Univerzita Palackého v Olomouci
Právnická fakulta

Jiří Doubrava

Počítačová kriminalita (trestněprávní a kriminologické aspekty)

Diplomová práce

Olomouc 2011

Prohlašuji, že jsem diplomovou práci na téma „Počítačová kriminalita (trestněprávní a kriminologické aspekty)“ vypracoval samostatně a citoval jsem všechny použité zdroje.

V Šumperku dne 24. ledna 2011 ……

Jiří Doubrava

Obsah

Úvod

Jednou z nejrychleji se rozvíjejících součástí lidského života tvoří oblast informačních technologií. Dnes nové a moderní technologie jsou za krátkou dobu staré a téměř k nepoužití. Vývoj jde dopředu a nelze jej zastavit. Počítače se zrychlují, roste jejich vnitřní paměť, jsou mnohostranně využitelné a dostupné již téměř komukoli. Ale jak už to v reálném životě bývá, vidina moci a vlastního prospěchu může člověka dovést až ke zneužití těchto technologií k páchání trestné činnosti.

Rozvoj informačních technologií a lidská povaha jsou dva faktory, které významnou měrou přispěly ke vzniku počítačové kriminality. Tento relativně nový druh kriminality je stále na vzestupu, o čemž svědčí nárůst jednotlivých forem i případů této trestné činnosti.

Téma počítačové kriminality jsem si zvolil záměrně vzhledem k jeho aktuálnosti a zajímavosti. Na danou problematiku byla zpracována řada publikací, včetně dokumentů a článků přístupných v elektronické podobě na internetu. V důsledku přijetí nového trestního zákoníku, účinného od 1. ledna 2010, se změnila i právní úprava, týkající se počítačové kriminality. Publikací, které se zabývají jednotlivými změnami v této souvislosti, je však podstatně méně.

Cílem této diplomové práce bude podat přehledný exkurz do problematiky počítačové kriminality se zaměřením na její trestněprávní a kriminologické aspekty. V úvodní části se zaměřím na vymezení pojmu a obsahu počítačové kriminality, dále na její historický vývoj a současně na jednotlivé příčiny vzniku této formy kriminality. Pokusím se odpovědět na otázku, zda lze nalézt obecnou charakteristiku pachatele počítačové kriminality a jaké jsou jejich nejčastější motivy. Pozornost chci věnovat nejčastějším projevům a formám počítačové kriminality a jejich postihu dle současné trestněprávní úpravy. Za důležité považuji uvést, jakých změn doznala právní úprava počítačových deliktů v souvislosti s přijetím již výše zmíněného trestního zákoníku. V části zaměřené na boj s počítačovou kriminalitou se zmíním nejen o významu prevence a represe, ale budu se snažit přiblížit jednotlivé prostředky, které orgány činné v trestním řízení využívají k odhalování a vyšetřování této trestné činnosti. Na závěr práce bych uvedl některé reálné hrozby a často diskutované otázky související s budoucím vývojem počítačové kriminality.

1 Vymezení pojmu a obsahu počítačové kriminality

Počítačová kriminalita jako český ekvivalent anglického computer crime, IT crime či chcete-li cybercrime, se jako pojem dostal do podvědomí lidí z hlediska právní a kriminologické terminologie teprve v sedmdesátých letech. V našem právním prostředí především z důvodu jistého technologického zpoždění až v letech osmdesátých.[1] Jak je patrno již ze samotného názvu, počítačová kriminalita jako pojem v sobě zahrnuje protiprávní jednání ve spojení s počítačem. Přitom samotný výraz počítačová kriminalita má obdobný význam jako zavedené pojmy „násilná kriminalita", „kriminalita mladistvých" apod.[2] Pod těmito obecnými pojmy lze vidět skupinu trestných činů, které se vyznačují určitým společným znakem. V našem případě je tímto společným znakem počítač, ať již jako nástroj nebo předmět trestné činnosti. Některé zdroje zmiňují a objasňují pojem kriminalita informačních technologií jako pojem širší a zahrnující též oblast telekomunikací.[3] V dnešní době se obě oblasti téměř stírají. Mnoho činů, které směřují proti telekomunikačním zařízením, je pácháno právě za pomoci počítačů.

V odborné literatuře se můžeme setkat s různými názory, jak vymezit obsah pojmu počítačová kriminalita. Jako relativně nový obor, který se neustále a rychle vyvíjí, je nesmírně těžké nalézt obecnou definici, která by zahrnovala veškeré aspekty a charakteristické rysy. Podle toho z jakého úhlu pohledu se na celou problematiku díváme, můžeme dojít k různým závěrům. O jednu z prvních publikovaných definic u nás se pokusil kolektiv Smejkal, Sokol, Vlček. Ve své publikaci uvedli, že pod pojmem počítačová kriminalita je třeba chápat *„páchání trestné činnosti, v níž figuruje počítač jako souhrn hardwarového a softwarového vybavení data nevyjímaje, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět této trestné činnosti, ovšem s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako movité věci, nebo jako nástroj trestné činnosti."*[4] Jedním z předpokladů je tedy spáchání trestného činu, jehož cílem či prostředkem je počítač jako celek. Obecně bychom poté počítačovou kriminalitu mohli vymezit jako protiprávní jednání, které naplňuje znaky trestného činu a je zde určitá již výše zmíněná spojitost s počítačem. Naopak do tohoto pojetí nelze zařadit klasickou trestnou činnost, kde je počítač brán pouze jako jakákoliv jiná věc movitá. To je zcela v souladu s moderním pojetím

[1] SMEJKAL, Vladimír a kol. *Právo informačních a telekomunikačních systémů.* 2. vydání. Praha: C.H.Beck, 2004, s. 691.
[2] Tamtéž, s. 692.
[3] Viz např. MATĚJKA, Michal. *Počítačová kriminalita.* Praha: Computer Press, 2002, s. 3.
[4] SMEJKAL, Vladimír, SOKOL, Tomáš, VLČEK, Martin. *Počítačové právo.* Praha: C.H.Beck, 1995, s. 99.

a pohledem na tuto problematiku. Pokud by pachatel neoprávněně disponoval s počítačem bez záměru využít jeho obsah, čili data a informace v něm obsažené, nemůžeme toto jeho jednání klasifikovat jako formu počítačové kriminality.

Bez zajímavosti není ani pohled velkých mezinárodních organizací, které tuto problematiku sledují a diskutují. Již v rámci 8. konference OSN v devadesátých letech minulého století byla počítačová kriminalita zmíněna jako jedna z nejnebezpečnějších forem kriminálních deliktů.[5] Krátce poté byl vypracován Manuál OSN pro prevenci a kontrolu počítačového zločinu,[6] v němž se uvádí, že počítačová kriminalita zahrnuje *„Tradiční zločinné aktivity jako krádež, podvod nebo padělání, tedy činy trestné ve většině zemí na světě. Počítač rovněž tvoří prostředí pro nové činy spočívající ve zneužití počítačů, které jsou nebo by měly být ve své podstatě trestné.“* [7] Za zmínku stojí také názor osoby, která se danou problematikou prakticky zabývala, dnes již bývalého vedoucího skupiny informační kriminality při policejním prezidiu mjr. Jiřího Dastycha, který nahlíží na počítačovou kriminalitu takto: *„Počítačová kriminalita je mnohdy i přes své nesporné prvky moderních technologií jen jinou tváří různých standardních trestných činů. Obecně počítačová kriminalita představuje velkou množinu všech kriminálních aktivit, spojených s počítačem jako nástrojem, případně cílem trestné činnosti.“*[8]

Již na první pohled je zřejmé, že většina zmíněných definic či pojetí tohoto fenoménu dnešní doby je ve své podstatě tvořena stejným základem. Je však nutné předeslat, že vývoj počítačových a jiných informačních technologií, který, zdá se, nebere konce, může do budoucna zcela zvrátit nebo alespoň pozměnit chápání počítačové kriminality jako takové. V takovém případě vyvstane otázka, zda-li s nástupem nových možností a technologií nebude nutné se zamyslet nad novým termínem, který by více odrážel realitu moderní doby.

[5] SMEJKAL, Vladimír, SOKOL, Tomáš, VLČEK, Martin. *Počítačové právo*. Praha: C.H.Beck, 1995, s. 98.
[6] Manuál OSN pro prevenci a kontrolu počítačového zločinu *(United Nations Manual on the prevention and control of computer-related crime)* [online]. OSN, 1994. Dostupný na <http://www.uncjin.org/Documents/EighthCongress.html>.
[7] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, a.s., 2007, s. 91.
[8] DASTYCH, Jiří. Počítačová kriminalita. *Hlásí se policie* [online]. 1998 [cit. 12. prosince 2010]. Dostupné na <http://www.dolphin.cz/policie/brezen98/pocitace.html>.

2 Počítačová kriminalita jako fenomén dnešní doby

2.1 Příčiny vzniku

Počítačová kriminalita jako nový obor zločinnosti a předmět zkoumání by nevznikla bez jednoho z nejpřelomovějších vynálezů poslední doby. Sestrojení počítače znamenalo velký přelom ve vědeckém a postupem času i v běžném životě mnoha lidí. Právě vědecko-technický pokrok, který měl za následek, že se z počítače stal mnohoúčelový přístroj schopný provádět nejrůznější operace a příkazy, vedl ve svém důsledku k postupnému utváření této formy trestné činnosti. Je všeobecně známo, že většina vynálezů stvořených s dobrými úmysly, které jsou schopny se uplatnit a zasáhnout téměř do všech oblastí lidské činnosti a života, mohou být nakonec zneužity k různým formám protiprávního jednání. Nejinak je tomu v případě informačních technologií a samotného počítače, postupem času vše navíc umocněno jejich vzájemným propojením ať již nejprve do lokálních, či následně do celosvětových sítí.

Postupné pronikání nových technologií, počítače nevyjímaje, do stále více oblastí lidského života s sebou přineslo nové dosud nepředstavitelné možnosti a bylo jen otázkou času, kdy se najde osoba, která toho využije ve svůj prospěch. Právě pachatelé si začali jako první uvědomovat, jak mocnou zbraň počítače a jiné informační technologie představují. Svoji roli sehrálo mnoho kriminogenních faktorů,[9] mezi které řadíme mimo jiné složitost těchto technologií, což může v oboru znalém pachateli vyvolat myšlenku, že nemůže být odhalen. Mezi další okolnosti, které nahrávají páchání této formy trestné činnosti, je velká důvěra samotných uživatelů ve zpracované výstupy z informačních technologií.[10] Jinými slovy drtivá většina z nás bezmezně věří v informace zpracované počítačem a kontrolu provádí až už je pozdě. Těchto činitelů a vlastností počítačů je celá řada a zkušení pachatelé je dokáží náležitě využít.[11] S trochou nadsázky bychom mohli použít slogan z jedné reklamy na nejmenovaný energetický nápoj a říci, že využití počítačové techniky dává pachatelům trestné činnosti křídla.[12]

Další z příčin celkového rozvoje a rozmachu počítačové kriminality je moment, kdy

[9] Rizikoví činitelé, které motivují, vyvolávají, usnadňují nebo podporují páchání trestných činů. Definici formuloval prof.PhDr.Rudolf Kohoutek,CSc. ABZ slovník cizích slov [cit. 14. prosince 2010]. Dostupné na <http://slovnik-cizich-slov.abz.cz/web.php/slovo/kriminogenni-faktory>.
[10] MATĚJKA, Michal. *Počítačová kriminalita.* Praha: Computer Press, 2002, s. 8.
[11] Viz např. SMEJKAL, Vladimír a kol. *Právo informačních a telekomunikačních systémů.* 2. vydání. Praha: C.H.Beck, 2004, s. 692-693; MATĚJKA, Michal. *Počítačová kriminalita.* Praha: Computer Press, 2002, s. 8-9.
[12] SMEJKAL, Vladimír, SOKOL, Tomáš, VLČEK, Martin. *Počítačové právo*. Praha: C.H.Beck, 1995, s. 98.

došlo k prvnímu vzájemnému propojení více počítačů.[13] Vznikly tak nejprve lokální a později vzdálené sítě typu ARPANET,[14]které byly zdokonaleny a dovedeny do podoby dnešní celosvětové sítě známé pod označením internet. Vzniklo tak zcela nové působiště, pro které se ustálil název kyberprostor, chcete-li anglicky cyberspace. Hranice kyberprostoru může být omezena pouze samotnými informačními technologiemi, jejichž vývojem a zdokonalováním se bude tato hranice nadále posouvat. *„Kyberprostor žádnými mezemi nedisponuje – je v podstatě nekonečný – neomezený – a stále se jako prostor může rozrůstat, což jej odlišuje od prostorů skutečných.“*[15] Tento virtuální prostor si postupem času vytváří svá vlastní pravidla a přesouvá se do něj velká část společenských aktivit, potřeb a rysů.[16] Není tedy příliš překvapivé, že se na tomto poli působnosti objevují jednání, které označujeme jako protiprávní, a proti kterým se snaží společnost bojovat a předcházet jim. Každý jedinec má možnost si v tomto virtuálním světě vytvořit svoji fiktivní identitu, která se v ničem nepodobá té reálné a o to složitější je poté takovou osobu odhalit a dopadnout. Jedná se o negativní dopad, který s sebou nese tento pokrok a převrat v moderních informačních technologiích. Úkolem společnosti a patřičných orgánů je najít účinné metody, jak tento problém eliminovat.

O důležitosti a významu vzniku počítačových sítí svědčí i v literatuře publikované rozdělení na dobu „před sítěmi“ a „po nich“.[17] Dostáváme se tak do fáze, kdy ke spáchání byť i klasického trestného činu, jakým je krádež či podvod, postačí pachateli jeho znalosti a přístup na síť. Nemusí se doslova ani hnout ze svého domu či pracoviště a svůj čin může spáchat tzv. „online“. Svou roli zde hraje i psychologická stránka věci, a to v tom smyslu, že se pachatel pod dojmem anonymity cítí více v bezpečí doma před monitorem, než kdyby byl nucen svůj čin provést na daném místě fyzicky. Dalším faktorem, který jistě přispěl ke vzniku a celosvětovému rozmachu počítačové kriminality je rychlost, s jakou lze čin nebo útok provést. Stejně tak hraje roli teritorialita, která se v důsledku propojení celosvětové sítě v oblasti počítačového zločinu stírá a hranice jednotlivých států zde nehrají téměř žádnou roli. O to složitější je takové protiprávní počínání stíhat a zároveň koordinovat veškeré snahy o regulaci tohoto jednání.

---

[13] K prvnímu síťovému propojení mezi čtyřmi univerzitními počítači došlo v roce 1968. Viz. JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, a.s., 2007, s. 15.

[14] Advanced Research Projects Agency Network byla počítačová síť spuštěná v roce 1969 v USA a je dnes chápána jako předchůdce dnešního internetu, který využívá jiný typ protokolu tzv. TCP/IP.

[15] POLČÁK, Radim, ŠKOP, Martin, MACEK, Jakub. *Normativní systémy v kyberprostoru (úvod do studia).* Brno: Masarykova univerzita, 2005, s.25.

[16] Blíže viz JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, a.s., 2007, s. 16.

[17] SMEJKAL, Vladimír. *Internet a §§§.* 2. aktualizované a rozšířené vydání. Praha: Grada Publishing, spol. s r.o., 2001, s. 186-187.

V neposlední řadě bych zmínil lidskou zvědavost a touhu po uznání, která především v počátcích stála u zrodu počítačové kriminality. Mluvíme o době, kdy nově nastupujícím technologiím rozuměla pouze malá skupina lidí, především z řad odborníků a tzv. „fandů“, tedy osob, které propadly výpočetní a informační technice a toužily do ní proniknout. Tato vyvíjená činnost byla často úzce spjata s undergroundem, tedy určitou alternativní kulturou neboli jiným myšlenkovým proudem, který má snahu bojovat s vládnoucí vrstvou a jí nastoleným společenským řádem.[18]

2.2 Historický vývoj

Mimo příčiny, které podnítily vznik počítačové kriminality, je významné zaměřit se na jednotlivé etapy historického vývoje této formy trestné činnosti. K tomu nám pomohou určité stěžejní či záchytné body, které se v minulosti udály a díky nimž můžeme celé období rozdělit do určitých fází. Někteří autoři zabývající se touto problematikou uvádí svá vlastní rozdělení či se spíše zaměřují na jednotlivé trestné činy spojené s počítačovou kriminalitou nejprve v jejím počátku a následně v dnešní době.[19] Existuje tedy více názorů a pojetí ohledně rozdělení historického vývoje, nicméně pro lepší pochopení a přehlednost se podržíme členění, které ve své publikaci uvádí Michal Matějka.[20] Ten vyčleňuje tři základní etapy vývoje a již teď předesílám, že se shodují s časovým rozdělením dějin lidstva pouhým názvem.

2.2.1 Pravěk

První fází, nazvanou s ohledem na úplný počátek vývoje informačních technologií jako pravěk, je myšleno „*období od vynálezu telefonu do uvedení prvního PC na trh v roce 1981*.“[21] Právě telefon jako vůbec první elektronický dálkový prostředek hlasové komunikace a následný rozvoj telefonních ústředen s sebou přinesly i první případy nelegálních aktivit. Zrodili se tzv. „*telefandové*“[22], neboli nadšenci, kteří využívali telefonních sítí ke své komunikaci zdarma či na cizí účet. Mezi sebou si vyměňovali své poznatky a společně vymýšleli a zdokonalovali systém jak obelstít provozovatele telefonických zařízení a sítí.

[18] Viz MATĚJKA, Michal. *Počítačová kriminalita.* Praha: Computer Press, 2002, s. 9-10.
[19] Viz např. KABAY, M.E. *A Brief History of Computer Crime: An Introduction for Students* [online]. [cit. 15. prosince 2010]. Dostupné na <http://www.mekabay.com/overviews/history.pdf>; SMEJKAL, Vladimír a kol. *Právo informačních a telekomunikačních systémů.* 2. vydání. Praha: C.H.Beck, 2004.
[20] MATĚJKA, Michal. *Počítačová kriminalita.* Praha: Computer Press, 2002, str. 17.
[21] Tamtéž
[22] Pojem odvozený od slova „phreaks“ (složené z „phone“ a „freak“). Viz STERLING, Bruce. *Zátah na hackery (Hackers Crackdown)* [online]. 1992 [cit. 15. prosince 2010]. Přeložil Bárta Václav. Dostupné na <http://martin.hinner.info/crackdown/hacker_crackdown.pdf>.

Uběhlo však mnoho let než došlo ke spojení telefonních linek s počítačem. První elektronický počítač byl sestrojen již ve 40. letech 20. století s názvem ENIAC.[23] O jeho využití ke kriminálním aktivitám však nelze hovořit a to vzhledem k jeho velikosti a obsluze. Nacházel se ve speciálně upravené místnosti a přístup k němu měli jen vyškolení odborníci. Právě tito specialisté byli čas od času nuceni provádět zásahy do stále nedokonalého programového vybavení počítače s cílem zjistit a napravit jeho nedostatky. V této době lze také hledat původ dnes často používaných termínů „hacking" nebo „hacker". Jejich význam je odvozen od již zmíněných zásahů, pro které je v angličtině používán výraz „hacks".[24] Z toho vyplývá, že role tehdejšího „hackera" byla veskrze pozitivní, nicméně časem tento pojem nabyl úplně jiného významu.[25]

Případy zneužívání především telekomunikačních zařízení se vyskytovaly již v 60. letech minulého století a pokračují dodnes. Práce na zpřístupnění počítače široké veřejnosti nabíraly na obrátkách a bylo tak nadmíru jasné, že vývoj informačních technologií již nelze zastavit.

2.2.2 Středověk

Druhým mezníkem v historii počítačové kriminality bylo představení osobního počítače (personal computer – zkráceně PC)[26] a jeho uvedení na trh. S velkou rychlostí se rozšířil zprvu na pracoviště velkých společností, ale netrvalo dlouho a stal se tento pomocník součástí mnoha domácností. Vzhledem k tématu je však podstatná jiná věc, a to ta, že se počítač dostal do rukou znalých a technologicky zdatných osob, kterým tak umožnil se realizovat na poli počítačového zločinu. Zpočátku to byli právě počítačoví nadšenci z řad studentů, zaměstnanců a odborníků IT (information technology) oborů, kteří se mnohdy sdružovali a zakládali různé skupiny orientované na stejný cíl. Motivem většiny členů byla touha po uznání od svých kolegů a jejich záměry se tak od záměrů dnešních pachatelů trestných činů souvisejících s počítači značně lišily. O veškeré své úspěchy se velice rádi dělili s jinými, a proto mnoho z nich přispívalo do již existujících publikací nebo si vytvářeli

[23] Viz MATĚJKA, Michal. *Počítačová kriminalita.* Praha: Computer Press, 2002, str. 20 nebo též WEIK, Martin H. *The ENIAC Story* [online]. [cit. 15.prosince 2010]. Dostupné na <http://www.martinhweik.com/eniac_story.html>.
[24] MATĚJKA, Michal. *Počítačová kriminalita.* Praha: Computer Press, 2002, str. 20.
[25] Blíže MATĚJKA: *Počítačová*…, s. 20.
[26] První osobní počítač s označením 5150 od společnosti IBM byl uveden na trh 12.8.1981. Viz Vintage IBM 5150 [online]. Dostupné na <http://www.ibm5150.net/history.html>.

své vlastní. Jedna z nejznámějších a dnes již legendárních skupin nesla název Legion of Doom.[27]

Podobně zaměřené skupiny se začaly formovat a vyvíjet činnost v době, kdy došlo k propojení počítače s telefonní linkou, což můžeme brát jako jeden z dalších přelomových událostí z hlediska historie a vývoje počítačové kriminality. Toto spojení informačních a telekomunikačních technologií posunulo možnosti a ambice všech zúčastněných. Právě vznik počítačových sítí umožnil vzdálený přístup k počítači, čímž se změnily i kriminogenní podmínky, typy pachatelů i obětí a hlavně způsob provedení neboli modus operandi.[28] Přesto všechno se pachatelé této formy trestné činnosti nedopouštěli jednání, které by ohrožovalo státní bezpečnost či zdraví lidí.[29] V mnohých případech pouze poukázali na nedokonalost obranných mechanismů a zabezpečovacích systémů, o čemž svědčí i fakt, že jsou známy případy, kdy se útočníci dostali k přísně střeženým či utajeným materiálům bez jejich dalšího využití. Primárním cílem nebyly ani finanční ústavy, alespoň ne v tomto období. Kdo tratil byly především telekomunikační společnosti, jejich ztráty však nebyly nikterak závratné.

Mezi nejznámější pachatele tohoto období zcela jistě řadíme Kevina Mitnicka, jehož případ neoprávněného nabourávání se do systémů cizích počítačů za účelem získání zdrojových kódů byl velmi medializovaný. Orgánům činným v trestním řízení se podařilo tohoto muže vypátrat a postavit před soud. Byl odsouzen k několika letům odnětí svobody a byl mu udělen trest zákazu používání počítačů a mobilních telefonů po určitou dobu od propuštění.[30] Přesto však Kevin Mitnick nepatří mezi klasické pachatele dnešní doby. Jeho cílem nebylo způsobení škody či vlastní obohacení. Podle svých slov veškerá jeho činnost v tomto směru směřovala k poznání a znamenala pro něj intelektuální výzvu. Motiv pachatelů se postupem času v závislosti na vývoji a rozšíření všech druhů informačních technologií změnil a postupně se vyprofiloval nový typ pachatele.

2.2.3 Novověk

Přes všechny činy a útoky spáchané v předchozím období si málo kdo uvědomoval úplnou hrozbu a možný dosah počítačové kriminality. Rychlé vystřízlivění přinesl případ Citibank, který se udál v roce 1994. Ten ve své podstatě ukázal, kam se bude ubírat vývoj

[27] Historii této legendární skupiny lze nalézt na webových stránkách jednoho z takových časopisů s názvem Phrack. Viz The History of The Legion Of Doom [online]. Dostupné na <http://www.phrack.org/issues.html?issue=31&id=5>.
[28] SMEJKAL, Vladimír a kol. *Právo informačních a telekomunikačních systémů.* 2. vydání. Praha: C.H.Beck, 2004, s. 706.
[29] MATĚJKA, Michal. *Počítačová kriminalita.* Praha: Computer Press, 2002, str. 25.
[30] Blíže viz KULHAVÝ, Petr. *Kevin Mitnick – slavný podvodník nebo obávaný hacker?* [online]. Root.cz, 26. září 2003 [cit. 15. prosince 2010]. Dostupné na <http://www.root.cz/clanky/kevin-mitnick-podvodnik-hacker/>.

trestné činnosti páchané pomocí informačních technologií, především počítačů. Ve zmíněném případu se ruské hackerské skupině, vedené Vladimirem Levinem, podařilo obejít ochranu počítačů finančního ústavu Citibank a převést neuvěřitelných 10 milionů dolarů na své účty po celém světě. Levin byl dopaden a vydán do Spojených států amerických, kde byl shledán vinným a odsouzen ke třem letům odnětí svobody a k zaplacení peněžitého trestu 240 tisíc dolarů.[31] Podstatné je, že případ jasně ukázal, že se motiv pachatelů postupně mění a cílem této trestné činnosti začíná být finanční prospěch. Z hlediska typu pachatele je zřejmé, že právě v této době započala éra tzv. profesionálů v oblasti počítačové kriminality.

Postupně se začaly objevovat jiné zcela nové formy této trestné činnosti, které vyvolaly potřebu reakce ze strany společnosti. Počítačová kriminalita se stala jedním z diskutovaných témat na různých fórech a konferencích za účasti odborníků a představitelů z mnoha zemí. Mezi zmiňované nové formy lze zařadit virové hrozby šířící se jako vlna, které se s rozvojem internetu dotkly mnoha koncových uživatelů.[32] Na počátku nového tisíciletí se objevila nová forma sdílení dat prostřednictvím tzv. systému peer-to-peer (P2P). Zatímco doposud se uživatel za účelem stažení požadovaných dat připojoval k určitému serveru, odkud chtěná data stáhl, tento nový systém P2P je založen na zcela jiném principu sdílení. Jedná se o princip komunikace mezi samotnými uživateli, kteří tak mohou sdílet data bez využití jakéhokoliv serveru. Tím se mnohonásobně rozšířila kapacita a objem dat, které mohou být přenášeny. Celý systém tak nahrává těm, kteří šíří či stahují hudbu, filmy nebo potřebný software, podléhající ochraně autorským právem. Vyvstal tak nový problém týkající se počítačového pirátství a porušování autorského práva, se kterým je velmi těžké bojovat. Především díky své jednoduchosti a rychlosti se stal tento způsob opatřování dat masovou záležitostí a těší se tak velké oblibě.

Probírané období se nese ve znamení spojení počítače a celosvětové sítě internet, které znamenalo vytvoření nových forem a kvantitativní nárůst jednotlivých případů počítačové kriminality. Je otázkou, kam až využití informačních technologií může zajít. Z hlediska budoucnosti je jednou z největších hrozeb zneužití těchto technologií ze strany teroristických hnutí a skupin. Pro tuto problematiku se ustálil pojem „kyberterorismus“, jehož principem je *„zneužívání výpočetní a telekomunikační techniky včetně internetu jako prostředku a prostředí*

[31] Viz Cyber Crime and Information Warfare: A 30-Year History, Citibank 1994 [online]. [cit. 16. prosince 2010]. Dostupné na <http://images.businessweek.com/ss/10/10/1014_cyber_attacks/5.htm>.

[32] Jeden z prvních počítačových virů byl vypuštěn v roce 1988 a měl ho na svědomí Robert Morris. Koncem 90. let 20. století počet napadených počítačů prudce vzrostl. Mezi nejznámější počítačové viry tohoto období patří vir Melissa nebo vir s prozaickým názvem ILOVEYOU. Historický přehled a vývoj blíže viz VŠETEČKA, Roman. *Viry jsou staré několik desetiletí. Chcete znát jejich vývoj?* [online]. iDNES.cz, 4. listopadu 2004 [cit. 16. prosince 2010]. Dostupné na <http://technet.idnes.cz/tec_technika.asp?r=bezpecnost&c=A041103_5285981_bezpecnost>.

pro uskutečnění teroristického útoku. Jedná se podobně jako u klasického konvenčního teroristického útoku o plánovanou činnost, motivovanou zpravidla politicky či nábožensky."[33] Velká část vyspělé civilizace je přímo závislá na chodu informačních technologií, které ovládají a řídí takové sektory, jakými jsou například zdravotnictví, doprava, bankovnictví či administrativní chod země. Pokud by se teroristům podařil tento systém vyřadit z provozu byť i na krátkou dobu, mělo by to zcela jistě nedozírné následky. K odvrácení nastíněného scénáře jistě přispěje prevence v oblasti počítačové kriminality, kam jistě můžeme zařadit vývoj bezpečnostních systémů, které by takovým neoprávněným průnikům zamezily.

2.2.4 Vývoj na našem území

I přes skutečnost, že se výpočetní a jiná technika k nám dostávala se značným zpožděním, lze i na našem území dohledat trestné činy spojené s počítači v poměrně brzké době. Pokud jde o časové zařazení, tak mluvíme o období 70. – 80. let minulého století. Jedná se však spíše o činy, které mají povahu poškozování takového zařízení, což bylo tehdy klasifikováno jako sabotáž či poškozování majetku v socialistickém vlastnictví samozřejmě dle trestního zákona platného v dané době.[34] Zmíněného jednání se dopouštěli především zaměstnanci, kteří měli k podobné technice přístup, jelikož drtivá většina tehdejších domácností výbavou tohoto typu nedisponovala.

Stejně jako jinde ve světě si postupem času pachatelé na našem území rychle osvojili potřebné dovednosti a začali využívat počítač jako nástroj k usnadnění mnohých klasických trestných činů. Byl hojně využíván k falšování dokladů, výrobě padělků či různým formám podvodů. Po pádu komunistického režimu mělo právě celospolečenské uvolnění tehdejších poměrů a přísun zboží ze zahraničí vliv na postupné rozšíření a nárůst případů počítačového pirátství. Po uvedení mechaniky CD-R[35] na český trh jako možné součásti osobního počítače se pořizování nelegálního materiálu posunulo o úroveň výše. K tomu samozřejmě přispěl i postupný rozvoj a využití internetu na našem územní. Rychlými kroky jsme se v oblasti informačních a telekomunikačních technologií přiblížili vyspělému západu a tím nezůstali pozadu ani na poli počítačové kriminality.

[33] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, a.s., 2007, s. 129.
[34] Blíže viz SMEJKAL, Vladimír a kol. *Právo informačních a telekomunikačních systémů.* 2. vydání. Praha: C.H.Beck, 2004, s. 703.
[35] Mechanika umožňující zápis dat na nosič informací jakým je CD.

3 Subjekty počítačové kriminality

Stejně jako v jiných formách trestné činnosti, tak i v oblasti počítačové kriminality se vyskytují subjekty, které jsou v rozdílném postavení. Do kategorie subjekty počítačové kriminality bychom v širším významu a smyslu mohli zařadit kromě pachatelů a poškozených i orgány činné v trestním řízení. O nich však bude blíže pojednáno níže v sekci zaměřené na prevenci a boj s počítačovou kriminalitou. V souvislosti s výkladem o pachatelích a poškozených je důležité zmínit také pojem oběť trestného činu, který se svým významem od pojmu poškozeného do jisté míry liší.

3.1 Pachatelé a jejich motivy

Z hlediska trestního práva je pachatel hmotněprávní pojem, který se svým obsahem liší od pojmů jako podezřelý, obviněný či obžalovaný, používaných v různých fázích trestního řízení. Trestní zákoník definuje pachatele jako toho, *„kdo svým jednáním naplnil znaky skutkové podstaty trestného činu nebo jeho pokusu či přípravy, je-li trestná“*.[36] Pachatelem může být dle platné právní úpravy pouze fyzická osoba, což je zcela v souladu se zásadou individuální odpovědnosti za spáchaný čin.[37] Pro úplnost je nutné dodat, že podmínkou trestní odpovědnosti fyzické osoby je dovršení zákonem stanoveného věku a příčetnost, neboli způsobilost být pachatelem trestného činu z hlediska duševních vlastností a schopností.

Některé trestné činy mohou být spáchány pouze subjektem se zvláštní vlastností, způsobilostí nebo v určitém postavení. Všechny tyto znaky mohou být obsahem skutkové podstaty trestného činu a charakterizovat možného pachatele.[38] Pokud tyto znaky skutková podstata neobsahuje, může být případným pachatelem jakákoliv fyzická osoba, splňující podmínky trestní odpovědnosti stanovené v zákoně. Toto obecně platné pravidlo se vztahuje i na trestné činy spadající pod obor počítačové kriminality.

Pokud bychom měli obecně charakterizovat pachatele počítačové kriminality, dojdeme k závěru, že jednotná charakteristika či profil v dnešní době neexistuje. Profil a typy pachatelů této trestné činnosti se stejně jako počítačová kriminalita vyvíjí v závislosti na nových formách a nelze je příliš zobecňovat. Pokud pohlédneme zpět do historie, tak se nám okruh samotných pachatelů zužuje. Je to dáno tím, že počítače a jiné informační technologie byly přístupné úzkému okruhu lidí, především z řad zaměstnanců větších společností, které

[36] Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.
[37] JELÍNEK, Jiří a kol. *Trestní právo hmotné.* 1. vydání. Praha: Leges, 2009, s. 181.
[38] Tamtéž, s. 199.

takovou technikou disponovaly. Postupem času se společně s rozvojem techniky a nových forem počítačové kriminality měnil i obraz a vlastnosti pachatele. Okruh pachatelů se natolik rozšířil, že již není možné hovořit o tzv. typickém pachateli tohoto druhu kriminality. V minulosti se často hovořilo o počítačové kriminalitě jako o kriminalitě „bílých límečků“[39], což dnes již neplatí, alespoň ne bezvýjimečně. Pachatelé především finančních deliktů byli často vysoce inteligentní lidé v takovém postavení, které s sebou neslo pravomoc a odpovědnost. V předešlých letech se popis charakterových vlastností takových osob vytvářel lépe než-li v dnešní době. V osobnosti pachatele se kromě vyššího IQ odrážela také hamižnost, touha po moci, vytrvalost a bezohlednost.[40] Často také platilo, že takové osoby měli problémy se sociální interakcí a začleňováním do společnosti.

Přes nesporný fakt, že lze stále výše zmíněný popis uplatnit na mnoho pachatelů této trestné činnosti, se již dnes ukazuje, že jej nelze použít obecně na všechny osoby, které se dopouštějí trestných činů spojených s počítači. Příkladem může být počítačové pirátství, kterého se dnes dopouští velké množství osob různého zaměření, postavení a s odlišnými vlastnostmi. Lze konstatovat, že disponuje-li osoba potřebnými znalostmi a prostředky, může být potencionálním pachatelem počítačové kriminality.

Z kriminologického hlediska je zajímavé zaměřit se na možné a časté motivy pachatelů počítačových trestných činů. Zjištění motivu může výrazně pomoci při vyšetřování a dopadení pachatele. Stále platí, že převažujícím motivem je touha po zisku, tedy osobní obohacení.[41] Objevují se však i jiné motivy. Mezi ty nejčastější můžeme zařadit pocit převahy nad zaměstnavatelem, veřejnými orgány i samotnou veřejností, pocit nedocenění, pocit beztrestnosti, touha po riziku, kompenzaci či dokonce msta.[42] Jednotlivé motivy se mohou v praxi různě prolínat a kumulovat.

3.2 Poškození a oběti této formy trestné činnosti

Poškozený a oběť trestného činu jsou pojmy, které se svým obsahem neztotožňují. K rozlišení obou pojmů lze využít zákonného vymezení, kdy trestní řád definuje poškozeného jako toho, *„komu bylo trestným činem ublíženo na zdraví, způsobena majetková, morální*

[39] SMEJKAL, Vladimír, SOKOL, Tomáš, VLČEK, Martin. *Počítačové právo*. Praha: C.H.Beck, 1995, s. 135.
[40] PORADA, Viktor, KONRÁD, Zdeněk. *Metodika vyšetřování počítačové kriminality*. 1. vydání. Praha: Vydavatelství PA ČR, 1998. s. 12.
[41] Viz MUSIL, Stanislav. *Počítačová kriminalita: Nástin problematiky. Kompendium názorů specialistů* [online]. Praha: Institut pro kriminologii a sociální prevenci, 2000 [cit. 18. prosince 2010]. Dostupné na <http://www.ok.cz/iksp/docs/256.pdf>.
[42] Tamtéž. Blíže také SMEJKAL, Vladimír, SOKOL, Tomáš, VLČEK, Martin. *Počítačové právo*. Praha: C.H.Beck, 1995, s. 135.

nebo jiná škoda.“[43] Z toho vyplývá, že poškozeným může být jak osoba fyzická, tak i právnická, včetně státu. Naopak obětí trestného činu se v teorii trestního práva rozumí pouze osoba fyzická, které dle zákonné dikce *„v důsledku trestného činu vznikla škoda na zdraví. Za oběť se považuje i osoba pozůstalá po oběti, která v důsledku trestného činu zemřela, byla-li rodičem, manželem nebo dítětem zemřelého a současně v době jeho smrti s ním žila v domácnosti, nebo osoba, které zemřelý poskytoval nebo byl povinen poskytovat výživu“*. [44]

Při důsledné aplikaci těchto pojmů do oblasti počítačové kriminality dojdeme k závěru, že oběti, tedy osoby, kterým vlivem spáchaného trestného činu vznikla újma na zdraví, se vyskytují jen sporadicky. V drtivé většině případů trestné činnosti spojené s počítači, kdy dochází k porušení či ohrožení zájmu chráněného trestním zákoníkem, se znaky újmy na zdraví nevyskytují. Naopak převažuje majetková škoda. O tom také svědčí fakt, že cílem pachatelů se stávají větší společnosti, především finanční ústavy. Mezi poškozenými se také často objevují nadnárodní společnosti či dokonce stát a jeho orgány. Pachatelé si zcela logicky za svůj cíl vybírají subjekty, které disponují velkým majetkem a kapitálem, aby případný prospěch získaný z této formy trestné činnosti byl co největší. Přesto, že tyto společnosti vynakládají nemalé prostředky na svůj zabezpečovací systém, najímají kvalifikované administrátory, kteří mají celý chod na starosti, jsou nejčastějším terčem útoků. Otázkou je kolik takových útoků zůstane zamlčeno a bez potrestání. Z logiky věci žádná z těchto společností nemá zájem, aby se tyto případy dostaly na veřejnost. Důvodem je samozřejmě obava o zachování představy nedotknutelnosti a důvěryhodnosti. Naopak druhá skupina tvořená samotnými jednotlivci, kteří nedisponují takovými možnostmi ani prostředky, je nejméně pravděpodobným cílem.[45] V převážné většině případů, kde figuruje jednotlivec jako poškozený, dochází k útokům na jeho soukromí, osobní data či případně k morální újmě.

[43] Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů.
[44] Zákon č. 209/1997 Sb., o poskytnutí peněžité pomoci obětem trestné činnosti a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.
[45] GŘIVNA, Tomáš a kol. *Kyberkriminalita a právo*. Praha: Auditorium, 2008, s. 35.

4 Základní dělení a jednotlivé formy počítačové kriminality

Počítačovou kriminalitu můžeme rozčlenit na její jednotlivé formy, tedy konkrétní druhy trestné činnosti, které můžeme obsahově zařadit pod tento pojem. Nicméně stejně důležité je zmínit její základní dělení ze zcela jiného hlediska. K tomu nám pomůže počítač, tedy zařízení, od něhož je odvozen samotný název tohoto druhu kriminality a který může hrát v trestné činnosti rozličnou roli. Z hlediska postavení počítače a jeho využití při páchání trestné činnosti lze uvést následující rozdělení:[46]

I. Protiprávní jednání (trestné činy), kde je počítač cílem a terčem útoku.
II. Protiprávní jednání (trestné činy), kde počítač vystupuje jako nástroj či prostředek k jejich páchání.

4.1 Protiprávní jednání směřující proti počítači

Jak již bylo výše zmíněno, trestné činy směřující proti počítači jako věci movité bez dalšího využití jeho vnitřního obsahu nelze z našeho pohledu začlenit do dnešního pojetí počítačové kriminality. Případ, kdy se pachatel zmocní cizího počítače a jeho hardware vybavení aniž by využil v něm obsažené informace, software či jiná data, dopustí se trestného činu krádeže dle § 205 trestního zákoníku, ale s počítačovou kriminalitou to má pramálo společného.

Počítač však není jen bezobsažná věc, ale je brán a chápán jako nosič informací se svým vlastním obsahem. Jeho součástí je hardware, který umožňuje nahrávání a ukládání informací, záznamů či programů, které můžeme souhrnně nazvat jako data. Z tohoto pohledu se počítač může stát cílem či předmětem protiprávního jednání, které může směřovat právě proti jeho obsahu. Jedná se především o trestné činy ve vztahu k software a jiným datům, která se nacházejí na pevném disku počítače či jiném k tomu určeném úložišti. Jinými slovy je lze charakterizovat jako trestné činy ve vztahu k nehmotnému majetku.[47] Typickým příkladem takového jednání je neoprávněný průnik do systému za účelem například krádeže dat, ať již osobních či jiných, průmyslová špionáž, bankovní podvody apod.[48] O jednotlivých formách této trestné činnosti bude blíže pojednáno v následujících kapitolách.

[46] Viz MATĚJKA, Michal. *Počítačová kriminalita.* Praha: Computer Press, 2002, str. 49 nebo též SMEJKAL, Vladimír, SOKOL, Tomáš, VLČEK, Martin. *Počítačové právo*. Praha: C.H.Beck, 1995, s. 100.
[47] SMEJKAL, Vladimír a kol. *Právo informačních a telekomunikačních systémů.* 2. vydání. Praha: C.H.Beck, 2004, s. 694.
[48] MATĚJKA, Michal. *Počítačová kriminalita.* Praha: Computer Press, 2002, str. 6.

4.2 Počítač jako prostředek k páchání trestné činnosti

Rozšíření počítačů do mnoha oblastí lidského života s sebou přineslo možnost jeho využití pro páchání nebo usnadnění trestné činnosti. V tomto případě je počítač v roli nástroje či prostředku, který případnému pachateli přináší zcela nové možnosti. Díky svým vlastnostem umožňuje páchat některou „tradiční" trestnou činnost snadněji, rychleji, či dokonce z velké vzdálenosti. V rukou zkušených a znalých osob se může stát prostředkem pro tzv. dokonalý zločin, kdy ani nejmodernější technologie a postupy při vyšetřování nedokáží takové jednání odhalit. Mezi nejčastější případy, kdy je počítač využíván jako nástroj, se řadí počítačové pirátství a s tím spojené porušování autorského práva, různé formy podvodného jednání, pomluvy, šíření poplašných zpráv, pornografie, extremismus či jiné novější formy trestné činnosti spadající do počítačové kriminality.

Z výše uvedeného rozdělení vyplývá, že v některých případech lze prostřednictvím počítače provést útok na jiný počítač. V těchto případech počítač figuruje jako prostředek a zároveň předmět trestné činnosti. Jedná se především o případy neoprávněného proniknutí do cizího systému a tím překonání bezpečnostních opatření, která tomu mají zabránit. Takové jednání si bez využití počítačové techniky nelze představit.

4.3 Tradiční formy trestné činnosti s využitím počítače

Jedná se o takové formy trestné činnosti, které byly páchány již v době před nástupem a celospolečenským rozšířením informačních technologií včetně samotného počítače. Řadíme zde takové činy, které lze provést jak tradiční cestou bez využití počítačové techniky, tak nově s její pomoci. Právě vlivem informačních technologií tato protiprávní jednání nabyla nové formy a změnila mnohdy od základu svou podobu.[49]

4.3.1 Průmyslová špionáž

V dnešní době se pojmem průmyslová špionáž rozumí protiprávní činnost korporací prováděná s cílem získat potřebné informace o konkurenci a využít je ve svůj prospěch. Václav Jirovský ji například ve své publikaci definuje jako *„špionáž páchaná s komerčními cíli a ve své podstatě nemá nic společného s aktivitami rozvědky, které jsou zaměřeny na*

[49] MATĚJKA, Michal. *Počítačová kriminalita.* Praha: Computer Press, 2002, str. 60.

bezpečnost státu.“[50] Tato činnost, která vede k nelegálnímu sběru informací o konkurenčních subjektech, existovala již před vynálezem počítače, ale právě s jeho využitím a využitím počítačové sítě se její provedení značně zjednodušilo.[51] Děje se tak často skrze hackerské průniky do systémů konkurence s cílem získat potřebné materiály a informace, které mohou být následně mnohostranně využity. V tomto případě by takové jednání bylo postižitelné stejně jako samotný hacking (viz 4.4.1).

Stále častěji společnosti využívají i legálních aktivit v této oblasti, nazývaných „business intelligence“. Jedná se o činnost se stejným významem a cílem, ovšem za využití dostupných a právem aprobovaných prostředků. Těmi můžou být veškeré veřejnosti přístupné zdroje, jakými jsou materiály publikované konkurencí, nezávislými organizacemi či dostupné z veřejných rejstříků apod.[52]

4.3.2 Podvod a zpronevěra

Trestného činu podvodu se pachatelé dopouštěli již dávno před vznikem počítače a používali k tomu více či méně sofistikované metody. S nástupem internetu se otevřelo zcela nové prostředí, které znamenalo další rozvoj různých podvodných aktivit s cílem obohatit se na úkor druhých. Jednotlivé případy se vyznačují nejčastěji tím, že pachatel uvede někoho v omyl nebo využije něčího omylu ve svůj prospěch a v důsledku toho vzniká poškozenému škoda na majetku. Příkladem může být vznik mnoha webových stránek a e-shopů s různou tématikou, které nabízí ve skutečnosti neexistující zboží či služby ve snaze vylákat peníze z neopatrných uživatelů.[53] Velkou roli zde hraje i psychologická stránka věci, což znamená, že se pachatelé snaží působit velmi důvěryhodně a používají k tomu mnohdy rafinovaných metod.

S rozvojem bankovního sektoru došlo k postupnému nárůstu případů bankovního podvodu. Zde je situace pro pachatele o něco složitější, a to z důvodu, že tyto finanční ústavy kladou velký důraz na bezpečnost. Proto mají nejčastěji tyto případy na svědomí zaměstnanci s potřebným přístupem a jedná se především o činy, které mají charakter neoprávněné manipulace s bankovními záznamy (účty, hlavní knihou, bankovními příkazy apod.).[54]

---

[50] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, a.s., 2007, s. 169.
[51] MATĚJKA, Michal. *Počítačová kriminalita.* Praha: Computer Press, 2002, str. 52.
[52] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, a.s., 2007, s. 169-170.
[53] MATĚJKA, Michal. *Počítačová kriminalita.* Praha: Computer Press, 2002, str. 61.
[54] SMEJKAL, Vladimír a kol. *Právo informačních a telekomunikačních systémů.* 2. vydání. Praha: C.H.Beck, 2004, s. 716.

Všechna výše zmíněná jednání by mohla být klasifikována jako trestný čin podvodu dle § 209 trestního zákoníku.

Určitý specifický druh podvodu vyjadřuje skutková podstata trestné činu provozování nepoctivých her a sázek, kterou v reakci na nárůst tzv. počítačových her zákonodárce zařadil do trestního zákona (zákon č. 140/1961 Sb.) v roce 1991.[55] Skutková podstata tohoto trestného činu doznala v novém trestním zákoníku určitých změn, kdy došlo k jejímu zpřesnění a zároveň zpřísnění postihu za toto jednání.

Počítač lze snadno využít také ke spáchání trestného činu zpronevěry, kterého se dopouští osoby, kterým byly svěřeny například finance za účelem jejich správy a ty pak zneužijí ke svému vlastnímu obohacení. Uvedené protiprávní jednání může být posouzeno jako trestný čin zpronevěry dle § 206 trestního zákoníku.

4.3.3 Padělání

Tvrzení, že lze počítač chápat jako nástroj sloužící k usnadnění některých druhů trestné činnosti platí v případě padělání dvojnásob. Ještě před jeho využitím bylo k padělání dokumentů, peněz a jiných veřejných listin potřeba složitých postupů a dobrých znalostí. S rozvojem moderních grafických zařízení se pro padělatele vše zjednodušilo. Naopak to klade velký důraz na bezpečnost a prevenci, k čemuž jsou využívány mnohé metody, které mají takovému jednání zabránit. Jsou vyvíjeny a zdokonalovány mnohé ochranné prvky, které se stávají součástí všech padělatelných předmětů, na kterých lpí veřejnoprávní ochrana a jejichž padělání je trestné.

Na tato protiprávní jednání pamatuje i trestní zákoník, který obsahuje skutkovou podstatu trestného činu padělání a pozměnění peněz (§ 233), neoprávněného opatření, padělání a pozměnění platebního prostředku (§ 234), padělání a pozměnění předmětů k označení zboží pro daňové účely a předmětů dokazujících splnění poplatkové povinnosti (§ 245), padělání a pozměnění známek (§ 246), padělání a pozměnění veřejné listiny (§ 348). Z hlediska počítačové kriminality v souvislosti s paděláním je zajímavé ustanovení § 236 trestního zákoníku, dle kterého je trestná výroba a držení padělatelského náčiní a kde je mimo jiné příkladně uveden počítačový program jako jeden z možných prostředků k danému protiprávnímu jednání.

4.3.4 Pomluva

[55] JELÍNEK, Jiří a kolektiv. *Trestní zákon a trestní řád s poznámkami a judikaturou a předpisy souvisící.* 25. aktualizované vydání. Praha: Linde Praha, 2007, s. 316.

Trestný čin pomluvy, jehož podstatou je sdělení nepravdivého údaje o jiném za předpokladu, že je takový údaj způsobilý poškodit danou osobu zejména v jeho rodinném či profesním životě, lze spáchat celou řadou způsobů. Škodlivost takového činu je do jisté míry závislá na skutečnosti, k jak širokému okruhu lidí se takový nepravdivý údaj dostane. To si zajisté uvědomuje i zákonodárce, který stanoví přísnější postih je-li takový čin spáchán prostřednictvím veřejně přístupných sdělovacích prostředků. Kvalifikovaná skutková podstata trestného činu pomluvy (§ 184 odst. 2 trestního zákoníku) doznala oproti staré právní úpravě určité změny. Příkladný výčet, jakými způsoby lze tento čin spáchat, byl rozšířen o veřejně přístupnou počítačovou síť, kterou se rozumí *„funkční propojení počítačů s cílem vytvořit informační systém pracující s tzv. dálkovým přístupem.“*[56] Takovou sítí se rozumí především internet, který má na rozdíl od jiných prostředků tu „výhodu“, že k ní má přístup prakticky každý.

Spáchání tohoto činu prostřednictvím internetu se pro pachatele jeví jako mnohem snazší záležitost, k čemuž přispívá i fakt, že se pachatel pod dojmem anonymity cítí, jako by nemohl být dopaden. Často jsou však orgány činné v trestním řízení schopné zjistit motiv takové osoby a za pomoci dalších metod pachatele vypátrat.

4.3.5 Hoaxes

Poměrně novou formou protiprávního jednání, které se plně rozmohlo až s nástupem internetu a informačních technologií obecně, je šíření zpráv, které obsahují nepřesné či zkreslené informace včetně nepravdivých varování (tzv. hoaxes).[57] Právě s využitím internetu nebezpečnost takového jednání roste a hlavním důvodem je rychlost, s jakou lze takovou poplašnou zprávu rozšířit mezi velkou část naší populace. Nebezpečnost lze také spatřovat ve schopnosti těchto zpráv vyvolat strach či paniku a ovlivnit tak chovaní mnoha lidí.

Tento druh poplašných zpráv zasílaných adresátům nejčastěji prostřednictvím e-mailů často obsahuje nepravdivé údaje a informace o hrozbě nových počítačových virů, škodlivosti některých surovin či dokonce o možnosti nákazy nebezpečným virem.[58] Z obsahu některých zpráv lze snadno pochopit, že se jedná o výmysl, avšak mnohé z nich mohou na první pohled představovat reálnou hrozbu a v části populace tak vzbudit znepokojení a obavy. Popsané úmyslné jednání může být trestné dle § 357 trestního zákoníku. V případě, že je taková zpráva

[56] ŠÁMAL, Pavel a kol. *Trestní zákoník II. §140 až 421 : Komentář*. 1. vydání. Praha: C.H. Beck, 2010, s. 1642-1644.
[57] Hoax.cz [online]. *Co je to hoax.*[cit. 21. prosince 2010]. Dostupné na <http://www.hoax.cz/hoax/co-je-to-hoax>.
[58] MATĚJKA, Michal. *Počítačová kriminalita.* Praha: Computer Press, 2002, str. 68-69.

sdělena prostřednictvím internetu, který lze za určitých okolností považovat za hromadný informační prostředek, připadá v úvahu klasifikace dle kvalifikované skutkové podstaty tohoto trestného činu šíření poplašné zprávy (§ 357 odst. 2).

4.3.6 Projevy extremismu

Společnost se i v dnešní době potýká s projevy extremistických skupin, které se snaží svoji ideologii šířit a propagovat. Ať už jsou jejich motivy náboženské, politické či rasové, vyznačují se často nesnášenlivostí vůči jiným skupinám a hnutím. Veřejná počítačová síť jim umožnila přenést své aktivity do kyberprostoru, který mohou využít ke společné komunikaci, k propagaci svých postojů a myšlenek, případně i k získání nových členů a stoupenců. Právě moderní informační technologie a zejména internet přispěly k celosvětovému nárůstu případů extremismu a jednotlivým skupinám umožnily navázat kontakt s vyznavači stejné ideologie z jiných oblastní či zemí.

Zde narážíme na velký problém, kterým může být exteritoriální povaha tohoto jednání. Existují země s odlišnou právní úpravou týkající se svobody projevu, což znamená možný konflikt při uplatňování práva. Zatímco v anglosaských zemích se uplatnilo pojetí trestat zásadně skutky, v mnoha zemích kontinentální Evropy se můžeme setkat s trestnými činy, které lze spáchat pouhým slovem.[59] V důsledku toho se lze setkat s případy, kdy je na internetu uveřejněn obsah s prvky extremismu, který je veřejně přístupný v zemích, kde se otázka trestnosti takového činu velmi liší.

Vážnost situace donutila členské státy Rady Evropy přijmout dokument, který by harmonizoval vnitrostátní právní úpravu v této oblasti a výrazně tak přispěl k jejich spolupráci na mezinárodní scéně v boji proti extremismu. Byl přijat Dodatkový protokol k Úmluvě o počítačové kriminalitě, týkající se kriminalizace činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů. Tato úprava nebyla zapracována do samotné Úmluvy právě z důvodu obavy o její ratifikaci ze strany USA, od kterých se očekávalo, že k tomuto dokumentu přistoupí, ale jejichž právní úprava je v tomto směru značně benevolentnější. Vše bylo vyřešeno přijetím již zmíněného Dodatkového protokolu k Úmluvě, jehož cílem je harmonizovat trestněprávní úpravu v oblasti boje proti rasismu a xenofobii na internetu a prohloubit a zintenzivnit mezinárodní spolupráci. [60]

[59] MATĚJKA, Michal. *Počítačová kriminalita.* Praha: Computer Press, 2002, str. 67-68.
[60] GŘIVNA, Tomáš a kol. *Kyberkriminalita a právo*. Praha: Auditorium, 2008, s. 145-146.

Dodatkový protokol výslovně stanoví jednání spáchaná prostřednictvím počítačového systému, která mají být dle národních právních úprav jednotlivých smluvních států trestná:[61]

i. šíření rasistických a xenofobních materiálů,
ii. rasisticky a xenofobně motivovaná pohrůžka,
iii. rasisticky a xenofobně motivovaná urážka,
iv. popření, hrubé snižování, schvalování nebo ospravedlnění genocidy nebo zločinů proti lidskosti.

Dále stanoví trestnost návodu a pomoci k výše uvedenému jednání. Pro zajímavost Česká republika Dodatkový protokol narozdíl od samotné Úmluvy[62] dosud nepodepsala. Trestní zákoník platný na našem území však obsahuje řadu ustanovení, které vycházejí z ústavněprávních a mezinárodněprávních principů chránících rovnost lidí bez rozdílu národnosti, jazyka, rasy, politického přesvědčení a náboženství (srov. zejména čl. 3 odst. 1 Listiny základních práv a svobod, čl. 2 a 7 Všeobecné deklarace lidských práv, čl. 14 Evropské úmluvy a čl. 26 Mezinárodního paktu o občanských a politických právech).[63] Ochranu poskytuje proti všem jednáním tohoto druhu provedených jakoukoliv formou, včetně prostřednictvím počítačového systému.

4.3.7 Dětská pornografie

Počítačová technika a s ní spojená veřejně přístupná počítačová síť s sebou přinesly nárůst různých druhů nežádoucí pornografie, zejména té dětské. Je nutné rozlišovat mezi „klasickou“ pornografií, která je v mnoha zemích beztrestná a pornografií „závadnou“, jejíž obsah je z hlediska mravnosti nepřípustný a tudíž trestný.

Trestní zákoník obsahuje skutkové podstaty trestných činů týkajících se pornografie v ustanoveních § 191 až § 193 zvláštní části. Ve spojitosti s počítačovou kriminalitou lze především mluvit o trestném činu šíření pornografie (§ 191) a trestném činu výroby a jiného nakládání s dětskou pornografií (§ 192), k jejichž spáchání lze mimo jiné využít právě počítač. Provozovatelé internetových stránek s pornografickou tématikou tak mají povinnost alespoň formou varování upozornit na nepřístupnost obsahu osobám mladším 18 let a mnohdy požadují potvrzení nebo prohlášení o zletilosti ze strany návštěvníka takovéto stránky.

Tato problematika je natolik závažná, že je součástí mnoha mezinárodních smluv a dokumentů přijatých s cílem zefektivnit boj proti dětské pornografii. Své místo zaujímá i ve

[61] Tamtéž, s.146.
[62] Česká republika Úmluvu o počítačové kriminalitě podepsala 9. února 2005. K ratifikaci však k dnešnímu dni nedošlo.
[63] JELÍNEK, Jiří a kol. *Trestní právo hmotné.* 1. vydání. Praha: Leges, 2009, s. 789.

zmiňované Úmluvě o počítačové kriminalitě v článku 9 s názvem „Přestupky týkající se dětské pornografie“.[64] Jednotlivá ustanovení tohoto článku poté smluvním stranám ukládají přijmout veškerá opatření proti uvedeným jednáním, vymezují pojem „dětská pornografie“ a stanoví, kdo je tvz. „nezletilou osobou“.[65]

4.3.8 Neoprávněné nakládání s osobními údaji

„*Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.“*[66] Právě s rozvojem mnoha forem elektronické komunikace, internetového bankovnictví, elektronického podpisu či nově informačního systému datových schránek roste i hrozba zneužití osobních údajů. Výše zmíněné právo je chráněno z hlediska správního práva prostřednictvím zákona č. 101/2000 Sb., o ochraně osobních údajů, který mimo jiné vymezuje základní pojmy, stanoví práva a povinnosti při zpracování osobních údajů, jakož i sankce za případné správní delikty povinných subjektů.

Trestněprávní ochranu zajišťuje trestní zákoník obsahující ustanovení postihující protiprávní jednání směřující proti právem chráněnému zájmu na ochranu osobních údajů. Ustanovení § 180 (neoprávněné nakládaní s osobními údaji) trestního zákoníku se skládá ze dvou základních skutkových podstat (§ 180 odst. 1, § 180 odst. 2).[67] První z nich stanoví trestnost jednání, kdy osoba *„neoprávněně zveřejní, sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje, které byly o jiném shromážděné v souvislosti s výkonem veřejné moci, a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají“*, zatímco druhá postihuje jednání, kdy osoba *„poruší státem uloženou nebo uznanou povinnost mlčenlivosti tím, že neoprávněně 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 nebo oprávněných zájmech osoby, jíž se osobní údaje týkají.“* [68] V obou případech postačí jako forma zavinění nedbalost.

Mezi okolnosti podmiňující použití vyšší trestní sazby byl do § 180 odst. 3 písm. b) nově začleněn způsob spáchání tohoto činu prostřednictvím veřejně přístupné počítačové sítě. Obezřetnost při poskytování či vkládání svých osobních údajů na veřejnou síť je základní předpoklad k zabránění jejich zneužití.

---

[64] V autentickém znění „Offences related to child pornography“. Viz BAYEROVÁ, Monika. Evropská úmluva o počítačové kriminalitě a sexuální zneužívání dětí. *Trestněprávní revue,* 2003, roč. 2, č. 5, s. 156.
[65] Tamtéž
[66] Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod, ve znění ústavního zákona č. 162/1998 Sb.
[67] JELÍNEK, Jiří a kol. *Trestní právo hmotné.* 1. vydání. Praha: Leges, 2009, s. 534.
[68] Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

4.3.9 Počítačové pirátství

Počítačové pirátství úzce souvisí s porušováním autorského práva, ke kterému docházelo za pomoci různých prostředků a metod ještě před nástupem počítače. Avšak teprve s využitím počítačové techniky byl zaznamenán obrovský nárůst těchto případů, kdy dochází k porušení autorského práva. Mezi díla chráněná autorským zákonem řadíme *„dílo literární a jiné dílo umělecké a dílo vědecké, které je jedinečným výsledkem tvůrčí činnosti autora a je vyjádřeno v jakékoli objektivně vnímatelné podobě včetně podoby elektronické, trvale nebo dočasně, bez ohledu na jeho rozsah, účel nebo význam“*. [69] Dle zákonné úpravy se dílem rozumí i počítačový program a databáze, pokud jsou vlastním duševním výtvorem autora.

Nejčastěji se protiprávní jednání spočívající v porušení autorského práva vztahuje k audiálním či audiovizuálním záznamům a počítačovým programům. Nelegálnímu kopírování na audiokazety či videokazety již zdá se odzvonilo a vše se nyní přesouvá do prostředí internetu. Mluvíme o moderním počítačovém pirátství, kdy s postupným zvyšováním přenosové rychlosti na internetu lze stáhnout hudbu, film, hru nebo program doslova během pár vteřin. Problém nastává v okamžiku jedná-li se o pirátské kopie těchto děl chráněných autorským právem. Zde může dojít k naplnění skutkové podstaty trestného činu porušení autorského práva, práv souvisejících s právem autorským a práv k databázi dle § 270 trestního zákoníku. Toto ustanovení stanoví trestnost jednání toho, kdo *„neoprávněně zasáhne nikoli nepatrně do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, zvukovému či zvukově obrazovému záznamu, rozhlasovému nebo televiznímu vysílání nebo databázi.“*[70]

Ve spojitosti s počítačovým pirátstvím se často zmiňuje pojem warez. Jedná se o nelegální výrobu a šíření software prostřednictvím CD nebo DVD nosičů, serverů[71] nebo dnes velmi rozšířeného systému peer-to-peer. Ačkoli je jeho název odvozen od slova software, nevztahuje se již pouze k počítačovým programům a aplikacím, nýbrž poskytuje přístup i k pirátským kopiím hudebních a filmových nahrávek či počítačových her. I zde připadá v úvahu právní kvalifikace dle § 270 trestního zákoníku, naplňuje-li zmíněné jednání všechny znaky skutkové podstaty tohoto ustanovení.

Počítačová kriminalita zahrnuje i jiné formy protiprávního jednání, při nichž dochází k porušování autorského práva. Jedná se především o činnost známou pod názvem

[69] Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.
[70] Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.
[71] Nejčastěji pomocí nechráněných FTP serverů. FTP (File Transfer Protocol) je protokol sloužící k přenosu souborů mezi počítači prostřednictvím počítačové sítě.

„cracking“. K této činnosti je dnes výhradně zapotřebí počítačové a jiné informační technologie, a proto o ní bude blíže pojednáno v následující kapitole.

4.4 Nové formy trestné činnosti s využitím počítače

Tato kapitola uvádí nejčastější protiprávní jednání, která se objevila až s nástupem moderních informačních technologií. Řadíme zde trestnou činnost páchanou výlučně za pomoci počítačové techniky. I přesto, že tyto formy trestné činnosti spojuje společný prostředek, tak každá z nich představuje významově zcela jiný druh protiprávního jednání sledující rozličný cíl.

4.4.1 Hacking

O vzniku a původním významu tohoto pojmu jsem se zmínil již výše, proto bude věnována pozornost spíše dnešnímu pojetí. Dnes již všeobecně chápaný a užívaný termín hacking ve své podstatě znamená překonání bezpečnostních opatření s cílem neoprávněně proniknout do počítačového systému. Přitom motiv takového jednání může být různý. Mnoho pachatelů (hackerů) se daného jednání dopouští s cílem zjistit, jak celý systém funguje a uskutečnění takového činu berou jako výzvu.[72] Najdou se však i tací, jejichž úmysl směřuje ke způsobení škody nebo tak činí za účelem vlastního prospěchu.

Z pohledu nového trestního zákoníku je uvedené jednání trestné bez ohledu na motiv a úmysl s jakým jej pachatel činí. Na rozdíl od staré právní úpravy[73], kde se k trestnosti takového činu vyžadoval úmysl pachatele způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch, je dnešní pojetí mnohem přísnější a zcela v souladu s Úmluvou o počítačové kriminalitě. Pachatele této formy počítačové kriminality lze postihnout dle ustanovení trestního zákoníku obsahující skutkovou podstatu trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací. Samotné neoprávněné získání přístupu k počítačovému systému je trestné dle § 230 odst. 1. Byla navíc využita možnost stanovená Úmluvou zakomponovat do tohoto ustanovení jako podmínku trestnosti překonání bezpečnostního opatření. Tím se rozumí veškerá opatření, která systém chrání a zamezuje volnému přístupu do systému nebo jeho části. Téměř každý systém je napadnutelný, ovšem s využitím nejrůznějších forem bezpečnostních opatření lze snížit riziko na minimum.

4.4.2 Cracking

[72] MATĚJKA, Michal. *Počítačová kriminalita.* Praha: Computer Press, 2002, str. 53-54.
[73] Starý trestní zákon č. 140/1961 Sb.

S problematikou neoprávněného pronikání do systému počítače a warezu je úzce spojena další forma počítačové kriminality nazvaná cracking. Jak jsem již výše předeslal, jedná se o činnost, při níž v mnohých případech dochází k porušení autorského práva. Cracking lze vymezit jako *„prolamování nebo obcházení ochranných prvků elektronických nebo programových produktů s cílem jejich neoprávněného použití.“*[74] Jinými slovy jedná se o překonávání technické ochrany, která bývá součástí chráněných produktů. Úkolem těchto ochranných opatření je alespoň omezit autorem nepovolené užití díla.[75] Nabízí se otázka, na kolik jsou tyto ochranné prvky účelné, jelikož prozatím veškeré podobné „zábrany“ byly postupem času překonány.

Autorský zákon v ustanovení § 43 stanoví, že *„do práva autorského neoprávněně zasahuje ten, kdo obchází účinné technické prostředky ochrany práv podle tohoto zákona.“*[76] V návaznosti na toto ustanovení lze konstatovat, že osoba, která se dopustí výše zmíněného zásahu nikoli nepatrným způsobem, může svým jednáním naplnit znaky skutkové podstaty trestného činu porušení autorského práva, práv souvisejících s právem autorským a práv k databázi dle § 270 trestního zákoníku. Cracking lze využít i ke zjištění přístupových údajů potřebných k neoprávněnému vniknutí do cizího systému, proto o něm lze za určitých okolností mluvit ve spojitosti s trestným činem neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 trestního zákoníku.

4.4.3 Spamming

Zpočátku se pojmem spamming rozumělo rozesílání nevyžádaných zpráv různého obsahu (především reklamního) prostřednictvím elektronické pošty. Postupně se však rozšířil počet způsobů, jakými lze tato nevyžádaná a nežádoucí sdělení šířit. Byly tak postiženy i jiné formy komunikace – např. sociální sítě typu facebook, diskuzní fóra či komentáře. Původci těchto zpráv získávají e-mailové adresy z mnoha zdrojů. Při elektronické komunikaci či poskytovaní služeb na internetu je v drtivé většině případů vyžadována kontaktní emailová adresa, která může být později využita k zasílání tohoto druhu zpráv.

Z trestněprávního hlediska je postih takového jednání dost komplikovaný. Pouze zasílání nevyžádané pošty není dle naší právní úpravy trestné. Lze si však představit situaci, kdy za určitých okolností může dojít k naplnění skutkové podstaty trestného činu

[74] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, a.s., 2007, s. 106.
[75] SÝKORA, Martin. *Technické prostředky ochrany autorských práv* [online]. 31. ledna 2010 [cit. dne 29. prosince 2010]. Dostupné na <http://www.pravoit.cz/article/technicke-prostredky-ochrany-autorskych-prav>.
[76] Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

neoprávněného nakládání s osobními údaji dle § 180 trestního zákoníku. Adresu elektronické pošty lze považovat za osobní údaj ve smyslu tohoto ustanovení pouze tehdy, lze-li z ní identifikovat jejího vlastníka.

4.4.4 Carding

Pod pojmem carding obecně chápeme zneužití platební karty, která se postupně stává jedním z nejrozšířenějších platebních prostředků současnosti. Krátce po jejím uvedení do oběhu se však stala předmětem protiprávního jednání, které si klade za cíl získat informace potřebné k jejímu zneužití. K tomu pachatelé využívají nejrůznějších, mnohdy velmi rafinovaných metod. Technicky nejjednodušší způsob je získání samotné platební karty např. krádeží. Jsou známy i metody mnohem složitější. Od podvodného vylákání tzv. PIN[77] potřebného k získání přístupu až po využití mechanismů pro čtení údajů přímo z platební karty vložené do bankomatu.

Do nového trestního zákoníku nebyla převzata skutková podstata trestného činu neoprávněného držení platební karty, která byla součástí staré právní úpravy. Trestnost takového jednání však vyplývá z ustanovení § 234 trestního zákoníku o neoprávněném opatření, padělání a pozměnění platebního prostředku. Účelem tohoto ustanovení tedy není jen ochrana před zneužitím platební karty, ale i jiných platebních prostředků, jako jsou elektronické peníze, příkaz k zúčtování apod.

Zajímavou otázkou je, zda lze platební kartu považovat za nosič informací ve smyslu ustanovení § 230 odst. 2 trestního zákoníku. Jelikož sama o sobě je schopna nést potřebné informace, jako například údaje o osobním kódu či stavu účtu včetně limitu možného výběru, lze usuzovat, že takovýmto druhem nosiče informací je.[78] Z toho plyne, že po splnění dalších znaků uvedených v tomto ustanovení lze v souvislosti s platební kartou uvažovat i o případném naplnění skutkové podstaty trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací dle zmíněného § 230 odst. 2 trestního zákoníku.

4.4.5 Sniffing

Rozvoj elektronické komunikace s sebou přinesl kromě spammingu také jinou formu protiprávního jednání, odborně nazvanou sniffing. Jedná se o neoprávněné monitorování či

[77] PIN (Personal Identification Number) neboli osobní identifikační číslo slouží k ochraně před neoprávněným přístupem.
[78] SMEJKAL, Vladimír, SOKOL, Tomáš, VLČEK, Martin. *Počítačové právo*. Praha: C.H.Beck, 1995, s. 115.

odposlouchávání komunikace na síti.[79] K této činnosti lze využít mnoha prostředků, z nichž patrně nejjednodušší je využití speciálních programů tzv. snifferů[80], které fungují na principu sledování vybraného síťového uzlu, což umožňuje získat potřebné informace včetně přístupových údajů nebo obsahu elektronické komunikace. Znamená tak jednoznačný zásah do soukromí osob a jimi posílaných zpráv. Často se však poškozená osoba o takovém jednání ani nedozví, což znamená, že mnoho pachatelů zůstane nepotrestáno. Jednou z možností jak se proti této činnosti bránit je šifrování komunikace po síti, čímž lze předejít případnému zneužití získaných informací.

Pachatele tohoto činu lze dle současné trestněprávní úpravy postihnout dle § 182 trestního zákoníku za trestný čin porušení tajemství dopravovaných zpráv. Z odst. 1 písm. b) tohoto ustanovení plyne, že se jej dopustí osoba, která *„úmyslně poruší tajemství datové, textové, hlasové, zvukové či obrazové zprávy posílané prostřednictvím sítě elektronických komunikací a přiřaditelné k identifikovanému účastníku nebo uživateli, který zprávu přijímá“*.[81] V odst. 1 písm. c) stejného ustanovení je poté stanovena trestnost jednání, při kterém dojde k porušení tajemství neveřejného přenosu počítačových dat do počítačového systému či z něj. Druhá základní skutková podstata tohoto trestného činu postihuje pachatele, který takové tajemství prozradí nebo využije (§ 182 odst. 2). Trestní zákoník stanoví vyšší trest pro zaměstnance provozovatele počítačového systému, který se dopustí stejného jednání nebo umožní spáchat takový čin jiné osobě (§ 182 odst. 5).

4.4.6 Cybersquatting

Podstatou cybersquattingu je spekulace s názvy internetových domén. Vše funguje tak, že si osoba či společnost zaregistruje doménu pod celospolečensky známým názvem, nejčastěji určitého podniku či jeho produktu, kterou se poté snaží tomuto subjektu prodat za co možná nejvýhodnějších podmínek. K tomu docházelo především v počátcích, kdy jednotlivé společnosti teprve vstupovali do prostředí internetu a chtěli zcela logicky vlastnit doménu nesoucí jejich název. Pod toto označení spadá i jiná forma jednání, kdy si subjekt zaregistruje svou doménu pod názvem dobře známého produktu či služby jiné společnosti a na této stránce opravdu tento druh zboží či služby poskytuje. Nejen že tím poškozuje danou společnost, ale i pro samotné uživatele je to značně matoucí.

[79] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, a.s., 2007, s. 106.
[80] MATĚJKA, Michal. *Počítačová kriminalita.* Praha: Computer Press, 2002, str. 74.
[81] Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

Ačkoli se na tuto problematiku vztahují především soukromoprávní předpisy týkající se tzv. nekalé soutěže, lze se tímto jednáním dopustit i trestného činu porušení předpisů o pravidlech hospodářské soutěže dle § 248 trestního zákoníku. Jednou z podmínek trestní odpovědnosti pachatele tohoto činu je způsobení újmy jiným soutěžitelům nebo spotřebitelům nebo opatření neoprávněné výhody sobě nebo jinému, a to vše ve větším rozsahu. Za určitých okolnosti připadá v úvahu kvalifikace dle skutkové podstaty trestného činu porušení práv k ochranné známce a jiným označením (§ 268 trestního zákoníku).

4.4.7 Cyberstalking

Jedná se o složený název, vycházející především z pojmu stalking, kterým se v anglicky mluvících zemích označuje pronásledování jiné osoby. Z kriminologického hlediska jej lze definovat jako *„úmyslné, zlovolné pronásledování a obtěžování jiné osoby, které snižuje kvalitu jejího života a ohrožuje její bezpečnost.“*[82] Tuto činnost lze páchat nejen vtíráním se do blízkosti postižené osoby, ale i prostřednictvím dopisů, telefonických hovorů či SMS zpráv.[83] S rozvojem nových forem elektronické komunikace se stalking přesunul i do prostředí internetu. V současné době jsou to sociální sítě (Facebook, Twitter apod.), které sdružují miliony lidí po celém světě, kteří mohou být potencionální „kořistí“ pro takzvané stalkery. Cyberstalking tedy není nic jiného než výše popsané jednání páchané prostřednictvím těchto moderních komunikačních prostředků.

Nový trestní zákoník obsahuje narozdíl od staré právní úpravy skutkovou podstatu, dle které lze stalking účinně postihnout. Jedná se o ustanovení § 354 trestního zákoníku (nebezpečné pronásledování), které v odst. 1 písm. c) výslovně zmiňuje prostředky elektronických komunikací, které lze k tomuto jednání využít. Předpokladem je však dlouhodobost takového počínání, které je navíc způsobilé vzbudit v poškozeném důvodnou obavu o jeho život nebo zdraví nebo o život a zdraví osob jemu blízkých.

[82] ČÍRTKOVÁ, Ludmila. Psychologické poznatky k nebezpečnosti pronásledování (stalking). *Kriminalistika* [online]. 2004 [cit. 4. ledna 2011]. Dostupné na <http://aplikace.mvcr.cz/archiv2008/casopisy/kriminalistika/2004/0404/cirtkova_info.html>.
[83] Tamtéž.

5 Právní úprava v oblasti počítačové kriminality

5.1 Vývoj trestněprávní úpravy v oblasti počítačové kriminality

Na prudký vývoj informačních technologií a jejich využití pro páchání trestné činnosti reaguje trestní právo vždy s určitým zpožděním. Přesto je nadmíru jasné, že se bez regulace jednání v oblasti počítačové kriminality již neobejdeme. Poté co počítač a jiné informační technologie vstoupily do mnoha oblastí soukromého a veřejného života dochází k neustálému zdokonalování právní i věcné ochrany těchto technologií a dat, jimi zpracovaných.[84]

První trestné činy spojené s počítači se objevily již v 70. a 80. letech minulého století a byly často kvalifikovány jako sabotáž (§ 97 zákona č. 140/1961 Sb.). Právní posouzení těchto činů bylo tehdy velmi ovlivněno politickými názory. Postupně byly tyto skutky často překvalifikovány na, pro pachatele příznivější, poškozování majetku v socialistickém vlastnictví (§ 136-137 tehdejšího trestního zákona z roku 1961).[85] Trestní zákon platný v té době neobsahoval skutkovou podstatu, která by stanovila postih za neoprávněný přístup k počítačovému systému, jak tomu bylo např. v USA, kde se takové zákony vytvářely již v průběhu 80. let 20. století, a to jak na federální úrovni, tak na úrovni jednotlivých států. Postupný nárůst trestné činnosti s využitím počítače s sebou přineslo naléhavou potřebu přijmout takovou trestněprávní úpravu, která by byla účinná a umožnila postihnout i tato protiprávní jednání.

Pozitivní krok byl učiněn počátkem 90. let minulého století, kdy došlo k zařazení nových skutkových podstat do tehdejšího trestního zákona. V souvislosti s počítačovou kriminalitou se jedná především o ustanovení § 257a (poškození a zneužití záznamu na nosiči informací), § 178 (neoprávněné nakládání s osobními údaji) či § 250c (provozování nepoctivých her a sázek), která se tak stala součástí trestního zákona z roku 1961.[86] Tato ustanovení měla postihovat především podvodná jednání s využitím výpočetní techniky, se kterými se v té době tzv. „roztrhl pytel“.

Skutková podstata trestného činu poškození a zneužití záznamu na nosiči informací byla do tehdejšího trestního zákona zařazena zákonem č. 557/1991 Sb. a účinnosti nabyla 1. ledna 1992. Jednalo se o první trestněprávní ustanovení, které postihovalo protiprávní jednání

[84] SMEJKAL, Vladimír. Kriminalita v prostředí informačních systémů a rekodifikace trestního zákoníku. *Trestněprávní revue*, 2003, 2.ročník, č. 6, str. 161.
[85] SMEJKAL, Vladimír a kol. *Právo informačních a telekomunikačních systémů.* 2. vydání. Praha: C.H.Beck, 2004, s. 703.
[86] Tamtéž, s. 706.

namířená proti počítači a jeho obsahu. V původním znění byla stanovena trestnost jednání pachatele, který *„v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch získá přístup k nosiči informací a*

a) *takových informací neoprávněně užije,*
b) *informace zničí, poškodí nebo učiní neupotřebitelnými, nebo*
c) *učiní zásah do technického nebo programového vybavení počítače“.*[87]

Počítač lze považovat za nosič informací ve smyslu tohoto ustanovení. Tato skutková podstata doznala určitých změn v důsledku novely z roku 2002. Došlo k přeformulování a doplnění tohoto ustanovení, což napomohlo k efektivnějšímu postihu pachatelů této trestné činnosti. Poté až do účinnosti nového trestního zákoníku zněla základní skutková podstata takto: *„Kdo získá přístup k nosiči informací a v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch*

a) *takových informací neoprávněně užije,*
b) *informace zničí, poškodí, změní nebo učiní neupotřebitelnými, nebo*
c) *učiní zásah do technického nebo programového vybavení počítače nebo jiného telekomunikačního zařízení,*

bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti nebo peněžitým trestem nebo propadnutím věci nebo jiné majetkové hodnoty.“[88]

Přitom není rozhodné, zda jde o oprávněný přístup k nosiči informací nebo nikoli.

Přes veškerou snahu se však tímto počinem nepodařilo eliminovat všechna jednání směřující proti informačním systémům. Lze vytknout především absenci ustanovení, které by postihovalo samotný neoprávněný průnik do počítačového systému. Tedy případ, kdy pachatel vnikne do systému cizího počítače, aniž by měl úmysl způsobit jakoukoli škodu či získat neoprávněný prospěch. Takové jednání by patrně zůstalo bez postihu, jelikož jej nelze pod tuto skutkovou podstatu podřadit.

Z hlediska zavinění se u pachatele vyžadoval úmysl, jelikož ustanovení § 257a neznalo nedbalostní kvalifikaci. To v praxi například znamenalo nemožnost stíhat zaměstnance, kteří neúmyslně způsobili škodu na počítači svého zaměstnavatele.[89] Škoda se přitom mohla vyšplhat do astronomických výšek.

V průběhu té doby již probíhala práce na rekodifikaci trestního práva hmotného, která vyvrcholila přijetím nového trestního zákoníku (zákon č. 40/2009 Sb.), účinného od 1. ledna

[87] Původní znění § 257a zákona č. 140/1961 Sb. (trestní zákon), dle novely z roku 1991.
[88] Novelizované znění § 257a zákona č. 140/1961 (trestní zákon).
[89] SMEJKAL, Vladimír. Kriminalita v prostředí informačních systémů a rekodifikace trestního zákoníku. *Trestněprávní revue*, 2003, 2.ročník, č. 6, str. 166.

2010. Jednotlivým změnám, které doznal nový trestní zákoník v souvislosti s tímto ustanovením bude věnována samostatná kapitola (viz níže).

Svým vývojem prošla i jiná ustanovení mající souvislost s počítačovou kriminalitou. Jedná se především o ustanovení § 270 trestního zákoníku[90] o porušení autorského práva, práv souvisejících s právem autorským a práv k databázi. Skutková podstata tohoto trestného činu byla součástí i trestního zákona platného do 31. prosince 2009 a ve své podstatě odkazuje na zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a změně některých zákonů (autorský zákon). Autorský zákon je právní předpis, který poskytuje ochranu před neoprávněnými zásahy do práva autorského. Z ustanovení § 270 trestního zákoníku nově vyplývá, že osoba, která zasáhne do zmíněných zákonem chráněných práv pouze nepatrně, nebude trestně odpovědná. Samotné ustanovení bylo rozšířeno i o jiné znaky, které nebyly součástí staré právní úpravy.[91]

Často je dáváno do spojitosti s trestnou činností s využitím počítače i ustanovení § 180 trestního zákoníku. Ani tato skutková podstata trestného činu neoprávněného nakládání s osobními údaji není zcela nová. Součástí starého trestního zákona se stala díky novele z roku 1993 a následně byla doplněna novelou z roku 2000. Také současná podoba této skutkové podstaty v platném trestním zákoníku doznala jistých změn.[92]

Na závěr této kapitoly bych uvedl zcela nový trestný čin nebezpečného pronásledování (§ 354 trestního zákoníku), který dokonce nebyl obsažen ani ve vládním návrhu trestního zákoníku a chybí tak i důvodová zpráva k tomuto ustanovení.[93] Stal se součástí nového trestního zákoníku v reakci na sílící hrozbu ze strany těch, kteří i prostřednictvím informačních a telekomunikačních technologií soustavně pronásledují a obtěžují jiné osoby. Jedná se tak z hlediska trestněprávní úpravy o jednoznačně pozitivní počin.

5.2 Stávající právní úprava počítačové kriminality

S účinností nového trestního zákoníku došlo ke změně právní úpravy v oblasti počítačové kriminality. Předlohou pro ustanovení týkající se výlučně trestné činnosti spojené s počítači byla Evropská úmluva o počítačové kriminalitě (dále jen Úmluva). Do trestního zákoníku byly zakotveny skutkové podstaty dvou trestných činů uvedených v hlavě páté, sdružující trestné činy proti majetku, čímž došlo k zapracování především článků 2 až 8 Úmluvy. Jedná se o skutkové podstaty trestných činů neoprávněného přístupu k počítačovému

[90] Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.
[91] Srov. § 270 zákona č. 40/2009 Sb. a § 152 zákona č. 140/1961 Sb.
[92] Srov. § 180 zákona č. 40/2009 Sb. a § 178 zákona č. 140/1961 Sb.
[93] JELÍNEK, Jiří a kol. *Trestní právo hmotné.* 1. vydání. Praha: Leges, 2009, s. 787.

systému a nosiči informací (§ 230) a opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231). Na základě požadavků z praxe byla tato ustanovení doplněna o trestný čin poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 232).[94] Jelikož se jedná o zásadní změnu v oblasti trestněprávní úpravy počítačové kriminality, budou tyto tři trestné činy blíže rozebrány.

5.2.1 Neoprávněný přístup k počítačovému systému a nosiči informací

Ustanovení § 230 trestního zákoníku obsahuje dvě základní skutkové podstaty (§ 230 odst. 1 a § 230 odst. 2). První odstavec přináší změnu v náhledu na neoprávněný průnik do počítačového systému. Na jeho základě lze nyní postihnout samotný neoprávněný přístup k počítačovému systému nebo jeho části po překonání bezpečnostních opatření. Trestnost tohoto jednání již tedy není vázána na splnění dalších podmínek. Předmětem ochrany tohoto ustanovení je počítačový systém, který je zde chráněn před ohrožením jeho bezpečnosti.[95]

Druhá základní skutková podstata tohoto trestného činu (§ 230 odst. 2) postihuje jednání osoby, která získá přístup k počítačovému systému nebo k nosiči informací a zároveň naplní alespoň jednu z alternativně stanovených podmínek, uvedených pod písmeny a) až d).[96] Jedná se tak o případy, kdy osoba s takovým přístupem:

- neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,
- neoprávněně vymaže nebo jinak zničí data uložená v počítačovém systému nebo na nosiči informací nebo je poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými,
- padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá, nebo
- neoprávněně vloží data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítače či jiného podobného zařízení.

Samotný fakt, zda dojde k získání přístupu k počítačovému systému nebo nosiči informací oprávněně či nikoli je zde zcela irelevantní.

[94] JELÍNEK, Jiří a kol. *Trestní právo hmotné.* 1. vydání. Praha: Leges, 2009, s. 620.
[95] ŠÁMAL, Pavel a kol. *Trestní zákoník II. §140 až 421 : Komentář*. 1. vydání. Praha: C.H. Beck, 2010, s. 2085.
[96] Tamtéž, s. 2089.

V odst. 3 písm. a) tohoto ustanovení se pak k výše zmíněným jednáním přidává úmysl pachatele způsobit jinému škodu či jinou újmu nebo získat pro sebe či jiného neoprávněný prospěch. K samotné škodě ani získání prospěchu však dojít nemusí. Postačí, že pachatel jednal v tomto úmyslu.[97] Pod písm. b) je poté stanoven úmysl pachatele neoprávněně omezit funkčnost počítačového systému, případně jiného technického zařízení na zpracování dat. Jedná se o zvláště přitěžující okolnost namířenou především proti hrozbě ze strany počítačových virů. Pachateli, který jedná alespoň v jednom z těchto úmyslů, lze uložit přísnější trest.

V odst. 4 a 5 ustanovení § 230 jsou poté vyjádřeny další okolnosti podmiňující použití vyšší trestní sazby.

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

Tato zcela nová skutková podstata (§ 231) byla do trestního zákoníku zařazena pod vlivem ustanovení čl. 6 Úmluvy. Základním předpokladem pro trestnost jednání uvedeného v tomto ustanovení je úmysl pachatele spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) nebo výše zmíněný trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1,2. K naplnění skutkové podstaty trestného činu dle § 231 trestního zákoníku poté dojde, jestliže osoba jednající v tomto úmyslu vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává jakýkoli prostředek, který lze využít k získání neoprávněného přístupu do počítačového systému nebo jeho části. Příkladný výčet takových prostředků je uveden v odst. 1 tohoto ustanovení pod písm. a) a b).

Ve své podstatě se jedná o přípravné jednání neboli o tzv. předčasně dokonaný trestný čin.[98] Již samotné obstarání zmíněného zločinného nástroje po splnění dalších zákonem stanovených podmínek lze postihovat jako samostatný trestný čin.[99]

Obsahem odst. 2 a 3 tohoto ustanovení jsou poté okolnosti podmiňující použití vyšší trestní sazby.

---

[97] ŠÁMAL, Pavel a kol. *Trestní zákoník II. §140 až 421 : Komentář*. 1. vydání. Praha: C.H. Beck, 2010, s. 2093-2094.
[98] Tamtéž, s. 2098.
[99] SOKOL, Tomáš, SMEJKAL, Vladimír. Postih počítačová kriminality podle nového trestního zákona. *Právní rádce* [online]. 22. července 2009 [cit. 11. ledna 2011]. Dostupné na <http://pravniradce.ihned.cz/c1-37865090-postih-pocitacove-kriminality-podle-noveho-trestniho-zakona>.

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

Výčet trestných činů přímo souvisejících s počítači uzavírá ustanovení § 232 trestního zákoníku, které nově postihuje i nedbalostní zásahy do vybavení počítače včetně dat v něm uložených. Tato úprava jde dokonce nad rámec závazků plynoucích z Úmluvy o počítačové kriminalitě.

Skutkovou podstatu tohoto trestného činu naplní ten, kdo z hrubé nedbalosti porušením povinnosti vyplývající ze zaměstnání, povolání, postavení nebo funkce, či povinnosti uložené podle zákona nebo smluvně převzaté, zasáhne alespoň jedním ze zákonem stanovených způsobů do dat či vybavení počítače, a tím způsobí na cizím majetku značnou škodu.[100] Hrubou nedbalost vymezuje trestní zákoník v § 16 odst. 2.

Okolností podmiňující použití vyšší trestní sazby dle odst. 2 tohoto ustanovení je způsobení škody velkého rozsahu.

5.3 Evropská úmluva o počítačové kriminalitě

Existuje celá řada mezinárodních smluv a dokumentů, které se zabývají problematikou počítačové kriminality. Její globální charakter a rychlost, s jakou se tato forma trestné činnosti vyvíjí, přiměla členské státy Rady Evropy vypracovat dokument, jehož hlavním účelem by bylo harmonizovat trestněprávní úpravu jednotlivých států a prohloubit jejich spolupráci v boji proti této formě kriminality. Veškerá snaha vyvrcholila přijetím již několikrát zmíněné Úmluvy o počítačové kriminalitě (angl. Convention on cybercrime).[101]

Práce na Úmluvě započaly již v roce 1997 po vytvoření Výboru expertů pro kriminalitu v počítačovém prostoru. Uplynulo přes čtyři roky, než došlo k jejímu konečnému schválení Výborem ministrů Rady Evropy. Přesto, že byla k podpisu otevřena v Budapešti již 23. listopadu 2001, vstoupila v platnost až o téměř tři roky později, konkrétně 1. července 2004. Česká republika se řadí mezi státy, které ji sice podepsaly, ale doposud neratifikovaly. Krátce nato byl přijat i Dodatkový protokol k Úmluvě o počítačové kriminalitě. V něm vyjádřený závazek ke kriminalizaci některých činů s rasovým a xenofobním obsahem byl zařazen do samostatného protokolu z již výše zmíněného důvodu (viz 4.3.6).

[100] Srov. § 232 odst. 1 zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.
[101] Convetion on Cybercrime, Budapešť, 23. listopadu 2001. Dostupné na <http://conventions.coe.int/treaty/en/treaties/html/185.htm>.

Úmluva čítá kromě preambule celkem 48 článků rozdělených do 4 následujících kapitol:[102]

I. Kapitola – Používání pojmů (čl. 1)
II. Kapitola – Opatření přijímaná na národní úrovni (čl. 2 - čl. 22)
III. Kapitola – Mezinárodní spolupráce (čl. 23 – čl. 35)
IV. Kapitola – Závěrečná ustanovení (čl. 36 – čl. 48)

Kapitola první vymezuje důležité pojmy jako „počítačový systém“, „počítačová data“, „poskytovatel služeb“ nebo „provozní data“, které se prolínají v celém textu Úmluvy.[103]

Kapitola druhá je poté rozdělena na část hmotněprávní a část procesněprávní. Součástí té hmotněprávní jsou protiprávní jednání, která by měla být dle národní právní úpravy trestnými činy. Jednotlivé trestné činy jsou rozděleny do 4 kategorií:[104]

1. Trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů
   - Protiprávní přístup (čl. 2)
   - Protiprávní zachycení informací (čl. 3)
   - Zásah do dat (čl. 4)
   - Zásah do systému (čl. 5)
   - Zneužití zařízení (čl. 6)
2. Trestné činy související s počítači
   - Falšování údajů související s počítači (čl. 7)
   - Podvod související s počítači (čl. 8)
3. Trestné činy související s obsahem
   - Trestné činy související s dětskou pornografií (čl. 9)
4. Trestné činy související s porušením autorského práva a práv příbuzných autorskému právu
   - Trestné činy související s porušením autorského práva a práv příbuzných autorskému právu (čl. 10)

Mnoho z těchto protiprávních jednání bylo zahrnuto do nového trestního zákoníku, a to především do trestných činů neoprávněného přístupu k počítačovému systému a nosiči informací (§ 230) a opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231).

[102] Viz GŘIVNA, Tomáš a kol. *Kyberkriminalita a právo*. Praha: Auditorium, 2008, s. 105.
[103] Blíže tamtéž, s. 105-107.
[104] Tamtéž, s. 168-172.

Procesněprávní část obsahuje kromě ustanovení o pravomoci a působnosti také souhrn opatření (čl. 16 – čl. 21), která by měla přispět k odhalení pachatelů těch trestných činů, k jejichž kriminalizaci zavazuje Úmluva, jiných trestných činů, které byly spáchány pomocí počítačového systému nebo pomoci při shromažďování důkazů o trestném činu v elektronické podobě.[105]

Kapitola třetí o mezinárodní spolupráci má spíše podpůrnou povahu k jiným bilaterálním či multilaterálním dohodám, týkajícím se spolupráce v trestních věcech. Přesto však obsahuje řadu vlastních požadavků ohledně vydávání osob, vzájemné pomoci nebo postupu při vyřizování žádostí o poskytnutí pomoci v případě neexistence jiné aplikovatelné mezinárodní smlouvy.[106]

Závěrečná kapitola poté shrnuje veškeré podmínky týkající se mimo jiné platnosti, přistoupení, uplatnění dodatků či vypovězení Úmluvy. Z jejího znění vyplývá, že k Úmluvě mohou přistoupit nejen členské státy Rady Evropy, ale i jiné státy, které se účastnily její přípravy.

[105] GŘIVNA, Tomáš a kol. *Kyberkriminalita a právo*. Praha: Auditorium, 2008, s. 123.
[106] Viz BAYEROVÁ, Monika. Evropská úmluva o počítačové kriminalitě a sexuální zneužívání dětí. *Trestněprávní revue,* 2003, roč. 2, č. 5, s. 156; blíže také GŘIVNA, Tomáš a kol. *Kyberkriminalita a právo*. Praha: Auditorium, 2008, s. 179-187.

6 Způsoby boje proti počítačové kriminalitě

6.1 Preventivní opatření

Obecně lze říci, že veškerá snaha o potlačení či zamezení jakékoli trestné činnosti stojí na dvou hlavních faktorech, a to prevenci a represi. Ani jedna z těchto složek by bez druhé nemohla být účinná. Na druhou stranu účinná preventivní opatření jsou často schopna předejít protiprávnímu jednání a tím se vyhnout následnému odstraňování vzniklých škod. Jinými slovy budou-li preventivní opatření úspěšná, nebude třeba přistoupit k represi ze strany státních orgánů.

V oblasti počítačové kriminality má prevence ještě větší význam, jelikož případy spojené s touto problematikou se velice těžko odhalují a i v případě úspěchu není jednoduché konkrétního pachatele vypátrat nebo mu jeho čin dokázat. Preventivní opatření můžeme rozlišovat z hlediska psychologického a technologického.[107] Prostřednictvím psychologické prevence lze formovat náhled osob na určitý problém. Jedním z hlavních, ne-li nejdůležitějších faktorů, je zde samotná výchova.[108] Na chování nás všech má nesporný vliv prostředí v jakém jsme vyrůstali a s jakými postoji a názory jsme se setkávali. I zde je možné hledat původ ve smýšlení mnoha lidí, kteří si stále neuvědomují nebo nejsou schopni připustit společenskou škodlivost některých činností spadajících do počítačové kriminality. Mluvíme především o trestné činnosti spojené s porušováním autorského práva či neoprávněným průnikem do systému. Hlavním úkolem psychologické prevence v oblasti počítačové kriminality je důsledně a vhodnou formou osvěty poučovat veřejnost o tom, v čem spočívá podstata ochrany před společensky nepřijatelnými projevy této formy trestné činnosti.

Technologická prevence je založena na zcela jiném principu jak předcházet protiprávnímu jednání na poli počítačové kriminality. Jedná se o taková opatření, která využívají technologické postupy a prvky s cílem zabránit páchání trestné činnosti. V praxi se jedná o vývoj různých ochranných prostředků (např. ochranné a bezpečnostní programy typu Firewall, DRM[109] apod.), které by případný pachatel nebyl schopen obejít. Ve skutečnosti jsou tyto prostředky v mnohých případech neúčelné, protože se vždy našel někdo, kdo je dokázal časem prolomit.

---

[107] MATĚJKA, Michal. *Počítačová kriminalita.* Praha: Computer Press, 2002, str. 77.
[108] MUSIL, Stanislav. *Počítačová kriminalita: Nástin problematiky. Kompendium názorů specialistů* [online]. Praha: Institut pro kriminologii a sociální prevenci, 2000 [cit. 12. ledna 2011]. Dostupné na <http://www.ok.cz/iksp/docs/256.pdf>.
[109] DRM (Digital Rights Management) jsou technické prostředky ochrany práv. Mohou být součástí samotného nosiče dat (CD,DVD apod.) s cílem zabránit neoprávněnému kopírování.

V neposlední řadě může mít z hlediska prevence v oblasti počítačové kriminality pozitivní vliv i právní úprava, která by účelně a efektivně postihovala všechna jednání, směřující proti právem chráněným zájmům a tím vyvolala v pachateli obavu, že jím spáchaný trestný čin bude odhalen a následně potrestán. Svou roli může sehrát i povědomí o existenci odborníků z řad orgánů činných v trestním řízení, speciálně vyškolených pro tento druh kriminality.

6.2 Represivní opatření

Druhou neodmyslitelnou složkou boje proti počítačové kriminalitě je represe, neboli následný postih za spáchaný trestný čin. Je nutné si uvědomit, že v oblasti trestního práva platí zásada subsidiarity trestní represe, podle které lze uplatnit stanovenou trestněprávní sankci až v případě, kdy ostatní právní či mimoprávní prostředky selžou.[110] Význam represivních opatření spočívá především v působení na společnost, ale i na samotného pachatele ve snaze zamezit páchání další trestné činnosti. Uložená trestněprávní sankce by měla být přiměřená vzhledem k povaze a závažnosti spáchaného trestného činu a poměrům pachatele.[111]

Samotnému postihu předchází fáze zaměřená na odhalení a vyšetření trestného činu, vypátrání a zajištění pachatele a důkladné právní posouzení celé věci. Tuto funkci plní orgány činné v trestním řízení, tedy policejní orgány, státní zastupitelství a soudy.

6.3 Odhalování a vyšetřování trestných činů souvisejících s počítači

Základním předpokladem pro řádné objasnění a vyšetření jakéhokoli trestného činu je jeho odhalení. Jinými slovy k tomu, aby orgány činné v trestním řízení mohly provést šetření, musí se o takovém činu vůbec dozvědět. Zde narážíme na jeden z velkých problémů při potírání počítačové kriminality. Ta se totiž vyznačuje vysokým stupněm latence. Fakt, že se poškozená osoba o takovém činu buď vůbec nedozví, nebo jej potažmo neohlásí, je pro odhalování jednotlivých případů této formy trestné činnosti zcela zásadní. To platí zejména pro velké společnosti, které v obavě o poškození své pověsti a ztrátu důvěryhodnosti ze strany klientů mnohdy takový čin vůbec neoznámí a celou záležitost řeší raději za zavřenými dveřmi.

[110] JELÍNEK, Jiří a kol. *Trestní právo hmotné.* 1. vydání. Praha: Leges, 2009, s. 28-29.
[111] Srov. § 38 odst. 1 zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

Veškeré podněty, které mohou přispět k odhalení trestných činů, spadajících do oblasti počítačové kriminality, musí být brány se vší vážností. O páchání trestné činnosti se kriminalisté mohou dozvědět z různých zdrojů. Potřebné informace jim mohou poskytnout samotní občané prostřednictvím ústního, telefonického nebo písemného oznámení.[112] Děje se tak nejen ze strany samotných poškozených, ale v praxi stále častěji ze strany subjektů, které se touto formou snaží zbavit své konkurence. Takový případ může nastat v situaci, kdy se tento subjekt (oznamovatel) například dozví, že konkurenční společnost používá nelegální software a vše ochotně nahlásí. Dalším podnětem pro zahájení činnosti orgánů činných v trestním řízení jsou anonymní trestní oznámení, která však mnohdy obsahují nepřesné či dokonce nepravdivé údaje, což práci na jejich prověřování velmi znesnadňuje. Jiným zdrojem je činnost investigativních novinářů a veřejné sdělovací prostředky, které mohou přinést nové poznatky v procesu odhalování jednotlivých forem počítačové kriminality. V neposlední řadě jsou to také výsledky operativně pátrací činnosti kriminální policie. Kriminalisté mohou při odhalování počítačové kriminality využít veškerých zákonných prostředků. Potřebné informace a údaje lze získat například monitorováním podezřelých inzerátů a obsahu webových stránek, využíváním informátorů apod. Takto nashromážděný materiál se dále prověřuje za účelem posouzení, zda se jedná o protiprávní jednání naplňující znaky trestného činu. Nejvyšší informační hodnotu mají právě podněty získané samotnou činností pracovníků kriminální policie.[113] Pachatelé využívající počítačovou techniku pro páchání trestné činnosti jsou ve většině případů velmi zběhlí a dokáží po sobě „zamést“ všechny stopy, které by je mohly usvědčit. Z toho vyplývá, že nejen pro vyšetřování, ale i pro odhalování této trestné činnosti je zapotřebí kvalifikovaných odborníků, kteří jsou za pomoci moderních technologií a metod schopni pachatele odhalit a vypátrat.

Vědní obor, který se zabývá vyšetřováním trestných činů se nazývá kriminalistika. Ta se snaží na základě dlouhodobého a všestranného zkoumání trestných činů, pachatelů, způsobů jejich spáchání (modus operandi) i prostředí v jakém jsou páchány vytvořit efektivní a účelné metody a postupy, které by napomohly při vyšetřování.[114] Tyto poznatky lze aplikovat i na oblast počítačové kriminality, čímž vznikají specifické postupy a metody, které mohou kriminalistům značně ulehčit a urychlit jejich práci.

Při vyšetřování případů počítačové kriminality se musí postupovat precizně, obezřetně, ale zároveň co nejrychleji. Již na samém počátku je nutné stanovit tzv. vyšetřovací

[112] PORADA, Viktor, KONRÁD, Zdeněk. *Metodika vyšetřování počítačové kriminality*. 1. vydání. Praha: Vydavatelství PA ČR, 1998. s. 24.
[113] Tamtéž, s. 23.
[114] GŘIVNA, Tomáš a kol. *Kyberkriminalita a právo*. Praha: Auditorium, 2008, s. 86.

rámec, který rozdělí práci vyšetřovatelů do jednotlivých etap. Počítačová kriminalita zahrnuje různorodou trestnou činnost, proto nelze vytvořit takový plán, který by se aplikoval na všechny její formy. Přesto lze říci, že v prvotní fázi se vyšetřovatelé zaměřují na shromažďování a vyhodnocování veškerých dostupných informací o případné trestné činnosti. Až na základě zjištěných poznatků dojde ke stanovení dalšího postupu a případnému rozšíření okruhu vyšetřovatelů. Případy počítačové kriminality se často vyznačují svou rozsáhlostí a složitostí, a proto je nutné přibrat odborníky či vytvořit tým specialistů, kteří budou mít případ na starosti. Důležitým předpokladem pro správné fungování takového týmu je propracovaná organizace práce a kvalifikovaný vedoucí, který by rozděloval jednotlivé úkoly a zajišťoval dohled nad jejich řádným plněním.[115]

Nasvědčují-li získané a prověřené informace, že skutečně došlo ke spáchání trestného činu, je zapotřebí pachatele vypátrat a zajistit veškeré důkazy, které by ho usvědčily. Nevyplívá-li z dosavadních informací kdo se takového činu dopustil, je nutné vymezit okruh potenciálních pachatelů. K tomu je nutné stanovit možné motivy pachatele (pachatelů) a určit, která osoba by mohla mít z daného jednání prospěch. Totožnost pachatele lze mnohdy vyčíst již ze samotného způsobu spáchání trestného činu.[116]

K vypátrání pachatele a zajištění potřebných důkazů pro další fáze trestního řízení lze využít veškerých dostupných prostředků, které zákon připouští. Obsahové a formální náležitosti jednotlivých procesních úkonů, které mají orgány činné v trestním řízení k dispozici, jsou stanoveny zákonem.[117] V souvislosti s vyšetřováním případů počítačové kriminality se nejčastěji využívá domovní prohlídky, prohlídky jiných prostor a pozemků, prostředků k zajištění věci (vydání věci, popř. odnětí věci), odposlechu a záznamu telekomunikačního provozu, včetně výslechu samotného podezřelého či případných svědků.

Za důkazní prostředek lze dle trestního řádu považovat vše, co může přispět k objasnění věci a posloužit jako podklad pro rozhodnutí. Při vyšetřování trestných činů spadajících do počítačové kriminality dochází především k zajištění samotného počítače včetně jeho obsahu, veškerých potřebných nosičů dat (CD, DVD, externí hard disk apod.) a jiných věcí, které by vyšetřovatelům posloužily jako zdroj potřebných informací či důkazů. Jelikož se počítač a ostatní potřebné materiály nachází většinou v domácnosti nebo na pracovišti, využívá se k zajištění těchto věcí domovní prohlídky, respektive prohlídky jiných prostor a pozemků. Obě uvedené prohlídky lze vykonat pouze tehdy, je-li důvodné podezření,

[115] GŘIVNA, Tomáš a kol. *Kyberkriminalita a právo*. Praha: Auditorium, 2008, s. 88.
[116] PORADA, Viktor, KONRÁD, Zdeněk. *Metodika vyšetřování počítačové kriminality*. 1. vydání. Praha: Vydavatelství PA ČR, 1998. s. 16.
[117] Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů.

že se v těchto prostorách nachází věc či osoba důležitá pro trestní řízení.[118] Listina základních práv a svobod stanoví přípustnost domovní prohlídky pouze pro účely trestního řízení, a to na písemný odůvodněný příkaz soudce.[119] Rozlišení mezi domovní prohlídkou a prohlídkou jiných prostor a pozemků má z hlediska procesních náležitostí zcela zásadní význam. Domovní prohlídku nařizuje v přípravném řízení na návrh státního zástupce soudce a v řízení před soudem předseda senátu. Na příkaz soudce nebo předsedy senátu ji poté vykoná policejní orgán. Prohlídku jiných prostor (tzn. kanceláří, skladů či jiných prostor nesloužících k bydlení) nebo pozemků je oprávněn nařídit předseda senátu a v přípravném řízení též státní zástupce nebo policejní orgán. Policejní orgán může nařídit prohlídku jiných prostor nebo pozemků pouze se souhlasem státního zástupce. V situaci, kdy věc nesnese odkladu a zároveň zmíněného souhlasu nebo nařízení nelze předem dosáhnout, či v případě, kdy k tomu dá oprávněná osoba písemný souhlas, má policejní orgán právo prohlídku vykonat i bez takového souhlasu či nařízení.

Samotné prohlídce by měla předcházet důkladná příprava, zvlášť za předpokladu, že se na daném místě bude nacházet počítačová technika. Důležité je eliminovat hrozbu znehodnocení či ztráty dat uložených nejen na pevném disku počítače, ale i na jiných nosičích dat. Aby nemohlo dojít k následné manipulaci s počítačem a ke ztrátě důkazního materiálu, je nutné zajistit všechny osoby, které se nacházejí na místě prohlídky a „odstřihnout“ počítač od lokální či vzdálené sítě umožňující vzdálený přístup.[120]

K ohledání místa, na kterém se nachází počítačová technika, je nutné přizvat počítačového odborníka nebo soudního znalce a tím tak předejít zbytečnému znehodnocení cenných důkazů. Vyšetřovací tým by měl mít k dispozici takové technologické prostředky, které by umožnily získat co největší množství důkazního materiálu. Veškerá data, která by mohla souviset s trestnou činností je potřeba náležitým způsobem zazálohovat a zadokumentovat. V souladu s trestním řádem je osoba povinna v přípravném řízení na výzvu policejního orgánu nebo státního zástupce vydat věc, kterou je nutné pro účely trestního řízení zajistit. Takovými věcmi mohou být nejen počítače a různé druhy nosičů dat, tiskárny, ale i listiny a písemnosti. Nebude-li požadovaná věc dobrovolně vydána, může dojít za zákonem stanovených podmínek k jejímu odnětí. V mnohých případech je zapotřebí zajištěné důkazní

[118] Srov. § 82 odst.1,2 zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů.
[119] Viz. čl. 12 Listiny základních práv a svobod.
[120] SMEJKAL, Vladimír, SOKOL, Tomáš, VLČEK, Martin. *Počítačové právo*. Praha: C.H.Beck, 1995, s. 147-148.

prostředky převést na speciální pracoviště k provedení důkladné kriminalistické expertizy.[121] V České republice se analýzou datového obsahu počítačů a datových médií zabývá obor kriminalistické počítačové expertizy v Kriminalistickém ústavu Praha.[122] Tato expertiza se zaměřuje na zkoumání technických, ale i programových prostředků výpočetní techniky, včetně jejího obsahu.[123] O jednotlivých úkonech, včetně o tom, které věci byly vydány nebo odňaty je nutné sepsat protokol.

Další prostředek, který může výrazně přispět k objasnění případů počítačové kriminality je odposlech a záznam telekomunikačního provozu. Tento institut lze využít pouze tehdy, je-li vedeno trestní řízení pro zvlášť závažný zločin nebo pro jiný úmyslný trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva.[124] Jelikož se jedná o značný zásah do soukromí osob, může takový odposlech nebo záznam telekomunikačního provozu nařídit pouze předseda senátu a v přípravném řízení soudce na návrh státního zástupce. Příkaz musí být písemný a řádně odůvodněn. Prostřednictvím tohoto prostředku lze získat cenné informace z telefonních hovorů, z výpisů o uskutečněném telekomunikačním provozu, jakož i z prostředků elektronické komunikace (e-mailů apod.). Aby mohly být výsledky této činnosti použity jako důkaz v trestním řízení, je nutné vše důkladně zaprotokolovat.

Důležité informace pro vyšetřování může poskytnout také výslech svědků i samotného podezřelého. Při výslechu je nutné dbát zákonných ustanovení a vyslýchanou osobu řádně poučit. Vyšetřování trestných činů, spadajících do počítačové kriminality, je někdy velmi komplikované a vyžaduje znalosti v daném oboru. Z toho důvodu je zapotřebí se na výslech předem připravit a zajistit přítomnost osoby, která se v této problematice vyzná.[125]

Vytyčený plán, postup a metody vyšetřování se samozřejmě mění v závislosti na tom, o jakou formu počítačové kriminality se v konkrétním případě jedná. Vždy je však základem trestný čin odhalit, vypátrat pachatele a zajistit takové množství důkazů, na jejichž základě by byl pachatel odsouzen a náležitě potrestán. Orgány činné v trestním řízení musí při provádění procesních úkonů a zajišťování důkazů postupovat vždy v souladu se zákonem. Důkazy získané nezákonným způsobem by nemusely být v případném soudním řízení připuštěny.

---

[121] GŘIVNA, Tomáš a kol. *Kyberkriminalita a právo*. Praha: Auditorium, 2008, s. 94.
[122] Blíže viz webové stránky Policie ČR. Dostupné na <http://www.policie.cz/clanek/celorepublikove-utvary-kriminalisticky-ustav-praha-zpravodajstvi-test-4.aspx?q=Y2hudW09Mw%3d%3d>.
[123] LÁTAL, Ivo. Počítačová (informační) kriminalita a úloha policisty při jejím řešení. *Policista* [online]. 1998 [cit. 15. ledna 2011]. Dostupné na <http://aplikace.mvcr.cz/archiv2008/casopisy/policista/prilohy/pc_krimi.html>.
[124] Viz ustanovení § 88 odst. 1 zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů.
[125] GŘIVNA, Tomáš a kol. *Kyberkriminalita a právo*. Praha: Auditorium, 2008, s. 96.

7 Předpoklady budoucího vývoje počítačové kriminality

Ačkoli lze budoucí vývoj v oblasti počítačové kriminality pouze odhadovat, je téměř jisté, že informační technologie a možnosti jejich využití se budou nadále rozšiřovat. Historie počítačové kriminality ukázala, že lze očekávat nástup nových forem této trestné činnosti, na které bude muset společnost adekvátně reagovat. Nadále bude platit, že pachatel, který disponuje potřebnými prostředky (zejména finančními a technickými), bude mít před represivními orgány vždy navrch. Řešení spočívá v již zmíněné prevenci, ve využití nejmodernějších technologií při vyšetřování a v efektivní a účelné právní úpravě.

Jedním z nejdiskutovanějších témat poslední doby, a zdá se že i blízké budoucnosti, je a bude otázka počítačového pirátství. Nelegální pořizování a šíření pirátských kopií software, hudebních a filmových nahrávek se natolik rozmohlo, že se stalo doslova masovou záležitostí. Mění se celkový pohled společnosti na autorskoprávní ochranu a stejně tak dochází k velkému posunu v náhledu na to, co je a co není v této oblasti společensky přijatelné. Lidé již delší dobu odmítají platit „přemrštěné“ ceny za tato díla a stále častěji se uchylují k jejich získání nelegální cestou. Bude zajímavé sledovat, zda se změní obchodní politika ochránců a držitelů práv k těmto dílům a dojde ke snížení koncových cen nebo zda setrvají na svém postoji a budou dál urputně prosazovat zpřísnění postihu za porušení autorského práva.

V budoucnu bude nutné vyřešit i otázku teritoriality práva. Problematická je především oblast internetu, která žádné hranice nezná a kde doposud neexistuje právní úprava, která by řešila spory vzniklé z nesouladu právních řádů jednotlivých státu. Na základě širokého konsensu subjektů mezinárodního práva by mělo dojít k přijetí takové úpravy, která by tyto hraniční situace vyřešila.

Mnoho publikací zabývajících se počítačovou kriminalitou přináší z hlediska jejího možného vývoje představu o zneužití informačních technologií ze strany organizovaných zločineckých skupin. Zatím je pouhou otázkou nakolik se tak již stalo, ale faktem je, že zmiňovaný kyberprostor může představovat ideální prostředí pro organizovanou trestnou činnost. Prostřednictvím počítačových systémů a sítí mohou členové těchto skupin zastírat svou pravou identitu, zrychlit a zefektivnit svoji činnost a ušetřit tak nemalé prostředky. To vše může do budoucna přispět k nárůstu počtu případů počítačové kriminality, za kterými budou stát tyto zločinecké skupiny.

Vývoj počítačové kriminality bude z velké části záležet i na přístupu orgánů činných v trestním řízení. Ty by měly postupovat rychle, rozhodně a mít k dispozici veškeré zákonné i technologické prostředky, které by vedly k dopadení a potrestání pachatele.

7.1 Kyberterorismus

Již výše byl kyberterorismus zmíněn jako jedna z největších hrozeb pro budoucí vývoj počítačové kriminality. Obecně lze terorismus vymezit jako *„protizákonné použití síly a násilí proti osobám či majetku s cílem zastrašit nebo donutit vládu, civilní obyvatelstvo nebo jeho část a tím dosáhnout svých politických nebo společenských cílů.“*[126] Pokud ke spáchání teroristického útoku bude využito výpočetní a telekomunikační techniky, lze mluvit o kyberterorismu. Vzhledem k tomu, že se mnohé oblasti lidské činnosti staly na informačních technologiích doslova závislé, nelze vyloučit ani zneužití těchto technologií ze strany teroristů. Takový útok by mohl vzhledem k povaze informačních sítí zasáhnout řadu míst po celém světě, a to během relativně krátké doby. Kybernetický útok umožňuje dosáhnout stanoveného cíle bez použití zbraní či sebevražedných misí. Rozsah následků takového činu může být však daleko větší. V blízké budoucnosti se může jednat o zcela reálnou hrozbu, a to i přesto, že lze jen odhadovat, jakými prostředky jednotlivé teroristické skupiny v současné době disponují. Společnost by měla být na toto nebezpečí připravena a měla by učinit veškerá možná opatření, která by toto riziko snížila na minimum.

[126] Code of Federal Regulations (28CFR0.85) [online]. [cit. dne 17. ledna 2011]. Dostupné na <http://www.gpoaccess.gov/cfr/retrieve.html>.

Závěr

Již od 90. let minulého století je počítačová kriminalita považována za jednu z nejnebezpečnějších forem kriminality vůbec. Toto téma je pravidelně otevíráno a diskutováno téměř na všech mezinárodních konferencích, zaměřených na prevenci a vývoj kriminality ve světě. Nutno podotknout, že představuje minimálně stejnou hrozbu pro společnost, jako kriminalita násilná, organizovaná, drogová apod. Její vývoj je z velké části závislý na rozvoji a dostupnosti informačních, popřípadě telekomunikačních technologií. Dalo by se říci, že právě rychlost, s jakou jsou tyto technologie uváděny do běžného života, má zásadní vliv na podobu a rozsah jednotlivých forem počítačové kriminality.

Cílem této diplomové práce bylo podat relativně ucelený pohled na vybrané trestněprávní a kriminologické aspekty počítačové kriminality. Jelikož se jedná o oblast značně rozsáhlou, pozornost byla věnována z mého pohledu těm nejvíce signifikantním otázkám a projevům tohoto druhu kriminality. Z uvedeného historického vývoje je patrné, že během relativně krátké doby a v závislosti na prudkém rozvoji nových technologií se objevily zcela nové formy této trestné činnosti. Dle mého názoru počítačová kriminalita již není výsadou úzké skupiny odborníků či tzv. „insiderů“, ale okruh potenciálních pachatelů se značně rozšířil. Důvod vidím ve zvyšující se dostupnosti počítačové techniky pro širokou veřejnost, jakož i ve vzrůstajících znalostech a schopnostech jejího využití.

Ve své práci mimo jiné uvádím nejčastější projevy trestné činnosti, páchané v souvislosti s informačními technologiemi a zabývám se jejich trestněprávním postihem. Hlavním účelem trestního práva je ochrana společenských a individuálních zájmů či hodnot před nejzávažnějšími případy protiprávního jednání ze strany fyzických osob. Právní úprava v oblasti trestního práva by měla pružně reagovat na nové formy trestné činnosti, tedy včetně nových forem počítačové kriminality. Z tohoto pohledu považuji zmiňované přijetí nového trestního zákoníku za zcela pozitivní a žádoucí. V souladu s Evropskou úmluvou o počítačové kriminalitě v něm došlo k zařazení nových skutkových podstat týkajících se počítačových deliktů. Nově lze bez dalšího (bezpodmínečně) postihovat jednání spočívající v neoprávněném získání přístupu k počítačovému systému. Ačkoli jsem zaznamenal názory, které považují toto ustanovení za nadbytečné či neopodstatněné, dle mého názoru tomu tak není. Neoprávněný průnik do počítačového systému podle mě představuje podstatný zásah do soukromí osob, ať už je úmysl pachatele jakýkoli. Dalším výrazným a veskrze kladným počinem v boji proti počítačovým deliktům je zakotvení skutkové podstaty, na základě které

lze postihovat jednání spočívající v zásahu do technického vybavení počítače či jeho obsahu z hrubé nedbalosti. Lze konstatovat, že stávající trestněprávní ustanovení týkající se počítačové kriminality jsou do značné míry obsáhlejší, přesněji definované a lépe odráží současnou situaci v této oblasti. To, zda bude mít nová právní úprava pozitivní dopad i v praxi, budeme moci hodnotit až s určitým časovým odstupem.

Efektivní právní úprava je pouze jedním z předpokladů úspěšného boje s počítačovou kriminalitou. Neméně důležitý je přístup orgánů činných v trestním řízení k odhalování a vyšetřování jednotlivých případů. K tomu je zapotřebí vyškolených a kvalifikovaných odborníků, kteří mají k dispozici právní a technologické prostředky, umožňující pachatele takového činu vypátrat a postihnout.

Jedno je jisté, a to že počítačová kriminalita se nevytratí, zvlášť ne ze společnosti na informačních technologiích doslova závislé. Dá se ale předpokládat, že s dalším rozvojem těchto technologií se časem změní i způsob páchání (modus operandi) jednotlivých forem této trestné činnosti, či se objeví formy zcela nové. Domnívám se, že pouze účelná preventivní opatření a neustálé sledování a vyhodnocování nových trendů na poli počítačové kriminality mohou výrazně přispět k předcházení této trestné činnosti.

Shrnutí

V dnešní době je počítačová kriminalita považována za jednu z nejrychleji se rozvíjejících forem kriminality vůbec. Cílem této práce bylo vymezit a poukázat na některé hlavní trestněprávní a kriminologické aspekty související s touto formou trestné činnosti.

Úvodní kapitola se týká samotného pojmu počítačové kriminality. Její pojmové a obsahové vymezení a stejně tak uvedení odlišných pojetí je velice důležité pro pochopení dané problematiky.

Následující kapitola je rozdělena do dvou podkapitol, které pojednávají o příčinách vzniku a historickém vývoji tohoto fenoménu dnešní doby, kterým počítačová kriminalita bezesporu je. Vynález počítače a jeho následné rozšíření do všech oblastí lidského života měly za následek postupné utváření této formy trestné činnosti. Pro přehlednost a lepší pochopení je historický vývoj rozdělen do tří základních časových etap.

Třetí kapitola je věnována subjektům počítačové kriminality. Je zaměřena především na pachatele a jejich nejčastější motivy, na osoby poškozené, respektive oběti.

Kapitola čtvrtá je z hlediska obsahu nejrozsáhlejší. Uvádí základní dělení počítačové kriminality z hlediska postavení počítače a jeho využití při páchání trestné činnosti. Dále podává přehled nejčastějších forem této trestné činnosti, objasňuje jejich význam a zabývá se otázkou jejich případného postihu dle platné právní úpravy.

Další samostatná kapitola této práce se zabývá právní úpravou v oblasti počítačové kriminality. První část této kapitoly se věnuje vývoji trestněprávní úpravy v této oblasti se zaměřením na vybrané skutkové podstaty trestných činů a jejich změny. Následující podkapitola je zaměřena na rozbor tzv. „počítačových trestných činů“, které se staly součástí nového trestního zákoníku. Kapitolu uzavírá část věnovaná Evropské úmluvě o počítačové kriminalitě, která je v práci mnohokrát zmíněna.

Následující šestá kapitola se týká jednotlivých způsobů boje s počítačovou kriminalitou. Jako dvě hlavní složky tohoto boje uvádí prevenci a represi. Důraz je však kladen především na proces odhalování a vyšetřování této formy trestné činnosti.

Závěrečná kapitola je zaměřena na možný budoucí vývoj počítačové kriminality. Obsahuje nejen prognózy, ale i nástin problematických otázek, které bude nutné v dohledné době řešit. Poslední část se dotýká velké budoucí hrozby, spočívající ve zneužití informačních technologií ze strany teroristů.

Summary

Nowadays, cybercrime is considered to be one of the most developing forms of criminality whatsoever. The goal of this work is to define and outline certain criminal law and criminology aspects connected with this form of criminal activity.

Initiating chapter is concerned with the very term of cybercrime. Its conceptual and material definition as well as introduction of different concepts is very important for understanding of this issue.

Following chapter is divided into two subchapters which describe the origination and historical evolution of this phenomenon up to current days where it undoubtedly exists. Invention of a computer and its subsequent expansion into all areas of human life caused gradual creation of this form of criminal activity. Historical development is divided into three time periods in order to be well-arranged and better understood.

Third chapter is dedicated to subjects of cybercrime. It is focused mainly at offenders and their most frequent motives, injured persons and victims.

From its content point of view, the fourth chapter is the largest one. It analyzes basic division of cybercrime in relation to the position of a computer and its use in committing the crime. It further givers overview of the most frequent forms of this criminal activity, clarifies their meaning and discusses the question of their respective sanction under the legal regulation in force.

Another separate chapter is concerned with legal regulation in the area of cybercrime. The first part of this chapter is dedicated to the development of criminal law regulation in this area with focus on selected bodies of crimes and their changes. Next subchapter is aimed the analysis of so-called “computer crimes” which became a part of the new penal code. Chapter is concluded with a passage dedicated to European Convention on Cybercrime which is mentioned in the work numerously.

The sixth chapter is connected to individual means of fight against cybercrime. As two main elements of this fight, it states prevention and repression. Emphasis is given primarily on the procedure of discovery and investigation of this form o crime.

Final chapter is concerned with possible future evolution of cybercrime. It includes not only prognoses but also outline of problematic issues which will have to be resolved in near future. Last part of the work is linked to the big future threat consisting in abuse of information technologies by terrorists.

Seznam použitých zdrojů

Knižní publikace:

GŘIVNA, Tomáš a kol. *Kyberkriminalita a právo*. Praha: Auditorium, 2008. 220 s. ISBN 978-80-903786-7-4.

JELÍNEK, Jiří a kol. *Trestní právo hmotné.* 1. vydání. Praha: Leges, 2009. 895 s. ISBN 978-80-87212-24-0.

JELÍNEK, Jiří a kol. *Trestní zákon a trestní řád s poznámkami a judikaturou a předpisy souvisící.* 25. aktualizované vydání. Praha: Linde Praha, 2007. 1086 s. ISBN 978-80-7201-675-4.

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.

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

POLČÁK, Radim, ŠKOP, Martin, MACEK, Jakub. *Normativní systémy v kyberprostoru (úvod do studia).* Brno: Masarykova univerzita, 2005. 102 s. ISBN 80-210-3779-2.

PORADA, Viktor, KONRÁD, Zdeněk. *Metodika vyšetřování počítačové kriminality*. 1. vydání. Praha: Vydavatelství PA ČR, 1998. 55 s. ISBN 80-85981-75-0.

SMEJKAL, Vladimír. *Internet a §§§*. 2.aktualizované a rozšířené vydání. Praha: Grada Publishing, spol. s r.o., 2001. 284 s. ISBN 80-247-0058-1.

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

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

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.

Odborné časopisy:

BAYEROVÁ, Monika. Evropská úmluva o počítačové kriminalitě a sexuální zneužívání dětí. *Trestněprávní revue,* 2003, roč. 2, č. 5, s. 156 – 157.

SMEJKAL, Vladimír. Kriminalita v prostředí informačních systémů a rekodifikace trestního zákoníku. *Trestněprávní revue*, 2003, roč. 2, č. 6, s. 161 – 167.

Internetové zdroje:

Code of Federal Regulations (28CFR0.85) [online]. [cit. dne 17. ledna 2011]. Dostupné na <http://www.gpoaccess.gov/cfr/retrieve.html>.

Cyber Crime and Information Warfare: A 30-Year History, Citibank 1994 [online]. [cit. 16. prosince 2010]. Dostupné na <http://images.businessweek.com/ss/10/10/1014_cyber_attacks/5.htm>.

ČÍRTKOVÁ, Ludmila. Psychologické poznatky k nebezpečnosti pronásledování (stalking). *Kriminalistika* [online]. 2004 [cit. 4. ledna 2011]. Dostupné na <http://aplikace.mvcr.cz/archiv2008/casopisy/kriminalistika/2004/0404/cirtkova_info.html>.

DASTYCH, Jiří. Počítačová kriminalita. *Hlásí se policie* [online]. 1998 [cit. 12. prosince 2010]. Dostupné na <http://www.dolphin.cz/policie/brezen98/pocitace.html>.

Hoax.cz [online]. *Co je to hoax.*[cit. 21. prosince 2010]. Dostupné na <http://www.hoax.cz/hoax/co-je-to-hoax>.

KABAY, M.E. *A Brief History of Computer Crime: An Introduction for Students* [online]. [cit. 15. prosince 2010]. Dostupné na <http://www.mekabay.com/overviews/history.pdf>.

KOHOUTEK, Rudolf. *Pojem kriminogenní faktory* [online]. ABZ.cz [cit. 14. prosince 2010]. Dostupné na <http://slovnik-cizich-slov.abz.cz/web.php/slovo/kriminogenni-faktory>.

KULHAVÝ, Petr. *Kevin Mitnick – slavný podvodník nebo obávaný hacker?* [online]. Root.cz, 26. září 2003 [cit. 15. prosince 2010]. Dostupné na <http://www.root.cz/clanky/kevin-mitnick-podvodnik-hacker/>.

LÁTAL, Ivo. Počítačová (informační) kriminalita a úloha policisty při jejím řešení. *Policista* [online]. 1998 [cit. 15. ledna 2011]. Dostupné na <http://aplikace.mvcr.cz/archiv2008/casopisy/policista/prilohy/pc_krimi.html>.

MUSIL, Stanislav. *Počítačová kriminalita: Nástin problematiky. Kompendium názorů specialistů* [online]. Praha: Institut pro kriminologii a sociální prevenci, 2000 [cit. 18. prosince 2010]. Dostupné na <http://www.ok.cz/iksp/docs/256.pdf>.

SOKOL, Tomáš, SMEJKAL, Vladimír. Postih počítačová kriminality podle nového trestního zákona. *Právní rádce* [online]. 22. července 2009 [cit. 11. ledna 2011]. Dostupné na <http://pravniradce.ihned.cz/c1-37865090-postih-pocitacove-kriminality-podle-noveho-trestniho-zakona>.

STERLING, Bruce. *Zátah na hackery (Hackers Crackdown)* [online]. 1992 [cit. 15. prosince 2010]. Přeložil Bárta Václav. Dostupné na <http://martin.hinner.info/crackdown/hacker_crackdown.pdf>.

SÝKORA, Martin. *Technické prostředky ochrany autorských práv* [online]. 31. ledna 2010 [cit. dne 29. prosince 2010]. Dostupné na <http://www.pravoit.cz/article/technicke-prostredky-ochrany-autorskych-prav>.

Vintage IBM 5150 [online]. Dostupné na <http://www.ibm5150.net/history.html>.

VŠETEČKA, Roman. *Viry jsou staré několik desetiletí. Chcete znát jejich vývoj?* [online]. iDNES.cz, 4. listopadu 2004 [cit. 16. prosince 2010]. Dostupné na <http://technet.idnes.cz/tec_technika.asp?r=bezpecnost&c=A041103_5285981_bezpecnost>.

WEIK, Martin H. *The ENIAC Story* [online]. [cit. 15.prosince 2010]. Dostupné na <http://www.martinhweik.com/eniac_story.html>.

http://conventions.coe.int/treaty/en/treaties/html/185.htm

http://www.uncjin.org/Documents/EighthCongress.html

Právní předpisy:

Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod, ve znění ústavního zákona č. 162/1998 Sb.

Zákon č. 209/1997 Sb., o poskytnutí peněžité pomoci obětem trestné činnosti a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.

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

Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů.

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