1 Vymezení základních pojmů

Pojem počítačová kriminalita se pokusila definovat již řada autorů a expertních skupin zabývajících se tímto druhem kriminality. Z českých autorů bych uvedl definici Prof. Porady: „*počítačovou kriminalitou z kriminalistického hlediska rozumíme skupinu trestných činů páchaných prostředky výpočetní techniky v podmínkách komunikačních sítí, systémů, programového vybavení a databází výpočetní techniky".*[1] Počítačová kriminalita se někdy označuje jako kriminalita informačních technologií, někdy se používá názvů cyber-crime, IT crime, computer crime. Kriminalita informačních technologií bývá občas vnímána jako širší pojem než počítačová kriminalita (zahrnuje i kriminalitu v oblasti telekomunikací).[2]

Počítačovou kriminalitou se zabývaly především dvě mezinárodní organizace- Rada Evropy a OSN. Rada Evropy (resp. Komise expertů pro zločin v kyberprostoru) definuje ve Statutu počítačovou kriminalitu jako: „*Trestný čin namířený buďto proti integritě, dostupnosti nebo utajení počítačových systémů nebo trestný čin v tradičním slova smyslu, při kterém je použito moderních informačních a telekomunikačních technologií."* OSN ve svém Manuálu definuje počítačovou kriminalitu takto: *„Počítačovou kriminalitu představují jednak tradiční zločinecké aktivity jako krádež, podvod nebo padělání, tedy činy, které jsou trestné ve většině zemí světa. K tomu se přidružují nové způsoby zneužití počítačů, které jsou, nebo by měly být trestnými"*.[3]

Jako synonymum k pojmu počítačová kriminalita se někdy užívá pojmu kybernetická kriminalita, avšak o synonymum se nejedná. Tento pojem se odvozuje nikoliv od pojmu kybernetika, ale od pojmu

[1] PORADA, Viktor; KONRÁD, Zdeněk. *Metodika vyšetřování počítačové kriminality*. 1. vydání. Praha : Vydavatelství PA ČR, 1997. s. 7

[2] MATĚJKA, Michal. *Počítačová kriminalita*. 1. vydání. Praha : Computer Press, 2002. s. 3

[3] JIROVSKÝ, Václav. *Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha : Grada Publishing, a.s., 2007. s. 4-5

kybernetický prostor[4]. Kybernetickou kriminalitou (kybernalitou) rozumíme takovou činnost, kterou je porušován zákon nebo která je v rozporu s morálními pravidly společnosti. Jedná se o takový druh kriminality, který směřuje proti počítačům, počítačovým systémům a datům nebo je sám počítač prostředkem k spáchání protiprávního počítačového deliktu. Kybernetickou kriminalitu můžeme zjednodušeně definovat jako *„jakýkoliv čin směřující k narušení nebo zneužití počítače nebo počítačového systému a informací v něm obsažených“.*[5]

Dalším relevantním pojmem týkajícím se počítačové kriminality je kyberzločin. Kyberzločin lze definovat jako: „*a) trestný čin ohrožující ICT-informační a síťovou bezpečnost (trestný čin proti počítačové integritě), b) trestný čin využívající ICT ke spáchání tradičních trestných činů (trestný čin vztahující se k počítačům) a c) trestný čin vztahující se k obsahu, jako například dětská pornografie, pomluva a porušení práv k duševnímu vlastnictví (trestný čin vztahující se k obsahu počítačových dat).“* [6]

Všechny kyberzločiny se odehrávají v novém „kybernetickém“ světě, nazývaném kyberprostor (cyberspace). Kyberprostorem označujeme virtuální svět tvořený moderními technologiemi, který existuje paralelně k světu „reálnému“.[7]

V tomto prostoru je třeba nutno vymezit pravidla fungování, která se v některých aspektech vymykají pravidlům, podle kterých žije lidstvo již po staletí. Abychom mohli v tomto prostoru žít a fungovat, je třeba přizpůsobit stará pravidla tomuto vývoji, stanovit pravidla nová, vymezit hranice a meze, ve kterých je třeba se pohybovat a stanovit sankce za překračování těchto mezí. Na rozdíl od fyzického prostoru, kde je každá osoba identifikovatelná, popsatelná,

[4] ŠÁMAL, Pavel a kol. *Trestní zákoník II. §140 až 421 : Komentář*. 1. vydání. Praha : C.H. Beck, 2010. s. 2083

[5] JIROVSKÝ, Václav. *Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha : Grada Publishing, a.s., 2007. s. 91

[6] GŘIVNA, Tomáš a kol. *Kyberkriminalita a právo*. 1. vydání Praha : Auditorium, 2008. s. 34

[7] *Wikipedia.cz* [online]. 2010-04-30 [cit. 2010-08-23]. Kyberprostor. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Kyberprostor>

v kyberprostoru se setkáváme pouze s virtuálním obrazem určitého jedince, který v některých případech může být těžko identifikovatelný, případně jej nelze vůbec identifikovat. Kybernetický prostor nemá hmotnou podstatu, je imaginární. Jeho vznik a existence je však závislá na světě reálném. Komentář k trestnímu zákoníku hovoří o kyberprostoru takto: *„ Kyberprostor je sběrný, popisný termín pro všechno od Internetu a světové sítě až po imaginární a metaforický prostor, který v něm existuje*“.[8]

Softwarové pirátství lze definovat jako *„útoky proti nakládání s počítačovými programy (nelegální kopírování, šíření a plagiátorství programů) k získání prospěchu pro sebe nebo pro jiného, tj. s komerčním využitím“.*[9]

[8] ŠÁMAL, Pavel a kol. *Trestní zákoník II. §140 až 421 : Komentář*. 1. vydání. Praha : C.H. Beck, 2010. s. 2084-2085

[9] SMEJKAL, Vladimír a kol. *Právo informačních a telekomunikačních systémů*. 2. aktualizované a rozšířené vydání. Praha : C.H. Beck, 2004. s. 723

2 Historie počítačové kriminality

Pro počátek počítačového věku byly rozhodující dva momenty. Prvním z nich byl vynález telefonu, který v době svého vzniku s počítačem téměř nesouvisel, ale později umožnil propojení počítačů mezi sebou, neboť první způsoby komunikace mezi počítači byly uskutečněny prostřednictvím telefonní linky. Propojení počítačů prostřednictvím telefonu znamenalo vznik tzv. kyberprostoru. Druhým významným momentem bylo sestrojení prvního počítače ENIAC, který znamenal počátek počítačového věku (14. února 1946). První počítače sice zabíraly celou místnost a stály několik desítek tisíc dolarů, ale informační technologie se od této doby poměrně rychle rozvíjely a počítač se během dvou desetiletí stal relativně snadno dostupnou technologií. [10]

Na konci let šedesátých a v průběhu sedmdesátých let se zrodil z hlediska počítačové kriminality důležitý termín- hacking (hacker). Pojem hacking v původním smyslu slova měl jiný význam, než jej chápeme v současnosti. Hackerem se označovala osoba, zpravidla programátor, který sice zasahoval do počítače, počítačových systémů, programů a dat, ale ne za účelem jejich zneužití nebo zničení. Slovem „hacks“ se označovaly takové zásahy, které měly přimět systém k lepšímu fungování a odstranit jeho chyby a nedostatky. Hacking byl tedy chápán jako pozitivní (prospěšná) činnost programátora.

Na protest proti vietnamské válce začínají vznikat první hackerská hnutí (tzv. yippies). V této době hacking znamená již něco jiného. Jeho cílem už nejsou jen zásahy do systému za účelem odstranění chyb a zdokonalení systému, ale protiprávní nabourávání a zneužívání technologií. Mezi zakladatele tohoto hnutí patřil Abbie Hoffmann a John Draper. Jejich prvotní činnost spočívala v tom, že objevovali způsoby, jak obelstít telefon, aby nemuseli za telefonování platit. Postupně se začali nabourávat do telefonních ústředen,

[10] MATĚJKA, Michal. *Počítačová kriminalita*. 1. vydání. Praha : Computer Press, 2002. s. 19-20

telefonních systémů a postupem času se jejich činnost začala vztahovat i na počítače. Výsledky své „práce“ publikovali v časopise Youth International Party Line. Tato nelegální činnost se později začala označovat jako phreaking. Na konci sedmdesátých let došlo k dalšímu významnému kroku, když vznikla tzv. BBS (Bulletin Board Systém). Na základě toho mohl každý vlastník počítače propojit svůj počítač s telefonní linkou a „vstoupit“ tím do kyberprostoru.[11]

V šedesátých a sedmdesátých letech začíná docházet k podstatnému porušování autorských práv, neboť se začínají kopírovat hudební nahrávky na kotoučové a později kazetové magnetofony.

Za zlomový bod v oblasti informačních technologií lze považovat představení počítače typu IBM PC dne 12. 8.1981. Tento počítač byl cenově dostupný pro širší okruh lidí a tak se postupně dostával do každé domácnosti. Došlo také k již zmíněnému propojení počítače s telefonní linkou a vznikl předchůdce dnešního internetu v podobě systémů BBS. V této době vzniká proslulá hackerská skupina Legion of Doom (Legie zkázy). Jednou z aktivit této skupiny bylo nabourání se do telefonního systému místní telefonní společnosti (tzv. floridský skandál), což však mělo dalekosáhlé důsledky. Došlo k důslednému vyšetřování nejen ze strany telefonní společnosti, ale především ze strany policie a prokuratury (operace Sundevil). V roce 1986 byl Kongresem Spojených států amerických přijat zákon o počítačovém podvodu a zneužití počítače. Na počátku roku 1990 došlo v USA ke kolapsu celostátní telefonní sítě v důsledku softwarové chyby. Tento kolaps byl přesto připisován hackerům a policie začala razantně zasahovat proti hackerským hnutím. Legion of Doom téměř zanikla a někteří její členové byli obžalováni. Vznikl zvláštní útvar pro boj s počítačovými zločinci jak na vnitrostátní, tak federální úrovni (FCIC).[12]

[11] MATĚJKA, Michal. *Počítačová kriminalita*. 1. vydání. Praha : Computer Press, 2002. s. 20-22

[12] Tamtéž s. 22-25

Další významnou akcí v historii počítačové kriminality byl případ zvaný Grateful Dead. Došlo ke krádeži kódu společnosti Apple Macintosh, který byl touto firmou důkladně utajován. FBI při vyšetřování zaměřila svoji pozornost na hackera Johna Barlowa, který patřil do hackerské komunity zvané WELL. Tato komunita sdružovala hackery v původním smyslu tohoto slova a měla značný vliv. John Barlow tuto krádež nespáchal a ostře se ohradil proti jednání policie, která házela hackerskou komunitu „do jednoho pytle" a považovala každého hackera za zločince. To bylo podnětem k tomu, aby společně s Michaelem Kaporem založil Nadaci elektronického pohraničí (EFF), která se zabývala soudními spory a lobbovala za práva osob v oblasti kyberprostoru. Významný případ týkající se otázky postihu hackerů za své jednání byl Dokument 911. Jednalo se o tajný a cenný dokument obsahující kód k systému tísňového volání 911. Tento dokument byl ukraden a následně hackery prodáván na hackerských stránkách. Hackeři byli policií chyceni a postaveni před soud. Nakonec byli zproštěni viny, neboť bylo prokázáno, že informace obsažené v dokumentu jsou poměrně lehce zjistitelné, aniž by muselo dojít k nějakému závažnému nabourání daného systému.[13]

V této době dochází k jedné podstatné změně, mění se typický pachatel počítačového zločinu. Doposud byl hacking spíše intelektuální výzvou, hackeři si ve většině případů dokazovali, že jsou natolik schopní, aby bezpečnostní systémy prolomili. Od konce osmdesátých let se objevuje velký počet hackerů, jejichž cílem není jen získání slávy, ale jejich primárním cílem je materiální zisk- peníze. Na počátku devadesátých let došlo k dvěma významným kauzám- Citibank a Orchard Street Finger-Hackers. V případě Orchard Street došlo k prodeji ukradených kódů umožňujících telefonní spojení ilegálním imigrantům. V případě Citybank došlo k tomu, že hackerská skupina vedená Vladimirem Levinem[14]

[13] MATĚJKA, Michal. *Počítačová kriminalita*. 1. vydání. Praha : Computer Press, 2002. s. 27

[14] Vladimir Levin. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, , last modified on 20. srpna 2010 [cit. 2010-09-27]. Dostupné z WWW: <http://en.wikipedia.org/wiki/Vladimir_Levin>.

protiprávně získala přístup k počítačům a ukradla z účtů deset miliónů dolarů. Toto období je spjato s třemi významnými hackery- Robertem Morrisem, Kevinem Poulsenem a nejvýznamnějším z trojice, Kevinem Mitnickem[15]. Celá devadesátá léta znamenala rozvoj informačních technologií, umožňující nové nelegální aktivity (ty nejvýznamnější jsou popsány v dalších kapitolách této práce). I zde by se dalo zmínit mnoho významných případů (např. Proces Intel z roku 1996, kdy došlo k průmyslové špionáži jednoho zaměstnance společnosti Intel; virové hrozby typu Melissa, která sice neměla destruktivní charakter, ale tím, jak rychle se rozšířila po světě, poukázala na nebezpečnost virů do budoucnosti; DoS útoky, jejichž cílem není cílový počítač poškodit, nýbrž zahltit v takovém měřítku, že přestane fungovat; případ Napster, Yahoo vs. LICRA a další).[16]

Důležitým mezníkem bylo dle mého názoru 11. září 2001, kdy došlo k teroristickému útoku ve Spojených státech amerických. Samotný čin až tak nesouvisel s počítačovou kriminalitou, ale začalo se veřejně diskutovat o tom, jak předejít dalším útokům a o hrozbách dalšího teroristického útoku v souvislosti s použitím informačních technologií.

V posledním desetiletí se objevila celá řada protiprávních činností prováděných prostřednictvím informačních technologií, z nichž nejvýznamnější uvádím v dalších kapitolách této práce.

---

[15] Kevin Mitnick. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, , last modified on 20.září 2010 [cit. 2010-09-27]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Kevin_Mitnick>.

[16] MATĚJKA, Michal. *Počítačová kriminalita*. 1. vydání. Praha : Computer Press, 2002. s. 27-33

3 Dělení počítačové kriminality

V literatuře existuje mnoho způsobů dělení počítačové kriminality. Téměř všechny definice se shodují v tom, že lze počítačovou kriminalitu rozdělit do dvou kategorií[17]:

A) Protiprávní jednání směřující *proti počítači.* Počítač je zde přímo terčem útoku. Dochází k narušení systému za účelem např. krádeže dat, špionáže, bankovního podvodu, zneužití osobních údajů apod.

B) Protiprávní jednání spáchaná s *využitím počítačů*. Počítač v tomto případě slouží pouze jako nástroj trestné činnosti (např. porušování autorského práva).

Z jiného hlediska lze počítačovou kriminalitu rozdělit na[18]:

1) Protiprávní jednání „tradiční“, kde počítač pouze usnadňuje jejich spáchání, ať už je přímo jejich terčem (online loupež v bance) nebo jejich nástrojem (šíření pornografie, extremismus).
2) Protiprávní jednání „zcela nová“, která se objevila s nástupem moderních informačních technologií.

Další klasifikace vychází z Úmluvy Rady Evropy o počítačové kriminalitě, která dělí trestné činy do čtyř kategorií (viz. kapitola 7.1).

[17] MATĚJKA, Michal. *Počítačová kriminalita*. 1. vydání. Praha : Computer Press, 2002. s. 6

[18] Tamtéž s. 7

4 Jednotlivé formy počítačové kriminality a jejich trestněprávní postih

4.1 Trestná činnost proti počítačům a počítačovým systémům

4.1.1 Krádež, loupež

Tato tradiční protiprávní jednání souvisí s počítačovou kriminalitou jen okrajově. O krádeži dle §205 TZ hovoříme v souvislosti s počítačovou kriminalitou tehdy, pokud dojde k odcizení počítače, hardwaru s počítačem souvisejícího, záznamových médií atd.

Stejně tak může být spáchána loupež dle § 173 TZ, pokud je proti jinému použito násilí nebo pohrůžky bezprostředního násilí v úmyslu zmocnit se příslušného zařízení.

4.1.2 Hacking

Termín hacking zjednodušeně znamená proniknutí do systému jinou než standartní cestou a prolomení bezpečností ochrany tohoto systému. V dnešní době je hacking chápán spíše v negativním slova smyslu, tedy jako něco protiprávního. Avšak ne vždy bylo „hackování“ prováděno s úmyslem tento systém poškodit, ale naopak se jednalo o snahu vylepšit bezpečnost tohoto systému a případně odstranit jeho chyby. Postupem času však docházelo k nástupu hackerů, jejichž úmysly byly především materiální a jejichž hlavním cílem bylo někoho poškodit nebo se obohatit.

Dle nového trestního zákoníku je tento druh protiprávního jednání trestný dle §230 TZ, neoprávněného přístupu k počítačovému systému a nosiči informací (anglicky nazýváno termínem „hacking“). Toto ustanovení je v souladu s Úmluvou o počítačové kriminalitě a pachatel může být dle odst. 1 daného ustanovení potrestán trestem

odnětí svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty. Podmínkou trestnosti je, aby pachatel překonal bezpečnostní opatření (tzn. takové opatření, které brání volnému přístupu k počítačovému systému nebo nosiči informací) a získal tím neoprávněně přístup k počítačovému systému nebo jeho části. Odst. 1 neobsahuje znak v podobě úmyslu způsobit škodu nebo jinou újmu, tento znak je zvlášť přitěžující okolností v odstavcích 3 až 5.[19]

4.1.3 Spamming

Spam se dříve užíval zejména pro zasílání nevyžádané elektronické pošty obvykle s reklamním obsahem, později se však rozšířil i na ostatní druhy internetové komunikace (diskuzní fóra atd.).[20] Charakteristickým znakem spammingu je tedy hromadný charakter této zprávy, která je rozesílána na mnoho e-mailů současně. Dalším důležitým znakem je nevyžádanost těchto zpráv.[21] Tento způsob nepříjemného obtěžování uživatele vznikl v souvislosti s užíváním e-mailu. E-mailové adresy, které jsou cílem pro spamming, jsou získávány nejrůznějšími způsoby (www konference, icq, různé typy registračních stránek poskytujících služby atd.). Vzniká celá řada programů, která jsou schopná tyto spamy v elektronické poště filtrovat. Avšak i spameři se postupně přizpůsobují a jsou schopní na tyto filtrovací a ochranné mechanismy reagovat a obejít je.

Co se týče právního postihu spammingu, samotný spamming podle českého trestního práva patrně postižitelný není. Pokud však bude možno z adresy dostatečně identifikovat příjemce tohoto spamu,

---

[19] ŠÁMAL, Pavel a kol. *Trestní zákoník II. §140 až 421 : Komentář*. 1. vydání. Praha : C.H. Beck, 2010. S. 2086

[20] *Wikipedia.cz* [online]. 2010-08-18 [cit. 2010-08-23]. Spam. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Spam >.

[21] JIROVSKÝ, Václav. *Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha : Grada Publishing, a.s., 2007. s. 104

mohl by za určitých okolností naplňovat skutkovou podstatu trestného činu neoprávněného nakládání s osobními údaji dle §180 TZ.

Posílání spamů je také postižitelné podle jiných právních předpisů jako správní delikt (např. podle zákona o elektronických komunikacích, zákona o regulaci reklamy atd.).

4.1.4 Phreaking

Tímto pojmem nazýváme činnost, kdy dochází k zneužívání telekomunikačních služeb, aniž by došlo k zaplacení této služby. Jedná se o případy, kdy osoby neoprávněně užívají telekomunikační služby. Zpočátku se jednalo o nabourávání do telefonních linek, které umožňovalo bezplatné volání do kterékoli části země, v závažnějších případech odposlouchávání některých telefonních hovorů. Později však došlo k nabourávání počítačových systémů prostřednictvím těchto telekomunikačních prostředků. [22]

Z hlediska platného trestního práva by se dala tato činnost podřadit trestný čin poškození cizí věci (§228 TZ), neoprávněný přístup k počítačovému systému a nosiči informací (§ 230 TZ), poškození a ohrožení provozu obecně prospěšného zařízení (§ 276 TZ), porušování tajemství dopravovaných zpráv (§ 182 TZ).

Trestný čin poškození a ohrožení provozu obecně prospěšného zařízení přichází v úvahu v případě, že dojde k poškození majetku jiných osob. K trestnému činu porušování tajemství dopravovaných zpráv dojde v případě, že někdo úmyslně poruší tajemství posílané prostřednictvím sítě elektronických komunikací.[23] Přenosem prostřednictvím sítě elektronických komunikací rozumíme např. telefax, přenos prostřednictvím e-mailu a dalších komunikačních programů- Skype, ICQ, Microsoft MSN .[24]

---

[22] MATĚJKA, Michal. *Počítačová kriminalita*. 1. vydání. Praha : Computer Press, 2002. s. 72

[23] §182 a § 276 zákona č. 40/2009 Sb., trestní zákoník

[24] ŠÁMAL, Pavel a kol. *Trestní zákoník II. §140 až 421 : Komentář*. 1. vydání. Praha : C.H. Beck, 2010. 1630

4.1.5 Carding

Obecně se tímto pojmem označuje zneužití platební karty. Tato trestná činnost se dostala do popředí zejména v posledním desetiletí, kdy se placení (nebo vybírání peněžních prostředků) prostřednictvím platební karty stalo běžnou součástí života téměř každého člověka. Platební karty umožňují lidem vybrání peněz kdykoli a téměř kdekoli. Na druhou stranu však každý tento výběr dává možnost k zneužití této karty.

Způsobů zneužití platební karty je mnoho, mezi nejprimitivnější patří krádeže čísla platební karty, případně karty samotné, dále různé generátory (které jsou schopné vygenerovat číslo platební karty), sociální inženýrství. Nové způsoby „vykrádání“ platebních karet se objevily v poslední době v souvislosti s platbami přes internet.[25]
Poměrně novou metodou zneužití platební karty je tzv. „skimming“, ke kterému došlo již v několika případech i u nás.[26] Skimming znamená kopírování platebních karet prostřednictvím speciálního kopírovacího zařízení, které je umístěno na bankomat. Přístroj na skimming se vloží přímo do panelu bankomatu a snímá informace z platební karty při jejím vložení do bankomatu. Zloději navíc instalují kameru, která zachytí PIN při zadávání do klávesnice.[27]

Dle současného trestního zákoníku mohou tato jednání naplňovat skutkové podstaty trestných činů neoprávněného opatření, padělání a pozměnění platebního prostředku (§234 TZ), podvodu (§209 TZ), případně neoprávněného nakládání s osobními údaji (§180 TZ).

Starý trestní zákon (č. 140/1961 Sb.) obsahoval ustanovení o trestném činu neoprávněného držení platební karty. Dle nového trestního zákoníku je trestné opatření, padělání a pozměnění

[25] MATĚJKA, Michal. *Počítačová kriminalita*. 1. vydání. Praha : Computer Press, 2002. s. 58

[26] *Idnes.cz* [online]. 2010-08-20 [cit. 2010-08-23]. Na bankomatech České spořitelny opět byly falešné čtečky. Dostupné z WWW: <http://ekonomika.idnes.cz/na-bankomatech-ceske-sporitelny-opet-byly-falesne-ctecky-pz0-/ekonomika.asp?c=A100816_182730_ekonomika_fih) >

[27] *Penize.cz* [online]. 2010-03-10 [cit. 2010-08-23]. Skimming, phishing, pharming. Dostupné z WWW: < http://www.penize.cz/debetni-karty/69791-skimming-phishing-pharming

platebního prostředku. Toto ustanovení tedy poskytuje ochranu českým i jiným než tuzemským platebním prostředkům (tzn. nejen platební kartě, ale i elektronickým penězům, příkazu k zúčtování, cestovnímu šeku atd.).[28]

4.1.6 Průmyslová špionáž

V odborné literatuře je definována například takto: *„Průmyslová špionáž je špionáž páchaná s komerčními cíli a ve své podstatě nemá nic společného s aktivitami rozvědky, které jsou zaměřeny na bezpečnost státu*.“[29] Jedná se tedy o formu informačního boje mezi korporacemi, jejímž cílem je získání podstatných informací o činnosti a technologiích jiných. Tato forma protiprávní činnosti existovala již před vznikem počítače, ale se vznikem počítače a internetu se hodně rozšířila.[30] Vznikla tím možnost nabourat se prostřednictvím informačních technologií do utajených a chráněných složek jiných firem a získat cenné informace. Tyto informace se dají získat různými způsoby- odposlechy telefonních linek, mobilních telefonů, dálkové mikrofony, skryté kamery, ale také nabourání do systému hackerem a tak dále.

Průmyslová špionáž může mít však i legální část nazývanou „business inteligence“. Jedná se o zaměstnance (skupiny zaměstnanců), jejímž úkolem je legální shromažďování informací o konkurenci. Jejich činnost spočívá v získávání informací publikovaných v časopisech, novinách, prezentovaných na konferencích a také o legální sledování konkurenčních aktivit.[31]

---

[28] ŠÁMAL, Pavel a kol. *Trestní zákoník II. §140 až 421 : Komentář*. 1. vydání. Praha : C.H. Beck, 2010. s. 2128

[29] JIROVSKÝ, Václav. *Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha : Grada Publishing, a.s., 2007. s. 169

[30] MATĚJKA, Michal. *Počítačová kriminalita*. 1. vydání. Praha : Computer Press, 2002. s. 52

[31] JIROVSKÝ, Václav. *Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha : Grada Publishing, a.s., 2007. s. 169-170

4.2 Trestná činnost související s obsahem

4.2.1 Závadná pornografie

Šíření závadné pornografie se stalo v souvislosti s rozvojem internetu poměrně častou nelegální aktivitou. Internet je v tomto případě ideálním místem, kde lze tyto materiály získávat a na druhou stranu je nelegálně rozšiřovat.

Nový trestní zákoník ve svých ustanoveních implementuje závazky vyplývající s mezinárodních smluv a práva EU. Jedná se zejména o Úmluvu o ochraně dětí před sexuálním vykořisťováním a zneužíváním ze dne 25.10.2007, která postihuje nejen výrobu a šíření dětské pornografie, ale též její získání a držení. Z aktů práva EU se jedná zejména o rámcové rozhodnutí Rady 2000/275/JHA ze dne 29.5.2000 o boji proti dětské pornografii na internetu. Nejdůležitější úmluvou samozřejmě zůstává Úmluva o kybernetické kriminalitě.[32]

Z hlediska českého trestního práva je otázka šíření pornografie řešena v §191 až 193 TZ. Jedná se o trestné činy šíření pornografie, výroba a jiné nakládání s dětskou pornografií a zneužití dítěte k výrobě pornografie. V § 191 TZ uvádí trestní zákoník jednotlivé formy nabízení závadné pornografie a stanoví podmínky pro to, aby se toto šíření stalo trestným dle českého trestního práva. Dle § 192 týkajícího se dětské pornografie se považuje za trestné kromě různých forem šíření dětské pornografie také její přechovávání.[33] Důvodem pro kriminalizaci přechovávání dětské pornografie je její větší závažnost oproti jiným formám pornografie. Její prohlížení patrně trestné nebude, pokud si jej osoba neukládá na nosič informací.[34]

---

[32] ŠÁMAL, Pavel a kol. *Trestní zákoník II. §140 až 421 : Komentář*. 1. vydání. Praha : C.H. Beck, 2010. s. 2085

[33] JELÍNEK, Jiří a kol. *Trestní právo hmotné*. 1. vydání. Praha : Leges, 2009. s. 560

[34] JELÍNEK, Jiří a kol. *O novém trestním zákoníku : Sborník příspěvků z mezinárodní konference Olomoucké právnické dny, květen 2009*. 1. vydání. Olomouc : Leges, 2009. s. 91-93

4.2.2 Extremismus

Internet je ideálním místem a komunikačním prostředkem pro extremistické skupiny. Objevuje se zde celá řada extremistických hnutí- pravicové, levicové, náboženské skupiny a hnutí a jiné. Internet je prostředím, kde mají tyto skupiny možnost prezentovat a vyjadřovat své názory, publikovat, účastnit se internetových diskuzí a celkově prezentovat svou ideologii a myšlení. Jedná se zároveň o významný komunikační prostředek jak uvnitř extremistické organizace, tak při navazování kontaktů s jinými skupinami, uvnitř jednoho státu či v zahraničí.

Rozvoj informačních technologií, resp. internetu, tedy určitě znamenal i rozvoj extremismu. Pro mnoho lidí se extremistické názory stávají více dostupnými a mají možnost se díky tomuto komunikačnímu prostředku zapojit do extremistických aktivit, i když v místě svého bydliště zrovna žádnou extremistickou skupinu nemají. Stejně tak členové těchto skupin mají možnost nové členy prostřednictvím internetu verbovat. Šíření extremistických informací a propagandy prostřednictvím internetu není téměř vůbec nákladné, což je pro autory velká výhoda. Další nespornou výhodou a hlavním důvodem, proč se spousta lidí uchyluje k projevování svých extremistických myšlenek prostřednictvím internetu, je to, že autor těchto projevů je těžko identifikovatelný.[35]

Z hlediska právní úpravy existuje řada dokumentů mezinárodní povahy obsahující určité principy a zásady, které by neměly být překročeny a měly by být dodržovány v každém státě. Z hlediska úpravy vnitrostátní však můžeme najít značné odlišnosti. V některých státech jsou trestné již tzv. verbální delikty, které se dají spáchat již vyslovením určitého názoru s extremistickým či rasistickým podtextem a osoba spáchá splněním některých dalších podmínek stanovených v zákoně trestný čin. Naopak jsou země, kde byl zákonodárce benevolentnější a za trestný čin označil až určitý

[35] GŘIVNA, Tomáš a kol. *Český právní řád a ochrana kyberprostoru : vybrané problémy*. Praha : Karolinum, 2008. s. 37-39

spáchaný skutek související s extremismem. Právě tohle se jeví jako problém, neboť internet má exteritoriální povahu a určité jednání provedené prostřednictvím internetu může být v jedné zemi trestné a v jiné nikoliv.[36]

Z hlediska mezinárodní právní úpravy je třeba uvést, že Úmluva o počítačové kriminalitě otázku extremismu neřeší a zabývá se jí Dodatkový protokol k Úmluvě o počítačové kriminalitě týkající se kriminalizace činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů. Ustanovení o extremismu a xenofobii byly z Úmluvy o počítačové kriminalitě vynechány z toho důvodu, že bylo třeba, aby tuto Úmluvu ratifikovaly i Spojené státy americké, které jsou však v těchto otázkách značně liberálnější. Protokol byl přijat převážně za tím účelem, aby se harmonizovalo trestní právo hmotné v otázkách rasismu, extremismu a xenofobie šířené prostřednictvím počítačových sítí. Dalším důvodem přijetí Protokolu byla snaha o zlepšení mezinárodní spolupráce nutná k tomu, aby byly takové osoby identifikovány a za své činy potrestány.[37]

Protokol vymezuje čtyři způsoby škodlivého jednání, které by měly být považovány dle vnitrostátního trestního práva za trestný čin[38]:

- rasisticky a xenofobně motivovaná urážka
- rasisticky a xenofobně motivovaná pohrůžka
- šíření rasistických a xenofóbních materiálů
- popření, hrubé snižování, schvalování a ospravedlnění genocidy a zločinů proti lidskosti

[36] MATĚJKA, Michal. *Počítačová kriminalita*. 1. vydání. Praha : Computer Press, 2002. s. 67-68

[37] GŘIVNA, Tomáš a kol. *Kyberkriminalita a právo*. 1. vydání Praha : Auditorium, 2008. s. 144-146

[38] Tamtéž s. 146

Trestný je i návod a pomoc k těmto uvedeným jednáním. Česká Republika Protokol podepsala 9. února 2005, ale dosud jej neratifikovala.

Z hlediska vnitrostátního práva obsahuje český trestní zákoník řadu ustanovení poskytujících ochranu před extremismem (zahrnující i ochranu před jeho projevy v kyberprostoru). Jedná se o teroristický útok dle §311 TZ, násilí proti skupině obyvatelů a jednotlivci dle §352 TZ, hanobení národa, rasy, etnické nebo jiné skupiny osob dle §355 TZ, podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod dle §356 TZ, založení, podpora a propagace hnutí směřujícího k potlačení práv a svobod člověka dle §403 TZ, projev sympatií k hnutí směřujícímu k potlačení práv a svobod člověka dle §404 TZ, popírání, zpochybňování, schvalování a ospravedlňování genocidia dle § 405 TZ a podněcování útočné války dle §407 TZ. [39]

Rasismus, extremismus a xenofobie patří mezi vážné problémy dnešní společnosti. Z toho důvodu je třeba sledovat činnost těchto skupin a hnutí i v kyberprostoru a jejich nežádoucí chování rázně postihovat. Autoři rasistických projevů na internetu by měli být vyhledáni a za svou činnost přísně potrestáni.

4.3 Trestná činnost s využitím počítače

4.3.1 Podvod a zpronevěra

S rozvojem informačních technologií se podvod stal poměrně častou nelegální činností prováděnou prostřednictvím internetu. Ve většině případů je však i toto jednání je postižitelné dle současné právní úpravy. Podvodných jednání na internetu je celá řada- aktivity označované jako letadla či pyramidy, podvodné e-maily, nabízení

[39] zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů

neexistujících služeb (často v souvislosti s pornografií), falešné e-shopy[40]. Tato jednání mají jeden charakteristický znak, pachatelé vylákají od osob peníze pod záminkou další výdělku nebo poskytnutí nějaké služby a tyto peníze jim ve většině případů už nevrátí.

Výše uvedená podvodná jednání mohou být trestná dle § 209 trestního zákoníku.

Další nelegální činností související s počítačem je počítačová zpronevěra. Jedná se o případy, kdy zaměstnanec mající přístup k finančním prostředkům společnosti tyto prostředky zpronevěří a užije k tomuto jednání počítač. Toto jednání může naplňovat skutkovou podstatu trestného činu zpronevěry dle § 206 TZ.

4.3.2 Phishing, Pharming

Jedná se o způsoby podvodného jednání prováděného prostřednictvím internetu. Phishingem nazýváme nelegální činnost, kdy se pachatel snaží prostřednictvím internetu získat podvodným jednáním citlivé informace o jiných osobách (čísla kreditních karet, e-maily, různá přístupová hesla). Charakteristickým rysem tohoto jednání je rozesílání e-mailů, které na první pohled vypadají jako žádosti zaslané bankami a jinými obdobnými institucemi za účelem získání osobních (identifikačních) údajů od jejich klientů. Oběti těchto trestných činů se nechají oklamat uvedeným jednáním a poskytnou své identifikační údaje, které mohou vést například k vykradení jejich účtu.[41]

V poslední době se objevuje obdobná činnost zvaná VoIP phishing. Místo zprávy prostřednictvím elektronických komunikací pachatel zavolá jiným osobám a představí se jako zástupce např. banky a požaduje sdělení identifikačních údajů.[42]

---

[40] MATĚJKA, Michal. *Počítačová kriminalita*. 1. vydání. Praha : Computer Press, 2002. s. 60-63

[41] *Hoax.cz* [online]. 2009-01-20 [cit. 2010-08-23]. Co-je-to-phishing. Dostupné z WWW: <http://www.hoax.cz/phishing/co-je-to-phishing>

[42] *Interval.cz* [online]. 2006-07-26 [cit. 2010-08-23]. Phishing aneb rhybaření 1. Dostupné z WWW: <http://interval.cz/clanky/phishing-aneb-rhybareni-1/>

Další protiprávní podvodné jednání, pharming, se podobá výše popsanému phishingu. Stejně jako u phishingu je motivem jednání pachatele získání důležitých osobních a identifikačních informací od oběti. Principem je „*napadení DNS (databáze, která obsahuje systém internetových domén a příslušných adres) nebo přepsání IP adresy, což způsobí přesměrování klienta na stránky internetového bankovnictví“*.[43]

Pachatel se snaží získat identifikační údaje regulérního uživatele internetového bankovnictví, platebního systému, různých internetových obchodů. Poté, co tyto potřebné údaje získá, může oběti vykrást účet nebo získat některé další citlivé soukromé údaje.[44]

4.3.3 Sniffing

Sniffingem rozumíme neoprávněné monitorování (odposlouchávání) elektronické komunikace.[45] Jedná se o činnost, kdy komunikace na internetu je monitorována subjektem, který není adresátem této komunikace. Tento subjekt získává důležité informace (e-maily, hesla, soubory atd.), které mu následně umožňují páchání další trestné činnosti, např. průnik do jiného systému. Proti těmto neoprávněným zásahům se lze bránit šifrováním elektronické komunikace. Záznamy o provozu sítě a ostatní záznamy umožňující identifikovat osobu jsou chráněny podle telekomunikačního zákona a zákona na ochranu osobních údajů. Správce sítě tedy není oprávněn poskytnout tyto informace třetím osobám, může být však o jejich poskytnutí požádán Policií ČR. [46]

Z hlediska trestněprávní kvalifikace lze sniffing podřadit pod TČ porušování tajemství dopravovaných zpráv dle §182 TZ a porušování

---

[43] *Wikipedia.cz* [online]. 2010-03-01 [cit. 2010-08-23]. Pharming. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Pharming>

[44] *Lupa.cz* [online]. 2007-03-23 [cit. 2010-08-23]. Pharming je zpět a silnější. Dostupné z WWW: <http://www.lupa.cz/clanky/pharming-je-zpet-a-silnejsi/>.

[45] JIROVSKÝ, Václav. *Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha : Grada Publishing, a.s., 2007. s. 106

[46] MATĚJKA, Michal. *Počítačová kriminalita*. 1. vydání. Praha : Computer Press, 2002. s. 74

tajemství listin a jiných dokumentů uchovávaných v soukromí dle §183 TZ. V novém trestním zákoníku byla i v tomto případě zohledněna Úmluva o počítačové kriminalitě a daná ustanovení se výslovně vztahují i na elektronickou a datovou komunikaci.

Ustanovení trestního zákoníku o porušování tajemství dopravovaných zpráv obsahuje v odstavcích 1 a 2 dvě základní skutkové podstaty a v odstavci 5 zvláštní skutkovou podstatu. Z hlediska počítačové kriminality je pro nás podstatné v odst. 1 písm. b), které poskytuje ochranu *„proti úmyslnému porušení tajemství posílané zprávy prostřednictvím sítě elektronických komunikací“* a dále písm. c), které chrání „*proti úmyslnému porušení tajemství neveřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci“*.[47] Odst. 2 obsahuje základní skutkovou podstatu, která sankcionuje prozrazení nebo užití tajemství, o němž se dozvěděl (kromě jiných v zákoně uvedených způsobů) prostřednictvím přenosu sítě elektronických komunikací, který nebyl určen jemu. Zvláštní skutková podstata se týká trestnosti *„provozovatele poštovních služeb, telekomunikační služby nebo počítačového systému nebo kohokoli jiného vykonávajícího komunikační činnosti“*.[48]

4.3.4 Elektronická pomluva, msta, útoky na čest

Jeden z nejstarších trestných činů, pomluva, dostal s rozvojem informačních technologií nový rozměr. Pachatelům se tímto dostal do rukou prostředek, jak relativně jednoduše tento trestný čin spáchat. Každá osoba, mající přístup k počítači a internetu, se může dopustit tohoto jednání. Kromě jednoduchosti se zde projevuje další aspekt, anonymita takového jednání. Pachatelé si často myslí, že prostřednictvím internetu tento trestný čin (v některých případech si

[47] §182 zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů

[48] ŠÁMAL, Pavel a kol. *Trestní zákoník II. §140 až 421 : Komentář*. 1. vydání. Praha : C.H. Beck, 2010. s. 1620-1630

patrně ani neuvědomují, že se o trestný čin jedná) páchají anonymně a nemohou být zjistitelní a případně postižitelní, ale opak je pravdou. Šíření nepravdivých údajů, případně pravdivých údajů zkresleně, může poškodit osobu jak v osobním, tak v profesním životě a může mít nenapravitelné důsledky.

Z hlediska trestního práva je toto jednání postižitelné dle §184 TZ, trestného činu pomluvy. Příslušné ustanovení poskytuje ochranu cti a dobré pověsti člověka před pomluvou, která může vážným způsobem narušit jeho společenský a profesní život. Odstavec 2 uvádí, že tento trestný čin může být spáchán mimo jiné i prostřednictvím veřejně přístupné počítačové sítě a jiným obdobně účinným způsobem. Veřejně přístupnou počítačovou sítí se rozumí *„funkční propojení počítačů s cílem vytvořit informační systém pracující s tzv. dálkovým přístupem“.* [49]

4.3.5 Hoaxes, urban legends

Dalšími protiprávními činnostmi souvisejícími s informačními technologiemi jsou tzv. hoaxes (poplašné či podvodné zprávy a varování), urban legends (různé druhy historek, mýtů) a další způsoby vyvolání chaosu prostřednictvím internetu. Tyto zprávy mohou mít různý charakter a různou míru závažnosti. Chytře formulovaná zpráva však může u lidí vyvolat paniku a chaos a vzhledem k povaze internetu se rozšíří do všech koutů světa během jediného momentu. Můžeme rozlišovat několik forem těchto zpráv: poplašné zprávy (snaží se manipulovat s adresátem zprávy, aby určitým způsobem jednal nebo něco konal), zábavné (jedná se často o řetězové maily kolující v elektronických poštách, které si mezi sebou přeposílají přátelé), různé druhy proseb.[50] Konkrétně se může se jednat o poplašné zprávy upozorňující na teroristický útok, zprávy týkající se nakažlivých chorob, varování o škodlivosti různých

[49] ŠÁMAL, Pavel a kol. *Trestní zákoník II. §140 až 421 : Komentář*. 1. vydání. Praha : C.H. Beck, 2010. s. 1642-1644

[50] *Wikipedia.cz* [online]. 2010-03-31 [cit. 2010-08-23]. Hoax. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Hoax >

produktů, mobilních telefonů atd..[51] Ve většině případů se bude jednat o zprávy neškodné, které člověk nebere vážně, ale pokud tato zpráva je formulována tak, aby vzbudila znepokojení u většího počtu lidí, může se dle platného trestního práva jedna o trestný čin šíření poplašné zprávy dle §357 TZ.

Příslušné ustanovení obsahuje přísnější trestní sankci v odstavci 2, pokud „*pachatel úmyslně způsobí nebezpečí vážného znepokojení alespoň části obyvatelstva nějakého místa tím, že tuto poplašnou zprávu nebo jinou nepravdivou zprávu sdělí mimo jiné hromadnému informačnímu prostředku“*. Mezi hromadné informační prostředky můžeme vedle tisku, televize a rozhlasu řadit i Internet, pokud plní roli hromadného sdělovacího prostředku.[52]

4.3.6 Cyberstalking

Nový trestní zákoník uvádí v hlavě X (trestné činy proti pořádku ve věcech veřejných) v § 354 nový trestný čin- nebezpečné pronásledování. V zahraničí se toto jednání často označuje jako stalking. Vzhledem k tomu, že docházelo poslední dobou stále častěji k případům pronásledování a v horších případech i následného ublížení na zdraví či způsobení jiné újmy, bylo toto jednání zahrnuto v TZ pod samostatný paragraf. Existuje řada definic stalkingu, jak v české odborné literatuře, tak zahraniční. Stalking můžeme vymezit jako *„různé varianty pronásledování v podobě více či méně zřetelného zastrašování či vyhrožování oběti, zahrnující jak psychické, tak až její fyzické terorizování“.*[53] Jedná se tedy o takové chování, kdy pachatel pronásleduje určitou osobu.

V souvislosti s informačními technologiemi můžeme hovořit o tzv. cyberstalkingu. Toho se dopustí osoba, která jiného dlouhodobě

[51] MATĚJKA, Michal. *Počítačová kriminalita*. 1. vydání. Praha : Computer Press, 2002. s. 69

[52] ŠÁMAL, Pavel a kol. *Trestní zákoník II. §140 až 421 : Komentář.* 1. vydání. Praha : C.H. Beck, 2010. s. 3024

[53] Tamtéž s. 3005

pronásleduje tím, že jej vytrvale prostřednictvím prostředků elektronických komunikací kontaktuje a toto jednání je způsobilé vzbudit v něm důvodnou obavu a jeho život nebo zdraví nebo o život a zdraví osob jemu blízkých.[54] Cyberstalking může zahrnovat zasílání nevyžádaných mailů a zpráv (které obsahují pro adresáta nepříjemný obsah), posílání zpráv prostřednictvím chatů a blogů, různé způsoby šíření pomluv prostřednictvím internetu, posílání spamů a různé druhy útoků zasahujících počítač oběti.[55]

Zahrnutí stalkingu do nového trestního zákoníku bylo podle mého názoru nutným krokem, neboť těchto jednání neustále přibývalo a dle minulé právní úpravy nemohlo být toto protiprávní jednání efektivně postihováno. V případě cyberstalkingu se na první pohled zdá, že samotné jednání není až tak škodlivé, ale opak je pravdou. Neustálé pronásledování osoby prostřednictvím internetu, zasílání výhrůžných e-mailů, pomlouvání na veřejných fórech může mít nepříznivý vliv na osobní i profesní život oběti stalkingu.

4.3.7 Padělání

V dřívější době bylo padělání listin, bankovek a jiných veřejných listin poměrně složitou záležitostí. Rozvoj moderní techniky padělání a pozměňování dokumentů podstatně usnadnil, neboť s sebou přinesl kvalitní grafické programy, software, kvalitní technologii tisku.[56] Na druhou stranu se však začaly tisknout bankovky a jiné veřejné listiny opatřené různými ochrannými prvky podstatně ztěžující či znemožňující jejich padělání (mezi tzv. prvky peněz patří např. vodoznak, okénkový proužek, skrytý obrazec, mikrotext).[57]

---

[54] ŠÁMAL, Pavel a kol. *Trestní zákoník II. §140 až 421 : Komentář*. 1. vydání. Praha : C.H. Beck, 2010. s. 3003

[55] JELÍNEK, Jiří a kol. *Trestní právo hmotné*. 1. vydání. Praha : Leges, 2009. s. 787-788

[56] MATĚJKA, Michal. *Počítačová kriminalita*. 1. vydání. Praha : Computer Press, 2002. s. 62-63

[57] JELÍNEK, Jiří a kol. *Trestní právo hmotné*. 1. vydání. Praha : Leges, 2009. s. 632

Trestní zákoník obsahuje ustanovení o padělání a pozměnění peněz v § 233, padělání a pozměňování známek v § 246, padělání a pozměnění předmětů k označení zboží pro daňové účely a předmětů dokazujících splnění poplatkové povinnosti v § 245 a padělání a pozměnění veřejné listiny v § 348. K padělání těchto peněz, dokumentů a veřejných listin zpravidla slouží moderní výpočetní technika a příslušný software.

Zvláštní skutkovou podstatou je potom trestný čin výroba a držení padělatelského náčiní dle §236 TZ. Zařízením k padělání a pozměnění se v tomto případě rozumí jakýkoli přístroj nebo jiné technické zařízení přizpůsobené pachatelem k padělání a pozměnění peněz, veřejných listin a jiných dokumentů.[58]

4.3.8 Neoprávněné nakládání s osobními údaji

V poslední době se internet stal součástí téměř každé domácnosti. Lidé si zřizují e-maily, zakládají si profily na různých internetových sítích (Facebook, Twitter) a na seznamkách, instalují si komunikační programy (ICQ, QIP), píší na svůj blog, účastní se internetových diskuzí a tímto jednáním vkládají své osobní informace na internet.

Neoprávněné nakládání s osobními údaji může být postihnuto jednak z hlediska trestního práva, jednak z hlediska správního práva. Z hlediska správního práva připadá v úvahu zákon č. 101/2000 Sb., o ochraně osobních údajů. Který obsahuje i případné sankce za neoprávněné nakládání s osobními údaji.[59]

Trestní právo obsahuje v § 180 TZ trestný čin neoprávněné nakládání s osobními údaji. Ustanovení obsahuje dvě samostatné základní skutkové podstaty. První skutková podstata postihuje jednání, kdy osoba „*neoprávněně sdělí, zpřístupní, zveřejní, jinak*

[58] ŠÁMAL, Pavel a kol. *Trestní zákoník II. §140 až 421 : Komentář*. 1. vydání. Praha : C.H. Beck, 2010. s. 2159

[59] §44 zákona č. 100/2001 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů

zpracovává nebo si přisvojí osobní údaje, které byly získané v souvislosti s výkonem veřejné moci a způsobí tím vážnou újmu na právech a oprávněných zájmech osoby, jíž se tyto osobní údaje týkají". Druhá skutková podstata se týká takového jednání, kdy pachatel „*poruší státem uloženou nebo uznanou povinnost mlčenlivosti tím, že zveřejní, sdělí nebo zpřístupní třetí osobě osobní údaje získané v souvislosti s výkonem svého povolání, zaměstnání nebo funkce a způsobí tím vážnou újmu na právech a oprávněných zájmech osoby"*.[60]

Dle §180 odst. 3 písm. b) lze tento trestný čin spáchat prostřednictvím veřejně přístupné počítačové sítě nebo jiným obdobným způsobem. Veřejně přístupnou počítačovou síti se v tomto případě myslí např. internet, Minitel.[61]

Trestní postih se tedy týká informací získaných v souvislosti s výkonem veřejné moci, povolání nebo zaměstnání, zatímco správní postih za toto jednání se týká informací získaných jinak (např. v soukromé sféře).

V souvislosti s užíváním sociálních sítí je třeba zmínit, že lidé často své osobní údaje nejen nechrání, ale veřejně vystavují a dávají k dispozici, takže jejich zneužití je poměrně jednoduché. Proto by si měl každý uvědomit, co všechno na internetu sdílí dalším uživatelům a jestli tyto údaje nejsou natolik citlivé, že by ho mohly nějakým způsobem poškodit.

4.3.9 Kyberterorismus

Obecně lze terorismus definovat jako: „*extremistický směr, jehož prostředkem je teror, využívající jako prostředek nátlaku psychické nebo fyzické násilí, výhrůžky a vydírání vytváření strachu a*

[60] ŠÁMAL, Pavel a kol. *Trestní zákoník II. §140 až 421 : Komentář.* 1. vydání. Praha : C.H. Beck, 2010. s. 1607-1610

[61] Tamtéž s. 1613

další formy násilí“.[62] Existuje několik různých druhů terorismu, např. náboženský terorismus, kriminální terorismus, politický terorismus atd. V této kapitole bych se však zabýval terorismem, který se týká informačních technologií- tzv. kyberterorismus. Tímto pojmem se rozumí *„ zneužívání výpočetní a telekomunikační techniky včetně internetu jako prostředku a prostředí pro uskutečnění teroristického útoku“*.[63] Jedná se o činnost, která je stejně jako klasický terorismus motivována nábožensky nebo politicky a je zpravidla prováděna jednotlivcem nebo menšími organizovanými skupinami. Kyberterorismus se vyznačuje protiprávními útoky nebo nebezpečím útoku proti počítačům a počítačovým sítím v kyberprostoru. Směřuje proti jednotlivci, skupině osob nebo společnosti jako celku s cílem způsobit jim škodu a vzbudit v nich strach.[64]

V posledních letech se počet teroristických akcí podstatně zvýšil a jednotlivé země přijaly různé bezpečnostní opatření, které by měly těmto útokům zabránit. Teroristé budou do budoucna hledat nové cesty, jak provést útoky a přitom způsobit značnou škodu na životech či majetku osob. Podle mého názoru by právě tento druh terorismu mohl být v budoucnu velkým nebezpečím. Lidé používají informační technologie stále častěji a tím se vystavují možnosti nebezpečí útoku prostřednictvím počítače a internetu. Proto nesmíme nebezpečí kyberterorismu podceňovat a je třeba učinit potřebná opatření k tomu, aby nemohlo k těmto útokům docházet.

4.4 Trestná činnost související s porušováním autorských a jiných práv

4.4.1 Warez

[62] KUCHTA, Josef a kol. *Základy kriminologie a trestní politiky*. 1. vydání. Praha : C.H. Beck, 2005. s. 490

[63] JIROVSKÝ, Václav. *Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha : Grada Publishing, a.s., 2007. s. 128

[64] Tamtéž s. 129-130

Tímto pojmem označujeme trestnou činnost, která se vyznačuje výrobou a šířením pirátského softwaru. Tato nelegální činnost vznikla již před vznikem internetu samotného, kdy docházelo ke kopírování audio kazet a později i videokazet.[65] Internet však tuto činnost podstatně usnadnil, neboť umožnil šíření pirátských kopií filmů, her, softwaru i hudby zdarma. Někdy dokonce dochází k tomu, že část těchto pirátských kopií je dostupná na internetu ještě předtím, než je oficiálně představen originál.

Toto jednání může dle českého trestního zákoníku naplňovat skutkovou podstatu trestného činu dle § 270, porušení autorského práva, práv souvisejících s právem autorským a práv k databázi. Tento čin je spáchán jednáním, kdy někdo *„neoprávněně zasáhne nikoli nepatrně do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, zvukovému a zvukově obrazovému záznamu, rozhlasovému a televiznímu vysílání nebo databázi“.*[66] V tomto případě jde o normu trestního práva s blanketní dispozicí, neboť odkazuje na AZ[67] a další právní předpisy tento zákon provádějící.

4.4.2 Cracking

Pojem cracking úzce souvisí s výše zmíněnými pojmy hacking a warez. Jedná se o takový zásah do systému, jehož cílem je prolomení ochrany proti kopírování nebo neoprávněnému použití. Cracking používá celou řadu metod k nabourání systému, které vedou nejen k porušování autorských práv, ale i k prolomení bezpečnostní ochrany systému.[68] Cracking se používá k proniknutí do systému, kdy cílem není zprovoznění určitého programu, ale zjištění informací

[65] JIROVSKÝ, Václav. *Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha : Grada Publishing, a.s., 2007. s. 68

[66] §270 odst. 1 zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů

[67] Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a změně některých dalších zákonů (autorský zákon)

[68] MATĚJKA, Michal. *Počítačová kriminalita*. 1. vydání. Praha : Computer Press, 2002. s. 73

nezbytných pro neoprávněný přístup do systému.[69] Právní kvalifikace této činnosti spadá pod § 270 TZ, trestný čin porušování autorského práva, práv souvisejících s právem autorským a práv k databázi. Za určitých okolností přichází v úvahu též §230 TZ, neoprávněný přístup k počítačovému systému a nosiči informací.

4.4.3 Cybersquatting

Cybersquatting, neboli doménové pirátství, znamená zaregistrování domény určitého subjektu (většinou se jedná o velké podniky) s cílem tuto doménu tomuto subjektu prodat.[70] Motivem tohoto jednání je vyjednání co nejvyšší částky, za kterou je subjekt ochoten tuto doménu koupit. Cybersquatting v současnosti pomalu ustupuje do pozadí. Svůj význam měl v době, kdy velké firmy přicházely na trh a chtěly svým zákazníkům nabízet výrobky prostřednictvím svých stránek. Mezi další formy doménového pirátství můžeme řadit různá nekalosoutěžní jednání, kdy si někdo založí stránku se jménem známého produktu a provozuje na ní e-shop.[71]

Právní kvalifikace oblasti domén spadá spíše do soukromého práva, resp. do oblasti porušování práv průmyslových a ustanovení o nekalé soutěži. Z hlediska trestního práva by přicházelo v úvahu naplnění skutkové podstaty TČ porušení předpisů o pravidlech hospodářské soutěže dle §248 TZ a porušení práv k ochranné známce a jiným označením dle §268 TZ.

[69] JIROVSKÝ, Václav. *Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha : Grada Publishing, a.s., 2007. s. 106

[70] MATĚJKA, Michal. *Počítačová kriminalita*. 1. vydání. Praha : Computer Press, 2002. s. 74

[71] JIROVSKÝ, Václav. *Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha : Grada Publishing, a.s., 2007. s. 107

5 Postih počítačové kriminality v novém trestním zákoníku – shrnutí

V předchozí kapitole jsem uvedl jednotlivá protiprávní jednání, která spadají do problematiky počítačové kriminality. V této kapitole uvádím charakteristiku tří hlavních trestných činů páchaných ve vztahu k počítačovým záznamům a počítačovým datům. Zákonodárce v trestním zákoníku vymezil škodlivá jednání tak, aby byla příslušná ustanovení v souladu s Úmluvou o počítačové kriminalitě.

Většina trestných činů proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů je obsažena v hlavě páté o trestných činech proti majetku. Tzv. odposlech dat je upraven v §182 mezi trestnými činy proti právům na ochranu osobnosti, soukromí a listovního tajemství.[72]

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

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

Ustanovení §230 obsahuje dvě základní skutkové podstaty:

V odstavci 1 je chráněna důvěryhodnost počítačových dat a počítačového systému. Jedná se o ochranu před ohrožením bezpečnosti. Sekundárně je zde chráněna integrita a dostupnost

[72] ŠÁMAL, Pavel a kol. *Trestní zákoník II. §140 až 421 : Komentář*. 1. vydání. Praha : C.H. Beck, 2010. s. 2084

počítačových dat a systémů. V odstavci 2 je primárně chráněna integrita počítačových dat a systémů. V tomto případě je poskytována ochrana před neoprávněnými zásahy a před neoprávněným užíváním uložených počítačových dat.[73]

Toto ustanovení trestního zákona zahrnuje pět protiprávních jednání dle Úmluvy o počítačové kriminalitě[74]:

a) Neoprávněný přístup k počítačovému systému nebo jeho části- odst. 1
b) Neoprávněný zásah do dat nebo do počítačového systému- odst. 2 písm. a), b), d)
c) Falšování údajů souvisejících s počítači- odst. 2 písm. c)
d) Podvod související s počítači- odst. 3 písm. a)
e) Neoprávněný zásah do systému- odst. 3 písm. b)

Odstavec 1 příslušného ustanovení se týká jednání, kdy pachatel překoná bezpečnostní opatření a neoprávněně tím získá přístup k počítačovému systému. V novém trestním zákoníku je tedy trestný samostatně neoprávněný přístup k počítačovému systému nebo jeho části. Není nezbytné, aby osoba učinila ještě něco dalšího (např. manipulace s informacemi uvnitř systému). Trestné je tedy již samotné „hacknutí systému“.[75]

Dle odstavce 2 je trestné jednání, kdy osoba získá přístup k počítačovému systému a splní jednu z dalších podmínek uvedených v zákoně:

- neoprávněně užije uložená data
- neoprávněně data vymaže nebo jinak poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými

[73] ŠÁMAL, Pavel a kol. *Trestní zákoník II. §140 až 421 : Komentář*. 1. vydání. Praha : C.H. Beck, 2010. s. 2085

[74] Tamtéž s. 2085-2086

[75] *Pravniradce.ihned.cz* [online]. 2009-07-22 [cit. 2010-08-23]. Postih počítačová kriminality podle nového trestního zákona. Dostupné z WWW: <http://pravniradce.ihned.cz/c4-10077480-37865090-F00000_d-postih-pocitacove-kriminality-podle-noveho-trestniho-zakona>

- pozmění nebo padělá uložená data tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, že by to byla data pravá
- neoprávněně vloží data do systému nebo učiní jiný zásah do programového nebo technického vybavení počítače[76]

Přísnějším trestem bude dle odstavce 3 potrestána osoba, která spáchá čin uvedený v odst. 1 nebo 2 v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch nebo v úmyslu neoprávněně omezit funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat. Odstavec 4 obsahuje kvalifikovanou skutkovou podstatu trestného činu k odstavci 1 a 2.[77]

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

Podle tohoto ustanovení je trestné takové jednání, kdy si osoba opatří nebo přechovává zařízení nebo jiný prostředek včetně počítačového programu, počítačové heslo, přístupový kód nebo jakýkoli jiný podobný prostředek, pomocí něhož lze proniknout do počítačového systému s úmyslem spáchat trestný čin neoprávněného přístupu k počítačovému systému nebo porušení tajemství dopravovaných zpráv.[78] Opatřování a přechovávání přístupových zařízení není samo o sobě trestné, pokud zde není úmysl spáchat některý z uvedených trestných činů. Jedná se o předčasně dokonaný

[76] ŠÁMAL, Pavel a kol. *Trestní zákoník II. §140 až 421 : Komentář*. 1. vydání. Praha : C.H. Beck, 2010. s. 2081-2086

[77] §230 odst. 3 a 4 zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů

[78] *Pravniradce.ihned.cz* [online]. 2009-07-22 [cit. 2010-08-23]. Postih počítačová kriminality podle nového trestního zákona. Dostupné z WWW: <http://pravniradce.ihned.cz/c4-10077480-37865090-F00000_d-postih-pocitacove-kriminality-podle-noveho-trestniho-zakona>

trestný čin, neboť postihuje jednání, které je materiálně pouze přípravou.[79]

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

Nový trestní zákoník postihuje i některé nedbalostní zásahy do dat a vybavení počítače. Příslušné ustanovení poskytuje ochranu před nedbalostním poškozovacím jednáním (jedná se o hrubou nedbalost), kterým je způsobena značná škoda.

[79] ŠÁMAL, Pavel a kol. *Trestní zákoník II. §140 až 421 : Komentář*. 1. vydání. Praha : C.H. Beck, 2010. s. 2098

6 Metodika vyšetřování počítačové kriminality

6.1 Obecná charakteristika

Pro počítačovou kriminalitu, stejně jako pro další druhy kriminality, existují specifické metody používané pro vyšetřování různých počítačových deliktů. Tyto metody byly vytvořeny na základě dlouholetého zkoumání počítačových deliktů, způsobu jejich páchání, jejich pachatelů a obětí.[80] Na rozdíl od jiných trestných činů jsou počítačové delikty svým způsobem zvláštní, neboť se většina z nich odehrává v kyberprostoru, virtuálním světě, který nemá hmotnou podstatu.

Počítačová kriminalita má určité charakteristické rysy odlišující ji od ostatních druhů kriminality. Zjistit digitální stopy (počítačové stopy) je často velmi obtížné a k jejich identifikaci a dešifrování je třeba finančně náročný software a hardware. Tyto stopy mohou mít krátkou životnost a proto je třeba je zajistit ihned pro případ jejich zničení. Škody způsobené počítačovými delikty jsou v některých případech těžko zjistitelné a obtížně se vyčíslují, což není problémem jen počítačové kriminality a softwarové pirátství, ale duševního vlastnictví celkově.[81] Vyšetřování počítačových deliktů je složitá činnost a proto ji většinou nelze svěřit jen jedné osobě, ale je zapotřebí tým odborníků zabývající se informačními technologiemi. S tím mají občas problém orgány činné v trestním řízení, které nemají dostatek kompetentních a vzdělaných odborníků v této oblasti. Pokud chceme vyšetřovat i složitější delikty v oblasti informačních technologií, je třeba, aby i vyšetřující osoby měly potřebné schopnosti a znalosti. Zároveň je nezbytné, aby tyto orgány spolupracovaly s počítačovými experty a odborníky v oblasti informačních technologií. Jedním z charakteristických rysů

[80] GŘIVNA, Tomáš a kol. *Kyberkriminalita a právo*. 1. vydání Praha : Auditorium, 2008. s. 86

[81] JIROVSKÝ, Václav. *Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha : Grada Publishing, a.s., 2007. s. 251-252

počítačové kriminality je její vysoká latence. Pokud se má počítačové kriminalitě účinně čelit, je třeba, aby poškozené osoby oznamovaly orgánům činným v trestním řízení, že došlo ke spáchání trestného činu a poskytly jim náležitou spolupráci.

Dalším specifikem týkajícím se oblasti počítačové kriminality je příslušná legislativa. V posledním desetiletí se objevilo mnoho nových škodlivých jednání směřujících proti počítači nebo s počítačem související, z nichž některé jsou natolik společensky škodlivé, že je třeba na ně reagovat. To je v působnosti zákonodárce, který musí (na základě diskuzí s expertními skupinami, orgány činnými v trestním řízení a odbornou veřejností atd.) rozhodnout, která z těchto jednání jsou ještě v mezích zákona, a která tuto mez překračují a měla by být tudíž postihnuta normami správního a trestního práva, případně na základě jiných právních předpisů. Najít ideální variantu není jednoduché a je obtížné vymezit tato nežádoucí jednání v právních předpisech tak, aby byl postih efektivní a účinný. K vyšetřování a odhalování těchto protiprávních jednání samozřejmě nestačí jen jejich vymezení v zákoně, ale je zapotřebí dát příslušným orgánům (u nás orgánům činným v trestním řízení) pravomoci na to, aby mohly počítačovou kriminalitu odhalovat a trestat. I zde je situace poměrně obtížná, na jedné straně totiž existuje zájem na tom, aby byly počítačové delikty řádně odhaleny a efektivně potrestány. Na druhou stranu je třeba dbát na to, aby nebylo vyšetřováním neúměrně zasahováno do ústavních a jiných zákonem zaručených práv a oprávněných zájmů osob. Příslušné vyšetřovací orgány by měly mít přístup pouze k těm informacím a údajům, které jsou nezbytně nutné pro vyšetřování.

Oblast informačních technologií se vyznačuje dynamickým rozvojem a složitostí informačních systémů. Vznikají stále nová škodlivá jednání, která je třeba odhalovat a případně je trestat. Pachatelé těchto deliktů jsou ve většině případů velmi inteligentní a snaží se při své činnosti zamést za sebou veškeré stopy. Proto je třeba, aby poškozený trestný čin nebo přestupek oznámil co

nejrychleji, aby měly orgány činné v trestním řízení možnost na tuto situaci reagovat a zajistit stopy a důkazy.

Jak jsem již zmínil, pojem počítačová kriminalita zahrnuje velké množství škodlivých jednání, z nichž některé jsou trestné dle českého trestního zákoníku. Mezi typické počítačové delikty patří tyto trestné činy: neoprávněný přístup k počítačovému systému a nosiči informací podle §230 TZ, opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat podle §231 TZ, poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti podle §232 TZ (které jsou podrobněji rozebrány v kapitole 5). Trestní zákoník obsahuje řadu dalších ustanovení postihující protiprávní jednání v prostoru: porušování autorského práva, práv souvisejících s právem autorským a práv k databázi podle §270 TZ, porušování tajemství dopravovaných zpráv podle §182, nebezpečné pronásledování podle § 354 a jiné.[82]

Od roku 1999 působí u Ředitelství služby kriminální policie kriminálního úřadu Policejního prezidia Skupina informační kriminality. Činnost tohoto pracoviště lze rozdělit na dvě oblasti. První oblastí je odhalování a vyšetřování kriminality týkající se duševního vlastnictví, resp. oblasti informačních technologií a druhá oblast se týká odhalování a vyšetřování trestné činnosti na internetu.[83]

6.2 Typické způsoby páchání

Prof. Porada definuje způsoby páchání počítačových trestných činů jako *„ systém operacionálních elementů trestného činu a činnosti s ním spjatých, který zahrnuje nejen samotný způsob zneužití výpočetní techniky, ale i způsoby jednání pachatele před jejím*

[82] zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů

[83] GŘIVNA, Tomáš a kol. *Kyberkriminalita a právo*. 1. vydání Praha : Auditorium, 2008. s. 86-87

zneužitím, jakož i způsob jednání pachatele při a po realizaci výsledků zneužití výpočetní techniky“.[84]

Typické způsoby páchání počítačových trestných činů lze rozdělit do těchto skupin[85]:

a) *neoprávněné zásahy do vstupních dat*

   Pachatelem může být pouze osoba, která má přístup na pracoviště, kde jsou vstupní doklady uloženy a zpracovány.

b) *neoprávněné změny v uložených datech*

   Pachatelem je v tomto případě osoba, která má přístup do systému a může manipulovat s údaji. Jeho jednání spočívá v tom, že protiprávně změní některé údaje a využije tohoto zásahu k dosažení sledovaného cíle.

c) *neoprávněné pokyny k počítačovým operacím*

   Pachatel má přístup k souborům a na základě jeho protiprávního jednání dojde k protiprávním počítačovým operacím.

d) *neoprávněné pronikání do počítačů, počítačového systému a jeho databází*

   Motivem pachatele je získání neoprávněného přístupu do systémů a překonání bezpečnostních a ochranných prvků.

e) *napadení cizího počítače, jeho programového vybavení a dat v databázích*

Činnost pachatele typicky spočívá v napadení počítače a systému počítačovým virem.

6.3 Podněty k vyšetřování

Příslušný policejní orgán zahajuje prověřování a objasňování skutečností nasvědčujících tomu, že byl spáchán trestný čin na

[84] PORADA, Viktor; KONRÁD, Zdeněk. *Metodika vyšetřování počítačové kriminality*. 1. vydání. Praha : Vydavatelství PA ČR, 1997. s. 10

[85] Tamtéž s. 10-12

základě vlastních nebo cizích podnětů. Mezi nejčastější podněty patří[86]:

1) *výsledky operativně pátrací činnosti služby kriminální policie*
   Orgány kriminální policie na základě vlastních poznatků získaných při vyšetřování podezřelých hospodářských a finančních aktivit a na základě dalších signálů získávají informace o připravované nebo páchané trestné činnosti související s počítačovou kriminalitou. Tyto orgány shromažďují relevantní informace nasvědčující tomu, že dochází k páchání trestné činnosti.
2) *podněty kontrolních a revizních orgánů různých institucí*
3) *ústní a písemné oznámení občanů*
   Často se podávají prostřednictvím trestního oznámení vůči určité osobě nebo na neznámého pachatele. Podává jej většinou osoba nebo instituce poškozená v důsledku počítačového deliktu.
4) *ostatní druhy podnětů* (patří mezi ně podněty prostřednictvím sdělovacích prostředků- noviny, televize, internet, anonymní oznámení, podněty bezpečnostních agentur atd.).

6.4 Metodika vyšetřování (postup)

Přestože je každý počítačový delikt určitým způsobem specifický, lze vymezit některé společné rysy vyšetřování počítačové kriminality. Jedná se o formální proces vyšetřování těchto trestných činů, jehož jednotlivými stádii si musí každé vyšetřování projít.

V první řadě se jedná o zjištění způsobu, jakým pachatel vnikl do systému a vymezení jednotlivých kroků tohoto průniku. Tato fáze zahrnuje stanovení všech možností průniku, vytvoření hypotézy a rekonstrukce tohoto průniku. Jedná se o fázi, kde samotný poškozený

[86] PORADA, Viktor; KONRÁD, Zdeněk. *Metodika vyšetřování počítačové kriminality*. 1. vydání. Praha : Vydavatelství PA ČR, 1997. s. 23

zjišťuje příčiny tohoto vniknutí do systému, ale ještě nespolupracuje s příslušnými policejními orgány.[87]

Druhou fází je zhodnocení zjištěných údajů a rozhodnutí o tom, zda je nutné dávat podnět policejním orgánům nebo zda zásah nebyl natolik závažný a postačí pouze důkladnější zabezpečení systému a odstranění nedostatků. Při vyšetřování počítačové kriminality je nutno postupovat rychle. V případě delší časové prodlevy je pravděpodobné, že pachatel zničí digitální stopy, které by ho mohly usvědčit. Zároveň hrozí, že pachatel nebude vypátrán a bude moct pokračovat v další trestné činnosti.[88]

Na základě podnětů poškozeného či jiných osob nebo na základě vlastních poznatků se bude vyšetřující orgán soustředit na získání nezbytných údajů k identifikaci pachatele a zároveň zjištění místa, z kterého útočník do systému proniká a nabourává jej. Vyšetřovatel bude zjišťovat, zda již někdo manipuloval s napadeným počítačem a soubory dat. Pokud již došlo k manipulaci s napadeným systémem (např. kontrolním orgánem poškozené instituce), pak si vyšetřovatel vyžádá kontrolní nebo revizní zprávu. Pokud k této manipulaci zatím nedošlo, přibere znalce z oboru informačních technologií, který společně s pracovníky poškozené instituce zajistí příslušnou techniku, programy a data nezbytná k vyšetřování počítačového deliktu.[89]

Na počátku objasňování případu stanoví orgány činné v trestním řízení typické verze o charakteru trestného činu (verze, zda byl či nebyl spáchán trestný čin se znaky počítačové kriminality). Tyto verze se zpravidla vytyčují po provedení prvotních vyšetřovacích

[87] JIROVSKÝ, Václav. *Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha : Grada Publishing, a.s., 2007. s. 255

[88] JIROVSKÝ, Václav. *Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha : Grada Publishing, a.s., 2007. s. 255-256

[89] PORADA, Viktor; KONRÁD, Zdeněk. *Metodika vyšetřování počítačové kriminality*. 1. vydání. Praha : Vydavatelství PA ČR, 1997. s. 16

úkonů. Postupně se k těmto verzím shromažďují informace a důkazy důležité pro vyšetřování daného počítačového deliktu.[90]

Mezi typické počáteční úkony při vyšetřování počítačové kriminality patří zjištění potřebných vysvětlení, zajišťovací úkony (domovní prohlídky, vydání a ohledání věci a ohledání počítačového hardwaru na místě zajištění), vyžádání znaleckých posudků a odborných vyjádření. Volba počátečných úkonů se bude odvíjet od toho, o jaký druh počítačové kriminality se jedná a jaké vykazuje znaky.

Důležitým faktorem při vyšetřování počítačové kriminality je spolupráce veřejnosti a poškozeného s orgány činnými v trestním řízení. Ve většině případů se jedná o spolupráci s poškozeným, který se stal obětí počítačové deliktu a je tudíž v jeho zájmu, aby byl pachatel vypátrán a potrestán. Zároveň může uplatňovat vůči pachateli náhradu škody nebo učinění nezbytných opatření (např. návrat do původního stavu).

Dalším úkolem orgánů činných v trestním řízení je vystopovat cestu, po které pachatel do systému vnikl. Jedná se o nejtěžší část vyšetřování počítačového deliktu, neboť celé toto vyšetřování se odehrává v kyberprostoru. Většina těchto pachatelů pochází z vnějšího prostředí a jsou natolik inteligentní, aby po sobě nezanechali moc stop. Cílem této fáze bude vystopování konkrétního počítače, z kterého byl útok na systém proveden. Problémem je, že pachatelé často páchají útoky z „veřejných“ počítačů (univerzity, knihovny, internetové kavárny) a i když policejní orgány zjistí, z kterého počítače byl útok spáchán, je těžké tento útok přiřadit ke konkrétní osobě. Zároveň pachatelé vytvářejí různé falešné stopy a mezilehlé systémy, které podstatně ztěžují práci policejních orgánů. Podstatnou roli při stopování (trasování) pachatele hrají tzv. logy,

[90] PORADA, Viktor; KONRÁD, Zdeněk. *Metodika vyšetřování počítačové kriminality*. 1. vydání. Praha : Vydavatelství PA ČR, 1997. s. 31-33

což jsou záznamy o provozu určitého systému. Často se však stává, že pachatel logy zničil nebo pozměnil, IP adresy jsou falešné atd.[91]

Při vyšetřování počítačové kriminality se lze setkat s různými kriminalistickými stopami. Může se jednat o stopy daktyloskopické, mechanoskopické či fonoskopické. Nejdůležitější roli však budou hrát tzv. počítačové stopy (digitální stopy). Počítačovou stopu lze charakterizovat jako *„změnu na nosiči informací, vzniklou v souvislosti s trestným činem, při jehož spáchání byla využita výpočetní technika a která je zjistitelná a využitelná pomocí současných metodických prostředků, postupů a operací“*.[92] Během vyšetřování tohoto druhu trestné činnosti se objevují jak stopy materiální a jiné soudní důkazy, tak stopy paměťové.

Prof. Porada ve své publikaci[93] rozlišuje 3 kategorie počítačových stop:

a) stopy na výpočetní technice včetně neoprávněných zásahů do této techniky
b) stopy na záznamových médiích a informace uložené na nich (CD, DVD, interní a externí pevné diskety atd.)
c) stopy na organizační a kancelářské technice umožňující zaznamenání a uchování digitálních informací (zařízení umožňující vkládání a uchovávání určité informace- telefony, diáře, diktafony atd.)

Další kategorií stop týkajících se počítačové kriminality jsou stopy účetní, listinné a věcné důkazy a stopy dokazující padělání. Mezi paměťové stopy můžeme zařadit např. výpověď výslech zaměstnanců, kteří jsou povinni podat svědectví týkající se spáchané trestné činnosti.

---

[91] JIROVSKÝ, Václav. *Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha : Grada Publishing, a.s., 2007. s. 255-256

[92] PORADA, Viktor; KONRÁD, Zdeněk. *Metodika vyšetřování počítačové kriminality*. 1. vydání. Praha : Vydavatelství PA ČR, 1997. s. 14

[93] Tamtéž s. 14-15

V případě, že jsou shromážděny potřebné materiály, je třeba je důkladně analyzovat. V případě vyšetřování počítačových deliktů je třeba brát v úvahu, že poškozený (nebo poškozená instituce) často nemůže dát k dispozici potřebnou techniku vyšetřujícím orgánům, neboť tyto technologie potřebuje nezbytně pro svůj provoz. Je třeba tedy vytvořit kopie pevného disku, programů a dat, které byly napadeny a tyto informace převést na počítač. Tato fáze obsahuje mnoho dalších úkonů, které jsou spíše technického charakteru- analyzování logů, systému, který byl napaden, nalezení změn, které byly zásahem provedeny v souborech atd. To může být provázeno i celou řadou dalších opatření- např. fotodokumentací, označení systému tak, aby bylo možno situaci v budoucnu rekonstruovat atd.[94]

V této fázi je nesmírně důležité zajištění a označení důkazu. To znamená postupovat tak, aby byly zjištěné poznatky použitelné jako důkazy před soudem. Je nutné, aby vyšetřující orgány postupovaly v souladu se zákonem a dodržovaly ustanovení příslušných právních předpisů.

V souvislosti s hledáním pachatele počítačového deliktu by se měl vyšetřující orgán zaměřit na to, jaký je motiv jednání pachatele. Mezi typické motivy jednání pachatele patří: snaha o získání finančních prostředků, dobrého společenského postavení a moci, vyřizování osobních účtů s jinými osobami (msta, závist), touha projevit své individuální schopnosti za cenu diskreditace svých konkurentů, politické motivy, krycí motivy k utajení jiné trestné činnosti páchané pachatelem.[95]

Cílem vyšetřujících orgánů je shromáždění co největšího množství důkazů o napadení systému. Předmět dokazování se bude odvíjet od druhu spáchané protiprávní činnosti. Přesto bude u všech forem dokazováno: na kterém počítači byl útok proveden, jakým způsobem byl proveden, jestli byl spáchán jeden nebo více skutků,

[94] JIROVSKÝ, Václav. *Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha : Grada Publishing, a.s., 2007. s. 258

[95] PORADA, Viktor a kol. *Kriminalistická metodika vyšetřování*. Plzeň : Aleš Čeněk s.r.o., 2007. s. 186

zda byl trestný čin spáchán jednou či více osobami, jaký byl jejich motiv, okolnosti spáchání trestného činu, zda byla způsobena škoda či nikoliv atd.[96]

Je důležité, aby orgány činné v trestním řízení vyhledávaly a zajišťovaly důkazy v souladu se zákonem, aby mohly být později použity po účely trestního řízení a k usvědčení pachatele před soudem.

6.5 Mezinárodní spolupráce při vyšetřování počítačové kriminality

K některým počítačovým deliktům nedochází pouze na území jednoho státu, ale jejich příprava, páchání a následky mohou nastat na území dvou či více států. Aby mohlo dojít k řádnému odhalení a vyšetření této trestné činnosti, je nezbytné, aby jednotlivé státy mezi sebou spolupracovaly. Pokud by tomu tak nebylo, nabízela by se pachatelům jedinečná možnost páchat počítačové delikty prostřednictvím kyberprostoru v jiném státě a nebyli by za tyto útoky trestáni. Tato spolupráce může probíhat jednak formou vzájemné právní pomoci (např. Interpol) nebo neformální cestou, kterou si státy navzájem poskytují důležité informace a spolupracují spolu.[97]

Spolupráce formou vzájemné právní pomoci vzniká na základě mezinárodních dohod uzavřených mezi dvěma či více státy. Interpol ustanovil několik pracovních skupin s odborníky v oblasti informačních technologií. Zároveň došlo k vydání příručky počítačové kriminality, která obsahuje metodiku vyšetřování trestných činů. Mezinárodní spolupráce vyžaduje propojení jednotlivých expertních skupin vyšetřujících počítačovou kriminalitu a jejich vzájemnou spolupráci. Stěžejním mezinárodním dokumentem pro boj

[96] PORADA, Viktor; KONRÁD, Zdeněk. *Metodika vyšetřování počítačové kriminality*. 1. vydání. Praha : Vydavatelství PA ČR, 1997. s. 20

[97] GŘIVNA, Tomáš a kol. *Kyberkriminalita a právo*. 1. vydání Praha : Auditorium, 2008. s. 97

s počítačovou kriminalitou je Úmluva o počítačové kriminalitě přijata v roce 2001 na Mezinárodní konferenci o počítačové kriminalitě.[98]

[98] GŘIVNA, Tomáš a kol. *Kyberkriminalita a právo*. 1. vydání Praha : Auditorium, 2008. s. 98-99

7 Mezinárodní úprava počítačové kriminality

7.1 Úmluva o počítačové kriminalitě

Trestná činnost prováděná v kyberprostoru je velkým nebezpečím dnešní doby. Pachatelé jsou schopni páchat trestnou činnost prostřednictvím počítače z jednoho státu na území státu jiného. Zatímco každý stát má své vnitrostátní zákony, které lze uplatňovat ve většině případů jen na svém území, kyberprostor nijak omezen není. Pokud se má počítačové kriminalitě úspěšně čelit, je třeba harmonizovat trestní právo hmotné a procesní jednotlivých států a zajistit vzájemnou spolupráci mezi policejními a vyšetřujícími orgány jednotlivých států.[99]

Jedním z významných kroků k této harmonizaci a spolupráci bylo přijetí Úmluvy o počítačové kriminalitě v roce 2001. Úmluva byla vypracována Výborem expertů pro kriminalitu v kyberprostoru založeným v roce 1997. V platnost vstoupila 1. července 2004. Česká republika Úmluvu podepsala, ale dosud neratifikovala. V roce 2005 vstoupil v platnost Dodatkový protokol k Úmluvě o počítačové kriminalitě týkající se kriminalizace činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů. Jak již bylo v této práci zmíněno, otázka kriminalizace trestných činů s rasistickým a xenofobním obsahem byla z Úmluvy záměrně vypuštěna a vložena do Dodatkového protokolu, neboť hrozilo, že kvůli této části by Úmluva nebyla ratifikována Spojenými státy americkými.[100]

Úmluva o počítačové kriminalitě se člení do preambule a 4 kapitol, které zahrnují 48 článků. Kapitola I. obsahuje výklad některých používaných pojmů v Úmluvě. Kapitola II.(opatření přijímaná na národní úrovni) obsahuje závazky týkající se trestního

[99] GŘIVNA, Tomáš a kol. *Kyberkriminalita a právo*. 1. vydání Praha : Auditorium, 2008. s. 103-104

[100] Tamtéž s. 104-105

práva hmotného a procesního a ustanovení o působnosti vnitrostátních norem. Kapitola III. obsahuje otázky mezinárodní spolupráce a závěrečná ustanovení jsou obsažena v kapitole IV.
Úmluva ve svém textu opakovaně používá některé pojmy, které bylo v Kapitole I. třeba definovat- počítačový systém, počítačová data, poskytovatel služeb a provozní data. Zajímavostí je, že Úmluva nikde ve svém textu nedefinuje pojem počítačová kriminalita, tento pojem byl definován Výborem expertů pro kriminalitu v kyberprostoru, ale do Úmluvy nebyl zařazen (tuto definici uvádím v úvodní kapitole této práce).

Kapitola II. obsahuje ve své hmotněprávní části výčet trestných činů, které dělí do čtyř kategorií (ty obsahují devět trestných činů). Mimo to obsahuje v hlavě páté i otázky pokusu a pomoci, odpovědnosti právnických osob a otázky sankcí a opatření. Úmluva[101] dělí trestné činy na:

a) Trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů, které zahrnují:
   - Neoprávněný přístup
   - Neoprávněné zachycení informací
   - Zásah do dat
   - Zásah do systému
   - Zneužití zařízení
b) Trestné činy související s počítači
   - Falšování údajů související s počítači
   - Podvod související s počítači
c) Trestné činy související s obsahem
d) Trestné činy související s dětskou pornografií

(do této kategorie by spadaly také trestné činy související s rasismem, extremismem a xenofobií, které však byly zahrnuty do Dodatkového protokolu)

e) Trestné činy související s porušením autorského práva a práv příbuzných k autorskému právu

[101] Úmluva o počítačové kriminalitě, přijatá v Budapešti 23. listopadu 2001

V procesní části Kapitoly II. jsou obsažena ustanovení týkající se působnosti Úmluvy a dále některá procesní opatření: bezodkladné uchovávání počítačových dat, bezodkladné uchovávání a částečné poskytnutí provozních dat, příkaz k vydání, prohlídka a zajištění uložených počítačových dat, shromažďování provozních dat v reálném čase a zachycení dat o obsahu. Úmluva stanoví, že tyto procesní opatření lze použít na (čl. 14):[102]

a) Trestné činy, k jejichž kriminalizaci zavazuje Úmluva
b) Jiné trestné činy, které byly spáchány prostřednictvím počítačového systému
c) Shromažďování důkazů o trestném činu v elektronické podobě

Kapitola III. Úmluvy obsahuje obecná i konkrétní ustanovení týkající se závazků v oblasti mezinárodní spolupráce. V této kapitole jsou upraveny ustanovení o obecných principech týkajících se mezinárodní spolupráce, principech týkajících se vydávání osob, obecných principech týkajících se vzájemné pomoci, postupech týkajících se žádostí o vzájemnou pomoc v případě neexistence aplikovatelných mezinárodních smluv, dále ustanovení o vzájemné pomoci týkající se prozatímních opatření, vzájemné pomoci týkající se pravomocí k vyšetřování. V čl. 35 se smluvní strany zavazují, že určí kontaktní místo, které bude neustále k dispozici a bude poskytovat pomoc pro účely vyšetřování a řízení týkající se počítačových trestných činů.[103]

Kapitola IV. Úmluvy obsahuje závěrečná ustanovení, zahrnující mimo jiné ustanovení o tom, které státy se mohou stát smluvní stranou Úmluvy, otázky podpisu a účinnosti, přistoupení k Úmluvě, územní působnost, změny a doplňky, řešení sporů, vypovězení Úmluvy.

7.2 Další mezinárodněprávní dokumenty v boji proti počítačové kriminalitě

[102] GŘIVNA, Tomáš a kol. *Kyberkriminalita a právo*. 1. vydání Praha : Auditorium, 2008. s. 173-178

[103] Tamtéž s. 179-187

Nejdůležitějším právně závazným dokumentem v boji proti počítačové kriminalitě je již mnohokrát zmíněná Úmluva o počítačové kriminalitě přijatá Radou Evropy. Kromě této Úmluvy však existuje i celá řada dalších dokumentů obsahujících závazky k ochraně kyberprostoru.

V rámci OSN byla vydána Rezoluce o boji se zneužíváním informačních technologií ze dne 22. ledna 2001, Rezoluce 56/261, kterou se vyhlašuje plán činnosti pro implementaci Vídeňské deklarace o zločinu a trestní spravedlnosti: Výzvy 21. století.[104]

OECD v roce 1986 přijala doporučení týkající se zásahů proti počítačovým systémům, zásahů do dat a padělání počítačového systému. V rámci EU byly přijaty další nástroje: Rámcové rozhodnutí Rady 2005/222/SV o útocích proti informačním systémům. Rámcové rozhodnutí Rady 200/375/JHA o boji proti dětské pornografii na internetu, Směrnice Evropského parlamentu a Rada 97/66/ES o zpracování osobních údajů a ochraně soukromí v telekomunikačním sektoru a další.[105]

[104] GŘIVNA, Tomáš a kol. *Český právní řád a ochrana kyberprostoru : vybrané problémy*. Praha : Karolinum, 2008. s. 23
[105] Tamtéž s. 27-33

Závěr

Problematika počítačové kriminality je značně obsáhlá a není v možnostech této práce postihnout všechny její aspekty. Proto jsem se snažil zaměřit na výběrové otázky týkající se počítačové kriminality. Je nutné mít na paměti, že oblast informačních technologií je neustále se rozvíjející obor a některá jednání uvedené v této práci budou časem zastaralá a naopak se objeví i některá nová jednání, která prozatím nejsou v této práci zahrnuta.

Cílem této práce bylo zaměřit se na počítačovou kriminalitu jak z hlediska trestního práva, tak z hlediska kriminalistického. V trestněprávní části jsem se především zabýval jednotlivými protiprávními jednáními, která jsou dle našeho vnitrostátního práva považovány za trestné. Mnoho těchto jednání se navzájem prolíná a lze je klasifikovat dle stejných trestněprávních ustanovení. Často bude také docházet k souběhu těchto trestných činů. V kriminalistické části jsem se zabýval především metodikou vyšetřování počítačové kriminality, tedy jednotlivými kroky, tedy postupem orgánů činných v trestním řízení při vyšetřování počítačové kriminality.

Významným krokem v boji proti počítačové kriminalitě jistě můžeme zařadit přijetí nového trestního zákoníku, účinného od 1. ledna 2010. Zatímco starý trestní zákoník obsahoval z počítačových deliktů pouze skutkovou podstatu poškození a zneužití záznamu na nosiči informací v §257a, nový trestní zákoník sebou přinesl některé nové skutkové podstaty v oblasti počítačové kriminality. Právní úprava počítačové kriminality je tedy v novém trestním zákoníku rozsáhlejší a přesnější. Nový trestní zákoník vychází z Úmluvy o počítačové kriminalitě a reflektuje vývoj v oblasti informačních technologií. Je však nutno zmínit, že se spolu s dalším vývojem informačních technologií budou v budoucnu objevovat nová škodlivá jednání a bude na ně třeba reagovat novelizacemi v zákoně.

Z hlediska vyšetřování počítačové kriminality je nezbytné, aby orgány činné v trestním řízení měly k dispozici odpovídající techniku a software. Stejně tak je třeba, aby měly dostatek kvalifikovaných,

vzdělaných a zkušených odborníků z oblasti informačních technologií, kteří jsou schopní držet s pachateli těchto trestných činů krok. Důležitým faktorem je i rozvíjení mezinárodní spolupráce mezi jednotlivými státy, které umožní postihovat a trestat jednání pachatelů z jiných států.

Počítačová kriminalita je negativní jev související s dnešní společností a bude problémem i do budoucna. Proto je nutné dbát na prevenci a snažit se tomuto jednání předejít. Pokud se prevence ukáže jako neúspěšná, je třeba tyto trestné činy odhalovat a účinně trestat.

Resumé

Resumé v českém jazyce

Počítače jsou součástí našeho denního života. Oblast informačních technologií je oblastí neustále se rozvíjející. Negativním jevem tohoto rozvoje je vzestup různých protiprávních jednání.

Úvodní část této práce popisuje základní pojmy týkající se počítačové kriminality a softwarového pirátství. Tato část zahrnuje definice počítačové kriminality, kyberzločinu, kyberprostoru, softwarového pirátství. Uvedení této terminologie je nezbytné pro pochopení dané problematiky.

Další kapitola zahrnuje historický pohled na vývoj počítačové kriminality a softwarového pirátství. Jedná se především o rozmezí od šedesátých let do devadesátých let.

Třetí a čtvrtá kapitola této diplomové práce obsahuje rozdělení počítačové kriminality a je rozdělená do čtyř podkapitol. „*Trestné činy proti počítačům a počítačovým systémům“* (zabývá se protiprávními jednáními jako hacking, cpamming, phreaking, carving atd.). *„Trestná činnost související s obsahem“ (*zabývá se závadnou pornografií, extremismem a rasismem v kyberprostoru). *Trestná činnost s využitím počítače“* (zahrnující phishing, pharming, sniffing, cyberstalking, počítačový podvod a jiné). Poslední podkapitola se zabývá „*trestnou činností směřující proti autorským a jiným právům“.*

Pátá část této diplomové práce uvádí shrnutí typických počítačových trestných činů uvedených v českém trestním zákoníku. Zahrnuje také změny, které přinesl nový trestní zákoník.

Šestá kapitola se zabývá metodikou vyšetřování počítačové kriminality. Uvádí postup a metody vyšetřování počítačové kriminality a mezinárodní spolupráci v oblasti vyšetřování počítačové kriminality.

Poslední kapitola obsahuje popis mezinárodních organizací a jejich dokumentů týkajících se boje proti počítačové kriminalitě.

Cílem této práce bylo popsat hlavní problémy týkající se počítačové kriminality a softwarového pirátství z hlediska

kriminalistiky a trestního práva. Dané téma je velmi rozsáhlé, proto jsem se zaměřil především na oblast počítačové kriminality.

Resumé v angličtině

Computers are a part of our common lifes. The section of informatic technologies is constantly evolving. The negative part of this development is the rise of various illegal activities.

The opening part of this thesis describes basic concepts concerning computer criminality and software piracy. It contains definitions of cyber crime (comptuter crime), cyberspace, software piracy. This terminology is necessary for understanding this topic.

The next part describes historical point of view of computer criminality and software piracy. This part contains the history of computer criminality from the 60ties to 90ties.

The third and fourth part of this thesis contains the divisions of computer criminality. This chapter is divided into four sub-chapters. *„Cyber crimes against computers and computer systems“ (*which deals with illegal activies such as hacking, spamming, phreaking, carding etc.). „*Crimes with relation to content of the computer“ (which deals with illegal pornography*, extremism and rasism in cyberspace). „*Crimes commited by using computer“ (includes phishing, pharming, sniffing, cyberstalking, computer fraud etc.).* The last sub-chapter deals with *„crimes against copyright law and other similar law“.*

The fifth part of this thesis is the review of typical computer crimes in Czech criminal code. It contains the changes, which brought the new criminal code.

The sixth chapter deals with metodology of investigation of computer crimes. It includes the procedure and methods of investigation and international cooperation concerning the computer criminality.

The last chapter of this thesis desribes international organizations and documents concerning computer criminality and software piracy.

The main aim of this thesis was to describe the main problems of computer criminality in light of criminology and criminal law. This topic is very extensive, so I described mainly the part of computer criminality.

Použité zkratky

Autorský zákon, AZ	zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů
EU	Evropská unie
FBI	Federal Bureau of Investigation, Federální úřad pro vyšetřování v USA
OECD	Organizace pro hospodářskou spolupráci a rozvoj
OSN	Organizace spojených národů
Protokol, Dodatkový protokol	Dodatkový protokol k Úmluvě o počítačové kriminalitě týkající se kriminalizace činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů, přijatý 28. ledna 2003
TZ, trestní zákoník	zákon č.40/2009 SB, trestní zákoník
TČ	trestný čin uvedený ve zvláštní trestního zákoníku
Úmluva	Úmluva o počítačové kriminalitě, přijatá v roce 2001 Mezinárodní konferenci o počítačové kriminalitě v Budapešti, účinná od 1.7.2004

Použitá literatura

Publikace:

1) CRAIG, Paul. *Softwarové pirátství bez záhad*. Tomáš Hlaváč. 1. vydání. Praha : Grada Publishing, a.s., 2008. 212 s. ISBN 978-80-247-1765-4.

2) DUNNIGAN, James F. *Bojiště zítřka : Jak čelit globálnímu nebezpečí kyberterorismu*. Kateřina Došlíková. 1. vydání. Praha : Baronet, 2004. 356 s. ISBN 80-7214-642-4.

3) GREGUŠOVÁ, Daniela. *Počítačové právo*. Brno : Institut dalšího vzdělávání, 2002. 227 s. ISBN 80-86629-04-X.

4) GŘIVNA, Tomáš, et al. *Český právní řád a ochrana kyberprostoru : vybrané problémy*. Praha : Karolinum, 2008. 140 s. ISBN 978-80-246-1703-9.

5) GŘIVNA, Tomáš; POLČÁK, Radim. *Kyberkriminalita a právo*. 1. vydání Praha : Auditorium, 2008. 220 s. ISBN 978-80-903786-7-4.

6) HARRIS, Shon a kol. *Hacking - manuál hackera*. Tomáš Znamenáček. Praha : Grada Publishing, a.s., 2008. 400 s. ISBN 978-80-247-1346-5.

7) JELÍNEK, Jiří a kol. *Trestní právo hmotné*. 1. vydání. Praha : Leges, 2009. 896 s. ISBN 978-80-87212-24-0.

8) JELÍNEK, Jiří a kol. *O novém trestním zákoníku : Sborník příspěvků z mezinárodní konference Olomoucké právnické dny, květen 2009*. 1. vydání. Olomouc : Leges, 2009. 224 s. ISBN 978-80-87212-21-9.

9) JIROVSKÝ, Václav a kol. *Sborník přednášek konference CYTER 2009*. Praha : České vysoké učení technické v Praze, 2009. 90 s. ISBN 978-80-01-04372-1.

10) JIROVSKÝ, Václav. *Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha : Grada Publishing, a.s., 2007. 288 s. ISBN 978-80-247-1561-2.

11) KUCHTA, Josef a kol. *Základy kriminologie a trestní politiky*. 1. vydání. Praha : C.H. Beck, 2005. 544 s. ISBN 80-7179-813-4.

12) MATĚJKA, Michal. *Počítačová kriminalita*. 1. vydání. Praha : Computer Press, 2002. 106 s. ISBN 80-7226-419-2.

13) MUSIL, Jan; KONRÁD, Zdeněk; SUCHÁNEK, Jaroslav. *Kriminalistika*. 2., přeprac. a dopl. vyd. Praha : C.H. Beck, 2004. 583 s. ISBN 80-7179-878-9.

14) MUSIL, Stanislav. *Počítačová kriminalita : Nástin problematiky*. Praha : Institut pro kriminologii a sociální prevenci, 2000. 282 s. ISBN 80-86008-80-0.

15) PORADA, Viktor a kol. *Kriminalistika : (úvod, technika, taktika)*. Plzeň : Aleš Čeněk s.r.o., 2007. 309 s. ISBN 978-80-7380-038-3.

16) PORADA, Viktor a kol. *Kriminalistická metodika vyšetřování*. Plzeň : Aleš Čeněk s.r.o., 2007. 231 s. ISBN 978-80-7380-042-0.

17) PORADA, Viktor a kol. *Kriminalita související s informačními a komunikačními technologiemi a identifikace osob na základě projevu lokomoce člověka : Vybrané problémové okruhy výzkumu*. 1. vydání. Karlovy Vary : Vysoká škola Karlovy Vary, 2007. 262 s. ISBN 978-80-254-0797-4.

18) PORADA, Viktor a kol. *Kriminalistika*. Brno : CERM, 2001. 746 s. ISBN 80-7204-194-0.

19) PORADA, Viktor; KONRÁD, Zdeněk. *Metodika vyšetřování softwarového pirátství*. 1. vydání. Praha : Vydavatelství PA ČR, 1999. 54 s. ISBN 80-7251-024-X.

20) PORADA, Viktor; KONRÁD, Zdeněk. *Metodika vyšetřování počítačové kriminality*. 1. vydání. Praha : Vydavatelství PA ČR, 1997. 55 s. ISBN 80-85981-75-0.

21) SMEJKAL, Vladimír a kol. *Právo informačních a telekomunikačních systémů*. 2. aktualizované a rozšířené vydání. Praha : C.H. Beck, 2004. 770 s. ISBN 80-7179-765-0.

22) SMEJKAL, Vladimír. *Internet a §§§*. 1. vydání. Praha : Grada Publishing, a.s., 2001. 284 s. ISBN 80-247-0058-1.

23) SMEJKAL, Vladimír; SOKOL, Tomáš; VLČEK, Martin. *Počítačové právo*. Praha : C.H. Beck, 1995. 264 s. ISBN 80-7179-009-5.

24) SUCHÁNEK, Jaroslav a kol. *Kriminalistická problematika při odhalování, vyšetřování a prevenci počítačové kriminality*. 1. vydání. Praha : Vydavatelství PA ČR, 1997. 204 s. ISBN 80-85981-50-5.

25) ŠÁMAL, Pavel a kol. *Trestní zákoník II. §140 až 421 : Komentář*. 1. vydání. Praha : C.H. Beck, 2010. 2011 s. ISBN 978-80-7400-178-9.

Internetové zdroje:

26) *Hoax.cz* [online]. 2009-01-20 [cit. 2010-08-23]. Co-je-to-phishing. Dostupné z WWW: <http://www.hoax.cz/phishing/co-je-to-phishing>.

27) *Idnes.cz* [online]. 2010-08-20 [cit. 2010-08-23]. Na bankomatech České spořitelny opět byly falešné čtečky. Dostupné z WWW: <http://ekonomika.idnes.cz/na-bankomatech-ceske-sporitelny-opet-byly-falesne-ctecky-pz0-/ekonomika.asp?c=A100816_182730_ekonomika_fih) >.

28) *Interval.cz* [online]. 2006-07-26 [cit. 2010-08-23]. Phishing aneb rhybaření 1. Dostupné z WWW: <http://interval.cz/clanky/phishing-aneb-rhybareni-1/>.

29) Kevin Mitnick. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, , last modified on 20.září 2010 [cit. 2010-09-27]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Kevin_Mitnick>.

30) *Lupa.cz* [online]. 2007-03-23 [cit. 2010-08-23]. Pharming je zpět a silnější. Dostupné z WWW: <http://www.lupa.cz/clanky/pharming-je-zpet-a-silnejsi/>.

31) *Penize.cz* [online]. 2010-03-10 [cit. 2010-08-23]. Skimming, phishing, pharming. Dostupné z WWW: < http://www.penize.cz/debetni-karty/69791-skimming-phishing-pharming

32) *Pravniradce.ihned.cz* [online]. 2009-07-22 [cit. 2010-08-23]. Postih počítačová kriminality podle nového trestního zákona. Dostupné z WWW: <http://pravniradce.ihned.cz/c4-10077480-37865090-F00000_d-postih-pocitacove-kriminality-podle-noveho-trestniho-zakona>.

33) *Profit.cz* [online]. 2009-10-27 [cit. 2010-08-23]. Počítačová kriminalita : byznys za miliardy. Dostupné z WWW: http://www.profit.cz/clanek/pocitacova-kriminalita-byznys-za-miliardy.aspx

34) Vladimir Levin. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, , last modified on 20. srpna 2010 [cit. 2010-09-27]. Dostupné z WWW: <http://en.wikipedia.org/wiki/Vladimir_Levin>.

35) *Wikipedia.cz* [online]. 2010-08-18 [cit. 2010-08-23]. Spam. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Spam >.

36) *Wikipedia.cz* [online]. 2010-04-30 [cit. 2010-08-23]. Kyberprostor. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Kyberprostor>.

37) *Wikipedia.cz* [online]. 2010-03-31 [cit. 2010-08-23]. Hoax. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Hoax >.

38) *Wikipedia.cz* [online]. 2010-03-01 [cit. 2010-08-23]. Pharming. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Pharming>.

Právní předpisy

Zákon č. 100/2001 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů

Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a změně některých dalších zákonů (autorský zákon)

Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů