Univerzita Karlova v Praze
Právnická fakulta

Jan Hospodka

POČÍTAČOVÁ KRIMINALITA

Diplomová práce

Vedoucí diplomové práce: doc. JUDr. Tomáš Gřivna, Ph.D.

Katedra: Katedra trestního práva

Datum vypracování práce (uzavření rukopisu): 26. 6. 2011

Prohlašuji, že jsem předkládanou diplomovou práci vypracoval samostatně za použití zdrojů a literatury v ní uvedených.

V Praze dne 26. 6. 2011

Jan Hospodka

Poděkování:

Děkuji především vedoucímu diplomové práce doc. JUDr. Tomáši Gřivnovi, Ph.D., jemuž vděčím za rady a četné připomínky. Poděkování patří také lidem, kteří mě inspirovali a pomohli radou při studiu.

Obsah:

Seznam použitých zkratek:

TZ	zákon č. 40/2009 Sb., trestní zákoník
ZSVM	zákon č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů (zákon o soudnictví ve věcech mládeže)
autorský zákon	zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon)
LZPS	zákon č. 2/1993 Sb., listina základních práv a svobod
IT	informační technologie
CD	Compact Disc
DVD	Digital Versatile Disc nebo Digital Video Disc
IP adresa	adresa internetového protokolu (v současnosti verze IPv4, do budoucna se počítá se zavedením verze protokolu IPv6)
USB	Universal Serial Bus – univerzální sériová sběrnice
ČSÚ	Český statistický úřad
URL	Uniform Resource Locator - jednotný lokátor zdrojů, jinými slovy internetová adresa webových stránek
MC	Music Cassette
VHS	Video Home System
FTP	File Transfer Protocol
PIN	Personal Identification Number

Úvod

Pojmy počítačová i kybernetická kriminalita[1] jsou v poslední době zmiňovány stále častěji jak laickou, tak i odbornou veřejností. Veřejnost však často tápe, co se pod pojmem kybernetická kriminalita skrývá a nedokáže si vytvořit ucelený obrázek toho, co všechno se dá pod tento pojem zařadit. Veřejnost můžeme dělit na veřejnost odbornou (s právním vzděláním) a laickou (bez právního vzdělání). Laická veřejnost většinou spoléhá na definice pojmu vytvořené médii, definice jimi předkládané jsou však v naprosté většině případů nepřesné, protože sami autoři definicí problematice příliš nerozumí. Ani právník, který se v rámci své praxe zaměřuje na trestní právo, ať již v rovině vědecké, nebo při výkonu povolání v rámci justice[2], si však často není jistý, jaká jednání by měl zařadit pod pojem kybernetická kriminalita, což je způsobeno především relativní novostí počítačové kriminality. V takových chvílích většinou odborník sahá po zákonu, kde je právní pojem definován nebo nahlédne do komentáře k příslušnému zákonu kde je pojem užit, popřípadě hledá odpověď v ustálené judikatuře soudů. Problém nastává v okamžiku, kdy takové vymezení pojmu neexistuje, což je případ i kybernetické kriminality.

V takové situaci se musí právník pokusit vymezit pojem sám a určit tak, co se dá označit za počítačovou kriminalitu, což je velice nesnadné. Obzvláště hrozí, že při vymezování kybernetické kriminality sklouzne k extrému. Buď pod kybernetickou kriminalitu zahrne téměř veškerou trestnou činnost, která nějak souvisí s počítači nebo se naopak omezí na velice úzkou definici kybernetické kriminality, kdy bude za kybernetickou kriminalitu pokládat pouze kriminalitu páchanou proti počítačům a počítačovým systémům.

Vzhledem k tomu, že si na vymezení pojmu sám netroufám, rozhodl jsem se jej převzít od T. Gřivny tak, jak jej vymezil v rámci přednášky z kriminologie konané

[1] nadále budu oba pojmy, tedy počítačová kriminalita a kybernetická kriminalita, užívat ekvivalentně
[2] soudce, státní zástupce, advokát

v prosinci 2009, avšak s drobnými úpravami. T. Gřivna na této přednášce vymezil kybernetickou kriminalitu, jako soubor 4 druhů útoků:

1) Útoky proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů
2) Útoky spočívající v šíření závadného (nelegálního nebo nežádoucího) obsahu
3) Útoky spočívající v porušování práv duševního vlastnictví
4) Útoky využívající kyberprostor k dalším formám trestné činnosti

Mnou Výše zmíněná úprava se týká především přejmenování první skupiny útoků na *Útoky vedené proti počítačům a počítačovým systémům*. Vzhledem k tomu, jaká jednání jsem do této skupiny útoků zařadil, se totiž tento název jeví jako vhodnější. Současně jsem z poslední kategorie vyčlenil jako samostatné téma *Podvodná jednání na Internetu*. Tato jednání jsou totiž natolik četná a mají tolik podob, že si dle mého názoru zaslouží samostatnou kapitolu v rámci této diplomové práce.

Vzhledem k tomu, že je kybernetická kriminalita velice široké téma, rozhodl jsem se v rámci této diplomové práce se více zaměřit na útoky spočívající v porušování práv duševního vlastnictví, konkrétně pak na neoprávněné zásahy do majetkových práv autorů k jejich autorským dílům a trestněprávní odpovědnost osob, jakýmkoli způsobem s těmito zásahy spjatých. Druhým důvodem zaměření se na útoky spočívající s porušování práv duševního vlastnictví, byla i skutečnost, že okolo těchto zásahů do autorských práv se za poslední léta objevilo mnoho mýtů a ani odborná veřejnost již často neví, co je pravda a co nikoli.

Útoky vedené proti počítačům a počítačovým systémům

Jak již název napovídá, do této skupiny spadají útoky pachatelů, které jsou vedeny přímo proti počítačům a počítačovým systémům, popřípadě proti datům na nich umístěným.

Existuje pouze několik druhů útoků, přičemž těmito útoky si pachatel připravuje půdu pro úspěšné provedení hlavního útoku. Z trestněprávního hlediska se tak ve vztahu k hlavnímu útoku jedná o přípravu trestného činu, v mnohých případech je však již toto jednání samostatným trestným činem.

Trestné činy zabývající se útoky proti počítačovým sítím a počítačům jsou zařazeny do hlavy V. mezi *Trestné činy proti majetku*, kdy postih daného jednání řeší § 230 – 232 zákona č. 40/2009 Sb., trestního zákoníku, ve znění pozdějších předpisů (dále jen „**TZ**“ nebo „**trestní zákoník**“), na trestné činy páchané v prostředí Internetu se však vztahují i jiná ustanovení trestního zákoníku.

Pachatelé

Pachatelé typických útoků pro kybernetickou kriminalitu jsou všeobecně označováni jako hackeři. Jak uvádí Jirovský, V., původně bylo označení „hacker“ určitou formou ocenění znalostí a schopností skupiny programátorů, k nimž ostatní programátoři vzhlíželi, protože se jednalo o programátory, kteří byli natolik schopní a kreativní, že dokázali za použití zcela běžného vybavení neortodoxními metodami dosáhnout kýženého cíle.[3]

V 90. letech 20. století se rozlišovali hackeři a crackeři, kdy hackeři byli v rámci IT komunity nadále ctěni především pro svou schopnost proniknout do systému bez toho, aby na něm způsobili jakékoli škody. Následně pak tito hackeři poskytovali

[3] Jirovský, V. Kybernetická kriminalita (nejen o hackingu, crackingu, virech a trojských koních bez tajemství). Praha: Grada, 2007, s. 47 an.

informace správcům napadeného systému zahrnující jednak údaje o tom, jak překonali zabezpečení systému a dále též doporučení, jak daný bezpečnostní problém vyřešit. Dnes se tito hackeři nejčastěji označují jako white hats.

Opakem těchto hackerů byli crackeři, jejichž cílem nebylo neškodné proniknutí do systému, ale pouhá destrukce za použití stejných technik, jaké používali hackeři. Těmito jedinci bylo a je v IT světě všeobecně opovrhováno. Dnes se pro tyto jedince používá termín black hats, ačkoli se mezi oběma pojmy nedá učinit rovnítko, protože do skupiny black hats se řadí i hackeři, kteří se věnují kriminální činnosti, ovšem nepůsobí v napadeném systému destruktivně, ale spíše v pozici špiona v rámci průmyslové špionáže.

Termín cracking se dnes již v původním významu neužívá. V současnosti termín cracking označuje překonávání ochrany autorskoprávně chráněného obsahu. Paralela s původním významem slova je však patrná dodnes. Snahou člověka, jenž překonává ochranu proti kopírování, je totiž vyřazení dané ochrany, stejně jako bylo cílem crackingu úplné vyřazení napadeného systému.

Pro doplnění výkladu je nutné ještě zmínit, že se dnes rozlišuje i třetí skupina hackerů, tzv. grey hats, kteří jsou jistým přechodovým stádiem mezi white hats a black hats. Tito hackeři se věnují jak trestné činnosti, tak občas naopak vypomáhají při zabezpečování počítačů a informačních systémů.[4] Jak uvádí V. Jirovský, jsou tito hackeři v situaci, kdy si volí, na kterou stranu se nakonec přikloní, tedy volí si svou budoucí kariéru.

Krádež strojového času

Jedná se o typ útoku, kdy pachatel neoprávněně získá prostřednictvím počítačové sítě přístup do počítače a jeho výpočetní kapacitu využívá například ke zkrácení doby

[4] Blíže Jirovský, V. Kybernetická kriminalita (nejen o hackingu, crackingu, virech a trojských koních bez tajemství). Praha: Grada, 2007, s. 54 an.

vyhodnocování určitých dat. Cílem pachatele tak nejsou data v počítači uložená, ale výpočetní kapacita samotného zařízení.

Toto jednání je trestné podle ustanovení § 230 odst. 1 TZ, jako neoprávněný přístup k počítačovému systému. Tohoto trestného činu se dopustí ten, *kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části.*

Překonáním bezpečnostního opatření, může být jednak prolomení programové ochrany počítače hrubou silou, ale též i obejití ochrany počítače, například nalezením tzv. zadních vrátek v systému (vytvořených jinou osobou ať už záměrně, nebo vzniklé nedbalostí tvůrce softwaru[5]), jejich vytvořením, případně nalezením chyb v samotném zabezpečení (hacking).

Jak vyplývá z dikce zákona, je pro spáchání trestného činu nezbytné, aby došlo k překonání zabezpečení. Dokud k tomu nedojde, jedná se stále pouze o pokus ve smyslu § 21 TZ.

V souvislosti s průnikem do systému je třeba vyřešit ještě jeden problém, a to je situace, kdy počítač oběti není nikterak zabezpečen. V takovém případě se však nebude jednat o trestný čin, protože nedochází k překonání bezpečnostního opatření. Trestné tak například nebude, pokud někdo získá přístup k počítači proto, že poškozený nezabezpečil přístup do systému přístupovým heslem. Pak již stačí pachateli jen změnit nastavení počítače.

[5] V rámci týmu programátorů má každý člen přesně vymezenou funkci a podle toho i omezená oprávnění k přístupu do jiné části programu. Jednotlivé části programů jsou programátory psány často nezávisle na sobě a tyto části se dávají dohromady až v konečné fázi tvorby programu. Během následného testování finálového produktu dochází k odstraňování nekompatibility jednotlivých částí. V konečném produktu jsou tedy jednotlivé části již navzájem provázané. Vzhledem k provázanosti programu, se však kvůli opravě jedné chyby, musí provést hned několik dalších oprav v jiných jeho částech. Díky omezenosti oprávnění jednotlivých programátorů, každá oprava vyžaduje často spolupráci nejméně dvou osob. To samotné testování velice zdržuje, proto si programátoři vytvářejí v programech zadní vrátka, aby mohli kdykoli cokoli opravit, bez nutnosti spolupráce s kolegou, který má danou věc na starosti. Obzvláště u softwaru časově náročnějšího na tvorbu se však programátoři často střídají a každý další si vytváří vlastní zadní vrátka do programu, pokud je pak programátor po ukončení práce zapomene odstranit, není pro hackera po jejich nalezení, proniknutí do systému problém.

Pokud se jedná o vzdálený přístup prostřednictvím kyberprostoru, zde se i s ohledem na politiku společnosti Microsoft, jejíž operační systémy Windows jsou nejrozšířenějšími na světě, v praxi nemůže stát, že by počítačový systém byl zcela bez ochrany.

V zásadě jsou mezi uživateli rozšířeny tři operační systémy: Windows, Mac OS, Linux, přičemž většina ostatního softwaru pracuje na platformě operačního systému Windows. To je též důvodem, proč je právě Windows nejrozšířenějším a používá ho většina laické veřejnosti. Právě laická veřejnost je nejzranitelnější skupinou na Internetu, protože často nemá nejmenší tušení, že je třeba se starat o počítačovou bezpečnost, což si uvědomila společnost Microsoft a do svého operačního systému implementovala firewall[6] a nabízí zdarma i antivirový program. Jejich operační systém se ihned po instalaci dokonce sám dožaduje instalace antivirového programu.

Pokud se jedná o zbylé dva operační systémy, ty jsou v ČR užívány spíše pokročilejšími uživateli, kteří jsou si plně vědomi nebezpečí na Internetu a starají se o bezpečnost svých operačních systémů sami.

Proti dostupnosti a utajení počítačových dat

Mezi soukromými subjekty, ale i orgány státní správy, se čím dál tím více dokumentů uchovává v digitalizované podobě, což nejen že umožňuje snadnější a rychlejší přístup k informacím, ale šetří i prostor nezbytný pro skladování velkého množství agendy a koneckonců i finanční prostředky. Stále častěji jsou pak v digitalizované podobě uchovávány i dokumenty obsahující citlivé informace, jejichž zneužití by mohlo způsobit obrovské škody, a to nejen na úrovni ekonomické.

Informace (zejména ty citlivé a veřejně nedostupné) pak mají jistou hodnotu, kterou ovlivňuje nikoli jen vzácnost informace (kolika dalším osobám je informace známa),

[6] Jedná se o zařízení, ale častěji o program, sloužící ke kontrole toku dat mezi počítačovými sítěmi, jehož hlavním úkolem je zabránit neoprávněnému průniku do počítačového systému.

ale i o jak pomíjivou informaci se jedná, respektive jak rychle klesá cena této informace v průběhu času.[7]

Vzhledem k tomu, že se jedná o cennou komoditu, najdou se pochopitelně jedinci, kteří jsou ochotni za tyto informace zaplatit, a tudíž i jedinci, kteří těmito informacemi disponují a jsou ochotni tyto informace za úplatu dále sdělit, ačkoli k tomu nemají oprávnění, nebo těmito informacemi sice nedisponují, jsou však schopni a ochotni k těmto informacím proniknout přes nejrůznější zabezpečení, která jsou za účelem ochrany těchto dat zavedena[8].

Dané jednání se posuzuje jako neoprávněný přístup k počítačovému systému a nosiči informací ve smyslu § 230 odst. 2 TZ.

Dle § 230 odst. 2 TZ, se dopustí trestného činu ten, *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.

Jak vyplývá z jazykového výkladu ustanovení, je irelevantní, zda bylo přístupu dosaženo oprávněně či neoprávněně. Samotné získání přístupu je trestné až

[7] Blíže k hodnotě informace a vztahu dat a informací Požár, J. a kol. Základy teorie informační bezpečnosti. Praha: Policejní akademie ČR; 2007; s. 10 an.
[8] uplatňuje se klasický zákon trhu, tedy: „Kde je poptávka, tam je i nabídka."

v případě, že dojde ke zneužití takového přístupu jedním či více taxativně vymezenými způsoby.

Pokud se jedná o zneužití dat ve smyslu ust. § 230 odst. 2 písm. a) TZ, je zde chráněno subsidiárně především právo autorské a obchodní tajemství, jde tedy především o trestněprávní postih průmyslové špionáže[9]. V případě § 230 odst. 2 písm. b) – d) TZ důvodem, proč se vůbec k trestněprávnímu postihu těchto jednání přikročilo, je fakt, že jakékoli narušení integrity počítačového systému, způsobuje snížení důvěryhodnosti dat v něm obsažených, čímž je způsobována škoda.
Tímto ustanovením je současně chráněn i jakýkoli nosič informací, který obsahuje uvedená data, tedy disky CD, DVD, USB paměti, harddisky počítačů apod.

Opatřování programů a zařízení sloužících k páchání této trestné činnosti, jakož i jejich výroba, dovoz a vývoz, jsou trestné podle § 231 TZ.

Sniffing

Útok spočívá v neoprávněném zachytávání a čtení zasílaných zpráv. Pachatel v tomto případě útočí především proti důvěrnosti dat, která často zneužívá při následných počítačových útocích. Jako nástroj zde slouží počítačový program, jenž má za úkol pro pachatele sledovat provoz na počítačové síti a zaznamenávat obsah zpráv vyhovujících pachatelem stanoveným podmínkám, tzv. sniffer. Záznam je následně automaticky zasílán pachateli prostřednictvím počítačové sítě na určené místo, kde si jej pachatel vyzvedává.

Uvedeným jednáním se pachatel dopouští porušování tajemství dopravovaných zpráv dle § 182 odst. 1, písm. b) TZ, protože zachytává zprávy v průběhu jejich přepravy.[10]

[9] činnosti, kterým se věnují především tzv. black hats, více viz výklad týkající se pachatelů trestné činnosti
[10] usnesení Nejvyššího soudu ČR ze dne 21. 5. 2009, sp. zn. 11 Tdo 349/2009

Opatřování programů a zařízení sloužících k páchání této trestné činnosti, jakož i jejich výroba, dovoz a vývoz, jsou trestné podle § 231 TZ.

DoS útoky (Denied of Service) a DDoS útoky (Distributed Denied of Services)

Útoky tohoto typu spočívají v odpírání služeb počítačového systému.

Cílem pachatele tak v tomto případě nejsou samotná data, ale paralyzace oběti, respektive jejího počítačového systému.

Tento druh útoku probíhá nejčastěji dvojím způsobem:

a) pomocí tzv. pingování serveru:

   Pachatel v tomto případě využívá mechanismu při navazování kontaktu počítače se serverem. Každý počítač při navazování spojení s určitým serverem odesílá malý objem dat na určenou adresu za účelem ověření, zda vůbec daný server existuje. Pokud se mu vrátí odpověď, začíná samotná komunikace počítače a serveru. Podstata útoku spočívá ve změně objemu takto odesílaných dat, který je mnohonásobně větší. Místo toho, aby tak server odpovídal v řádech milisekund, odpovídá v řádech sekund, což při větší četnosti dotazů znamená, že dochází k prodloužení odezvy serveru, a tudíž k horší dostupnosti dat na něm uložených. Při velkém počtu takových „pingnutí“, může dojít i k zamrznutí (počítač nereaguje na dotazy) či celkovému zkolabování systému. Naštěstí je možné provést opatření, která zabrání úspěšnosti útoku, stanovením maximální velikosti najednou přijatých dat v rámci jednoho „pingnutí“.

b) pomocí velkého počtu dotazů:

   V tomto případě spočívá útok v synchronizovaném útoku z mnoha počítačů, které patří předchozím obětem hackera[11]. Útočník dá těmto „ovládaným“ počítačům příkaz vznést v jeden okamžik na určitý server dotazy. Server je

[11] je všeobecně známé, že nezřídka jsou takové sítě ovládaných počítačů předmětem obchodu mezi samotnými hackery

tak stejně jako při „pingování“, zavalen množstvím dotazů, které není schopen vyřídit, v důsledku čehož taktéž zkolabuje. Od „pingování“ se liší především tím, že zasílaný objem dat od jednotlivých počítačů je standardní, díky četnosti dotazů, je však v součtu stejně velký. V současné době není možné provést opatření, aby se podobným situacím zabránilo.

Výše uvedené jednání by se dle mého názoru dalo trestněprávně posoudit jako trestný čin poškození cizí věci ve smyslu § 228 TZ, protože svým jednáním útočník činí servery dočasně neupotřebitelnými a v důsledku jeho jednání tak vzniká škoda například v podobě ušlého zisku společnosti.

Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 232 TZ)

Toto ustanovení trestního zákoníku směřuje proti trestuhodné nedbalosti počítačových odborníků, spočívající například v tom, že počítačový odborník při zásahu do počítačového systému neprovede zálohu dat, ačkoli je zde velké riziko jejich poškození, přičemž následně skutečně dojde k poškození těchto dat v důsledku jeho nedbalosti. V tomto ustanovení se projevuje neustále vzrůstající hodnota informací, které jsou umístěny na nosičích informací a v počítačích.

Podvodná jednání v kyberprostoru

Podvodné jednání v prostředí kyberprostoru je velmi častým jevem. Pachatel zde zneužívá důvěry oběti, aby z ní vylákal finanční prostředky, přihlašovací údaje nebo citlivé informace.

Současně zde má výhodnější postavení než by měl při osobním kontaktu, protože může oslovit najednou větší počet potencionálních obětí a vyhýbá se rizikům spojeným s osobním jednáním, zejména odhalení lži prostřednictvím nečekané otázky oběti, v důsledku nonverbální komunikace, nebo nečekaného vývoje situace. Pachateli je kyberprostorem poskytována i jistá míra anonymity, protože je v podstatě vyloučena jeho identifikace obětí. Identifikace konkrétního pachatele je k tomu navíc ještě obtížnější, protože i když se vyšetřovatelům podaří identifikovat konkrétní počítač podle IP adresy, je nutné prokázat, že se daného jednání dopustila konkrétní osoba, což je mnohdy velice obtížné, ne-li nemožné.

Obecně existuje mnoho druhů podvodných jednání na Internetu a pouhé vyjmenování všech způsobů, jak se snaží lidé prostřednictvím počítače ilegálním způsobem obohatit na úkor jiného, by vydalo na několik stránek, proto dále uvádím pouze několik z nejznámějších druhů podvodů.

Phishing

Pro tento druh podvodů je charakteristické, že je zneužívána důvěra oběti a skutečnost, že naprostá většina populace nemá příliš hluboké znalosti v oblasti výpočetní techniky, či bezpečnostních opatření a standardních postupů při řešení problémů se zabezpečením. Snahy o vzdělávání veřejnosti, ze strany především finančních institucí, jsou veřejností často pokládány za reklamní sdělení a v důsledku toho ignorovány nebo jsou tyto informace umístěny na takových místech, kde jsou pro veřejnost prakticky nedostupné.

Pachatel tohoto jednání vzbuzuje v oběti důvěru a následně manipuluje se svou obětí, aby dosáhl kýženého cíle. Cílem může být získání citlivých informací, osobních dat nebo přístupu k bankovnímu účtu oběti.

Jak tedy phishingový útok probíhá? Scénář útoku je vždy stejný, liší se pouze v detailech.

Oběť je kontaktována prostřednictvím e-mailu, který je odeslán z e-mailového účtu velice podobného e-mailovým účtům užívaným institucí, za níž se pachatel vydává. V samotné zprávě je následně oběť informována o smyšlené události spočívající například v narušení bezpečnosti, přičemž zpráva obsahuje i odkaz na falešnou webovou stránku, která je po grafické stránce často velice podobná stránkám dané instituce a liší se pouze v URL adrese, kde má oběť zadat své přihlašovací údaje. Tyto údaje jsou pak postoupeny pachateli, který tímto získává přístup k bankovnímu účtu oběti a prostředkům na něm.

Vážení klienti,

v posledních dnech sledujeme zvýšený výskyt podvodných e-mailů, které lákají z klientů přímého bankovnictví České spořitelny jejich bezpečnostní údaje. Stejně jako při předchozích útocích na naše klienty tyto e-maily předstírají, že odesílatelem zprávy je Česká spořitelna a navádějí adresáta k otevření stránky v internetu z přiloženého odkazu. Po otevření odkazu je klientovi zobrazena podvodná stránka napodobující službu SERVIS 24 Internetbanking České spořitelny.[12]

Nigerijské podvody (dopisy)

Název tohoto druhu podvodů se odvíjí od západoafrického státu Nigerie, odkud byly odeslány první e-maily tohoto typu. Následně se tento druh podvodů rozšířil i mezi

[12] Zpráva byla uveřejněna dne 18.5.2010 na stránkách České spořitelny, a.s., dostupná je na adrese http://www.csas.cz/banka/content/inet/internet/cs/news_ie_955.xml

většinu ostatních afrických států, přízvisko Nigerijské, však již těmto podvodným jednáním zůstalo.

U tohoto druhu podvodu, je oběť kontaktována anglicky psaným e-mailem (ačkoli v poslední době se pachatelé za účelem zvýšení úspěšnosti útoků uchýlili i k automatickým překládacím programům[13]), ve kterém je oběť informována o smyšlené příležitosti k rychlému zbohatnutí. Zpráva dále obsahuje instrukce k převodu finanční částky, jejíž poukázání je zdůvodněno nejčastěji správními poplatky v zemi odesilatele nebo vkladem do podnikání.

Finanční prostředky jsou následně pachatelem vybrány dříve, než poškozený zjistí, že se stal obětí podvodu.

Tento druh podvodů však nepoškozuje pouze oběť, ale i stát, ze kterého pachatel kontaktuje svou oběť. E-mail totiž většinou obsahuje i oficiálně působící potvrzení státní instituce o pravdivosti uvedených informací. V důsledku tohoto jednání tak dochází i k poškozování ekonomických zájmů daného státu a potažmo i jeho občanů, protože potencionální investoři ztrácejí důvěru v instituce a potvrzení vydávaná orgány státu, a pokud se přímo nerozhodnou ustoupit od investičního záměru, vyžadují velké množství potvrzení osvědčujících jednu a tu samou skutečnost.

Případy podvodných dopisů došly až tak daleko, že dokonce negativně ovlivnily i nigerijskou ekonomiku. Potřeba, prověřovat partnery v Nigérii totiž prodražila podnikání zahraničních investorů v této zemi. Zárukou, že jednáte se správnými lidmi, nebylo ani to, že jednání bylo na úrovni registrovaných společností či přes vládní hlavičkový papír. Protože byla pošpiněna image i Nigerijské centrální banky, vydával dokonce ústav v největších zahraničních denících inzeráty, v nichž upozorňoval, že pokud je nabídka příliš lákavá na to, aby to byla pravda, pak to pravděpodobně není pravda.[14]

[13] on-line verzí překládacího programu je například překladač společnosti Google International LLC, dostupný na http://translate.google.cz

[14] Článek byl uveřejněn dne 9.2.2004, on-line je dostupný na stránce http://technet.idnes.cz/sw_internet.asp?r=sw_internet&c=A040205_5251433_sw_internet

Dialer

Jedná se o typ útoku, který se v dnešní době již nevyužívá zejména z důvodu pokroku v oblasti informačních technologií a rozšíření vysokorychlostního připojení. Útoky tohoto druhu byly rozšířené především v 90. letech minulého století, kdy mezi připojeními osobních počítačů k Internetu dominovalo tzv. vytáčené připojení, tedy připojení probíhající prostřednictvím modemu a běžné telefonní linky přes poskytovatele připojení k Internetu. Postupem času se však od tohoto připojení začalo ustupovat především z ekonomických důvodů, nízké rychlosti připojení a dále též z důvodu toho, že v době připojení k počítačové síti Internet byla blokována telefonní linka.

Útok probíhal tak, že útočník umístil na Internet program, který běžný uživatel při prohlížení Internetu nevědomky nainstaloval do svého počítače. Program následně změnil přihlašovací údaje pro připojení a při dalším přihlášením k síti byl uživatel přihlášen přes odlišného poskytovatele, často s mnohem vyšším tarifním zpoplatněním.

Jak jsem uvedl výše, tento typ útoku se dnes již nevyužívá především z toho důvodu, že neustále roste počet uživatelů využívajících vysokorychlostní připojení. Podle údajů ČSÚ, činil podíl vytáčeného připojení v EU v roce 2009 necelých 12%, v ČR pak 9,7% připojení.[15]

Salami attack (salámový útok)

Jedná se o typ podvodu, jehož oběťmi se nejčastěji stávají finanční instituce, přičemž v tomto typu podvodu spočívá činnost pachatele ve zneužití bezpečnostní chyby informačního systému finančních subjektů.

Nejčastějšími pachateli těchto útoků jsou zaměstnanci finančních institucí s perfektní znalostí interního informačního systému. V zahraniční literatuře se tento typ podvodu

[15] Informace ze dne 27.6.2010, on-line dostupné na http://www.czso.cz

řadí mezi tzv. „white collar crimes“, tedy zločiny bílých límečků podle charakteristického oděvu zaměstnanců finančních institucí.

Naprostá většina činností spojených s financemi je v současnosti automatizována, především pak jednotlivé finanční operace. Samotný útok spočívá v tom, že pachatel vytváří program, který zneužívá chyby systému při těchto operacích.

Při provádění finančních operací je stanoveno např. u připisování úroku, jak má být daná částka zaokrouhlena a na kolik desetinných míst. Může však dojít k tomu, že případný vzniklý přebytek není nikde evidován (což je právě onou chybou systému), čehož zneužívá pachatel a tento přebytek prostřednictvím programu automaticky poukazuje na svůj bankovní účet. V rámci celého systému se jedná o natolik nepatrné transakce, že nevzbuzují vzhledem k výši připisovaných částek příliš mnoho pozornosti, pročež odhalení tohoto druhu podvodu je v naprosté většině případů dílem náhody.

Jak výše uvedený popis způsobu páchání tohoto druhu podvodu napovídá, specifickou vlastností tohoto jednání je jeho četnost. Celková škoda tak může být velmi velká.[16]

Trestněprávní kvalifikace uvedených jednání

Ve všech výše uvedených případech se jedná o trestný čin podvodu dle § 209 TZ, který je zařazen v hlavě V. zvláštní části trestního zákoníku.

Tohoto trestného činu se může dopustit kdokoli, protože není stanoven žádný speciální subjekt. Jedná se o úmyslný trestný čin, pro jeho spáchání je tedy třeba alespoň nepřímého úmyslu.

[16] Požár, J. a kol. Základy teorie informační bezpečnosti. Praha: Policejní akademie ČR, 2007, s. 45

Naplnění skutkové podstaty trestného činu se dopustí ten, *kdo sebe, nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu, nebo zamlčí podstatné skutečnosti*. Jak vyplývá ze samotné skutkové podstaty, nejdůležitějšími znaky je vznik majetkové škody, která je důsledkem omylu oběti, a úmysl pachatele využít takového omylu k vlastnímu, či cizímu obohacení.

Rozeberme si tedy skutkovou podstatu. Jak je uvedeno výše, důležitá je skutečnost, že se oběť mýlí ve svých představách a domněnkách v důsledku přičinění pachatele. V zásadě je možné spáchat tento trestný čin trojím způsobem:

a) Pachatel trestného činu v tomto případě svým aktivním jednáním u své oběti úmyslně vyvolal mylnou představu o skutečnosti a tuto představu udržuje, aby se následně na úkor své oběti obohatil on, nebo třetí osoba.
b) Pachatel svým aktivním jednáním neuvádí oběť v omyl, ale je si vědom, že oběť má mylné představy o skutečnosti, či disponuje nesprávnými informacemi. Místo toho, aby však uvedl vše na pravou míru, rozhoduje se této skutečnosti využít (úmyslně udržuje stav oběti), aby opět sebe, či jinou osobu na úkor oběti obohatil.
c) Pachatel poskytuje své oběti zcela pravdivé informace, ale zamlčí jí důležitou skutečnost, a tím opět vyvolává u oběti mylné představy. Cílem jednání je opět obohacení sebe sama, či jiné osoby.

Jak vyplývá z výše uvedeného, ve všech třech případech je pachatel přesvědčen, že by jeho oběť daný úkon neučinila v případě, že by znala pravdu nebo alespoň to, co pachatel pokládá za pravdu.
Velmi důležitý je stav mysli pachatele v době spáchání trestného činu, tedy jaké měl pachatel představy pokud jde o skutečnosti a jednání dalších osob. Tento výklad zahrnuje především výše uvedený phishing a nigerijské podvody.

Abychom však mohli s jistotou označit za podvody i další dva výše uvedené typy podvodů, tedy dialeru a salami attack, musíme nahlédnout do výkladového ustanovení § 120 trestního zákoníku, dle kterého lze spáchat trestný čin podvodu

i prostřednictvím provedení zásahu do počítačových informací nebo dat, zásahu do programového vybavení počítače nebo jiné operace na počítači, zásahu do elektronického nebo jiného technického zařízení, nebo využitím takového zásahu provedeného jiným.

V případě dialeru tak dochází ke spáchání zásahem do programového vybavení počítače, čímž je uváděn uživatel v omyl, protože ten se i nadále domnívá, že se připojuje přes stávajícího poskytovatele připojení k Internetu.

U salami attack spočívá jednání v tom, že pachatel objeví chybu v systému, která vznikla opomenutím jiné osoby (tvůrce softwaru), místo toho, aby ji však nahlásil svým nadřízeným, aby byla opravena, případně tuto chybu sám opravil, udržuje své nadřízené v nevědomosti a využívá tak mylné domněnky, že je systém v pořádku a k podobnému opomenutí při tvorbě softwaru nedošlo.

V případě trestného činu podvodu však není trestný pouze dokonaný trestný čin, respektive pokus trestného činu, který je dle § 21 odst. 2 TZ stejně trestný jako čin, k jehož dokonání pokus směřoval, ale trestná je i příprava trestného činu ve smyslu § 20 trestního zákoníku. Podmínky trestnosti přípravy trestného činu jsou stanoveny v § 20 odst. 1 TZ, dle kterého se musí jednat o přípravu ke spáchání zvlášť závažného zločinu (§ 14 odst. 3 TZ) a ve zvláštní části trestního zákoníku musí být navíc výslovně stanoveno, že je příprava trestná. Jak jsem uvedl již výše, je jedním z hlavních znaků trestného činu vznik škody. Výše vzniklé škody je pak též jedním ze znaků kvalifikované skutkové podstaty. O podvod, který se dá označit za zvlášť závažný zločin, se bude jednat ve dvou případech, pokud má podvod mít za cíl usnadnění nebo umožnění spáchání vlastizrady, teroru, nebo teroristického útoku, nebo, a což bude dle mého názoru mnohem častější případ, pokud je způsobena škoda velkého rozsahu, což je dle § 138 odst. 1 TZ škoda ve výši nejméně 5.000.000,- Kč. Pro trestnost přípravy je důležité, že nemusí vůbec dojít k pokusu ani dokonání samotného podvodu, stačí již to, že dochází k úmyslnému vytváření podmínek pro jeho spáchání, současně je důležitá představa pachatele týkající se výnosu, který ze spáchání trestného činu očekává.

Trestné tedy bude v případě phishingu a nigerijských dopisů i vytváření fiktivní, či lživé zprávy, u dialeru a salami attack tvorba software, který by měl provést změnu, nebo automaticky provádět převody peněžních prostředků.

Porušování práv duševního vlastnictví

Duševní vlastnictví je produktem tvořivosti člověka a je pro něj charakteristické, že potřebuje hmotný nosič informace, aby mohlo být objektivně vnímatelné. Má v podstatě charakter změny, ke které došlo na daném nosiči informace.

Pod pojem duševní vlastnictví spadají především práva autorská, práva související s právem autorským, ale i práva k ochranné známce a jiným označením. Daná problematika je pak řešena v rámci hlavy VI. dílu 4. zvláštní části trestního zákoníku nazvaném *Trestné činy proti průmyslovým právům a proti autorskému právu.* Rozhodl jsem se věnovat pouze porušování autorských práv a práv souvisejících s právem autorským (dále jen „**autorská práva**“) a právy k databázi, protože v prostředí kyberprostoru příliš často nedochází k porušování práv k ochranné známce a jiným označením.

Porušování autorských práv je postihováno v rámci ustanovení § 270 TZ jako trestný čin *Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi*.

Autorská práva

Stěžejním pojmem v případě ochrany autorských práv je termín *autorské dílo*, který je vymezen v § 2 odst. 1 zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů (dále jen „**autorský zákon**“ nebo „**AZ**“)[17], kdy se za autorské dílo pokládá *dílo literární a jiné dílo umělecké a dílo vědecké, které je jedinečným výsledkem tvůrčí činnosti autora a je vyjádřeno v jakékoli objektivně vnímatelné podobě včetně podoby elektronické.* Ustanovení § 2 odst. 2 autorského zákona pak

[17] § 270 trestního zákoníku, využívá tzv. blanketní dispozice, tedy sám nestanoví, co je chápáno autorským dílem a právy autora k dílu, ale odkazuje na zvláštní předpis, tuto oblast upravující. Tímto zvláštním předpisem je zákon č. 121/2000 Sb., autorský zákon

dodává,

že za autorské dílo *se považuje též počítačový program a databáze.* Ustanovení zákona je značně obecné, což značí, že úmyslem zákonodárce bylo poskytnout pokud možno co nejširší ochranu autorským dílům, a to nejen těm, která jsou momentálně známa široké veřejnosti (výčet uvedený v autorském zákoně má charakter pouze demonstrativní, nikoli taxativní), ale i dílům druhově zcela odlišným, která se v budoucnu objeví. Charakteristickou vlastností takových děl musí však být skutečnost, že půjde o produkt tvůrčí činnosti autora a tento produkt bude objektivně vnímatelný (již zmíněná charakteristická závislost na hmotném nosiči informace).

Neoprávněný zásah do autorských práv

Neoprávněným zásahem do autorských práv rozumíme především porušení práv autora stanovených v § 11 a 12 autorského zákona. Rozlišujeme práva tzv. osobnostní, kam patří právo na zveřejnění díla, právo osobovat si autorství k dílu, právo autora udělit svolení k jakékoli změně nebo jinému zásahu do svého díla, přičemž nesmí být dílo užito takovým způsobem, který by snižoval jeho hodnotu. Druhou skupinou práv autora jsou pak práva majetková, kam patří především právo autora užít dílo, rozmnožovat ho a šířit. Tato svá majetková práva může autor propůjčit i jiné osobě.

V souladu s Bernskou úmluvou[18] osobnostní práva zanikají smrtí autora, i nadále jsou však zachována práva stanovená v § 11 odst. 5 autorského zákona[19]. Práva majetková upravuje § 27 daného zákona, kdy základní dobou trvání je doba života autora a dalších 70 let po jeho smrti, smrtí autora tedy nezanikají.

[18] čl. 6, Bernské úmluvy o ochraně literárních a uměleckých děl ze dne 9.9.1886 ve znění poslední (pařížské) revize z roku 1971 vyhl. MZV č. 133/1980 Sb.

[19] § 11 odst. 5 zákona č. 121/2000 Sb. - Po smrti autora si nikdo nesmí osobovat jeho autorství k dílu, dílo smí být užito jen způsobem nesnižujícím jeho hodnotu a musí být uveden autor díla, nejde-li o dílo anonymní. Ochrany se může domáhat kterákoli z osob autorovi blízkých, toto oprávnění mají, i když uplynula doba trvání majetkových práv autorských. Této ochrany se může vždy domáhat i právnická osoba sdružující autory nebo příslušný kolektivní správce podle tohoto zákona (§ 97 autorského zákona)

Po uplynutí doby trvání majetkových práv se z autorského díla stává ve smyslu ustanovení § 28 autorského zákona, dílo volné, které může kdokoli bezplatně užít. Jelikož ustanovení § 270 trestního zákoníku poskytuje ochranu majetkovým právům, jejich zánikem pozbývá dílo i trestněprávní ochrany.

Za života autora je v zásadě k užití díla třeba oprávnění, které autor uděluje uživateli tzv. licenční smlouvou, která je upravena v rámci autorského zákona v ustanoveních § 46 a násl.

Volná užití a zákonné licence

Z pravidla, že k užití díla je třeba souhlasu autora uděleného formou licenční smlouvy, existuje určitá skupina výjimek, kdy fakticky dochází k nakládání s dílem, avšak autorský zákon je buď nepokládá za užití díla, nebo přímo zakládá oprávnění určitých subjektů k nakládání s dílem v zákoně stanoveným způsobem. Tuto výjimku obsahují ustanovení § 30 – 39 autorského zákona nesoucí společný název *Volná užití a zákonné licence*.

V souvislosti s kybernetickou kriminalitou je důležité především to, co autorský zákon pokládá a nepokládá za užití díla a za zásah do autorského práva. Danou oblast upravují § 30 – 30b AZ, pro oblast kybernetické kriminality je pak použitelné a stěžejní pouze ustanovení § 30 autorského zákona, protože § 30a AZ upravuje rozmnožování autorského díla na papír a podobný podklad a § 30b AZ upravuje použití autorského díla pro předvedení přístroje zákazníkovi.

Vzhledem ke skutečnosti, že kybernetická kriminalita se odehrává v kyberprostoru, kde se jako hmotný nosič informace nevyužívá papír, či jiný podobný podklad ve smyslu § 30a AZ, můžeme toto ustanovení vyloučit a dále se jím nemusíme zabývat, protože dané ustanovení upravuje především kopírování dokumentů na kopírovacích strojích.

Pokud se jedná o ustanovení § 30b autorského zákona, toto se vztahuje na případy, kdy autorské dílo slouží jako prostředek k prezentaci schopností zařízení, tedy v případě počítačů se bude jednat o prezentaci výkonu hardwaru prostřednictvím aplikací kladoucích vysoké nároky na výkon zařízení. Za tímto účelem budou nejvíce využívána audiovizuální díla a programy, kdy užívání autorskoprávně chráněných bude mít charakter jednorázového užití (demonstrace výkonu), nikoli užívání soustavného, jak je tomu právě u kybernetické kriminality.

Dle § 30 odst. 1 autorského zákona se nepovažuje za užití díla *užití pro osobní potřebu fyzické osoby, jejímž účelem není dosažení ať už přímého, nebo nepřímého hospodářského, nebo obchodního prospěchu*. Osobní potřebou se pak rozumí ve smyslu příslušných ustanovení občanského zákoníku užití pro potřebu fyzické osoby a osob sdílejících s ní společnou domácnost (*fyzické osoby, které spolu trvale žijí a společně uhrazují náklady na své potřeby*[20]) a dále pro potřebu osob blízkých. Tento výklad osobní potřeby by mohl být napadán z důvodu značné extenzivnosti, avšak výklad je ovlivněn reálnou aplikací ustanovení. Pokud bychom přistoupili na výklad restriktivní, znamenalo by to, že vnímat autorské dílo by mohla pouze jediná fyzická osoba v době, kdy by byly ostatní fyzické osoby obývající společnou domácnost nepřítomné. Aplikace ustanovení § 30 odst. 1 autorského zákona by se tak mnohdy stala fakticky nemožnou. Proto se pod osobní potřebu subsumují i osoby blízké a osoby obývající společnou domácnost, širší výklad by naopak dle mého názoru byl nezákonným, jelikož by porušoval ustanovení čl. 34 odst. 1 LZPS, poněvadž by autorská díla zcela pozbyla právní ochranu. Výše uvedený výklad ustanovení se tedy jeví jako nejvhodnější kompromis mezi oběma extrémy.

Co autorský zákon v § 30 odst. 1 autorského zákona myslí termínem *užití pro osobní potřebu,* je konkretizováno v § 30 odst. 2 autorského zákona, které říká, že *zásahem není pořízení záznamu, rozmnoženiny, či napodobeniny díla pro osobní potřebu*.

[20] § 115, zákona č. 40/1964 Sb., občanský zákoník

Databáze

Jak jsem uvedl výše, za autorské dílo je pokládána i databáze. V případě databáze však musí být splněna podmínka, že se jedná o databázi, která je specifická způsobem výběru nebo uspořádáním, musí se v ní tak jistým způsobem promítat kreativita autora. Jako typický druh databáze nepodléhající ochraně autorskoprávní se většinou uvádí telefonní seznam, autorskoprávní ochraně však určitě bude podléhat databáze podnikatelů[21], vytvořená například společností Seznam.cz, a.s., protože je specifická tím, že obsahuje i provozní doby podnikatelů, odkazy na jejich webové stránky, kontaktní údaje na ně atd., přičemž pravdivost a aktuálnost údajů jsou průběžně kontrolovány.[22]

Počítačové programy

Program jako takový není v autorském zákoně definován, v rámci § 65 odst. 1 autorského zákona je pouze uvedeno, že program je chráněn jako dílo literární. Definice programu je tak ponechána praxi a právní vědě.

Program by se dal definovat jako soubor instrukcí zakódovaných do programovacího jazyka určujících jak se má za splnění určitých podmínek počítač zachovat nebo, jak uvádí komentář k Trestnímu zákoníku, *nehmotný výsledek autorovy tvůrčí činnosti, tedy určitá struktura daná organizací dat, posloupností instrukcí a volbou algoritmů a způsobem komunikace s uživatelem, který je většinou zapsán ve zdrojovém textu, nebo strojovém (binárním) kódu*[23]. Za autorské dílo je pokládán (dle autorského zákona) program, který je původní, tedy je autorovým vlastním duševním výtvorem. V této souvislosti vzniká otázka, zda je možné, aby existoval program, který by nebyl původní, tedy nebyl autorovým duševním výtvorem. Domnívám se, že taková

[21] termín podnikatel je použit ve smyslu § 2 odst. 2, zákona č. 513/1991 Sb., obchodního zákoníku
[22] Zmíněná databáze je využívána v rámci služby Firmy.cz
[23] Šámal, P.a kol., Trestní zákoník II. § 140 až 421. Komentář. 1. vydání. Praha: C.H.Beck, 2010; s. 2500

situace nastat nemůže už ze samotné podstaty programování, tedy tvorby programů, kdy při programování jde v první řadě o vyřešení určitého specifického problému, k této činnosti je pak bezpodmínečně třeba kreativní myšlení.

Oprávnění k užití programu

Veškeré výše uvedené informace týkající se užívání v rámci volného užití a zákonné licence platí pro všechny druhy děl s výjimkou programu neboli softwaru. Software je totiž na základě § 30 odst. 3 autorského zákona vyňat z okruhu děl, která v případě nekomerčního užívání díla fyzickou osobou pro vlastní potřebu je možné užívat v rámci tzv. volného užití. Toto faktické užívání je v případě programu pokládáno za užívání díla i ve smyslu autorského zákona, tudíž je k jeho užívání třeba souhlasu autora uděleného licenční smlouvou. Za zmínku stojí, že autorský zákon obsahuje ve svém § 66 omezení rozsahu práv autora k počítačovému programu, přičemž v jednotlivých odstavcích jsou upraveny způsoby nakládání s programem nezbytné pro samotné užívání programu. Doslovným výkladem oprávnění autora by totiž v případě softwaru došlo k faktické nemožnosti tento software užívat, protože by nebylo možné nainstalovat program na harddisk počítače a následně ho na počítači spouštět.

V souvislosti se skutečností, že je třeba k veškerému užívání softwaru třeba licenční smlouvou udělený souhlas, je nutné podotknout, že k neoprávněnému užívání a tudíž i k neoprávněnému zásahu do práv autora dochází nejen při užívání softwaru bez toho, aby byl uživateli poskytnut souhlas autora v podobě licenční smlouvy, ale i v případě, že je software užíván ve větším rozsahu, či k účelům, k nimž autor v rámci licenční smlouvy souhlas neposkytl[24]. Tento problém může například nastat, pokud si uživatel zakoupí komerční software[25], kdy v rámci uzavírání kupní smlouvy je uzavírána licenční smlouva opravňující nabyvatele k užití programu k nekomerčním účelům[26]. Jestliže pak uživatel využije tohoto programu ke

[24] jedná se tedy o překročení rozsahu poskytnuté licence
[25] vysvětlení pojmu níže
[26] Typickým příkladem mohou být balíčky kancelářských programů od společnosti Microsoft

komerčním účelům, například k podnikání, dostává se do rozporu s licenční smlouvou, čímž neoprávněně zasahuje do práv autora k dílu.

V souvislosti s rozsahem licenčních oprávnění poskytovaných jejich autory se rozlišují následující 4 skupiny programů:

1) Free software – charakteristickým znakem tohoto software je skutečnost, že autor je buď neznámý, nebo je známý, ale poskytl tento software pro volné užívání bez jakéhokoli omezení. Software je pak samotnými uživateli zdokonalován a upravován, jeho užívání není nikterak zpoplatněno.

2) Freeware[27] – tento software je většinou určen pro nekomerční účely, licence k jeho užívání je v tomto případě bezplatná, užívání software pro komerční účely je pak zpoplatněno.

3) Shareware – je druhem software, který je ve své podstatě již softwarem komerčním. Jedná se často o komerční software, jehož některé funkce jsou deaktivovány nebo je užívání programu omezeno časově[28], či počtem spuštění. Po uplynutí stanovené lhůty, či provedení stanoveného počtu úkonů se program sám zablokuje a požaduje zakoupení licence k jeho dalšímu užívání[29]. Smyslem tohoto kroku je snaha oslovit velký počet potencionálních zákazníků a umožnit jim si produkt otestovat a následně je přimět k uzavření licenční smlouvy. V podstatě se tak jedná o reklamní strategii výrobců softwaru.

4) Komerční software – do této skupiny spadá většina softwaru. Software je v tomto případě poskytován za úplatu, jeho tvorba je zdrojem obživy jeho tvůrců.

[27] Často dochází k jeho zaměňování s free software
[28] např. po dobu 30 dnů od instalace
[29] Pro případ, že by se uživatel snažil odstraněním a následnou opětovnou instalací obejít ochranu programu a zajistit si tak bezplatné užívání díla, zůstává v systémové složce soubor, který pokud je při následné instalaci programu detekován, způsobí že se program zablokuje a požaduje zakoupení licence

V souvislosti s Internetem je ještě třeba zmínit, že způsob získání samotného software není v zásadě z hlediska ustanovení §270 odst. 1 TZ důležitý, rozhodná je existence, případně rozsah oprávnění uděleného prostřednictvím licenční smlouvy ze strany autora.

Z důvodu přehlednosti jsem se také rozhodl nejprve vyložit vývoj a trestněprávní postih v oblasti šíření audio a audiovizuálních děl a teprve následně vývoj a postih v případě programů, z důvodu odlišné úpravy těchto děl v rámci autorského zákona.

Způsoby sdělování díla

Počátky ilegálního kopírování a následného šíření autorských děl můžeme vysledovat do doby zavedení MC a VHS[30] mezi širokou veřejnost v 80. letech minulého století. Kopírování těchto kazet probíhalo nejčastěji v jednotlivých domácnostech, a takto vytvořené kopie byly dále šířeny v okruhu přátel a známých.

Milníkem v šíření autorských děl tímto způsobem bylo zavedení CD a později i DVD. Při kopírování MC a VHS kazet byl totiž pachatel omezen schopnostmi přehrávače, na němž kopíroval obsah. Zkopírování jedné 90 minutové MC kazety, tak trvalo 90 minut. V tomto směru znamenalo zavedení CD výrazný pokrok, protože zkopírování obsahu trvalo jen zlomek tohoto času a simultánně mohlo být vytvářeno hned několik kopií. Ilegální kopírování tím nabylo na objemu a škody způsobované pachateli nahrávacím společnostem začaly narůstat. Rovněž se okruh osob, jimž byl pachateli dále obsah poskytován, rozšířil i o ostatní členy společnosti, někteří se na distribuci těchto ilegálních kopií snažili i vydělávat. Proti ilegálnímu kopírování děl se producenti snažili bojovat zavedením ochran proti kopírování, ale bez úspěchu[31].

[30] Jedná se o zkratky MC – Micro Cassette, VHS – Video Home System
[31] Ochrany proti kopírování obsahovaly již VHS kazety dodávané do videopůjčoven

S rozšířením vysokorychlostního připojení k Internetu mezi veřejnost se přenesla činnost pachatelů do prostoru počítačových sítí. Právě tento krok jim umožnil šířit obsah rychleji mezi větší okruh osob a s relativně menším rizikem dopadení. Z počátku se jednalo spíše o využívání FTP serverů[32], na které měla přístup skupina lidí v rámci uzavřené počítačové sítě vysokoškolských kolejí[33]. Později se však začal okruh osob, které měly k těmto datům přístup, rozšiřovat. Skutečný boom pak zaznamenalo ilegální šíření autorskoprávně chráněných děl v souvislosti se vznikem tzv. peer-to-peer sítí. Uvedený protokol byl vytvořen za účelem komunikace mezi uživateli prostřednictvím počítačové sítě pro aplikaci Skype. Díky své schopnosti rychle přenášet velká množství dat a nezávislosti na existenci centrálního serveru, ze kterého by byla data poskytována jednotlivým uživatelům, byl však přímo ideální i pro ilegální sdělování autorsky chráněného obsahu.

V současnosti probíhá šíření autorskoprávně chráněného obsahu především prostřednictvím peer-to-peer sítí a datových úložišť:

a) Peer-to-peer sítě

   Šíření obsahu prostřednictvím peer-to-peer sítí závisí na vytvoření tzv. torrentu neboli odkazu k zapojení do sítě. K využívání tohoto protokolu je nezbytné mít nainstalován některý z klientů[34]. Pokud se uživatel rozhodne stahovat data, zapojuje se do sítě, v níž současně stahuje a dále sděluje fragmenty stahovaného souboru, přičemž dalšímu sdělování nemůže zabránit. Jak jsem uvedl výše, neobjevuje se zde centrální server, proto je velice obtížné takovému sdělování dat zabránit.

[32] FTP (anglicky File Transfer Protocol), blíže http://cs.wikipedia.org/wiki/File_Transfer_Protocol
[33] V tomto směru jsou zřejmě nejproslulejší vysokoškolské koleje na Strahově v Praze, kde dle tvrzení očitých svědků v době zásahu Policie v roce 2007 studenti vyhazovali pevné disky svých počítačů z oken kolejí.
[34] např.: BitLord, či BitComet

b) Datová úložiště

V tomto případě je autorsky chráněný obsah umístěn na servery společností, které poskytují služby tzv. datového úložiště[35], tedy prostoru na serveru, kam může kdokoli uložit svá data, uživateli je vygenerován odkaz ke stažení uvedených dat, který následně může zaslat jiné osobě. Tato služba má primárně sloužit ke kompenzaci nedokonalosti e-mailové komunikace poskytovateli e-mailových služeb je totiž omezována velikost zasílaných příloh e-mailu. Současně jsou taková data dostupná pro jejich majitele kdekoli na světě.

Pro oba dominantní způsoby šíření autorsky chráněného obsahu je důležitá existence webových stránek, kam jsou umisťovány odkazy na tento obsah.
V případě tzv. datových úložišť jsou to nejčastěji různá diskusní fóra, kam uživatelé umisťují odkazy ke stažení těchto dat, v případě peer-to-peer sítí jsou to pak specializované webové stránky jako jsou mininova.org[36] nebo momentálně asi nejznámější stránka thepiratebay.org[37].

Trestněprávní posouzení jednání

Jak je to tedy s trestněprávní odpovědností jednotlivých osob, které na ilegálním šíření autorských děl participují.

a) Peer-to-peer sítě

V případě výše uvedeného šíření díla prostřednictvím peer-to-peer sítí, zde vystupují v podstatě tři osoby, jednak je to uploader, který torrent vytváří a odesílá prostřednictvím torrentu autorskoprávně chráněný obsah, dále je to downloader,

[35] největším poskytovatelem těchto služeb, je švýcarská společnost RapidShare AG, http://rapidshare.com
[36] http://www.mininova.org/
[37] http://thepiratebay.org/

který daná data přijímá, a nakonec je tu osoba správce či provozovatele databáze torrentů.

Uploader:

Jak jsem uvedl výše, uploader je prvním sdílejícím, který poskytl autorskoprávně chráněný obsah širší veřejnosti, čímž však zasáhl do autorských práv, konkrétně do práva autora díla na sdělování díla[38] veřejnosti ve smyslu ustanovení § 18 odst. 1, 2 autorského zákona. Jedná se o majetková práva autora k dílu, v případě § 18 AZ jde konkrétně o sdělování díla veřejnosti, kterým se dle § 18 odst. 1 AZ rozumí *zpřístupňování díla v nehmotné podobě, živě nebo ze záznamu, po drátě nebo bezdrátově*, odstavec 2 toho samého paragrafu tuto definici pojmu dále rozvíjí a výslovně uvádí, že sdělováním díla je *také 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*. Nemůže být pochyb o tom, že právě odstavec 2 je zaměřen na postih sdělování děl prostřednictvím Internetu. Současně je z dikce ustanovení § 18 odst. 2 autorského zákona jasné, že ke sdělování díla dochází okamžikem, kdy se dílo stane dostupným pro jinou osobu, tedy například nabídkou díla učiněnou vytvořením a umístěním torrentu na některý ze serverů, není nezbytné, aby jiná osoba nabídku přijala.

Důvodem, proč se zdržuji tímto výkladem, je skutečnost, že na toto ustanovení autorského zákona nepřímo odkazuje § 270 TZ, který využívá tzv. blanketní dispozice. Základní skutkovou podstatu trestného činu ve smyslu ustanovení § 270 odst. 1 TZ naplní ten, kdo *neoprávněně zasáhne nikoli nepatrně do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, zvukovému či zvukově obrazovému záznamu, rozhlasovému nebo televiznímu vysílání nebo databázi*. Ustanovení trestního zákoníku tedy samo nestanoví, co jsou zákonem chráněná práva k autorskému dílu a odkazuje na zvláštní zákon upravující práva k autorskému dílu, kterým je právě výše uvedený autorský zákon.

[38] v prostředí kyberprostoru se většinou nesprávně hovoří o tzv. sdílení dat

Ve vymezení skutkové podstaty je ještě jeden stěžejní pojem, a to *nikoli nepatrný zásah*, v tomto případě se jedná nejspíše o odkaz na výkladové ustanovení § 138 odst. 1 TZ, které se vztahuje k výši škody způsobené pachatelem trestného činu. Škodou nikoli nepatrnou se dle tohoto ustanovení rozumí škoda nejméně 5000,- Kč, přičemž v tomto případě bude mít tato škoda charakter ušlého zisku vlastníka autorských práv, do jehož práva bylo pachatelem neoprávněně zasaženo.

Další, i když výslovně v § 270 TZ neuvedenou podmínkou trestnosti jednání je jeho úmyslnost. Úmysl se vyžaduje ve smyslu § 13 odst. 2 TZ vždy, pokud není výslovně uvedeno, že postačuje zavinění z nedbalosti. Vzhledem k tomu, že ustanovení § 270 TZ neuvádí, že by postačovalo zavinění z nedbalosti, je nezbytné úmyslné zavinění. Úmysl pak musí zahrnovat jednání pachatele, nikoli však již porušení zákona. Uploader při odesílání dat, vždy jedná úmyslně.

Trestněprávní odpovědnost uploadera se tak zdá být zcela jasná za předpokladu, že autorskoprávně chráněný obsah stáhne dostatečný počet lidí a bude tak splněna i podmínka vzniku škody, která činí nejméně 5000,- Kč. Takový uploader se dopouští trestného činu porušení autorského práva, práv souvisejících s právem autorským a práv k databázi ve smyslu ustanovení § 270 TZ.

Downloader:

Použití tohoto označení pro osobu stahující data prostřednictvím peer-to-peer sítě se v tomto případě z technického hlediska jeví jako nevhodné, pro přehlednost jsem se však rozhodl zvolit toto označení.

V případě downloadera, tedy osoby stahující autorskoprávně chráněný obsah tak jak jsem si ji vymezil výše, též přichází v úvahu jeho trestněprávní odpovědnost, abychom ji však mohli dovodit, musíme přihlédnout k ustanovení § 2 odst. 3 autorského zákona, zde je uvedeno, že *právo autorské se vztahuje na dílo dokončené, jeho jednotlivé vývojové fáze a části.*

Jak jsem uvedl výše, uživatel, který chce stahovat data prostřednictvím peer-to-peer sítě, se do ní zapojuje a současně stahuje a dále sdílí fragmenty souboru. Samotnému dalšímu sdílení dat pak nemůže uživatel nikterak zabránit, protože současné stahování a další sdílení stažených dat je základní vlastností daného protokolu. Díky tomuto se downloader dostává do téměř identické situace jako výše uvedený uploader s tím rozdílem, že downloader neodesílá celé dílo, ale pouze jeho fragmenty a mnohdy ani nemusí tušit, že nějaká data odesílá. Skutečnost, že odesílá pouhé fragmenty díla, je však irelevantní vzhledem k výše uvedené citaci ustanovení § 2 odst. 3 autorského zákona, protože autorskoprávní ochraně podléhá jak celé dílo, tak i jeho části.
Pokud se jedná o úmyslnost jednání downloadera, i zde platí, že se tento svého jednání dopouští úmyslně, ačkoli jeho úmysl již nezahrnuje další sdílení dat.

I downloader se tak stejně jako výše uvedený uploader dopouští trestného činu porušení autorského práva, práv souvisejících s právem autorským a práv k databázi ve smyslu ustanovení § 270 TZ.

Výše uvedený výklad se však týkal pouze stahování díla z hlediska odesílání dat dále na Internet, je ale nezbytné si právně posoudit i samotné stahování díla z Internetu.

Teoreticky by mohlo připadat v úvahu postižení stahování díla z Internetu dle § 214 TZ jako podílnictví. Abychom však mohli s určitostí říci, zda připadá trestněprávní odpovědnost za stahování díla z Internetu v úvahu, musíme si rozebrat samu skutkovou podstatu podílnictví. Dle § 214 odst. 1 písm. a) TZ se trestného činu podílnictví dopustí ten, kdo *ukryje, na sebe nebo jiného převede nebo užívá věc, nebo jinou majetkovou hodnotu, která byla získána trestným činem spáchaným na území České republiky nebo v cizině jinou osobou, nebo jako odměna za něj*.

Při stahování autorského díla dochází bezesporu k převádění díla na další osobu, i když se technicky vzato jedná o pouhou kopii díla, nikoli o dílo originální.

Vzhledem k tomu, že autorské dílo má povahu záznamu tvůrčí činnosti autora na hmotném nosiči informací, nejedná se o věc, ale o jinou majetkovou hodnotu.
Jak vyplývá z ustanovení § 214 odst. 1 písm. a) TZ je nezbytné, aby sama majetková hodnota byla nejprve získána trestným činem spáchaným osobou odlišnou od pachatele trestného činu podílnictví. Vývoj situace proto musí být následující: První pachatel se dopustí trestného činu (tzv. hlavního trestného činu) díky němuž získá věc nebo jinou majetkovou hodnotu a tuto má po určitý čas v držení, následně ji poskytne jiné osobě, která se v případě, že ji přijme, dopouští trestného činu podílnictví, což potvrzuje i ustálená judikatura Nejvyššího soudu České republiky, který například v roce 2007 judikoval že: *„Pokud má dojít ke spáchání trestného činu podílnictví podle § 251 tr. zák., je nutné, aby se do dispozice podílníka dostala věc, která byla získána tzv. hlavním trestným činem.“*[39]
Odlišný výklad by dle mého názoru navíc porušoval jednu z hlavních zásad trestního práva hmotného, a to zákaz analogie v neprospěch pachatele[40]. Současně by zde docházelo ke kolizi s ustanovením § 30 odst. 1 autorského zákona, které pořizování kopie autorského díla pro osobní potřebu povoluje.

Pro trestněprávní postih stahování autorského díla je proto stěžejním způsob, jakým bylo dílo získáno. Pokud se totiž jedná o samotné stahování díla, jedná se nejčastěji o využití legální licence ve smyslu ustanovení § 30 odst. 1 autorského zákona, přičemž se toto pořízení rozmnoženiny díla nepokládá za užití díla a tudíž ani za zásah do autorského práva.

V souvislosti se sdělováním děl prostřednictvím peer-to-peer sítí jsou tato díla nejčastěji prvotně získávána trojím způsobem:

1) záznamem televizního vysílání
2) okopírováním díla z nosiče informací, zakoupeného v obchodě
3) okopírováním díla v průběhu jeho veřejné projekce (tzv. kinorip)

[39] Usnesení Nejvyššího soudu České republiky sp.zn. 8 Tdo 607/2007, ze dne 31.5.2007
[40] Jelínek, J. a kol. Trestní právo hmotné. 1. vydání. Praha: Leges, 2009, s. 22 an.

4) získáním díla od některého zaměstnance subjektu, který participuje na distribuci díla, či zaměstnance subjektu, kterému je kopie díla poskytnuta za účelem jeho zapsání do evidence

1) V případě záznamu televizního vysílání se jedná o zcela legální formu získání autorského díla v souladu s ustanovením § 30 odst. 1, respektive odst. 2 autorského zákona.

2) V případě zakoupení nosiče s autorským dílem se jedná o uzavření kupní smlouvy, v níž je inkorporována i smlouva licenční, přičemž při následujícím kopírování využívá vlastník pouze svého práva podle § 30 odst. 2 autorského zákona.

   Na tomto místě však pokládám za nutné upozornit na ustanovení § 43 odst. 1 autorského zákona, které by v praxi mohlo činit problémy, protože stanoví, že *do práva autorského neoprávněně zasahuje ten, kdo obchází účinné technické prostředky ochrany práv*. Důvodem proč zde toto ustanovení autorského zákona uvádím je to, že v podstatě veškeré prodávané nosiče s autorskoprávně chráněným obsahem jsou vybaveny hardwarovými, či softwarovými ochrannými prostředky. Toto ustanovení tak v praxi koliduje s ustanovením § 30 odst. 1, 2 autorského zákona, což vyvolává otázku, zda obcházením ochrany, kteréžto je nezbytné, aby si mohl vlastník CD, či DVD vytvořit kopii v souladu s § 30 odst. 1, 2 autorského zákona, náhodou nedochází k porušování ustanovení § 270 TZ. Domnívám se, že nikoli protože klíčové ustanovení § 270 TZ zní: „*zasáhne nikoli nepatrně do zákonem chráněných práv k autorskému dílu“*. Dané ustanovení nezní *„zasáhne nikoli nepatrně do autorského práva“*, pokládám proto za nezbytné vykládat ustanovení § 270 TZ pouze tak, že se vztahuje na práva k samotnému autorskému dílu, tedy na autorova práva majetková. Porušování § 43 odst. 1 autorského zákona je dle ust. § 105a odst. 1 písm. b), tohoto zákona pokládáno v případě fyzických osob za přestupek, v případě osob právnických se dle ust. § 105b odst. 1 písm. b) autorského zákona pokládá takové jednání za jiný správní delikt.

3) Okopírování díla v průběhu veřejné projekce (výroba tzv. kinoripů) probíhá tak, že pachatel pořídí záznam představení v kině na skrytou videokameru a s tímto záznamem dále nakládá. Toto jednání je však již užitím díla ve smyslu ustanovení § 30 odst. 3 autorského zákona přičemž k tomuto užití díla není pořizovatel záznamu zmocněn vlastníkem autorských práv k dílu. Pachatel se tak dopouští zásahu do práv k autorskému dílu ve smyslu § 270 TZ.

4) Jak uvádí V. Jirovský[41], často je ilegální šíření autorskoprávně chráněného obsahu produktem organizované činnosti hned několika osob, z nichž nejméně jedna má v rámci svého povolání přednostní přístup k autorskoprávně chráněnému obsahu. Tato osoba zneužívá svého přístupu k autorským dílům a pořizuje ilegální kopie děl, které následně ve spolupráci s ostatními členy skupiny distribuuje dále. Vzhledem ke skutečnosti, že osoba zneužívající svého přístupu je většinou vázána povinností chránit tato díla, stanovenou ať již zákonem nebo v rámci své pracovní smlouvy, dopouští se svým jednáním porušení povinnosti při správě cizího majetku dle § 220 TZ v jednočinném souběhu s trestným činem porušení autorského práva, práv souvisejících s právem autorským a práv k databázi dle § 270 TZ.[42]

Z výše uvedeného vyplývá, že jako podílnictví ve smyslu § 214 trestního zákoníku by mohlo být posuzováno stahování tzv. kinoripů a dále děl uniknuvších v důsledku porušení povinností při správě cizího majetku, protože tyto kopie autorských děl jsou od prvopočátku produktem trestné činnosti.

Downloader se tedy dopouští porušení autorského práva, práv souvisejících s právem autorským a práv k databázi dle § 270 TZ a v případě že stahuje kopie děl, vzniklé na

[41] více Jirovský, V. Kybernetická kriminalita (nejen o hackingu, crackingu, virech a trojských koních bez tajemství). Praha: Grada, 2007, s. 69

[42] Asi nejznámějším českým případem úniku autorského díla tímto způsobem, byl případ filmu Vratné lahve režiséra Jana Svěráka z roku 2007, kdy dva zaměstnanci Ministerstva kultury pořídili kopii filmu a tento pak nabídli široké veřejnosti ke stažení, trestní stíhání proti nim, bylo nakonec podmínečně zastaveno, zkušební doba činila 18 měsíců, článek uveřejněn dne 23. 7. 2008, online dostupné na http://kultura.ihned.cz/c1-26062070-stihani-piratu-kteri-sirili-film-vratne-lahve-bylo-pozastaveno

základě spáchaného trestného činu, v jednočinném souběhu i trestného činu podílnictví dle § 214 TZ.

Správce, či provozovatel databáze torrentů:
Činnost provozovatele databáze torrentů se skládá v podstatě pouze z uveřejňování odkazů vygenerovaných uploadery, popřípadě z vytvoření automatického systému, který tuto činnost provádí za něj. Jeho stránky jsou tedy jakýmsi místem setkání nabídek uploaderů a poptávek downloaderů, sám se však do této jejich činnosti více nezapojuje.

S ohledem na výše uvedené musím konstatovat, že se provozovatel databáze nedopouští žádné trestné činnosti. Jeho postih dle ustanovení § 270 TZ je totiž vyloučen ustanovením § 18 odst. 3 autorského zákona, které stanoví, že *sdělováním díla veřejnosti není pouhé provozování zařízení umožňujícího, nebo zajišťujícího takové sdělování.* Rovněž nepřipadá v úvahu jeho odpovědnost v podobě účastenství ve formě pomoci ve smyslu ustanovení § 24 odst. 1 písm. c) TZ (bližší výklad níže v rámci výkladu k odpovědnosti poskytovatele služeb datového úložiště).

b) Datová úložiště:

V případě šíření autorskoprávně chráněného obsahu prostřednictvím datových úložišť se situace poněkud liší. V rámci tohoto šíření působí stejně jako u výše uvedeného šíření prostřednictvím peer-to-peer sítí osoba uploadera, která na datové úložiště umisťuje autorské dílo, dále je tu downloader, který autorské dílo ze serveru stahuje, pak je zde provozovatel datového úložiště a nakonec provozovatel diskusního fóra.

Uploader:
Jak už bylo řečeno, uploader je osobou, která umisťuje autorské dílo na servery provozovatelů služeb datového úložiště. Po nahrání dat na příslušný server je uploaderovi automaticky vygenerován odkaz ke stažení těchto dat, který on následně umisťuje na různá diskusní fóra. Tímto svým jednáním, tedy umístěním autorského

díla na server, stejně jako uploader v případě peer-to-peer sítí, sděluje autorské dílo veřejností ve smyslu ustanovení § 18 odst. 1 autorského zákona, čímž zasahuje do práv autora k dílu a tím naplňuje skutkovou podstatu trestného činu porušení autorského práva, práv souvisejících s právem autorským a práv k databázi ve smyslu ustanovení § 270 TZ.

Downloader:

Situace downloadera se v případě stahování díla ze serverů provozovatele služeb datového úložiště podstatně liší od situace downloadera v případě stahování prostřednictvím peer-to-peer sítí, protože v tomto případě downloader pouze autorské dílo stahuje, dále jej však nesděluje.

Díky tomu, platí pro downloadera v případě stahování ze serverů datového uložiště pouze druhá část výše uvedeného výkladu týkajícího se dowloadera v rámci peer-to-peer sítí. Downloader tak nebude trestněprávně odpovědný, protože při stahování díla jedná pouze v rámci legální licence ve smyslu ustanovení § 30 odst. 1 autorského zákona, za předpokladu že nebude stahovat autorské dílo získané spácháním trestného činu, v takovém případě by mohl být postižen pro trestný čin podílnictví ve smyslu ustanovení § 214 TZ.

Provozovatel služeb datového úložiště:

Provozovatel je nepochybně nezbytným článkem celého procesu sdílení autorských děl tímto způsobem. Vzniká proto otázka zda je možné ho trestněprávně postihnout, za to, že právě jím poskytované služby umožňují šíření autorských děl bez souhlasu vlastníků práv k nim.

Teoreticky by mohla připadat v úvahu odpovědnost provozovatele za účastenství ve formě pomoci ve smyslu ustanovení § 24 odst. 1 písm. c) TZ k trestnému činu porušení autorského práva, práv souvisejících s právem autorským a práv k databázi ve smyslu ustanovení § 270 TZ. Není však splněna hlavní podmínka, a to že se musí jednat o úmyslné jednání, jehož cílem je usnadnění páchání trestné činnosti pachateli,

protože provozovatel své služby poskytuje za účelem kompenzace nedokonalostí e-mailové komunikace, tedy se zcela legálním záměrem. Velikost příloh e-mailů je poskytovateli služeb omezená, aby se nezahlcovaly e-mailové schránky uživatelů a tím se zbytečně nezaplňovaly servery poskytovatelů. Vzhledem k tomu, že úmysly provozovatelů nesměřují k napomáhání porušování autorských práv a primárně jsou jimi poskytované služby určené k legálním činnostem, ocitají se v podobné situaci v jaké byla v roce 1984 společnost SONY. V případě japonské společnosti SONY se jednalo o ilegální kopírování autorských děl prostřednictvím videorekordérů, jejichž výrobcem tato společnost byla. Soud v tomto sporu nakonec rozhodl následujícím způsobem: „*výrobce není odpovědný za užívání svého výrobku či služeb protiprávním způsobem, pokud je tento výrobek, či služba primárně určen/a k užívání legálním způsobem*“[43]. V prostředí kontinentálního práva není judikatura soudů pramenem práva, výjimku v případě České republiky tvoří pouze nálezy Ústavního soudu uveřejňované ve Sbírce zákonů, nelze však popřít, že síla tohoto argumentu je velká, pročež se k názoru obsaženému ve výše uvedeném rozhodnutí přiklání velká část odborné veřejnosti zabývající se autorským právem.

Domnívám se však, že by za jistých okolností mohla být dovozena civilněprávní odpovědnost provozovatele a to za předpokladu, že se dozví o skutečnosti, že je na jeho serverech umístěn autorskoprávně chráněný obsah a neučiní nic čím by zabránil vzniku dalších škod. Svým jednáním by mohl porušit obecnou povinnost předcházet škodám ve smyslu § 415 občanského zákoníku. Zajisté si jsou toho vědomi i sami provozovatelé, protože pokud je jim nahlášen neoprávněně umístěný autorskoprávně chráněný obsah na jejich serverech tento obsah bezodkladně odstraňují.

Provozovatel diskusního fóra:

V případě provozovatele diskusního fóra je situace podobná jako u provozovatele databáze torrentů, ani jeho proto nelze postihnout pro porušování ustanovení § 270 TZ, protože provozuje pouze databázi a to není pokládáno za sdělování díla

[43] ***Sony Corp. of America v. Universal City Studios, Inc.***, 464 U.S. 417 (1984), online dostupné na http://lawbrain.com

na základě § 18 odst. 3 autorského zákona, tudíž nedochází k zásahům do práv autora k dílu.

Provozovatelé se však často neomezují na pouhý provoz fóra, na němž jsou umístěny odkazy ke stažení autorských děl, ale hrají v samotném sdílení dat mnohem větší roli[44]. Mnohdy se totiž sami provozovatelé diskusních fór snaží chránit uploadery, kteří na jejich fóra umisťují odkazy ke stažení autorských děl. Nejčastěji má jejich ochrana charakter zatajování identity uploadera, omezování přístupu neprověřených uživatelů k příspěvkům uploadera apod. Jsem toho názoru, že těmito opatřeními však již překračují zákon a dopouští se trestného činu nadržování ve smyslu § 366 TZ. Skutkovou podstatu trestného činu nadržování naplní ten, kdo *pachateli trestného činu pomáhá v úmyslu umožnit mu, aby unikl trestnímu stíhání, trestu nebo ochrannému opatření nebo jejich výkonu.*

Jak jsem uvedl výše, uploader se dopouští trestného činu podle § 270 TZ v okamžiku, kdy sděluje dílo dále, čímž zasahuje do práv autora k dílu. Sdělováním se pak rozumí dle § 18 odst. 2 autorského zákona *také 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*.

V okamžiku uveřejňování odkazů je tedy uploader již pachatelem trestného činu a tím, že mu provozovatel fóra poskytuje ochranu, mu v podstatě umožňuje vyhnout se trestnímu postihu, přičemž i skrývání odkazů ke stažení před neprověřenými uživateli by mohlo být chápáno jako nadržování, protože tyto odkazy mohou být pro orgány činné v trestním řízení velice významným zdrojem informací. V součinnosti s poskytovatelem služeb datového úložiště mohou totiž určit, z jaké IP adresy byla data na server nahrána a dostat se tak na stopu pachatele, nebo alespoň omezit okruh podezřelých.

[44] V případě provozovatelů databáze torrentů jsem se s podobným jednáním nesetkal, proto jsem se touto otázkou v jejich případě nezabýval.

Sdělování programů

Vývoj sdělování programů byl poněkud odlišný od vývoje sdělování audio a audiovizuálních děl. Od prvopočátku byly totiž programy chápány spíše jako příslušenství hardwaru nezbytné pro jeho správnou funkčnost, nikoli jako samostatné autorské dílo svého druhu. Z počátku počítače navíc neumožňovaly snadný přenos dat mezi jednotlivými zařízeními ani velikost harddisků neumožňovala instalaci příliš velkého počtu programů, to se změnilo až se zavedením MC (které však byly brzy nahrazeny 3,5 palcovými disketami) a s pokrokem v oblasti kapacity harddisků.

Přenos programů prostřednictvím disket byl zpočátku relativně snadný, vzhledem k malému rozšíření antivirových programů, které byly jen sporadicky aktualizovány, byl však spojen s velkým rizikem nakažení cílového počítače virem. Postupně se přidala i komplikace v podobě malé kapacity disket a stále rostoucí velikosti programů. Pro přenos programu bylo potřeba stále více disket, což bylo překážkou v jejich ilegálním kopírování. I zde převládalo šíření programů v okruhu přátel a známých.

Zlom přišel stejně jako v případě audio a audiovizuálních děl se zavedením CD a DVD. Kopírování se stalo snazším, stejně jako přenos dat. Díky rozšíření povědomí o základech počítačové bezpečnosti a větší dostupnosti antivirových programů se současně snížilo riziko pro příjemce, že si do počítače zanese virovou nákazu a přijde o svá data. Tohoto si byli vědomi i sami výrobci programů a začali své programy vybavovat různými ochranami proti ilegálnímu kopírování, ovšem stejně jako v případě audio a audiovizuálních děl šlo o boj předem prohraný[45].

Největší rozmach ilegálního kopírování programů přišel stejně jako v případě ostatních autorských děl v souvislosti se zavedením vysokorychlostního internetového připojení. Začaly se totiž ve větší míře šířit nejen samotné programy, ale i informace o tom jak který druh ochrany překonat, přičemž dokonce začaly

[45] Tento výsledek není ani v nejmenším překvapivým, pokud přihlédneme k tomu, že proti jednomu programátorovi, který vytvořil program zabraňující nezákonnému užívání produktu, stojí mnohonásobně více programátorů, kteří se právě tento program snaží překonat.

vznikat specializované vyhledávače, kde si mohl uživatel najít příslušný licenční klíč, nebo program sloužící k překonání ochrany proti kopírování[46]. Metody šíření programů se v podstatě neliší od metod využívaných k šíření ostatních druhů autorských děl.

Trestněprávní posouzení šíření programů

Vzhledem ke skutečnosti, že jsem se podrobně zabýval výkladem odpovědnosti jednotlivých subjektů zapojených do ilegálního šíření autorských děl výše, zde se omezím pouze na srovnání trestněprávní odpovědnosti jednotlivých subjektů pro případ, že je předmětem šíření program.

a) peer-to-peer sítě

Uploader:

Z hlediska uploadera se nic nemění a je trestněprávně odpovědný ze spáchání trestného činu porušení autorského práva, práv souvisejících s právem autorským a práv k databázi dle § 270 TZ.

Downloader:

Pokud se jedná o odpovědnost za odesílání dat při stahování, platí to co ve výše uvedeném případě pro ostatní autorská díla. Downloader se svým jednáním dopouští trestného činu porušení autorského práva, práv souvisejících s právem autorským a práv k databázi dle § 270 TZ.

Komplikovanější však bude situace v případě stahování a následného užívání programů bez uzavřené licenční smlouvy či nad její rámec.

[46] např.: http://www.astalavista.com

Jak jsem uvedl již výše, jsou programy upraveny odlišně od ostatních druhů autorských děl. Nevztahuje se na ně totiž úprava obsažená v § 30 odst. 1 autorského zákona, ale úprava obsažená v § 30 odst. 3 autorského zákona. Díky tomu je i užívání programu k nekomerčním účelům pokládáno za užívání ve smyslu autorského zákona a je nezbytné, aby k jeho užití byl uživatel oprávněn licenční smlouvou. Požadavek na existenci oprávnění k užití díla se pak samozřejmě promítá i do trestněprávní odpovědnosti osob, které participují na neoprávněném sdělování autorských děl prostřednictvím kyberprostoru.

Trestněprávní postih tedy nenastupuje přímo ve vztahu ke stažení díla, ale až ve vztahu k jeho užívání kdy užívání díla bez toho, aby k danému způsobu užívání byl downloader zmocněn licenční smlouvou je zásahem do práv autora k dílu a naplňuje tak skutkovou podstatu § 270 TZ. Na druhou stranu, pokud by downloader měl uzavřenu licenční smlouvu, byl by trestněprávně odpovědný pouze za uploadování dat, taková situace je dle mého názoru ovšem pouze hypotetická, protože takový uživatel by si vyžádal kopii programu přímo od distributora, který by mu ji v naprosté většině případů sám ochotně poskytl.

V případě stahování díla prostřednictvím torrentů se tak downloader nejčastěji dopouští vícečinného souběhu stejnorodého, kdy nejprve naplňuje skutkovou podstatu trestného činu dle § 270 TZ uploadováním dat v průběhu stahování a následně naplňuje skutkovou podstatu trestného činu dle § 270 TZ užíváním díla bez potřebného oprávnění uděleného licenční smlouvou.

Správce, či provozovatel databáze torrentů:

Stejně jako v případě ostatních druhů děl, ani v tomto případě provozovatel nenese trestněprávní odpovědnost.

b) Datová úložiště:

Uploader:

Odpovědnost uploadera je stejná jako v případě uploadování ostatních autorských děl, tedy je odpovědný ze spáchání trestného činu porušení autorského práva, práv souvisejících s právem autorským a práv k databázi dle § 270 TZ.

Downloader:

U downloadera platí opět pouze část výkladu týkající se stahování a následného užívání programů bez licenční smlouvy či nad její rámec, protože downloader při stahování díla zákon neporušuje, ovšem při jeho neoprávněném užívání již ano.

Provozovatel služeb datového úložiště a provozovatel diskusního fóra:

Jejich trestněprávní odpovědnost se nikterak neliší od situace, kdy se jedná o ostatní autorská díla (viz str. 41 an. této diplomové práce).

Pro úplnost je třeba ještě uvést, že osoby které uveřejňují sériová čísla nebo licenční klíče či vyvíjejí programy překonávající ochrany které mají zabránit ilegálnímu sdělování autorských děl, se nedopouštějí žádného trestného činu a není možné dovodit ani jejich odpovědnost co by účastníků ve formě návodu či pomoci dle § 24 TZ, protože samo překonávání ochrany není trestným činem, ale pouhým přestupkem, či jiným správním deliktem.[47]

[47] více viz. výklad týkající se peer-to-peer sítí, konkrétně downloadera a vytváření záložní kopie díla

Šíření pornografie

Pornografická díla jsou díly, která však díky své specifické povaze musí být více regulována právním řádem, a to nejen z hlediska ochrany práv autora v případech kdy dílo splňuje podmínky stanovené autorským zákonem a tudíž se tedy jedná o autorské dílo, ale též z hlediska tvorby a následné distribuce těchto děl mezi širokou veřejnost.

Již v úvodu do této kapitoly jsem lehce nastínil, že ne všechna pornografická díla jsou díly autorskými, nyní tedy vysvětlím, proč jsem tak učinil. Nemůže být sporu o tom, že komerční pornografická díla vydávaná různými produkčními společnostmi splňují podmínky, že dílo je *jedinečným výsledkem tvůrčí činnosti autora* a je *objektivně vnímatelné*, stanovené v § 2 odst. 1 autorského zákona. Zaznamenané situace jsou totiž pečlivě naaranžované, dialogy jsou předem připravené a taková díla se tedy liší od běžných druhů fotografií otištěných v časopisech, či filmových snímků promítaných v běžných kinech pouze množstvím sexuálně dráždivých výjevů. Na druhou stranu existují pornografická díla, která postrádají prvky nezbytné pro to, aby mohla být označována za díla autorská. Narážím především na dnes tolik populární nahrávání sebe sama při pohlavním styku s jinou osobou, které je bezesporu objektivně vnímatelné, v naprosté většině případů se však bude jednat o dílo, které nebude výsledkem tvůrčí činnosti autora ve smyslu autorského zákona.[48]

Dalším problémem je sama definice pornografického díla. Český právní řád nestanoví, co je pornografickým dílem a pouze uvádí formy, ve kterých se může vyskytovat. Definování pornografického díla tak bylo ponecháno právní praxi a právní vědě. Autoři učebnice trestního práva hmotného[49] se přiklání k definici uvedené v § 132 slovenského trestního zákona[50], kde je pornografické dílo charakterizované tak, že *zvláště intenzívním a vtíravým způsobem zasahuje a podněcuje sexuální pud, překračuje podle převládajících názorů ve společnosti*

[48] Touto otázkou se zabýval i Nejvyšší soud České republiky v roce 2003, v rámci usnesení č. 5 Tdo 631/2003, ze dne 18.06.2003
[49] Jelínek, J. a kol. Trestní právo hmotné. 1. vydání. Praha: Leges, 2009
[50] zákon č. 300/2005 Z.z.

uznávané hranice, sexuální slušnosti, uráží neakceptovatelným způsobem cit pro sexuální slušnost, vyvolává pocit studu[51]. Z uvedené definice nepřímo vyplývá, že je třeba jistá míra vůle na straně tvůrce takového díla, aby dílo podobným způsobem působilo.

Samo vyobrazení nahého lidského těla proto není trestné, i kdyby pohled na toto vyobrazení jednotlivce vzrušoval sebevíc (např.: akty, nebo antické sochy), důležitý je záměr tvůrce, tedy jak chce, aby jeho výtvor působil.

Existuje mnoho druhů pornografie, některé jsou ze společenského hlediska přijatelné, jiné nikoli. Nepřijatelné druhy pornografie jsou pak postaveny mimo zákon a stejně tak i jednání spočívající v zpřístupňování tohoto obsahu. I v případě legálních forem pornografie se však subjekt může dopustit trestného jednání, pokud zpřístupní pornografické dílo dítěti.

Český trestní zákoník obsahuje tři skutkové podstaty trestných činů, které souvisí právě s pornografií. Je to jednak výroba a nakládání s tvrdou pornografií dle § 191 odst. 1 TZ, dále zpřístupňování pornografie dítěti dle § 191 odst. 2 TZ a nakonec výroba a jiné nakládání s dětskou pornografií § 192 TZ. K výrobě a distribuci pornografie se ještě váže § 193 TZ, který upravuje trestný čin zneužití dítěte k výrobě pornografie.

Trestní zákoník rozeznává následující skupiny pornografických děl:

a) písemná
b) fotografická
c) filmová
d) počítačová
e) elektronická

[51] Novotný, O., Vokoun, R. a kol. Trestní právo hmotné – II. Zvláštní část. Praha : ASPI, 2007, s. 275

Stanovený výčet má však povahu demonstrativní, proto může být postiženo jednání spočívající v nakládání s pornografickým dílem i jiným, než výše uvedeným způsobem.

Rozeberme si tedy jednotlivé skutkové podstaty v pořadí, v jakém jsou uvedeny v trestním zákoníku.

Výroba a nakládání s tvrdou pornografií (§ 191 odst. 1 TZ)

Tvrdou pornografií je myšlen druh pornografie, který je i v oblasti pornografických děl extrémním. Trestní zákoník rozlišuje dvě skupiny takových děl:

a) v nichž se projevuje násilí či neúcta k člověku
b) v nichž se popisuje, zobrazuje nebo jinak znázorňuje pohlavní styk se zvířetem

a) Jak jsem uvedl výše, tento druh pornografických děl je extrémním i v rámci pornografické tvorby. V rámci děl (nejčastěji audiovizuálních) dochází nejčastěji k ponižování, týrání, nezřídka i k usmrcení herců, vše je přitom pácháno v souvislosti se sexuálním chováním. Tato videa následně slouží k sebeukájení deviantních jedinců.

b) Zvíře je v tomto případě objektem pohlavního pudu (zoofilie), nebo je stylizováno do role sexuálního partnera (sodomie). Ke spáchání trestného činu může dojít jednak *popisem pohlavního styku se zvířetem*, tedy jakýmkoli literárním dílem, ale i třeba zvukovou nahrávkou apod., a dále *zobrazením nebo jiným znázorněním pohlavního styku se zvířetem*, čímž jsou míněna nejen audiovizuální díla a díla fotografická, ale též různá jiná znázornění jako například v rámci namalovaného obrazu apod.

U těchto děl jsou postihovány *výroba, dovoz, vývoz, průvoz, nabízení, činění veřejně přístupným, zprostředkovávání, uvádění do oběhu, prodej nebo jiné opatření takových děl*.

Výrobou se rozumí nejen průmyslová nebo řemeslná výroba, ale jakékoliv zhotovení zvrácené ponografie[52]. *Dovozem, vývozem a průvozem* pak transport takových děl umístěných na hmotném nosiči informací (VHS kazeta, CD, DVD, harddisk apod.). Z výše uvedeného je jasné, že pokud se takové dílo nachází na hmotném nosiči informací a ten fyzicky překročí hranice státu, jedná se podle místa určení o dovoz, vývoz, případně průvoz, otázkou však zůstává, jak to bude v případě, že pachatel využije kyberprostoru jako nástroje k přenosu dat. I pachatelé této trestné činnosti se totiž v souvislosti se zavedením vysokorychlostního internetového připojení, přesunuli do kyberprostoru.

Z hlediska odpovědnosti majitele serveru na němž může být takové dílo umístěno, odkazuji na výklad týkající se odpovědnosti majitelů serverů, na nichž je umístěn autorskoprávně chráněný obsah.

Jsem toho názoru, že o průvoz, vývoz, či dovoz se v případě šíření děl počítačovou sítí jednat nebude, protože pokud cestují data mezi počítači prostřednictvím Internetu, mohou cestovat přes několik desítek států, i když se počítače nachází jen několik stovek metrů od sebe (v rámci jediného státu) a toto chování nemůže ani jeden z uživatelů ovlivnit, nehledě na to, že lze jen velice obtížně určit okamžik spáchání, tedy okamžik kdy data překročila hranice státu a současně nesmíme zapomínat na to, že kyberprostor nezná hranic. Museli bychom si tedy velice obtížně dovozovat hranice a tento krok by již porušoval zásadu *nullum crimen sine lege stricta*[53].

Nabízení se dá definovat jako jakékoli předložení díla jehož cílem je dosáhnout převzetí jinou osobou. *Činění veřejně přístupným* by se dalo definovat jako umístění díla na místě veřejně přístupném, v případě Internetu například umístěním na webové stránky. *Zprostředkovávání* je všeobecně chápáno jako poskytnutí příležitosti k nějakému úkonu[54], v tomto případě se bude nejspíše jednat o umožnění seznámení

[52] Jelínek, J. a kol. Trestní právo hmotné. 1. vydání. Praha: Leges, 2009, s. 557
[53] zákaz analogie v neprospěch pachatele
[54] zprostředkování definuje například obchodní zákoník v § 642 an.

se, či pořízení takového díla. *Uvádění do oběhu* znamená, že pachatel se snaží nejčastěji o prodej díla širšímu okruhu osob.

Zpřístupňování pornografie dítěti (§191 odst. 2 TZ)

Od výše uvedeného jednání spočívajícího ve výrobě a nakládání s ilegálním druhem pornografie se tato skutková podstata liší především tím, že pornografie takto sdělovaná je nejčastěji zcela legální. Jednání se stává ilegálním v důsledku nakládání s tímto obsahem zakázaným způsobem.

K naplnění této skutkové podstaty může dojít dvojím způsobem:

a) nabízením, přenecháváním nebo zpřístupněním dítěti
b) vystavováním nebo jiným zpřístupňováním na místě, které je dětem přístupné

Stěžejním je zde pojem dítěte ve smyslu trestního zákoníku, kterým se dle § 126 TZ rozumí osoba mladší **18 let**, přičemž v této oblasti panuje shoda v pojetí dítěte s Úmluvou o právech dítěte[55].

a) *Přenecháním* je myšleno jakékoli jednání, kdy je dílo předáno do sféry působnosti dítěte, tedy nevztahuje se pouze na nabízení za úplatu jako ve výše uvedeném případě nakládání s tvrdou pornografií, ale postih je mnohem širší.

   Termín *zpřístupnění* je opět zvolen pro širší postih jednání, než ve výše uvedeném případě nakládání s tvrdou pornografií. Bude se tedy jednat jak o veřejné zpřístupňování, tak i jakékoli další zpřístupnění, například doma, nebo kdekoli jinde. Pokud se jedná o *nabízení*, to jsem definoval již u první skutkové podstaty uvedené výše, proto si dovolím odkázat na tuto definici.

b) *Vystavování* je v podstatě formou seznamování s dílem širokou veřejností. Místem, které je dětem přístupné je myšleno prostředí kde se obvykle děti zdržují, nebo je navštěvují. Přímo učebnicovým příkladem jednání, které by

[55] zákon č. 104/1991 Sb.

naplňovalo tuto skutkovou podstatu v oblasti kyberprostoru, by bylo umístění pornografických děl na stránky určené pro děti, jako jsou stránky Alík.cz[56], což se již v minulosti stalo.

Výroba a jiné nakládání s dětskou pornografií (§ 192 TZ)

Co je dětskou pornografií, není v trestním zákoníku stanoveno, musí tedy opět vypomoci právní praxe, právní věda a autoři jednotlivých publikací věnovaných této problematice.

J. Dunovský vymezuje dětskou pornografii jako *jakékoli zobrazování dítěte, účastnícího se skutečné nebo předstírané explicitní sexuální aktivity, ať již je to jeho zpodobení, provedené jakýmkoli způsobem*[57].

Poněkud odlišně je dětská pornografie definována v rámci Rámcového rozhodnutí Rady EU, jako *pornografický materiál, který zobrazuje skutečné dítě, které se aktivně, nebo pasivně účastní jednoznačně sexuálního jednání, a to včetně dráždivého vystavování přirození nebo ohanbí dítěte, nebo skutečnou osobou se vzhledem dítěte, účastnící se výše uvedeného jednání, či realistické znázornění neexistujícího dítěte, účastnícího se výše uvedeného jednání.*[58]

Na základě historického vývoje právní úpravy postihu dětské pornografie a analogie s výše uvedenou definicí pornografie[59] můžeme říci, že dětská pornografie ve smyslu trestního zákoníku je jedním z druhů tvrdé pornografie, někdy též označované jako pornografie deviantní. V rámci této pornografie je dítě stylizováno do pozice sexuálního objektu, případně sexuálního partnera. Kromě tzv. „běžné“ dětské pornografie, existuje ještě tzv. virtuální dětská pornografie, o níž pojednám níže.

[56] http://alik.idnes.cz/
[57] Dunovský, J., Mitlöhner, M., Hejč, K., Hanušová-Tlačilová, J. Problematika dětských práv a komerčního sexuálního zneužívání u nás a ve světě, Praha: Grada, 2005, s. 23
[58] Rámcové rozhodnutí Rady č. 2004/68/SVV ze dne 22.12.2003
[59] myšlena je definice z § 132 slovenského trestního zákona č. 300/2005 Z.z.

Objektem trestného činu je, jak uvádí F. Ščerba, autor kapitoly v učebnici trestního práva hmotného[60], *zájem na ochraně některých morálních hodnot spočívajících v odsuzování dětské pornografie, sekundárním objektem je ochrana dětí před jejich zneužíváním pro pornografické účely.*

K naplnění skutkové podstaty trestného činu může dojít trojím způsobem:

a) přechováváním dětské pornografie
b) výrobou a nakládáním s dětskou pornografií
c) kořistěním z takového pornografického díla

a) Přechovávání dětské pornografie je trestným činem dle § 192 odst. 1 TZ. Smyslem této úpravy je snaha zcela vymýtit dětskou pornografii tím, že se kriminalizuje nejen výroba a nakládání s tímto druhem pornografie jako je tomu u jiných druhů tvrdé pornografie, ale též tím že se postihuje i samotné držení čímž se zákonodárce snaží docílit eliminace poptávky po tomto druhu pornografie. Na základě základních zákonů trhu se pak očekává i úplné eliminace nabídky a samotné tvorby této pornografie.

   Přechováváním se rozumí *jakýkoli způsob držení dětské pornografie. Pachatel ji nemusí mít přímo u sebe, ale postačí, že ji má ve své moci. Není při tom rozhodné, zda pachatel takové dílo přechovává pro sebe, či pro jinou osobu, nezáleží ani na délce přechovávání.*[61] Držením tak bude i případ kdy je dětská pornografie fakticky umístěna na serverech poskytovatele e-mailových služeb, které se nachází v jiném státě. Důležité je, že k ní má pachatel přístup kdykoli o to projeví zájem.

   Aby mohl být držitel dětské pornografie trestně odpovědný za držení této pornografie, je v souladu s ustanovením § 13 odst. 2 TZ třeba úmyslného zavinění, protože ustanovení § 192 TZ výslovně neuvádí, že postačuje nedbalost. Proto pokud bude pachatel držet dětskou pornografii, ovšem bude

[60] Jelínek, J. a kol. Trestní právo hmotné. 1. Vydání. Praha: Leges, 2009, s. 559
[61] Jelínek, J. a kol. Trestní právo hmotné. 1. Vydání. Praha: Leges, 2009, s. 560

> žít v přesvědčení, že se o dětskou pornografii nejedná, což bude i z objektivního hlediska naprosto oprávněný předpoklad vzhledem k pohlavní vyspělosti účinkujících a jejich vystupování (za předpokladu že nebude jinak seznámen s věkem účinkujících), nebude trestně odpovědný pro držení dětské pornografie[62].

V této souvislosti je třeba se zmínit o tzv. virtuální dětské pornografii. Rámcové rozhodnutí Rady EU v rámci definice dětské pornografie zmiňuje taktéž virtuální dětskou pornografii, tedy dětskou pornografii, která znázorňuje postavu dítěte, které však reálně neexistuje a tudíž tato pornografie nevznikla v důsledku zneužívání dětí.

Virtuální dětská pornografie

Při stanovování trestnosti výroby a jiného nakládání s dětskou pornografií, je v tomto ohledu trestní zákoník dosti neurčitý, trestnost výroby a přechovávání této sub-kategorie dětské pornografie, je tak otázkou pro trestněprávní vědu.

Komentář k trestnímu zákoníku[63] se přiklání k názoru J. Herczega, uveřejněnému v jeho pojednání, věnujícímu se této problematice. Autor pojednání zastává názor, že virtuální dětská pornografie není v důsledku vypuštění dítěte ze samotné tvorby této pornografie natolik škodlivá, aby tento druh pornografie musel být kriminalizován, a že by virtuální dětská pornografie mohla sloužit pedofilním jedincům coby náhražka sloužící k jejich uspokojení prostřednictvím masturbačních fantazií čímž by se snížilo riziko jejich snah o následnou realizaci těchto fantazií[64].

Tento pohled na danou problematiku je v zásadě možný, osobně však zastávám názor opačný. Pokládám totiž virtuální dětskou pornografii za téměř stejně nebezpečnou a nepřípustnou jako „běžnou“ dětskou pornografii, pročež zastávám názor, že by měla

[62] bude se jednat o negativní skutkový omyl
[63] Šámal, P.a kol., Trestní zákoník II. § 140 až 421. Komentář. 1. vydání. Praha: C.H.Beck, 2010, s. 1704 a násl.
[64] blíže Herczeg, J., Virtuální dětská pornografie: Zločin bez oběti? In: Vanduchová, V., Gřivna, T., Pocta Otovi Novotnému k 80. Narozeninám, Praha : ASPI, Wolters Kluwer, 2008, s. 42

být její výroba, nakládání i její držení stejně trestné, jako „běžná“ dětská pornografie. Pro tento svůj postoj mám hned několik důvodů.

V první řadě je to samotný objekt trestného činu, tak jak je vykládán právní teorií. Jak je uvedeno výše, objektem trestného činu je kromě snahy chránit děti před zneužíváním k výrobě tohoto druhu pornografie i zájem na zachování morálních hodnot společnosti. Vypuštění dítěte ze samotné tvorby pornografického díla je jednoznačně pozitivní skutečností, která hovoří ve prospěch virtuální dětské pornografie coby alternativy pro pedofilní jedince i tak ale stejně není vyloučeno porušování morálních hodnot společnosti ke kterému i nadále dochází.

Dalším argumentem pro trestnost této pornografie je skutečnost, jak pedofilní jedinci vnímají sebe sama. Je všeobecně známou skutečností, že pedofilní jedinci sebe sama vnímají jako jedince s odlišnou sexuální orientací, přičemž na svém sexuálním zaměření na nedospělé osoby neshledávají nic deviantního. Sami se pak nejčastěji srovnávají s homosexuálně orientovanými osobami a do budoucna očekávají, že se jim ze strany společnosti dostane stejné míry tolerance a pochopení jako homosexuálně orientovaným jedincům.

Toleranci společnosti k virtuální dětské pornografii, by proto mohli pedofilní jedinci vnímat jako jistou formu nevyřčeného souhlasu společnosti s jejich deviantním chováním a příchodu toužebně očekávaného pochopení ze strany společnosti. To by mohlo vést i k přechodnému nárůstu počtu zneužívaných dětí, než by bylo opět ze strany společnosti jasně deklarováno, že jejich závěry týkající se tolerování zneužívání dětí jsou mylné a sexuální zneužívání dětí je i nadále nepřípustné. Pochopitelně se mohu mýlit a taková situace vůbec nemusí nastat, osobně bych si však nepřál zjistit, že jsem se nemýlil. K závěru, že taková situace může nastat a s největší pravděpodobností by nastala mě přivedla argumentace, kterou ospravedlňují sexuální turisté pohlavní styk s dětmi z chudších zemí[65], ti totiž omlouvají své chování tím, že sexuální styk s dětmi je v dané kultuře přijatelnější.

[65] Dunovský, J., Mitlöhner, M., Hejč, K., Hanušová-Tlačilová, J. Problematika dětských práv a komerčního sexuálního zneužívání u nás a ve světě. Praha: Grada, 2005, s. 140

Současně je zde i jistá míra rizika, že sexuální styk s dětmi by mohli začít vyhledávat nejen osoby pedofilní, ale i jedinci, kteří rádi experimentují v sexuální oblasti.

Dalším argumentem pro trestnost virtuální dětské pornografie je pak i faktická nevymahatelnost některých ustanovení trestního zákoníku v důsledku pokroku v oblasti počítačové grafiky. Obecným cílem úpravy právních vztahů prostřednictvím zákona je vytvoření úpravy, která by odpovídala měnící se společnosti a byla neustále aktuální a nevyžadovala příliš mnoho zásahů ze strany zákonodárce. Obzvláště se na tuto vlastnost zákona klade důraz právě v oblasti trestního práva (právní jistota). Oblast výpočetní techniky a počítačové grafiky v posledních několika letech prodělala značný pokrok, díky čemuž působí zejména počítačové hry mnohem realističtěji, než dříve. Již dnes je tak dosti nesnadné rozeznat zda se jedná o počítačovou grafiku, či nikoli. Vývoj v této oblasti však nestagnuje a dále pokračuje. Pokud bychom přistoupili na legálnost virtuální dětské pornografie, zajisté by se našla nejedna společnost snažící se o uspokojení poptávky nově vzniklého trhu. Ze strany zákazníků by byly pochopitelně kladeny nároky na pokud možno co největší realističnost obsahu, což by vedlo k tomu, že by se brzy nemuselo téměř dát rozeznat (v horizontu několika let), zda se jedná o pornografické dílo virtuální nebo reálné. S ohledem na skutečnost, že pro naplnění skutkové podstaty přechovávání dětské pornografie se vyžaduje úmysl, stačilo by pachateli pouze tvrdit, že se domníval, že se jedná o virtuální dětskou pornografii, nikoli o pornografii zobrazující reálné dítě. Tím by se ustanovení § 192 odst. 1 TZ stalo prakticky nevymahatelným a záměr zákonodárce zcela vymýtit dětskou pornografii by byl zmařen.

A konečně posledním argumentem pro trestnost virtuální dětské pornografie je skutečnost, že by tato pornografie mohla pedofilního jedince vydráždit a místo toho, aby pro něj byla legální alternativou, mohla by ho naopak motivovat ke spáchání trestného činu pohlavního zneužití ve smyslu § 187 TZ v rámci jeho snahy realizovat svou sexuální představu.

Nejspíše si tato rizika uvědomil i zákonodárce a v zájmu právní jistoty a zamezení diskuzí kolem legálnosti virtuální dětské pornografie se rozhodl příslušné ustanovení § 192 odst. 1 TZ novelizovat v souladu s výše uvedeným Rámcovým rozhodnutím Rady č. 2004/68/SVV a přidat do vymezení skutkové podstaty slova *skutečnou osobu se vzhledem dítěte, či realistické znázornění neexistujícího dítěte* a tím jasně stanovit, že se nepřipouští ani držení jakýchkoli pornografických děl, která by mohla sloužit jako alternativní pro pedofilní jedince. Tato novela Trestního zákoníku v současnosti prochází legislativním procesem, je však otázkou zda bude nakonec přijata a stane se součástí našeho právního řádu, nebo bude zamítnuta.

b) Rozsah jednání, která jsou postihována v rámci výroby a nakládání s dětskou pornografií se nikterak neliší od výroby a nakládání s tvrdou pornografií. Pokud se jedná o výklad jednotlivých pojmů užitých při vymezení skutkové podstaty, dovolím si odkázat na výklad těchto pojmů v rámci výkladu k § 191 odst. 1 TZ.

c) *Kořistěním* z takového pornografického díla se rozumí *jakékoli způsoby získávání majetkového prospěchu z pornografického díla, ve kterém se zobrazuje, nebo jinak využívá dítě.*[66]

Za zmínku stojí, že okolností pro použití vyšší trestní sazby je skutečnost, že se pachatel dopouští jednání uvedeného pod písm. b), prostřednictvím veřejné počítačové sítě (Internetu).

Zneužití dítěte k výrobě pornografie (§ 193 TZ)

Objektem trestného činu *je mravní rozvoj a mravní výchova dětí, resp. zájem na zdravém vývoji dětí v oblasti sexuality a zájem na ochraně před zneužíváním dětí k výrobě dětské pornografie.*[67]

[66] Jelínek, J. a kol. Trestní právo hmotné. 1. vydání. Praha: Leges, 2009, s. 560
[67] Jelínek, J. a kol. Trestní právo hmotné. 1. vydání. Praha: Leges, 2009, s. 561

K naplnění skutkové podstaty může dojít dvojím způsobem:

a) pachatel přiměje, zjedná, najme, zláká, svede nebo zneužije dítě k výrobě pornografického díla nebo
b) kořistí z účasti dítěte na takovém pornografickém díle

Jak vyplývá z vymezení skutkové podstaty v TZ, může být pachatelem kdokoli, tedy nejen osoba která má odpovědnost za dítě.

Pokud se jedná o vymezení pojmů uvedených pod písmenem a), odkazuji na jejich vymezení výše. Nejčastějšími způsoby jakými pachatel bude působit na dítě, aby se sexuálně explicitního jednání účastnilo, budou přinucení, manipulace, nebo jiný způsob přesvědčení k účasti na výrobě pornografického díla.

Opět se jedná o úmyslný trestný čin s tím, že pachatel musí být se skutečností, že se jedná o dítě seznámen.

Kořistění z účasti dítěte na tvorbě dětské pornografie je získávání protihodnoty, coby úplaty za poskytnutí dítěte k účasti na tvorbě této pornografie. V tomto případě se tak nebude jednat o kořistění ve smyslu ust. § 192 TZ.

Ostatní trestná činnost páchaná v kyberprostoru

Do této sběrné kategorie jsem zařadil některá jednání, k nimž dochází v kyberprostoru, nebylo možné je zařadit do některé z výše uvedených kategorií a jejich charakteristickou vlastností je, že k jejich páchání není kyberprostor nezbytně nutný, avšak je k jejich páchání hojně využíván. Současně se nedají tato jednání jinak skupinově označit, protože jsou velice různorodá a kromě skutečnosti, že k nim může prostřednictvím kyberprostoru docházet, je nic jiného nespojuje.

Carding

Carding, neboli kopírování platebních karet, je jedním z trestných činů, které spadají do kategorie trestných činů počítačových, tedy pro jeho spáchání není nezbytná počítačová síť, ovšem bez počítače jej nelze spáchat. K páchání této trestné činnosti dochází nejčastěji dvojím způsobem.

Prvním způsobem je veřejně známé kopírování platebních karet prostřednictvím zařízení připevněných na bankomatech jednotlivých poskytovatelů bankovních služeb. Aby pachatel uspěl, musí se mu podařit získat jak údaje umístěné na platební kartě tak i tzv. PIN kód, který je známý pouze oprávněnému držiteli platební karty. K tomuto dochází následujícím způsobem, na bankomat je umístěno tzv. skimmovací zařízení, které je schopné kopírovat data na platebních kartách[68] a současně je zde umístěna i kamera, či folie pro zaznamenávání PIN kódů. Po následném odstranění zařízení z bankomatu jsou získaná data stažena z paměti zařízení a okamžitě odeslána prostřednictvím Internetu dalším členům skupiny, kteří operují v zahraničí, kde tito pomocí získaných dat vytvoří kopie platebních karet a ty následně použijí k získání finančních prostředků z účtů obětí.

[68] Skimmovací zařízení čte data umístěná na magnetickém proužku platební karty. Tomuto mělo zabránit zavedení čipových karet, kvůli zpětné kompatibilitě však zůstal zachován i magnetický proužek.

Jedná se o druh kriminality, která je většinou doménou organizovaných skupin především původem z Rumunska a Bulharska.

Na přelomu roku 2009 a 2010 však média přišla se zprávou, že ke kopírování platebních karet může dojít i při placení platební kartou pomocí bezdrátového terminálu.[69] Jak v článku uvádí R. Smolík, odborník na bezpečnost platebních karet, *ve světě je tento způsob kopírování karet znám jako wardriving, protože signál zasílaný z bezdrátového terminálu, je odposlouchávána nejčastěji z automobilu na parkovišti nedaleko provozovny, v níž je placeno*.

Trestněprávní posouzení

Carding se postihuje dle ustanovení § 234 TZ jako neoprávněné opatření, padělání a pozměnění platebního prostředku. Tohoto trestného činu se dopustí každý, *kdo sobě, nebo jinému bez souhlasu oprávněného držitele opatří, zpřístupní, přijme nebo přechovává platební prostředek jiného*. Následně jsou demonstrativně uvedeny jednotlivé platební prostředky, mezi kterými je výslovně uvedena nepřenosná platební karta. Jedná se však pouze o výčet demonstrativní, tedy nejde o konečný výčet, díky čemuž zůstává otevřená cesta pro ochranu jiného platebního prostředku, který by se v budoucnu mohl objevit.

Podmínky pro použití vyšší trestní sazby jsou výše škody a spáchání trestného činu jako člen organizované skupiny. Trestní zákoník rozeznává dvojí typ organizovanosti, organizovanou skupinu, což je „*sdružení více osob, v němž je provedeno určité rozdělení úloh mezi jednotlivé členy a jeho činnost se v důsledku toho projevuje určitou plánovitostí a koordinovaností, kterou se spáchání činu usnadňuje a zvyšuje se pravděpodobnost dosažení sledovaného cíle*“[70] a dále organizovanou zločineckou skupinu, jejíž definici můžeme nalézt ve výkladových ustanoveních trestního zákoníku v § 129 TZ. Organizovaná zločinecká skupina je vyšším stupněm organizované skupiny. Dle definice se jedná o *společenství více*

[69] http://www.zlatakoruna.info/clanky/39-10-platebni-karty/20859-novy-zpusob-kopirovani-dat-z-platebnich-karet
[70] usnesení Nejvyššího soudu ČR, sp.zn. 11 Tdo 113/2008, ze dne 17.4.2008

osob (opět nejméně tří osob) s vnitřní organizační strukturou, s rozdělením funkcí a dělbou činností, která je zaměřena na soustavné páchání úmyslné trestné činnosti. Organizovanou skupinu u kvalifikovaných skutkových podstat v rámci § 234 trestního zákoníku musíme proto vykládat dle výkladového pravidla a minori ad maius, tedy od menšího k většímu, že jde o organizovanou zločineckou skupinu, zde bude působit jako přitěžující okolnost. Příprava tohoto trestného činu je trestná, pochopitelně za předpokladu, že povede ke spáchání zvlášť závažného zločinu.

Nebezpečné pronásledování

Nebezpečné pronásledování je novým trestným činem, zavedeným do české právní úpravy trestním zákoníkem. Vzhledem ke skutečnosti, že se jedná o nový trestný čin, rozhodl jsem se zabývat se jím poněkud hlouběji.

Skutková podstata trestného činu nebezpečného pronásledování je ve světě známá pod pojmem stalking, Jedná se o anglický termín znamenající v překladu doslova *stopování* nebo *pronásledování*, kdy právě toto slovo nejlépe vystihuje chování pachatelů (nadále budu používat termíny „**stalking“** a „**nebezpečné pronásledování**“ jako synonyma).

Poprvé bylo toto chování zaznamenáno v souvislosti s pronásledováním mediálně známých osobností v USA (především v souvislosti s masovým rozšířením televize), jejich fanoušky. První použití termínu stalking v souvislosti s níže uvedeným jednáním je pak zaznamenáno až v 90. letech minulého století, kdy byl tento termín použit v rámci výzkumu psychopatologických projevů chování.[71]

Pachatel stalkingu se snaží vyhledávat osobu, na kterou se zaměřil, kontaktovat ji, být jí na blízku, nezřídka se však uchýlí i k výhrůžkám a napadání oběti. Z výše uvedeného by se mohlo zdát, že jde o formu náklonnosti, která již překročila

[71] Válková, H. Česká podoba stalkingu podle § 354 TrZ v širších než jen v trestněprávních souvislostech. Trestněprávní revue č. 9/2009, s. 257 an.

rozumnou míru, stalking je však spíše forma patologické posedlosti jedné osoby jinou.

V zásadě přicházejí v úvahu dva hlavní modely chování, kdy v prvním případě žije pachatel v chorobných představách, že má vztah s veřejně známou osobností a tuto osobnost pak pronásleduje, nebo pachatel s jinou osobou vztah měl, či má a cílem snažení pachatele je absolutní ovládání oběti. Teoreticky ale připadá v úvahu i třetí model, který je jistou modifikací druhého výše uvedeného modelu chování, kdy se pachatel snaží navázat s obětí vztah, je odmítnut a jeho cílem je znepříjemňování života oběti a její přinucení k navázání vztahu s ním, často právě prostřednictvím vydírání, či výhrůžek.

Nebezpečné pronásledování (§ 354 TZ)

Důvodem proč se přistoupilo k trestněprávnímu postihu tohoto chování je především skutečnost, že dané jednání je nejen společensky nežádoucí, ale též to, že se podepisuje na psychice oběti, omezuje ji v běžném životě a vyvolává u ní často paranoiu. Jinými slovy pachatelem je ohrožována především psychická integrita oběti, přičemž fyzické napadení oběti je obvykle dalším stádiem stalkingu. Nejspíše z těchto důvodů zařadil zákonodárce nebezpečné pronásledování do hlavy X., dílu 5. zvláštní části trestního zákoníku, mezi trestné činy narušující soužití lidí.

Jak uvádí trestní zákoník, trestného činu se dopustí ten, *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.

Jak vyplývá koneckonců i zařazení trestného činu v rámci trestního zákoníku, objektem trestného činu je zájem společnosti na poklidném soužití jednotlivých členů společnosti. Pachatelem se může stát kdokoli (není speciální subjekt).

Objektivní stránka trestného činu spočívá ve splnění dvou podmínek, jednak musí pachatel svou oběť dlouhodobě pronásledovat a současně toto jeho počínání musí být způsobilé vyvolat u oběti důvodné obavy o bezpečnost její, či jejích blízkých.

Příslušné ustanovení zákona obsahuje dále taxativní výčet jednání, jimiž může dojít k naplnění skutkové podstaty, a který v podstatě popisuje nejčastější způsoby, jakými se pachatelé snaží kontaktovat své oběti. Vzhledem k tomu, že tato práce nemá za cíl suplovat komentář k trestnímu zákoníku, zaměřím se pouze na způsoby, které souvisí s tématem této práce.

Je třeba ještě zmínit, že ač se jedná o trestný čin úmyslný, není nutné, aby úmysl zahrnoval i způsobení následku. Zcela tak postačuje, že se pachatel dopouští úmyslného jednání, které je následek způsobilé vyvolat. Následkem je pak myšlena důvodná obava o život a zdraví oběti, či osob jí blízkých, přičemž se bere v úvahu, zda jednání bylo objektivně způsobilé vyvolat obavu, čímž se eliminují subjektivní vlastnosti oběti, tedy její vyšší psychická odolnost, či naopak její labilita.

Kyberstalking

Z pohledu této práce je stěžejní ustanovení § 354 odst. 1 písm. c) trestního zákoníku, kdy je výslovně stanoveno, že skutkovou podstatu trestného činu nebezpečného pronásledování naplní ten, *kdo jiného vytrvale kontaktuje prostřednictvím prostředků elektronické komunikace, písemně, nebo jinak*.

Dané ustanovení se snaží postihnout jistou formu stalkingu pro kterou se vžilo označení *kyberstalking*. Jedná se o vytrvalé pronásledování oběti prostřednictvím prostředků moderní komunikace jako například mobilního telefonu,

pronásledováním oběti na diskusních fórech, chatech, sociálních sítích, kontaktování e-mailem, útoky proti počítači a počítačové síti oběti[72] apod.

Vzhledem k tomu, že prostředky moderní komunikace hrají v životě lidí stále větší roli a lidé jsou jimi obklopeni v podstatě permanentně je útok vedený jejich prostřednictvím mnohem efektivnější, než srovnatelné útoky páchané osobně. Pachatel má totiž možnost svou oběť pronásledovat takříkajíc na každém kroku.

S ohledem na výše uvedené mám tak jisté výhrady k zařazení kyberstalkingu do základní skutkové podstaty nebezpečného pronásledování. Vzhledem k vyšší efektivitě útoků je k narušení psychické integrity oběti potřeba mnohem kratší doba, než je potřeba k dosažení stejného poškození oběti v případě běžných forem stalkingu. Přihlédneme-li ke skutečnosti, že jedním z hlavních znaků skutkové podstaty je dlouhodobost pronásledování, je zde reálná hrozba, že se bude na útoky běžné a na kyberstalking aplikovat stejná časová podmínka, tedy minimální doba po kterou se musí pachatel dopouštět daného jednání.

Komentář k trestnímu zákoníku[73] v souvislosti s výkladem termínu *dlouhodobě* (TZ pojem dlouhodobosti nedefinuje), odkazuje na ustálený výklad tohoto pojmu, kdy jako dlouhodobé je chápáno jednání, kdy je ze strany pachatele vynuceno nejméně 10 kontaktů s obětí po dobu 4 týdnů, přičemž nejde pouze o nahodilé kontakty, ale o kontakty záměrné, vedené úmyslem pachatele působit na oběť.

Tento výklad dlouhodobosti se zdá být bezproblémovým v případech, kdy se bude jednat o běžné formy stalkingu, protože v průběhu 4 týdnů se může pachatel dopustit pouze několika desítek pokusů o kontakt. Oběť tedy v tomto případě může utrpět újmu, následky však nemusí být příliš závažné a trestněprávní postih nastupuje včas, aby zabránil eskalaci situace a způsobení dalších škod oběti.

[72] toto jednání, tedy útoky proti počítači oběti, by se posuzovalo dle § 230 TZ
[73] Šámal, P.a kol., Trestní zákoník II. § 140 až 421. Komentář. 1. vydání. Praha: C.H.Beck, 2010; s. 3008.

Problém však nastává v případě kyberstalkingu, protože v tomto případě může za stejnou dobu, tedy 4 týdnů dojít ke stovkám, či tisícům pokusů o kontakt, tudíž je oběť vystavena nesrovnatelně vyššímu tlaku, než v případě běžného stalkingu.

Jevilo by se proto jako vhodnější, kdyby kyberstalking byl zařazen mezi kvalifikované skutkové podstaty trestného činu. Vzhledem k tomu, že však k tomuto nedošlo, bude muset tento problém řešit praxe například tím, že v případě kyberstalkingu bude více přihlížet k intenzitě vedeného útoku a podle toho bude posuzovat zda nedošlo k naplnění skutkové podstaty trestného činu mnohem dříve, než za výše uvedené 4 týdny.

Osobně bych se však přikláněl k novelizaci ustanovení zákona, kdy by bylo výslovně řečeno, že v případě extrémně velké četnosti útoků se k časové podmínce nepřihlíží. Bylo by tak možné zasáhnout proti pachateli včas a ochránit tak oběť tohoto závadného jednání. Současně by se tímto vyřešila i možná námitka ze strany obžalovaných, že soudy již překračují výkladem pojmu výše navrženým způsobem své kompetence a dochází tak k narušování dělby moci ve státě, případně že dochází k porušování základních zásad trestního práva hmotného.

Jako další problém vidím výši trestu, která může být za toto jednání uložena. V případě základní skutkové podstaty je to trest odnětí svobody až na 1 rok, v případě kvalifikované skutkové podstaty je to trest odnětí svobody v délce trvání od 6 měsíců do 3 let. Tyto tresty jsou dle mého názoru s ohledem na to jakým následkům mají zabránit, velice nízké a neplní funkci preventivní, kterážto je jednou z funkcí trestního postihu v rámci trestního práva.[74]

Čtyři měsíce pronásledoval 35letý muž v Ústí nad Labem svou bývalou družku a několik lidí v jejím okolí. Nyní mu hrozí až roční pobyt za mřížemi, neboť se zpovídá z trestného činu nebezpečného pronásledování. Policisté případ uzavřeli ve zkráceném řízení. „Neustále jí volal a posílal textové zprávy s tím, že jí ublíží, zohaví nebo zabije. Jeho chování se stupňovalo a nabíralo na intenzitě. Vše

[74] blíže Jelínek, J. a kol. Trestní právo hmotné. 1. vydání. Praha: Leges, 2009, s. 347 an.

vyvrcholilo v den, kdy s mačetou v ruce napadl jejího kolegu z práce, za což je již také obviněn," řekla mluvčí ústecké policie Veronika Hyšplerová. .[75]

Hanobení národa, rasy, etnické skupiny nebo jiné skupiny osob (§ 355 TZ)

Tento trestný čin útočí na jednu z nejzákladnějších hodnot demokratické společnosti, a to na rovnost všech lidí ve společnosti nezávisle na rase, vyznání, nebo etnickém původu, zakotvenou v čl. 1 a čl. 3 odst. 1, Listiny základních práv a svobod.[76]

Základní skutková podstata je stanovena v § 355 odst. 1 TZ kdy trestného činu se dopustí ten, kdo veřejně hanobí:

a) některý národ, jeho jazyk, některou rasu nebo etnickou skupinu
b) skupinu osob pro jejich skutečnou nebo domnělou rasu, příslušnost k etnické skupině, národnost, politické přesvědčení, vyznání nebo proto, že jsou skutečně nebo domněle bez vyznání

Veřejným hanobením se chápou různá prohlášení, která mají pokud možno rozdělit společnost, zesměšnit, ponížit, či znevážit určitou skupinu obyvatelstva. Aby se jednalo o veřejné spáchání činu, musí k tomuto jednání dojít dle § 117 trestního zákoníku před nejméně třemi současně přítomnými osobami, nebo prostřednictvím tiskovin, filmu, televize, rozhlasu, či veřejně přístupné počítačové sítě (Internetu).

Navíc není nezbytné, aby členové skupiny, kterou se pachatel snaží znevážit, byli skutečně příslušníky například národnostní menšiny, zcela stačí, že se pachatel domnívá, že jimi jsou.

Okolnostmi podmiňujícími použití vyšší trestí sazby je spáchání tohoto trestného činu společně se dvěma osobami (minimálně 3 spolupachatelé), případně spáchání trestného činu tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem.

[75] článek uveřejněn dne 23.11.2010 v 10:09 h., on-line dostupný na http://www.novinky.cz/krimi/217408-muz-pronasledoval-byvalou-druzku-na-jejiho-kolegu-sel-s-macetou.html
[76] zákon č. 2/1993 Sb.

Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod (§ 356 TZ)

Trestného činu se dopustí ten, kdo veřejně podněcuje k nenávisti k některému národu, rase, etnické skupině, náboženství, třídě nebo jiné skupině osob nebo k omezování práv a svobod jejich příslušníků.

Na rozdíl od výše uvedeného trestného činu, v tomto případě se jedná o trestný čin, jehož hlavním motivem je nenávist k dané skupině osob, cílem pachatele je vyvolat stejné, nebo obdobné pocity jaké sám pociťuje vůči skupině i u ostatních osob. Opět je zde jedním z hlavních znaků veřejnost pachatelova počínání.

Okolností pro použití vyšší trestní sazby, je jednak spáchání trestného činu tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem, nebo pokud se pachatel za účelem páchání této trestné činnosti organizuje.

Na území ČR se nejčastěji hovoří o páchání této trestné činnosti v souvislosti s neonacistickými skupinami, které takto útočí především na romskou menšinu. Nejčastěji pak dochází k hanobení národa a podněcování k nenávisti v rámci proslovů, které doprovázejí setkání příznivců těchto skupin. Tyto skupiny však již pronikly i do prostředí Internetu a uveřejňují na svých webových stránkách různé články, jejichž cílem je právě podnítit nenávist vůči menšinám u jejich čtenářů[77]. Je nutné podotknout, že tyto skupiny jsou velice opatrné, pokud jde o volbu slov a své podněcování k nenávisti skrývají za ušlechtilé motivy, jako je např. pomoc lidem v nouzi.

Tohoto trestného činu se však poměrně často dopouštějí i běžní občané (nečlenové radikálních skupin) v rámci různých veřejných diskuzí k novinovým článkům, které se dotýkají národnostních menšin. Mnozí provozovatelé informačních serverů tento

[77] například stránky hnutí Národní odpor http://www.odpor.org/

problém řeší buď tím, že takovou diskuzi ani neotevírají, nebo ji otevřou pouze pro uživatele, jejichž identitu si předem ověřili. Pachatelé se totiž velice často schovávají právě za anonymitu Internetu, o tu však přicházejí právě ověřením identity provozovatelem informačního serveru.[78]

Za prohlášeními těchto běžných občanů je však dle mého názoru spíše, než nenávist k těmto skupinám, pocit frustrace vyvolaný mediálními prezentacemi některých trestních kauz, v nichž příslušníci národnostních menšin figurovali coby pachatelé. Občané na základě takto získaných informací nabývají dojmu, že soudy rozhodují především v případě příslušníků romské menšiny mírněji (tedy že se jedná o jakousi privilegovanou skupinu obyvatelstva) a tito proto mají výrazně lepší postavení před trestním soudem, než ostatní občané. Soudy by se proto právě v takových případech měly snažit lépe vysvětlovat, proč vzhledem k uveřejněným informacím nakonec uložily mírnější trest.

Kybernetická šikana

Jedná se o poměrně nový fenomén, související především s rozmachem sociálních sítí, jako je Facebook[79], či Twitter[80]. Zatímco „běžná“ šikana je charakteristická útoky na oběť, která se nějak odlišuje od většiny vrstevníků, nedostává se jí ochrany a podpory ze strany ostatních a je poměrně častá především v prostředí kde se vytváří určitá komunita, v rámci níž vzniká napětí, jako jsou školní zařízení, či armáda, kybernetická šikana se od této „běžné“ šikany podstatně odlišuje.

Kybernetická šikana má svá specifika. Především se velice rozšiřuje okruh osob, které se mohou stát pachateli, nebo naopak oběťmi. Obětí se totiž může stát i jinak ve společnosti uznávaný jedinec, který na první pohled nikterak nevybočuje z kolektivu, případně i osoba, která jinak požívá autority, jako jsou nadřízení v zaměstnání, nebo učitelé ve školách. Pachatelem pak může být i jinak nenápadný

[78] k tomuto kroku přikročil například informační server novinky.cz
[79] http://www.facebook.com
[80] http://twitter.com/

jedinec, který nedisponuje fyzickou převahou, ani nemusí být obzvláště oblíbeným v kolektivu.

Útok je veden prostřednictvím kyberprostoru a moderních technologií, kdy cílem pachatele je oběť zesměšnit, nebo poškodit její dobré jméno. Často útok spočívá v připomenutí, nebo zveřejnění traumatizující, či ponižující situace, která byla zachycena na kameru, nebo mobilní telefon. Toto se nejčastěji děje formou umístění takového videa na Internet.[81]

V poslední době se stává poměrně častým jevem urážení a znevažování učitelů jejich vlastními žáky, kdy se například student mstí prostřednictvím kyberprostoru svému učiteli za ohodnocení svého výkonu při zkoušení.

Trestněprávní posouzení jednání

Z trestněprávního hlediska se může jednat o přečin[82] pomluvy ve smyslu § 184 TZ, kdy toto ustanovení řeší pomlouvání jiné osoby, tedy sdělování údaje nepravdivého, který je způsobilý způsobit oběti újmu. Skutečnost že k tomuto jednání došlo v prostředí kyberprostoru je pak okolností podmiňující použití vyšší trestní sazby.

Skutková podstata trestného činu však nebude naplněna v případech, kdy dochází ke zveřejňování různých videí, nebo v případě znevažování prostřednictvím urážlivých poznámek na adresu oběti v prostředí kyberprostoru.

Dalším problémem je i častý nízký věk pachatelů. Jak jsem uvedl výše, kyberšikany se dopouští velice často děti. Děti jsou zákonem č. 218/2003 Sb., zákon o soudnictví ve věcech mládeže (dále jen „**ZSVM**“)[83], děleny na dvě skupiny, na osoby mladší 15 let, jejichž trestní odpovědnost je vyloučena dle § 25 TZ a na děti starší 15 let ale mladší 18 let, označované v § 2 odst. 1 písm. c) ZSVM jako „mladiství“. V případě

[81] blíže k problematice například http://www.lupa.cz/clanky/kybersikana-na-vzestupu/
[82] ve smyslu ustanovení § 14 odst. 2 trestního zákoníku
[83] vztah speciality k TZ

dětí ve smyslu § 126 TZ, tedy osob mladistvých dle ZSVM, je trestněprávní odpovědnost omezená a v rámci posuzování trestnosti jednání, je nezbytné ve smyslu ustanovení § 5 odst. 1 ZSVM též přihlížet k rozumové a mravní vyspělosti pachatele. Vzhledem k tomu, že mnoho mladistvých pachatelů chápe pomlouvání pedagogů v kyberprostoru jako neškodnou zábavu, na níž nevidí nic špatného. Je pravděpodobné, že by soud vyloučil trestněprávní odpovědnost pachatele podle § 5 odst. 1 ZSVM.
Jediný postih, který tak pachateli hrozí je výchovné opatření ve smyslu § 15 – 20 ZSVM, případně opatření ve smyslu § 93 ZSVM, předpokládám však, že k těmto krokům by přistoupil soud pro mládež pouze ve zvláště závažných případech.

Ani v případě dospělého pachatele však není zcela jisté, že by soud vyhodnotil pomlouvání jiné osoby v kyberprostoru jako pomluvu ve smyslu § 184 odst. 1, 2 TZ. Narážím zde především na skutečnost, že trestní soudy nejsou příliš ochotné, zabývat se pomluvami, čemuž nasvědčují diskuze kolem zrušení trestného činu pomluvy při příležitosti rekodifikace trestního práva hmotného a dále na zásadu subsidiarity trestní represe. Dá se tudíž předpokládat, že trestní soud zakročí pouze v extrémních případech.

Nezbývá proto, než konstatovat, že pokud se chce oběť kyberšikany účinně bránit, musí uplatnit svá práva na ochranu osobnosti prostřednictvím civilního soudního řízení, v rámci něhož může uplatnit nejen nárok na upuštění od neoprávněných zásahů do jejích osobnostních práv ve smyslu § 13 odst. 1 zákona č. 40/1964 Sb., občanského zákoníku, ale může též vznést nárok na náhradu nemajetkové újmy v penězích, ve smyslu ustanovení § 13 odst. 2 občanského zákoníku, v případě že bylo do jejích osobnostních práv zasaženo dostatečně závažným způsobem.

Praha - Šikanování přes SMS zprávy nebo po internetu zažilo za poslední půlrok každé desáté dítě od 8 do 15 let. Vyplývá to z dnes zveřejněného průzkumu projektu na minimalizaci šikany. Zástupci občanského sdružení Aisis a Nadace O2, kteří projekt organizují, se navíc zaměřili i na kyberšikanu namířenou na učitele. Výsledky ukázaly, že více než pětina dětí pokládá za zábavné svého kantora natáčet na video a

pak jej zesměšňovat. Pojem kyberšikana také podle průzkumu skoro polovina dětí vůbec nezná.[84]

[84] Článek uveřejněn dne 16.2.2010, on-line dostupný na http://www.ct24.cz/domaci/81165-kazde-desate-dite-zazilo-za-posledni-pulrok-kybersikanu/

Závěr:

Od dob vzniku prvního počítače uplynulo již mnoho let, mezitím se počítače rozšířily mezi širokou veřejnost a staly se běžnou součástí domácností. S masivním rozšířením počítačů se však objevila i počítačová kriminalita. Zavedením a rozšířením vysokorychlostního Internetu se tato ryze počítačová kriminalita následně přetvořila v kybernetickou kriminalitu.

Zcela oprávněně občané očekávali, že budou svými státy proti tomuto novému druhu kriminality ochráněni, to však vzhledem k povaze kyberprostoru není možné. I přes to se všechny vyspělé státy snaží svým občanům jistou míru bezpečnosti zajistit. Bohužel, mnohé státy v minulosti podcenily závažnost společensky nekonformního jednání, k němuž dochází v kyberprostoru. Jejich právní úprava tak na tuto situaci není připravená a díky zdlouhavosti legislativního procesu ještě nějakou dobu připravena nebude.

Nový trestní zákoník č. 40/2009 Sb. zavedl řadu nových trestných činů, které mají postihnout závadné jednání v kyberprostoru, což je dle mého mínění krok správným směrem. Z tohoto trestního zákoníku však přímo čiší, jak moc je ze strany zákonodárce celá problematika podceňována. Do budoucna bude proto určitě třeba, novelizovat některá ustanovení trestního zákoníku a přizpůsobit je vývoji v oblasti informačních technologií. Vzhledem k technologickému pokroku jaký každým dnem prodělává společnost a stále větší závislosti lidstva na počítačích, se to co dnes působí jako výmysl autorů science-fiction literatury, brzy může stát skutečností a jediné kliknutí myší, může mít katastrofální následky. Proto by zákonodárce neměl problematiku počítačové kriminality ani v nejmenším podceňovat.

Pokud se jedná o porušování autorských práv, jemuž je věnována velká část této práce, domnívám se, že velkou míru spoluviny na nárůstu tohoto druhu kriminality nesou samotné oběti této trestné činnosti. Většina pachatelů této trestné činnosti se jí totiž učí již na základní škole v souvislosti s ilegálním kopírováním počítačových her. Výrobci počítačových her se v rámci svých marketingových strategií zaměřují

na děti, záměrně v nich vyvolávají pocit, že bez jejich počítačové hry nebudou šťastné. Tlak na dítě pak vyvíjí nepřímo i dětský kolektiv, který podlehl tlaku výrobců a jehož hlavním tématem hovorů jsou právě počítačové hry. Ceny těchto počítačových her se pohybují většinou kolem 1000,- Kč za kus, což je však pro mnohé z rodičů a tudíž i jejich děti nedostupné, dítě se proto pokouší obstarat si hru jinak, tedy ilegálně. Pokud takto jedná opakovaně, zdokonaluje se a je pravděpodobné, že se v budoucnu (v dospělosti) ani nebude snažit o legální zakoupení autorských děl (především programů a audiovizuálních děl).

Možným řešením by bylo zahájení jednání mezi výrobci a zákazníky, v rámci kterého by se hledal širší konsenzus na ceně autorských děl, dokonce se domnívám, že by to vedlo k podstatnému zvýšení příjmů těchto společností a snížení míry porušování autorských práv, protože mnozí potencionální pachatelé by se v případě pro ně přijatelné ceny díla, rozhodli pro legální pořízení díla. Tento postup by velice pomohl i orgánům činným v trestním řízení, které jsou dlouhodobě kritizovány za neúčinný boj proti porušování autorských práv, protože by se míra této kriminality radikálně snížila a dá se též předpokládat, že by se i zvýšil počet podnětů od občanů, protože vlastníci autorských práv by si tímto vstřícným krokem získali veřejnost na svou stranu a ta by již odmítala dále ukrývat pachatele.

Prameny:

Učebnice:

Čírtková, L. Forenzní psychologie. Plzeň: Aleš Čeněk, s.r.o., 2004

Jelínek, J. a kol.: Trestní právo hmotné. 1. Vydání. Praha: Leges, 2009

Kuchta, J., Válková, H., Základy kriminologie a trestní politiky; 1. vydání; Praha; C.H.Beck; 2005

Novotný, O., Vokoun, R. a kol. Trestní právo hmotné – I. Obecná část. Praha : ASPI, 2007

Novotný, O., Vokoun, R. a kol. Trestní právo hmotné – II. Zvláštní část. Praha : ASPI, 2007

Novotný, O., Zapletal, J. a kol. Kriminologie. 3. přepracované vydání. Praha: ASPI, Wolters Kluwer, 2008

Porada, V. Metodika vyšetřování počítačové kriminality. Praha: Policejní akademie ČR, 1998

Požár, J.; Základy teorie informační bezpečnosti; Policejní akademie České republiky v Praze; 2007

Komentáře:

Šámal, P.a kol., Trestní zákoník I. § 1 až 139. Komentář. 1. vydání. Praha: C.H.Beck, 2009

Šámal, P.a kol., Trestní zákoník II. § 140 až 421. Komentář. 1. vydání. Praha: C.H.Beck, 2010

Telec, T., Tůma, P. Autorský zákon. Komentář. 1. vydání. Praha: C.H.Beck, 2007

Monografie:

Čermák, J. Internet a autorské právo. 2. aktualizované a rozšířené vydání. Praha: Linde, 2003

Dunovský, J., Mitlöhner, M., Hejč, K., Hanušová-Tlačilová, J. Problematika dětských práv a komerčního sexuálního zneužívání u nás a ve světě, Praha: Grada, 2005

Gřivna, T., Polčák, R. Kyberkriminalita a právo. Vyd. 1. Praha: Auditorium, 2008

Gřivna, T. Kybernetická kriminalita. Habilitační práce. Praha, 2010

Herczeg, J. Trestné činy z nenávisti. Praha: ASPI, Wolters Kluver, 2008

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

Jirovský, V. Kybernetická kriminalita (nejen o hackingu, crackingu, virech a trojských koních bez tajemství). Praha: Grada, 2007

Knappová, M., Švestka, J., Dvořák, J. a kol. Občanské právo hmotné. Svazek III. 4. aktualizované a doplněné vydání. Praha: ASPI, Wolters Kluwer, 2007

Matějka, M. Počítačová kriminalita. Praha: Computer press, 2002

Smejkal, V., Sokol, T., Vlček, M. Počítačové právo. Praha: C.H.Beck, 1995

Smejkal, V. Internet @ §§§. Praha: Grada, 1999

Vanduchová, V., Gřivna, T. (eds.), Pocta Otovi Novotnému k 80. Narozeninám, Praha: ASPI, Wolters Kluwer, 2008

Vlček, M. Počítače a kriminalita. Praha: Academia, 1989

Články z periodik:

Blatníková, Š. Pachatelé komerčního sexuálního zneužívání dětí v ČR – informace z výzkumu. Trestněprávní revue č. 11/2010

Cejp, M. Pokusy o předvídání možného vývoje kriminality. Trestněprávní revue č. 4/2010

Dressing, H., Maul-Backer, H., Gass, P. Posuzování stalkingu z kriminalistického a psychiatrického hlediska. Trestněprávní revue č. 10/2007 (překlad Hájek, J.)

Herczeg, J., Gřivna, T. Právo na přístup k Internetu, blokace stránek a digitální gilotina. Trestněprávní revue č. 5/2010

Poremská, M. Pornografie v USA. Trestněprávní revue č. 8/2008

Poremská, M. Vliv elektronické komunikace na praní špinavých peněz. Trestněprávní revue č. 8/2009

Válková, H. Česká podoba stalkingu podle § 354 TrZ v širších než jen v trestněprávních souvislostech. Trestněprávní revue č. 9/2009

Válková, H., Hulmáková, J. Trestněprávní ochrana dětí podle nového trestního zákoníku. Trestněprávní revue č. 10/2010

Visinger, R. Jak postihovat stalking? Zamyšlení nad novou právní úpravou. Trestněprávní revue č. 11/2009

Studie a materiály veřejné správy:

Seventh annual BSA/IDC global software piracy study, 2009

Sukovská. Analýza současného stavu a trendů vývoje trestné činnosti na úseku informačních technologií a Internetu včetně návrhu řešení. Praha, Odbor bezpečnostní politiky Ministerstva vnitra, 2006

Usnesení vlády České republiky, č. 949 ze dne 16.8.2006, K národnímu plánu boje proti komerčnímu sexuálnímu zneužívání dětí na období 2006 – 2008

Internetové zdroje:

http://www.epravo.cz
http://www.mvcr.cz
http://www.csas.cz
http://www.wikipedia.cz
http://www.google.cz
http://www.idnes.cz
http://www.czso.cz
http://www.firmy.cz
http://www.rapidshare.com
http://www.warforum.cz
http://www.astalavista.com
http://www.mininova.org
http://www.thepiratebay.org
http://www.ihned.cz
http://www.lawbrain.com
http://www.zlatakoruna.info

http://www.nsoud.cz
http://www.novinky.cz
http://www.odpor.org
http://www.facebook.com
http://www.twitter.com
http://www.lupa.cz
http://www.ct24.cz
http://www.itpravo.cz

Abstract:

Title of thesis:

Computer criminality

Abstract:

The main purpose of the thesis is a specification of so called COMPUTER or so called CYBERNETIC CRIMINALITY. The term itself could be defined in a restricted as well as in an extensive way. This thesis attempts to achieve a medium definition reflecting both these extremes. The thesis is divided into five chapters. Each chapter describes particular group of wrongful conducts. The crucial criteria for cathegorizing are similar features common to all these types of wrongful conduct. Each wrongful conduct is characterized by a detailed description of particular offense, its standard course and its legal assessment in accordance with the Criminal Act No. 40/2009 Collection of Laws, as amended by furher legislation.

The first chapter deals with offences against computers and computer systems - in other words, offences against the data stored within the system or transmitted inside them. It mainly focuses on unauthorized and illegal interventions into data integrity, unauthorized and illegal penetrations into computer systems and attempts to restrict the availability of computer systems for particular time periods.

The second chapter deals with fraudulent behaviour in the cyberspace which aims at bringing about damage to their victims and attempts to enrich on their credit. Each subchapter thoroughly describes the main ways of commiting such computer frauds. The outline of the frauds has only a demonstrative character depicting the description of the most important and interesting types.

Third chapter deals with the breaches of the law of intellectual property, particularly - the breaches of copyrights and related laws. Concerning the content of this chapter, it proved to be the most valuable and extensive one and it deals with the criminal liability of individual persons for spreading a legally-protected copyright content and of those persons participating in this criminal activity.

The fourth chapter deals with illegal spreading and illegal secretion of child pornography. This chapter provides a detailed look into so called virtual child

pornography. This chapter also analysis this offence as a common topic among erudite public and points out the fact that its harmfulness has not been determined precisely yet.

The last chapter is a collection of all remaining illegal activities commited in the cyberspace. Special attention is devoted mainly to Czech law de lege ferendae. The most visible example of the final chapter is so called ´dangerous following ´ - in other words ´Stalking´ and its computer modification commited in the course of the usage of information technology - so called cyberstalking. An increased attention is also paid to a new activity called ´Cybernetic bullying´ which started spreading in connection with the spreading of information technologies and the rise of so called social networks.

Klíčová slova/Key words:

počítač/computer, duševní vlastnictví/intellectual property, kriminalita/criminality