodnutích Nejvyššího soudu ČR, sp.zn. 4 Tz 124/2004 a 5 Tdo 160/2005, ve kterých se uvádí, že ke škodě nemohlo dojít, neboť narušovatel (obžalovaný) neměl s kolektivními správci autorských práv uzavřenou žádnou licenční smlouvu. Obžalovaný se tak pouze bezdůvodně obohatil.

Pokud bychom dali za pravdu uvedeným názorům, že ušlá odměna autora v případě neoprávněného užití je pouze bezdůvodným obohacením, znamenalo by to v podstatě, jak trefně (s nadsázkou) uvádí Minárik,[108] že porušování autorských práv nikomu neškodí. Autor této práce však s tímto absurdním závěrem, na rozdíl od všech jmenovaných autorů, nesouhlasí, a to hned z několika důvodů. První z nich (neprávní) vyplývá pouze ze „selského rozumu“. Je totiž zjevné, že porušování autorských práv škodí autorům, kteří přicházejí o licenční odměny.

Druhý (a nejzásadnější) argument plyne z teorie soukromého práva a praxe civilních soudů, které už po dlouhá léta setrvávají na názoru, že institut bezdůvodného obohacení má subsidiární povahu. Právní vztah tak může být podle něj posouzen, jen jestliže nárok nevyplývá z jiného zákonného ustanovení. Nárok z odpovědnosti za bezdůvodné obohacení může být proto opodstatněn toliko tehdy, jestliže povinnost vydat přijaté plnění neupravuje jiný právní titul, například náhrada škody.[109] K tomu Švestka a kol. dodává, že: „V případech

[106] Telec, I., Tůma, P.: op. cit., s. 433 a násl.
[107] Idem, s. 433
[108] Minárik, T.: op. cit., s. 72
[109] K tomu srov. např. Švestka, J., Spáčil, J., Škárová, M., Hulmák, M. a kol.: Občanský zákoník I, II. 2. vydání. C. H. Beck, Praha 2009, s. 1324, dále Rozsudek Nejvyššího soudu ČR ze dne 25. 3. 2008,

obohacení získaného trestným činem budou zřejmě splněny předpoklady odpovědnosti pachatele za způsobenou škodu. Ustanovení o bezdůvodném obohacení se proto uplatní zejména tam, kde pro nedostatek zavinění (např. pro nepříčetnost) nelze dovodit odpovědnost za škodu, nebo v případech, kde poškozeným je neznámá osoba apod.“

Uplatnění tohoto obecného pravidla i pro oblast autorského pravidla ostatně vyplývá z návětí § 40 odst. 4 AutZ, dle kterého se na náhradu škody i bezdůvodné obohacení uplatní zvláštní právní předpisy, tedy zejména ObčZ a ObchZ. Nárok na náhradu autorské odměny ušlé neoprávněným užitím díla z titulu náhrady ušlého zisku tedy bude mít přednost před náhradou z titulu bezdůvodného obohacení, pokud budou tyto nároky mít stejný skutkový základ (ušlá autorská odměna za neoprávněné užití díla na jedné straně a neoprávněný majetkový prospěch z nezaplacení autorské odměny).

Je zajímavé, že citovaný komentář AutZ, tedy soukromoprávního předpisu, opírá své závěry o dvě rozhodnutí trestního oddělení Nejvyššího soudu ČR, nikoliv o rozhodnutí ve věcech civilních. Autor této práce, aniž by chtěl pochybovat o orientaci trestních soudců Nejvyššího soudu ČR v civilní problematice, se nemůže se závěry ohledně bezdůvodného obohacení neoprávněných uživatelů autorských děl ztotožnit. Nejvyšší soud k tomuto závěru dospěl úvahou, že (v konkrétní věci) mezi autorem, resp. kolektivním správcem, a neoprávněným uživatelem autorského díla není uzavřena žádná licenční smlouva, a proto nevyplývá pro autora povinnost licenční odměnu zaplatit. Jelikož toto právo není absolutní povahy, nýbrž relativním nárokem ze smluvního vztahu, musí se jednat na straně neoprávněného uživatele o bezdůvodné obohacení. Tato úvaha je však zavádějící, neboť kdyby mezi neoprávněným uživatelem a kolektivním správcem autorských práv licenční smlouva byla uzavřena, vymáhala by se povinnost k úhradě odměny primárně právě ze smlouvy, nikoliv z titulu náhrady škody (resp. z tohoto titulu až druhotně).

Navíc uvedený názor přehlíží skutečnost, že škoda nemusí vždy vznikat porušením smluvní povinnosti, ale i zákonné, jako je tomu v tomto případě. Zároveň je i zachována příčinná souvislost mezi vznikem škody (konkrétně ušlým ziskem) a porušením povinnosti, tj. neoprávněným užitím díla. Kdyby totiž bylo dílo užito oprávněně, tj. na základě licenční smlouvy, byl by uživatel povinen zaplatit příslušnou licenční odměnu a autor by o zisk nepřišel. K tomu dochází implicitně i Tůma a Telec v uvedeném komentáři, a proto dovozuje bezdůvodné obohacení z absence znaku „obohacení“ u náhrady škody.[110] Konečně je třeba

---

sp.zn. 33 Odo 79/2006 dostupný na adrese http://www.nsoud.cz a Stanovisko Nejvyššího soudu ČSR ze dne 28. 3. 1975, sp.zn. Cpj 34/74, bod A I., publikováno pod č. R 26/1975 civ.

[110] Telec, I., Tůma, P.: op. cit., s. 433 a násl.

poznamenat, že obě zmíněná rozhodnutí byla vyhlášena před novelizací ustanovení § 40 provedené velkou novelou autorského zákona č. 216/2006 Sb., která konkretizovala možnost výpočtu výše ušlého zisku, předchozí úprava se o ušlém zisku vůbec nezmiňovala. Rovněž pak byla vydána ještě před platností a účinností nového trestního zákoníku, přičemž původní úprava tohoto trestného činu se škodou jako zvláště přitěžující okolností vůbec nepočítala.

Nezbývá proto než uzavřít, že v případech, kdy je neoprávněně užito dílo, k jejímuž užití by autor nedával bezúplatnou licenci, vzniká na straně autora škoda v podobě ušlého zisku (odměny), kterou může po neoprávněném uživateli požadovat z titulu náhrady škody. Konkrétní výše nároku pak závisí na vůli autora, a to v tom směru, zdali se bude snažit prokázat skutečnou výši ušlého zisku, což může být velmi obtížné, nebo se spokojí s určením výše daným fikcí v § 40 odst. 4 věta za středníkem AutZ, tedy ve výši odměny, která by byla obvyklá za získání takové licence v době neoprávněného nakládání s dílem.

Zároveň by ovšem mohl po narušiteli požadovat i bezdůvodné obohacení, a to v tom případě, kdyby neoprávněný uživatel na autorském díle dále profitoval, například je umístil na své webové stránky, aby zvýšil jejich návštěvnost, a těžil tak ze zvýšených příjmů z reklam na nich rovněž umístěných. Výše takovéhoto bezdůvodného obohacení, pokud k nějakému dojde, je dána kogentně fikcí ve výši dvojnásobku odměny, která by byla za získání potřebné licence obvyklá v době neoprávněného nakládání s dílem. Má tak i sankční charakter.

Výše uvedeného úvahy jsou zcela zásadní pro trestní kvalifikaci neoprávněného zásahu do autorských práv. Právě obě dvě kategorie budou totiž základním kritériem pro určení, zdali pachatel rovněž naplnil kvalifikovanou skutkovou podstatu TČ podle § 270 odst. 2 písm. b) či odst. 3 písm. a) tr.zák. V případě výše škody se bude muset vycházet ze škody skutečné, ta se ovšem při přiměřeném použití postupu pro stanovení výše škody na věci podle § 137 in fine tr.zák. bude pravděpodobně určovat jako obvyklá cena licence v době a místě páchání trestného činu.

U neoprávněného prospěchu se bude muset vycházet z fikce dané AutZ pro bezdůvodné obohacení, tedy ve výši dvojnásobku obvyklé odměny, ovšem po odečtení jeho nákladů na tento prospěch.[111]

[111] K tomu srov. Jelínek, J. a kol.: Trestní zákoník a trestní řád s poznámkami a judikaturou. 1. vydání. Leges, Praha 2009, s. 168

Na druhou stranu nebude vždy jednoduché určit rozsah zásahu do autorských práv konkrétním kyberzločinem. To platí, zejména pokud pachatelův primární motiv nebylo získání peněžního prospěchu (typicky peer to peer sítě). Nelze totiž říci, že „značný či velký rozsah" je určen zejména částkou, kterou by oprávnění z autorských práv obdrželi při legálním užití těchto děl (např. při prodeji hudebních CD) všemi, kdo díky neoprávněnému užití díla pachatelem jej takto získají, jak se snaží tvrdit zejména nahrávací společnosti a kolektivní správci autorských práv. Je totiž velice pravděpodobné, že by uživatelé v případě nemožnosti této nelegální cesty vůbec dílo (resp. hmotný nosič, na kterém je zaznamenáno) zakoupili. Praxe se proto uchyluje často k tomu, že otázku určení prospěchu či rozsahu ponechává nevyřešenou a kvalifikuje jednání pachatele pouze podle základní skutkové podstaty.[112]

1.4.3.3. Zvláštní případ účastenství[113] na TČ podle § 270 tr.zák.

Účastníkem na dokonaném trestném činu nebo jeho pokusu je podle § 24 odst. 1 písm. a), b), c) tr.zák. ten, kdo úmyslně:

a) *spáchání trestného činu zosnoval nebo řídil (organizátor),*
b) *vzbudil v jiném rozhodnutí spáchat trestný čin (návodce),*
c) *umožnil nebo usnadnil jinému spáchání trestného činu, zejména opatřením prostředků, odstraněním překážek, vylákáním poškozeného na místo činu, hlídáním při činu, radou, utvrzováním v předsevzetí nebo slibem přispět po trestném činu (pomocník).*

Česká právní úprava účastenství 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 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

[112] Viz rozhodnutí ve věci „obalycd.cz" – příloha č. 3 a ve věci „Rafťáci" (viz níže v kapitole 1.4.5 Zvláštní části práce), 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

[113] Zde v tzv. užším smyslu účastenství

pomocníka (v extrémních případech i návodce[114]) na trestném činu podle § 270 tr.zák. (§ 24 odst. 1 písm. c), event. b), § 270 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 (obecné znaky TČ).

Při splnění těchto podmínek můžeme kvalifikovat jednání poskytovatelů odkazu jako účastenství ve formě pomoci na trestném činu porušení autorského práva, práv souvisejících s právem autorským a práv k databázi dle § 24 odst. 1 písm. b), § 270 tr.zák.[115]

---

[114] 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 internetu

Při porušování autorských práv prostřednictvím internetu může docházet i k jednočinnému souběhu s jinými trestnými činy. Tak například je možný jednočinný souběh TČ podle § 270 a TČ neoprávněného podnikání podle § 251 tr.zák. v případě provozování výdělečných serverů s neoprávněně zpřístupněnými autorskými díly bez živnostenského oprávnění. Není vyloučen ani souběh s trestným činem porušení práv k ochranné známce a jiným označením dle § 268 tr.zák. (např. provozování stránek nazvaných „SONY BMG free download“, na kterých budou neoprávněně poskytována autorská díla), popř. s TČ porušení předpisů o pravidlech hospodářské soutěže podle § 248 odst. 1 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, poskytovatelů připojení a tvůrců peer to peer systémů

1.4.4.1. Trestní odpovědnost poskytovatelů volného prostoru

Trestní odpovědnost poskytovatelů volného prostoru[116] je dle čl. 14 směrnice č. 2000/31/ES o elektronickém obchodu vyloučena, pokud poskytovatel neměl vědomost o obsahu porušujícím autorská práva, a když se o porušení dozvěděl, učinil kroky k odstranění tohoto obsahu nebo znemožnění přístupu k němu. V podstatě shodnou úpravu obsahuje i § 5 zákona č. 480/2004 Sb., o některých službách informační společnosti, který tuto směrnici provádí. 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

---

[115] Obdobně došel k závěru o trestnosti poskytování odkazů v rámci trestnosti účastníka na trestném činu i Nejvyšší soud Norského království, viz Krog, G., P.: The Norwegian „Napster case“ – Do hyperlinks constitute the „Making Available to the Public“ as a Main or Accessory Act? In: Computer Law & Security Report. Vol. 22. Elsevier Science B.V., 2006, s. 73 a násl.

[116] *Poskytovatelem volného prostoru* (hosting provider) se rozumí právnická nebo fyzická osoba, která 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)

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 využívají, je příliš vzdálený, než aby se u poskytovatelů připojení dala vyvozovat soukromoprávní odpovědnost za porušování autorských práv, a to včetně i tzv. spoluodpovědnosti.[117] Tím spíše proto nemůžeme dovodit, vzhledem k blanketnímu ustanovení § 152 tr.zák. a nutnosti naplnění materiálního znaku trestného činu, trestní odpovědnost poskytovatelů připojení.

1.4.4.3. Trestní odpovědnost tvůrců peer to peer systémů

Poměrně zajímavá je i problematika odpovědnosti (civilní, administrativní i trestní) tvůrců systémů peer to peer sítí (k porušování autorských práv v těchto sítích viz výše, kapitola 1.3.2.2. Zvláštní části práce). Nutno předeslat, že autorovi této práce není znám jediný případ, kdy by tato odpovědnost byla řešena našimi soudy. Důvod je prostý, drtivá většina peer to peer systémů pochází ze zahraničí. To však nebrání se případnou odpovědností tvůrců těchto systémů blíže zabývat.

Je nesporné, že v peer to peer sítích dochází k masivnímu porušování autorských práv. Mohou však být hnáni k odpovědnosti samotní tvůrci těchto systémů, když ty samozřejmě mohou být užívány nejen k sdílení děl podléhajících autorskému právu, ale v podstatě jakéhokoliv materiálu v elektronické formě? S odpovědí na tuto otázku se můžeme inspirovat v zahraničí, konkrétně ve Spojených státech amerických, kde již odpovědnost tvůrců systémů peer to peer byla i soudně řešena (prozatím pouze v civilní rovině).[118]

Jako za průlomové lze označit rozhodnutí Nejvyššího soudu USA ve věci MGM v. Grokster[119], ve které velké filmové nahrávací společnosti v čele s MGM Studios, Inc. žalovaly společnosti volně distribuující software umožňující volné sdílení souborů v peer to peer sítích. Nejvyšší soud USA zde judikoval, že:[120] „*Ten, kdo šíří zařízení s cílem propagovat jeho použití k porušování autorských práv, jak vyplývá z jeho zjevných vyjádření nebo jiných podobných kroků podporujících porušování, je odpovědný za tato výsledná porušení třetími*

---

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

[118] K různým případům soudních sporů s tvůrci peer to peer systémů ve světě a velice zajímavé analýze snah o extrateritoriální dosah jednotlivých soudních rozhodnutí srov. Adrian, A.: The Pirate Bay Deep-sixed: Copyright Protected Works and the Territoriality Principle in: Computer Law & Security Report. Vol. 22. Elsevier Science B.V., 2006, s. 392 a násl.

[119] Rozhodnutí Nejvyššího soudu USA ve věci Metro-Goldwyn-Mayer Studios, Inc., et al. v. Grokster, Ltd., et al. ze dne 27.6.2005, sp.zn. 545 U.S. 913 (2005); v anglickém znění dostupné včetně disentních stanovisek na adrese: http://caselaw.lp.findlaw.com/cgi-bin/getcase.pl?court=US&navby=case&vol=000&invol=04-480, zobrazeno 15.8.2012, 16:25

[120] Překlad autora práce

stranami." Nejvyšší soud proto shledal (civilní) odpovědnost tvůrců peer to peer systémů, a to na základě tzv. inducement liability (odpovědnosti návodce). Přitom se musel vypořádat s tzv. obranou (námitkou) „Sony defence" využívanou tvůrci technologií, které lze využít jak porušování práv, tak i k užívání po právu. Ve zkratce byla tato procesní obrana založena případem Sony Corp. Of America v. Universal Studios, Inc., sp.zn. 464 U.S. 417 (1984)[121], ve kterém soudy dospěly k názoru, že výrobci nemají být odpovědni za porušení autorských práv třetími osobami, pokud technologie, která k tomu byla využita může sloužit jak k legitimnímu, tak i protiprávnímu účelu.[122] Nižší soudy pak i na základě této obrany odmítaly shledat tvůrce Groksteru a dalších podobných technologií peer to peer sítí odpovědnými, a to zejména proto, že tito neměli žádnou kontrolu nad obsahem sdíleným v těchto sítích, neboť jejich architektura byla vystavěna na decentralizovaném systému (na rozdíl např. od výše uvedeného Napsteru).[123]

Nejvyšší soud USA však na rozdíl od nižších soudů vyvodil odpovědnost tvůrců decentralizovaných systémů peer to peer sítí ze zřejmých důkazů o tom, že tito výrobci vymýšleli a šířili tyto systémy s úmyslem ulehčit porušování autorských práv. Ten byl dovozován přímo z některých interních dokumentů žalovaných tvůrců systémů peer to peer a materiálů určených k propagaci jejich produktů, ze kterých nejen plynula pasivní vědomost o používání jejich systémů k porušování autorských práv, ale byl i výslovně uveden plán převzetí klientů Napsteru sdílejících autorsky chráněná díla po jeho uzavření. Rovněž pak žalované společnosti zasílali svým klientům reklamní materiál, ve kterém nabízeli možnost získání (zdarma) autorsky chráněného materiálu. Konečně jejich úmysl k usnadnění porušování autorských práv vycházel dle Nejvyššího soudu ze samotného podnikatelského modelu žalovaných společností, které mohly mít zisk jen v tom případě, že by nabízely atraktivní (rozuměj autorsky chráněná) díla.[124] Tyto důkazy o úmyslu napomáhat (a někdy i navádět) k porušování autorských práv umožnily Nejvyššímu soudu dospět k závěru o odpovědnosti žalovaných producentů peer to peer systémů za porušování autorských práv třetích osob a vyhnout se tak „obraně Sony" dříve judikované.

---

[121] Rozhodnutí Nejvyššího soudu USA ve věci Sony Corporation of America et al. v. Universal City Studios, Inc., et al. ze dne 17.1.1984, sp.zn. 464 U.S. 417 (1984), v anglickém znění dostupné včetně disentních stanovisek na adrese: http://www.law.cornell.edu/copyright/cases/464_US_417.htm, zobrazeno 15.8.2012, 17:55

[122] Kramer, K., M.: Metro-Goldwyn-Mayer Studios v. Grokster—The Supreme Court's Balancing Act Between the Risks of Third-Party Liability for Copyright Infringement and Rewards of Innovationin: Santa Clara Computer & High Technology Law Journal. vol. 22. Santa Clara University, Santa Clara 2005, s. 169 a násl.

[123] Idem, s. 170

[124] Rozhodnutí Nejvyššího soudu USA ve věci Metro-Goldwyn-Mayer Studios, Inc., et al. v. Grokster, Ltd., et al., část I. A

I když nelze zcela srovnávat americký právní systém a kontinentální systém práva u nás, je možné se některými závěry amerických soudů inspirovat, a to i pro případnou trestní odpovědnost. Otázka trestní odpovědnosti producentů softwaru k užití systémů peer to peer sítí totiž nabývá na aktuálnosti se zavedením trestní odpovědnosti právnických osob od 1.1.2012. Pokud tedy budou v případné konkrétní věci důkazy o úmyslu tvůrců systémů napomáhat k páchání trestného činu porušování autorského práva, práv souvisejících s právem autorským a práv k databázi, bude dle názoru autora této práce možné trestně stíhat i společnosti, které tyto systémy produkují a šíří, a to jako účastníky ve formě pomoci na uvedeném trestném činu dle § 24 odst. 1 písm. c), § 270 tr. zák. ve spojení s § 1 odst. 2, § 7, 8, 9 odst. 1 zákona o trestní odpovědnosti právnických osob.[125] Stejně tak by mohly být trestně postiženy jako účastníci ve formě pomoci i konkrétní fyzické osoby, které úmyslně tvorbou systémů peer to peer sítí a její propagací napomáhaly porušování autorských práv. Vzhledem ke konstrukci účastenství jako úmyslného jednání (srov. návětí § 24 odst. 1 tr.zák.) však bude muset být úmysl napomoci k takovému porušování bezpečně prokázán.

1.4.5. Kazuistika

K porušování autorských práv zpřístupněním na webových serverech nebo jeho sdílením v peer to peer sítích, které znamená citelné škody, nemusí docházet jen v případě kasovních filmových trháků, hudebních šlágrů či počítačových programů. Autorovi této práce je znám případ z praxe, kdy došlo k porušení autorských práv k vědeckému dílu, které mělo za následek nezanedbatelné škody. V daném případě se jednalo o zpřístupnění jedné z učebnic nakladatelství Leges, s.r.o. na v českých podmínkách poměrně známém serveru „Ulož.to“. Tento server provozovaný společností Nodus Technologies s.r.o. slouží k poskytování volného prostoru k nahrávání souborů, které si z tohoto serveru mohou uživatelé následně stáhnout. Je poměrně známé, že na tomto serveru jsou takto sdíleny soubory jak s obsahem nezávadným, tak i soubory, které podléhají autorskoprávní ochraně.

Právě na tento server byla nahrána kompletní (a poměrně žádaná) učebnice uvedeného nakladatelství. Poté, co se nakladatelství o nahrání učebnice dozvědělo, informovalo o porušování autorských práv provozovatele serveru. Ten vzápětí stahování učebnice ze serveru zamezil. Po čase se však učebnice objevila na serveru znovu. I v tomto případě

[125] Úvahy o podmínkách trestní odpovědnosti právnických osob na účastenství přesahují rámec této práce, pro její účely postačí pouze poznamenat, že zákon o trestní odpovědnosti právnických osob výslovně trestnost právnické osoby za účastenství neupravuje, proto se ve smyslu § 1 odst. 2 tohoto zákona použije subsidiárně úprava obsažená v trestním zákoníku.

následoval shodný postup nakladatelství i reakce poskytovatele volného prostoru. Zároveň se však nakladatelství informovalo u příslušných policejních orgánů o možnostech dalšího postupu vůči osobě (osobám), která neoprávněně na server učebnici nahrála. Z těchto konzultací vyplynulo, že policejní orgány jsou při vyšetřování tohoto typu trestné činnosti značně omezeny. V daném případě totiž mají jedinou možnost, jak zjistit pachatele, pokud jeho identitu nezná a nevyzradí poskytovatel volného prostoru sám, a to vyžádat si údaje o uskutečněném elektronickém provozu. K tomu však potřebují v přípravném řízení příkaz soudce, který tak závažný zásah do základních svobod jednotlivce často odmítají povolit. Autorům (v našem případě nakladatelství) tak v praxi nezbývá než čas od času kontrolovat nejznámější servery poskytující volný prostor, zdali se tam neoprávněně neobjevilo jejich dílo.

České trestní soudy však v minulosti již rozhodovaly několik případů porušování autorských práv na internetu. Na následujících řádcích jsou některá z rozhodnutí uvedena v úplném znění v anonymizované podobě. Ve většině případů se však jedná o trestní příkazy, a tak není odůvodnění podrobnější.[126]

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

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
ke dni 3.4.07
OBVODNÍ SOUD PRO PRAHU 10
26 -03- 2007

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)

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
16

Za správnost vyhotovení:
Andrea Šléglová

TRR082 - (Tr.ř. 82 - trestní příkaz)

b) Rozhodnutí ve věci „Rafťáci“ (viz výše):[127]

Spisová značka: **6 T 46/2007**

Toto rozhodnutí nabylo právní moc:
25.5.2007
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

[127] Zdroj: Idem

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 í /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 Vobornik 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 výši 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):[128]

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.xoom.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 :

[128] 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 200[illegible] **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.[129] 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 je často mlčky trpěno i samotnými vysokými školami. Oprávnění z autorských práv se proto snaží nalézt cestu prostřednictvím prevence, v poslední době např. masová kampaň České protipirátské unie, ve které se upozorňuje na trestnost neoprávněného užívání děl.[130] Na druhou stranu o pozitivním vývoji v ochraně autorských práv a vyšším standardu jejího poskytování svědčí skutečnost, že Česká republika byla od roku 2010 vyřazena ze seznamu zemí monitorovaných pro zvýšenou míru pirátství každoročně vydávaného Úřadem obchodního zmocněnce USA,[131] do kterého byla zapsána v roce 2008.[132] V roce 2012 pak byla Česká republika v této zprávě Úřadu obchodního zmocněnce dokonce vyzdvižena pro svou aktivitu při informování zainteresovaných stran o ochraně a vynucování dodržování autorských práv.[133]

---

[129] K tomu srov. velice zajímavý výzkum provedený na cca 250 respondentech formou vyplňovaného anonymního dotazníku na webových stránkách uveřejněný v článku Volevecký, P.: Kybernetická trestná činnost jako předmět vědeckovýzkumné činnosti in: časopis Trestní právo č. 5/2011, s. 11 a násl.

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

[131] Viz 2010 Special 301 Report. Office of the United States Trade Representative, s. 1, dostupné na http://www.ustr.gov/about-us/press-office/reports-and-publications/2010-3, zobrazeno dne 3.5.2012, 21:50

[132] Viz příloha č. 4

[133] Srov. 2012 Special 301 Report. Office of the United States Trade Representative, s. 11, dostupné na http://www.ustr.gov/about-us/press-office/reports-and-publications/2012-2, zobrazeno dne 3.5.2012, 21:55

2. Hackerství

2.1. Úvod

Hackerství neboli hacking je obecně ve společnosti pojímáno jako to, co ztělesňuje internetovou kriminalitu. Je tomu tak 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, že projevy hackingu jsou namířeny zejména proti veřejným autoritám, establishmentu, atd.[134] V praxi však toto označení zahrnuje jednání, jejichž původci tvoří velice diversifikovanou skupinu osob od členů organizovaného zločinu až po proti autoritám revoltujícího teenagera, kteří mají často diametrálně odlišný zájem a rovněž i rozdílné 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[135] liší tím, že svým jednáním nechtějí způsobovat škodu ani nic ničit, ze svého jednání nemají žádný zisk. Pokud po svém průniku zasahují do systému, je to proto, aby si udrželi přístup i nadále nebo po sobě zahlazovali stopy.[136]

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

---

[134] Obdobně si obecného vnímání hackingu všímá Završnik, A.: op. cit., s. 40 a násl.

[135] 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 někdy nazývají „knackery".

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

dříve, když k němu měl 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[137]) a zisky z něj a jím způsobené škody dosahují někdy astronomických částek. Bývá prostředkem nejrůznějších finančních podvodů a machinací, průmyslových špionáží a nekalosoutěžních jednání. Obecně je považováno za nejnebezpečnější.

5.) Hacking jako vojenská zbraň. Hackerství představuje v současné době významnou hrozbu bezpečnosti všech států na celém světě.[138] Každý rok slýcháváme o tom, že byly zaznamenány zahraniční špionážní útoky prováděné hackery ve službách státu. Není tak vyloučeno, že se do budoucna budou využívat hackeři ve vojenských konfliktech, a to s velmi drastickými a masovými následky.

Z výše uvedeného členění vyplývá i různá typologie pachatelů:[139]

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

---

[137] autor@chip.cz: Internetové mafii na stopě, časopis CHIP.CZ, č. 1/2008, str. 157 a násl.
[138] Blíže viz Geers, K.: The Challenge of Cyber Attack Deterrence in: Computer Law & Security Review. Vol. 26. Elsevier Science B.V., 2010, s. 298 a násl.
[139] Zdroj: Zpráva společnosti McAfee o internetové kriminalitě, časopis CHIP.CZ, č. 5/2007, str. 16 a násl.

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.

V literatuře ovšem lze nalézt i definici hackera z hlediska orgánů činných v trestním řízení.[140] Za hackera se v nich označuje osoba:

1. „Která má zálibu v technické obratnosti a zdatnosti,
2. Kterou baví programování,
3. Která vyhledává intelektuální výzvy spočívající v kreativním řešení problémů nebo překonávání limitů a
4. a) v případě pozitivní definice hackera (tzv. etický hacker) osoba, která hackingem nenaplňuje skutkovou podstatu trestného činu.

   b) v případě negativní definice hackera se tento pojem vztahuje k počítačovému narušiteli, který se snaží objevit citlivé informace a který tím páchá trestnou činnost.“

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, která 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

[140] Kaoa, D.-Y., Fu-Yuan, Huang, F., F.-Y., Wang, S.-J.: Persistence and Desistance: Examining the Impact of Re-integrative Shaming to Ethics in Taiwan Juvenile Hackers in: Computer Law & Security Review. Vol. 25. Elsevier Science B.V., 2009, s. 466

vyšší.[141] V roce 2008 měl již podle zprávy bezpečnostní společnosti Symantec celkový počet škodlivých virů překročit hranici 1 000 000![142]

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-mailoví a síťoví červi. 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-mailů, resp. e-mailových klientů. E-mailový červ se nikdy neobejde alespoň bez částečné asistence koncového uživatele, neboť ten musí červa z přiloženého souboru k e-mailu spustit nebo minimálně otevřít infikovaný e-mail.[143] E-mailové červy dosáhly svého vrcholu počátkem tohoto desetiletí (kdo by neznal červa s názvem „I love you“, který důmyslně využíval tzv. sociální inženýrství[144]), v současné době však jejich využívání stagnuje.

Síťoví červi 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 mezery 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 jejích 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 vypsanou společností Microsoft ve výši 5.000.000,- dolarů již ani ne týden po vypuštění červa. Byl jím mladý

[141] Nádeníček, P.: Počítačové viry známé a neznámé. 1. díl Úvod do problematiky & souborové viry in: časopis PC WORLD, č. 11/2005
[142] http://news.bbc.co.uk/2/hi/technology/7340315.stm, zobrazeno 9.8.2009, 11:05
[143] Nádeníček, P.: Počítačové viry známé a neznámé. 2. díl E-mailový červ, starý dobrý známý in: časopis PC WORLD, č. 1/2006
[144] V podrobnostech k sociálnímu inženýrství viz hlava 3. Zvláštní části

německý programátor Sven Jaschen, jenž byl následně odsouzen k trestu odnětí svobody v délce trvání 21 měsíců s podmíněným odkladem výkonu trestu 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,- €.[145]

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."[146] 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 využívala 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.

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",[147] 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. Takto zahlcený server následně pod návalem dotazů kolabuje a je vyřazen z provozu.

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 jejich kombinace. Nelze zapomenout také na zničující či žertovné projevy trojských koní.

---

[145] Nádeníček, P.: Počítačové viry známé a neznámé. 3. díl Síťový červ – zatraceně rychlý chlapík in: časopis PC WORLD, č. 2/2006

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

[147] K definici pojmu bot viz Jirásek, P., Novák, L: Český slovník kybernetické bezpečnosti in: Gogela, R., Jirásek, P., Novák, L., Polčák, R., Požár, J.: Pracovní příručka bezpečnostního manažera. První vydání. Policejní akademie ČR & Česká pobočka AFCEA, Praha 2011, s. 41

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.[148] Tohoto velice rafinovaného prostředku využila i společnost SONY BMG jako účinného prostředku ochrany autorských práv. Po skandálu, který vyvolalo zjištění, že se na jí vyrobené disky vkládá i rootkit, a následných žalobách od tohoto způsobu ochrany opustila.[149] 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

Jak je již uvedeno výše, nemusí hacking sloužit jen k pobavení hackera. Často je součástí rafinovaného kriminálního jednání, které má zejména za účel někoho výrazně poškodit a je prostředkem tučných zisků (zejména při průniků do systémů organizací). Hackerské jednání se nevyskytuje 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 některých hackerů ze záliby. V ostatních případech

[148] Přibyl, T.: Causa rootkit, časopis PC WORLD, č. 3/2006, s. 52 a násl.
[149] Přibyl, T.: Rootkity in: IT Professional - IT Security, č. 1/2007, s. 12 a násl.

hackerství za účelem zisku (hospodářského hackingu) má toto jednání určitý typizovaný průběh, který můžeme rozdělit na určité fáze:[150]

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[151] používají rozličné serverové služby. Celá řada serverových služeb při skenování portů zároveň zobrazuje číslo verze. I tato informace může být pro hackera velice cenná, neboť 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.[152] 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 předstírá externího IT specialistu řešícího „aktuální problém systému".

---

[150] Čepička, D., Arnold, A., Behrens, D.: Odhalte triky hackerů, časopis PC WORLD, č. 12/2007, s. 68 a násl.
[151] Porty slouží k tomu, aby jedna IP adresa uživatele mohla být použita pro více služeb běžících na serveru.
[152] viz hlava 3. Phishing zvláštní části této práce

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.[153]

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).

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 k 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.[154] 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 kombinace postupně všech možných písmen, čísel a znaků pomocí speciálních aplikací. 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

---

[153] Více o tomto např. na: http://www.linuxbasement.com/content/finuxs-student-hackers-guide-wep-hacking, zobrazeno 22.12.2008, 15.40

[154] Čepička, D., Arnold, A., Behrens, D.: op. cit., s.68 a násl.

řešení, k němuž však potřebuje přístupové heslo…, účinný je také nátlak). Jinou obvykle využívanou metodou je „dumpster diving“, tedy zjednodušeně řečeno prohledávání odpadků, kde by mohly být útržky papírků s hesly.[155]

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[156]

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)[157]

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)[158]

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 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.

---

[155] Idem
[156] Blíže viz http://en.wikipedia.org/wiki/SQL_injection, zobrazeno 10.7.2011, 13:05
[157] Blíže viz http://en.wikipedia.org/wiki/Cross-site_scripting, zobrazeno 10.7.2011, 13:25
[158] Balážik, M: Principy ochrany digitální identity. 2. díl: Útoky proti identitě a standardní bezpečnostní opatření in: časopis IT Systems č. 3/2012, s. 54 a násl.

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 zazáplatována. Pachatel tedy musí např. vrátit zpět seznam naposledy používaných 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)[159] a

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

antispamu (prostředku na ochranu před nevyžádanými nebo nechtěnými zprávami a soubory).

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. Trestněprávní kvalifikace jednání hackerů

Trestní zákoník přinesl zcela novou úpravu trestněprávní ochrany počítačových dat a systémů, která se skládá ze tří trestných činů v §§ 230 – 232 trestního zákoníku, z nichž dva jsou úmyslné (TČ podle § 230 a 231) a jeden nedbalostní (TČ podle § 232). Naneštěstí se zákonodárce uchýlil ke zcela kazuistické úpravě:

§ 230

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.

§ 231

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 § 182 odst. 1 písm. b), c) nebo trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1, 2 vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává

a) 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

b) 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.

§ 232

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.

Tyto trestné činy jsou systematicky zařazeny do Hlavy páté trestního zákoníku, trestných činů proti majetku a lze je 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 počítačových systémů a jejich částí před neoprávněným zásahem. Tím však není okruh chráněných zájmů zdaleka vyčerpán, trestní zákoník těmito ustanoveními taktéž nepřímo chrání obchodní a bankovní tajemství, autorská díla, citlivé údaje, atd., pokud je nosič informace či počítačový systém obsahuje.[160]

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

2.6.1.1. Trestný čin podle § 230 odst. 1 tr.zák.

Prvním z uvedených trestných činů je trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 trestního zákoníku. Toto ustanovení obsahuje ve skutečnosti 2 základní skutkové podstaty. První z nich se nachází v odst. 1 a má sloužit k postihu neoprávněného přístupu k počítačovému systému tím, že pachatel překoná určitá bezpečnostní opatření oběti jako přístupové heslo, „firewall“, antivirový štít nebo zakódování. Tato bezpečnostní opatření však nemusí mít povahu softwarového nástroje (ač tomu tak je v praxi nejčastěji), zákonodárce tím, že tato bezpečnostní opatření nikterak blíže nedefinoval, připustil, aby tyto prostředky ochrany dat měly povahu i hardwarového zařízení.

Ustanovení § 230 odst. 1 tr.zák. se uplatňuje na jednání, která mají povahu pouhé přípravy k samotnému poškození, užití nebo změně chráněných dat a která by jinak nemohla být trestná, a to ani podle nové úpravy v trestním zákoníku, neboť předmětný trestný čin neoprávněného přístupu není ani zvlášť závažným zločinem ve smyslu § 14 odst. 3 věta za středníkem tr.zák., ani není u tohoto ustanovení uvedeno, že by jeho příprava měla být trestná, což jsou dvě obligatorní podmínky trestnosti přípravy podle tr.zák. Zákonodárce

[160] Jelínek, J. a kol.: Trestní právo hmotné. 2. vydání. Linde Praha, a.s., Praha 2010, s. 625 a násl.

takto překonal jeden z významných nedostatků předchozí právní úpravy. Napříště již proto bude možné trestně postihovat např. tzv. hacking pro zábavu, tedy jednání hackerů, jejichž jediným cílem je samotné překonání různých bezpečnostních opatření, a to bez úmyslu takto získaného přístupu do systému a tam uložených informací nějak využívat, popřípadě je poškozovat nebo měnit. Mnohým hackerům totiž o data v počítačovém systému ani nejde, své snažení považují za jakýsi sportovní zápas s protivníkem – tvůrci a správci bezpečnostních opatření. Jiní zase tímto způsobem testují schopnosti a možnosti jimi vytvořených škodlivých programů (tzv. malware). Je zřejmé, že i takováto jednání dosahují určitého stupně společenské škodlivosti, a měla by být proto trestná.

2.6.1.2. Trestný čin podle § 230 odst. 2 tr.zák.

Druhá základní skutková podstata je upravena v odst. 2 citovaného ustanovení trestního zákoníku a jedná se o detailnější rozpracování původní skutkové podstaty podle § 257a trestního zákona z roku 1961. Sankcionuje v podstatě jakékoliv neoprávněné nakládání s daty a zásahy do technického nebo programového vybavení počítače, popř. jiného technického zařízení pro zpracování dat, a to užití dat, vymazání dat, zničení či jiného poškození dat, změny dat, potlačení dat, snížení kvality dat, činění dat neupotřebitelnými, padělání nebo pozměnění dat, vkládání nových dat nebo učinění jiného zásahu.[161, 162]

Přístup k počítačovému systému či jeho části a nosiči informací 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 (zaměstnavatelem, známým, atd.).

Za data lze označit jakékoliv údaje. Podle Českého slovníku kybernetické bezpečnosti[163] jde o reprezentaci informací formalizovaným způsobem vhodným pro komunikaci, výklad a zpracování. Volevecký[164] v tomto směru zastává názor, že jakákoliv informace je zároveň datem, avšak ne všechna data se musejí stát informacemi. Autor této práce si tímto závěrem není jist, neboť i ta nejjednodušší data určitou informační hodnotu mají, a to, pokud bychom je převedli na binární kód, zda obsahují 0 či 1, popř. jejich kombinaci.

[161] Volevecký, P.: Kybernetické trestné činy v trestním zákoníku in: časopis Trestní právo č. 7 – 8/2010, s. 25
[162] Ohledně kritiky tohoto ustanovení viz část III Úvahy de lege lata a de lege ferenda, kapitola 2.1.1.
[163] Jirásek, P., Novák, L: op. cit., s. 55
[164] Volevecký, P.: op. cit., s. 25

Nosičem informací se míní (hmotný) nosič dat v elektronické podobě (CD, DVD, HDD, paměťové karty, paměti mobilního telefonu, atd.).[165]

Počítačovým systémem je dle čl. 1 Úmluvy jakékoliv zařízení nebo skupina vzájemně propojených nebo souvisejících zařízení, z nichž jedno nebo více provádí na základě programu automatické zpracování dat.

K trestnosti hackerství se vyžaduje úmyslná forma zavinění, a to bez ohledu na to, zda je orientovaná ke způsobení škody nebo jiné újmy jinému nebo neoprávněného prospěchu pro sebe nebo jiného.

Subjektem tohoto jednání může být kdokoli, a to včetně právnické osoby.

2.6.1.3. Kvalifikované skutkové podstaty uvedené v § 230 odst. 3, 4 a 5 tr.zák.

Odstavec 3 TČ neoprávněného přístupu k počítačovému systému a nosiči informací obsahuje dvě okolnosti podmiňující použití vyšší trestní sazby, a to pokud pachatel spáchá tento trestný čin jednak v úmyslu způsobit jinému škodu nebo jinou újmu, nebo získat sobě nebo jinému neoprávněný prospěch (písm. a) citovaného ustanovení) a jednak v úmyslu omezit funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat. První jmenovaná zvláště přitěžující okolnost měla zavést ochranu před počítačovými podvody. Druhá pak má sloužit k trestněprávní ochraně před počítačovou sabotáží, se kterou se v poslední době velice často setkáváme v případě již výše zmíněných DoS útoků.

Naplnění kvalifikovaných skutkových podstat TČ podle § 230 odst. 4 a 5 tr.zák spočívá ve spáchání jinak obvyklých těžších následků (účinků) a ve spáchání takového činu jako člen organizované skupiny.[166]

2.6.1.4. Trestný čin podle § 231 tr.zák. a § 232 tr.zák.

Trestný čin opatřování a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných dat podle § 231 tr.zák. rovněž provádí závazky plynoucí z Úmluvy, konkrétně jejího čl. 6, upravující zneužití zařízení.[167] Toto ustanovení dopadá na některá další přípravná jednání spojená s hackingem jako výroba a distribuce programů a návodů ulehčujících nebo přímo umožňujících získání neoprávněného přístupu a kontroly nad

[165] Šámal, P. a kol.: Trestní zákoník II. § 140 – 421. Komentář. První vydání. C. H. Beck, Praha 2010, s. 2089
[166] Ohledně kritiky těchto ustanovení viz část III Úvahy de lege lata a de lege ferenda, kapitola 2.1.1.
[167] K tomu srov. část III. hlavu 2. této práce.

počítačem někoho jiného nebo na neoprávněnou manipulaci a uchovávání hesel, přístupových kódů, postupů, jak je překonávat, apod.

Dalším trestným činem, který trestní zákoník nově zavádí, je TČ poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti podle § 232 tr.zák. Jak již z názvu tohoto trestného činu vyplývá, slouží k postihu nedbalostních jednání spočívajících v zásahu do dat a komunikačních zařízení vedoucích k způsobení minimálně značné škody, tedy ve smyslu § 138 odst. 1 tr.zák. alespoň ve výši 500.000,- Kč. Zákonodárce touto skutkovou podstatou zřejmě reagoval na skutečnost, že i tato nedbalostní forma jednání může znamenat rozsáhlé a těžko napravitelné škody. K trestnosti je třeba hrubé nedbalosti[168] a pachatel musí porušit svou zvláštní povinnost.

2.6.1.5. Souběhy TČ podle § 230 odst. 1, 2, § 231 a jiných trestných činů

Ze skutečnosti, že § 230 tr.zák. obsahuje v podstatě dvě základní skutkové podstaty, vyvěrá poměrně zajímavá otázka, a to zdali je, či není vyloučen jednočinný souběh obou skutkových podstat. V teorii i praxi je zastáván názor, že konkrétní skutek by měl být posouzen podle všech trestně hmotně právních ustanovení, které na něj dopadají.[169] Pokud tedy určité jednání naplňuje více skutkových podstat trestného činu, mělo by být posouzeno jako jednočinný souběh těchto skutkových podstat trestného činu nebo přímo více trestných činů.

Obecně je jednočinný souběh určitých skutkových podstat trestných činů vyloučen ve třech případech. Prvním z nich je poměr speciality trestných činů (skutkových podstat), druhým poměr subsidiarity a posledním případem je tzv. faktická konzumpce skutkových podstat. Otázka tedy zní, mělo by být jednání hackera, který nejprve získá přístup do počítačového systému překonáním určitých bezpečnostních opatření a následně do něj například vloží předem připravený program – tzv. keylogger –, jak podle prvého odstavce § 230 tr.zák., tak i podle odstavce druhého, nebo bude takový souběh vyloučen z některého z výše uvedených důvodů?

Správná odpověď vychází z toho, co již bylo řečeno výše. Ustanovení odst. 1 totiž míří na jednání považovaná za zvláště trestnou přípravu k trestnému činu rozvedenému v odst. 2. Tomu ostatně odpovídá i návětí druhého odstavce: „*Kdo získá přístup k počítačovému systému nebo k nosiči informací…*“, které nutně zahrnuje jakékoliv jednání spadající do odstavce prvého. Ustanovení odstavce prvého tak vlastně doplňuje ochranu poskytovanou

---

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

[169] Jelínek, J. a kol.: op. cit., s. 329 a násl.

ustanovením odstavce druhého, a to proti méně společensky škodlivým útokům téhož druhu (jednání hackerů, kteří po neoprávněném získání přístupu do počítačového systému s daty tam uloženými nikterak nenakládají), pročež je jejich souběh vyloučen z důvodu poměru subsidiarity skutkové podstaty v odst. 1 vůči skutkové podstatě v odst. 2.[170]

Vzhledem ke konstrukci okolnosti podmiňující použití vyšší trestní sazby uvedené v § 230 odst. 3 tr.zák se rovněž nabízí otázka, zdali je možný jednočinný souběh této kvalifikované skutkové podstaty a TČ podvodu podle § 209 tr.zák., včetně jeho zvláštních forem pojistného, úvěrového a dotačního podvodu (§ 210, 211 a 212 tr.zák.).

Jelikož předmětná zvláště přitěžující okolnost byla do trestního zákoníku vložena k postihu počítačových podvodů a samotné jazykové znění § 230 odst. 2 písm. c), odst. 3 písm. a) tr.zák. zcela zahrnuje jednání, kdy pachatel v úmyslu sebe nebo jiného obohatit získá přístup k počítačovému systému nebo nosiči informací a padělá nebo pozmění určitá data (tj. uvede někoho v omyl), a tím způsobí na majetku jiného škodu, zdá se, že tato ustanovení by mohla být k obecnému podvodu ve vztahu speciality. Citovaná ustanovení tr.zák. by tak dopadala na zvláštní případy podvodu spáchaných zásahem do počítačového systému nebo nosiče informací, které lze obecně považovat za typově závažnější podvodná jednání. Tomu odpovídá i trestní sazba, neboť při způsobení škody nikoli nepatrné, avšak ne škody větší[171] hrozí pachateli v rámci TČ podle § 230 odst. 2, 3 písm. a) tr.zák. trest odnětí svobody od 6 měsíců do tří let oproti horní hranici dvou let v případě TČ podvodu podle § 209 tr.zák.

Pouhým srovnáním trestních sazeb u vyšších odstavců obou dotčených trestných činů (§ 230 odst. 4 a 5 a § 209 odst. 4 a 5 tr.zák.) je však situace opačná, neboť v nich hrozí výrazně vyšší trest u TČ podvodu (např. při způsobení škody velkého rozsahu 5 až 10 let u podvodu oproti 3 až 8 rokům u TČ podle § 230 tr.zák.). Závěr o vyloučení souběhu obou trestných činů z důvodu speciality by pak vedl zcela k absurdním důsledkům, že když pachatel někoho „jen obyčejně“ podvede a způsobí mu škodu značnou, hrozil by mu skoro stejný trest, jako kdyby někdo někoho rafinovaně podvedl nabouráním do počítačového systému oběti a pozměněním tam uložených dat, přičemž by způsobil škodu velkého rozsahu, tedy o řád vyšší.

Z uvedeného tak plyne jediný možný závěr, že jednočinný souběh uvedených TČ je vyloučen v případě naplnění pouze základní skutkové podstaty TČ podvodu podle § 209 odst. 1 tr.zák. a kvalifikované skutkové podstaty v odst. 2 tohoto trestného činu (případ zvlášť trestné

[170] K tomu srov. výklad o vyloučení souběhu z důvodu subsidiarity, Jelínek, J. a kol.: op. cit., s. 331 a násl.
[171] Tj. dle § 138 odst. 1 škody v rozmezí 5.000,- Kč až 50.000,- Kč

recidivy podvodu). Při naplnění okolností uvedených v odst. 3, 4 a 5 tohoto ustanovení však již jednočinný souběh vyloučen z důvodu speciality nebude.

Na druhou stranu bude zcela jistě z důvodu speciality vyloučen souběh TČ neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 tr.zák. a TČ poškození cizí věci podle § 228 tr.zák a neoprávněného užívání cizí věci podle § 207 tr. zák.[172]

Podobně jako v případě výše uvedeném není možné spáchat trestný čin opatření a přechovávání přístupového zařízení a hesla v jednočinném souběhu s trestným činem neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230, a to z důvodu poměru subsidiarity, neboť se opět jedná o zvláště trestnou přípravu.

Jak je již zmíněno výše, bývá často hackerské jednání prostředkem ke spáchání mnoha jiných trestných činů, není proto vyloučen jednočinný souběh trestného činu podle § 230 tr.zák s TČ Krádeže (§ 248 tr.zák.), porušení autorského práva, práv souvisejících s právem autorským a práv k databázi (§ 270 tr.zák.), či neoprávněného nakládání s osobními údaji dle § 180 tr.zák. Taktéž bude možné kvalifikovat jednání hackerů, kteří se ať už hardwarovými nebo softwarovými prostředky nabourají do systému oběti a poruší tajemství tam uloženého elektronického dokumentu (dat) jako trestný čin porušení tajemství listin a jiných dokumentů uchovávaných v soukromí podle § 183 tr.zák. v jednočinném souběhu s TČ podle § 230 tr.zák. Obdobně bude možný jednočinný souběh s TČ porušení tajemství dopravovaných zpráv podle § 182 v případě, že se hacker „naboural“ do systému poskytovatele služby elektronické pošty a zachytí adresátu dopravovaný e-mail, který mu ještě nebyl doručen (pokud už by doručení do e-mailové schránky proběhlo, jednalo by se již o TČ porušení tajemství listin uchovávaných v soukromí).

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 je na účty svých kompliců ve Finsku, Izraeli, Německu, USA a Nizozemí. Tři z těchto pomocníků byli záhy zadrženi při výběru převedených částek v Tel Avivu, San Franciscu a

[172] Shodně např. Volevecký, P.: op. cit., s. 26

Rotterdamu. Výslechy přivedly vyšetřovatele na stopu Vladimíra Levina, tehdy žijícího v Sankt Petrsburku. 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.[173]

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 pravomocně 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.[174]

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 8 lety, což rozhodně neodpovídá závažnosti tohoto jednání.

---

[173] Zdoj: http://en.wikipedia.org/wiki/Vladimir_Levin, zobrazeno: 7.6.2008, 13:53
[174] Zdroj: 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, aukcí a dalších aktivit, kde se užívají citlivé osobní údaje (čísla účtů, přístupová hesla, adresy, atd.), se začala objevovat i trestná činnost, jejímž cílem bylo tyto údaje získat a následně zneužít. Postupně tyto aktivity získávaly 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 jednoduchého a okamžitého rozšíření po celém světě. Jednou z těchto podvodných aktivit je i phishing, někdy překládaný do češtiny jako r(h)ybaření.

Phishing je jako druh kybernetické kriminality v mnoha ohledech specifický. Na jedné straně se v podstatě jedná jen o podvodné jednání, na druhou stranu jeho zvláštní charakter profitující z již zmíněných výhod internetového prostředí jej od jiných druhů podvodů známých s reálného světa zcela zásadně odlišuje. Phishing tak stojí na pomezí mezi tzv. přímou internetovou kriminalitou, u které kriminální aktivity sem náležející nemají obvykle výrazně podobný ekvivalent mimo kybernetický svět, a internetovou kriminalitu nepřímou, u níž naopak nelegální aktivity zcela existují i mimo kybernetický svět.

Toto ambivalentní postavení phishingu pak může někdy činit potíže i při jeho trestněprávní kvalifikaci. Je to dáno zejména nesprávným pochopením tohoto druhu kriminality, popř. konkrétního způsobu spáchání trestného činu. Tato část práce proto bude mít za cíl tento jev popsat, srovnáním jeho historických předchůdců vysvětlit způsob jeho fungování a následně jej trestněprávně kvalifikovat.

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.[175, 176] Nejčastějšími prostředky této komunikace

[175] Wikipedia: http://en.wikipedia.org/wiki/Phishing, zobrazeno 20.3.2012, 14:50
[176] Podobně též Volovecký, P.: Kybernetické hrozby a jejich trestně právní kvalifikace in: časopis Trestní právo č. 1/2011, s. 15

bývají e-mail a programy typu „instant messaging“.[177] Pachatelé se nejčastěji ukrývají za identitu banky oběti, internetové obchody jako e-bay, PayPal, Amazon či za servery typu YouTube.

Etymologicky tento pojem vychází z anglické parafráze na slovo „fishing“, tedy „rybaření“. Důvod je zřejmý. Pachatel phishingu vhazuje své oběti návnadu, na kterou se jí snaží „chytit“. Zároveň rybaření odpovídá phishingu i v tom, že stejně jako případný pachatel i rybář ví, že se na jeho návnadu všechny ryby v rybníce nechytí. Oběma však bohatě postačí, když alespoň nějaká oběť jejich lovu na jejich návnadu zabere. V literatuře se někdy lze setkat s českým překladem slova phishing v podobě „rhybaření“[178], ten se však u široké veřejnosti neujal a obvykle se tento jev i v českých podmínkách označuje původním názvem z angličtiny.

Podstatou phishingu je využívání tzv. sociálního inženýrství. To zahrnuje umění získat pomocí určitých psychologických technik citlivé údaje či další informace od oběti samotné.[179] Pachatel se tak často snaží získat důvěru oběti, která pak potřebné informace či údaje vlastně sdělí dobrovolně. Tuto důvěru může získat buď bezprostředním kontaktem (Human Based Social Engineering)[180], což však od pachatele vyžaduje velkou míru odvahy a sebejistoty, nebo se informace vyloudí z oběti prostřednictvím elektronických prostředků (Computer based Social Engineering)[181]. Tato varianta na pachatele neklade zdaleka tak vysoké nároky na komunikační a rétorické schopnosti, navíc skýtá velkou míru anonymity. Potenciální pachatel nadto může těžit z masovosti sítě elektronických komunikací, která mu umožňuje napadnout na ráz obrovské množství potenciálních obětí. Děje se tak např. elektronickou poštou, na různých internetových diskusních fórech, sociálních sítích či na vlastních webových stránkách.

---

[177] 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.

[178] Srov. např. Baudiš, P.: Staronové nebezpečí Rhybaření in: časopis CHIP.CZ, č. 4/2006, s. 14 a násl.

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

[180] Janczewski, L., Fu, L., R.: Social Engineering-Based Attacks – Model and New Zealand Perspective in Proceedings of the IMCSIT, č. 5/2010, s. 848

[181] http://www.social-engineer.org/framework/Computer_Based_Social_Engineering_Tools, zobrazeno 20.1.2012, 18:05

3.3. Předchůdci phishingu

3.3.1. Španělský vězeň

O phishingu jako takovém se začíná hovořit až s rostoucím rozvojem internetu v druhé polovině 90. let minulého století a zejména s rozmachem elektronického bankovnictví, na které bývá phishing často zaměřen. Je však zřejmé, že phishing měl své předchůdce ještě v dobách, kdy internet v dnešní podobě vůbec neexistoval. Sociální inženýrství se totiž neomezuje, jak už bylo řečeno, pouze na elektronický svět. Jedním z prvních předchůdců dnešního phishingu bylo jednání známé pod názvem španělský vězeň. Toto podvodné jednání sahá až do druhé poloviny 19. století[182] a bylo dokonce podrobně literárně zpracováno v povídce Arthura Traina z roku 1910.[183] Jeho podstatou je přesvědčení oběti, že jistý velmi bohatý vězeň bude ochoten se o své bohatství podělit, pokud prostřednictvím svého důvěrníka obdrží určitý obnos na podplacení stráží, které jej vězní. Poté, co oběť požadovanou částku důvěrníkovi zaplatí, objeví se neočekávané komplikace, pro které bude třeba uhradit další a další prostředky. Jediného, čeho se pak oběť tohoto podvodu dočká, je přivedení sebe sama na mizinu.

3.3.2. Nigerijské listy

V dnešní době by se na takovou báchorku nechal nachytat asi málokdo. Stačí však příběh jen trochu pozměnit, aby zapadl do současných poměrů, a je na světě velice rafinované podvodné jednání, které v malých obměnách dokázalo způsobit obrovské škody. Právě španělským vězněm se totiž beze zbytku inspirovali tvůrci tzv. nigerijských listů, také známých pod označením „419 scam“[184]

V tomto případě pachatelé využívají obecně nízkou povědomost osob o politickoekonomické situaci v západoafrických zemích. Záminka pro samotné vylákání peněz je různá. Někdy to bývá převedení 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 jsou po převratu ohroženi na životě a

[182]AN OLD SWINDLE REVIVED; The "Spanish Prisoner" and Buried Treasure Bait Again Being Offered to Unwary Americans", The New York Times, 20 March 1898, s. 12
[183]Train, A.: The Spanish Prisoner in: The Cosmopolitan Magazine New York, New York, č. 43, Březen 1910, s. 465 a násl.

[184] Výraz odkazuje na číslo ustanovení nigerijského trestního zákoníku upravujícího podvodné jednání.

majetku, a tak se rozhodli emigrovat, přičemž nechtějí za sebou zanechat veškerý poctivě a namáhavě vydělaný majetek. K tomu však nutně potřebují asistenci…

Stejně jako u španělského vězně se však záhy objeví problémy – např. nutnost založit konto v místní bance, na které budou nejprve peněžní prostředky přeposlány, potřeba zaplatit poplatek za zřízení společnosti, přes kterou se majetek vyvede ze země, dále platbu finančnímu úřadu, poplatek za převod samotný, atp. Vylákané „poplatky" dosahují často i hodnot tisíců dolarů, a tak oběť pozvolna přichází o nemalé peněžní sumy, ale proklamovaného zisku se nikdy nedočká. Tyto taktiky vždy spoléhají na zákonitosti fungování lidské psychiky, kdy oběť v okamžiku, kdy se rozhodne prvotní částku zaplatit, není ochotna se své investice vzdát a neustále následuje vidinu snadného zbohatnutí. Jak se zvyšuje částka, kterou oběť pachatelům poskytla, je stále obtížnější ztrátu přijmout a naopak roste (částečně ze zoufalství) očekávání, že právě poslední splátka byla ta opravdu poslední a nyní bude již jen následovat sladká odměna.

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 rozhodly „asistovat" převedení peněz přímo na místě.[185]

3.3.2.1. Příklad původních nigerijských listů

Zde je ukázka typického úvodního dopisu:[186]

„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

[185] Wikipedia: http://en.wikipedia.org/wiki/Nigerian_letters, zobrazeno 6.6.2008, 13:53
[186] Zdroj: http://www.snopes.com/crime/fraud/nigeria.asp, zobrazeno 21.7.2008, 13:40

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 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.“

3.3.2.2. Vlastní zkušenost autora se současnými nigerijskými listy

Jak již bylo uvedeno výše, pozadí, za kterým se skrývá podvodné jednání, může nabývat nejrůznějších podob. Autor této práce sám čelil poměrně rafinovanému podvodnému útoku, a to při nákupu ojetého mopedu na německých serverech sdružujících inzeráty potenciálních prodávajících. Poté, co autor (německy) odpověděl na inzerát k prodeji skútru za cca 850 €, což byla cena sice výhodná, avšak nikoliv nereálná, přišla od „majitele“ motocyklu tato e-mailová odpověď:

„Sir,

Re: 2010 Yamaha Aerox 50 r with 5400 km

Because of my financial problems that i have got i am willing to give it for € 700,- - shipping included .
It is in perfect condition with no damage on it . Technical inspection and emissions testing is passed and stamped as well.. It has title of ownership, cleared of any obligations or fees and comes with all the documents you need to register it.You will not have to pay additional taxes for this (VAT reclaimable).(the bike is register in Germany and have german documents) It's my personal bike. I have worked in Germany for one year and I've purchased the motorcycle there. My company wanted me back home, so currently I'm in England (United Kingdom).The motorcycle it's now located in ENGLAND - United Kingdom.

it`s a pity to keep such a motorcycle and not to use it.
UK registration tax is too high and have some financial problems to deal with and selling this motorcycle at this low price is the only option that I have right now. I am aware that I'm selling it way too cheap but I have no other solution.

I list my motorcycle under Europe Handler websites so I can sell it faster and for more publicity.The price is correct and the motorcycle can be transported to any location.My motorcycle is already at one Transport company from UK. I paid them to take care for my motorcycle sale protection. I can deliver the motorcycle to any location in Europe on my cost.

Please write me back to discuss only if you are interested!“

Z textu vyplývá, že požadovaná motorka je stále na prodej, nyní dokonce o 150 € levněji, avšak v současné době není k dispozici v Německu, ač tam byla zakoupena, ale v docích v Anglii, kam byl pisatel povolán zaměstnavatelem. Jelikož je registrace ve Spojeném Království příliš vysoká, nevyplatí se majiteli moped na ostrovech provozovat, a tak se ho rozhodl prodat. Moped majitel inzeroval přes německého prodejce, aby zvýšil publicitu inzerátu a prodej urychlil. Motorka je v současné době uschována u jednoho britského dopravce, na náklady majitele je možné ji dopravit na kterékoliv místo v Evropě. Ke zprávě bylo rovněž přiloženo 7 podrobných fotografií prodávané motorky.

Z odpovědi sice nikterak nevyplývá, že by zájemce musel uhradit jakékoliv prostředky navíc, je však možné (a vysoce pravděpodobné), že by v další komunikaci byl ze strany majitele vznesen požadavek na (zálohovou) platbu předem, nejlépe prostřednictvím služeb Western Union, která zaručuje prakticky absolutní anonymitu příjemce. Rovněž by bylo lze očekávat požadavek na platbu pojištění přepravy apod.

Autor této práce byl s obdobnými praktikami na automobilových serverech obeznámen, avšak i pro něj bylo překvapivé, že podvodníkům stojí za snahu pokoušet své štěstí i na serverech inzerujících mopedy, jejichž cena je na rozdíl od automobilů řádově nižší. Navíc se

u motocyklů nemůže uplatnit zástěrka nepoužitelnosti automobilů s levostranným řízením v Anglii. Přesto však již sama zpráva vzbuzuje určité pochybnosti. Jednak je neobvyklé, že majitel posílá svou zprávu v angličtině, ačkoliv zájemce odpovídal na inzerát ve spisovné němčině, navíc když majitel měl dle svých slov rok pracovat v Německu. I kdyby se za tu dobu německy nenaučil, prozrazuje podvodníka samotný jazyk. Ačkoliv o sobě tvrdí, že je v Anglii doma, z textu je patrné (kromě jiných chyb), že angličtinu příliš neovládá, neboť přestože v názvech států důsledně dodržuje psaní velkých písmen („Germany“, „England“, „United Kingdom“), v případě přídavného jména „německý“, tj. „German“, píše toto slovo s malým počátečním písmenem, což je typické pro kontinentální země.

Uvedená zpráva vyvolala ihned u svého příjemce podezření z podvodného jednání. Přesto je třeba poznamenat, že pro osobu, která se rozhodla např. právě ke koupi motocyklu a už se viděla, jak se stane jeho hrdým majitelem, je tato nabídka opravdu lákavá – přeci jen, co kdyby to nebyl podvod… I pro autora této práce, který metody sociálního inženýrství a nigerijských listů velmi dobře zná, bylo pokušení opravdu velké. Jak potom musí působit na neinformované osoby?

Autor, nyní však již z čirého zájmu, napsal (v angličtině) majiteli, že zájem o motorku stále má, je sice ochoten ji převzít na majitelem původně udávaném místě v Dortmundu, v žádném případě však nebude hradit žádné poplatky ani zálohy za uvedenou motorku. Ze zprávy však bylo jasně patrné, že její autor je obeznámen s podvodnými praktikami. Odpověď od „majitele“ přišla nečekaně z e-mailové adresy s doménou registrovanou ve východní Evropě. Tato zpráva by však již pro svou vulgaritu nemohla být v této práci publikována…

Samotné nigerijské listy by měly, pokud by byly využívány pouze klasické prostředky komunikace (např. dopisy), jen omezený rozsah. Co však z nich učinilo celosvětovou hrozbu, je elektronická pošta. Ta totiž umožňuje rozesílat podvodné dopisy (pod jakoukoliv záminkou k vylákání peněz) neomezenému počtu adresátů. Tím tento způsob podvodů vydláždil cestu phishingu.

3.4. Modus operandi phishingu

Phishingové praktiky se tedy inspirovaly v podvodných jednáních typu nigerijských listů ve dvojím směru. Jednak v metodách sociálního inženýrství, jednak v masivním využívání prostředků elektronických komunikací (zejména služby elektronické pošty, diskusních internetových fór, sociálních sítí apod.). To z těchto jednání činí velice nebezpečnou

kriminální činnost, protože pachatel může oslovit miliony potenciálních obětí na celém světě. Zároveň dokáže díky obrovskému počtu potenciálních obětí snižovat pravděpodobnost neúspěchu a zároveň svou relativní anonymitou snižuje i riziko odhalení.

Jediné, co je pachateli phishingu na překážku, jsou jazykové rozdíly. Zde se totiž ukazuje značná výhoda češtiny jako obtížného a v poměru k celkovému počtu obyvatelstva 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 seriózní 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 takřka jen 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 své potenciální oběti. Se současným rozvojem softwarových nástrojů automatického překladu ovšem lze do budoucna předpokládat nárůst počtu phishingových útoků na české občany ze zahraničí.

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), vyplnila 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.

3.4.1. Konkrétní podoba phishingu

Jedna z nejčastějších podob phishingu spočívá ve snaze pachatele vylákat z oběti údaje a hesla k internetovému bankovnictví, popř. číslo kreditní (platební)[187] karty, její dobu platnosti a tzv. Card Validation Code (CVC), tedy číslo k ověření platnosti karty nacházející se na její zadní straně. Pomocí těchto údajů pak může útočník z bankovního (karetního) účtu oběti odčerpat někdy i všechny finanční prostředky.

3.4.1.1. Přípravná fáze

Samotný útok obvykle probíhá v několika fázích. První z nich (přípravná fáze) zahrnuje opatřování potřebného (obrovského) počtu e-mailových adres potenciálních obětí. Toho lze dosáhnout hned několika způsoby. Jedním z nich je odkoupení (či jiné obstarání) databáze cizích e-mailových adres nashromážděných např. při sjednávání pojištění po internetu, registrace na různá fóra, atd. Ke koupi těchto databází může dojít buď od internetových obchodníků přímo (v rozporu se zásadami ochrany osobních údajů), nebo bývá sama terčem např. hackerských útoků na systémy, kde jsou tyto databáze uloženy. V dnešní době se objevují dokonce i webové servery a internetová fóra s omezeným přístupem (tzv. carding forums), kde probíhá čilý černý trh s kradenými osobními a finančními údaji.[188] Další způsob spočívá ve využití počítačového generátoru adres. Jedná se vlastně o počítačový program, který za pomocí slovníkových hesel, telefonních seznamů apod. a seznamu registrovaných domén uměle vytváří jednotlivé e-mailové adresy s tím, že lze očekávat, že existující adresy budou obsahovat kombinaci takovýchto slov. Při tomto způsobu sice vzniká obrovské množství neexistujících adres, to však útočníkům nevadí, pokud získají dostatečný počet adres existujících.

V této souvislosti je třeba si uvědomit, že phishingu značně napomáhá neostražitost uživatelů internetu, kteří neváhají svou soukromou e-mailovou adresu vyplnit při registraci i na stránkách, jejichž solidnost je minimálně pochybná. Koncový uživatel totiž prakticky nemá žádnou kontrolu, co se s jeho údaji vyplněnými při registraci děje a zda není třeba právě jeho e-mailová adresa poskytnuta třetím osobám. Pokud by si uživatelé internetu zřizovali více e-mailových schránek, přičemž jednu by např. používali k oficiální komunikaci a jednu jako tzv.

---

[187] Ve společnosti se obvykle oba výrazy zaměňují, resp. převažuje využívání výrazu „kreditní karty“ i pro karty platební. Z hlediska bankovního je však mezi oběma značný rozdíl, neboť prvně uvedený výraz slouží k čerpání prostředků z již bankou poskytnutého úvěru, jedná se tak v podstatě o úvěrovou kartu, v druhém případě se jedná o kartu sloužící k čerpání peněz – platbě – z běžného či sporožirového účtu.

[188] K tomu blíže v: Peretti, K. K.: Data Breaches: What the Underground World of “Carding” Reveals in: Santa Clara Computer and High Technology Journal, vol. 2. Santa Clara University, Santa Clara 2008, s. 375 a násl.

„spamovou“ schránku, která by byla využívána při nejrůznějších registracích na webových serverech, jistě by tím do značné míry omezili možnost být adresátem pokusů o phishing.

Součástí přípravné fáze pak rovněž bývá i vytvoření webových stránek pod takovou doménou, která odpovídá očekávání oběti o webové stránce, kam bude údaje (dobrovolně) vyplňovat. Pokud tedy útok míří kupříkladu na klienty určité banky, bude se útočník snažit napodobovat webové stránky internetového bankovnictví tohoto bankovního ústavu, a to pod doménou (adresou), která tomuto účelu bude odpovídat. Oběť pak snadněji uvěří, že jí vyplněné údaje míří do správných rukou. Zároveň pachatel s webovými stránkami vytvoří i e-mailovou adresu, ze které bude uskutečněn samotný útok a která bude rovněž názvem odpovídat obětí očekávanému odesílateli. Většina obětí phishingu totiž nepředpokládá, že by mohla obdržet e-mailovou zprávu od neznámého podvodníka, kterému adresu nikdy neposkytla, a tak slepě důvěřuje obsahu zpráv, které se tváří, že pochází od známých obchodníků, bank, apod.

3.4.1.2. Samotný phishingový útok

Po zmíněných přípravách následuje vlastní phishingový útok. Ten spočívá v rozeslání e-mailové zprávy na získané adresy schránek, která má za úkol přimět oběť k vyzrazení požadovaných údajů. Právě v této chvíli se uplatní metody sociálního inženýrství. I ta nejdůvěřivější osoba totiž nevyzradí tak důvěrné informace zcela bez důvodu. Zástěrka bývá v tomto ohledu různorodá, nejčastěji se lze setkat s tím, že pachatel vydávající se za bankovní ústav bude jejího klienta informovat o přechodu na nové (lepší) webové rozhraní internetového bankovnictví, pročež je zapotřebí, aby se klient na nich přeregistroval pomocí původních přihlašovacích údajů.

Rafinovanější varianta využívá obeznámenosti veřejnosti s existencí phishingu, a proto v tomto případě útočník kontaktuje oběť s tím, že její banka aktivně reaguje na zvyšující se phishingové nebezpečí. Z toho důvodu banka zavádí bezpečnější systém, kam se má klient přihlásit (pomocí stávajících údajů) a autentifikovat jejich pravost. Vždy je však v e-mailové zprávě uveden odkaz, který klienta přesměruje přímo na „zabezpečené“ stránky. V tuto chvíli nastává rozhodující chvíle, zda se phishingový útok vydaří, či nikoliv. Pokud bude oběť zprávě důvěřovat, útočníkovi s největší pravděpodobností v sítích uvízne. Odradit by jej totiž mohlo už jen podezřelé či nekvalitní zpracování webového rozhraní stránek, na které je odkaz poslal. V případě, že oběť „klikne“ na odkaz uvedený v e-mailové zprávě a na stránkách vytvořených útočníky údaje do podstrčeného formuláře vyplní, získají pachatelé okamžitě přístupové údaje k internetovému bankovnictví.

V nejrafinovanějších (a nejnebezpečnějších) případech útoků pak není poskytnut v e-mailu přímo link na pachatelovy stránky, ale je zde ukrytý např. javascript, který dokáže modifikovat zapsanou správnou adresu v prohlížeči uživatele. Někdy jsou při phishingu taktéž využívány hackerské metody jako cross site scripting.[189]

Typický phishingový e-mail má tuto podobu:[190]

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.

Zde je příklad z českého prostředí, nejprve poněkud úsměvný:[191]

„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.*

---

[189] Baudiš, P.: Staronové nebezpečí Rhybaření, časopis CHIP.CZ, č. 4/2006, s. 14
[190] Zdroj: http://en.wikipedia.org/wiki/Phishing, zobrazeno 11.8.2011, 21:35
[191] Zdroj: http://blog.jancermak.cz/phishing-ceska-sporitelna-sbirka-nejpopularnejsiho-spam-phishingu-poslednich-dni/2008/03/19/, zobrazeno 17.6.2008, 16:23

** 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:[192]

„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.“

3.4.1.3. Závěrečná fáze phishingu

Poslední fáze phishingového útoku konečně zahrnuje neoprávněné odčerpání prostředků z bankovního účtu oběti pomocí vylákaných přihlašovacích údajů, popř. zakoupení

[192] Idem

hodnotného zboží prostřednictvím vyzískaných údajů o kreditní kartě oběti. Jelikož elektronické peněžní přesuny bývají poměrně dobře vysledovatelné, využívají často pachatelé – organizátoři – nastrčených osob (bílých koní). V případě bezhotovostního odčerpání peněžních prostředků oběti tyto za určitou odměnu zakládají bankovní účty, na které následně phishingem podvodně získané finanční prostředky přicházejí. Ať již pomocí platebních karet v bankomatech či přímo na pobočce jsou neoprávněně nabyté prostředky vybírány a v hotovosti či právě pomocí platebních příkazů Western Union předávány hlavním pachatelům. V případě nákupu zboží pomocí údajů z platebních a kreditních karet spolupracují tito bílí koně nezřídka nevědomky. Pouze přijmou nikterak obtížnou „administrativní“ práci v podobě kontroly obsahu a přeposílání zásilek, které jim po uzavření „pracovní smlouvy“ začnou být ve velkém počtu doručovány, na předem dané adresy. Tímto způsobem je pak možné zastřít původ zboží z phishingových aktivit.

3.5. Prevence

V případě phishingu musí prevence této kriminality spočívat zejména ve 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 jevem (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. Rovněž by mělo být nezbytností zřízení další e-mailové schránky („spamové“), která by byla užívána pro registrace na různých webových stránkách. Původní e-mailová schránka by tak sloužila pouze k oficiální komunikaci s již ověřenými subjekty. Jejich uživatel by pak mohl přistupovat k jednotlivým zprávám do nich doručených právě s vědomím různého účelu, ke kterému by tyto schránky sloužily.

3.6. Trestní odpovědnost

3.6.1. Trestněprávní kvalifikace

Jednání pachatelů phishingu, pokud dojde k neoprávněnému odčerpání finančních prostředků oběti, lze podle českého trestního zákoníku kvalifikovat nejčastěji jako trestný čin podvodu dle ust. § 209 tr.zák.:

§ 209
Podvod

(1) Kdo 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, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Odnětím svobody na šest měsíců až tři léta bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 a byl-li za takový čin v posledních třech letech odsouzen nebo potrestán.

(3) Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 větší škodu.

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

a) spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny,
b) spáchá-li takový čin jako osoba, která má zvlášť uloženou povinnost hájit zájmy poškozeného,
c) spáchá-li takový čin za stavu ohrožení státu nebo za válečného stavu, za živelní pohromy nebo jiné události vážně ohrožující život nebo zdraví lidí, veřejný pořádek nebo majetek, nebo
d) způsobí-li takovým činem značnou škodu

(5) Odnětím svobody na pět až deset let bude pachatel potrestán,

a) způsobí-li činem uvedeným v odstavci 1 škodu velkého rozsahu, nebo
b) spáchá-li takový čin v úmyslu umožnit nebo usnadnit spáchání trestného činu vlastizrady (§ 309), teroristického útoku (§ 311) nebo teroru (§ 312).

(6) Příprava je trestná.

Tento trestný čin je systematicky zařazen do hlavy páté trestního zákoníku, 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 (§ 138 odst. 1 tr.zák.).

Pachatelem může být kdokoliv, včetně právnické osoby.

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 poškodit na nemajetkových právech (veřejně zostudí, hanobí, pomlouvá, atd.), bude možné jeho jednání kvalifikovat podle ustanovení § 209 tr.zák. jako trestný čin poškození cizích práv:

§ 181
Poškození 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 zákazem činnosti.

(2) Odnětím svobody až na tři léta bude pachatel potrestán,

a) způsobí-li činem uvedeným v odstavci 1 jinému značnou újmu na právech,

b) získá-li takovým činem pro sebe nebo pro jiného značný prospěch, nebo

c) vydává-li se při takovém činu za úřední osobu.

(3) Odnětím svobody na šest měsíců až pět let bude pachatel potrestán,

a) způsobí-li činem uvedeným v odstavci 1 jinému újmu na právech velkého rozsahu, nebo

b) získá-li takovým činem pro sebe nebo pro jiného prospěch velkého rozsahu.

Trestný čin dle § 181 tr.zák. spadá pod Trestné činy hrubě narušující občanské soužití hlavy II. trestního zákoníku. Objektem tohoto trestného činu jsou nemajetková práva osob.

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

Subjektem může být opět kdokoli (nemůže však jím být právnická osoba) a po subjektivní stránce se vyžaduje úmyslné zavinění.

Podle toho, jak pachatel phishingu neoprávněně obdržené údaje využije, může být jeho trestná činnost kvalifikována krom TČ podle § 209 tr.zák či § 181 tr.zák. i v rámci souběhu s různými jinými trestnými činy, např. TČ neoprávněného opatření, padělání a pozměnění

platebního prostředku podle § 234 odst. 1 tr.zák (pokud jsou vylákány přístupové údaje k elektronickému bankovnictví a tyto následně použity k výběru finančních prostředků z bankovního konta oběti),[193] nebo Hanobení národa, rasy, etnické nebo jiné skupiny osob dle § 355 tr.zák. (pod ukradenou identitou z phishingu pachatel veřejně hanobí občany židovské národnosti).

3.7. Závěr

Phishing je kriminální jednání značně nebezpečné. K jeho uskutečnění postačí elementární znalost fungování elektronické pošty, přitom šíře zasažených obyvatel bývá značná. Má rovněž obyčejně velice závažné důsledky, když odcizení přístupových údajů k účtu může vést až k vyvedení všech finančních prostředků z něj, 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.[194] Bankovní ústavy by proto měly 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.[195]

---

[193] K problematice možnosti postihu pouhého vylákání přístupových údajů k internetovému bankovnictví viz část III Úvahy de lege lata a de lege ferenda, kapitola 2.1.3. této práce

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

[195] Pro zajímavost je v příloze č. 5 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[196] 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.[197] 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.[198] 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 trestního zákona z roku 1961 ve znění platném do 1.7.1990 s hrozbou trestu odnětí svobody až na dvě léta v základní skutkové podstatě. Výsledky výpočtů mohly sloužit různým účelům od využití pro osobní potřebu až po tehdy zakázané soukromé podnikání. Zde se již pachatel dopustil výše uvedeného trestného činu v souběhu s trestným činem nedovoleného podnikání dle § 118 trestního zákona v tehdy platném znění. Typické pro trestný čin dle § 133 trestního zákona v tehdy platném znění byla však charakteristická vysoká latence tohoto druhu počítačové kriminality způsobená zejména vztahem občanů k „společnému, socialistickému vlastnictví“. Novelou č. 175/1990 Sb. byl trestný čin podle §

[196] Taktéž počítačového času
[197] Musil, S.: Počítačová kriminalita. První vydání. IKSP, Praha 2000, s. 11
[198] 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

133 z trestního zákona vypuštěn a krádeže počítačového času jsou od té doby kvalifikovány jako neoprávněné užívání cizí věci.[199]

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 v rozporu s pokyny zaměstnavatele k soukromým účelům. Může se tak dít častým prohlížením webových 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.[200] Je taktéž zřejmé, že tato forma je stižena velmi vysokou latencí. Ta vychází z již zmíněného historického vývoje krádeže strojového času 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.

---

[199] Blíže v kapitole Trestní odpovědnost této hlavy zvláštní části

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

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.[201]

Druhá varianta bývá obvykle označována jako krádež konektivity. Konektivita je vyjádřením schopnosti připojit se k síti internetu a charakteristika (rychlost) 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 své 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.

I zde ovšem platí, že nejlepší obranou proti krádežím konektivity je její prevence. K zamezení velké většině těchto jednání by bohatě postačovalo, kdyby oprávnění uživatelé přístup k tzv. přístupovým bodům (Access Points) šifrovali.[202] Rovněž je také třeba dbát na samotnou kvalitu šifrování. S rozvojem dešifrovacích programů a výpočetní kapacitou počítačů jsou některé způsoby šifrování, které postačovaly ještě před několika lety, dnes již (poměrně) jednoduše za pomocí určitých programů dešifrovatelné. Proto je třeba využívat vždy nejaktuálnější způsoby šifrování, které nabízí nejvyšší standard ochrany.

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 (Access 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

[201] V konkrétních podrobnostech hackerského jednání a jeho trestní odpovědnosti odkazuji na výklad v hlavě 2. Hackerství této části práce

[202] Srov. též Selvadurai, N., Islam, R., Gillies, P.: Unauthorised Access to Wireless Local Area Networks: The Limitations of the Present Australian Laws, in: Computer Law & Security Review. Vol. 25. Elsevier Science B.V., 2009, s. 537

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 spíše náhodně, např. při údržbě či opravách. V tomto případě můžeme již mluvit o krádeži, případně neoprávněném přístupu k počítačovému systému a nosiči informací.[203]

4.3. Trestní odpovědnost

4.3.1. Zneužívání počítačového času a jeho škodlivost pro společnost

Jako u mnoha jiných druhů internetové kriminality bude i v případě zneužívání počítačového času v souvislosti s internetem hledisko subsidiarity trestní represe významným korektivem pro určení, zda bude proti delikventovi uplatňována trestní odpovědnost. To platí zejména u vnitřní formy krádeže strojového času, neboť zde 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)[204] 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, a to zejména proto, že žalobkyně pracovala v exekutorské kanceláři, nebyla dle soudu intenzita tohoto porušení natolik významná, aby splnila podmínku porušení pracovních povinností zvláště hrubým způsobem. Okamžité zrušení pracovního poměru tak nebylo ze strany zaměstnavatele oprávněné. Je zřejmé, že pokud intenzita porušení pracovněprávních povinností žalobkyně nebyla ani dostatečná k naplnění

[203] Viz dále
[204] Usnesení Nejvyššího soudu ČR ze dne 17.10.2006, sp.zn.: 21 Cdo 84/2006

důvodu okamžitého zrušení pracovního poměru, tedy nejpřísnější pracovněprávní odpovědnosti, těžko bychom mohli dovodit (i kdyby z formálního hlediska byla naplněna skutková podstata nějakého trestného činu) trestní odpovědnost této zaměstnankyně (*arg. a minori ad maius*).

V jiném případě vnitřní krádeže počítačového času řešeném ve Spolkové republice Německo Spolkový pracovní soud (Bundesarbeitsgericht) svým rozsudkem ze dne 7.7.2005 sp.zn. 2 AZR 581/04[205] 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 byly splněny podmínky trestní odpovědnosti, je nutné zvážit více aspektů. Určujícím dle názoru autora této práce 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 prospěchu, např. podnikání. Dle mého názoru tak ani v posuzovaném německém případě nebyl stupeň společenské škodlivosti takový, aby nepostačovala k potrestání odpovědnost pracovněprávní, i když je jistě o něco vyšší než v popsané české kauze.

U krádeže konektivity bude určujícím kritériem společenské škodlivosti jednak doba trvání trestné činnosti a jednak opět účel aktivit pachatele. Proto bude hardwarová krádež konektivity většinou trestná. 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. V této věci rozhodoval i Nejvyšší soud ČR (sp.zn.: 7 Tdo 64/2005), když odmítl dovolání žalovaného 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."[206]

---

[205] Zdroj: http://www.lawcommunity.de/volltext/130.html, zobrazeno 9.6.2008, 15:17

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

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 § 207 odst. 1 alinea 2 tr.zák.:

§ 207
Neoprávněné užívání cizí věci

(1) Kdo se zmocní cizí věci nikoli malé hodnoty nebo motorového vozidla v úmyslu je přechodně užívat, nebo

kdo na cizím majetku způsobí škodu nikoli malou tím, že neoprávněně takové věci, které mu byly svěřeny, přechodně užívá,

bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti.

(2) Odnětím svobody na šest měsíců až tři léta nebo zákazem činnosti bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 jako osoba, která má zvlášť uloženou povinnost hájit zájmy poškozeného,

b) spáchá-li takový čin jako člen organizované skupiny, nebo

c) *způsobí-li takovým činem značnou škodu.*

(3) Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán,

a) způsobí-li činem uvedeným v odstavci 1 škodu velkého rozsahu, nebo

b) spáchá-li takový čin v úmyslu umožnit nebo usnadnit spáchání trestného činu vlastizrady (§ 309), teroristického útoku (§ 311) nebo teroru (§ 312).

Tento trestný čin je systematicky zařazen mezi trestné činy proti majetku do hlavy páté zvláštní části trestního zákoníku.

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 § 138 odst. 1 tr.zák. rozumí škoda ve výši alespoň 25.000,- Kč. Trestní zákoník tak vyjadřuje daleko nižší typovou škodlivost 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. To už samo o sobě bude vylučovat trestnost takřka jakékoliv krádeže počítačového času, neboť zaměstnanec si bude muset být vědom nejenom možnosti způsobení škody nikoliv malé, ale dokonce i s ní být minimálně srozuměn.

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.

Doslovné znění TČ neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 2 písm. a) tr.zák. může svádět ke kvalifikaci vnitřní krádeže počítačového podle tohoto trestného činu. Autor této práce však s takovou kvalifikací nesouhlasí. Bylo by totiž absurdní, aby zaměstnanec, který neoprávněně použije jakoukoliv věc ve vlastnictví zaměstnavatele, která mu jím byla svěřena, musel k trestnosti svého počínání zároveň toto činit s úmyslem způsobit tak škodu alespoň 25.000,- Kč, oproti zaměstnanci, který by neoprávněně využíval internetové připojení zaměstnavatele (tedy i jeho hardware a software) a který by tak mohl být trestný vždy bez ohledu na jakoukoliv škodu a zavinění k ní se vztahující. Rovněž by bylo nesmyslné, aby takové jednání sice nebylo důvodem pro okamžité zrušení pracovního poměru, ale přitom bylo trestným činem. Ustanovení § 230 odst. 2 písm. a) tr.zák. tak bude dopadat na případy speciální k neoprávněnému užívání věci, jako bude např. počítačová špionáž, kdy pachatel získá některá citlivá data uložená v systému oběti (zaměstnavatele), tyto si zkopíruje a použije pro svou potřebu, či je někomu předá (poskytne). Na „obyčejné“ užití internetu v rozporu s pokyny zaměstnavatele však dopadat nebude.

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 jiného zařízení pro automatické zpracovávání dat (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 § 207 odst. 1 alinea 1 tr.zák. (a to pokud se

jedná pouze o krátkodobé jednání),[207] a trestný čin neoprávněného přístupu k počítačovému systému nebo nosiči informací podle § 230 odst. 1 tr.zák. (v případě že bude síť zakódovaná), nebo jako krádež dle § 247 odst. 1 písm. a) tr.zák.:

§ 205
Krádež

(1) Kdo si přisvojí cizí věc tím, že se jí zmocní, a

a) způsobí tak na cizím majetku škodu nikoliv 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) čin spáchá na území, na němž je prováděna nebo byla provedena evakuace osob,

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

(2) Kdo si přisvojí cizí věc tím, že se jí zmocní, a byl za takový čin v posledních třech letech odsouzen nebo potrestán, bude potrestán odnětím svobody na šest měsíců až tři léta.

(3) Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 nebo 2 větší škodu.

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

a) spáchá-li čin uvedený v odstavci 1 nebo 2 jako člen organizované skupiny,
b) spáchá-li takový čin za stavu ohrožení státu nebo za válečného stavu, za živelní pohromy nebo jiné události vážně ohrožující život nebo zdraví lidí, veřejný pořádek nebo majetek, nebo
c) způsobí-li takovým činem značnou škodu.

(5) Odnětím svobody na pět až deset let bude pachatel potrestán,

a) způsobí-li činem uvedeným v odstavci 1 nebo 2 škodu velkého rozsahu, nebo
b) spáchá-li takový čin v úmyslu umožnit nebo usnadnit spáchání trestného činu vlastizrady (§ 309), teroristického útoku (§ 311) nebo teroru (§ 312).

(6) Příprava je trestná.

Jak vyplývá ze znění § 207 odst. 1 alinea 1 tr.zák., musí k naplnění skutkové podstaty TČ neoprávněného užívání cizí věci 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.

[207] Znění viz výše

Jiná je situace u zmiňované krádeže. V tomto případě dochází k dlouhodobému využívání konektivity či její části, čímž je jistě možné způsobit škodu nikoli nepatrnou, tedy dle § 138 odst. 1 tr.zák. škodu alespoň 5.000,- Kč, a to zejména pokud oprávněný přijde v důsledku pachatelova jednání o připojení k internetu zcela.

Otázku, zda konektivita může vůbec být předmětem krádeže, lze zodpovědět interpretací § 134 odst. 1 věta 1 tr.zák., který stanoví, že věcí se rozumí i ovladatelná přírodní síla. Trestněprávní nauka tak dovozuje, že věcí je i elektrická energie, parní energie, atd.[208] 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.[209]

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 (vyjma právnických osob) a vyžaduje se úmyslné zavinění.

Pokud však ke krádeži konektivity nebo jejímu neoprávněnému krátkodobému využívání dojde po tom, co pachatel musel překonat určité bezpečnostní opatření (typicky pomocí vlastního softwaru překoná šifrování sítě), bude současně trestný i pro trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 odst. 1 tr.zák.[210, 211]

V případě krádeže konektivity spolu s provedeným zásahem do počítačového systému či jiného technického zařízení pro zpracování dat lze toto jednání kvalifikovat jako TČ neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 odst. 2 písm. d) tr.zák.[212] Při naplnění obou skutkových podstat se může jednat i o jednočinný souběh trestného činu krádeže a TČ podle § 230 odst. 2 písm. d) tr.zák. Tyto dva trestné činy totiž postihují jiný objekt. V prvém případě je to vlastnictví konektivity, resp. ochrana před

---

[208] Srov. přiměřeně např. Jelínek, J. a kol.: Trestní právo hmotné. Obecná část. Zvláštní část. 3. přepracované a aktualizované vydání. Linde Praha, a.s., Praha 2008, str. 698 a usnesení Nejvyššího soudu ČR ze dne 5.5.2004, sp.zn. 7 Tdo 487/2004

[209] Shodně např. Matejka, J.: Za krádež konektivity do vězení? Už i v ČR, na adrese http://www.lupa.cz/clanky/za-kradez-konektivity-do-vezeni-uz-i-v-cr/, zobrazeno 10.5.2011, 10:30

[210] znění a podrobnosti o tomto trestném činu viz hlava 2. Hackerství této části práce

[211] V některých právních úpravách v zahraničí však k trestnosti není požadováno překonání bezpečnostních opatření a za trestné se považuje samotné neoprávněné získání přístupu k počítačovému systému – srov. např. Singapurskou úpravu v Leng, T., K.: Wireless Internet Access and Potential Liabilities in: Computer Law & Security Report. Vol. 23. Elsevier Science B.V., 2007, s. 550 a násl.

[212] Viz poznámka č. 208

omezením nebo zbavením internetového připojení. V druhém případě je to ochrana počítače či jiného technického zařízení pro zpracování dat. Vztah speciality je proto zde dle názoru autora této práce vyloučen.

4.4. Závěr

Zneužívání počítačového času v souvislosti s internetem a krádeže konektivity jsou, ač málo diskutovány, v naší společnosti poměrně častým jevem, který se může značně lišit co do společenské škodlivosti. Případy tzv. vnitřního zneužívání počítačového času nejsou povětšinou společensky škodlivé natolik, aby byla uplatňovaná trestní odpovědnost delikventa, a 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, a to na úkor svých obětí.

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. S trochou nadsázky by její kořeny mohly sahat až do dob pravěkých v podobě různých jeskynních maleb výrazných svou sexuální tématikou či sošek pravěkých Venuší (např. v Čechách známá Věstonická Venuše či jedna z nejstarších nalezených, Venuše z Hohle Fels[213]), které však spíše symbolizovaly plodnost.

Hranice mezi uměním, erotikou, uctíváním plodnosti a pornografií v dnešním slova smyslu byla vždy neostrá, ostatně pojem pornografie vznikl až v devatenáctém století ve Francii.[214] Tak tomu bylo zejména v době, kdy erotika byla součástí umění. To vše však změnil příchod fotografie a filmu, které umožňovaly vytvářet explicitní sexuální vyobrazení bez nároku na to být označována za jakékoliv umění. Záhy po vynálezu filmu bratry Lumièrovými v roce 1895 vznikla i filmová díla s erotickou tématikou, a to konkrétně Le Coucher de la Marie od Eugèna Piroua z roku 1896.[215] Otevřela se tak cesta vzniku pornografického průmyslu. Další milník v historii pornografie představuje příchod internetu, který znamenal boom pro její šíření a zpřístupnění.

Přijímání erotické a pornografické tvorby se v průběhu času velmi měnilo a lišilo se i v závislosti na konkrétním místě. Vnímání erotiky např. v Indii v průběhu středověku se tak značně odlišovalo od jejího přijímání, přesněji však odsuzování v puritánské Anglii. Tomu odpovídá i vývoj trestněprávního postihu pornografie.

Jelikož předmětem této práce není kriminologická a trestněprávní analýza pornografické kriminality jako celku, ale rozbor internetové kriminality, bude se tato hlava zvláštní části této práce krátce zabývat zejména těmi aspekty pornografie, které jsou podmíněny právě internetem, a jejichž sankcionováním se trestní právo zabývá.

5.2. Vymezení pojmu pornografické dílo

Pojem pornografického díla není v žádném právním předpise České republiky legálně definován. Legální definici pornografického díla nepřinesl ani nový trestní zákoník, když dle

---

[213] http://www.nature.com/news/2009/090513/full/news.2009.473.html, zobrazeno 10.4.2012, 15:06
[214] http://en.wikipedia.org/wiki/Pornography, zobrazeno 10.4.2012, 16:25
[215] Bottomore, S.: "Eugène Pirou" in: Herbert, S., McKernan, L. eds.: Who's Who of Victorian Cinema, British Film Institute, 1996

jeho důvodové zprávy není jeho součástí „*definice pornografického díla především s ohledem na to, že posuzování tohoto pojmu nečiní v praxi potíží. Ve smyslu platné judikatury se za pornografické dílo považuje jakýkoli předmět, který zvláště intenzivním a vtíravým způsobem zasahuje a podněcuje samotný sexuální pud. Současně takové dílo hrubě porušuje uznávané morální normy společnosti a vyvolává pocit studu.*“[216] Autor této práce si uvedeným názorem není úplně jistý. Jinou definici pornografického díla totiž přinesl Ústavní soud ČR v usnesení ze dne 19.04.2004, sp.zn.: IV.ÚS 606/03, U 23/33 SbNU 453, podle kterého 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*“. Z uvedeného je tedy patrné, že Ústavní soud na rozdíl od důvodové zprávy k trestnímu zákoníku a judikatury Nejvyššího soudu akcentuje v definici morální aspekty (vzbuzení morálního pohoršení), což i plně koresponduje s chráněným zájmem v případě trestního postihu pornografie, tj. veřejné morálky, ochrany před zvláštním druhem obtěžování v oblasti mravnosti a mravní výchovy dětí.[217] Tento objekt byl ostatně přímo vyjádřen v původním názvu trestného činu šíření pornografie, tedy ohrožování mravnosti.

Rovněž odlišnou definici využívá současná trestněprávní teorie, která naopak akcentuje sexuální stránku pornografie, když za „*pornografické dílo se považuje takové dílo, jehož jediným účelem je vyvolat (zvyšovat) sexuální vzrušení*“.[218] Podobnou definici stanoví slovenský trestný zákon č. 300/2005 Z.z. v ustanovení § 132 odst. 2, podle kterého „p*ornografiou sa na účely tohto zákona rozumie zobrazenie súlože, iného spôsobu pohlavného styku alebo iného obdobného sexuálneho styku alebo zobrazenie obnažených pohlavných orgánov smerujúce k vyvolaniu sexuálneho uspokojenia inej osoby*“.

Dle názoru autora této práce je výhodné definici pornografie vázat na obecné pojetí morálky, neboť vzhledem k posunu jejího obsahu v čase může tato definice přetrvat delší dobu. Jak již bylo nastíněno výše, vnímání, co ještě pornografií je a co už není, se v čase vyvíjelo a kupříkladu ještě na začátku 20. století by za pornografii byly označovány i některé dnešní hollywoodské trháky, kde při určitých scénách jsou jejich aktéři vyobrazeni nazí přímo při

[216] Důvodová zpráva k § 188 – 190 (dnes 191 – 193) vládního návrhu trestního zákoníku, Poslanecká sněmovna Parlamentu České republiky, 5. volební období, 2006-2010, sněmovní tisk č. 410/0
[217] Jelínek J. a kol.: Trestní právo hmotné. 2. vydání. Praha: Leges, 2010, s. 561
[218] Idem

souloži. Z toho důvodu se autor této práce přiklání k výše zmíněné definici Ústavního soudu ČR.

Za pornografické dílo však není možné považovat samotné zobrazení nahého lidského těla v adekvátní situaci (např. při koupání). O pornografickém charakteru pak musí rozhodovat obsah celého díla, tedy objektivní celková tendence a povaha tohoto díla.[219] V tomto smyslu nebudou z hlediska trestního práva za pornografické označovány umělecká díla, a to i když by vyvolávala sexuální vzrušení či vzbuzovala pocit studu, předměty pornografického charakteru historické hodnoty či předměty určené k vědeckým, osvětovým apod. účelům.[220]

5.3. Druhy a formy pornografie

5.3.1. Druhy pornografie

Z hlediska intenzity se rozlišuje pornografie lehká („soft core“) a tvrdá („hard core“). Liší se od sebe zejména tím, že soft core detailně nezobrazuje penetraci pohlavních orgánů. Buď k ní vůbec nedochází (typicky u „pouhého obnažování“), nebo je zakryta pohledu diváka ať už samotnými těly aktérů, nebo přikrývkou, kamerovými triky apod. U hard core pornografie se adresátům naskýtá možnost penetraci genitálií (pohlavním orgánem, prsty, různými předměty) zcela detailně pozorovat.

Z kriminologického hlediska je třeba rozlišovat pornografii prostou a pornografii deviantní (zvrácenou),[221] která zobrazuje pedofilní, sadomasochistické, zoofilní, nekrofilní apod. praktiky.

Oproti tomu je v komentáři k trestnímu zákoníku autorského kolektivu pod vedením prof. Šámala[222] obsaženo člení pornografie podle obsahu na:

a) tvrdou, v níž se projevuje násilí či neúcta k člověku nebo které znázorňuje pohlavní styk se zvířetem,
b) pornografii dětskou a
c) pornografii prostou, kterou tvoří ostatní pornografická díla.

---

[219] Idem
[220] Šámal, P. a kol.: Trestní zákoník II. § 140 – 421. Komentář. 1. vydání. C. H. Beck, Praha 2010, s. 1695
[221] Jelínek J. a kol., op. cit., s. 562
[222] Šámal, P. a kol., op. cit., s. 1695

Toto členění má však smysl pouze z hlediska české trestněprávní úpravy, neboť „tvrdost" obsahu první skupiny při tomto dělení lze spatřovat pouze v tom, že jeho výroba a jiné nakládání zakládá trestní odpovědnost podle § 191 odst. 1 tr. zákoníku. Některá pornografická díla zobrazující neúctu k člověku však mohou být zařazena do „soft core" pornografie, což uvedené členění nereflektuje. Naopak při tomto dělení by za tvrdou pornografii nebylo lze označit pornografii nekrofilní a ani jinou deviantní pornografii než sadomasochistickou či zoofilní.

5.3.2. Formy pornografie

Forma pornografického díla může být rozličná. Trestní zákoník je demonstrativně vypočítává jako písemná, fotografická, filmová, počítačová a elektronická. Lze si i představit pornografické dílo zachycené na zvukovém nosiči (gramofonová deska, audio kazeta, CD…) a ve formě plastiky (sochy). U písemných děl bude často obtížné rozlišit mezi „uměleckým" literárním dílem a pornografií, zejména pokud je autor znám i neerotickou publikační činností. Jako typický příklad lze uvést román Guillauma Apollinaira Hrdinské činy mladého dona Juana,[223] který je doslova protkán explicitními popisy sexuálních praktik jednotlivých postav románu.

5.3.3. Pornografie jako kriminologický jev

V případě, že budeme na pornografii nahlížet pod zorným úhlem kriminologie, je třeba si uvědomit, že ne vždy je pornografie vnímána jako společensky škodlivý jev. Existují různé praktiky a stupně pornografie (od erotických děl a lehkého porna, přes „hardcore" explicitně zobrazující pohlavní styk v nejrůznějších polohách (někdy i počtech osob) až po extrémně tvrdou (zvrácenou) pornografii). 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 (skutečně) dětských či sadistických pornografických děl.

[223] Apollinaire, G.: Les Exploits D'Un Jeune Don Juan. Paříž: 1907

5.4. Typy jednání v prostředí internetu

5.4.1. Šíření zvrácených praktik

V prostředí sítě internetu se můžeme setkat s 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. ke stažení, nebo je sdílí v peer to peer sítích.

Internet tak umožňuje nevídanou přístupnost těchto zvrácených praktik, když podle některých studií[224] vzrostl mezi lety 1997 a 2005 počet vyobrazení dětské pornografie dostupných na internetu o 1.500 %! 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.[225]

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 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 organizaci National Center 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.[226]

---

224 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

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

226 http://missingkids.com/missingkids/servlet/NewsEventServlet?LanguageCountry=en_US&PageId=3644, zobrazeno 31.5.2008, 16.20

5.4.2. Zpřístupňování pornografie dětem a mladistvým

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 dostupným 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 neinternetové distribuci pornografických děl (nikoliv extrémních praktik – viz výše), ale zároveň považuje za trestnou distribuci prostřednictvím internetu.

Autor této práce osobně nevnímá 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 samozřejmě nemělo být umožněno přístup k takovýmto materiálům.

Na tomto místě je důležité se taktéž zmínit o tom, že drtivá většina pornografických[227] děl na internetu není zpřístupněna za účelem jejich zhlédnutí dětmi. Na rozdíl od serverů poskytujících např. neoprávněně hudbu či odkazy na tyto servery,[228] se stránky věnované pornografii, i když jsou tam taktéž umístěny reklamy, týkají 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 děl, který se uskutečňuje výhradně elektronickými (internetovými) platebními kartami, ke kterým děti nemají obvykle přístup.[229]

---

[227] Dále v tomto oddíle ve významu pornografie bez zvrácených praktik
[228] Viz hlava 1 zvláštní části této práce
[229] Podobně probíhá i nákup zboží, které jsou předmětem reklam umístěných na pornografických serverech

Dle názoru autora této práce by neměla prevence zpřístupňování pornografických děl dětem být uskutečňována tím, že bude kriminalizováno 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 pruderií)[230] 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).

5.5. Trestněprávní aspekty

5.5.1. Pornografie a společenská škodlivost

Jak plyne z výše uvedeného výkladu, je vnímání společenské škodlivosti pornografie třeba pojímat různě u odlišných typů jednání vztahujících se k pornografii na internetu. Jako spolehlivě nejzávažnější musí být pokládána jakákoliv pornografie zobrazující skutečné 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. V Evropě se obvykle animovaná dětská pornografie posuzuje stejně jako reálné zneužívání dětí a je trestná. Podobně k ní přistupuje i současná úprava trestního zákoníku.[231]

5.5.2. Úprava zpřístupňování pornografie dětem a výroba a šíření deviantní pornografie

Nový trestní zákoník, stejně jako trestní zákon z roku 1961 ve znění účinném do 31.12.2009,[232] postihuje pornografii v rámci třech různých trestných činů, z nichž první, šíření pornografie podle § 191 tr. zák., upravuje jednak zpřístupňování jakékoliv pornografie dětem a jednak vybrané formy výroby a šíření deviantních pornografických děl:

---

[230] Musil, S.: Počítačová kriminalita. IKSP, Praha 2000, str. 276
[231] Blíže v části III Úvahy de lege lata a de lege ferenda, kapitola 2.1.4. této práce
[232] Úprava postihu pornografie totiž na sklonku platnosti původního trestního zákona z roku 1961 vycházela z návrhu nového trestního zákoníku

§ 191

Šíření pornografie

(1) 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, v němž se projevuje násilí či neúcta k člověku, nebo které popisuje, zobrazuje nebo jinak znázorňuje pohlavní styk se zvířetem, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Kdo písemné, fotografické, filmové, počítačové, elektronické nebo jiné pornografické 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.

(3) Odnětím svobody na šest měsíců až tři léta 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 jeden rok až pět 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 je zcela nově zařazen nikoliv mezi trestné činy narušující soužití lidí (nyní zařazených jako díl 5. hlavy X tr.zák., trestné činy proti pořádku ve věcech veřejných), nýbrž do hlavy III tr.zák., trestné činy proti lidské důstojnosti v sexuální oblasti.

K pojmu pornografické dílo viz výše. Objektem tohoto trestného činu je zájem na ochraně před zvláštním druhem obtěžování v oblasti mravnosti a mravní výchova mládeže, lidská důstojnost a ochrana psychické integrity jedince, obecně také občanské soužití.[233]

Objektivní stránka základní skutkové podstaty uvedené v odst. 1 tohoto ustanovení spočívá v konkrétních formách výroby a šíření (zpřístupňování) sadomasochistických a zoofiliích pornografických děl. V případě další základní skutkové podstaty, která je upravena v odst. 2 citovaného ustanovení, spočívá objektivní stránka v tam uvedených podobách zpřístupňování jakékoliv pornografie dětem, a to včetně jejího vystavování na místech, které je dětem přístupné. Pachatelem může být kdokoli.

---

[233] Jelínek, J. a kol.: op. cit., s. 561

Z hlediska internetové kriminality je zvláště významná kvalifikovaná skutková podstata v § 191 odst. 3 písm. b) tr.zák., která podmiňuje použití vyšší trestní sazby tím, že pachatel spáchá tento trestný čin veřejně přístupnou počítačovou sítí, čímž má zákonodárce na mysli zejména internetovou síť.[234]

Subjektivní stránka vyžaduje zavinění úmyslné. Problematické bude zejména stanovit formu zavinění v případě zpřístupnění pornografie dětem prostřednictvím internetu. Mnoho provozovatelů serverů zabývajících se pornografií ji totiž zpřístupňovat nezletilým nechce, a ani s tím nejsou srozuměni. Jelikož ale nemohou 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.[235] Je zřejmé, že tato stránka neodradí „zvídavé" děti od vstupu, dle názoru autora této práce však může mít toto řešení vliv na posouzení zavinění pachatele, který se tak zbaví trestní odpovědnosti za tento úmyslný trestný čin.

5.5.3. Úprava postihu dětské pornografie a jejího držení

Dětská pornografie je v trestním zákoníku postihována v rámci trestného činu výroby a jiného nakládání s dětskou pornografií podle § 192 tr. zákoníku a trestného činu zneužití dítěte k výrobě pornografie podle § 193 tr.zák.:

§ 192
Výroba a jiné nakládání s dětskou pornografií

(1) Kdo přechovává fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě nebo osobu, jež se jeví být dítětem, bude potrestán odnětím svobody až na dva roky.

(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, které zobrazuje nebo jinak využívá dítě nebo osobu, jež se jeví být dítětem, 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 nebo propadnutím majetku bude pachatel potrestán, spáchá-li čin uvedený v odstavci 2

---

[234] Ohledně možnosti postihu podle této skutkové podstaty v případě rozeslání pornografického díla e-mailem, viz část III Úvahy de lege lata a de lege ferenda, kapitola 2.1.4. této práce
[235] Ukázka viz přílohu č. 6 této práce

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 nebo propadnutím majetku bude pachatel potrestán, spáchá-li čin uvedený v odstavci 2

a) jako člen organizované skupiny působící ve více státech, nebo

b) úmyslu získat pro sebe nebo pro jiného prospěch velkého rozsahu.

§ 193

Zneužití dítěte k výrobě pornografie

(1) Kdo přiměje, zjedná, najme, zláká, svede nebo zneužije dítě k výrobě pornografického díla nebo kořistí z účasti dítěte na takovém pornografickém díle, bude potrestán odnětím svobody na jeden rok až pět let.

(2) Odnětím svobody na dvě léta až šest let bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1

a) jako člen organizované skupiny, nebo

b) v úmyslu získat pro sebe nebo pro jiného značný prospěch.

(3) Odnětím svobody na tři léta až osm let bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1

a) jako člen organizované skupiny působící ve více státech, nebo

b) v úmyslu získat pro sebe nebo pro jiného prospěch velkého rozsahu.

První z uvedených trestných činů oproti předcházející úpravě postihuje nejen držení dětské pornografie, ale i její výrobu, šíření a kořistění na ní, jak ostatně vyplývá z nového názvu tohoto trestného činu. Zároveň tak byl postih výroby a různých forem šíření dětské pornografie zcela vyčleněn z úpravy trestného činu šíření pornografie podle § 191 odst. 1 tr.zák., se kterou do přijetí nového trestního zákoníku byl spojen, a přesunut do tohoto samostatného (speciálního) trestného činu. Posledním trestným činem vztahujícím se k postihu pornografie je zneužití dítěte k výrobě pornografie podle § 193 tr. zákoníku. Ten byl přejat ve zcela nezměněné podobě z předchozí úpravy v trestním zákoně účinné od 1.12.2007.

Zákonodárce tím, že přenesl postih dětské pornografie do dvou samostatných trestných činů, dal zcela jasně najevo, že ve středu jeho zájmu trestní represe pornografických děl je zejména postih dětské pornografie. To je vyjádřeno i poměrně značným snížením trestních sazeb u trestného činu šíření pornografie. Tak např. již v základní skutkové podstatě postihující výrobu a jiné nakládání se zoofilní a sadomasochistickou pornografií hrozí nyní pouze trest odnětí svobody až na jeden rok oproti 6 měsícům až tří let v případě původní úpravy.

Úplné vyčlenění dětské pornografie dle názoru autora tohoto článku dobře vystihuje rozdílnost postihu dětské pornografie a ostatních deviantních forem pornografie. V druhém případě je totiž chráněna zejména veřejná morálka v sexuální oblasti, v prvém případě jsou však primárně chráněny děti před jejich zneužíváním pro pornografické účely. V případě šíření pornografie jsou tak především chráněni její destinatáři ať už povšechně v podobě obecných mravů nebo konkrétně děti v případě § 191 odst. 2 tr.zák. Ochrana osob či předmětů, které jsou v/na pornografických dílech zobrazeny či popsány již tak důležitá není.[236] U dětské pornografie naopak trestní represe slouží k ochraně dětských aktérů, tedy osob účastnících se výroby pornografie. Vůdčí myšlenka k tomuto rozlišení je jednoduchá – tvrdší postih za zneužívání dětí k výrobě pornografie implikuje méně fakticky zneužívaných dětí. Tomu odpovídá i zvýšená trestní sazba u dětské pornografie oproti jejím ostatním deviantním formám.

I u těchto trestných činů je vyžadováno zavinění. Stejně jako v případě TČ podle § 191 tr.zák. bude i u trestného činu výroby a jiného nakládání s dětskou pornografií z hlediska internetové kriminality důležitá kvalifikovaná skutková podstata v § 192 odst. 3 písm. b) tr.zák. obsahující zvláště přitěžující okolnost v podobě spáchání tohoto trestného činu veřejně přístupnou počítačovou sítí.

Novelou trestního zákoníku č. 330/2011 Sb., byly změněny základní skutkové podstaty TČ výroby a jiného nakládání s dětskou pornografií v odst. 1 a 2 ohledně okruhu pornografických děl, na které dopadá postih dětské pornografie, a to rozšířením o díla zobrazující nebo jinak využívající *osobu, jež se jeví být dítětem*. Tato změna přinesla do značné míry další rozšíření trestní represe týkající se dětské (či zdánlivě dětské) pornografie. Toto doplnění se autorovi této práce jeví být dosti problémové a bude diskutováno v následující části této práce, v kapitole 2.1.4.

Ani u jednoho z trestných činů postihujících dětskou pornografii není trestná příprava. K tomu je totiž třeba, aby tak trestní zákoník u příslušného trestného činu výslovně stanovil, navíc přichází v úvahu jen u zvlášť závažných zločinů, jimiž jsou ty úmyslné trestné činy, na něž trestní zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně deset let.[237] Žádný z výše uvedených trestných činů podle § 191 – 193 tr.zák. obě tyto podmínky nesplňuje, a to ani v nejvyšších odstavcích (maximální horní hranice trestní sazby je zde 8 let v případě § 192 odst. 4 a § 193 odst. 3 tr.zák.). Dle stávající úpravy v trestním zákoníku

[236] Ochranu zneužití zvířat k výrobě pornografie lze postihovat podle trestného činu týraní zvířat podle § 302 tr.zák.
[237] Srov. § 20 odst. 1 a § 14 odst. 3 in fine tr.zák.

tak nelze trestně postihnout pachatele, kteří spáchání těchto trestných činů pouze připravovali.

Určitou korekci netrestnosti přípravy výroby a šíření dětské pornografie představuje samotný trestný čin zneužití dítěte k výrobě pornografie podle § 193, který lze považovat za předčasně dokonaný trestný čin, resp. za zvláště trestné účastenství na trestném činu výroby a jiného nakládání s dětskou pornografií. Podle něj bude za dokonaný trestný čin odsouzen i např. pachatel, který svede nebo zláká dítě k výrobě pornografie, aniž by pornografické dílo začal vůbec vyrábět, tedy bude trestný za jednání, které materiálně představuje pouze přípravu k výrobě dětské pornografie. Podobně bude trestný i ten, kdo kořistí na účasti dítěte na výrobě dětské pornografie kupříkladu tím, že za úplatu dítě jemu svěřené k pornografické produkci každý týden přiveze…[238] I zde se tak bude jednat o zvláště trestnou účast na trestném činu. Konečně lze za zvláště trestné účastenství pokládat i ustanovení § 192 odst. 2 alinea 2 tr.zák., které stanoví trestnost i za kořistění ze samotného pornografického díla (nikoliv však z účasti dítěte na její výrobě jako v předchozím případě).

5.5.4. Vzájemný vztah jednotlivých ustanovení postihujících pornografii a případy vyloučení jednočinného souběhu

Rozdělení postihu výroby a šíření pornografie na trestné činy upravující pouze dětskou pornografii a na trestný čin šíření pornografie postihující ostatní druhy pornografie s sebou přineslo určitou změnu v náhledu na možnost jednočinných souběhů dotčených trestných činů. Podle nového trestního zákoníku tak trestný čin výroby a jiného nakládání s dětskou pornografií podle § 192 odst. 2 tr.zák. je speciálním ustanovením k trestnému činu šíření pornografie podle § 191 odst. 1 tr. zák., neboť dopadá na zúžený okruh případů, a to konkrétně výrobu a šíření pouze pornografie dětské. V daném případě tak bude přicházet v úvahu jedině jednočinný souběh trestného činu podle § 191 odst. 2 tr.zák. a trestného činu podle § 192 odst. 2 tr.zák., a to pokud pachatel vyrobí nebo šíří dětskou pornografii za účelem ji zpřístupnit dítěti, což také následně učiní.

Zajímavý je rovněž vztah trestného činu výroby a jiného nakládání s dětskou pornografií podle § 192 odst. 2 tr.zák. a trestného činu zneužití dítěte k výrobě pornografie podle § 193 tr.zák. Jak již bylo uvedeno výše, představuje posléze uvedený trestný čin zvláště trestnou přípravu či pomoc k trestnému činu podle § 192 odst. 2 vztahujícího se k výrobě dětské pornografie, která je ovšem znatelně přísněji trestná. Z toho vyplývá, že trestný čin zneužití dítěte k výrobě pornografie je speciálním trestným činem a jednočinný souběh s trestným

[238] Šámal, P. a kol., op. cit., s. 1710, marg. č. 4

činem podle § 192 odst. 2 tr.zák., pokud jde o výrobu, je vyloučen. Obdobně to platí o kořistění z dětského pornografického díla a z účasti dítěte na takovém pornografickém díle.[239] Na druhou stranu nebude vyloučen jednočinný souběh obou uvedených trestných činů, pokud po výrobě pornografického díla dojde následně k jinému nakládání s pornografickým dílem.[240]

Z výše uvedeného vyplývá, že ač lze považovat trestné činy postihující dětskou pornografii za speciální k trestnému činu šíření pornografie podle § 191 tr.zák., přičemž trestný čin zneužití dítěte k výrobě pornografie podle § 193 tr.zák. je navíc speciální k trestnému činu výroby a jiného nakládání s dětskou pornografií podle § 192 odst. 2 tr.zák., lze si (nejen teoreticky) představit případ takového jednání pachatele internetové kriminality, které by naplňovalo skutkovou podstatu všech uvedených trestných činů. Bylo by tomu tak, pokud by pachatel např. najmul dítě k výrobě pedofilního pornografického filmu, který by následně zpřístupnil na webových stránkách, jenž by byly jinak určeny dětem, přičemž by takový postup zamýšlel od počátku. V takovém případě by naplnil (podle okolností) jak skutkovou podstatu trestného činu podle § 191 odst. 2 písm. b), odst. 3 písm. b) tr.zák., tak i trestných činů podle § 192 odst. 2 al. 2, odst. 3 písm. b) a § 193 odst. 1 tr.zák.

5.6. 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. Na druhou stranu se autor této práce nemůže ztotožnit s absolutní kriminalizací držení pornografických děl, a to i virtuálních, které ve

[239] K tomu viz idem
[240] Jiný a zřejmě nesprávný názor zaujal kolektiv autorů pod vedením prof. Šámala, podle kterého by takový případ mohl být postižen jako souběh s trestným činem šíření pornografie podle § 191 tr. zákoníku. Srov. Šámal, P. a kol., op. cit., s. 1701, marg. č. 24

skutečnosti žádnému dítěti neubližují. Tato přehnaná kriminalizace jde nad rámec nezbytnosti a ve svém důsledku může být i kontraproduktivní.

III 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 možné 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 zabývá. V rámci vyskytujících se kriminálních jednání bylo určeno, na která 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 normy, které slouží k unifikaci postihu nejzávažnějších forem trestné činnosti související s internetem. Analýze (de lege lata) 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. Trestní zákoník de lege lata a de lege ferenda z pohledu internetové kriminality

V českém právním řádu jsou trestné činy kodifikované v jednom zákoníku, kterým je zákon č. 40/2009 Sb., trestní zákoník. Při jeho přípravě byla snaha do něj promítnout závazky vyplývající z mezinárodních smluv a našeho členství v evropských strukturách (např. úprava předávání vlastních občanů na základě eurozatykače, promítnutí v podmínkách ukládání trestu vyhoštění, atd.).

Co se týče internetové kriminality, byla do trestního zákoníku včleněna některá ustanovení, která měla reagovat na rozvoj kybernetické kriminality. Zákonodárce v případě některých jednání 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. phishingu, úvěrových, pojistných aj. podvodů 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 zákona č. 557/1991 zavedla trestný čin poškození a zneužití záznamu na nosiči informací dle § 257a trestního zákona z roku 1961. Úprava tohoto trestného činu se však v průběhu doby (a s bouřlivým rozvojem internetu) ukázala nedostatečnou a musela být několikrát novelizována.[241]

[241] K nedostatkům původní úpravy v trestním zákoně a jejím vývoji srov. blíže v Krupička, J.: Trestně právní regulace ochrany počítačových dat v novém trestním zákoníku a její srovnání s právní úpravou vybraných evropských zemí in: Šturma, P. (ed): I. Celostátní studentská vědecká konference SVOČ v oboru právo a právní věda. Sborník č. 49. Univerzita Karlova v Praze, Právnická fakulta, Praha 2011, s. 26 a násl.

Nový trestní zákoník měl v oblasti ochrany počítačových dat odstranit některé nedostatky původní úpravy a harmonizovat vnitrostátní trestní právo s mezinárodní Úmluvou o počítačové (správněji však kyber) kriminalitě (Budapešť, 2001), kterou Česká republika podepsala dne 9.2.2005[242], avšak doposud neratifikovala. Ačkoliv Česká republika není touto úmluvou vázána, zákonodárce již v důvodové zprávě k novému trestnímu zákoníku vyjadřuje vůli zavést trestněprávní úpravu kyberkriminality, která by s předmětnou úmluvou byla v souladu, a splnit tak případné budoucí závazky napřed.[243]

Úprava postihu hackingu tedy vznikla spojením původní úpravy v trestním zákoně z roku 1961 a provedením čl. 2, 4 a 5 Úmluvy o kyberkriminalitě upravující některé trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů spolu s čl. 7 Úmluvy upravujícího falšování údajů souvisejících s počítači. Výsledek je již na první pohled odstrašující! I při letmém srovnání Úmluvy a nového trestního zákoníku je patrné, že zákonodárce, aby náhodou neopomněl cokoliv z toho, co upravuje Úmluva, pouze přeložil výše uvedené články Úmluvy, smíchal je dohromady a vsadil do textu původní úpravy. Ve výsledku tak nejenže skutková podstata § 230 odst. 2 tr.zák. vyhlíží poněkud kasuisticky, ale i způsobuje nejistotu adresátů této normy ohledně toho, které konkrétní ustanovení bude aplikováno na jejich posuzované jednání. Na jedné straně se potenciální čtenář tohoto ustanovení dozví, že to není pouze pozměnění dat, které by bylo trestné, ale také jejich *poškození, potlačení, snížení jejich kvality nebo jejich učinění neupotřebitelnými*, které nejsou ničím jiným než synonyma či specifické formy jinak obecného slova „změna“.

Některá postihovaná jednání podle odst. 2 jsou zbytečně zdvojena. Písm. b) tohoto odstavce by mnohem lépe znělo, pokud by jej místo uvedeného lingvistického cvičení zákonodárce formuloval např. takto:

„b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně poškodí, změní, vymaže nebo jinak zničí.“

Význam vynechaných sloves je totiž shodný s těmi, které v ustanovení byly zachovány. Ze stejného důvodu se pak jeví zařazení celého písm. c) v odst. 2 jako zcela nadbytečné a přehlednosti (i pochopitelnosti) daného ustanovení nikterak nepřispívá, neboť upravuje buď

---

[242] Rada Evropy, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=13/04/2011&CL=ENG; zobrazeno: 3.4.2011 v 19:15 hod.

[243] Důvodová zpráva k § 228 – 230 (dnes 230 – 232) vládního návrhu trestního zákoníku, Poslanecká sněmovna Parlamentu České republiky, 5. volební období, 2006-2010, sněmovní tisk č. 410/0

určitou formu pozměnění dat, nebo jejich vložení, které je obsahem dalšího písm. d) předmětného ustanovení.

Zcela jiná by jistě byla situace, kdyby zákonodárce zařadil jednání popsané v písm. c) citovaného ustanovení do samostatné kvalifikované skutkové podstaty, aby tak mohl přísněji postihnout případy počítačového padělání, na které lze nahlížet, díky jeho určité rafinovanosti, jako na společensky závažnější jednání, než například „obyčejné“ poškození nebo změna počítačových dat. Jelikož tak však zákonodárce neučinil, pozbývá toto ustanovení smysl.

Pro praxi problematickým se jeví i ustanovení odstavce třetího § 230 tr.zák. To jako okolnost podmiňující použití vyšší trestní sazby uvádí, že pachatel spáchá čin v odstavci prvém nebo druhém s úmyslem způsobit jinému škodu (jinou újmu) nebo sobě či jinému získat neoprávněný prospěch. Úskalí spočívá v tom, že si lze obtížně představit případ, aniž by tato okolnost nebyla naplněna, obzvláště když podle českého trestního práva škoda, jiná újma či prospěch nemusí být pouze majetkového charakteru, ale také imateriálního. Bylo by proto vhodnější, aby zákonodárce podmínil naplnění této kvalifikované skutkové podstaty minimální hranicí majetkové škody nebo prospěchu, jako je tomu i v případě krádeže nebo podvodu.

I když, jak bylo řečeno ve druhé části této práce, upravují ostatní odstavce § 230 tr.zák. obvyklé zvláště přitěžující okolnosti, i zde naneštěstí nalezneme určité nepochopitelnosti. Pokud totiž porovnáme trestní sazby těchto kvalifikovaných skutkových podstat s jejich protějšky u jiných majetkových trestných činů, např. krádeže nebo podvodu (u značné škody je to 2 až 8 let), zjistíme, že v případě způsobení shodné výše škody v rámci neoprávněného přístupu k počítačovému systému a nosiči informací hrozí pachateli nesrovnatelně nižší trest (u značné škody od 1 roku do 5 let)!

Celý § 230 tr.zák. je typickou manifestací hypertrofie práva dnešní doby. Vše musí být nyní výslovně upraveno, a proto už dávno není v českých zákonech žádný prostor pro generalizaci a krátká a zřejmá ustanovení. Tento paragraf je 7. nejdelším ustanovením zvláštní části trestního zákoníku a pro případné adresáty této normy je obtížné jej dočíst alespoň do třetího odstavce, o jeho srozumitelnosti nemluvě. Legislativní technika spočívající v naroubování ustanovení mezinárodní úmluvy, které jsou normami spíše teleologického charakteru, na původní ustanovení vnitrostátní normy, je veskrze špatná a měla by být opuštěna. Naneštěstí však lze podobný postup českých legislativních orgánů očekávat i nadále.

Na druhou stranu lze spíše kladně hodnotit rozšíření trestní represe i na ta jednání, která mají charakter pouze přípravného jednání k samotnému hackerství (získání přístupu překonáním bezpečnostních opatření či opatření a přechovávání softwarových a hardwarových prostředků k hackingu) a která před přijetím trestního zákoníku nemohla být z důvodu nízké trestní sazby postižena jako příprava k trestnému činu.

Lze proto uzavřít, že ačkoliv se nová úprava ochrany počítačových dat v novém trestním zákoníku nedá označit za bezchybnou, je třeba říci, že je i přes své nesporné nedostatky krokem vpřed ve srovnání s poněkud nedostačující úpravou v původním trestním zákoně z roku 1961, při nejmenším alespoň splňuje požadavky Úmluvy o počítačové kriminalitě. Na druhou stranu je však patrné, že tato úprava nebyla připravena citlivě a může způsobovat zmatení o tom, jaké byly původní záměry normotvůrce. Některé tyto nedostatky mohou být vyřešeny pomocí vhodných interpretačních metod, jak bylo nastíněno v části druhé této práce. Některé si však nesporně zasluhují nápravu v podobě změny předmětných zákonných ustanovení, a to zejména vedoucí k jejich zeštíhlení a zjednodušení. Inspiraci v tomto směru může poskytnou zahraniční srovnání s některými evropskými zeměmi, které také provedly závazky z Úmluvy.[244]

2.1.2. Postih porušování autorských práv – staronová úprava?

Jak je zevrubně vysvětleno v hlavě 1. zvláštní části této práce, 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 scripta*. Naplnění formálních znaků skutkové podstaty trestného činu dle § 270 tr.zák. bude tak splněno i u sebebanálnějších jednání (jejichž zásah do autorských práv nebude shledán jako „nikoliv nepatrný“) a jediným korektivem trestní odpovědnosti tu bude 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. Pokud tedy pachatel bude porušovat autorská práva zveřejňováním (sdílením, poskytováním…) na internetu, bude k přísnějšímu trestnímu postihu třeba shledat spáchání tohoto trestného činu v poměrně vágní okolnosti „dopuštění se takového činu ve značném (popř. velkém) rozsahu.[245]

---

[244] K tomu blíže v části čtvrté této práce.
[245] Srov. § 270 odst. 2 písm. c) a odst. 3 písm. b) tr.zák.

Dle důvodové zprávy k novému trestnímu zákoníku je úprava TČ porušování autorského práva, práv souvisejících s právem autorským a práv k databázi dle § 270 tr.zák. prakticky totožná s původním zněním trestního zákona z roku 1961. I když do textu základní skutkové podstaty § 270 tr.zák. bylo přidáno (s ohledem na pouze formální pojetí trestného činu) sousloví „nikoliv nepatrně“, úprava tohoto trestného činu není ve výsledku úplně podobná. Důvod tohoto rozdílu je však nutné hledat systematicky na úplně jiném místě tr.zák., a to v ustanovení o právním omylu (§ 19 tr.zák.). 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 § 270 tr.zák. je. Tímto, dle mého názoru zcela nevhodným ustanovením, je prolomena zásada *ignorantia legis non excusat*[246] 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. Proto by měl do budoucna zákonodárce provést zevrubnou analýzu úpravy autorského práva a práv souvisejících ohledně těch práv, která si zasluhují zvýšenou ochranu trestním právem oproti těm, u nichž bude postačovat odpovědnost občanskoprávní, a tyto následně včlenit do skutkových podstat jednotlivých trestných činů. Tak by mohlo být například překonávání účinných prostředků ochrany autorských práv zahrnuto do trestných činů postihujících hacking a jiná práva zasluhující trestní ochranu by byla výslovně upravena v trestných činech proti autorskému právu.

Vzhledem k tomu, že autorská práva mají ryze soukromoprávní povahu a (odhlédneme-li od jejich osobnostní složky) jsou v podstatě majetková, vystihovalo by lépe chráněnému objektu těchto trestných činů, pokud by byly zařazeny do hlavy V. upravující majetkové trestné činy. Hospodářský charakter těchto práv je totiž velice diskutabilní, a proto zařazení trestného činu postihujícího porušení autorských práv do hlavy zvláštní části trestního zákoníku upravující hospodářské trestné činy nevystihuje dostatečně dobře jejich podstatu.

[246] Neznalost zákona neomlouvá

2.1.3. Vybrané problémové otázky právní úpravy trestního postihu phishingu

2.1.3.1. Phishing a trestnost podle § 230 a 231 tr.zák.

Jak již bylo uvedeno výše, měl nový trestní zákoník provést příslušná ustanovení Úmluvy. Mezi nimi je i podvod související s počítači upravený v čl. 8 Úmluvy. Zákonodárce se o to ostatně i snažil, a to v ustanovení § 230 odst. 2 písm. c), odst. 3 písm. a) tr.zák.[247] Z toho důvodu se nabízí otázka, zdali samotné phishingové jednání nenaplňuje i skutkovou podstatu TČ neoprávněného přístupu k počítačovému systému a nosiči informací. Dle názoru autora této práce však phishingové jednání v jeho čisté formě, tzn. nezahrnující hackingové aktivity, nemůže být podle tohoto trestného činu postiženo.

V praxi se lze setkat s názorem, že při phishingu pachatel „prostřednictvím e-mailu, zaslaného na e-mailovou adresu poškozeného nechá podvrhnout falešný internetový formulář, vložený na originální stránky banky“. Z toho důvodu je pak jednání pachatele phishingu posuzováno jako útok hackera.[248] Tato kvalifikace je však zcela nesprávná a vychází z určitého nepochopení modu operandi phishingu. Je totiž v praxi velice obtížné, aby pachatelé cokoliv „podvrhovali“, natož falešný internetový formulář k vyplnění přístupových údajů k elektronickému bankovnictví, na *originální* stránky jakéhokoliv bankovního ústavu. Ty totiž bývají velmi důkladně zabezpečené, uložené na obtížně přístupných serverech chráněných víceprvkovou ochranou, a proto by jejich narušení v takové míře bylo obtížné i pro velmi schopného hackera. Pachatelé phishingu proto na originální stránky banky nic nevkládají, místo toho (jak bylo rozvedeno výše) vytvoří webové stránky shodně vypadající s rozhraním využívaným poškozenou bankou a následně zašlou oběti e-mailovou zprávu, která ji má přesvědčit, aby přístupové údaje na těchto stránkách, kam ji nasměruje odkaz v e-mailové zprávě, zadala. Oběť tak pachatelům své přístupové údaje vlastně „dobrovolně“ předá v domnění, že je poskytuje svému bankovnímu ústavu.

Pachatele phishingu proto nezískávají přístup k počítačovému systému a takových informací neoprávněně neužívají v úmyslu získat sobě neoprávněný prospěch ve smyslu ustanovení § 230 odst. 2 písm. a), odst. 3 písm. a) tr.zák. upravující skutkovou podstatu neoprávněného přístupu k počítačovému systému a nosiči informací, nýbrž sice neoprávněně užívají určité informace (identifikační údaje k elektronickému bankovnictví), ale tyto informace obdrží na vlastní webový server od oběti, nikoliv že by museli získávat přístup k těmto informacím ať už

---

[247] Blíže k tomuto ustanovení a vztahu k trestnému činu podvodu viz hlavu 2, kapitolu 2.6.1.5. zvláštní části této práce

[248] K tomuto závěru dospěl např. Vrchní soud v Praze v rozsudku ze dne 20.8.2008, sp.zn. 9 To 56/2008 i Městský soud v Praze v předcházejícím rozsudku ze dne 7.2.2008, sp.zn. 57T 12/2007

u banky či přímo u oběti. Naplnění skutkové podstaty uvedeného trestného činu tak připadá v úvahu pouze u poměrně malého množství phishingových případů. Bude tomu tak zejména v situacích, kdy budou k získání informací použity hackingové metody, jako např. když e-mailová zpráva určená oběti bude obsahovat určitý škodlivý kód, typicky tzv. keylogger., pomocí něhož bude možné „odposlechnout" potřebné údaje. V případech, kdy ale pachatelé zvolí klasickou metodu phishingu, nebude toto jednání možné pod tuto skutkovou podstatu podřadit.

Z podobných důvodů nebude naplněna ani základní skutková podstata TČ podle § 230 odst. 1 tr.zák., neboť ta vyžaduje překonání bezpečnostního opatření, a tím neoprávněného získání přístupu k počítačovému systému nebo k jeho části, což se však v případě phishingu neděje, když pachatel získá přístupové údaje k elektronickému bankovnictví přímo od oběti, a nemusí tak překonávat žádné bezpečnostní opatření.

Phishing však nebude možné trestat ani podle nově zavedeného trestného činu opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat podle § 231 tr. zákoníku. Ten sice postihuje již samotné opatření, přechovávání a další způsoby zpřístupnění přístupových dat, kódů, hesel apod., ovšem pouze v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv nebo právě trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací, což opět není případ klasického phishingu.

2.1.3.2. Phishing a postih jako neoprávněné opatření platebního prostředku

Trestní zákoník nově rozlišuje ochranu proti padělání a pozměnění peněz na jedné straně a platebního prostředku na straně druhé. Zároveň byl s účinností k 1.11.2009 přijat nový zákon č. 284/2009 Sb., o platebním styku, který přináší definici platebního prostředku. Ten je v § 2 odst. 1 písm. d) vymezen jako „*zařízení nebo soubor postupů dohodnutých mezi poskytovatelem a uživatelem, které jsou vztaženy k osobě uživatele a kterými uživatel dává platební příkaz.*"

Jelikož skutková podstata trestného činu neoprávněného opatření, padělání a pozměnění platebního prostředku podle § 234 odst. 1 tr. zákoníku považuje mimo jiné za trestné i opatření a přechovávání platebního prostředku jiného, vyvstává tu otázka, zdali přístupové údaje k elektronickému bankovnictví naplňují výše uvedenou definici platebního prostředku,

pročež by bylo lze stíhat samotné podvodné vylákání těchto údajů jako tento dokonaný trestný čin. Ke kladnému závěru dospívá např. Volovecký.[249]

Autor této práce zastává názor, že nikoliv, a to proto, že shora uvedená definice označuje za platební prostředek až (celý) soubor postupů, které jsou vztaženy k osobě uživatele a kterými uživatel dává platební příkaz, nikoliv samotné přístupové údaje. Ty ostatně od platebního příkazu zřetelně rozlišuje, když v ustanovení § 2 odst. 3 písm. h) zákona o platebním styku dále definuje jedinečný identifikátor jako kombinaci písmen, číslic nebo symbolů, kterými se podle určení poskytovatele identifikuje uživatel nebo jeho účet při provádění platebních transakcí, což není nic jiného, než údaje, které pachatelé phishingem vylákávají.

Pachatelé phishingu tak dokonají trestný čin neoprávněného opatření, padělání a pozměnění platebního prostředku pouze v tom případě, že elektronický příkaz na základě podvodně získaných identifikačních údajů oběti zadají, čímž použijí padělaný platební prostředek jako pravý nebo platný podle § 234 odst. 3 alinea druhá tr. zákoníku, a to v jednočinném souběhu s trestným činem podvodu podle § 209 tr. zákoníku, popř. jeho pokusu. Dokud tak neučiní, bude jejich phishingové jednání možné posoudit pouze jako přípravu k těmto trestným činům, a to pouze pokud budou dány všechny podmínky její trestnosti.

2.1.3.3. Okamžik dokonání trestného činu podvodu v případě phishingového útoku

Jako další sporný moment stávající právní úpravy postihu phishingu lze označit otázku okamžiku dokonání trestného činu podvodu v případě, kdy je na základě phishingem vylákaných přístupových údajů k elektronickému bankovnictví zadán falešný elektronický platební příkaz. Někdy bývá za dokonaný považován jen takový útok, při kterém pachatel dokáže neoprávněně převedené prostředky na základě příkazu k úhradě z účtu vybrat. Dle názoru autora tohoto článku však takový závěr není správný. Trestný čin podvodu podle § 209 odst. 1 tr.zák. je dokonán v tom případě, když pachatel 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. V případě podvodných odčerpání finančních prostředků z bankovních účtů tak k dokonání musí dojít v okamžiku, kdy banka uvedena v omyl ohledně osoby příkazce (jeho identity) platební transakci provede. V ten okamžik totiž oprávněný klient banky ztrácí nad těmito žirálními penězi kontrolu (dispozici), kterou naopak získává příjemce z provedené platební transakce. To platí zejména v těch případech, kdy

[249] Volovecký, P.: Kybernetické hrozby a jejich trestně právní kvalifikace in: časopis Trestní právo č. 1/2011, s. 15

peněžní prostředky jsou připsány na účet bankovního ústavu odlišného od banky domnělého plátce, kde kontrolu nad těmito prostředky banka plátce dokonce zcela ztrácí.

Peníze na účtech představují pohledávku za bankou. Z pohledu trestního práva se na ně vztahují i ustanovení o věcech (§ 134 odst. 1 věta druhá tr.zák.), jejichž hodnota se rovná jejich nominální výši. Pokud jsou tedy v rámci podvodné činnosti převedeny peněžní prostředky na jiný účet (oprávněnou osobu s ním disponující), vzniká tím původnímu majiteli této majetkové hodnoty škoda, a naopak příjemci neoprávněný prospěch. Jejich zpětná výměna v nominální hodnotě je tak z hlediska okamžiku dokonání podvodu irelelevantní, neboť již předtím došlo k převodu majetkové hodnoty (věci) ve stejné nominální výši.

Pokud tedy v případě útoku, který využívá přístupových údajů k elektronickému bankovnictví získaných phishingem, dojde na základě elektronického příkazu k úhradě k bezhotovostnímu převodu finančních prostředků a tyto budou připsány na účet zřízený pachateli u jiné banky, bude okamžikem připsání těchto prostředků trestný čin podvodu dokonán.

2.1.4. Úprava šíření pornografie a postihu dětské pornografie

Úprava trestného činu šíření pornografie zaznamenala v poslední době význačné změny. S účinností trestního zákoníku byl zcela vyčleněn postih dětské pornografie do dvou samostatných trestných činů. To mělo za následek poměrně razantní snížení trestních sazeb v případě šíření jiné než dětské pornografie. Tyto změny lze obecně hodnotit velmi kladně. Na druhou stranu se poslední vývoj právní úpravy trestání pornografie nese v duchu významného rozšiřování kriminalizace držení dětské pornografie. Všechny tyto změny však neodstranily některé nejasnosti ohledně rozsahu kriminalizace pornografie, naopak přinesly otázky další. Právě těmi se budou zabývat následující řádky.

2.1.4.1. Postih šíření deviantní pornografie prostřednictvím e-mailu

Ačkoliv judikatura k trestným činům podle § 191 a 192 tr. zákoníku není příliš rozsáhlá, již nyní se objevuje vícero rozhodnutí Nejvyššího soudu ČR, které se šířením pornografie zabývají. Až překvapivě se však tato rozhodnutí rozcházejí při řešení otázky, zdali je možné případy, kdy pachatel k šíření pornografie využije e-mail, možné kvalifikovat jako okolnost podmiňující použití vyšší trestní sazby podle odst. 3 písm. b) uvedených ustanovení tr.zák., a

pokud ano, tak zda jako spáchané „veřejně přístupnou počítačovou sítí“ či „jiným obdobně účinným způsobem“.[250]

Z rozhodnutí Nejvyššího soudu lze vysledovat trojí přístup řešení této otázky:

První přístup reprezentovaný rozhodnutími sp.zn. 6 Tdo 1135/2010 a 4 Tz 79/2011 vychází z jednoduchého závěru, že přeposílání e-mailových zpráv s tématikou dětské pornografie do jiných e-mailových schránek dosud neustaveným osobám je uvedení do oběhu dětského pornografického díla prostřednictvím veřejně přístupné počítačové sítě, pročež byla uvedená okolnost podmiňující použití vyšší trestní sazby naplněna.

Druhý přístup zastoupený rozhodnutími sp.zn. 3 Tdo 669/2011 a 3 Tdo 414/2011 zastává názor, že i když je rozesílání pornografických děl e-mailem uvedením do oběhu prostřednictvím veřejně přístupné počítačové sítě, nejedná se vzhledem k důvěrnému charakteru e-mailových zpráv a omezenému okruhu adresátů o uvedení do oběhu způsobem veřejně přístupným, pročež nemůže být naplněn kvalifikační znak „veřejně přístupnou počítačovou sítí“. Pokud by však zprávy byly rozeslány většímu počtu adresátů, naplňovala by tato skutečnost znak „jiným obdobně účinným způsobem“.

Poslední přístup naznačený v rozhodnutích sp.zn. 8 Tdo 1467/2010 a 8 Tdo 407/2011 je doslova šalamounský. K jednoznačnému závěru totiž nedospívá, avšak nabízí eventuální řešení, a to že pokud rozeslání závadných e-mailů s postihovanou deviantní pornografií nenaplňuje znak „veřejně přístupnou počítačovou sítí“ (což však soud v rozhodnutích nikterak nezpochybňuje), je na místě zkoumat, zdali nebyl naplněn znak „jiným obdobně účinným způsobem“.

Podle autora této práce není ani jeden z uvedených názorů zcela bezchybný. K řešení tohoto problému je třeba vyjít jednak z výslovného znění jak ustanovení základní skutkové podstaty, tak i kvalifikované podle odst. 3. Zároveň je třeba znovu definovat pojem „veřejně přístupná počítačová síť“. Rozumí se jí funkční propojení počítačů do sítí s cílem vytvořit informační systém pracující s tzv. dálkovým přístupem, jakým je především internet a jiné podobné informační systémy.[251] Elektronická pošta je jedna ze služeb internetu. Bez internetu by nebylo lze o elektronické poště hovořit (odhlédneme-li od elektronické pošty v rámci

[250] K tomu srov. usnesení Nejvyššího soudu ČR ze dne 4.5.2011, sp.zn. 3 Tdo 414/2011; ze dne 27.4.2011, sp.zn. 8 Tdo 407/2011; ze dne 1.6.2011, sp.zn. 3 Tdo 669/2011; ze dne 13.7.2011, sp.zn. 7 Tdo 687/2011; ze dne 12.1.2012, sp.zn. 8 Tdo 1467/2010; ze dne 29.9.2010, sp.zn. 6 Tdo 1135/2010 či rozsudek Nejvyššího soudu ČR ze dne 27.1.2011, sp.zn. 4 Tz 79/2010

[251] Šámal, P., Púry, F., Rizman, S.: Trestní zákon. Komentář. 4. vydání. Praha: C. H. Beck, 2001, s. 1231, shodně též Šámal, P. a kol., op. cit., s. 1699, marg. č. 18

intranetových sítí).[252] Pokud tedy pachatel využívá k šíření e-mailovou poštu, činí tak veřejně přístupnou počítačovou sítí. K tomuto závěru ostatně dospěl i Nejvyšší soud takřka ve všech vyjmenovaných rozhodnutích.

Autor této práce se však nemůže ztotožnit se závěrem, že vzhledem k tomu, že v případě e-mailu nedochází k šíření závadného obsahu způsobem veřejně přístupným, nemůže být naplněn znak veřejně přístupnou počítačovou sítí. Takovou podmínku totiž zákon vůbec nestanoví. K tomu lze dospět zejména porovnáním se základní skutkovou podstatu (ať už podle § 191 odst. 1 tr. zákoníku či § 192 odst. 2 tr. zákoníku), kde se alternativně postihuje „učinění veřejně přístupným". Stejně tak se však trestá neveřejné „dovezení, vyvezení, provezení, nabídnutí, zprostředkování, uvádění do oběhu, prodání nebo jiné opatření".

Na druhou stranu je však naplnění znaku spáchání trestného činu „veřejně přístupnou počítačovou sítí vázáno na hledisko, zdali je toto dostatečně účinné, a to v poměru se spácháním „tiskem, filmem, rozhlasem, televizí" či jiným podobným případům (srov. slova „nebo jiným obdobně účinným způsobem"). Pro naplnění předmětného znaku tak nebude důležitý pouze technický aspekt, že se tak stalo prostřednictvím internetu (tedy veřejně přístupnou počítačovou sítí), ale i aspekt potenciální účinnosti takového jednání, tj. jak velký dopad může mít.

Z uvedeného tedy zřejmě vyplývá, že je třeba odmítnout závěr o eventuálním posouzení, tj. pokud nebude shledáno naplnění znaku veřejně přístupnou počítačovou sítí, je možné ještě uvažovat o jiném obdobně účinném způsobu (v pořadí třetí uvedený názor), neboť „jiný obdobný způsob" v tomto případě může sloužit pouze jako měřítko naplnění aspektu účinnosti znaku „veřejně přístupnou počítačovou sítí". Zcela shodný argument poslouží i k vyvrácení druhého shora uvedeného závěru o tom, že rozesílání e-mailem může naplnit pouze znak „jiným obdobně účinným způsobem". Ze stejného důvodu je konečně třeba odmítnout i první prezentovaný kategorický závěr, že v případě využití e-mailových zpráv musí být znak „spáchání veřejně přístupnou počítačovou sítí" naplněn vždy, když budou obvyklé případy, že rozeslání e-mailu nebude učiněno podobně účinným způsobem jako v případě filmu, tisku, televize, atd.

[252] Autor zde nadbytečně necituje rozsáhlé definice internetu a elektronické pošty, v tomto smyslu lze plně odkázat jednak na obecnou část této práce, jednak např. na usnesení Nejvyššího soudu sp.zn. 8 Tdo 407/2011, kde jsou tyto pojmy definovány i s odkazem na odbornou literaturu.

2.1.4.2. Trestnost tzv. virtuální dětské pornografie

V literatuře[253] se po zavedení trestnosti držení dětské pornografie objevily polemiky ohledně trestnosti tzv. virtuální (zdánlivé) dětské pornografie, tj. případy, kdy v pornografickém díle není znázorněno dítě skutečné, ale např. počítačem vytvořené (animované) nebo literárně popsané, popř. je v díle zobrazena osoba sice existující, ovšem se vzhledem dítěte, ačkoliv již dosáhla věku 18 let. Názory na její trestnost se v tomto směru dosti lišily, argumentováno bylo jak výkladem historickým, tak i teleologickým.[254] Tento problém měla vyřešit shora uvedená novela trestního zákoníku, která doplnila rozsah pojmu dětské pornografie i na pornografická díla „zobrazující osobu, jež se jeví být dítětem". Důvodová zpráva k této novele k tomuto lakonicky poznamenává, že se jedná „*o transpoziční bod článku 1 písm. b) Rámcového rozhodnutí Rady 2004/68/SVV ze dne 22. prosince 2003 o boji proti pohlavnímu vykořisťování dětí a dětské pornografii, v němž se dětskou pornografií rozumí materiál, který znázorňuje skutečné dítě, ale i materiál obsahující realistické zobrazení neexistujícího dítě.*" Pokud tomu tak je, proč legislativec nezvolil shodný pojem „realistické zobrazení neexistujícího dítěte"? Jediné racionální vysvětlení tak může být, že zákonodárce chtěl prolnout do jednoho pojmu jak případy uměle vygenerovaných dětí, tak případy, kdy v pornografickém díle je zobrazena skutečná dospělá osoba, avšak vykazující znaky dítěte. Výsledný efekt se však jeví být neuspokojivý, dle názoru autora této práce by bylo vhodné využít definici obsahu pojmu dětské pornografie shodně s uvedeným Rámcovým rozhodnutím, které je v tomto směru stručné, jasné a výstižné, namísto takto nejednoznačného vymezení.

Bez ohledu na výše uvedené se autor této práce neztotožňuje se zavedením trestnosti držení, výroby a šíření virtuální dětské pornografie. Jak už bylo zmíněno v hlavě V. zvláštní části této práce, v těchto případech zdánlivé dětské pornografie nedochází při její výrobě k zneužívání dětí. Není tak naplněn hlavní důvod kriminalizace tohoto druhu dětské pornografie. Jelikož pedofilie jako taková nelze ani vyléčit, ani potlačit, je zcela zásadní, aby bylo zamezeno jejím projevům (zejména sadistickým, tzv. nepravým pedofilům[255]) v reálném světě, tedy sexuálnímu zneužívání dětí a dalším sexuálně motivovaným útokům. Některé studie přitom uvádějí, že stíhání produkce animované pornografie nesnižuje prevalenci

[253] Šámal, P. a kol., op. cit., s. 1704, marg. č. 5; dále např. Jelínek J. a kol., op. cit., s. 559; Herczeg, J.: Virtuální dětská pornografie: Zločin bez oběti? In: Vanduchová, V., Gřivna, T. (red.): Pocta Otovi Novotnému k 80. narozeninám. ASPI, Wolters Kluwer, Praha 2008, s. 42

[254] Srov. idem.

[255] Blíže k problematice pedofilního pachatele např. Čírtková, L.: Forenzní psychologie. Plzeň: Nakl. Aleš Čeněk, 2004, s. 185 a násl.

sexuálních deliktů spáchaných na dětech, popř. tvrdí opak.[256] Z tohoto pohledu pak není důvod takovéto jednání trestat. Jako argument pro kriminalizaci nemůže obstát ani odkaz na povinnost provedení uvedeného Rámcového rozhodnutí, neboť to umožňuje ve svém čl. 3 odst. 2 trestní odpovědnost výroby a držení zdánlivé dětské pornografie nezavést. Toto přepínání trestní represe se tak dle názoru autora této práce jeví být spíše krokem politickým k vyhovění populistického požadavku na potírání pedofilie, než reálnou potřebou reagovat na společenskou škodlivost daného jednání a mělo by být revidováno.

2.1.5. Stalking

Oproti původnímu trestnímu zákonu i vládnímu návrhu trestního zákoníku obsahuje současná podoba nového trestního kodexu úpravu tzv. stalkingu (volně přeloženo jako „pronásledování", „lov" či „slídění"), tedy jednání pachatele spočívající ve *„zlovolném, úmyslném, opakovaném a dlouhodobém obtěžování jiné osoby, která toto pociťuje jako příkoří a snižuje jí to vzhledem k intenzitě obtěžování, četnosti, příp. i strachu z vlastní bezpečnosti kvalitu života."*[257] Zařazením tohoto nového trestného činu zákonodárce reagoval na tlak ze strany jak odborníků, obzvláště psychiatrů a kriminologů, tak i ze strany laické veřejnosti, a to zejména s rostoucí prevalencí a častější eskalací tohoto jednání s tragickými následky.[258]

Obtěžující pronásledování není samozřejmě jevem novým, naopak. V minulosti však k jeho postihu často postačovala ustanovení upravující trestné činy výtržnictví nebo omezování osobní svobody. Obrovský rozmach elektronických prostředků komunikace a internetu jako takového však pachatelům stalkingu („stalkerům") přinesl nový nástroj, který posunul tento druh kriminality do zcela jiné dimenze. Nikdy nebylo snazší někoho zkontaktovat, a to i proti jeho vůli, aniž by člověk opustil pohodlí svého domova. Navíc komunikace elektronickými prostředky, na rozdíl od kupříkladu telefonního hovoru, nabízí zcela adresné, okamžité, ovšem nikoliv „bezprostřední" sdělování pocitů, dojmů nebo postojů, ať už pozitivních či negativních. Je proto zřejmé, že se tak do rukou stalkerů dostala zbraň, kterou plně využívají, neboť jim umožňuje se tak vyhnout jednání, které by bylo možné podřadit pod skutkové podstaty TČ výtržnictví, pomluvy či omezování osobní svobody. Výše uvedené je

---

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

[257] Jelínek, J. a kol.: Trestní zákoník a trestní řád s poznámkami a judikaturou. 1. vydání. Leges, Praha 2009, s. 432

[258] http://www.novinky.cz/krimi/139145-stalking-konci-i-vrazdami-v-zakone-presto-neni.html, zobrazeno 11.10.2009, 12:20

v současné době umocňováno rozvojem tzv. sociálních sítí typu Facebook,[259] kde lze získat, pokud není uživatel obzvláště obezřetný, až neuvěřitelně osobní a důvěrné informace, které potenciální stalker jistě rád využije.

Pohnutky stalkerů k jejich jednání jsou různé. Existují i různé typologie pachatelů stalkingu, a to např. z hlediska psychopatologického,[260] rizikovosti pro oběť[261] či kombinace obou uvedených.[262] Konkrétní typologie pachatelů stalkingu však překračuje rámec této kapitoly, a proto v podrobnostech odkazuji na uvedené prameny.

Trestnost stalkingu byla trestním zákoníkem zavedena v ustanovení o TČ nebezpečného pronásledování:

§ 354
Nebezpečné pronásledování

(1) Kdo jiného dlouhodobě pronásleduje tím, že

a) vyhrožuje ublížením na zdraví nebo jinou újmou jemu nebo jeho osobám blízkým,
b) vyhledává jeho osobní blízkost nebo jej sleduje,
c) vytrvale jej prostřednictvím prostředků elektronických komunikací, písemně nebo jinak kontaktuje,
d) omezuje jej v jeho obvyklém způsobu života, nebo
e) zneužije jeho osobních údajů za účelem získání osobního nebo jiného kontaktu,

a toto jednání je způsobilé vzbudit v něm důvodnou obavu o jeho život nebo zdraví nebo o život a zdraví osob jemu blízkých, bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti.

(2) Odnětím svobody na šest měsíců až tři roky bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1

a) vůči dítěti nebo těhotné ženě,
b) se zbraní, nebo
c) nejméně se dvěma osobami.

Ustanovení § 354 odst. 1 písm. d) tr.zák. směřuje i na ochranu před kyberstalkingem, tedy pronásledování pomocí prostředků elektronických komunikací. Ze znění § 354 tr.zák. je však patrné, že zákonodárce zvolil velice úzkou kriminalizaci stalkingu, neboť tato úprava zdaleka nedopadá na každou jeho formu. Nový trestný čin postihuje totiž jen nejzávažnější formy, když podmiňuje trestnost jednání stalkera kumulativně znakem dlouhodobosti a objektivně posuzovanou způsobilostí vzbudit v jiném důvodnou obavu o život nebo zdraví oběti či osob

[259] Více o tomto např. na: http://cs.wikipedia.org/wiki/Facebook
[260] Dresssing, H., Maulk-Backer, H., Gass, P.: Posuzování stalkingu z kriminalistického a psychiatrického hlediska, http://www.ipravnik.cz/cz/clanky/trestni-pravo/art_5000/posuzovani-stalkingu-z-kriminalistickeho-a-psychiatrickeho-hlediska.aspx, zobrazeno 19.9.2009, 8:45
[261] Čírtková, L.: Psychologické poznatky k nebezpečnosti pronásledování (stalking), časopis Kriminalistika, č. 4/2004
[262] Idem

blízkých. Pokud jedna z těchto podmínek splněna nebude, nebude jednání stalkera trestné podle § 354 tr.zák.

Celkově lze k přijaté úpravě postihu stalkingu říci, že je jistě správným krokem reagujícím na aktuální rozmach tohoto jednání ve společnosti, na který je třeba (vzhledem k jeho zřejmé škodlivosti) reagovat i trestněprávní represí. K tomuto kroku se ostatně uchylují i mnohé okolní státy.[263] Zvolená úprava postihu je koncipována spíše úzce, je zaměřena pouze na nejzávažnější případy. Mnohé jiné však postiženy nebudou, ačkoliv je jejich společenská nebezpečnost, resp. škodlivost zjevná. Lze proto předpokládat, že podmínky trestnosti stalkingu budou do budoucna rozšiřovány, např. i na ty případy, kdy sice není jednání pachatele způsobilé vzbudit v oběti důvodnou obavu o život či zdraví jeho nebo osob blízkých, přesto však zjevně způsobuje oběti psychickou újmu.

[263] Jelínek, J. a kol.: Trestní zákoník a trestní řád s poznámkami a judikaturou. 1. vydání. Leges, Praha 2009, s. 432

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 upravujícími 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 47 států, z toho 37 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, ale také potřeba respektování základních lidských práv daných mezinárodními úmluvami (Pakt I a další úmluvy na ochranu základních práv a svobod).

Kapitola I přináší základní legální definice ústředních pojmů jako počítačová data, počítačový systém, poskytovatel služeb a přenosová data.

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 rovněž stanoví povinnost pro státy zavést ohledně uvedených jednání 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 a sběr přenosových dat.

Třetí sekce Úmluvy (čl. 22) je nazvána „Působnost“ („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.[264,265]

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. bezpečných přístavů, kde je páchána internetová kriminalita ve velkém) a dále zamezuje, díky úpravě užší spolupráce mezi státy, případům, kdy určité zjevně trestné

[264] K výkladu jednotlivých ustanovení Úmluvy viz Gřivna, T.: K ustanovením Úmluvy o počítačové kriminalitě in: Gřivna, T., Polčák, R. (eds.): Kyberkriminalita a právo. 1. vydání. Auditorium, Praha 2008, s. 103 a násl.
[265] Pracovní překlad Úmluvy lze nalézt např. v Gřivna, T., Polčák, R. (eds.): op.cit., s. 162 a násl.

jednání není sankcionováno proto, že se o něm ze zahraničí orgány činné v trestním řízení nedozví, nebo je jim dokonce identita pachatele tajena.

IV Srovnání ochrany počítačových dat se zahraničními právními úpravami

1. Úvod a metodika srovnání

Jak již bylo řečeno v předchozích částech této práce, obsahuje trestní zákoník zcela novou úpravu ochrany počítačových dat. Ta vychází zejména z Úmluvy o počítačové kriminalitě, kterou podepsala již většina evropských zemí. Ne všechny, včetně České republiky, ji však doposavad také ratifikovaly.[266] O to zajímavější je proto srovnání trestněprávních úprav jednotlivých evropských zemí. Většina z nich nějakým způsobem závazky z Úmluvy již provádí a svou úpravu jim přizpůsobila. Jsou zahraniční trestněprávní úpravy ochrany počítačových dat kvalitnější, na stejné úrovni či dokonce horší než nová úprava česká? Odpověď na tuto otázku se pokusí podat v následující části tato práce, a to ohledně úpravy slovenské, německé a švýcarské.

Hodnotící kritéria byla zvolena dvě. První z nich posuzovalo danou úpravu, zdali je v souladu s požadavky a závazky Úmluvy. Toto kritérium není pouze formální. Vychází z předpokladu, že závazky v mezinárodních úmluvách, nadto v oblasti trestního práva, které je jinak považováno za výsostnou oblast vnitrostátního práva, bývají výsledkem těch největších kompromisů. Pokud tedy posuzovaná úprava ani nesplňuje takovýto kompromis, který zaručuje jen tu nejmenší možnou ochranu, lze takovou úpravu hodnotit jako nedostatečnou.

Druhé kritérium spočívá v přehlednosti a pochopitelnosti dané právní úpravy pro adresáty norem. Jak totiž ukazuje případ České republiky, pouhé naplnění požadavků Úmluvy nečiní z předmětných ustanovení trestního zákoníku úpravu kvalitní. Je totiž potřeba, aby právní úprava byla pro průměrného adresáta normy pochopitelná a srozumitelná, v opačném případě nelze danou úpravu považovat za dobrou.

[266] K tomu srov. tabulku podpisů a ratifikací na http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=16/04/2011&CL=ENG, zobrazeno: 10.4.2011 v 13:30

2. Slovenská právní úprava

První zemí, jejíž právní úprava bude srovnávána s úpravou českou, je Slovensko. Od rozdělení federace v roce 1993 se postupem času obě původně shodné trestněprávní úpravy od sebe odlišily. To bylo umocněno zejména přijetím nového slovenského trestného zákona č. 300/2005 Z. z. a dokonáno novým českým trestním zákoníkem. Slovensko na rozdíl od České republiky již Úmluvu o kyberkriminalitě ratifikovalo 8. ledna 2008,[267] čímž se zavázalo ustanovení Úmluvy implementovat. Je proto zajímavé porovnat, zdali tak Slováci učinili lépe než český zákonodárce.

Slovenská právní úprava vychází z původního „československého" trestního zákona z roku 1961, avšak je doplněna o několik ustanovení, která měla zajistit soulad s Úmluvou:[268]

§ 247
Poškodenie a zneužitie záznamu na nosiči informácií

(1) Kto v úmysle spôsobiť inému škodu alebo inú ujmu alebo zadovážiť sebe alebo inému neoprávnený prospech získa neoprávnený prístup do počítačového systému, k inému nosiču informácií alebo jeho časti a

a) jeho informácie neoprávnene použije,
b) také informácie neoprávnene zničí, poškodí, vymaže, pozmení alebo zníži ich kvalitu,
c) urobí zásah do technického alebo programového vybavenia počítača, alebo
d) vkladaním, prenášaním, poškodením, vymazaním, znížením kvality, pozmenením alebo potlačením počítačových dát marí funkčnosť počítačového systému alebo vytvára neautentické dáta s úmyslom, aby sa považovali za autentické alebo aby sa s nimi takto na právne účely nakladalo,

potrestá sa odňatím slobody na šesť mesiacov až tri roky.

(2) Rovnako ako v odseku 1 sa potrestá, kto na účel spáchania činu uvedeného v odseku 1

a) neoprávnene sleduje prostredníctvom technických prostriedkov neverejný prenos počítačových dát do počítačového systému, z neho alebo v rámci počítačového systému, alebo
b) zaobstará alebo sprístupní počítačový program a iné zariadenia alebo počítačové heslo, prístupový kód alebo podobné údaje umožňujúce prístup do celého počítačového systému alebo do jeho časti.

Již na první pohled je slovenská právní úprava méně složitá a lépe čitelná. Ustanovení § 247 slovenského trestného zákona rovněž obsahuje 2 základní skutkové podstaty. Ta první v odstavci 1 je jen mírně pozměněnou původní úpravou, která dříve postihovala počítačové trestné činy. Velice se podobá trestnému činu zavedenému do českého právního řádu v roce

[267] Idem.
[268] Uváděny jsou pouze základní skutkové podstaty

1991, a proto trpí podobnými nedostatky jako česká úprava před svou novelizaci v roce 2002. Slovenský trestný zákon totiž váže trestnost získání neoprávněného přístupu na škodný úmysl, resp. získání neoprávněného prospěchu. Tato skutková podstata tak nemůže být využita k postihu pachatelů, kteří samotný přístup k počítačovému systému nebo nosiči dat získají ještě bez úmyslu způsobit jinému škodu nebo jinou újmu nebo získat neoprávněný prospěch pro sebe nebo jiného, jako například zaměstnanci v jejich práci, ale jinak naplní všechny formální znaky tohoto trestného činu specifikované v písm. a), b), c) nebo d)! Pokud nahlédneme do textu Úmluvy, není v ní možné nalézt jakékoliv ustanovení, podle kterého mohou státy – smluvní strany – požadovat (učinit výhradu), aby trestný čin např. „zásahu do dat“ dle čl. 4 Úmluvy musel být spáchán pouze po získání přístupu do počítačového systému s úmyslem způsobit škodu nebo získat prospěch. Z uvedeného je tedy zřejmé, že ačkoliv Slovensko ratifikovalo Úmluvu, a je tak zavázáno k jejímu provedení, svou právní úpravu v trestném zákoně nemodifikovalo dostatečně, aby s ní byla v souladu.

Druhá základní skutková podstata obsažená v odstavci 2 je provedením čl. 3 a 6 Úmluvy a vztahuje se na určitá přípravná jednání spojená s hackingem jako neoprávněné monitorování přenosu dat (v českém trestním zákoníku je odpovídající ustanovení § 182 odst. 1 písm. c) tr.zák.) nebo výroba a distribuce programů nebo zařízení, hesel atd. usnadňujících získání přístupu a kontroly nad počítačem někoho jiného (podobně jako v § 231 českého tr.zák.).

Obě základní skutkové podstaty jsou postihovány lehce přísněji s trestní sazbou od 6 měsíců do 3 let ve srovnání s maximem dvou let trestu odnětí svobody podle české úpravy.

Odstavce 3 a 4 předmětného ustanovení slovenského trestného zákona následně upravují obvyklé okolnosti podmiňující použití vyšší trestní sazby. Trestní sazba je tu zcela shodná jako u českého trestního zákoníku a je rovněž nižší ve srovnání s trestnými činy podvodu nebo krádeže.

Z výše uvedeného je zřejmé, že i když je slovenská právní úprava méně komplikovaná a lépe čitelná než český protějšek, vzhledem k nedostatkům způsobujícím zejména nesoulad s Úmluvou o kyberkriminalitě nemůže být tato úprava považována za vydařenější a lepší příklad k následování či změnám do budoucna.

3. Švýcarská právní úprava

Další srovnávanou právní úpravou je regulace švýcarská. Švýcarská konfederace byla do 31.12.2011 vůči Úmluvě o kyberkriminalitě v podobném vztahu jako Česká republika. Švýcarsko bylo jednou z prvních zemí, která Úmluvu podepsala, ale po dlouhou dobu ji neratifikovalo. To se ovšem změnilo 21.9.2011, kdy s účinností od 1.1.2012 Švýcarská konfederace Úmluvu ratifikovala. Samotná právní úprava ochrany počítačových dat se od českého nebo slovenského přístupu do značné míry odlišuje. Švýcarský zákonodárce totiž nezavádí do trestního zákoníku jeden koncentrovaný trestný čin implementující články 2 až 8 Úmluvy, které obsahují ochranu počítačových dat a systémů, ale místo toho rozptýlil předmětné trestné činy do vícera ustanovení, podobně jako je rozčleněna i samotná Úmluva. Ve švýcarském trestním zákoníku tak například nalezneme samostatný paragraf pro počítačový podvod systematicky zařazený hned za podvod obecný (podobně jako je v české úpravě zvláštní podvod pojistný, úvěrový a dotační), za který hrozí stejná sazba trestu odnětí svobody. Již na první pohled je předmětná právní úprava lépe uspořádaná, přehledná a snazší k pochopení.

Do švýcarského trestního zákoníku bylo celkově zavedeno 5 samostatných trestných činů poskytujících ochranu počítačových dat a systémů: Neoprávněný přístup k počítačovému systému (čl. 143bis StGB[269]), odcizení dat (čl. 143 StGB), poškození dat (čl. 144bis StGB), počítačový podvod (čl. 147 StGB) a výroba a distribuce zařízení sloužící k neoprávněnému dešifrování zakódovaných služeb (čl. 150bis StGB):[270]

Čl. 143bis

Neoprávněný přístup k počítačovému systému

(1) Kdo získá prostřednictvím zařízení k přenosu dat neoprávněný přístup k počítačovému systému, který byl zvláště chráněn proti jeho přístupu, bude ke stížnosti[271] potrestán odnětím svobody až na tři léta nebo peněžitým trestem.

(2) Kdo nabízí nebo zpřístupňuje přístupová hesla, programy nebo jiná data, o nichž ví nebo musí předpokládat, že jsou určená k spáchání činu podle odstavce 1, bude potrestán odnětím svobody až na tři léta nebo peněžitým trestem.

---

[269] Schweizerisches Strafgesetzbuch – švýcarský trestní zákoník

[270] Český překlad konkrétních ustanovení a názvů trestných činů je neoficiální a byl proveden autorem práce z úředního francouzského a anglického znění

[271] Švýcarské trestní právo má na rozdíl od českého práva širší uplatnění zásady oportunity, resp. zvláštního institutu trestnosti na návrh (ke stížnosti) poškozeného

Čl. 143

Odcizení dat

(1) Kdo v úmyslu sobě nebo jinému opatřit neoprávněný prospěch získá pro sebe nebo jiného data uložená nebo přenášená elektronicky nebo jiným podobným způsobem, a která nebyla určena pro něj a byly zvláště chráněna proti jeho přístupu, bude potrestán odnětím svobody až na 5 let nebo peněžitým trestem.

(2) Neoprávněné opatření dat ke škodě osoby v příbuzném nebo rodinném poměru může být postiženo pouze ke stížnosti poškozeného.

Čl. 144bis

Poškození dat

(1) Kdo neoprávněně změní, vymaže nebo učiní neupotřebitelnými data uložená nebo přenášená elektronicky nebo jiným podobným způsobem, bude ke stížnosti potrestán odnětím svobody až na tři léta nebo peněžitým trestem.

Odnětím svobody na 1 rok až pět let může být pachatel potrestán, způsobí-li takovým činem značnou škodu.[272] Trestní stíhání bude u takového činu zahájeno z úřední povinnosti.

(2) Kdo vyrobí, doveze, uvede na trh, propaguje, nabízí nebo jinak zpřístupní programy, o kterých věděl nebo musel vědět, že budou užity za účelem spáchání činu uvedeného v odstavci 1, nebo kdo poskytne postup k výrobě takovýchto programů, bude potrestán odnětím svobody až na tři léta nebo peněžitým trestem.

Odnětím svobody na 1 rok až pět let může být pachatel potrestán, spáchal-li čin uvedený v odst. (2) v úmyslu získat neoprávněný majetkový prospěch.

Čl. 147

Počítačový podvod

(1) Kdo v úmyslu získat pro sebe nebo jiného neoprávněný prospěch nesprávným, neúplným nebo nedovoleným užitím dat anebo jiným takovým způsobem ovlivní elektronické nebo podobné zpracování nebo přenos dat, a způsobí tak ke škodě jiného převod finančních aktiv, nebo ihned takovýto převod zakryje, bude potrestán odnětím svobody až na 5 let nebo peněžitým trestem.

(2) Odnětím svobody až na deset let nebo peněžitým trestem ve výši nejméně 90 denních sazeb může být pachatel potrestán, spáchal-li čin uvedený v odst. (1) v úmyslu získat neoprávněný majetkový prospěch.

(3) Počítačový podvod ke škodě osoby v příbuzném nebo rodinném poměru může být postižen pouze ke stížnosti poškozeného.

Čl. 150bis

Výroba a distribuce zařízení sloužící k neoprávněnému dešifrování zakódovaných služeb

---

[272] Za značnou škodu se ve Švýcarsku považuje škoda alespoň 10.000,- ChF, tj. cca 190.000,- Kč (srov. ATF 136 IV 117 consid. 4.3.1, strana 119)

(1) Kdo vyrobí, doveze, vyveze, převeze, uvede na trh nebo instaluje zařízení pro neoprávněné dešifrování zakódovaných televizních a rádiových programů nebo telekomunikačních služeb bude ke stížnosti potrestán peněžitým trestem

(2) Pokus spáchat čin uvedený v odst. 1 nebo účastenství na něm je rovněž trestné.

Švýcarská úprava do 31.12.2011 nebyla v souladu s čl. 6 Úmluvy, neboť v té době neznala ustanovení § 143bis odst. 2 StGB, které od nynějška postihuje neoprávněný prodej, distribuci nebo jiné zpřístupnění počítačového hesla, přístupového kódu nebo jiných podobných dat, pomocí nichž lze získat přístup k části nebo celému počítačovému systému. Úmluva totiž neumožňovala učinit výhradu neuplatňování trestní odpovědnosti za toto jednání (srov. čl. 6 odst. 1 písm. a) bod ii, odst. 3, čl. 42 Úmluvy ve spojení s čl. 143bis odst. 2 StGB). S vložením tohoto ustanovení se však švýcarský trestní zákoník stal plně souladným s požadavky Úmluvy.

V celkovém pohledu švýcarskou regulaci považovat za správnou cestu, jak pozměnit národní právní úpravu, aby byla v souladu s Úmluvou. Jasně totiž určuje, která jednání pachatelů budou postihována podle kterého konkrétního ustanovení. Tyto trestné činy jsou popsány na obecnější úrovni a nepůsobí příliš kasuisticky. Zákonodárce tu roboticky neopakuje každé slovo nebo frázi, které byly užity v Úmluvě či v předchozí právní úpravě, jak činí zákonodárce český. Tak například při formulování čl. 144bis odst. 1 StGB, který se uplatní na poškození dat, se dospělo k závěru, že bude dostatečné omezit se pouze na slovesa „*změní, vymaže nebo učiní neupotřebitelnými“* oproti *„vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými“* v § 230 odst. 2 písm. b) českého tr.zák.

4. Německá právní úprava

Poslední srovnávanou právní úpravou je regulace německá. Spolková republika Německo ratifikovala Úmluvu o kyberkriminalitě 9. března 2009, a proto lze očekávat, že německá právní úprava s ní bude v souladu. Podobně jako v případě švýcarského přístupu německý zákonodárce rovněž nekoncentroval právní úpravu ochrany počítačových dat pouze do jednoho nebo dvou paragrafů. Německou implementaci Úmluvy lze najít v osmi samostatných paragrafech trestního zákoníku. Jak již bylo řečeno výše, tento přístup obvykle vede k systematičtější a lépe pochopitelné úpravě, která nemá za následek ať už hypertrofický vzhled právní normy jako v případě českého trestního zákoníku, nebo překombinovanost předmětného ustanovení, která ve svém důsledku vede, i přes využití celých souvětí a výrazů z Úmluvy, k jeho nesouladu s jejími požadavky na implementaci, jako tomu je v případě slovenského protějšku.

Německý trestní zákoník obsahuje 4 skupiny trestných činů spojených s ochranou dat. První z nich je tvořena trestnými činy vyzvídání dat (§ 202a StGB), zachycení dat (§ 202b StGB) a přípravy k vyzvídání a zachycení dat (§ 202c StGB):[273]

§ 202a
Vyzvídání dat

(1) Kdo překoná bezpečnostní opatření, a tím pro sebe nebo jiného získá neoprávněný přístup k datům, která nebyla určena pro něj a byla zvlášť zabezpečena proti neoprávněnému přístupu, bude potrestán až na tři léta nebo peněžitým trestem.

(2) Za data podle odst. 1 se považují jen taková, která jsou uložena nebo přenášena elektronicky, magneticky, nebo jinak způsobem nikoliv bezprostředně vnímatelným.

§ 202b
Zachycení dat

(1) Kdo neoprávněně zachytí data (§ 202a odst. (2)), která nebyla určena jemu nebo jinému technickými prostředky z neveřejného počítačového systému nebo z elektromagnetického vyzařování počítačového systému, bude potrestán až na dvě léta nebo peněžitým trestem, pokud za tento čin zákon nestanoví přísnější trest podle jiného ustanovení.

§ 202
Příprava k vyzvídání a zachycení dat

[273] Uváděny jsou pouze základní skutkové podstaty, ohledně překladu viz. pozn. č. 250

(1) Kdo připravuje spáchání trestného činu podle § 202a nebo § 202b tím, že vyrobí, pro sebe nebo jiného obstará, prodá, jinému přenechá, distribuuje nebo jinak zpřístupní

1. *hesla nebo jiné bezpečnostní kódy umožňující přístup k datům (§ 202a (2)), nebo*
2. *programy za účelem spáchání takového trestného činu,*

bude potrestán odnětím svobody na 1 rok až 5 let nebo peněžitým trestem.

První skupina trestných činů provádí čl. 2, 3 a 6 Úmluvy o kyberkriminalitě. Jelikož Spolková republika Německo využila práva podat výhradu vůči aplikaci čl. 6 odst. 1 písm. a) bod i a písm. b) Úmluvy, trestní postih přípravných jednání ke spáchání trestných činů vyzvídání dat a zachycení dat podle § 202c StGB byl zaveden pouze ve vztahu k softwarovým nástrojům, a nikoliv už hardwarovým zařízením. Proto lze v této části ochranu dat poskytovanou německým trestním zákoníkem považovat za slabší, než je ochrana daná českým trestním kodexem. K tomu je však třeba poznamenat, že minimálním rozsahem provedení Úmluvy „trpí"i švýcarská úprava.

Druhá skupina počítačových trestných činů je representována pouze počítačovým podvodem podle § 263a, který implementuje čl. 8 písm. b) Úmluvy:[274]

§ 263a

Počítačový podvod

(1) Kdo s úmyslem získat pro sebe nebo jiného neoprávněný prospěch způsobí škodu na majetku jiného tím, že ovlivní výsledek počítačového zpracování dat nesprávným nastavením programu, užitím nesprávných nebo neúplných dat, neoprávněným použitím dat nebo jiným neoprávněným ovlivněním průběhu zpracování, bude potrestán odnětím svobody až na 5 let nebo peněžitým trestem.

(3) Kdo připravuje spáchání trestného činu podle odst. 1 tím, že vytvoří počítačové programy, jejichž účelem je spáchat takový trestný čin, nebo takové programy pro sebe nebo jiného opatří, nabízí je k prodeji, přechovává je nebo je jinému přenechá, bude potrestán odnětím svobody až na 3 roky nebo peněžitým trestem.

Na tomto místě je třeba poznamenat, že na trestný čin podvodu se *mutatis mutandis* užijí příslušná ustanovení obecného podvodu a rovněž s ním odpovídají i trestní sazby, které lze za počítačový podvod uložit.

Třetí skupina trestných činů se týká padělání dat, tedy je provedením čl. 7 Úmluvy. Skládá se z trestného činu padělání technických záznamů (§ 268 StGb) a padělání právně relevantních dat (§ 269 StGB):[275]

§ 268 - Padělání technických záznamů

---

[274] Uváděny jsou pouze základní skutkové podstaty, ohledně překladu viz. pozn. č. 250
[275] Uváděny jsou pouze základní skutkové podstaty, ohledně překladu viz. pozn. č. 250

(1) Kdo v úmyslu klamat v právním styku

1. *vyrobí nepravdivý technický záznam nebo takový technický záznam padělá anebo*
2. *nepravý nebo padělaný technický záznam užije,*

bude potrestán odnětím svobody až na 3 roky nebo peněžitým trestem.

(3) Stejně bude potrestán, kdo ovlivní výsledek záznamu tím, že zasáhne do procesu zaznamenávání.

§ 269

padělání právně relevantních dat

(1) Kdo v úmyslu klamat v právním styku přechovává nebo pozmění data určená jako důkaz tak, že na základě nich bude vytvořen padělaný nebo nepravdivě pozměněný dokument, nebo užije data za tímto účelem přechovávaná nebo pozměněná, bude potrestán odnětím svobody až na 5 let nebo peněžitým trestem.

Poslední skupinu tvoří dva trestné činy spojené se zásahem do dat a počítačových systémů upravené v § 303a a 303b StGB; pozměnění dat a počítačová sabotáž:[276]

§ 303a

Pozměnění dat

(1) Kdo neoprávněně vymaže, potlačí, učiní neupotřebitelnými nebo změní data [§ 202a odst. (2)], bude potrestán odnětím svobody až na 2 léta nebo peněžitým trestem.

§ 303b

Počítačová sabotáž

(1) Kdo učiní zásah do procesu zpracování dat, které jsou pro jiného značného významu tím, že

1. *spáchá trestný čin podle § 303a odst. (1),*
2. *s úmyslem způsobit jinému škodu vloží nebo přenese data (§ 202a odst. (2)),*
3. *zničí, poškodí, učiní neupotřebitelným, odstraní nebo pozmění počítačový systém nebo nosič informací,*

bude potrestán odnětím svobody až na 3 léta nebo peněžitým trestem.

(5) Na přípravu k činu podle odst. 1 se přiměřeně použije § 202c.

Německá právní úprava působí velice inspirativně, neboť je jednak plně v souladu s Úmluvou o kyberkriminalitě a jednak automaticky neopakuje její formulace, neboť ty nejsou vždy pro národní právo vhodné a rovněž takovýto přístup často vede k příliš komplikovaným ustanovením. Je zřejmé, že zákonodárce při vytváření novelizace trestního zákoníku k provedení Úmluvy svou práci neodbyl a předtím, než byla právní úprava novelizována, byla předmětná materie podrobně zanalyzována. To dovolilo zákonodárci implementovat jen

[276] Opět jsou uváděny pouze základní skutkové podstaty, ohledně překladu viz. pozn. č. 250

nezbytné minimum z formulací Úmluvy a umožnilo se vystříhat duplicitám v právní regulaci, tak očividné v českém trestním zákoníku.

Jediným problematickým momentem německé trestněprávní úpravy vychází z nejširšího možného využití výhrad, které Úmluva u některých článků umožňuje. V nejbližší budoucnosti lze očekávat, že trestní postih kyberzločinu bude gradovat. Pokud tedy německý zákonodárce implementoval závazky Úmluvy, která vznikala v prvním desetiletí tohoto století a která představuje do jisté míry kompromis, v nejužším možném rozsahu, bude s největší pravděpodobností nutné tuto trestněprávní ochranu rozšířit a předmětnou úpravu znovu novelizovat.

5. Vyhodnocení právních úprav

Aktuální česká úprava má mnoho nedostatků, zejména jí lze vyčíst nepřehlednost a v jistém smyslu i nepochopitelnost pro adresáty, která je dána postupem zákonodárce při jejím formování a až absurdní snahou zcela převést konkrétní formulace Úmluvy o kyberkriminalitě do vnitrostátního práva, nadto v kombinaci s právní úpravou původní. Na druhou stranu lze vyzdvihnout, že se zákonodárce pokusil vypořádat s některými zásadními nedostatky v původním trestním zákoně z roku 1961. Díky tomu ji lze hodnotit jako lepší než úpravu slovenskou, která sice formálně má být zcela v souladu s předmětnou Úmluvou, avšak fakticky se do slovenského trestného zákona všechny závazky z ní převést nepodařilo.

Na opačném pólu stojí úpravy německé a švýcarské, které na první pohled působí srozumitelněji a systematičtěji. Jejich hlavním negativem je snaha o implementaci co nejmenšího možného rozsahu závazků z Úmluvy, která pravděpodobně vyústí v nutnosti trestněprávní regulaci ochrany dat v brzké budoucnosti rozšířit.

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.

U internetové kriminality snad nejvíce platí, že k jejímu zamezení je daleko důležitější prevence než následná represe. Kromě zmíněného zvýšení informovanosti veřejnosti je rovněž důležité předcházet útokům kyberzločinců technickými prostředky obrany, jako jsou antiviry, firewally a kódovací nástroje. I zde platí známá poučka, že příležitost dělá zloděje. Je proto na místě využívat všech možných prostředků zabezpečení, a to i v jejich kombinaci. Zároveň je důležité mít na paměti, že stejně jako se vyvíjí technické nástroje útoků kyberzločinu, vyvíjí se i prostředky jejich odvrácení. Uživatele internetu se tak nesmí spokojit pouze s tím, že v určité době využili nejširší možnou kombinaci zabezpečení, neboť toto zabezpečení se snadno může stát zastaralé již za několik málo měsíců. I v tomto případě je tak nutné být bdělý a udržovat své bezpečnostní nástroje stále aktuální.

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.

Jak se čím dál více činností přesouvá do kybernetického světa, zvyšuje se i počet jednotlivých typů internetové kriminality, které sice mají často předobraz v reálném světě, v prostředí internetu však nabývají zcela jiných rozměrů. Za vše mluví aktuální problémy kyberšikany, kyberstalkingu či kybersquattingu. Internet je čím dál více vnímán jako prostředí důležité i z hlediska národní bezpečnosti. Již nyní se hovoří o kyberšpionech ve službách světových velmocí. Podobně se stává toto medium nástrojem kyberterorismu. Prozatím marný se ukázal boj orgánů činných v trestním řízení se stále častějšími DoS útoky proti serverům státních orgánů a dokonce proti internetu jako takovému. K tomu přispívá i absence jakéhokoliv globálního strážce internetu, neboť ten nepatří nikomu.

Pokud vezmeme v úvahu trestněprávní aspekty, 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 na poli ochrany před kyberkriminalitou prodělala modernizaci až s velkým zpožděním po zaznamenání jednotlivých typů internetové kriminality ve společnosti, nadto velmi neobratně. Tato skutečnost je patrná i ze srovnání se zahraničními úpravami, ze kterého sice vyplývá, že český trestní zákoník splňuje určitý minimální standard ochrany před internetovou kriminalitou daný Úmluvou o počítačové kriminalitě, avšak oproti např. trestněprávní regulaci švýcarské či německé je naše úprava nepřehledná, do značné míry pro adresáty norem nepochopitelná a zbytečně vyvolávající právní otázky o správném posouzení konkrétních činů.

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. bezpečné přístavy (internetové ráje), tedy země, které jsou (podobně jako v oblasti daní) 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 více jak deseti 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, která tak nemůže těžit zejména z jejích procesních institutů usnadňující odhalování a stíhání kyberkriminality.

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.

Criminal Law and Criminological Aspects of the Internet Criminality

Key words: Internet, Criminal law, Criminology

Abstract (EN):

Internet criminality is a very young phenomenon; the internet itself was presented in the recent form only about 20 years ago. Nevertheless, the relative youth of the internet does not mean that the internet crimes are less serious or less prevalent than other criminal activities. The mass, relative anonymity and progressive globalization of the internet together with bustling development of computer technology provide both the organized crime and individuals with perfect means to commit all sorts of offences.

With regard to its extant, this study is not supposed to serve as an overall and full detailed analysis of the internet criminality. The objective of this paper is a criminological description of socially dangerous phenomenons related to the internet, concretely the origin of these phenomenons in the society, the most frequent *modus operandi* of the internet crime, means of prevention and the criminal law qualification of the relevant criminal activities. The paper itself is divided into four separate parts.

The first part contains a general introduction into the problems of internet criminality. We can find there a definition of the term “internet” and “internet criminality”, its differentiation from the terms “computer criminality” and “cybernetic criminality” and its further classification. Futhermore, it provides basic characteristics of the offenders of internet criminality, reasons for the spread of this type of criminality and general criminal law issues related to the internet criminality.

The second part describes selected types of criminal activities committed directly or at the hand of internet. This part is divided into five titles; each of them contains criminological and consequently criminal law analysis of each type. The emphasis was placed on the most actual problems, i.e. criminal protection of the copyright, “hacking” and internet viruses, so called Nigerian scam letters and “phishing”, illegal internet distribution of pornography (especially the child pornography), and “abuse of the computer time” in context of the internet.

The third part consists of the critical analysis of the actual legislation (*de lege lata*) brought by the new Penal Code, effective from 1st January 2010, and suggests possibilities of future changes of the legislation (*de lege ferenda*) that may help to overcome current difficulties set by the new criminal code.

The last part of this thesis compares different criminal regulations of cybercrime of selected European countries (Slovakia, Switzerland and Germany) with Czech regulation using two points of view. The first one explores the conformity of the concerned regulation with the CoE Convention on Cybercrime as the minimal standard of criminal regulation of cybercrime. The second one analyzes the comprehensibility and certainty of the regulation for the recipients.

Trestněprávní a kriminologické aspekty internetové kriminality

Klíčová slova: Internet, Trestní právo, Kriminologie

Abstrakt (CZ):

Internetová kriminalita je velice mladý fenomén, když internet v současné podobě byl představen teprve před cca 20 lety. To však neznamená, že by internetové trestné činy byly méně závažné nebo méně rozšířené než ostatní kriminální jednání. Masovost, relativní anonymita a narůstající globalizace internetu spolu s překotným rozvojem moderních technologií poskytují jak organizovanému zločinu, tak i jednotlivcům skvělý nástroj k páchání nejrůznějších forem trestné činnosti.

Tato práce nemá sloužit vzhledem ke svému rozsahu k podrobné a všeobjímající analýze internetové kriminality. Cílem této práce je kriminologický rozbor společensky škodlivých jevů souvisejících s internetem, konkrétně původ těchto jevů ve společnosti, nejčastější způsob spáchání internetové kriminality, možnosti prevence a trestněprávní kvalifikace těchto jednání. Práce samotná je rozdělena do čtyř samostatných částí.

První část obsahuje obecný úvod do problematiky internetové kriminality. Můžeme zde najít definici pojmů „internet“, „internetová kriminalita“ a její odlišení od pojmů „počítačová kriminalita“ a „kybernetická kriminalita“, stejně jako její další třídění. Dále tato část nabízí základní charakteristiku pachatelů internetové kriminality, důvody jejího rozmachu a analýzu obecných trestněprávních otázek spojených s touto kriminalitou.

Druhá část popisuje vybrané typy kriminálních jednání spáchaných přímo nebo pomocí internetu. Tato část je rozdělena do pěti hlav; každá z nich obsahuje kriminologický a následně trestněprávní rozbor jednoho typu.

Třetí část práce se skládá z kritické analýzy stávající právní úpravy (*de lege lata*), kterou přinesl nový trestní zákoník účinný od 1. ledna 2010, a zároveň předkládá návrh možností případných budoucích změn právní úpravy (*de lege ferenda*), které by mohly pomoci překonat současné potíže, se kterými se adresáti norem při interpretaci a aplikaci nového trestního zákoníku potýkají.

Poslední část této práce srovnává různé trestněprávní regulace kyberzločinu vybraných evropských zemí (Slovensko, Švýcarsko a Německo) s úpravou českou, a to za využití dvou kritérií. První kriterion spočívá v souladu předmětných právních úprav s Úmluvou o počítačové kriminalitě Rady Evropy, jakožto minimálního standardu trestní úpravy kyberzločinu. Druhé hledisko srovnává srozumitelnost a určitost zkoumaných právních úprav pro adresáty norem.

Seznam literatury a jiných zdrojů informací

A. Seznam literatury

1.) Monografie, učebnice a komentáře:

1. Apollinaire, G.: Les Exploits D'Un Jeune Don Juan. Paříž: 1907
2. Barlow, H., D.: Introduction to Criminology. 7. vydání. HarperCollins College Publishers, Inc., New York, 1996
3. Čermák, J.: Internet a autorské právo. Linde Praha, a.s., Praha 2003
4. Čírtková, L.: Forenzní psychologie. Nakl. Aleš Čeněk, s.r.o., Plzeň 2004
5. Gottschalk, P.: Policing Cyber Crime. 1. vydání. Petter Gottschalk & Ventus Publishing ApS, 2000
6. Halder, D., Jaishankar, K.: Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. IGI Global, Hershey 2011
7. Holcr, K.. a kol.: Kriminológia. 1. vydání. Wolters Kluwer, Bratislava 2008
8. Jelínek, J.: Trestní odpovědnost právnických osob. 1. vydání. Linde Praha, a.s., Praha 2007
9. Jelínek, J. a kol.: Trestní právo hmotné. 2. vydání. Leges, Praha 2010
10. Jelínek, J. a kol.: Trestní právo hmotné. Obecná část. Zvláštní část. 2. aktualizované vydání. Linde Praha, a.s., Praha 2006
11. Jelínek, J. a kol.: Trestní právo hmotné. Obecná část. Zvláštní část. 3. přepracované a aktualizované vydání. Linde Praha, a.s., Praha 2008
12. Jelínek, J. a kol.: Trestní zákoník a trestní řád s poznámkami a judikaturou. 1. vydání. Leges, Praha 2009
13. Jelínek, J., Herczeg, J.: Zákon o trestní odpovědnosti právnických osob a řízení proti nim. Komentář s judikaturou. 1. vydání. Leges, Praha 2012
14. Jirovský, V.: Kybernetická kriminalita. Grada, Praha 2007
15. Knapp, V.: Teorie práva. 1. vydání. C. H. Beck, Praha 1995
16. Kuchta, J., Válková, H. a kol.: Základy kriminologie a trestní politiky. 1. vydání. C. H. Beck, Praha 2005
17. Matějka, M.: Počítačová kriminalita. Computer press, Praha 2002
18. Moore, R.: Cybercrime: Investigating High-Technology Computer Crime. 2. vydání. Elsevier, Oxford 2011
19. Musil, S.: Počítačová kriminalita. IKSP, Praha 2000
20. Novotný, O., Vanduchová, M., Šámal, P. a kol.: Trestní právo hmotné. Obecná část. 6. vydání. Wolters Kluwer ČR, a.s., Praha 2010
21. Novotný, O., Zapletal, J. a kol.: Kriminologie. 2. přepracované vydání. ASPI Publishing, Praha 2007
22. Požár, J. a kol.: Základy teorie informační bezpečnosti. 1. vydání. Policejní akademie České republiky v Praze, Praha 2007
23. Reid, S., T.: Crime and Criminology. Oxford University Press, New York 2009
24. Smejkal, V. a kol.: Právo informačních a telekomunikačních systémů. 2. aktualizované a rozšířené vydání. C.H.Beck, Praha 2004
25. Smejkal, V., Sokol, T., Vlček, M.: Počítačové právo. 1. vydání. C.H.Beck, Praha 1995
26. Šámal, P., Púry, F., Rizman, S.: Trestní zákon. Komentář. 6. vydání. C.H.Beck, Praha 2004
27. Šámal, P. a kol.: Trestní odpovědnost právnických osob. Komentář. 1. vydání. C. H. Beck, Praha 2012

28. Šámal, P. a kol.: Trestní zákoník II. § 140 – 421. Komentář. První vydání. C. H. Beck, Praha 2010
29. Švestka, J., Spáčil, J., Škárová, M., Hulmák, M. a kol.: Občanský zákoník I, II. 2. vydání. C. H. Beck, Praha 2009
30. Telec, I.: Autorský zákon. Komentář. 1. vydání. C. H. Beck, Praha 1997
31. Telec, I., Tůma, P.: Autorský zákon. Komentář. 1. vydání. C. H. Beck, Praha 2007, s. 347
32. Vito, G., F., Maahs, J., R.,Holme, R., M.: Criminology: Theory, Research, And Policy. 2. vydání. Jones and Barlett Publisher, Sudbury 2007
33. Wells, C.: Corporations and criminal responsibility, 2nd edition, Oxford 2001
34. Wiener, N.: Kybernetika a společnost. Academia, Praha 1963

2.) Články v časopisech a sbornících:

1. AN OLD SWINDLE REVIVED; The "Spanish Prisoner" and Buried Treasure Bait Again Being Offered to Unwary Americans", The New York Times, 20 March 1898, s. 12
2. 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
3. Adrian, A.: The Pirate Bay Deep-sixed: Copyright Protected Works and the Territoriality Principle in: Computer Law & Security Report. Vol. 22. Elsevier Science B.V., 2006, s. 392 a násl.
4. autor@chip.cz, Internetové mafii na stopě, časopis CHIP.CZ, č. 1/2008, str. 157 a násl.
5. Balážik, M: Principy ochrany digitální identity. 2. díl: Útoky proti identitě a standardní bezpečnostní opatření in: časopis IT Systems č. 3/2012, s. 54 a násl.
6. Baudiš, P.: Staronové nebezpečí Rhybaření, časopis CHIP.CZ, č. 4/2006, s. 14 a násl.
7. Bottomore, S.: "Eugène Pirou" in: Herbert, S., McKernan, L. eds.: Who's Who of Victorian Cinema, British Film Institute, 1996
8. Čepička, D., Arnold, A., Behrens, D.: Odhalte triky hackerů in: časopis PC WORLD, č. 12/2007, s. 68 a násl.
9. Čírtková, L.: Psychologické poznatky k nebezpečnosti pronásledování (stalking), časopis Kriminalistika, č. 4/2004
10. Dianiška, G. a kol.: Kriminológia. 2. vydání. Aleš Čeněk, Plzeň 2011
11. Dastych, J.: Počítačová kriminalita – stručný přehled v Musil, S.: Počítačová kriminalita. IKSP, Praha 2000, příloha 2
12. Deveci, H., A.: Personal Jurisdiction: Where Cyberspace Meets the Real World – Part 1 in: Computer Law & Security Report. Vol. 21. Elsevier Science B.V., 2005, s. 464 a násl.
13. Diamond, M., Uchiyama, A.: Pornography, Rape and Sex Crimes in Japan, International Journal of Law and Psychiatry. Vol. 22(1)/1999, s. 1 - 22
14. Geers, K.: The Challenge of Cyber Attack Deterrence in: Computer Law & Security Review. Vol. 26. Elsevier Science B.V., 2010, s. 298 a násl.

15. Gřivna, T.: K ustanovením Úmluvy o počítačové kriminalitě in: Gřivna, T., Polčák, R. (eds.): Kyberkriminalita a právo. 1. vydání. Auditorium, Praha 2008, s. 103 a násl.
16. Gutierrez, O., R.: Get Off My URL!; Congress Outlaws Cybersquatting in the Wild West of the Internet in: Santa Clara Computer & High Technology Law Journal. vol. 17. Santa Clara University, Santa Clara 2000
17. Herczeg, J.: Virtuální dětská pornografie: Zločin bez oběti? In: Vanduchová, V., Gřivna, T. (red.): Pocta Otovi Novotnému k 80. narozeninám. ASPI, Wolters Kluwer, Praha 2008, s. 42
18. Hunton, P.: The Growing Phenomenon of Crime and the Internet: A Cybercrime Execution and Analysis Model in: Computer Law & Security Review. Vol. 25. Elsevier Science B.V., 2009, s. 528 a násl.
19. Jaishankar, K.: Cyber Criminology: Evolving a novel discipline with a new journal, International Journal of Cyber Criminology, Vol 1. Issue 1, Editorial, January 2007
20. Janczewski, L., Fu, L., R.: Social Engineering-Based Attacks – Model and New Zealand Perspective in Proceedings of the IMCSIT, č. 5/2010, s. 848
21. Jelínek J.: K pojmu trestného činu v novém trestním zákoníku in: Jelínek, J. (ed): O novém trestním zákoníku. Sborník z mezinárodní konference Olomoucké právnické dny. Leges, Praha 2009, s. 20 a násl.
22. Jirásek, P., Novák, L: Český slovník kybernetické bezpečnosti in: Gogela, R., Jirásek, P., Novák, L., Polčák, R., Požár, J.: Pracovní příručka bezpečnostního manažera. První vydání. Policejní akademie ČR & Česká pobočka AFCEA, Praha 2011
23. Kaoa, D.-Y., Fu-Yuan, Huang, F., F.-Y., Wang, S.-J.: Persistence and Desistance: Examining the Impact of Re-integrative Shaming to Ethics in Taiwan Juvenile Hackers in: Computer Law & Security Review. Vol. 25. Elsevier Science B.V., 2009, s. 464 a násl.
24. Kramer, K., M.: Metro-Goldwyn-Mayer Studios v. Grokster—The Supreme Court's Balancing Act Between the Risks of Third-Party Liability for Copyright Infringement and Rewards of Innovationin in: Santa Clara Computer & High Technology Law Journal. vol. 22. Santa Clara University, Santa Clara 2005, s. 169 a násl.
25. Krog, G., P.: The Norwegian „Napster case" – Do hyperlinks constitute the „Making Available to the Public" as a Main or Accessory Act? In: Computer Law & Security Report. Vol. 22. Elsevier Science B.V., 2006, s. 73 a násl.
26. Krupička, J.: Trestně právní regulace ochrany počítačových dat v novém trestním zákoníku a její srovnání s právní úpravou vybraných evropských zemí in: Šturma, P. (ed): I. Celostátní studentská vědecká konference SVOČ v oboru právo a právní věda. Sborník č. 49. Univerzita Karlova v Praze, Právnická fakulta, Praha 2011, s. 25 a násl.
27. Leng, T., K.: Wireless Internet Access and Potential Liabilities in: Computer Law & Security Report. Vol. 23. Elsevier Science B.V., 2007, s. 550 a násl.
28. Minárik, T.: Peer-to-peer sítě z hlediska trestního práva in: Gřivna, T. (ed.): Český právní řád a ochrana kyberprostoru. 1. vydání. Karolinum, Praha 2008
29. Mowery, D. C., Simce, T.: Is the Internet a US invention? – an economic and technological history of computer networking in: Research Policy. Vol. 31, Elsevier Science B.V., 2002, s. 1361 a násl.
30. Nádeníček, P.: Počítačové viry známé a neznámé. 1. díl Úvod do problematiky & souborové viry, časopis PC WORLD, č. 11/2005
31. Nádeníček,P.: Počítačové viry známé a neznámé. 2. díl E-mailový červ, starý dobrý známý, časopis PC WORLD, č. 1/2006

32. Nádeníček, P.: Počítačové viry známé a neznámé. 3. díl Síťový červ – zatraceně rychlý chlapík, časopis PC WORLD, č. 2/2006
33. Nádeníček, P.: Počítačové viry známé a neznámé. 5. díl Trojský kůň: schopný podvodník schopný všeho, časopis PC WORLD, č. 4/2006
34. Peretti, K. K.: Data Breaches: What the Underground World of “Carding” Reveals in: Santa Clara Computer and High Technology Journal, vol. 2. Santa Clara University, Santa Clara 2008, s. 375 a násl.
35. Přibyl, T.: Causa rootkit, časopis PC WORLD, č. 3/2006, s. 52 a násl.
36. Přibyl, T.: Rootkity in: IT Professional - IT Security, č. 1/2007, s. 12 a násl.
37. Přibyl, T.: Druhý dech trojských koní, časopis PC WORLD, č. 2/2008, str. 110 a násl.
38. Redakce, časopis CHIP.CZ, č. 2/2006, str. 16
39. Růžička, M.: K formálnímu pojetí trestného činu s materiálním korektivem z pohledu státního zástupce in: Trestněprávní revue č. 6/2011, s. 159 a násl.
40. Selvadurai, N., Islam, R., Gillies, P.: Unauthorised Access to Wireless Local Area Networks: The Limitations of the Present Australian Laws, in: Computer Law & Security Review. Vol. 25. Elsevier Science B.V., 2009, s. 536 a násl.
41. Tang, G., H.: Is administrative enforcement the answer? Copyright protection in the digital era in: Computer Law & Security Report. Vol. 26. Elsevier Science B.V., 2006
42. Train, A.: The Spanish Prisoner in: The Cosmopolitan Magazine New York, New York, č. 43, Březen 1910, s. 465 a násl.
43. Volovecký, P.: Kybernetické hrozby a jejich trestně právní kvalifikace in: časopis Trestní právo č. 1/2011, s. 15 a násl.
44. Volevecký, P.: Kybernetická trestná činnost jako předmět vědeckovýzkumné činnosti in: časopis Trestní právo č. 5/2011. Praha 2011, s. 11 a násl.
45. Volevecký, P.: Kybernetické trestné činy v trestním zákoníku: časopis Trestní právo č. 7 – 8/2010, s. 19 a násl.
46. Woo, M., Lui, V.: New copyright Bill for Hong Kong; Hong Kong releases Copyright (Amendment) Bill 2006 in: Computer Law & Security report. Vol. 22. Elsevier Science B.V., 2006
47. Záh, S.: Nesahejte na to! Vše o nebezpečí, které na vás číhá na internetu, časopis PC WORLD, č. 10/2006
48. Završnik, A.: Definiční problémy a kriminologická specifika kyberzločinu in: Gřivna, T., Polčák, R. (eds.): Kyberkriminalita a právo. 1. vydání. Auditorium, Praha 2008
49. 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. Computer viruses hit one million, http://news.bbc.co.uk/2/hi/technology/7340315.stm, zobrazeno 9.8.2009, 11:05
3. Dresssing, H., Maulk-Backer, H., Gass, P.: Posuzování stalkingu z kriminalistického a psychiatrického hlediska, http://www.ipravnik.cz/cz/clanky/trestni-pravo/art_5000/posuzovani-stalkingu-z-kriminalistickeho-a-psychiatrickeho-hlediska.aspx, zobrazeno 19.9.2009, 8:45
4. Finux‘s student hackers guide to WEP hacking,

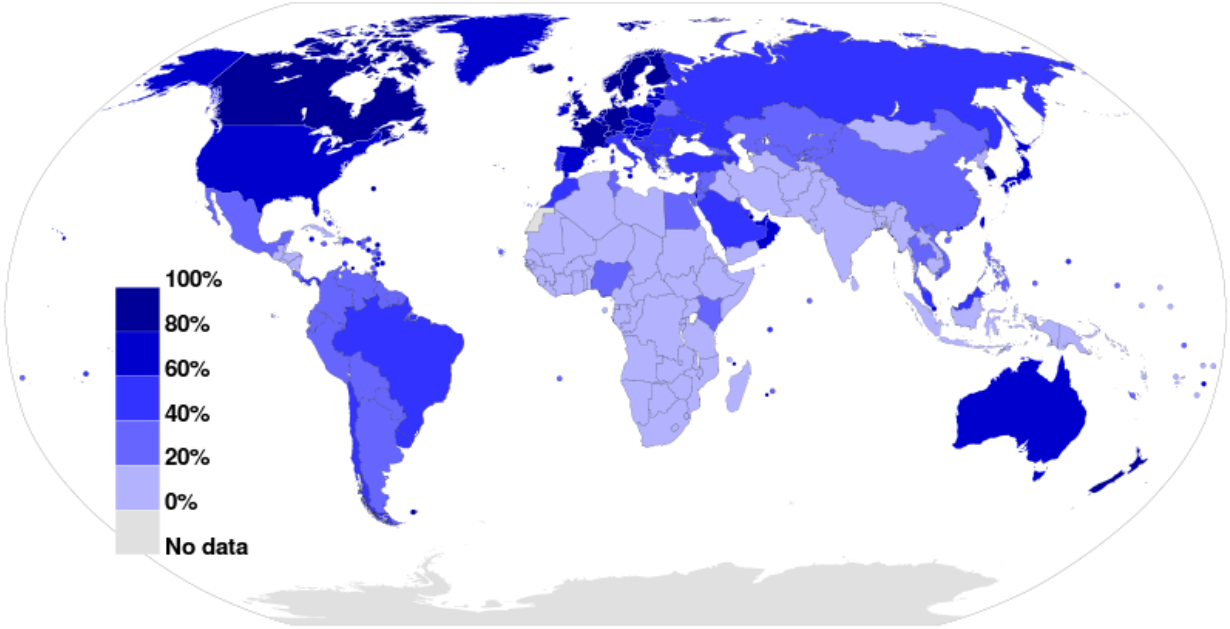
http://www.linuxbasement.com/content/finuxs-student-hackers-guide-wep-hacking, zobrazeno 9.10.2008, 16:35
5. http://blog.jancermak.cz/phishing-ceska-sporitelna-sbirka-nejpopularnejsiho-spam-phishingu-poslednich-dni/2008/03/19/, zobrazeno 17.6.2008, 16:23
6. http://caselaw.lp.findlaw.com/cgi-bin/getcase.pl?court=US&navby=case&vol=000&invol=04-480, zobrazeno 15.8.2012, 16:25
7. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=16/04/2011&CL=ENG
8. http://www.cpufilm.cz/rozsudky.html, zobrazeno 31.7.2008, 16:40
9. http://cs.wikipedia.org/wiki/Facebook, zobrazeno 25.9.2009, 15:19
10. http://www.freevideo.cz, zobrazeno 4.7.2008, 21:43
11. http://www.lawcommunity.de/volltext/130.html, zobrazeno 9.6.2008, 15:17
12. http://www.law.cornell.edu/copyright/cases/464_US_417.htm, zobrazeno 15.8.2012, 17:55
13. http://missingkids.com/missingkids/servlet/NewsEventServlet?LanguageCountry=en_US&PageId=3644, zobrazeno 31.5.2008, 16.20
14. http://www.nature.com/news/2009/090513/full/news.2009.473.html, zobrazeno 10.4.2012, 15:06
15. 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
16. http://www.novinky.cz/clanek/93889-pocitacovi-pirati-uz-obrali-banky-o-stovky-milionu.html, zobrazeno 15.7.2008, 13:05
17. Office of the United States Trade Representative, http://www.ustr.gov/about-us/press-office/reports-and-publications/
18. http://www.parade.com/articles/editions/2006/edition_02-19-2006/Andrew_Vachss, zobrazeno 19.6.2008, 20:15
19. http://www.snopes.com/crime/fraud/nigeria.asp, zobrazeno 21.7.2008, 13:40
20. http://www.social-engineer.org/framework/Computer_Based_Social_Engineering_Tools, zobrazeno 20.1.2012, 18:05
21. https://akela.mendelu.cz/~lidak/bis/seminar2004/seminarky/makovsky.doc., zobrazeno: 15.7.2008, 16:40
22. Matejka J., Čermák J.: Odpovědnost poskytovatelů volného prostoru na Internetu za cizí obsah, www.itpravo.cz, zobrazeno 19.7.2009, 13:25
23. Matejka, J.: Za krádež konektivity do vězení? Už i v ČR, http://www.lupa.cz/clanky/za-kradez-konektivity-do-vezeni-uz-i-v-cr/, zobrazeno 10.5.2011, 10:30
24. Pospíšil Martin: Německo: Místní působnost trestních norem a Internet, http://www.itpravo.cz/index.shtml?x=61318
25. 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
26. Wikipedia; http://en.wikipedia.org
27. World Internet Usage Statistics News and Population Stats, http://www.internetworldstats.com/stats.htm, zobrazeno 20.7.2008, 14:50

C. Judikatura:

1. Nález Ústavního soudu ČR ze dne 10.2.2011, sp.zn. III.ÚS 2523/10, N 16/60 SbNU, s. 171
2. Rozsudek německého Spolkového soudního dvoru ze dne 12.12.2000, sp.zn.: 1 StR 184/00
3. Rozsudek německého Spolkového pracovního soudu ze dne 7.7.2005 sp.zn. 2 AZR 581/04
4. Rozhodnutí United States District Court for the Northern District of California ve věci A&M Records, Inc. et. al. v. Napster, sp.zn. CV 99-5183 MHP, C 00-0074 MHP
5. Rozhodnutí Nejvyššího soudu USA ve věci Metro-Goldwyn-Mayer Studios, Inc., et al. v. Grokster, Ltd., et al. ze dne 27.6.2005, sp.zn. 545 U.S. 913 (2005)
6. Rozhodnutí Nejvyššího soudu USA ve věci Sony Corporation of America et al. v. Universal City Studios, Inc., et al. ze dne 17.1.1984, sp.zn. 464 U.S. 417 (1984)
7. Rozsudek Nejvyššího soudu ČR ze dne 30.9.2004, sp.zn. 4 Tz 124/2004
8. Rozsudek Nejvyššího soudu ČR ze dne 27.1.2011, sp.zn. 4 Tz 79/2010
9. Rozsudek Nejvyššího soudu ČR ze dne 25.3.2008, sp.zn. 33 Odo 79/2006
10. Stanovisko Nejvyššího soudu ČSR ze dne 28.3.1975, sp.zn. Cpj 34/74, publikováno pod č. R 26/1975 civ.
11. Usnesení Městského soudu v Praze ze dne 21.9.2011, sp.zn. 7 To 251/2011 uveřejněné v časopise Trestněprávní revue č. 4/2012, s. 97
12. Usnesení Nejvyššího soudu ČR ze dne 5.5.2004, sp.zn. 7 Tdo 487/2004
13. Usnesení Nejvyššího soudu ČR ze dne 1.3.2005, sp. zn. 5 Tdo 160/2005
14. Usnesení Nejvyššího soudu ČR ze dne 17.10.2006, sp.zn.: 21 Cdo 84/2006
15. Usnesení Nejvyššího soudu ČR ze dne 4.5.2011, sp.zn. 3 Tdo 414/2011
16. Usnesení Nejvyššího soudu ČR ze dne 27.4.2011, sp.zn. 8 Tdo 407/2011
17. Usnesení Nejvyššího soudu ČR ze dne 1.6.2011, sp.zn. 3 Tdo 669/2011
18. Usnesení Nejvyššího soudu ČR ze dne 13.7.2011, sp.zn. 7 Tdo 687/2011
19. Usnesení Nejvyššího soudu ČR ze dne 12.1.2012, sp.zn. 8 Tdo 1467/2010
20. Usnesení Nejvyššího soudu ČR ze dne 29.9.2010, sp.zn. 6 Tdo 1135/2010
21. Usnesení Nejvyššího soudu ČR ze dne 19.1.2011, sp.zn. 5 Tdo 17/2011
22. Usnesení Nejvyššího soudu ČR ze dne 16.2.2011, sp.zn. 8 Tdo 112/2011
23. Usnesení Ústavního soudu ČR ze dne 19.04.2004, sp.zn.: IV.ÚS 606/03, U 23/33 SbNU 453

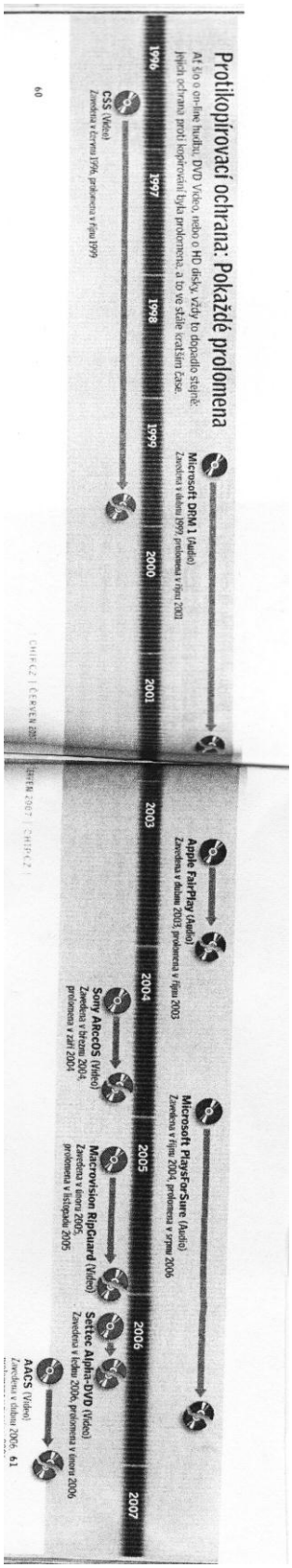
Přílohy

Příloha č. 1 – Mapa světa se zobrazením procentní míry uživatelů internetu v populaci jednotlivých států



Zdroj: http://en.wikipedia.org/wiki/File:InternetPenetrationWorldMap.svg, zobrazeno 16.6.2012, 13:35

Příloha č. 2 – Prolamování softwarových účinných prostředků ochrany autorských práv v časové ose



Zdroj: časopis CHIP.CZ, č. 6/2007, str. 60 a násl.

Příloha č. 3 – Rozsudek Okresního soudu ve Znojmě ("obalycd.cz") ze dne 24.7.2002 ve věci trestného činu podle § 152 odst. 1 tr. Zákona (dnes § 270 tr.zák.)

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. 0 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, byt' 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. 4 – Oznámení Úřadu obchodního zmocněnce USA 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

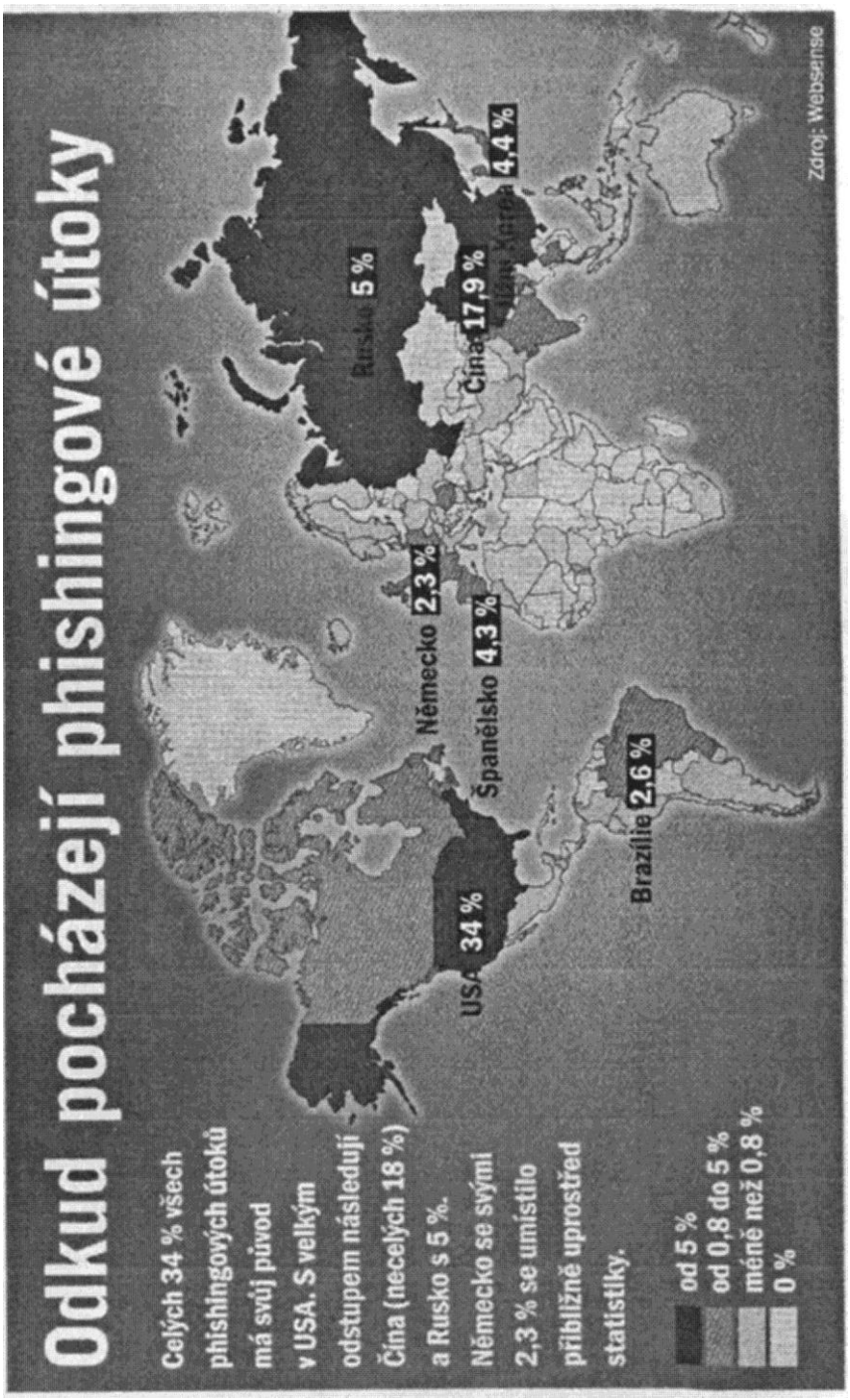
Washington, D.C. - U.S. Trade Representative Susan C. Schwab today announced the results of USTR's Out-of-Cycle Review of intellectual property rights (IPR) protection and enforcement in the Czech Republic under the “Special 301” provisions of U.S. trade law. As a result of the review, the Czech Republic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

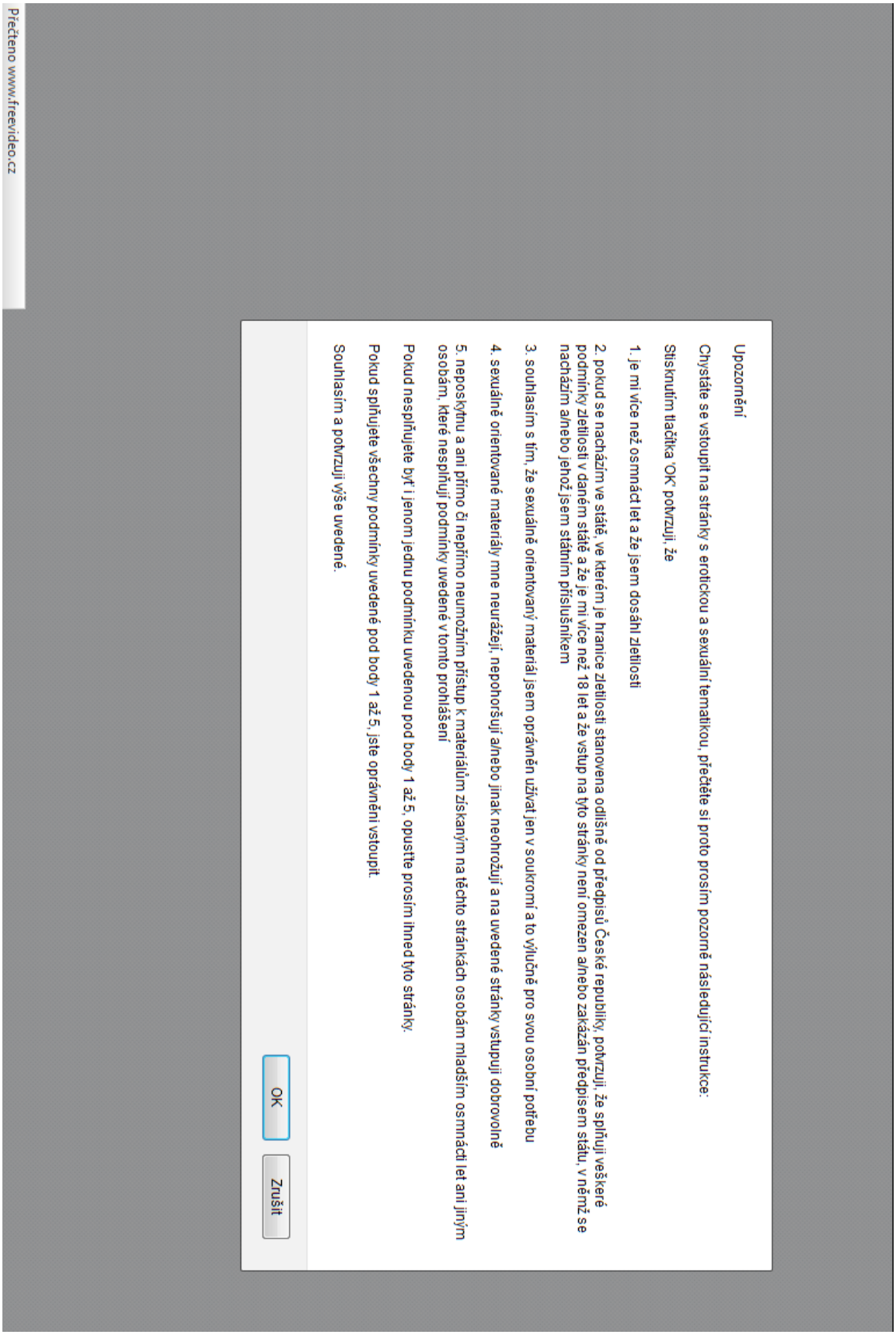
Zdroj:
http://www.ustr.gov/Document_Library/Press_Releases/2008/January/USTR_Announces_Results_of_Out-of-Cycle_Review_for_the_Czech_Republic.html?ht=, zobrazeno 8.7.2008, 17:28

Příloha č. 5 - Zobrazení celosvětového rozložení phishingových útoků z hlediska původce v roce 2006



Zdroj: CHIP.CZ, č. 5/2006

Příloha č. 6 – Ukázka oznámení před vstupem na stránky obsahující pornografický materiál



Zdroj: http://www.freevideo.cz, zobrazeno 2.7.2012, 21:43