ABSTRAKT

V mé rigorózní práci jsem se pokusil o přiblížení problematiky obecně spojené s informacemi, jako nejcennějšími statky dnešní doby. Informační společnost, jejíž jsme součástí, je těmito informacemi obklopena a k nakládání s nimi si osvojila určité mechanismy, postupy a technologie. Mou snahou bylo osvětlit používání informačně komunikačních technologií a rizika s tím spojená.

Můžeme říci, že dnešní vyspělá civilizace je takřka dokonale vzájemně provázaná a propojená. To je dáno zejména rostoucí dostupností počítačů a jiných komunikačních prostředků, dalším důvodem pak je stále se zvyšující technologická sofistikovanost jejich propojení. Primární roli zde hraje Internet, síť sítí, nabízející stále rychlejší, levnější a variabilnější propojení jeho jednotlivých článků. To umožňuje získávání a poskytování informací bez teritoriálního, obsahového, množstevního omezení. Technologický pokrok, který informační oblast zažívá, je nebývale dynamický a dá se říci i nekontrolovatelný. Výhody tohoto pokroku jdou ruku v ruce s nevýhodami a to konkrétně se zneužíváním počítačů a Internetu kriminalitou. Nabízí se tedy otázka, zda poměr mezi přínosem informačně komunikačních technologií a jejich zneužíváním nezůstává stejný a nemění se pouze jejich kvantitativní rozsah. Odpověď bohužel nebude možné nalézt, neboť prostředí Internetu, počítačů a informací obecně se každým okamžikem mění a lze jen těžko odhadnout, jakým směrem se ubírá.

Pro psaní této práce jsem považoval za nejdůležitější přistoupit k tématu z pohledu laického čtenáře a v první řadě osvětlit základní pojmy, které se tématu týkají. To bylo základním kamenem pro podrobnější zkoumání tématu. Dalším krokem bylo specifikovat počítačovou a Internetovou kriminalitu a vystihnout její zvláštnosti a to zejména s ohledem na místo jejího působiště, kyberprostor, a také na subjekty v ní zapojené. Boj proti kriminalitě musí být veden na mnoha úrovních, z kterých nejdůležitější pro nás bude dostatečně efektivní legislativní spolupráce na mezinárodní úrovni a to zejména z důvodu jejího přeshraničního působení. Podrobněji jsem se zabýval novým trestním zákoníkem, který komplexněji upravuje skutkové podstaty trestných činů, pod které lze subsumovat protizákonná jednání spojená s počítači a Internetem. Tato specifická jednání a způsoby jejich provádění jsem popsal v další kapitole s důrazem kladeným na nejtypičtější z nich, hacking. Podstatnou část mé práce jsem pak věnoval právu doménových jmen možnosti postihu jejich nezákonné registrace a užívání trestním právem.

Při úvahách o počítačové a Internetové kriminalitě je nutno uvědomit si skutečnost, že ji nelze kompletně vymítit. Jediným způsobem boje tedy bude zavedení co nejúčinnějších opatření minimalizace rizik. Těmi se zabývá tzv. počítačová bezpečnost, která klade důraz na ochranu před neoprávněnou manipulací s počítačovými systémy, daty, bezpečnou komunikaci a přenos dat a další bezpečnostní aspekty. Nad rámec legislativních opatření to znamená pečlivě uschovávat a zabezpečovat záznamová media jako kompaktní disky, USB paměti, přenosné harddisky. Druhou stranou mince je pak softwarová ochrana počítačových systémů. Ta je prováděna softwarovou ochranou počítačových systémů. V úvahu přicházejí antivirové programy, antispyware, firewally, šifrování dat, programy blokující nevhodné internetové stránky. Když uvážíme komplikovanost a technickou složitost informačních technologií, nezbytným prvkem potírání kriminality bude vzdělávání a osvěta. Dle mého názoru nejtěžším úkolem však bude vymýtit onu deziluzi menší nebezpečnosti, či škodlivosti kybernetických trestných činů, danou pravděpodobně nemateriálním charakterem jejich páchání a také nenásilným způsobem páchání. Domnívám se též, že počítačová a Internetová kriminalita se těší nedostatečné publicitě, která by jistě zvýšila povědomí o jejích mnohdy astronomických finančních dopadech.

Navzdory všem opatřením je nutno si uvědomit, že veškerá technologie byla vytvořena lidmi a doposud nebyl vynalezen bezpečnostní prvek, který by nebylo možné nějakým způsobem obejít. Ať již tedy budeme aplikovat jakákoliv bezpečnostní, legislativní, osvětová a vzdělávací opatření, je nutno si uvědomit, že základním elementem pokroku a zároveň zneužívání všech výdobytků moderní informační společnosti je fyzická osoba sama. Zde bude tedy zapotřebí začít a uvědomit si nebezpečí a možné dopady zdánlivě neškodné činnosti, jako je práce s počítačem.