VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z.Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

POČÍTAČOVÁ KRIMINALITA A JEJÍ PŘÍČINY

Autor práce: Mirvald Patrik

Studijní obor: Bezpečnostně právní činnost ve veřejné správě

Forma studia: Kombinovaná

Vedoucí práce: doc. JUDr. Roman Svatoš, Ph.D.

Katedra: Katedra právních oborů a bezpečnostních studií

2017

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v této práci.

Souhlasím, aby práce byla uložena v knihovně Vysoké školy evropských a regionálních studií v Českých Budějovicích a zpřístupněna v souladu s § 47b zákona č. 111/1998 Sb. v platném znění.

.....

Děkuji vedoucímu bakalářské práce doc. JUDr. Romanu Svatošovi, Ph.D., za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

MIRVALD, P. *Počítačová kriminalita a její příčiny: bakalářská práce.* České Budějovice : Vysoká škola evropských a regionálních studií, z.ú. 2017. 65 s. Vedoucí bakalářské práce : Roman Svatoš, doc. JUDr., Ph.D.

Klíčová slova: Počítačová kriminalita, nový fenomén trestné činnosti.

Tato bakalářská práce stručně mapuje počítačovou kriminalitu a její základní pojmy. Rozebírá aspekty počítačové kriminality a snaží se poukázat na její nejzávažnější formy. Cílem práce je popis počítačové kriminality a to, jak se její nárůst promítl do rekodifikace trestního zákona.

ABSTRACT

MIRVALD, P. *Cyber Crime and its Causes: Bachelor thesis.* České Budějovice : The College of European and Regional Studies, 2016. xxx p. Supervisor : Roman Svatoš, doc. JUDr., Ph.D.

Key words: cyber crime, new phenomenon of criminal aktivity

This bachelor thesis concisely surveys cybercrime and its basic terminology. Analyzes aspects of cybercrime and tries to point out its most severe forms. The aim of these bachelor thesis is a description of cybercrime and how its growth reflected in the recodification of criminal law.

Obsah

Úvod

Počítačová kriminalita[1] se bezprostředně dotýká v podstatě celé společnosti. Vzhledem k dynamickému rozvoji komunikačních technologií za poslední desetiletí, kdy se počítače a další zařízení, která lze připojit k síti Internet z důvodu snížení výrobních nákladů a tedy i poklesu jejich cen staly nedílnou součástí většiny domácností, je počítačová kriminalita každodenní hrozbou pro společnost. Tato hrozba se týká nejen domácností, ale i všech státních a nestátních institucí, neboť každý z těchto subjektů je propojen s kyberprostorem[2]. Toto propojení poskytuje řadu možností pro páchání trestné činnosti za použití počítačů nebo proti počítačovým systémům.

Počítačová kriminalita může v konečném důsledku vést i ke globálním hrozbám, neboť komunikační technologie dávají do rukou pachatelům počítačové kriminality velkou škálu možností, jak destabilizovat státní zřízení. Pod pojem počítačová kriminalita lze zahrnout široké spektrum trestné činnosti, která je páchána buď přímo za užití počítačů, nebo je tato trestná činnost namířena proti počítačovým systémům a nosičům dat, jako takovým. Příčiny počítačové kriminality, tedy pohnutky, které vedou pachatele k jejímu páchání, jsou různé. V mnoha případech je to touha pachatele o vlastní zviditelnění, neoprávněný prospěch, snadný zisk, ublížit jinému, neoprávněně se obohatit atd. Počítačů lze dále užít jako prostředků pro vydírání, nebezpečné pronásledování, kyberšikanu a šíření dětské pornografie. Mimo obvyklou počítačovou kriminalitu dále stojí tzv. internetové podsvětí nazvané „Deep/Dark Net“, na kterém lze např. nelegálně zakoupit zbraně.

Rozvoj počítačové kriminality s sebou přinesl nová společensky škodlivá jednání[3], která bylo velmi těžké postihovat dle platných právních norem. V důsledku nárůstu počítačové kriminality přistoupila řada států včetně České republiky k

[1] Počítačová kriminalita - Za počítačovou kriminalitu je označováno nelegální, nemorální a neoprávněné jednání zahrnující užití dat získaných užitím výpočetní techniky, nebo jejich změnou. SVATOŠ, R. *Kriminologie ve světle nového trestního zákoníku.* 1. vydání. České Budějovice : Vysoká škola evropských a regionálních studií, o. p. s., 2010. s. 123.

[2] JIRKOVSKÝ, V. *Kybernetická kriminalita nejen o hackingu, virech a trojských koních bez tajemství*. Praha, Grada Publishing, a.s., 2007, s. 15-17.

[3] Společenská škodlivost je podle důvodové zprávy k trestnímu zákoníku určována povahou a závažností trestného činu, která se podle § 39 odst. 2 uplatňuje při stanovení druhu trestu a jeho výměry, k čemuž je třeba doplnit, že společenská škodlivost je určována především intenzitou zejména naplnění jednotlivých složek povahy a závažnosti činu, ale zcela se tím nevyčerpává, neboť je spojena s principem ultima ratio.

novelizacím svých trestních předpisů, do kterých byla implementována ustanovení, na základě kterých lze postihovat pachatele tohoto druhu kriminality.

Prověřování počítačové kriminality a odhalování jejích pachatelů je specifickou policejní činností, která vyžaduje od policistů odbornou znalost nejen policejní práce jako takové, ale především znalost všech forem počítačové kriminality, sledování jejího vývoje a neustálé prohlubování již získaných znalostí na poli komunikačních technologií. Po policistech je dále požadováno, aby tyto znalosti byli schopni použít při odhalování pachatelů počítačové kriminality a jednání těchto pachatelů řádně přiřadili pod jednotlivé skutkové podstaty, uvedené ve zvláštní části zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších právních předpisů („TZ“)[4]. Jednotlivými druhy počítačové kriminality, odhalováním jejích pachatelů, jejím prověřováním, vyšetřováním a právní kvalifikací se bude zabývat tato bakalářská práce.

[4] ČESKO. Zákon č. 40/2009 Sb. trestní zákoník. In *Sbírka zákonů, Česká republika.* 2009, částka 11.

1 Cíl a metodika bakalářské práce

Bakalářská práce je rozdělena na dvě části. Jedná se o teoretickou a praktickou část, ve kterých bude postupováno dle stanovených cílů a metodiky.

První část práce je zaměřena na teoretickou analýzu počítačové kriminality a jejích příčin, popis jednotlivých forem počítačové kriminality a skutkových podstat z trestního zákoníku, pod které lze jednotlivé formy počítačové kriminality přiřadit. Tato část práce je založena na studiu oborné literatury a právních norem.

Vzhledem ke skutečnosti, že téma počítačová kriminalita a její příčiny je tématem velmi obsáhlým, je záměrem autora této práce výstižně a přehledně uvést jednotlivé formy počítačové kriminality. Autor se nejprve věnuje popisu jednotlivých forem počítačové kriminality, právní kvalifikaci těchto forem počítačové kriminality a způsobu prověřování těchto forem počítačové kriminality. U každého z popsaných příkladů je uvedena i právní kvalifikace dle trestního zákoníku, aby z uvedených příkladů bylo patrno, jak důležitá byla pro prověřování a vyšetřování počítačové kriminality rekodifikace trestního práva hmotného v České republice.

Cílem první části této práce je zhodnotit počítačovou kriminalitu, její základní pojmy, aspekty a poukázat na její nejzávažnější formy.

Praktická část bakalářské práce je založena na analýze kazuistiky případů počítačové kriminality, které byly ukončeny pravomocným rozhodnutím příslušného soudu. Její podstatou je hodnocení způsobů vyšetřování trestných činů na poli počítačové kriminality, analýza správné právní kvalifikace jednotlivých popsaných případů tak, že takto popsané případy a jejich právní kvalifikace byla akceptována ze strany soudů a došlo k pravomocným rozsudkům. Případy, které byly vybrány pro tuto práci, jsou případy, které autor práce vyšetřoval v rámci své praxe u Policie ČR, na Obvodním ředitelství policie Praha IV, 3. oddělení hospodářské kriminality.

Cílem praktické části bakalářské práce je provedení analýzy popsaných případů z hlediska další fáze trestního řízení. Druhotným cílem bakalářské práce je dále zhodnocení toho, jak se nárůst počítačové kriminality promítl do rekodifikace trestního práva hmotného. V závěrečné části bakalářské práce bude kladen důraz i na prevenci počítačové kriminality, kdy tato je velmi problematická. Hrozbám z internetu se lze do jisté míry

bránit plně zabezpečeným a neustále aktualizovaným počítačem, pravdou však je, že nejvíce škod je napácháno díky liknavosti a lehkomyslnosti uživatelů, kteří slepě kliknou na každý odkaz, který jim webová stránka podstrčí a čile komunikují s entitami na internetových seznamkách nebo diskusních fórech, kde na sebe prozradí i to, co by běžně nesdělili ani svým nejbližším. Pro krátké shrnutí prevence počítačové kriminality lze užít obdobu pranostiky „dvakrát čti a jednou klikni“.

Závěrečná část práce obsahuje stručné shrnutí práce, zhodnocení výsledků praktické části práce. Vzhledem k obsáhlosti tématu počítačová kriminalita a její příčiny nebylo možné striktně oddělit praktickou část od části teoretické, proto v některých fázích práce došlo k prolnutí těchto částí práce. Snahou autora bakalářské práce je, aby toto prolnutí bylo srozumitelné a dalo ucelený logický pohled na počítačovou kriminalitu.

2 Počítačová kriminalita, její hrozby a formy

„Počítačovou kriminalitou rozumíme takovou činnost, kterou je porušován zákon, nebo je v rozporu s morálními pravidly společnosti“[5]. Počítačová kriminalita je namířena proti počítačům, jejich hardware, software, ale také proti sítím, webovým stránkám, sociálním sítím, atd. Počítačovou kriminalitu můžeme chápat i jako prostředek pro kriminalitu obecnou, kdy počítače a sítě slouží k páchání jiné trestné činnosti, např. šíření dětské pornografie. Vyšetřováním počítačové kriminality se v České republice zabývá Služba kriminální policie a vyšetřování (dále jen „SKPV“), odbory hospodářské kriminality.

2.1 Kyberprostor

Pojem počítačová - kybernetická kriminalita, není odvozen od kybernetiky, ale od pojmu kybernetický prostor, pro který se vžilo označení kyberprostor. „Kyberprostor je tvořen stovkami a tisíci propojených počítačů, serverů, routerů, přepínačů a optických kabelů“[6]. Vznik kyberprostoru je datován do roku 1968, kdy v USA došlo ke vzniku malé sítě ARPHANET. V době vzniku první počítačové sítě nikdo nepředpokládal, že o nějakých 40 let později dojde k tak masovému rozvoji a počítačová síť World Wide Web bude rozšířena po celém světě. „Kyberprostor je sběrný, popisný termín pro všechno od Internetu a světové sítě až po imaginární a metaforický prostor, který v něm existuje“[7].

2.2 Hrozby počítačové kriminality

Jednou z nejzávažnějších hrozeb počítačové kriminality globálních rozměrů je kyberterorismus[8], který je konvergencí terorismu a kyberprostoru obecně chápaný jako nezákonný útok nebo nebezpečí útoku proti počítačům, počítačovým sítím a informacím v nich uložených v případě, že útok je konán za účelem zastrašit nebo donutit vládu nebo obyvatele k podporování sociálních nebo politických cílů. Tuto definici lze poměrně

[5] JIRKOVSKÝ, V. *Kybernetická kriminalita nejen o hackingu, virech a trojských koních bez tajemství.* Praha, Grada Publishing, a.s., 2007, s. 19.
[6] ŠÁMAL, P. a kol. *Trestní zákoník. 1. vydání*, Praha, C.H.Beck, 2009, s. 3285, s. 2083.
[7] ŠÁMAL, P. a kol. Trestní zákoník. 1. vydání, Praha, C.H.Beck, 2009, s. 3285, s. 2083.
[8] JIRKOVSKÝ, V. *Kybernetická kriminalita nejen o hackingu, virech a trojských koních bez tajemství.* Praha, Grada Publishing, a.s., 2007, s. 130-131.

dobře vysvětlit na příkladu, kdy terorista např. ovládne systém řízení počítačů v jaderné elektrárně, který je velmi rozsáhlý, získá kontrolu nad ovládáním regulačních tyčí reaktoru a začne vydírat vládu některého státu, že pokud neuposlechne jeho požadavků např. na vydání vězněných teroristů, způsobí přehřátí reaktoru a následný výbuch jaderného reaktoru, čímž dojde ke katastrofě, jejímž výsledkem budou tisíce obětí.

Z kyberprostoru však společnosti nehrozí pouze teroristické útoky. Kyberprostor je prostředí, ve kterém zločinecké skupiny, ale i jednotlivci páchají celou řadu činností, které jsou nebezpečné zejména z důvodu jejich anonymity. Velkou hrozbou především pro děti, ale i dospělé, jsou sociální sítě. Nedůsledná kontrola rodičů, co dítě dělá na sociální síti, nebo nedostatečná obezřetnost dospělých při užívání sociální sítě, může vyústit až k velké tragédii v podobě sexuálního zneužití a vraždy dítěte, vraždy nebo znásilnění důvěřivé ženy, nebo v mírnější formě k vydírání nebo okradení osob.

Nejčastějším jevem počítačové kriminality jsou však různé podvody v Internetu, vedoucí ke ztrátám finančních prostředků osob. Těchto podvodů je celá řada a možnosti pachatelů v podstatě neomezené. Nejrozšířenějšími jsou různé Phishingové útoky, které jsou zaměřeny k získávání hesel, čísel platebních karet a dalších citlivých údajů uživatele. Velkou hrozbou jsou rovněž různé inzertní portály, na kterých je k nalezení mnoho inzerátů, které lákají uživatele k nákupu např. nových mobilních telefonů za velmi nízké ceny s platbou dopředu.

V prostředí Internetu se dále uzavírají obchody týkající se dětské pornografie, chráněných druhů živočichů, obchody s padělaným zbožím, ale dají se zde nakoupit i drogy nebo objednat vražda. K těmto věcem se však již běžný „surfař“ nedostane, protože ty se odehrávají v uzavřené části Internetu v tzv. „Darknetu“[9], též nazývaném „Deepnet“. K přístupu do této sítě je třeba specifická znalost, mnohdy i speciální hardware. Celý systém „Deepnetu“ funguje v podstatě na principu P2P sítě, která je vedena přes několik proxy serverů. Uživatel zde nenalezne klasický Internet tak, jak jej zná, absentuje zde standardní vyhledávač a vše se děje za užití příkazů a hledání klíčových slov.

[9] AUTOR@CHIP.CZ. Darknet. *CHIP, Magazín o digitálních technologií*. 2016, č. 11, s 60. ISSN 1210-0684.

2.3 Formy počítačové kriminality

Počítačová kriminalita má mnoho podob a forem. Tou nejméně závažnou formou z pohledu státních zastupitelství a soudů je porušování autorských práv, kdy stát cestou orgánů činných v trestním řízení (dále jen „OČTŘ“) chrání spíše soukromé zájmy nadnárodních softwarových korporací, hudebního a filmového průmyslu. K porušování autorských práv dochází formou sdílení děl chráněných autorským zákonem cestou P2P (peer-to-peer)[10] sítí a nahráváním (dále jen uploadem[11]) děl na File Hostingové servery[12]. Mnohem závažnějšími formami jsou různé zásahy do soukromí uživatelů internetu, kdy se jedná o krádeže osobních dat, citlivých fotografií, následný obchod s nimi a vydírání uživatelů, nebo pronásledování formou nadměrné e-mailové a jiné komunikace nebo vyhrožování. Nejzávažnější formou počítačové kriminality jsou krádeže finančních prostředků za užití sofistikovaných programátorských metod tzv. Phishing[13]. Počítače, potažmo počítačová síť Internet, však také slouží jako nástroj trestné činnosti, kdy za užití internetu dochází k různým podvodným jednáním formou falešných inzerátů na prodej zboží nebo sjednávání nelegálních obchodů. Mimo klasickou počítačovou kriminalitu dále stojí kyberterorismus, který by popsán v kapitole zabývající se hrozbami počítačové kriminality. Kyberterorismus jako takový není klasickým druhem počítačové kriminality, z toho důvodu je v této práci pouze zmíněn v kapitole o hrozbách počítačové kriminality a nebude v této práci dále rozebírán.

[10] *Peer-to-peer*, neboli o uživatele k uživateli, je princip propojování v počítačových sítích, kde každá strana spojení jej může iniciovat a má stejnou odpovědnost. JIRKOVSKÝ, V. *Kybernetická kriminalita nejen o hackingu, virech a trojských koních bez tajemství*. Praha, Grada Publishing, a.s., 2007, s. 73.

[11] *Upload,* Odesílání dat například na server v síti internet. Je to přesný opak stahování (downloadu), kdy se data přijímají. In: *Svět hardware ...vše ze světa počítačů*, Slovník. Dostupné z WWW http://www.svethardware.cz/slovnik/u.

[12] *File Hostingové servery* či filehostingová služba je datové úložiště, kam mohou uživatelé nahrávat data a následně je stahovat. In: *IT SLOVNÍK.cz*, File hosting. Dostupné z WWW http://it-slovnik.cz/pojem/file-hosting/?utm_source=cp&utm_medium=link&utm_campaign=cp.

[13] *Phishing*, jedná se o podvodnou techniku na internetu, jak získat důležité a citlivé osobní údaje a informace, např. hesla. In: *IT SLOVNÍK.cz*, Phishing. Dostupné z WWW http://it-slovnik.cz/pojem/phishing/?utm_source=cp&utm_medium=link&utm_campaign=cp.

3 Porušování autorských práv

Nejméně závažnou formou počítačové kriminality je neoprávněné sdílení hudebních děl, audiovizuálních děl a software za užití Internetu. Neoprávněně sdílený autorský obsah je nazýván Warez[14]. Tento druh kriminality je páchán za užití P2P sítí, cestou File Hostingových serverů, v kombinaci s „warezovými" diskusními fóry, nebo za užití Embeddingu[15]. Další formou porušování autorských práv je neoprávněné užívání počítačového software.

3.1 Porušování autorských práv cestou P2P sítí

Touto formou lze nelegální rozmnoženiny autorských děl sdílet dvěma způsoby za užití Torrent[16] P2P sítě, nebo Direct Connect[17] sítě. U obou způsobů není nelegální obsah umístěn na Internetu, ale je umístěn u pachatele v PC a pachatel musí mít v PC instalován buď torrentového klienta, nebo u Direct Connect sítě tzv. hubsoft. V těchto případech většina uživatelů nesdílí nelegální autorský obsah z důvodu úmyslného porušování autorského zákona, ale z toho důvodu, že si sami chtějí stáhnout autorské dílo nasdílené jiným pachatelem. U obou uvedených P2P klientů však při stahování souborů dochází zároveň i k jejich odesílání jiným uživatelům dané P2P sítě, čímž dochází k porušování autorského práva. Samotné stahování děl není dle legislativy České

[14] *Warez* je termín, označující porušováni autorských práv. Jsou to například webové stránky na kterých jsou nabízeny ke stažení cracky do různých her, filmy, software a další. In: *IT SLOVNÍK.cz*, Warez. Dostupné z WWW http://it-slovnik.cz/pojem/warez/?utm_source=cp&utm_medium=link&utm_campaign=cp.

[15] *Embedding*, je forma podpory šíření videa na další internetové stránky pomocí vložení speciálního kódu. In: *STREAMHOSTING, Vaše video online*, Podpora, Slovník. Dostupné z WWW http://www.streamhosting.cz/cz/podpora/slovnicek/c103.

[16] *Torrent*, je malý soubor s koncovkou torrent, který obsahuje metadata o poskytovaných distribuovaných datech ve formě hash bloků těchto dat. JIRKOVSKÝ, V. Kybernetická kriminalita nejen o hackingu, virech a trojských koních bez tajemství. Praha, Grada Publishing, a.s., 2007, s. 73.

[17] *Direct Connect*, se výrazně liší od všech programů pro výměnu souborů. Je totiž částečně centralizovaný. Klienti se připojují k centrálním serverům, které se nazývají hub. Na hubech běží speciální aplikace takzvaný hubsoft (Strong DC++), přes který se provádí celá správa hubu. Jeho hlavním úkolem je udržovat aktuální seznam uživatelů a vyhledávat požadovaná data. Vyhledávání probíhá u všech připojených uživatelů. Existují jak malé (pár desítek či stovek) huby spíše komunitního rázu, tak relativně velké huby masovější huby s až 20 tisíci uživateli. In: *Wikipedie: Otevřená encyklopedie*. Dostupné z: WWW https://cs.wikipedia.org/wiki/Direct_Connect.

republiky trestné, tedy není zákonem nijak zakázáno[18], ale jeho neoprávněné sdílení je užití autorského díla v rozporu s autorským zákonem.

3.2 Porušování autorských práv cestou File Hostingových serverů

Při porušování autorského práva cestou File Hostingových serverů dochází k uploadu autorských děl na File Hostingové servery. Pachatelé této trestné činnosti se nazývají Uploadeři a odkazy ke stažení jimi uploadovaných děl zveřejňují na Warez fórech např. www.warcenter.cz, www.warforum.cz apod. Takto sdílený obsah lze dále vyhledat i přímo ve vyhledávači daného File Hostingového serveru. Nejznámějším světovým File Hostingovým serverem byl www.megaupload.com, v České republice to je www.ulozto.cz. Při páchání této trestné činnosti pachatelé cíleně neoprávněně šíří nelegální rozmnoženiny celých autorských děl v podobě hudebních alb, filmů a software. Za toto neoprávněné šíření děl inkasují finanční částky přímo od provozovatelů File Hostingových serverů buď přímo na svůj účet nebo formou kreditu ke stahování, který následně přeprodávají.

3.3 Porušování autorských práv cestou Embeddingu

K porušování autorských práv též dochází formou embeddování celých filmů na různé servery v destinacích jako je Čína, Rusko nebo Afrika. Tato díla jsou pak bez souhlasu autorů zpřístupněna na odkazu, který pachatel uveřejní na svých k tomuto účelu speciálně vytvořených stránkách např. www.sledujserialy.cz. Po zadání odkazu do webového prohlížeče se spustí přehrávání daného videa a kterýkoli uživatel internetu tak může tato videa sledovat. O tomto typu porušování autorského práva bylo rozhodnuto v Usnesením Nejvyššího soudu České republiky vydaného pod sp. zn. 8Tdo 137/2013-43.

3.4 Porušování autorských práv neoprávněným užívání software

Tento typ počítačové kriminality spočívá v užívání nelegálních rozmnoženin počítačových programů v rozporu s jejich licenčními podmínkami. Licenční smlouva je

[18] Každý může činit, co není zákonem zakázáno, a nikdo nesmí být nucen činit, co zákon neukládá. ČESKO. Ústavní zákon č. 2/1993 Sb. ve znění ústavního zákona č. 162/1998 Sb., *Listina základních práv a svobod*. In: *Sbírka zákonů, Česká republika*. 16. prosince 1992.

základní právní dokument, který vymezuje, jakým způsobem může uživatel nakládat s počítačovým programem. Pachateli, o kterých se orgány činné v trestním řízení dozví, jsou v převážné většině právnické osoby, které z důvodu úspory užívají nelegální rozmnoženiny počítačových programů související s jejich podnikatelským segmentem. Nejčastěji užívanými nelegálními rozmnoženinami počítačového software jsou aplikace společnosti Autodesk Incorporated, Adobe systém Incorporated a Microsoft Corporation. U této počítačové kriminality je velká latentnost[19], neboť o takovém druhu kriminality se OČTŘ dozví pouze z oznámení nebo při prověřování např. neoprávněného sdílení děl chráněných autorským zákonem popsaným výše, kdy při zajištění PC pachatele je znalecky zkoumána i legálnost užitého software.

3.5 Trestněprávní ochrana porušování autorského práva

Porušování autorského práva je v trestním zákoníku vymezeno v ustanovení § 270 Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi. Z tohoto ustanovení vyplývá „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 bude potrestán“[20]. Jedná se o trestněprávní normu s blanketní dispozicí[21]. „Právním základem autorského práva je čl. 34 LPS ve spojení s čl. 3 Úst, podle něhož práva k výsledkům tvůrčí duševní činnosti jsou chráněna zákonem“[22]. Základní úprava autorskoprávních vztahů je obsažena v zákoně č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (dále jen „autorský zákon“). Z autorského zákona vyplývá, že neoprávněným zásahem do práva autorského je zveřejnění díla bez souhlasu autora. Autorský zákon dále poskytuje ochranu počítačovému programu jako takovému, ale také účinným technickým prostředkům ochrany autorských práv.

[19] *Latentní kriminalita* – skrytá neboli neregistrovaná, jde o kriminalitu, o které se OČTŘ nedozvěděly a není uvedena v oficiálních statistikách. SVATOŠ, R. *Kriminologie ve světle nového trestního zákoníku.* 1. vydání. České Budějovice : Vysoká škola evropských a regionálních studií, o. p. s., 2010. s. 16.
[20] ŠÁMAL, P. a kol. *Trestní zákoník. 1. vydání*, Praha, C.H.Beck, 2009, s. 2495.
[21] *Právní norma s blanketní dispozicí* - odkazující na jiný zákon, v tomto případě na zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů. ŠÁMAL, P. a kol. *Trestní zákoník. 1. vydání*, Praha, C.H.Beck, 2009, s. 2497.
[22] ŠÁMAL, P. a kol. *Trestní zákoník. 1. vydání*, Praha, C.H.Beck, 2009, s. 2497.

4 Neoprávněné přístupy do počítačových systémů

Velmi rozšířenou trestnou činností na poli počítačové kriminality jsou neoprávněné přístupy do počítačových systémů. Cíle pachatelů neoprávněných přístupů jsou různé a dají se třídit dle typů útoků. Útoky na počítačové systémy jsou zaměřeny buďto proti počítačovým systémům jako takovým, s cílem jejich ochromení nebo ovládnutí, anebo jsou zaměřeny proti datům uloženým v počítačových systémech s cílem jejich zcizení a následného využití nebo zneužití jejich informačního charakteru. Uvedené typy útoků spolu někdy velmi úzce souvisí, neboť cílem pachatelů je v první řadě ochromení počítačového systému nebo získání přístupu do počítačového systému překonáním zabezpečovacího zařízení, tedy útok na počítačový systém a následné neoprávněné nakládání s daty v takto ochromeném, nebo pachateli zpřístupněném počítačovém systému. Pro potřeby bakalářské práce je v úvodu této kapitoly třeba vymezit, co je to počítačový systém z pohledu trestního zákoníku. „Počítačový systém se rozumí jakékoli zařízení nebo skupina vzájemně propojených nebo souvisejících zařízení, z nichž jedno nebo více provádí na základě programu automatické zpracování dat. Počítačový systém je tedy zařízení, sestávající z technického (hardware) a programového (software) vybavení, které je určené k automatickému zpracování digitálních dat. Počítačový systém však zahrnuje i síťově připojená zařízení, která pojmově nesplňují atributy počítače“[23]. Zjednodušeně řečeno, počítačový systém je z pohledu trestního zákoníku vše počínaje počítačem jako takovým, smartphonem atd., ale i webovými stránkami, nebo internetovým úložištěm dat.

4.1 Útoky proti webovým stránkám a serverům

Tento typ útoku používají pachatelé s cílem svého zviditelnění nebo zapříčinění nečinnosti daného serveru. Pokud je útok prováděn s cílem zviditelnění pachatelů, je server, na který útok směřuje, útočníky nejdříve vyřazen, poté nad ním útočník převezme kontrolu a nahradí obsah webových stránek umístěných na tomto serveru vlastním obsahem (např. útoky skupiny Annonymous). Útok probíhá v reálném čase a lze jej provést několika metodami.

[23] ŠÁMAL, P. a kol. *Trestní zákoník. 1. vydání,* Praha, C.H.Beck, 2009, s. 2087, s. 2088.

4.1.1 Metody útoků proti webovým stránkám a serverům

Metod, jak zapříčinit nefunkčnost webových stránek, jsou desítky a jejich kompletní výčet a popis funkcí by vydal na samostatnou práci. Z tohoto důvodu zde budou prezentovány a stručně popsány pouze dva nejčastější typy útoků. Nejznámějším typem útoku, směřujícím proti webovým stránkám s cílem jejich vyřazení, je „Denial of Service (dále jen DoS) a Distributed Denial of Service (dále jen DDoS)“[24]. Tento útok spočívá např. v zahlcení síťové karty, operační paměti nebo aplikace neustálým odesíláním jednoho a toho samého požadavku na danou komponentu, dokud nedojde k jejímu zahlcení. Velmi rozšířeným typem útoků na webové stránky je útok za užití techniky „SQL Injection“[25], který je prováděn přes podstrčený soubor „Cookies“[26].

4.2 Útoky proti počítačům a jiným zařízením

Cílem pachatelů je převážně zisk, kterého dosáhnou tím, že do počítače oběti instalují cestou staženého souboru, který bývá součástí např. „Cracku“[27] pro zprovoznění nelegálního software, nebo chybou zabezpečení tzv. Ransomware, tedy počítačový virus, který zašifruje soubory na disku napadeného počítače. Tento typ počítačového viru je povětšinou nahrán do hlavního spouštěcího oddílu operačního systému na pevného disku (Master Boot Record). Při opětovném spuštění systému oběť zjistí, že se nemůže dostat do svého počítače, ale je při startu systému uvedeným počítačovým virem přesměrována na webové stránky pachatelů, kde bývá často špatnou češtinou napsán text, že oběť porušila trestní zákon České republiky se smyšlenými ustanoveními a je jí vyměřena

[24] *DoS a DDoS útok*, je druhem útoku na webové služby, který má za cíl službu znefunkčnit a vyřadit přehlcením požadavky na tuto službu. Podtypem tohoto útoku je DDoS, při kterém je pouze využito velké množství rozptýlených počítačů. JIRKOVSKÝ, V. *Kybernetická kriminalita nejen o hackingu, virech a trojských koních bez tajemství.* Praha, Grada Publishing, a.s., 2007, s. 66.

[25] *SQL Injection* je technika napadení databázové vrstvy programu vsunutím kódu přes neošetřený vstup a vykonání vlastního, samozřejmě pozměněného, SQL dotazu. HARRIS, HARPER, EAGLE, NESS, LESTER, *Hacking – manuál hackera*, Grada Publishing, a.s. 2008, s 90.

[26] *Cookies*, jsou informace, které se ukládají v internetovém prohlížeči na straně klienta. Slouží například k uložení informace o tom, co obsahuje nákupní košík při nakupování v eshopu. In: IT SLOVNÍK.cz, Cookis. Dostupné z WWW
http://it-slovnik.cz/pojem/cookies/?utm_source=cp&utm_medium=link&utm_campaign=cp

[27] *Crack*, je pozměněný spouštěcí soubor aplikace, sloužící km jejímu spuštění. Pozměnění dat v souboru spočívá ve funkci, která umožní např. obejít zadání produktového klíče programu. JIRKOVSKÝ, V. *Kybernetická kriminalita nejen o hackingu, virech a trojských koních bez tajemství.* Praha, Grada Publishing, a.s., 2007, s. 69 - 70.

pokuta nejčastěji ve výši 2.000 EUR. Pokud nebude pokuta zaplacena, zůstane počítač uzamčen. Obdobné útoky směřují i proti smartphonům, tabletům a podobným zařízením.

4.3 Útoky proti integritě dat v počítačovém systému

Nejčastějším důvodem neoprávněných přístupů do počítačového systému formou překonání zabezpečovacího zařízení, je útok na data uložená v počítačovém systému. Útok na data je prováděn ve smyslu neoprávněné manipulace s nimi, změny těchto dat, zcizení těchto dat, potlačení jejich informační hodnoty nebo jejich padělání. K útokům proti datům uložených v počítačovém systému však může docházet, aniž by bylo překonáno bezpečnostní opatření, neboť pachatelé těchto útoků již heslo k počítačovému systému vlastní např. v souvislosti s výkonem svého povolání, nebo neoprávněně přechovávají přístupové zařízení a heslo do počítačového systému, které využijí k provedení útoku na integritu dat uložených v počítačovém systému.

4.4 Útoky formou překonání zabezpečovacího zařízení

Při páchání tohoto typu trestné činnosti pachatelé užívají nedokonalosti zabezpečení počítačového systému nebo jeho částí. Po překonání zabezpečovacího zařízení počítačového systému (nabourání do počítače oběti), může pachatel volně nakládat s počítačovým systémem a daty uloženými v počítačovém systému. Důsledky této činnosti jsou velké finanční ztráty obětí, krádeže citlivých fotografií a dokumentů, odposlech mnohdy citlivé e-mailové komunikace. Oběti těchto útoků se často stávají terčem vydírání pachatelů, kdy pachatelé těmto obětem hrozí, že zveřejní ukradená citlivá data. V současné době je mezi pachateli tohoto typu počítačové kriminality velmi populární prodej ukradených herních účtů typu Steam, PlayStation, apod., ve kterých mají oběti uloženy hry v ceně desetitisíců. Pachatelé tohoto typu počítačové kriminality dále přebírají kontrolu nad účty na sociálních sítí obětí, kde zveřejňují příspěvky, jako by je zveřejňovala oběť, kdy v těchto příspěvcích užívají citlivá data získaná svojí kriminální činností. Takové zveřejnění příspěvků může oběť tohoto typu trestné činnosti stát nemalé problémy např. v zaměstnání, kdy mnoho firem neustále kontroluje chování svých zaměstnanců v prostředí Internetu. Dalším jevem spojeným s touto trestnou činností je prodej osobních údajů obětí reklamním společnostem, kdy pachatelé za prodaná osobní data od reklamních společností inkasují nemalé provize, neboť cílená reklama je

v současné době velmi žádaným artiklem nejen v prostředí Internetu. V další podkapitole budou popsány nejznámější typy útoků na počítačové systémy obětí. Mnoha výše popsaným situacím však mohou oběti velmi snadno zabránit nebo alespoň minimalizovat rizika dbáním na to, aby byl jejich systém neustále aktualizován a správně zabezpečen vhodným bezpečnostním řešením – antivirovým programem. U tohoto typu kriminality platí v celosvětovém měřítku, že ke zjištění pachatele dojde jen v ojedinělých případech, neboť níže popsané metody jsou velmi sofistikované, veškeré toky dat prochází šifrovanou komunikací přes několik serverů typu Tor nebo Proxy serverů, které zajišťují anonymizaci pachatele. Pachatelé tohoto typu počítačové kriminality se umí velmi dobře maskovat. Stopování takového pachatele by muselo probíhat v reálném čase, tedy v době útoku na počítačový systém, což není možné, neboť oběť útok na její počítačový systém zaznamená až v momentě, kdy dojde např. k odčerpání finančních prostředků z jejího účtu. V současné době veškeré počítačové viry pracují skrytě, na pozadí operačního systému a mnohdy jsou velmi obtížně detekovatelné pro bezpečnostní opatření – antivirové nástroje.

4.4.1 Útok hrubou silou

Tato metoda mezinárodně nazvaná „Brute force“[28], spočívá v tom, že útočník napíše program (počítačový virus), který se pokouší kombinací všech znaků na klávesnici odhalit heslo, jímž je chráněn počítačový systém. Skutečnost je taková, že tomuto programu netrvá dlouho a heslo do počítačového systému odhalí, protože mnoho uživatelů používá jako heslo svoje jméno či jméno svého psa, které veřejně publikuje na sociálních sítí, nebo numerické heslo !12345678“.

4.4.2 Slovníkový útok

„Tento typ útoku je velmi podobný útoku hrubou silou s tím rozdílem, že počítačový virus vyzkouší veškerá slova jazyka, ve kterém je provozován operační

[28] JIRKOVSKÝ, V. *Kybernetická kriminalita nejen o hackingu, virech a trojských koních bez tajemství.* Praha, Grada Publishing, a.s., 2007, s. 62.

systém. Z toho důvodu většího zabezpečení počítačového systému je třeba sestavit heslo minimálně z kombinace velkých, malých písmen a číslic“[29].

4.4.3 Odposlech datové komunikace

Při tomto typu útoků pachatel užívá metody „Sniffing“[30], která spočívá v neoprávněném odposlouchávání komunikace na síti. Pachatelem tak mohou být odposlechnuty přihlašovací údaje do různých webových služeb, jejichž zabezpečení bylo administrátory zanedbáno. Pokud uživatel zadává své heslo na webových stránkách, které nevyužívají šifrovaného spojení, může být jeho heslo snadno odposlechnuto. Stránky bez šifrovaného spojení začínají takto: http, se šifrovaným spojením https.

4.4.4 Využití neukončeného spojení

„Pachatel využije toho, že se uživatel zapomeneme odhlásit ze systému. Některé stránky se proti takovým útokům chrání automatickým ukončením spojení při nečinnosti cca. 15 minut“[31].

4.4.5 Útok zadními vrátky

Pachatel pro tuto svojí činnost užije nebo napíše počítačový program nazývaný „Backdoor“[32], který mu umožní připojit se do systému bez nutnosti znalosti zabezpečovacího zařízení v podobě uživatelského jména a hesla. Backdoor je povětšinou součástí počítačového viru nazvaný „Trojský kůň“[33], který se do počítače oběti dostane buď užitím cracku ke zprovoznění nelegálního software, nebo v podobě instalace na první

[29] JIRKOVSKÝ, V. *Kybernetická kriminalita nejen o hackingu, virech a trojských koních bez tajemství*. Praha, Grada Publishing, a.s., 2007, s. 62.
[30] JIRKOVSKÝ, V. *Kybernetická kriminalita nejen o hackingu, virech a trojských koních bez tajemství.* Praha, Grada Publishing, a.s., 2007, s. 65-66.
[31] JIRKOVSKÝ, V. *Kybernetická kriminalita nejen o hackingu, virech a trojských koních bez tajemství*. Praha, Grada Publishing, a.s., 2007, s. 67.
[32] JIRKOVSKÝ, V. *Kybernetická kriminalita nejen o hackingu, virech a trojských koních bez tajemství*. Praha, Grada Publishing, a.s., 2007, s. 63.
[33] JIRKOVSKÝ, V. *Kybernetická kriminalita nejen o hackingu, virech a trojských koních bez tajemství*. Praha, Grada Publishing, a.s., 2007, s. 67.

pohled neškodného reklamního banneru. Poté, co se Backdoor dostane do počítače oběti, má pachatel celý tento počítačový systém i s jeho daty k volné dispozici.

4.4.6 Zachycení hesla

Pachatel pro tuto svoji činnost užije nebo napíše počítačový program nazývaný „Keylogger“[34], který zaznamenává stisknuté klávesy. Získané údaje v reálném čase odesílá cestou šifrovaného spojení zpět pachateli, kterému se tak dostávají do ruky přihlašovací údaje k internetovému bankovnictví, herním klientům typu Steam, přístupy na sociální sítě a do e-mailových schránek obětí. Keylogger je stejně tak jako Backdoor součástí počítačového viru typu Trojský kůň.

4.5 Útoky bez nutnosti překonání zabezpečovacího zařízení

Porušit integritu dat uložených v počítačových systémech mohou pachatelé i tím, že již mají přístup k počítačovému systému, kde se nacházejí data, na která chtějí zaútočit. Okruh pachatelů tohoto typu počítačové kriminality se rekrutuje z řad zaměstnanců různých společností, kteří pro výkon svého zaměstnání obdrží přístup do počítačového systému společnosti, kde jsou zaměstnáni. Motivem pachatelů pro páchání tohoto typu počítačové kriminality je v tomto případě krádež dat pro jejich následný prodej nebo osobní využití. Dalším motivem je zničení nebo změna těchto dat tak, aby zaměstnavatel tato data již nemohl dále využívat. Pro pachatele této trestné činnosti zpravidla platí společný znak, že se jedná o doposud bezúhonné občany bez kriminální minulosti. Ke spáchání uvedených činů jsou buď přesvědčeni jinou osobou, nebo se této trestné činnosti dopustí z pro ně morálně omluvitelných důvodů. U tohoto typu kriminality je vysoká objasněnost. Zpracovateli práce se za devět let působení na SKPV nestalo, aby v těchto případech nedošlo k ustanovení pachatele, sdělení obvinění a následnému pravomocnému odsouzení pachatele nebo k odklonu od trestního řízení po nahrazení škody, či odstranění jiného škodlivého následku.

[34] JIRKOVSKÝ, V. *Kybernetická kriminalita nejen o hackingu, virech a trojských koních bez tajemství.* Praha, Grada Publishing, a.s., 2007, s. 67.

4.5.1 Krádež dat uložených v počítačových systémech

Nejčastějšími příčinami krádeží dat v počítačových systémech, ke kterým mají pachatelé přístup v souvislosti se svým pracovním zařazením, dochází z toho důvodu, že pachatele buď osloví konkurenční společnost jeho zaměstnavatele, která má zájem o know-how zaměstnavatele pachatele, nebo sám chce začít podnikat na stejném segmentu trhu jako jeho zaměstnavatel. Pachatel, pokud má dostatečná oprávnění se k datům dostat (většina firem neřeší oprávnění uživatelů a přiděluje jim přístupy s administrátorským oprávněním), taková data ze systému vyexportuje, uloží na externí USB Disk, který následně předá konkurenční společnosti, nebo takto vyexportovaná data rovnou odešle e-mailem z pracovního počítače.

Ke krádežím dat uloženým v počítačových systémech dochází dále z toho důvodu, že pachatel zpracovává různé databáze klientů např. ve společnostech zabývajících se finančním poradenstvím nebo realitních kancelářích, tedy ve společnostech, kde je velká poptávka po zákaznících a tyto společnosti si „přetahují“ zákazníky všemi možnými způsoby. Pachatel je osloven konkurencí, nebo si sám chce založit podnikání na stejném segmentu trhu, proto databázi vyexportuje a výše popsaným způsobem buď předá další osobě, nebo data sám užije.

4.5.2 Změny nebo zničení dat uložených v počítačových systémech

Pachatelé tohoto typu počítačové kriminality, jsou povětšinou osoby, kterým končí pracovní poměr u zaměstnavatele, do jehož počítačového systému mají přístup. Data, která jsou ničena nebo měněna, bývají většinou data, která do počítačového systému zadal sám pachatel, který je považuje za vlastní, chce tato data dále využívat i po skončení pracovního poměru u zaměstnavatele, do jehož počítačového systému data uložil. Pachatel tedy po přístupu do počítačového systému např. pozmění telefonní čísla na klienty, nebo e-mailové adresy, anebo rovnou data vymaže. K vymazání nebo zničení dat se pachatel většinou neuchýlí, neboť by velmi brzy vyšlo najevo, že data byla zničena. Pachatelé tohoto typu počítačové kriminality se obyčejně hájí tím, že osoby vedené v databázích chtějí i po skončení pracovního poměru pachatele jednat pouze s ním a nepřejí si, aby je oslovoval někdo jiný ze společnosti, ve které byl pachatel zaměstnán.

4.6 Trestněprávní postih neoprávněným přístupům do počítačových systémů

S rozvojem komunikačních technologií došlo k masivnímu nástupu počítačové kriminality, kterou nebylo možno postihovat dle původních osvědčených postupů. Počítačová kriminalita se převážně odehrává *v* „novém sociálně interaktivním prostředí, jehož specifikum spočívá především v neexistenci časových a prostorových bariér, mnohonásobné konektivitě, anonymitě a možnostech změny on-line identity, což vytváří nové formy a zákonitosti závadného jednání, které jsou kvalitativně odlišné od jiných druhů kriminality"[35]. Na tuto skutečnost reagovalo mnoho zemí změnami v legislativě svých dosavadních trestněprávních norem. Česká republika nebyla v tomto případě výjimkou a v novém Trestním zákoníku na „tyto trendy reaguje a přichází s moderní a komplexní ochranou počítačových dat a systémů"[36]. „Převážná část trestných činů proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů je zasazena do hlavy V. o trestných činech proti majetku. Jedná se o tyto trestné činy:

1. Neoprávněný přístup k počítačovému systému a nosiči informací dle § 230 TZ.

2. Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat dle § 231 TZ.

3. Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti dle § 232 TZ.

4. Porušení tajemství dopravovaných zpráv dle § 182 TZ.

4.6.1 Neoprávněný přístup k poč. systému a nosiči informací

V tomto ustanovení trestního zákoníku jsou v prvním a druhém odstavci obsaženy dvě základní skutkové podstaty trestného činu. Naplněním podmínek uvedených v odstavcích 3, 4, 5 je přitěžující a zvlášť přitěžující okolností, která podmiňuje užití vyšší trestní sazby.

[35] ŠÁMAL, P. a kol. *Trestní zákoník. 1. vydání,* Praha, C.H.Beck, 2009, s. 2084 - 2085.
[36] ŠÁMAL, P. a kol. *Trestní zákoník. 1. vydání,* Praha, C.H.Beck, 2009, s. 2085.

Z odstavce jedna vyplývá, že „kdo překoná bezpečnostní opatření a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán“[37]. Tímto ustanovením je chráněn počítačový systém jako takový. Z uvedeného ustanovení tedy vyplývá, že je trestný již samotný neoprávněný přístup k počítačovému systému nebo k jeho části. Pro tento typ útoku se užívá mezinárodní označení „Hacking a pro pachatele označení Hacker“[38]. Podmínkou trestnosti je překonání bezpečnostního opatření pachatelem. Tato skutková podstata trestného činu neobsahuje znak v podobě úmyslu způsobit škodu, jinou újmu nebo získat neoprávněný prospěch. „Bezpečnostním opatřením je třeba rozumět každé opatření, jehož cílem je zabránit volnému přístupu k počítačovému systému nebo nosiči informací“[39]. Z hlediska trestního práva nezáleží na úrovni zabezpečení, pro trestnost činu je rozhodující, že počítačový systém je nějakým způsobem zabezpečen a pachatel toto zabezpečení překonal.

Z odstavce dvě vyplývá, že „kdo získá přístup k počítačovému systému nebo k nosiči informací a a) neoprávněně užije data uložená v tomto počítačovém systému nebo na nosiči informací, b) data uložená v tomto 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 nosiči informací nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat, bude potrestán“[40]. Tímto ustanovením je poskytována ochrana počítačovým datům, před neoprávněnými zásahy, kterými by mohlo dojít k jejich poškození, změně nebo k jejich neoprávněnému užívání. Podmínkou trestnosti pachatele je získání přístupu k počítačovému systému a naplnění alespoň jedné z podmínek, které jsou uvedeny pod písmeny a, b, c, d. Tato skutková podstata trestného činu neobsahuje znak v podobě úmyslu způsobit škodu, jinou újmu nebo získat neoprávněný prospěch. „Získáním přístupu se zde rozumí takové jednání, které umožní pachateli volnou dispozici s počítačovým systémem nebo nosičem informací a využití jeho informačního obsahu“[41].

[37] ŠÁMAL, P. a kol. Trestní zákoník. 1. vydání, Praha, C.H.Beck, 2009, s. 2081.
[38] JIRKOVSKÝ, V. *Kybernetická kriminalita nejen o hackingu, virech a trojských koních bez tajemství*. Praha, Grada Publishing, a.s., 2007, s. 47 - 52.
[39] ŠÁMAL, P. a kol. Trestní zákoník. 1. vydání, Praha, C.H.Beck, 2009, s. 2088.
[40] ŠÁMAL, P. a kol. *Trestní zákoník. 1. vydání, Praha*, C.H.Beck, 2009, s. 2081 - 2082.
[41] ŠÁMAL, P. a kol. *Trestní zákoník. 1. vydání, Praha*, C.H.Beck, 2009, s. 2089.

Přístup k počítačovému systému může pachatel získat např. v souvislosti s jeho zaměstnáním, náhodou, nebo odcizením nosiče informací, na kterém je přístup do počítačového systému uložen. Nosičem informací se rozumí takové médium, na které lze informace zapsat a následně je z tohoto média přečíst. „Za nosič informací je považován Hard disk počítače, operační paměť počítače RAM, USB disk, CD/DVD/Blue-Ray, ale např. i mobilní telefon“[42].

V mnoha případech tohoto typu počítačové kriminality dochází k naplnění obou výše popsaných základních skutkových podstat trestného činu dle § 230 TZ. V drtivé většině případů pachatel nejprve překoná bezpečnostní opatření počítačového systému nebo jeho části, aby mohl následně neoprávněně manipulovat s daty uloženými v počítačovém systému, ke kterému získal neoprávněně přístup.

4.6.2 Opatření a přechovávání přístupového zařízení a hesla

Z tohoto ustanovení vyplývá, že „Kdo v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) trestního zákoníku nebo trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1, 2 trestního zákoníku vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části, nebo b) počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části, bude potrestán“[43]. Uvedené ustanovení je zvláštní formou přípravy ke shora popsaným trestným činům a jeho cílem je uzákonění trestněprávního postihu popsaného jednání, neboť dle ustanovení § 20 odst. 1 TZ, by příprava ke shora popsaným trestným činům nebyla trestná. Je třeba mít na paměti, že samotné opatřování a přechovávání přístupových zařízení není trestné, pokud jimi pachatel nedisponuje v úmyslu spáchat výše pospané trestné činy. Opatřování a přechovávání přístupových zařízení může být

[42] ŠÁMAL, P. a kol. *Trestní zákoník. 1. vydání, Praha*, C.H.Beck, 2009, s. 2090.
[43] ŠÁMAL, P. a kol. *Trestní zákoník. 1. vydání, Praha*, C.H.Beck, 2009, s. 2097.

prováděno i v souvislosti se zaměstnáním osob, kdy jsou přístupová zařízení a hesla shromažďována z důvodu vykonávané práce danou osobou.

4.6.3 Poškození záznamu v poč. systému z nedbalosti

Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti je vymezeno v § 232 TZ. Z tohoto ustanovení vyplývá, že „kdo z „hrubé nedbalosti“[44] porušením povinnosti vyplývající ze zaměstnání, povolání, postavení nebo funkce nebo uložené podle zákona nebo smluvně převzaté a) data uložená v počítačovém systému nebo na nosiči informací zničí, poškodí, pozmění nebo učiní neupotřebitelnými, nebo b) učiní zásah do technického nebo programového vybavení počítače nebo jiného technického zařízení pro zpracování dat a tím způsobí na cizím majetku značnou škodu, bude potrestán“[45]. „Jednání pachatele odpovídá v zásadě jednání vymezenému v § 230 odst. 2 písm. b) a d) TZ“[46]. U tohoto trestného činu je nad rámec výše popsaného vymezení vyžadováno, aby ke spáchání tohoto trestného činu došlo v důsledku porušení povinností vyplývající z funkce nebo zaměstnání osoby a tímto činem byla způsobena značná škoda na cizím majetku. Zpracovatel této práce se s uvedeným trestným činem ještě nesetkal a není mu známo, že by byl vydán rozsudek na shora popsaný způsob jednání. V tomto bodě se však autor práce rozchází v názoru uvedeném v komentáři k trestnímu zákoníku, k této skutkové podstatě, ve kterém je uvedeno „Kriminalizace nedbalostní formy zavinění je v tomto případě diskutabilní“[47]. Autor práce se neztotožňuje s tím, že kriminalizace popsaného jednání je diskutabilní. Současný stav společnosti je takový, že mnoho jedinců nerespektuje povinnosti, které pro ně vyplývají ze smluv nebo jsou obecně závazné. Je všeobecně známo, že osoby, které pracují na firemních výpočetních stanicích, nerespektují směrnice, které v souvislosti s prací na těchto počítačích byly podepsány. Často i přes zákaz stahují nelegální obsah, neoprávněně instalují software apod. Pokud by se tedy teoreticky stalo, že se zaměstnanec nebude řídit podepsanou směrnicí, v rozporu s touto směrnicí stáhne do pracovního

[44] *Hrubou nedbalostí* se rozumí vyšší stupeň intenzity nedbalosti, ať již vědomé či nevědomé, a to na základě přístupu (postoje) pachatele k požadavku náležité opatrnosti, kterou zákon charakterizuje jako „zřejmou bezohlednost“. Tato definice je potřebná, neboť některé trestné činy jsou stíhatelné jen v případě tzv. hrubé nedbalosti. In: ŠÁMAL, P. a kol. *Trestní zákoník. 1. vydání, Praha*, C.H.Beck, 2009, s. 187.

[45] ŠÁMAL, P. a kol. *Trestní zákoník. 1. vydání, Praha*, C.H.Beck, 2009, s. 2103.
[46] ŠÁMAL, P. a kol. *Trestní zákoník. 1. vydání, Praha*, C.H.Beck, 2009, s. 2104.
[47] ŠÁMAL, P. a kol. *Trestní zákoník. 1. vydání, Praha*, C.H.Beck, 2009, s. 2104.

počítače nějaký soubor, k němuž bude přiřazen malware, který způsobí zcizení a následné nenávratné zničení dat, pak by se dalo postupovat v souladu s ustanovením § 232 TZ. Při posuzování těchto případů je třeba postupovat s vědomím, že povinnými znaky této SPTČ je způsobení značné škody z hrubé nedbalosti. Nelze tedy kriminalizovat každého, kdo shora popsaným způsobem poškodí počítačový systém společnosti ve které pracuje, ale pouze pachatele v důsledku jeho jednání došlo ke způsobení minimální škody 500.000,- Kč. Pokud pachatel svým jednáním nezpůsobí značnou škodu, je třeba odkázat poškozeného, aby se svých práv domohl dle jiného právního předpisu v souladu se zásadou subsidiarity trestní represe[48].

4.6.4 Porušení tajemství dopravovaných zpráv

V ustanovení dle § 182 TZ jsou v prvním a druhém odstavci obsaženy dvě základní skutkové podstaty trestného činu a v odstavci 5 zvláštní skutková podstata trestného činu. Naplnění podmínek uvedených v odstavcích 3, 4, 6 je přitěžující a zvlášť přitěžující okolností, která podmiňuje užití vyšší trestní sazby. Předmětem ochrany je zde tajemství uzavřeného listu nebo jiné písemnosti, ale i neveřejný přenos počítačových dat do počítačového systému z něj nebo v jeho rámci. Pro potřeby této bakalářské práce bude autor popisovat pouze náležitosti týkající se počítačové kriminality.

Z odstavce jedna vyplývá, „kdo úmyslně poruší tajemství b) datové, textové, hlasové, zvukové či obrazové zprávy posílané prostřednictvím sítě elektronických komunikací a přiřaditelné k identifikovanému účastníku nebo uživateli, který zprávu přijímá, nebo c) neveřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému, přenášejícího taková počítačová data, bude potrestán“[49]. Tato skutková podstata trestného činu chrání samotné porušení tajemství dopravovaných zpráv posílaných sítí elektronických komunikací a neveřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci. „Porušením tajemství se rozumí jakékoli neoprávněné narušení přepravované písemnosti, posílané zprávy nebo neveřejného přenosu

[48] *Zásada subsidiarity trestní represe* – ze které vyplývá princip *ultima ratio*, který v podstatě znamená, že trestní právo je nejkrajnější prostředek a že trestní odpovědnost pachatele a trestněprávní důsledky s ní spojené lze uplatňovat jen v případech společensky škodlivých, ve kterých nepostačuje uplatnění odpovědnosti podle jiných právních předpisů. NOVOTNÝ, F, SOUČEK, J. et al. *Trestní právo hmotné*. 3. vydání. Plzeň : Aleš Čeněk., 2010. s. 17.

[49] ŠÁMAL, P. a kol. *Trestní zákoník. 1. vydání, Praha*, C.H.Beck, 2009, s. 1622.

počítačových dat podle písm. a) až c) odst. 1 se snahou zjistit jejich obsah, aniž by tento obsah musel být někomu dalšímu sdělen. Porušení tajemství se tedy může vyčerpat jen vlastním zásahem narušitele, aniž by se s obsahem písemnosti, posílané zprávy nebo neveřejného přenosu počítačových dat seznámila další osoba“[50]. Za dopravovanou zprávu je ve smyslu tohoto ustanovení považována, textová, hlasová nebo obrazová zpráva zaslaná pomocí Internetu jako e-mail, dále zprávy zasílané cestou různých komunikačních aplikací např. Skype, nebo cestou sociálních sítí např. Facebook.

Z odstavce dva vyplývá, že „stejně bude potrestán, kdo v úmyslu způsobit jinému škodu nebo opatřit sobě nebo jinému neoprávněný prospěch a) prozradí tajemství, o němž se dozvěděl z písemnosti, telegramu, telefonního hovoru nebo přenosu prostřednictvím sítě elektronických komunikací, který nebyl určen jemu, nebo b) takového tajemství využije“[51]. Tato SPTČ chrání tajemství dopravované zprávy, které se pachatel dozvěděl, zpráva nebyla určena jemu a pachatel tajemství této zprávy vyzradil. „Prozrazením tajemství se rozumí sdělení (písemné nebo ústní) obsahu písemnosti nebo zprávy jiné osobě než té, které byly určeny (adresátovi)[52]. Využití tajemství je zde chápáno ve smyslu uplatnění znalosti tajemství ke způsobení škody jinému, nebo k opatření neoprávněného prospěchu pachatele.

Z odstavce pět vyplývá, „zaměstnanec provozovatele poštovních služeb, telekomunikační služby nebo počítačového systému anebo kdokoli jiný vykonávající komunikační činnosti, který a) spáchá čin uvedený v odstavci 1 nebo 2, b) jinému úmyslně umožní spáchat takový čin, nebo c) pozmění nebo potlačí písemnost obsaženou v poštovní zásilce nebo dopravovanou dopravním zařízením anebo zprávu podanou neveřejným přenosem počítačových dat, telefonicky, telegraficky nebo jiným podobným způsobem, bude potrestán“[53]. Tato zvláštní skutková podstata trestného činu postihuje zaměstnance telekomunikační služby nebo počítačového systému a obsahuje kvalifikovanou skutkovou podstatu trestného činu, která podmiňuje použití vyšší trestní sazby, neboť uvedení zaměstnanci mají zvláštní postavení pachatele. Dále se jedná o samostatnou základní skutkovou podstatu trestného činu tím, že povyšuje jednání výše uvedeného zaměstnance, které by bylo jinak kvalifikováno jako účastenství na trestném činu, ve formě pomoci k spáchání tohoto činu uvedeného v odstavci 1 nebo 2, na

[50] ŠÁMAL, P. a kol. *Trestní zákoník. 1. vydání, Praha*, C.H.Beck, 2009, s. 1626.
[51] ŠÁMAL, P. a kol. *Trestní zákoník. 1. vydání, Praha*, C.H.Beck, 2009, s. 1622.
[52] ŠÁMAL, P. a kol. *Trestní zákoník. 1. vydání, Praha*, C.H.Beck, 2009, s. 1622.
[53] ŠÁMAL, P. a kol. *Trestní zákoník. 1. vydání, Praha*, C.H.Beck, 2009, s. 1622 - 1623.

pachatelství. Z výše uvedeného tedy vyplývá, že pachatelem popsaného činu může být jen zaměstnanec telekomunikační služby nebo počítačového systému.

5 Podvody v počítačové síti Internet

V této kapitole bakalářské práce se bude autor zabývat počítačovou kriminalitou spáchanou za užití počítačů a počítačové sítě. Počítačová síť Internet vzhledem ke své relativní anonymitě pachatelů nabízí mnoho možností pro tyto pachatele, jak se dopouštět společensky škodlivých jednání formou uvedení obětí v omyl. Všechna podvodná jednání spáchaná v síti Internet mají společného jmenovatele v podobě nějaké podvodné nabídky na prodej zboží, služeb nebo nové verze internetového bankovnictví. Cílem pachatelů tohoto typu počítačové kriminality je především dosažení zisku, to ale neplatí vždy. Tento typ trestné činnosti je především založen na důvěře a naivitě obětí a zpravidla končí vždy stejně, tedy tím, že oběť odešle finanční prostředky v domnění, že platí za zboží, které jí bude doručeno nebo za službu, neznámému prodejci. Ne všechny podvodné nabídky na počítačové síti Internet však slouží k bezprostřednímu obohacení pachatele o finanční prostředky oběti. V některých případech pachatelé na Internet umísťují falešné nabídky, aby se dostali k nástroji pro páchání další trestné činnosti, spadající do počítačové kriminality.

5.1 Falešné inzeráty na prodej zboží

Nejčastějším typem podvodného jednání na počítačové síti Internet jsou nabídky prodeje zboží na inzertních portálech typu Aukro, Zboží.cz, Bazoš apod. Pachatel takové trestné činnosti na inzertní portál umístí inzerát s textem, ve kterém nabízí nejčastěji mobilní telefony, ale i jiný druh zboží, za výrazně nižší ceny, než jsou v obchodech. Podmínkou zaslání zboží je platba za toto zboží předem na zaslaný účet pachatele, nebo odeslání platebních prostředků některým z platebních portálů typu PayPal. V těchto případech pachatel na inzertním portálu vystupuje pod změněnou identitou, kdy oběti neváhá zaslat oskenované doklady cizí osoby, které získal např. v souvislosti s jinou trestnou činností, aby oběť uvěřila, že se jedná o skutečného prodejce. Po krátké e-mailové komunikaci mezi pachatelem a obětí, která probíhá z předem připravených e-mailových schránek pachatele, dojde k dohodě a oběť odešle finanční prostředky shora pospaným jednáním. V některých případech oběť dokonce obdrží od pachatele balík, který vypadá, jako by obsahoval skutečné objednané zboží. Pachatel se k odeslání balíku uchyluje tehdy, když po něm oběť požaduje fotografii balíku před odesláním a dále číslo

pro sledování poštovní zásilky. Po přijetí balíku a jeho rozbalení však oběť zjistí, že místo slíbeného mobilního telefonu se v balíku nachází např. úlomek cihly nebo jiná věc nulové hodnoty.

5.2 Falešné e-shopy

Počítačová síť Internet nabízí nepřeberné množství možností, jak může pachatel potencionální oběť uvést v omyl a získat tak neoprávněně prospěch. Velmi rozšířenou činností je zakládání falešných e-shopů. Na těchto e-shopech je umístěno nejžádanější zboží na trhu za výrazně nižší ceny, než je na běžných e-shopech. Falešné e-shopy se dělí na obchody, ve kterých lze nakoupit různý sortiment zboží, nebo na speciální obchody např. s dětskými potřebami. Podmínkou zakoupení zboží na těchto e-shopech je platba dopředu, na zveřejněný účet, nebo zaslání finančních prostředků prostřednictvím finančních bran typu Pay Pal. Oběť si vybere domnělé zboží, odešle finanční prostředky a zboží nikdy neobdrží.

5.3 Podvodné nabídky půjček finančních prostředků

K této trestné činnosti pachatelé užívají inzertních portálů typu Aukro, Zboží.cz, Bazoš apod. Na uvedených inzertních portálech pachatel inzeruje nabídku finanční půjčky bez nahlížení do registrů dlužníků. V uvedených typech inzerátů bývá uvedeno, že pachatel zastupuje smyšlenou společnost, která nabízí finanční půjčky a podmínkou získání půjčky je odeslání kopie občanského průkazu na uvedenou emailovou adresu z důvodu prověření klienta. Další podmínkou získání půjčky je odeslání finanční částky nepřesahující 2.000,- Kč na uvedené číslo účtu. Částky jsou pachatelem určovány dle výše půjčky. Odeslání finančních prostředků je pachatelem zdůvodňováno tím, že žadatel tak prokáže svoji bonitu a odeslaná částka bude brána jako první splátka sjednané půjčky. Pachatel s obětí komunikuje emailem, kde oběti sdělí, že jí půjčka bude poskytnuta do několika hodin od připsání odeslané částky na účet pachatele. Pachatel slíbí oběti, že jakmile bude částka připsána na jeho účet, do dvou hodin oběť na jí uvedené adrese kontaktuje obchodní zástupce, který jí přiveze finanční prostředky a smlouvu na uvedenou půjčku. Žádný obchodní zástupce však oběť nekontaktuje a žádné finanční prostředky nejsou oběti vyplaceny. U tohoto typu podvodů je velká latentnost, neboť oběti jednání pachatelů ani nehlásí. Jak bylo uvedeno výše, maximální částka, která je

pachatelem požadována je 2.000,- Kč, mnohdy se však jedná o částky nepřesahující 500,- Kč, kdy oběti uvedenou částku oželí a věc neoznámí Policii ČR.

Tohoto typu počítačové kriminality se však pachatelé nedopouštějí pouze v úmyslu získat pro sebe neoprávněný prospěch, ale i v úmyslu zmocnit se kopií dokladů obětí, které pak užijí k další trestné činnosti. Nejčastěji pachatelé užijí takto získaných dokladů k založení účtů u bank, které umožňují založit účet vzdáleně a přes takto založený účet zasílají finanční prostředky pocházející z jiné trestné činnosti. Nejčastěji se jedná o finanční prostředky pocházející z různých podvodů s falešnými e-shopy, nebo falešnými inzeráty.

5.4 Podvodné stránky internetového bankovnictví

Cílem této trestné činnosti je získání přístupových údajů do internetového bankovnictví obětí. Pachatelé zpravidla na sociální síti vytvoří falešný profil některé z bank a lákají oběti na přechod do nového typu internetového bankovnictví, které oběti naleznou na profesionálně vytvořené falešné stránce internetového bankovnictví. Jako lákadlo k domnělému přechodu na novější verzi bankovnictví je nějaká finanční odměna za tento přechod. Pachatelem vytvořená falešná webová stránka k internetovému bankovnictví je věrnou kopií skutečné webové stránky banky a je na první pohled k nerozeznání od skutečné webové stránky banky. Jediný viditelný rozdíl je v názvu domény. Například webová stránka internetového bankovnictví od České spořitelny, a.s. je servis24.cz, podvodná webová stránka má název domény např. servis24.ic.cz. Pokud si oběť nezkontroluje domény nebo se nechá nalákat na zisk nějaké finanční odměny a vyplní na podvržené webové stránce své údaje k internetovému bankovnictví, odevzdá tímto své přihlašovací údaje pachateli, který má tak volnou dispozici s účtem oběti. Obětí se však může stát i nepozorný uživatel, aniž by byl ovlivněn nějakým falešným profilem na sociální síti. Mnoho uživatelů internetového bankovnictví nedbá na bezpečnost, do internetového bankovnictví se přihlašuje tak, že do vyhledávače zadá název banky a do prvního odkazu, který mu vyhledávač poskytne, slepě vyplní údaje, aniž by zkontroloval doménu. Pachatelé této trestné činnosti jsou schopni docílit toho, aby jimi vytvořená falešná webová stránka byla např. ve vyhledávači google.com zobrazována na prvním místě před skutečnou stránkou banky.

5.5 Podvodné nabídky práce

Pácháním této trestné činnosti se pachatelé fyzicky dostávají k finančním prostředkům, kterých se zmocnili jinou trestnou činností v prostředí Internetu. Pachatel, který ví, že se zmocní finančních prostředků z účtu oběti, potřebuje k dokonání svého činu nějaký prostředek, přes který se k penězům dostane. Z toho důvodu pachatel zveřejní inzerát s nabídkou práce, která spočívá v tom, že si další osoba u některé z pachatelem navržených bank založí účet a číslo účtu zašle pachateli. Pachatel na tento účet odešle finanční prostředky, které získal z trestné činnosti. Osoba, která účet založila, následně prostředky vybere a cestou některé společnosti, např. Western Union, je odešle na danou adresu. Osobě, která na inzerát odpoví je pachatelem zaslána pracovní smlouva, která v této osobě má vyvolat pocit, že se jedná o legální činnost. U těchto typů případů není jasně dána soudní praxe, neboť v některých případech jsou osoby, které shora popsané vykonají, stíhány a odsouzeny pro trestný čin podílnictví z nedbalosti dle § 215 trestního zákoníku, v některých případech jsou tato jednání odložena již Policií ČR, nebo u soudu dochází ke zproštění obžaloby, neboť zde došlo k uvedení v omyl osoby tím, že jí bylo sděleno, že vykonává legální činnost a s danou osobou byla uzavřena smlouva na provádění této činnosti, takže si osoba myslela, že skutečně jedná v souladu se zákony.

5.6 Trestně právní postih podvodného jednání na Internetu

Shora popsaná jednání pachatelů lze postihovat dle několika ustanovení trestního zákoníku. Taková jednání pachatelů mají ve všech případech jeden společný znak, kterým je uvedení oběti v omyl. Oběti jsou zde primárně uváděny v omyl z toho důvodu, aby se pachatel na jejich úkor neoprávněně obohatil.

Ne všechna uvedení v omyl obětí však slouží k přímému obohacení pachatele o finanční prostředky oběti. Mnohdy jsou oběti uváděny v omyl proto, aby pachatel díky omylu oběti získal nástroj pro páchání další trestné činnosti v prostředí Internetu tak, že na základě falešné nabídky finanční půjčky vyláká od oběti doklady, které užije např. k založení účtů u některé z bank přes internet, kdy následně přes tento účet přepošle finanční prostředky, které získal jinou trestnou činností.

Většina podvodných jednání na Internetu je zasazena do hlavy V. trestního zákoníku, trestné činy proti majetku. Jedná se o tyto trestné činy:

1. Podvod dle § 209 TZ.

2. Poškození cizích práv dle § 181 TZ.

3. Podílnictví z nedbalosti dle § 215 TZ.

5.6.1 Podvod

Z tohoto ustanovení vyplývá, že „kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán“[54]. Předmětem ochrany tohoto ustanovení trestního zákoníku je tedy majetek, kdy vlastnictví majetku je jedním ze základních lidských práv. Uvedením oběti v omyl je myšleno, že „uvedení v omyl nebo využití omylu, popř. zamlčení podstatných skutečností, může směřovat nejen vůči poškozenému, ale i vůči jiné osobě. Omyl je rozpor mezi představou a skutečností. O omyl půjde i tehdy, když podváděná osoba nemá o důležité okolnosti žádnou představu nebo se domnívá, že se nemá čeho obávat. Omyl se může týkat i skutečností, které teprve mají nastat, pachatel však musí o omylu jiného vědět již v době, kdy dochází k jeho obohacení“[55]. Výše popsaným jednáním je tedy oběť uvedena v omyl tím, že platí za zboží, které jí bude doručeno, sjednává finanční půjčku, kdy je již dopředu jasné, že jí půjčka poskytnuta nebude, nebo si myslí, že se přihlašuje ke skutečnému internetovému bankovnictví. Tedy shora popsaným jednáním pachatel uvádí své oběti v omyl tím, že „předstírá okolnosti, které nejsou v souladu se skutečným stavem věci“[56]. V tomto případě pachatel uvádí oběti v omyl přímým konáním tak, že vytváří prostředky a nepravdivé informace, kterými oběť obelstí, kdy spoléhá na to, že si oběť pachatelem uvedené nepravdivé informace nijak neověří.

5.6.2 Poškození cizích práv

Z tohoto ustanovení vyplývá, že „kdo jinému způsobí vážnou újmu na právech tím, že uvede někoho v omyl, nebo využije něčího omylu, bude potrestán“[57]. V této

[54] ŠÁMAL, P. a kol. *Trestní zákoník. 1. vydání, Praha*, C.H.Beck, 2009, s. 1850.
[55] ŠÁMAL, P. a kol. *Trestní zákoník. 1. vydání, Praha*, C.H.Beck, 2009, s. 1853 - 1854.
[56] ŠÁMAL, P. a kol. *Trestní zákoník. 1. vydání, Praha*, C.H.Beck, 2009, s. 1854.
[57] ŠÁMAL, P. a kol. *Trestní zákoník. 1. vydání, Praha*, C.H.Beck, 2009, s. 1616.

skutkové podstatě jsou primárně chráněna nemajetková práva oběti. Jednání pachatele má v tomto případě povahu podvodného jednání, tedy uvedení oběti v omyl, nebo využití omylu. Oproti klasickému podvodu však není povinným znakem této skutkové podstaty způsobení minimální škody, ale vážné újmy na právech. Vážnou újmu na právech je třeba posuzovat „se zřetelem k okolnostem konkrétního případu, zejména s přihlédnutím k tomu, o jaké právo a v jaké oblasti společenských vztahů šlo, jaká byla intenzita újmy na zasaženém právu a jaké následky to mělo pro poškozeného, zejména zda šlo o poškození na právech lehce nebo obtížně odstranitelný“[58]. Pokud tedy pachatel uvede oběť v omyl tím, že nabízí finanční půjčku, na základě této nabídky od oběti vyláká doklady, které poté užije k založení bankovního účtu bez vědomí oběti, na takto založený bankovní účet dále převede finanční prostředky získané jinou trestnou činností, poškodí na právech oběť tím, že poté, co je uvedený účet zablokován Finančně analytickým útvarem Ministerstva financí ČR pro podezření z trestné činnosti, je osoba, na níž byl účet založen, automaticky zařazena mezi rizikové klienty bank, čímž je jí znemožněno požadovat bankovní produkty jako jsou úvěry, hypotéky apod.

5.6.3 Podílnictví z nedbalosti

Z dikce tohoto ustanovení vyplývá, že „kdo ukryje nebo na sebe nebo jiného převede z nedbalosti věc nebo jinou majetkovou hodnotu nikoli malé hodnoty, která byla získána trestným činem spáchaným na území České republiky nebo v cizině jinou osobou, nebo jako odměna za něj, bude potrestán“[59]. Z uvedeného vyplývá, že pachatelem tohoto trestného činu je jiná osoba, než je pachatel primárního trestného činu. Pro potřeby této bakalářské práce se jedná o osobu, která si na základě falešného inzerátu s nabídkou zaměstnání a fingované pracovní smlouvy založí bankovní účet, na tento účet jsou jí zaslány finanční prostředky, které pachatel získal trestnou činností. Osoba, která účet založila dle instrukcí z pracovní smlouvy, došlé finanční prostředky vybere a odešle pachateli. V tomto případě se uvedená osoba dopustí trestného činu podílnictví z nedbalosti, i když „nevěděla, že svým jednáním může takové porušení nebo ohrožení způsobit, ač o tom vzhledem k okolnostem a k svým osobním poměrům vědět měla a mohla“. Jak bylo uvedeno výše, je otázka odpovědnosti osoby pachatele v tomto případě diskutabilní, neboť se povětšinou jedná o osoby, které se nedokáží uplatnit na trhu práce.

[58] ŠÁMAL, P. a kol. *Trestní zákoník. 1. vydání, Praha*, C.H.Beck, 2009, s. 1617.
[59] ŠÁMAL, P. a kol. *Trestní zákoník. 1. vydání, Praha*, C.H.Beck, 2009, s. 1938.

Jedná se o osoby v předdůchodovém věku, samoživitelky apod. Tyto osoby jsou ve špatné finanční situaci, kdy pod tíhou reality jejich skutečného života a malé šance na uspokojení svých potřeb často nerozliší nebo si nepřipustí, že by se popsaným jednáním mohly dopustit trestného činu. I z toho důvodu je na území ČR v těchto případech výše zmíněná právní nejistota, protože každý jednotlivý státní zástupce na věc nahlíží jinak. Některý nařídí věc stíhat, jiný nařídí věc odložit a naopak mezi poškozené pachatelovým jednáním zařadit i osobu, která si účet založila, neboť byla uvedena v omyl tím, že se jedná o skutečné zaměstnání a jednáním pachatele jí byla způsobena závažná újma na právech.

6 Ostatní formy kriminality páchané za užití počítačů

Internet a jeho dostupnost, která má za následek rozvoj různých diskusních fór a sociálních sítí, není využíván jen pro dobro společnosti. Komunikační technologie daly pachatelům do rukou velmi silný nástroj, jak útočit na své oběti. Tato skutečnost se promítla i do rekodifikace trestního zákona, v podobě nových skutkových podstat postihujících „Stalking“[60]. Za užití počítačů lze zkrátka páchat široké spektrum trestné činnosti, která však již v mnoha případech není posuzována jako počítačová kriminalita, ale k jejímu páchání je pachateli často užíváno počítačů a počítačových sítí.

6.1 Trestné činy proti svobodě a právům na ochranu osobnosti

Internet je pachateli velmi často využíván jako prostředek k vydírání oběti. Pro tyto účely si pachatel vytvoří emailový účet nebo užije svůj stávající a odesílá oběti své požadavky elektronickou poštou. Toto jednání pachatele je posuzováno jako trestný čin vydírání dle § 175 TZ. Z tohoto ustanovení vyplývá, že „kdo jiného násilím, pohrůžkou násilí nebo pohrůžkou jiné těžké újmy nutí, aby něco konal, opominul nebo trpěl, bude potrestán“[61].

Internet je dále velmi často užíván k pomluvě jiného, ať již na diskusních fórech, sociálních sítích, nebo jsou za účelem pomluvy vytvořeny speciální webové stránky jako je např. webová stránka extopedie.cz. Pomluva je zakotvena v TZ v ustanovení § 184. Z tohoto ustanovení vyplývá, že „kdo o jiném sdělí nepravdivý údaj, který je způsobilý značnou měrou ohrozit jeho vážnost u spoluobčanů, zejména poškodit je v zaměstnání, narušit jejich rodinné vztahy nebo způsobit jim vážnou újmu, bude potrestán“[62]. Užití počítačové sítě Internet k pomluvě je podmínkou užití přísnější trestní sazby za spáchání tohoto trestného činu.

[60] *Stalking* je způsob chování, kdy se pachatel zaměří na nějakého člověka, po kterém slídí, obtěžuje a pronásleduje jej, vyhrožuje mu, často jej i fyzicky napadá a někdy i usmrtí; u své oběti svým chováním zároveň vyvolává pocity strachu. In: ŠÁMAL, P. a kol. *Trestní zákoník. 1. vydání, Praha*, C.H.Beck, 2009, s. 3006.
[61] ŠÁMAL, P. a kol. *Trestní zákoník. 1. vydání, Praha*, C.H.Beck, 2009, s. 1572.
[62] ŠÁMAL, P. a kol. *Trestní zákoník. 1. vydání, Praha*, C.H.Beck, 2009, s. 1642.

6.2 Trestné činy hospodářské

Z těchto trestných činů je za užití počítačů velmi často páchán pouze trestný čin Neoprávněného provozování loterie a podobných sázkových her dle § 252 TZ. Z tohoto ustanovení vyplývá, že „kdo neoprávněně provozuje, organizuje, propaguje nebo zprostředkovává loterii nebo podobnou sázkovou hru, bude potrestán“[63]. Tohoto trestného činu se pachatelé dopouštějí tím, že vytvoří webovou stránku např. soutěž o 1.000.000,- Kč. Soutěž spočívá v tom, že soutěžící odešle SMS zprávu ze svého telefonu se zvýšeným tarifem (cena 1 SMS je většinou 99,- Kč) a každá stá SMS vyhrává. V jednání provozovatele uvedené webové stránky může být spatřováno jednání dle uvedeného ustanovení. Provozovatelé podobných webových stránek se však většinou snaží pouze obohatit na úkor důvěřivých lidí, neboť jejich úmyslem není vyplatit uvedenou částku, ale získat neoprávněný prospěch ze SMS s vyšším tarifem. U tohoto typu kriminality je velká latentnost, neboť nedochází k oznámení ze strany účastníků „soutěže“, protože si myslí, že když neobdrží výhru, že neměli štěstí. Tuto trestnou činnost lze zaznamenat a potírat pouze aktivním vyhledáváním policejním orgánem, k čemuž v určité míře dochází.

6.3 Trestné činy narušující soužití lidí

Podobně jako u trestného činu vydírání je Internet užíván k páchání trestného činu Nebezpečné vyhrožování dle § 353 trestního zákoníku. Z uvedeného ustanovení vyplývá, že „kdo jinému vyhrožuje usmrcením, těžkou újmou na zdraví nebo jinou těžkou újmou takovým způsobem, že to může vzbudit důvodnou obavu, bude potrestán“[64]. Pachatelé ke spáchání tohoto trestného činu často užívají emaily nebo messneger sociální sítě.

Obdobného znění je ustanovení o trestném činu nebezpečné pronásledování dle § 354 trestního zákoníku, z kterého vyplývá, že „kdo jiného dlouhodobě pronásleduje tím, že vyhrožuje ublížením na zdraví nebo jinou újmou jemu nebo jeho osobám blízkým, vyhledává jeho osobní blízkost nebo jej sleduje, vytrvale jej prostřednictvím prostředků elektronických komunikací, písemně nebo jinak kontaktuje, bude potrestán“[65].

[63] ŠÁMAL, P. a kol. *Trestní zákoník. 1. vydání, Praha*, C.H.Beck, 2009, s. 2333.
[64] ŠÁMAL, P. a kol. *Trestní zákoník. 1. vydání, Praha*, C.H.Beck, 2009, s. 2999.
[65] ŠÁMAL, P. a kol. *Trestní zákoník. 1. vydání, Praha*, C.H.Beck, 2009, s. 3004.

Obě výše uvedená ustanovení mají jedno společné v podobě omezování práv osoby oběti. Jedná se o dvě nové skutkové podstaty trestného činu, kterými zákonodárce mimo jiné reagoval na rozvoj komunikačních technologií a zahrnul je do rekodifikačního procesu trestního zákona.

U obou popsaných skutků je opět velká latentnost, neboť oběti těchto útoků se jen velmi zřídka obracejí na OČTŘ. Jedná se však o celospolečenský problém, neboť k těmto trestným činům dochází velmi často. Většinou se nebezpečného pronásledování nebo vyhrožování dopouštějí muži vůči ženám (bývalým partnerkám). Nejjednodušší způsob jak tuto trestnou činnost páchat je pro pachatele užití komunikačních technologií, kdy se jedná o emaily, SMS zprávy apod.

7 Rekodifikace trestního zákona v souvislosti s počítačovou kriminalitou

Jedním z cílů této bakalářské práce je dále zhodnocení toho, jak se nárůst počítačové kriminality promítl do rekodifikace trestního práva hmotného, ke kterému došlo s účinností k 1. 1. 2010, kdy původní trestní zákon (zákon číslo 140/1961 Sb.) byl nahrazen současným trestním zákoníkem. Postihování jednotlivých forem počítačové kriminality bylo dle starého trestního zákona často velmi problematické, neboť metody různých útoků často přesahovaly rámec tohoto zákona, což vedlo k tomu, že mnohdy bylo velmi složité podřadit (subsumovat) větu skutkovou pod větu právní tohoto zákona. Jak počítačová kriminalita narůstala, útoky proti počítačovým systémům nebo za užití počítačů se stávaly stále sofistikovanější, začal být právním kvalifikacím těchto jednání trestní zákon doslova úzký. Pravdou je, že OČTŘ a to zejména policejní orgán, který vždy stojí na začátku řízení, si s nastalou situací musely vždy nějak poradit, mnohdy z toho však vznikaly doslova právní „kočkopsi".

Popsanou těžko udržitelnou situaci v podstatě vyřešila rekodifikace trestního práva hmotného, ve které bylo pamatováno i na počítačovou kriminalitu a do TZ přibyly zcela nové SPTČ, kterými jde v současné době postihovat drtivá většina útoků počítačových pirátů. V následujících podkapitolách bude uvedena právní úprava dle starého trestního zákona a poukázáno na změny, ke kterým došlo v novém trestním zákoníku.

7.1 Porušování autorského práva

Porušování autorského práva bylo ve starém trestním zákoně vymezeno v § 152 Porušování autorského práva, práv souvisejících s právem autorským a práv k databázi. V této SPTČ nebyla nijak řešena míra porušení autorského práva a tato skutečnost vedla k tomu, že bylo problematické určit, co je ještě přestupek a co již trestný čin zejména z toho důvodu, že při právní kvalifikaci se policejní orgán, ale i OČTŘ řídily ustanovením o výši škody, kde to, co je trestným činem, bylo odvozováno od způsobení škody nikoli nepatrné dosahující částky nejméně 5.000,-Kč. V době před masivním nástupem počítačové kriminality na poli porušování autorských práv ve smyslu neoprávněného sdílení děl podléhajících autorskoprávní ochraně, na počítačové síti Internet, bylo

ustanovení starého trestního zákona dostačující, neboť k porušování autorských práv docházelo převážně prodejem nelegálních rozmnoženin hudebních nosičů, VHS/DVD a software. Tyto nelegální rozmnoženiny byly nalézány především na stáncích a v tržnicích, kde škoda ze zajištěných nosičů mnohonásobně přesahovala škodu nikoli nepatrnou.

Porušování autorského práva je po rekodifikaci, jak již bylo uvedeno v trestním zákoníku, vymezeno v ustanovení § 270 TZ. Do věty první tohoto ustanovení přibyla nová formulace, kdo neoprávněně zasáhne nikoli nepatrně do zákonem chráněných práv k autorskému dílu“, oproti staré formulaci „kdo neoprávněně zasáhne do zákonem chráněných práv k autorskému dílu“. Touto formulací zákonodárce jasně řekl, že porušování autorského práva je trestným činem v momentě, kdy pachatelem způsobená škoda dosáhne hranice 5.000,- Kč. V okolnostech použití přísnější trestní sazby uvedených v odstavci druhém, bylo ve starém trestním zákoně užito pouze získání značného prospěchu a spáchání činu ve značném rozsahu. Naproti tomu v novém TZ byla přidána ještě třetí okolnost použití přísnější trestní sazby, kdy se pachatel porušování autorského práva dopouští pro svoji obchodní činnost nebo jiného podnikání. Po rekodifikaci trestního práva lze tedy užít přísnější trestní sazby např. za neoprávněné užívání počítačového software v hodnotě vyšší než 5.000,- Kč v obchodní společnosti, což dle původní právní úpravy v § 152 starého trestního zákona nebylo možné. Nový TZ navíc přidal i třetí odstavec, který zpřísňuje potrestání pachatelů, kteří se porušování autorského práva dopouštějí ve velkém rozsahu, nebo získají prospěch velkého rozsahu, čímž se zpřísnila i trestní sazba za tento čin, kdy horní hranice trestní sazby činí až deset let oproti úpravě ve starém trestním zákoně, kde horní hranice trestní sazby činila pět let. Rekodifikací trestního práva došlo k daleko přísnějšímu posuzování porušování autorských práv.

7.2 Neoprávněné přístupy k počítačovým systémům

Nejproblematičtější z pohledu trestního zákona bylo právní posuzování různých útoků proti počítačovým systémům nebo za užití počítačů. Dle trestního zákona bylo možno na všechny druhy kybernetických útoků užít pouze § 257a Poškození a zneužití záznamu na nosiči informací, kdy se na základě tohoto ustanovení dalo postihovat pouze neoprávněné užití informací z počítačového systému, zničení a poškození dat v tomto systému. Nijak zde nebylo řešeno to, jak se pachatel do počítačového systému dostal, zda

překonal nějaké bezpečnostní zařízení tím, že znal např. heslo k počítačovému systému, nebo proti tomuto počítačovému systému provedl útok, kterým si do tohoto počítačového systému získal přístup apod. Pravdou je, že v dřívějších dobách byly cíle počítačových útočníků jiné, než je tomu v současnosti. Prioritou útočníků bylo dostat se do počítačových systémů, vymazat jejich část nebo celý systém a poté o tom poreferovat svým kolegům „hackerům“. Možností, jak se obohatit útoky na počítačové systémy bylo málo, internetové bankovnictví bylo v České republice v „plenkách“, proto docházelo především k vyřazení webových stránek nejstarší metodou DoS nebo DDoS.

Pokud se pachatelům podařilo překonat bezpečnostní opatření nějakého počítačového systému a např. vyřadit webové stránky nebo vymazat obsah počítače, bylo pro právní kvalifikaci takového jednání dle starého trestního zákona užito ustanovení § 257 Poškozování cizí věci. Z tohoto ustanovení vyplývalo, že „kdo zničí, poškodí nebo učiní neupotřebitelnou cizí věc a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán.“ Z toho vyplývalo, že v podstatě nebylo možno trestně postihovat jednání útočníků proti webům, jejichž pořízení povětšinou nepřesáhlo částku vyšší než 5.000,- Kč. Uvedenou skutečnost si uvědomoval i zákonodárce, což způsobilo, že se po rekodifikaci trestního práva v TZ objevily tři nové SPTČ, Neoprávněný přístup k počítačovému systému a nosiči informací dle § 230 TZ, Opatření a přechovávání přístupového zařízení a hesla dle § 231 TZ a Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti dle § 232 TZ. Tyto SPTČ, byly podrobně pospány v teoretické části této bakalářské práce v kapitole 4. Lze pouze dodat, že díky uvedeným novým SPTČ dostal policejní orgán a OČTŘ do ruky silný nástroj v boji proti počítačové kriminalitě

8 Kazuistika počítačové kriminality

Prověřování a vyšetřování počítačové kriminality je velmi složitou, zdlouhavou a specifickou činností, ke které je třeba znalostí ze světa výpočetní techniky. Tyto znalosti je třeba správně využít k dokumentování důkazů o páchání počítačové kriminality tak, aby tyto důkazy byly následně procesně využitelné pro dané trestní řízení.

Klíčová je znalost, kde lze důkazy hledat a jaké kriminalistické stopy sledovat, neboť důkazy se nachází jak uvnitř operačních systémů počítačů, tak u poskytovatelů různých internetových služeb nebo Internetu jako takového. Pro prověřování počítačové kriminality je velmi důležité přesně vědět, jaké informace požadovat od provozovatelů internetových služeb, neboť pokud je těmto provozovatelům odeslána obecná žádost např. k nějakému emailovému účtu ve smyslu „nechť provozovatel sdělí informace k dané emailové schránce“, poskytovatel zpravidla doručí obecnou odpověď, kdy byl emailový účet založen, jméno a příjmení, které osoba email zakládající při jeho založení uvedla. Při obdobném typu žádosti je třeba mít přehled o všech službách, které poskytovatel provozuje a přesně vymezit, co je požadováno. Z toho vyplývá, že je-li špatně položen dotaz, co konkrétně je po provozovateli webových služeb požadováno, je zpět doručena odpověď, že provozovatel požadovaným nedisponuje apod.

Při prověřování počítačové kriminality bývá v mnoha případech stěžejním důkazem IP adresa[66], u níž rozlišujeme dva její typy. Jedná se o IP adresu dynamickou a statickou. Pokud má pachatel přidělenu statickou IP adresu, je velmi snadno vystopovatelný, protože je mu přidělena jediná IP adresa, která se nemění. Pokud má pachatel přidělenu dynamickou IP adresu, je třeba znát přesný čas na vteřiny, kdy se k síti připojoval a dopouštěl se protiprávního jednání, neboť, zjednodušeně řečeno, dynamická IP adresa není stálá, neustále se mění a v jeden okamžik na ní může být mnoho jiných zákazníků operátora, který adresu přiděluje. U vyžadování dat o telekomunikačním provozu k IP adresám je třeba mít na zřeteli zákon č. 127/2005 S., o elektronických komunikacích a o změně některých souvisejících zákonů (dále jen „zákon o elektronických komunikacích“), zejména ustanovení § 97 odst. 3 zákona o elektronických komunikacích, ve kterém je uvedeno, že poskytovatel internetového připojení má

[66] IP adresa, slouží k rozlišení síťových rozhraní připojených k počítačové síti. Zkratka IP znamená Internet Protocol, což je protokol, pomocí kterého spolu komunikují všechna zařízení v Internetu. In: MATEJKA. J. *Internet jako objekt práva*, CZ.NIC, z.s.p.o. 2013, s. 89.

povinnost uchovávat data o tomto provozu půl roku. Pokud bude vyžadována IP adresa starší půl roku, je odpověď od operátora taková, že operátor dle zákona nesmí uchovávat data starší než půl roku, tudíž požadované nemůže poskytnout.

V této části bakalářské práce budou uvedeny 3 kazuistiky, které se přímo vztahují k teoretické části bakalářské práce, kdy se jedná o kazuistiky vztahující se k porušování autorských práv, neoprávněným přístupům do počítačových systémů a k internetovým podvodům. Jedná se o kazuistiky případů, které prověřoval či vyšetřoval autor této bakalářské práce. Ve většině případů došlo k ukončení pravomocným rozhodnutím soudu. V některých případech prověřování a vyšetřování počítačové kriminality lze tato trestní řízení ukončit usnesením státního zástupce dle § 159a odst. 4 TŘ[67], nebo tzv. odklonem od trestního stíhání dle § 307 TŘ a § 309 TŘ, pokud pachatel nahradí škodu nebo uzavře s poškozeným dohodu o náhradě škody a splní další podmínky odklonu. Tento postup je uplatňován zejména u trestné činnosti na úseku porušování autorských práv, kdy se povětšinou jedná o prvopachatele a spáchání tohoto trestného činu bylo z jejich strany ojedinělým excesem v jinak řádném způsobu života.

8.1 Kazuistika porušování autorských práv

Na Obvodní ředitelství policie Praha bylo podáno trestní oznámení České protipirátské unie na neznámého pachatele vystupujícího pod přezdívkou „Pachatel“, pro podezření ze spáchání trestného činu Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi dle § 270 odst. 1 odst. 3 písm. b) TZ. Tohoto trestného činu se měl tento pachatel dopustit tím, že od určité doby bez souhlasu výrobců uložil na File Hostingové servery www.czshare.cz, www.hellshare.cz a www.fastshare.cz, 850 filmových děl a odkazy ke stažení těchto děl umístil na „diskusní“ fórum www.warcenter.cz a na svoou vlastní webovou stránku www.pachatel.cz, čímž byla způsobena škoda ve výši 1.500.000,- Kč.

Policejním orgánem byl ve věci vydán Záznam o zahájení úkonů trestního řízení dle § 158 odst. 3 zákona číslo 141/1961 Sb., o trestním řízení soudním ve znění pozdějších právních předpisů (dále jen „TŘ“), pro podezření ze spáchání zločinu Porušení

[67] ČESKO. Zákon č. 141/1961 Sb. o trestním řízení soudním (trestní řád). In *Sbírka zákonů, Česká republika.* 1961, částka 66.

autorského práva, práv souvisejících s právem autorským a práv k databázi dle § 270 odst. 1, odst. 3 písm. b) TZ.

Policejním orgánem byla od provozovatelů výše uvedených File Hostingových serverů zajištěna IP adresa, z které došlo k neoprávněnému sdílení filmových děl, dále veškeré registrační údaje pachatele, který prováděl neoprávněné sdílení děl. Dále bylo zajištěno číslo bankovního účtu pachatele, na které mu od provozovatelů File Hostingových serverů byla vyplácena provize za stažení jím nahraných souborů ostatními uživateli internetu.

Policejní orgán prostřednictvím státního zástupce požádal o vydání příkazu ke zjištění údajů o telekomunikačním provozu dle § 88a odst. 1 TŘ ke zjištěné IP adrese. Na základě této žádosti byl Obvodním soudem Praha vydán příkaz dle uvedeného ustanovení, kterým bylo nařízeno poskytovateli internetového připojení, aby sdělil, komu byla v určitých časech přidělena uvedená IP adresa. Poskytovatelem internetového připojení bylo sděleno, že uvedená IP adresa byla v časech připojení přidělena konkrétní osobě na konkrétní adrese. Policejní orgán dále prostřednictvím státního zástupce požádal o informace dle § 8 odst. 2 TŘ k zjištěnému bankovnímu účtu. U registrátora internetových domén bylo zjištěno, kdo registroval webovou stránku www.pachatel.cz a jak za registraci zaplatil. Policejním orgánem byly dále vyžádány informace ke zjištěným emailovým účtům a provedena lustrace zjištěných telefonních čísel.

Po nashromáždění výše uvedených důkazů došlo k jejich vyhodnocení, přičemž bylo zjištěno, že zájmová IP adresa byla v době neoprávněného sdílení děl přidělena konkrétní osobě, tato osoba je jediným disponentem zjištěného bankovního účtu, dále tato osoba provedla registraci uvedené webové stránky a užívá zjištěné emaily. Po zhodnocení zjištěných důkazů bylo rozhodnuto, že bude zahájeno trestní stíhání dle § 160 odst. 1 TŘ ustanovené konkrétní osoby pro zločin Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi dle § 270 odst. 1, odst. 3 písm. b) TZ. Při právní kvalifikaci skutku policejní orgán vycházel z množství, ve kterém pachatel neoprávněně díla na File Hostingové servery nahrál, nikoli z vyčíslené škody, která ve finále přesahovala dle sdělení České protipirátské unie (dále jen „ČPU“) 21.000.000,- Kč, kdy ČPU počítá 1x stažené dílo jako dílo, které by si jinak osoba, která jej stáhla, zakoupila, což je dle názoru policejního orgánu minimálně zavádějící a právní kvalifikace skutku byla opřena o rozsah 850 děl (nedlouho po této právní kvalifikaci policejního orgánu byl

Ústavním soudem vydán nález, který o vyčíslené škodě ČPU hovoří ve stejném duchu, jak je výše uvedeno).

Policejním orgánem byl proveden výslech obviněné ustanovené osoby, která shora popsané jednání, kladené jí za vinu, popřela. Obviněný ve své výpovědi uváděl nepravdu v tom smyslu, že výše uvedené File Hostingové servery používal pro nahrávání rodinných fotografií, videí a číslo účtu vyplnil, protože bylo při registraci na File Hostingových serverech požadováno. Vyšetřování bylo policejním orgánem ukončeno návrhem na podání obžaloby dle §166 odst. 3 TŘ.

Obvodním státním zastupitelstvím v Praze byla následně podána obžaloba pro skutek výše uvedený k Obvodnímu soudu v Praze. Obvodním soudem v Praze byl vyhlášen rozsudek jménem republiky, kterým byla ustanovená osoba odsouzena pro přečin Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi dle § 270 odst. 1, odst. 2 písm. c) TZ. „Proti tomuto rozsudku včas a řádně podali odvolání jednak Obvodní státní zástupkyně z Obvodního státního zastupitelství v Praze, jednak obžalovaný prostřednictvím svého obhájce. Odvolání státní zástupkyně Obvodního státního zastupitelství v Praze směřovalo proti všem výrokům napadeného rozsudku, kdy se zejména neztotožňuje s použitou právní kvalifikací, kdy jednání obžalovaného mělo být kvalifikováno jako zločin Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi dle § 270 odst. 1, odst. 3 písm. b) TZ. Odvolání obžalovaného směřovalo proti všem výrokům napadeného rozsudku“.

O věci dále rozhodoval Městský soud v Praze, který dle § 258 odst. 1 písm. b) TŘ zrušil napadený rozsudek v plném rozsahu a za podmínek § 259 odst. 3 TŘ se znovu rozhodl tak, že obžalovaný je vinen z přečinu Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi dle § 270 odst. 1, odst. 2 písm. c) TZ. Tuto právní kvalifikaci odvolací soud odůvodnil tím, že OČTŘ nebyly v přípravném řízení a rovněž státním zástupcem předloženy takové důkazy, které by odůvodňovaly jednoznačnou kvalifikaci jednaní obžalovaného dle ustanovení § 270 odst. 3 písm. b) TZ, přičemž odvolací soud postupoval v této otázce dle zásady in dubio pro reo[68]. Skutečnost

[68] *in dubio pro reo* – ve prospěch obviněného - Procesním důsledkem toho, že se nepodařilo bezpečně prokázat vinu obviněného a že obviněný nemusí dokazovat svoji nevinu, je pravidlo, že pochybnost prospívá. Judikatura zdůrazňuje, že použití zásady přichází v úvahu jen tehdy, jestliže pochybnosti, které vznikly v trestním řízení o nějaké skutečnosti, trvají i po provedení a zhodnocení všech dostupných důkazů. K uplatnění této zásady je možné přistoupit, pokud soud dospěje k závěru, že není možné se jednoznačně přiklonit k žádné ze skupiny odporujících důkazů k žádné ze dvou rozporných výpovědí. JELÍNEK, J. a kolektiv: *Trestní právo procesní*. 3. vydání. Praha: Leges, 2013, s. 143-144.

podmiňující užití přísnější právní kvalifikace nebyla v rámci hlavního líčení zcela prokázána, kdy odvolací soud tento právní názor opírá i o rozhodnutí Nejvyššího soudu ČR, sp. zn. 5Tdo 171/2014, jakož i o komentář k trestnímu zákoníku.

8.2 Kazuistika neoprávněného přístupu k počítačovému systému a nosiči informací

Na Obvodní ředitelství policie Praha bylo podáno trestní oznámení bankovního ústavu na jeho bývalou zaměstnankyni „Pachatelku“ a jejího přítele „Pachatele“, též bývalého zaměstnance tohoto bankovního ústavu, pro podezření ze spáchání přečinu Neoprávněný přístup k počítačovému systému a nosiči informací dle § 230 odst. 2 písm. a) TZ. Uvedeného přečinu se měl „Pachatelka“ a „Pachatel“ dopustit tím, že si „Pachatelka“ v určité době na svém bývalém pracovišti u bankovního ústavu vytvořila datový soubor, který obsahoval informace o klientech tohoto bankovního ústavu. Takto vytvořený soubor si určitého data zkopírovala na USB disk a tento USB disk v přesně nezjištěné době předala „Pachateli“, který v té době již nebyl zaměstnancem ani externím pracovníkem bankovního ústavu. „Pachatel“, následně přistupoval na neveřejné webové stránky bankovního ústavu, ke kterým si získal přístup ještě v době, kdy byl zaměstnán v bankovním ústavu od své kolegyně „Svědkyně“ při jejím zaškolování a následně užil dat, které mu předala „Pachatelka“, aby v uvedeném bankovním systému mohl dohledat informace o klientech tohoto bankovního ústavu pro svoji další potřebu.

Policejním orgánem byl ve věci vydán Záznam o zahájení úkonů trestního řízení dle § 158 odst. 3 TŘ pro podezření ze spáchání přečinu Neoprávněný přístup k počítačovému systému a nosiči informací dle § 230 odst. 2 písm. a) TZ, kterého se měli dopustit jak „Pachatel“, tak „Pachatelka“ ve spolupachatelství dle § 23 TZ výše popsaným jednáním. Uvedený záznam byl dále vydán pro přečin Opatření a přechovávání přístupového zařízení a hesla k počítačovém systému a jiných takových dat dle § 231 odst. 1 písm. b) TZ, kterého se měl dopustit „Pachatel“ tím, že toto přístupové heslo vylákal pod záminkou školení od „Svědkyně“ a následně jej použil pro spáchání shora uvedeného přečinu.

Policejním orgánem byly od bankovního ústavu vyžádány logovací soubory z počítače užívaného „Pachatelkou“, dále logovací soubory k přístupům do neveřejné části webových stránek bankovního ústavu, konkrétně k přístupům z přihlašovacích

údajů „Svědkyně“. Z logovacích souborů z pracovní stanice „Pachatelky“ vyplynulo, že skutečně v konkrétním čase vytvořila datový soubor, který obsahoval údaje o klientech bankovního ústavu. Vzhledem k pokročilému zálohování počítačové sítě v bankovním ústavu byl policejnímu orgánu z této zálohy předán i uvedený datový soubor vytvořený „Pachatelkou“. Z logovacích souborů přihlášení do neveřejné části webové stránky bankovního ústavu na přihlašovací údaje svědkyně bylo zjištěno, že k této části webové stránky ústavu bylo v konkrétních časech přistupováno ze dvou IP adres.

Policejní orgán prostřednictvím státního zástupce požádal o vydání příkazu ke zjištění údajů o telekomunikačním provozu dle § 88a odst. 1 TŘ ke zjištění IP adres, z kterých bylo přistupováno k neveřejné části webových stránek bankovního ústavu. Na základě této žádosti byl Obvodním soudem Praha vydán příkaz dle uvedeného ustanovení, kterým bylo nařízeno poskytovateli internetového připojení, aby sdělil, komu byly v určitých časech přiděleny obě zjištěné IP adresy. Poskytovatelem internetového připojení bylo sděleno, že jedna IP adresa byla v uvedených časech poskytována „Svědkyni“ na konkrétní adrese připojení a druhá „Pachateli“, opět na konkrétní adrese připojení.

Vzhledem k odpovědi poskytovatele internetového připojení, byl policejním orgánem odeslán dotaz dle § 8 odst. 1 TŘ, bankovnímu ústavu, zda v konkrétních časech „Svědkyně“ vykonávala pro bankovní ústav pracovní činnost spojenou s přistupováním do neveřejné části webových stránek přes tzv. „Home Office“. Z odpovědi bankovního ústavu vyplynulo, že v konkrétních časech „Svědkyně“ skutečně prováděla práci pro bankovní ústav.

Policejním orgánem byl se „Svědkyní“ sepsán Úřední záznam o podaném vysvětlení dle § 158 odst. 6 TŘ (dále jen ÚZ), z kterého vyplynulo, že „Svědkyni“ zaškoloval do počítačového systému bankovního ústavu „Pachatel“, který ji z důvodu zaškolení požádal o heslo k přístupu do tohoto počítačového systému. Svědkyně dále sdělila, že přístupové údaje, které kvůli zaškolení sdělila „Pachateli“, užívá od současné doby.

Policejním orgánem byl s „Pachatelkou“ sepsán ÚZ, tato však využila svého práva dle § 100 odst. 2 TŘ a odmítla k věci vypovídat. Stejným způsobem se při sepisování ÚZ vyjádřil i pachatel.

Po nashromáždění výše uvedených důkazů došlo k jejich vyhodnocení a bylo zjištěno, že se skutečnosti odehrály tak, jak bylo popsáno v trestním oznámení. Důkazními

materiály byl potvrzena i hypotéza policejního orgánu, že „Pachatelka“ i „Pachatel“ jednali ve spolupachatelství, kdy „Pachatel“ se na spáchání popsaného přečinu navíc připravil tím, že si obstaral přihlašovací údaje „Svědkyně“, kterých užil pro svou trestnou činnost.

Po zhodnocení zjištěných důkazů bylo zahájeno trestní stíhání dle § 160 odst. 1 TŘ proti „Pachatelce“ a „Pachateli“ pro spáchání přečinu Neoprávněný přístup k počítačovému systému a nosiči informací dle § 230 odst. 2 písm. a) TZ, kterého se jak „Pachatelka“, tak „Pachatel“ dopustili ve spolupachatelství dle § 23 trestního zákoníku. Dále bylo zahájeno trestní stíhání dle § 160 odst. 1 TŘ, proti „Pachateli“ pro přečin Opatření a přechovávání přístupového zařízení a hesla k počítačovém systému a jiných takových dat dle § 231 odst. 1 písm. b) TZ.

Policejním orgánem byl proveden výslech obviněných, kdy oba shodně jako při sepisování ÚZ odmítli k věci vypovídat. Vyšetřování bylo policejním orgánem ukončeno návrhem na podání obžaloby dle §166 odst. 3 TŘ.

Obvodním státním zastupitelstvím v Praze byla následně podána obžaloba pro skutek výše uvedený k Obvodnímu soudu v Praze. Obvodním soudem v Praze byl vydán trestní příkaz, kterým byli pachatelé odsouzeni pro přečin Neoprávněný přístup k počítačovému systému a nosiči informací dle § 230 odst. 2 písm. a) TZ, kterého se dopustili ve spolupachatelství dle § 23 TZ. Dále „Pachatel“ pro přečin Opatření a přechovávání přístupového zařízení a hesla k počítačovém systému a jiných takových dat dle § 231 odst. 1 písm. b) TZ. Tento trestní příkaz byl pachatelům řádně doručen a v zákonné lhůtě nabyl v obou výrocích právní moci a je vykonatelný.

8.3 Kazuistika podvodného jednání na internetu

Na Obvodní ředitelství policie Praha bylo Finančně analytickým útvarem Ministerstva financí ČR (dále jen „FAU“), podáno oznámení o okolnostech nasvědčujících spáchání trestného činu v souvislosti s nabízením půjček, kterého se mohl dopustit „Bankéř“ v souvislosti s nabídkou finančních půjček. Z oznámení vyplývalo, že tuto skutečnost FAU oznámil bankovní ústav, u kterého má „Bankéř“ veden účet č. 000000000000, na který opakovaně docházeli platby různé hodnoty s variabilními čísly plateb, která se jevila jako rodná čísla osob, které platby zaslali. Vzhledem k této

skutečnosti byl uvedený účet FAU zablokován na dobu 72 hodin a následně podáno výše uvedené oznámení.

Přílohou oznámení byl kompletní výpis účtu č. 000000000000, vedený na „Bankéře“, dále výzva bankovního ústavu, aby se „Bankéř“ vyjádřil k došlým platbám a dopis „Bankéře“, ve kterém uvádí, že je soukromou osobou, pracující pro zahraničního investora, která nabízí klientům nebankovní půjčky.

Policejním orgánem bylo provedeno vyhodnocení oznámení, kdy bylo zjištěno, že na účet č. 000000000000 bylo přijato celkem 60.000,- Kč, od 75 subjektů. Na uvedeném účtu však nikdy nebyla dostatečná hotovost pro poskytování nebankovních půjček, dále z tohoto účtu byly kartou hrazeny platby převážně v hernách a kasinech. Po zhodnocení těchto skutečností dospěl policejní orgán k závěru, že jednáním „Bankéře“ mohlo dojít ke spáchání přečinu Podvod dle § 209 odst. 1, odst. 3 TZ. Vzhledem k zjištěným skutečnostem a také vzhledem k tomu, že uvedený účet se nacházel v režimu blokace na 72 hodin FAU, bylo policejním orgánem rozhodnuto o vydání Záznamu o zahájení úkonů trestního řízení dle § 158 odst. 3 TŘ, pro výše uvedený přečin, kterého se měl dopustit „Bankéř“ tím, že nabízel za úplatu půjčky finanční hotovosti, které poškozeným nevyplatil.

Policejním orgánem byla provedena lustrace 75 variabilních symbolů z došlých plateb na účet č. 000000000000, které vypadaly jako rodná čísla. Výsledkem této lustrace bylo 75 konkrétních osob, s kterými byl sepsán ÚZ. Výpovědi ztotožněných osob byly obdobné a vyplynulo z nich, že na inzertním portálu www.portal.cz nalezli inzerát s nabídkou nebankovní půjčky, ve kterém „Bankéř“ vystupoval vždy pod jiným jménem a nabízel v těchto inzerátech nebankovní půjčky v různých hodnotách. Vždy sděloval, že pracuje pro soukromého investora nabízejícího nebankovní půjčky. Podmínkou získání této půjčky bylo složení poplatku jako zálohy, která je polovinou první splátky požadované půjčky a tento poplatek měl být složen na účet č. 000000000000. Složením poplatku měl žadatel prokázat, že bude schopen půjčku splácet. V inzerátu bylo dále uvedeno, že poté, co bude požadovaná částka připsána na účet č. 000000000000, bude žadateli půjčka dovezena obchodním zástupcem na dohodnuté místo, žádná finanční půjčka však nebyla poškozeným nikdy dovozena ani jinak vyplacena. „Bankéř“ s poškozenými jednal prostřednictvím deseti emailových účtů, které byly založeny pod jmény, kterými s poškozenými jednal.

Vzhledem k zjištěným skutečnostem byla dle § 8 odst. 1 TŘ vyžádána součinnost ke sdělení údajů s provozovatelem emailových účtů, které byly vytvořeny na jednom emailovém portále. Z odpovědi provozovatele emailových účtů vyplynulo, že všechny emailové účty byly založeny anonymně, ověřeny jedním autorizačním telefonním číslem a jsou propojeny s emailovým účtem na jméno „Bankéř“, kdy ověřovací telefonní číslo je totožné. Policejním orgánem byla provedena lustrace uvedeného telefonního čísla a bylo zjištěno, že toto telefonní číslo je vedeno na osobu „Bankéře“.

Po zhodnocení zjištěných důkazů bylo zahájeno trestní stíhání dle § 160 odst. 1 TŘ proti „Bankéři“ pro spáchání přečinu Podvod dle § 209 odst. 1, odst. 2 TZ, kterého se dopustil tím, že v konkrétním časovém období, ač nepracoval pro žádného soukromého investora a od samého začátku neměl poskytnutí půjčky v úmyslu, umístil na inzertní portál www.portal.cz inzeráty s nabídkou nebankovních půjček v různé výši s tím, aby žadatelé o nebankovní půjčku zaslali svou žádost na jeden z deseti smyšlených emailů, na nichž vystupoval pod smyšlenými jmény, v následné emailové komunikaci s jednotlivými žadateli sdělil těmto žadatelům, že podmínkou získání této nebankovní půjčky je složení poplatku jako zálohy, která je polovinou první splátky požadované půjčky, kdy tento poplatek měl být složen na účet č. 000000000000, přičemž složením poplatku měl žadatel prokázat, že bude schopen půjčku splácet, dále žadatelům o nebankovní půjčku sdělil, že poté, co bude jejich platba připsána na výše uvedené číslo účtu, bude jim do půl hodiny smyšleným obchodním zástupcem přivezena požadovaná nebankovní půjčka, avšak tato půjčka žadatelům nikdy nebyla zprostředkována a poskytnuta, čímž úmyslně uvedl v omyl všech 75 osob (v usnesení byla pospána každá transakce s datem platby a částkou zvlášť), a to tak, že v důsledku tohoto omylu způsobil na jejich majetku celkovou škodu ve výši 60.000,- Kč.

Policejním orgánem byl proveden výslech obviněného „Bankéře“, kdy jmenovaný doznal svoji trestnou činnost v plném rozsahu, svého činu litoval a přislíbil náhradu škody poškozeným. Vyšetřování bylo policejním orgánem ukončeno návrhem na podání obžaloby dle §166 odst. 3 TŘ.

Obvodním státním zastupitelstvím v Praze byla následně podána obžaloba pro skutek výše uvedený k Obvodnímu soudu v Praze. Obvodním soudem v Praze byl vydán trestní příkaz, kterým byl „Bankéř“ odsouzen pro přečin Podvod dle § 209 odst. 1, odst. 3 TZ. Tento trestní příkaz byl „Bankéři“ řádně doručen, v zákonné lhůtě nabyl právní moci a je vykonatelný.

8.3.1 Zhodnocení kazuistik z hlediska cílů bakalářské práce

Z popisu shora uvedených kazuistik je patrno, jak důležitá je pro prověřování a vyšetřování počítačové kriminality teoretická analýza tohoto druhu kriminality a jejich příčin. Pro tuto kapitolu byly vybrány kazuistiky z oblasti porušování autorských práv, neoprávněných přístupů k počítačovému systému a podvodů na počítačové síti Internet. Z popisu jednotlivých kazuistik je zřejmé, že teoretické znalosti tohoto druhu kriminality jsou důležitým faktorem při řešení těchto případů. Pochopení zákonitostí počítačových systémů, zákonitostí Internetu a orientace v jiných právních předpisech je velmi důležitá pro správné řazení jednotlivých forem tohoto druhu kriminality pod SPTČ, které jsou popsány v teoretické části této bakalářské práce. Z popisu uvedených kazuistik je patrno, že teoretické znalosti z teoretické části této bakalářské práce lze úspěšně aplikovat do praxe, při řešení případů tohoto druhu kriminality.

Druhotným cílem bakalářské práce je zhodnocení toho, jak se nárůst počítačové kriminality promítl do rekodifikace trestního práva. Z kazuistiky vztahující se k neoprávněnému přístupu do počítačového systému je patrno, že zařazení nových SPTČ do trestního zákoníku, které se týkají počítačové kriminality, dalo do rukou OČTŘ velmi silnou zbraň při boji s tímto druhem kriminality.

9 Prevence počítačové kriminality

Prevence počítačové kriminality v České republice je na velmi nízké úrovni. Ve zpravodajských relací se čas od času objeví reportáž o porušování autorských práv, o nějaké formě kybernetického útoku na běžné uživatele nebo státní instituce a podvodu. Tento typ zpráv je však velmi řídký, rozdrobený mezi různé televizní stanice a rozhodně se nedá mluvit o nějaké ucelené koncepci prevence. Velmi dobrou cestou v oblasti prevence počítačové kriminality šla Česká televize, která ve spolupráci se společností CZ.NIC, z.s.p.o, natočila krátké spoty nazvané Jak na Internet, které byly v roce 2015 vysílány po hlavní zpravodajské relaci. Toto je však žalostně málo.

Snad každý třetí občan České republiky má nějakou negativní zkušenost s počítačovou kriminalitou. Nejčastějším jevem jsou různé podvody s falešnými inzeráty na inzertních portálech a různé formy Ransomware útoků. Jak vyplývá z teoretické části této bakalářské práce, prevence počítačové kriminality by měla být zaměřena jak na osoby, kterých se počítačová kriminality dotýká coby obětí, tak na potenciální pachatele zejména v oblasti porušování autorských práv. V teoretické části bakalářské práce, byly popsány nejzávažnější formy počítačové kriminality, které byly dále rozebrány v praktické části práce, v popsaných kazuistikách. V návaznosti na teoretickou část této práce autor navrhne některá preventivní opatření, která by měla být provedena.

„Prevence kriminality, neboli také kriminální profylaxe, představuje pokus eliminovat trestnou činnost ještě před jejím započetím nebo před jejím pokračováním. Do prevence kriminality tak náležejí – v našem pojetí – veškeré aktivity směřující k předcházení páchání trestných činů, k snižování jejich výskytu cestou zamezení páchání neboli k neutralizaci příčin a podmínek vzniku trestných činů (kriminogenních faktorů). Patří sem opatření, jejichž cílem je zmenšování rozsahu a závažnosti kriminality, ať již prostřednictvím omezení kriminogenních příležitostí nebo působením na potenciální pachatele a oběti trestných činů“[69].

V oblasti prevence počítačové kriminality nelze příliš spoléhat na funkci represivní, ale i ta zde má své důležité místo, která „spočívá v ochraně společnosti před zločinem tak, že prostřednictvím systému sankcí (trestů v TZ), které postihuje jedince či

[69] SVATOŠ, R. *Prevence kriminality.* 1. vydání. České Budějovice : Vysoká škola evropských a regionálních studií, o. p. s., 2014. s. 14

skupiny, jež tyto kodifikované normy určitým právně stanoveným způsobem překročili.“[70] U počítačové kriminality je třeba společnosti neustále připomínat rizika spojená s užíváním komunikačních technologií v médiích, ale s prevencí by se mělo začít již na školách formou přednášek o tomto celospolečenském problému.

9.1 Návrh preventivních opatření

Prevenci počítačové kriminality by měla především zaštítit Policie ČR, neboť „činnost Policie ČR se nezakládá pouze na represi již nastalého asociálního jednání, ale rozšiřuje se – více než v minulosti - i do oblasti prevence“[71]. Tato činnost by měla být prováděna ve spolupráci s médii a právnickými osobami zabývajícími se podnikáním s internetovým připojením. Pro potřeby prevence počítačové kriminality je třeba vytvořit skupinu, která se bude výhradně věnovat této trestné činnosti. Zřízená skupina by měla zajistit spolupráci s výše uvedenými subjekty. Spolupráce „Policie ČR s ostatními právnickými a fyzickými osobami v oblasti prevence kriminality, je upravena v § 17 zákona o Policii ČR.“[72] V současné době je oznamovaná a následně prověřovaná počítačová kriminalita policejním prezidiem sledována, neboť povinností zpracovatelů počítačové kriminality Policie ČR, je ohlašovat každý trestný čin z této oblasti formou události v IS ETŘ[73]

V rámci prevence počítačové kriminality by dále měly být vytvořeny jednoduché prezentace, které by se rozeslaly do škol, aby byly alespoň prezentovány učiteli, neboť provádět přednášky na základních a středních školách tak, aby se dostalo na každou školu, je z kapacitních a finančních důvodů nemožné.

Vytvořené prezentace by měly obsahovat stručný popis nejzávažnějších forem počítačové kriminality. Dopady počítačové kriminality na běžný život, ale také varování pro potenciální pachatele, jaké trestněprávní následky pro ně páchání počítačové kriminality může mít.

[70] MUSIL, S. *Počítačová kriminalita*, Institut pro kriminologii a sociální prevenci, 2000, s. 224.
[71] SVATOŠ, R. *Prevence kriminality.* 1. vydání. České Budějovice : Vysoká škola evropských a regionálních studií, o. p. s., 2014. s. 73.
[72] SVATOŠ, R. *Prevence kriminality.* 1. vydání. České Budějovice : Vysoká škola evropských a regionálních studií, o. p. s., 2014. s. 82.
[73] IS ETŘ neboli integrovaný informační systém Policie ČR pro oblast trestního a přestupkového řízení a souvisejících procesů. In: POLICIE.cz, Článek, Databáze IS ETŘ. Dostupné z WWW http://www.policie.cz/clanek/databaze-is-etr.aspx.

Z uvedeného vyplývá závěr, že prevence počítačové kriminality by měla být prováděna jak „v oblasti represe ve formě kvalitního vzdělání pracovníků OČTŘ, kvalitní výpočetní techniky a spolupráce Policie ČR zejména se zahraničím v rámci získávání zkušeností“[74], tak v samostatné oblasti prevence a to výchovným působením na pachatele, vedením občanů k odpovědnosti, v organizačních opatřeních směřujících k zpřehlednění činnosti (ochrana hesly, uchování paměťových médií aj.) a v přímé obraně výpočetní techniky (bezpečnostní schránky pro uschování paměťových médií, zavádění opatření evidující přístup a monitoring činnosti aj.)“[75].

[74] SVATOŠ, R. *Kriminologie ve světle nového trestního zákoníku.* 1. vydání. České Budějovice : Vysoká škola evropských a regionálních studií, o. p. s., 2010. s. 125.
[75] SVATOŠ, R. *Kriminologie ve světle nového trestního zákoníku.* 1. vydání. České Budějovice : Vysoká škola evropských a regionálních studií, o. p. s., 2010. s. 125.

Závěr

Tato bakalářská práce se zabývala počítačovou kriminalitou, jejíž prověřování a vyšetřování v sobě nese mnohá úskalí, která především policejní orgán vždy stojící na začátku, musí překonávat. Počítačová kriminalita je specifická především svým rozsahem, neboť jak bylo uvedeno v práci, nespadají do ní pouze útoky mířené proti počítačovým systémům a počítačům jako takovým, ale řadí se pod ni i porušování autorských práv a lze do ní zahrnout i trestná činnost páchaná za užití výpočetní techniky. Dokazování počítačové kriminality je složitým procesem zejména z toho důvodu, že vyjma porušování autorských práv, kde je maximálně pět způsobů, jak do autorských práv neoprávněně zasáhnout, je v podstatě každý případ počítačové kriminality jiný a v něčem nový. Tato novost spočívá v tom, že i když pachatelé využijí obecně ověřených popsaných způsobů útoků, jsou tyto útoky modifikovány tak, aby byla ztížena práce policie. Pokud selže jeden způsob (např. při útoku na internetové bankovnictví pomocí falešných webových stránek, kdy pachatel získané informace zapisuje do textového souboru a pokud je díky nim odhalen, začne si je příště při nové fázi útoku zasílat např. na email), hned nastoupí jeho jiná obdoba, kterou musí vyšetřující orgány odhalit. Z toho důvodu je třeba, aby policisté, kteří se touto problematikou zabývají, byli nejenom profesně způsobilí v trestním řízení, ale aby měli i širší vědomosti o různých metodách užívaných pachateli a neustále si prohlubovali svoje znalosti na poli komunikačních technologií.

Cílem této bakalářské práce bylo zhodnocení počítačové kriminality obecně, jejích základních pojmů, aspektů a poukázání na její nejzávažnější formy. Druhotným cílem pak bylo zhodnocení toho, jak se masivní nárůst počítačové kriminality promítl do rekodifikace trestního práva hmotného. Již v úvodů práce bylo uvedeno, že se vytčené cíle práce prolínají oběma částmi této práce, tedy teoretickou i praktickou částí.

Zhodnocení počítačové kriminality bylo provedeno v kapitolách 2, 3, 4, 5, 6, kde byly popsány jednotlivé formy tohoto druhu kriminality. U každé z popsaných forem je uvedena i právní kvalifikace dle trestního zákoníku, v kapitole 8 z praktické části práce je popsáno, jak byly případy počítačové kriminality kvalifikovány před rekodifikací trestního práva. Zde narážíme na ono proklamované prolnutí teoretické a praktické části práce, neboť kdyby dle názoru autora došlo k oddělení právních kvalifikací od výše

uvedených kapitol, mohlo by dojít k znepřehlednění autorem zamýšleného popisu tohoto druhu kriminality.

Praktická část bakalářské práce je dále založena na kazuistikách tří nejrozšířenějších případů počítačové kriminality, spočívající v porušování autorských práv, neoprávněných zásahů do programového vybavení počítače nebo dat uložených v počítači a podvodů na počítačové síti Internet. Kazuistiky případů jsou popsány v kapitole 7 bakalářské práce. Tato kapitola byla do práce zahrnuta především z toho důvodu, že na základě popsaných kazuistik lze dovodit, že skutečnosti uvedené v teoretické části práce je možno převést do skutečné praxe, neboť se jedná o případy, které autor práce prověřoval a vyšetřoval v rámci své praxe u Policie ČR, kdy tyto případy skončily pravomocným rozhodnutím soudu. Autor touto kapitolou chtěl v podstatě říci, že teoretickým poznatkům, které jsou popsány ve výše uvedených kapitolách teoretické části, lze vdechnout život jejich převodem do praxe při prověřování a vyšetřování počítačové kriminality.

Dalším z cílů bakalářské práce bylo zhodnocení toho, jak se nárůst počítačové kriminality promítl do rekodifikace trestního práva. Toto zhodnocení bylo provedeno v kapitole 8. V uvedené kapitole bylo popsáno, jak byly jednotlivé druhy počítačové kriminality právně kvalifikovány dle trestního zákona a jak jejich kvalifikaci velmi usnadnil nový trestní zákoník. V této kapitole se autor práce nevěnoval podvodům na Internetu, neboť pokud se pachatel trestnou činností dopustil podvodu jak za účinnosti trestního zákona nebo trestního zákoníku, byl tento skutek vždy kvalifikován jako trestný čin podvod.

V samotném závěru práce se autor zaměřuje i na prevenci počítačové kriminality, která jak bylo uvedeno výše je velmi problematická. Autor práce má za to, že pro potřeby této práce bylo nejdříve třeba uvést, co je pod širokým pojmem prevence myšleno z kriminologického pohledu. Při psaní této kapitoly se autor práce zaobíral myšlenkou, že největší díl prevence leží především na každém uživateli. Dle názoru autora práce je nějaká větší prevence ze strany státu spíše utopií.

Na stánkách této práce bylo autorem několikrát zmíněno, co všechno by měli policisté, kteří se zabývají počítačovou kriminalitou, zvládnout, aby mohli spolehlivě zadokumentovat a objasnit tuto trestnou činnost. Situace v Policii ČR je však taková, že se na základních útvarech nachází jen málo skutečných odborníků. V médiích bylo

v nedávné době několikrát proklamováno, že vzniká speciální útvar Policie ČR zabývající se organizovanou počítačovou kriminalitou. Toto je jistě chvályhodný krok, neboť „perspektivnost“ počítačových útoků nezůstala neznámá ani organizovaným strukturám pachatelů. Převážná část počítačové kriminality však padá na základní útvary Policie ČR, kterými jsou Obvodní oddělení nebo ředitelství. Na těchto odděleních je velmi málo policistů, kteří jsou fundovaní v dané problematice. Bylo by velmi žádoucí, aby počet takových policistů - odborníků vzrostl. Tato skutečnost byla jednou z motivací při vybírání tématu bakalářské práce autora, neboť se jedná o práci veřejnou a mohla by alespoň malým dílkem přispět k tomu, aby se o potírání počítačové kriminality zajímalo více policistů i osob, které o práci u Policie ČR mají zájem. I Policie ČR by jistě uvítala odborníky z řad IT specialistů. Pravdou je, že každý IT specialista v civilním sektoru dostane minimálně dvojnásobný plat než u Policie ČR. Práce u Policie ČR by neměla být potenciálními zájemci chápána pouze jako práce kvůli výdělku. Podle mínění autora se totiž nejedná o práci, ale poslání, které by měl každý policista vykonávat hlavně srdcem!

Seznam použitých zdrojů

Literární zdroje

1. JIRKOVSKÝ, V. *Kybernetická kriminalita*, Grada Publishing, a.s. 2007, 279 s, ISBN 978-80-247-1561-2.

2. MUSIL, S. *Počítačová kriminalita*, Institut pro kriminologii a sociální prevenci, 2000, 299 s, ISBN 80-86008-80-0.

3. HARRIS, HARPER, EAGLE, NESS, LESTER, *Hacking – manuál hackera*, Grada Publishing, a.s. 2008, 393 s, ISBN 978-80-247-1346-5.

4. ŠTĚDROŇ, B., *Ochrana a licencování počítačového programu*, Wolters Kluwer Česká republika 2010, 197 s, ISBM 978-80-7357-555-7.

5. MATEJKA. J. *Internet jako objekt práva*, CZ.NIC, z.s.p.o. 2013, 256 s, ISBN 978-80-904248-7-6.

6. NOVOTNÝ, F, SOUČEK, J. et al. *Trestní právo hmotné*. 3. vydání. Plzeň : Aleš Čeněk., 2010, 393 s, ISBN 978-80-738-291-2.

7. SVATOŠ, R. *Prevence kriminality*. 1. vydání. České Budějovice : Vysoká škola evropských a regionálních studií, o. p. s., 2014, 132 s. ISBN 978-80-87472-76-7.

8. SVATOŠ, R. *Kriminologie ve světle nového trestního zákoníku.* 1. vydání. České Budějovice : Vysoká škola evropských a regionálních studií, o. p. s., 2010, 174 s. ISBN 978-80-86708-21-8.

9. JELÍNEK, J. a kolektiv: *Trestni pravo procesni*. 3. vydani. Praha: Leges, 2013, 864 s. ISBN 978-80-87576-44-1.

10. ŠÁMAL, P. a kol. *Trestní zákoník. 1. vydání*, Praha, C.H.Beck, 2009, s. 3285. ISBN 978-80-7400-109-3.

11. AUTOR@CHIP.CZ. Darknet. *CHIP, Magazín o digitálních technologií*. 2016, č. 11, 140 s. ISSN 1210-0684.

Elektronické zdroje

1. *Upload* [online]. 2016, [cit. 25. 11. 2016]. Dostupný z WWW http://www.svethardware.cz/slovnik/u.

2. *File Hostingové servery* [online]. 2016, [cit. 25. 11. 2016]. Dostupný z WWW http://it-slovnik.cz/pojem/file-hosting/?utm_source=cp&utm_medium=link&utm_campaign=cp.

3. *Phishing* [online]. 2016, [cit. 25. 11. 2016]. Dostupný z WWW http://it-slovnik.cz/pojem/phishing/?utm_source=cp&utm_medium=link&utm_campaign=cp.

4. *Warez* [online]. 2016, [cit. 25. 11. 2016]. Dostupný z WWW http://itslovnik.cz/pojem/warez/?utm_source=cp&utm_medium=link&utm_campaign=cp.

5. *Embedding* [online]. 2016, [cit. 25. 11. 2016]. Dostupný z WWW http://www.streamhosting.cz/cz/podpora/slovnicek/c103.

6. *Direct Connect* [online]. 2016, [cit. 25. 11. 2016]. Dostupný z: WWW https://cs.wikipedia.org/wiki/Direct_Connect.

7. *Cookies* [online]. 2016, [cit. 25. 11. 2016]. Dostupný z WWW http://itslovnik.cz/pojem/cookies/?utm_source=cp&utm_medium=link&utm_campaign=cp.

8. *IS ETŘ* [online]. 2016, [cit. 25. 11. 2016]. Dostupný z WWW http://www.policie.cz/clanek/databaze-is-etr.aspx.

Legislativní dokumenty

1. ČESKO. Zákon č. 40 České národní rady ze dne 9. února 2009 trestní zákoník. In *Sbírka zákonů, Česká republika.* 2009, částka 11. s 354 - 464. ISSN 1211-1244.

2. ČESKO. Ústavní zákon č. 2 České národní rady ze dne 16. prosince 1992 o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky. In: *Sbírka zákonů, Česká republika*. 1993, částka 1. s 17 – 23. ISSN 1211-1244.

3. ČESKO. Zákon č. 141 Československé socialistické republiky ze dne 29. listopadu 1961 o trestním řízení soudním (trestní řád). In *Sbírka zákonů, Československá socialistická republika*. 1961, částka 66. ISSN 333-348.

4. ČESKO. Zákon č. 141 Československé socialistické republiky ze dne 8. prosince 1961 trestní zákon. In *Sbírka zákonů, Československá socialistická republika*. 1961, částka 65. ISSN 313-348.

Seznam zkratek

SKPV – Služba kriminální policie a vyšetřování

OČTŘ – Orgány činné v trestním řízení

P2P – Peer-to-Peer

PC – počítač

LPS – Listina práv a svobod

DoS – Denial of Service

DDoS – Distributed Denial of Service

EUR – Euro

TZ – trestní zákoník

TŘ – trestní řád

ČPU – Česká protipirátská unie

ČNS – IFPI – Mezinárodní federace hudebního průmyslu, z. s.