Univerzita Karlova v Praze
Právnická fakulta
Katedra trestního práva

Počítačová a internetová kriminalita

Diplomová práce

Daniel Zeman

Vedoucí diplomové práce: doc. JUDr. Tomáš Gřivna, Ph.D.
Datum vypracování práce (uzavření rukopisu): 11. 5. 2011

„Prohlašuji, že jsem předkládanou diplomovou práci vypracoval/a samostatně, všechny použité prameny a literatura byly řádně citovány a práce nebyla využita k získání jiného nebo stejného titulu.“

V Praze dne 11. 5. 2011 Podpis

Rád bych poděkoval vedoucímu své diplomové práce doc. JUDr. Tomáši Gřivnovi, Ph.D. za jeho cenné rady, připomínky, čas, studijní materiály a také za ochotu a vstřícnost při tvorbě této práce.

Obsah

Úvod

Téma mé práce s názvem „Počítačová a internetová kriminalita“ jsem si vybral především z důvodu jeho aktuálnosti, ale také zkušeností, které v oboru mám. Informační a komunikační technologie jsou neoddělitelnou součástí našeho života v moderní společnosti a spolu s výhodami technologického pokroku se dostává do popředí také problematika s tím související. K jejímu zpracování není zapotřebí jen znalostí právních, ale především znalostí těchto technologií hlubších než uživatelských. Cílem je tedy snaha uchopit toto velice dynamické téma, důležitost počítačů a počítačových systémů v dnešní době. Za hypotézu tématu jsem stanovil to, že počítačovou a internetovou kriminalitu není a nebude možno zcela vymýtit a to zejména z důvodů náskoku informačních a komunikačních technologií před právním postihem, nutnosti odborných znalostí, nebývalé rychlosti rozvoje počítačů a internetu, částečné nekontrolovatelnosti a nepředvídatelnosti tohoto rozvoje. Metodami mého zkoumání bylo studium české a zahraniční odborné literatury, právních předpisů, odborných článků a materiálů z internetu. Zaměřil se na vysvětlení základních pojmů spojených s tématem a to jak z důvodu jejich mnohdy obtížné definice, tak důvodu potřeby jejich objasnění pro řádné porozumění a orientaci v této práci. Počítačová a internetová kriminalita, jako specifický druh řekněme „klasické“ kriminality, má svá specifika, která činí subjekty v ní zapojené jedinečnými. Tomu jsem také věnoval jednu celou kapitolu. V souvislosti s účinností nového trestního zákoníku od počátku roku 2010 jsem považoval za vhodné zabývat se těmi nejčastějšími trestnými činy, které mohou být spáchány pomocí počítačů a počítačových sítí, kterých je oproti předchozí právní úpravě o poznání více. Následně jsem se zaměřil na způsoby páchání tohoto druhu kriminality z pohledu spíše technického a praktického. Podrobněji jsem nakonec analyzoval podle mého názoru nejběžnější formu páchání této kriminality a to porušování autorského práva. Tato práce však nemá sloužit ke komplexnímu a detailnímu popisu počítačové a internetové kriminality, ale spíše objasnit právní a pro laika srozumitelně též technologické aspekty jejího páchání ve světle mezinárodních a národních právních dokumentů, jejího dosavadního vývoje, dopadů na společnost a aktuálního stavu.

1 Informační technologie v dnešní době

1.1Data a informace

Pojmy data a informace považuji jako ústřední pojmy celého tématu. Informace je chápána ambivalentně a záleží na vědním oboru, který na ní nahlíží. Můžeme říci, že informace je poznatek, týkající se jakýchkoliv objektů, např. fakt, událostí, věcí, procesů nebo myšlenek, včetně pojmů, který má v daném kontextu specifický význam.[1] V počítačové vědě, jsou data informace ve formě vhodné pro použití s počítačem.[2] Jsou jedním s nejdůležitějších artiklů dnešní doby a potřebujeme je ke každodennímu životu. Ať jde o jakkoliv významnou informaci, jejich získávání, zpracování, uschovávání a šíření je nezbytné pro komunikaci a rozvoj celé společnosti. Právo na přístup k informacím je v moderních demokraciích zaručeno na ústavní úrovni v souladu s mezinárodněprávními dokumenty a detailněji upraveno a regulováno na zákonné úrovni.[3] Lidský mozek má omezenou kapacitu a je pochopitelné, že si k práci s informacemi vytvořil pomůcky k usnadnění práce s nimi. Vědecký pokrok přinesl rozkvět tzv. informačních a komunikačních technologií, které jsou schopny zasáhnout do vývoje soudobého světa a otevřít nové cesty a způsoby efektivnější práce, zábavy, poznání.

1.2 Informačně komunikační technologie dnes

Význam informačních a komunikačních technologií (dále jen ICT) dnes je nepochybný a obrovský. Žijeme v informační společnosti[4], která si osvojila za svou historii řadu způsobů sdělování a přijímání informací. Kromě osobních interakcí se vyvinula potřeba komunikace „na dálku“ a to nejen mezi konkrétním komunikátorem a recipientem, ale i tzv. masová komunikace. Její rozsah začíná u novin a pokračuje přes elektronické prostředky jako telegraf, telefon, rozhlas, televizi až k Internetu. S nadsázkou se tyto prostředky dotýkají veškeré lidské činnosti dnes a denně po celém

[1] Norma ČSN ISO/IEC 2382-1. Informační technologie – Slovník. Část 1: Základní termíny (Český normalizační institut, Praha, 1997, s7.)
[2] Howe, D. The Free On-line Dictionary of Computing. Dostupný také z WWW: http://foldoc.org/data
[3] Viz ústavní zákon č. 2/1993 Sb. ze dne 16. prosince 1992 o vyhlášení Listiny základních práv a svobod (Listina základních práv a svobod) článek 17, zákon č. 106/1999 Sb. ze dne 11. května 1999 o svobodném přístupu k informacím, zákon č. 123/1998 Sb. ze dne 13. května 1998 o právu na informace o životním prostředí, a další
[4] Viz. např. Webster, F. Theories of information society. London : Routledge, 2006

světě. Ať již mluvíme o vědecké činnosti a výzkumu, armádě, ekonomické oblasti a bankovnictví, vzdělávání, volném času a zábavě, mediích, dopravě, pořádku a bezpečnosti, organizační činnosti, průmyslové výrobě, poznávání, v politice k prosazení vlivu, v zábavním průmyslu k zvýraznění známé osobnosti, počítače změnily a mění svět. Bereme je jako samozřejmost, ale stačí si jen představit život bez nich. Dá se tedy říci, že společnost jako taková je na nich závislá a to v tom smyslu, že na těchto technologiích spočívá, je na nich vystavěna. V jiném smyslu můžeme mluvit o jejich nadužívání. Zvykli jsme ti na ně tolik, že je mnohdy užíváme více, než je zdrávo a k účelům jiným, než předpokládaným. Na jednu stranu to činí informační společnost značně propojenou, koordinovanou a rychle se rozvíjející, na druhou stranu však pomocí těchto technologií velice zranitelnou.

1.3 Nový druh kriminality

Jakkoli může být a je přínos informačních a telekomunikačních technologií využit k prospěšným účelům, stejně dobře jej lze zneužít. Vznikl nový druh kriminality a to kriminalita počítačová, internetová nebo také kybernetická. Nový z toho důvodu, že společensky škodlivá jednání, která ji charakterizují, nelze ve většině případů podřadit pod stávající skutkové podstaty trestných činů. To se odráží v novelizaci stávajících právních předpisů, popřípadě v přijímání nových. Tato problematika je také předmětem úpravy mezinárodních smluv a též legislativy Evropské Unie.

2 Definice základních pojmů

Definice pojmů je důležitá z hlediska jednotnosti a ostrosti výkladu. U tohoto tématu, které je velice mladé, je tento úkol složitější. Jednotlivé pojmy jsou chápány rozdílně jak individuálně, tak institucemi tímto se zabývajícími.

2.1 Počítačový systém

Počítačovým systémem se rozumí jakékoli zařízení nebo skupina vzájemně propojených nebo souvisejících zařízení, z nichž jedno nebo více provádí na základě programu automatické zpracování dat.[5]

2.1.1 Bližší vymezení

Počítačový systém tedy používá hardware, což znamená technické, hmotné vybavení počítače. Rozlišujeme základní zpracovací jednotku a periferní zařízení, které plní určité specifické funkce v interakci se základní jednotkou (například monitor jako zobrazovací zařízení, klávesnice a myš jako vstupní zařízení). Programem se rozumí software a jde o množinu příkazů, instrukcí, deklarací a popř. jiných prvků programovacího jazyka. Pojem počítačový systém a pojem počítač bývají používány jako synonyma. Počítačový systém zahrnuje i síťově připojená zařízení, která pojmově nesplňují atributy počítače.[6]

2.1.2 Vývojový trend

Počítače nebyly původně určeny ke komunikaci, nýbrž jako výkonnější počítací stroje. Postupem času docházelo k zvyšování jejich výkonu. Za prvního přímého předchůdce současných elektronických počítačů lze považovat elektronkový ENIAC, jehož vývoj počal roku 1943, který byl sponzorován americkou armádou, zabírající plochu 167 čtverečních metrů.[7] K dnešnímu dni se pomocí miniaturizace a technologického pokroku počítač změnil nejen účelem, ale i vzezřením. Je nyní dostupný za několik tisíc korun téměř každému pro osobní účely. Kromě stabilních PC jsou využívány počítače přenosné. Téměř exponenciálně se zvyšuje jejich výkon a též

[5] Úmluva Rady Evropy č. 185 ze dne 23.11.2001 o kybernetické (počítačové) kriminalitě. Dostupná také z WWW: http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm, (dále jen Úmluva)
[6] Podrobněji v Šámal, P. a kol. Trestní zákoník II. § 140 až 421. Komentář 1. vydání. Praha : C. H. Beck, 2010, 2087s.
[7] About.com, http://inventors.about.com/od/estartinventions/a/Eniac.htm

kapacita. Srovnejme záznamová media. Disketa (1984, kapacita 1,44MB), DVD (1996, 4,7GB), Blue-ray disk (2008, 50GB). Otázkou nyní je, zda lze za počítač používat i mobilní telefony, konkrétně tzv. „smartphony“, v překladu chytré telefony, nebo PPC, což je zkratkou „pocket personal computer“, kapesní počítač. Mají totiž pevný disk, operační paměť i procesor jako běžné počítače a jejich výkon se mnohdy vyrovnává výkonu jen například o několik let starších PC.

2.2 Internet

Internet je celosvětový systém navzájem propojených počítačových sítí („síť sítí“), ve kterých mezi sebou počítače komunikují.[8]

2.2.1 Bližší vymezení

Internet tedy není ničím jiným, než jednotlivé počítačové systémy, propojené mezi sebou různými způsoby připojení. Nelze jej chápat jako jakýsi hmotný předmět, ke kterému se pomocí počítače připojujeme, i když je takto často personifikován. Lze jej charakterizovat také jako distribuovanou, decentralizovanou, demokratickou, neřízenou, otevřenou a robustní síť, která nemá žádné centrum a umožňuje rovný přístup všem svým členům.[9] Neexistuje přitom jediné centrum, odkud by byl Internet řízen. Je to prostředek komunikace, přenosu dat a to bezpochyby nejrozšířenější. Nelze jej také ztotožňovat se zkratkou WWW (world wide web), který je jen jednou ze služeb kterou nabízí, nebo spíše jedním způsobem jeho využití.

2.2.2 Historie Internetu

Prvním jménem spojovaným s vizí o „síti“ byl v roce 1962 J. C. R. Licklider, který již tehdy předvídal služby jako například internetové bankovnictví. Univerzita MIT (Massachusetts Institute of Technology) se stala místem zrodu Internetu, tam také zmíněný profesor působil. Krokem vpřed lze označit teorii paketů, jako přenosu dat, kde je zpráva rozložena na pakety a po přenosu z nich opět spojena dohromady. Tento vývoj dal vzniku projektu Advanced Research Projects Agency Network (ARPANET), který byl zahájen v roce 1969 pod záštitou Ministerstva obrany Spojených států amerických. Bylo to na pozadí odehrávající se studené války. Tato síť měla být komunikační

[8] Wikipedia, http://cs.wikipedia.org/wiki/Internet
[9] Jedlička, P. Internetová společnost: Sociální a ekonomické důsledky rozšíření internetu. Praha : FSV UK, 2001

převahou v době hrozby jaderné války s Ruskem. Veřejnosti byl představen tento projekt v roce 1972 na mezinárodní konferenci, kde byla také představena novinka e-mailu, elektronické pošty.[10]

Následný proces otevřel dveře k vytvoření Internetu, jak jej známe dnes. Jako univerzální nástroj komunikace, nabízející nové a nové způsoby jeho využití bez nutné změny jeho architektury. Jako síť otevřenou, umožňující propojení různorodých druhů sítí a počítačů, umožňující využití neomezenému počtu anonymních uživatelů. To samozřejmě skýtá bezpečnostní rizika, neboť uživatelé Internetu již nejsou zkušení, odborně vzdělaní vědci, jako to platilo o jeho tvůrcích.

V České Republice nastal rozkvět Internetu v 90. letech 20. století. Po pádu socialismu byly překážky spíše technologické, neboť jedinou komunikační sítí byla telefonická. 13. únor 1992 je považováno za oficiální datum připojení České republiky k Internetu, kdy se k internetovému uzlu v Linci připojily univerzitní počítače z pražského ČVUT.[11]

Údaj Českého statistického úřadu uvádí, že v roce 2008 bylo připojeno 32% domácností a na jaře 2009 mělo přes 90% domácích počítačů v ČR možnost připojit se k Internetu.[12]

Celosvětový počet uživatelů se pomalu přibližuje ke 2 miliardám.[13]

2.2.3 Škála služeb a způsoby připojení k Internetu

Kromě již zmíněného WWW Internet nabízí internetovou poštu (e-mail), konverzaci v reálném čase, internetové bankovnictví, internetovou telefonii (VoIP – Voice over Internet protocol), internetové zprávy, diskusní skupiny, FTP (file transfer protocol) jako možnost přenosu souborů, sociální sítě jako FACEBOOK, TWITTER, a mnoho dalších služeb.

Způsoby připojení k Internetu jsou víceré a postupem doby se též zefektivňují. Původní způsob byl vytáčený pomocí telefonní linky. Bylo sice pomalé, ale z hlediska internetové kriminality poskytovalo jen omezenou dobu jejího praktikování. Dnes se

[10] Internet Society (ISOC), History of the internet, Dostupné z WWW: http://www.isoc.org/internet/history

[11] České vysoké učení technické v Praze, Ústřední knihovna, Dostupné z WWW: http://knihovny.cvut.cz/vychova/vychova2/internet_zdroj_informaci/historie.html

[12] Český statistický úřad, Informační společnost v číslech 2008 , Dostupné z WWW: http://www.czso.cz/csu/redakce.nsf/i/informacni_spolecnost_v_cislech_2008_o

[13] Internet users, Update for 2010, Dostupné z WWW: http://www.internetworldstats.com

využívají způsoby nepřetržitého připojení a také bezdrátové připojení. To je nebezpečnější v důsledku ztížené lokalizace pachatele, který může být „v pohybu".

2.3 Počítačová kriminalita

Pod pojmem počítačová kriminalita je třeba chápat páchání trestné činnosti, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení včetně dat, nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď:

a) jako **předmět** této trestné činnosti, ovšem s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité, nebo

b) jako **nástroj** trestné činnosti.[14]

Ad absurdum pod tímto pojmem nelze chápat například způsobení újmy na zdraví člověku jeho opětovným udeřením použitím notebooku. Počítač je zde chápán jako nástroj ke zpracování dat.

Nicméně lze tento pojem jen stěží staticky definovat a to z důvodu dynamického a nekontrolovatelného vývoje počítačů a informačně komunikačních technologií. Musil to popisuje tak, že pojem počítačové kriminality nelze trvale vymezit jako ostře ohraničený pojem, a uzavírá: „*Abychom předem vyloučili jeho nevhodnou restrikci či přesah, pojmeme jej dynamicky jako tzv. „fuzzy" konstrukt ve smyslu otevřeného, jinak neostře vnímaného typu kriminality*."[15] Tento pojem je již dosti obsoletní, zejména v zahraniční odborné literatuře, kde je nahrazován pojmy obsahující „cyber", čehož význam je vysvětlen vzápětí.

První definice pojmu počítačová kriminalita zpočátku ani nemohly zahrnovat trestné činy spojené s propojením počítačů do počítačové sítě, Internet se například u nás masové rozmohl až v druhé polovině 90. let minulého století. Wall[16] považuje počítačovou kriminalitu jako první generaci kybernetického zločinu, jako trestné činy používající počítače coby pomocníky k páchání „klasické" trestné činnosti. Počítačová kriminalita může dnes vyvolávat vzpomínku na jednání typu krádež strojového času, což je dnes již spíše překonanou formou zneužívání informačních technologií, zejména v důsledku zpřístupnění počítačů exponenciálně většímu okruhu uživatelů. Dalším

[14] Smejkal, V., Sokol, T., Vlček, M. Počítačové právo. Praha : C. H. Beck. 1995, s. 220

[15] Musil S. (ed.) Počítačová kriminalita. Nástin problematiky. Kompendium názorů specialistů. Praha: IKSP, 2000

[16] Wall, D. S. Cybercrime: The Transformation of Crime in the Information Age. Policy press, 2007

argumentem proti tomuto termínu je fakt, že v právní teorii není běžným zvykem specifikovat kategorii trestných činů podle použitých prostředků.[17]

2.4 Internetová kriminalita

S technologickým pokrokem se objevily prostředky umožňující zejména komunikaci mezi počítači a též nové přístroje, již zmíněné smartphony, PPC a další, spojující dosud samostatné komunikační technologie (tzv. hybridní přístroje). Společným jmenovatelem těchto technologií se stala přítomnost dat a sítí – proto vznikl termín trestný čin v informačně komunikační teorii. Mezi mnoha informačně komunikačními sítěmi je Internet specifickou sítí, která užívá speciální komunikační protokol – Internetový protokol (IP). Odtud tedy Internetový trestný čin.[18]

2.5 Kyberprostor a kybernetická kriminalita

Tyto dva spolu související pojmy se používají zejména v mezinárodním právu, úzce spolu souvisí.

2.5.1 Kyberprostor (cyberspace)

Nejprve je vhodné přiblížit význam tohoto slova. Termín „cyberspace“ poprvé použil na počátku 80. let v povídce „Jak Vypálit Chrom“ William Gibson. Později ve svém cyberpunkovém románu „Neuromancer“ popsal kyberprostor jako „*konsenzuální datovou halucinaci, vizualizovanou v podobě imaginárního prostoru, tvořeného počítačovými daty, která nám nabízí mnohem lákavější představu o prostoru, čase nebo skutečnosti než je ta, ve které reálně žijeme.“* Gibbson nicméně neměl žádné odborné vzdělání v informačních technologiích.[19]

Můžeme říci, že kyberprostor je metaforou popisující nehmotný svět vytvořený moderními technologiemi, paralela ke světu reálnému. Je to virtuální svět a lidé v něm mohou například vzájemně komunikovat. „*Kyberprostor je „místem“, kde se telefonní konversace odehrává. Není to uvnitř telefonního přístroje, umělohmotného přístroje na vašem stole ani ve sluchátku druhé osoby ve druhém městě. Je to místo mezi těmito telefony*“[20]

[17] Gřivna, T., Polčák, R. (eds.). Kyberkriminalita a právo. Praha: Auditorium, 2008
[18] tamtéž
[19] Tim09 blog, http://tim09.blog.cz/0912/5-vyvoj-a-definice-konceptu-kybernetickeho-prostoru
[20] Sterling, B. Introduction to The Hacker Crackdown. London: Penguin, 1994

Obsahuje objekty a různé způsoby pohybu v něm, jako skutečný svět. K pohybu v něm ale nepotřebujeme více než pohyb prstů na klávesnici nebo pohyb myší. Kyberprostor ale není tvořen pouze počítači a Internetem. Mluvíme o něm například i v souvislosti s videohrami. Je však závislý na světě reálném, vystavěn na jeho informačně komunikačních technologiích.

2.5.2 Kybernetická kriminalita a kybernetický zločin

Kybernetická kriminalita bývá někdy ztotožňován s pojmem počítačová kriminalita. Tak to činí i Úmluva o *počítačové* kriminalitě. Její originální název je ovšem „Convention on cybercrime“, příhodnější překlad by tedy byl úmluva o kybernetické kriminalitě. Z tohoto důvodu uvádím při citaci této úmluvy obě alternativy. Také 10. kongres OSN o prevenci zločinnosti a nakládání s pachateli v roce 2000 se mimo jiné zabýval bojem proti počítačové kriminalitě. Kybernetická kriminalita byla definována ve dvou smyslech:

a) v užším smyslu: Jakékoliv nelegální jednání uskutečněné prostředky elektronických operací, jehož cílem je bezpečnost počítačových systémů a jimi zpracovávanými daty.

b) v širším smyslu: Jakékoliv nelegální jednání spáchané prostředky počítačového systému nebo sítě, nebo v jejich souvislosti, včetně takových zločinů jako nelegální držení, nabízení nebo distribuce informací pomocí počítače.

Tyto mezinárodní formy legislativy mají bezesporu nesmírný význam na poli harmonizace národních právních řádu, nicméně přesvědčivou a ustálenou definici kybernetické kriminality (též zkráceně kyberkriminality nebo dle Jirovského[21] kybernality), kybernetického zločinu (kyberzločinu) nepodávají.

Volevecký pod pojmem kybernetické trestné činnosti shledává trestnou činnost páchanou pomocí informačních technologií.[22] Kybernetickou kriminalitu v tomto smyslu můžeme označit jako jakékoliv nelegální jednání provozované v kyberprostoru. Potom přesahuje pojem počítačové a internetové kriminality a nepochybně bude

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

[22] Volevecký, P. Kybernetická trestná činnost v mezinárodních dokumentech ES/EU. Trestní právo č.7-8/2009

zahrnovat i takovou činnost páchanou pomocí telefonních přístrojů a to nejen těch mobilních kapesních počítačů, neboli smartphonů.[23]

Kyberzločin je pak, dle v právním diskursu více méně akceptované definice, chápán (kumulativně) jako:

a) trestný čin ohrožující ICT – informační a síťovou bezpečnost (trestný čin proti počítačové integritě nebo také trestný čin v úzkém pojetí),

b) trestný čin využívající ICT ke spáchání tradičních trestných činů (trestný čin vztahující se k počítačům) a

c.) trestný čin vztahující se k obsahu, jako například dětská pornografie, pomluva a porušení práv k duševnímu vlastnictví (trestný čin vztahující se k obsahu počítačových dat)[24]

Toto pojetí je dle mého názoru nejvhodnější, neboť kopíruje Úmluvu, kde jsou tato jednání popsána v Hlavě I-IV.

[23] viz. Kapitola 2.1.2

[24] Gřivna, T., Polčák, R. (eds.). Kyberkriminalita a právo. Praha: Auditorium, 2008

3 Specifika kybernetické kriminality a jejích subjektů

3.1 Odlišnost kybernetické kriminality

V této práci jsou naznačena specifika, kterými se počítačová a internetová kriminalita odlišuje od ostatních druhů „tradiční“ kriminality. Zde jsou pro přehled uvedena z mého pohledu ta nejdůležitější:

Využití informačních technologií

Tyto technologie zde hrají klíčovou a určující úlohu. Specifické technologie a postupy, kterých je k jejich využívání třeba, dávají náskok těm zasvěceným a nechávají běžné uživatele pozadu. Na jedné straně stojí specialisté, odborníci, kteří se podílejí a určují směr, kterým se tyto technologie budou ubírat, na druhé straně subjekty s minimálními znalostmi. Nicméně dostupnost, jednoduchost a pohodlnost jejich užívání dovoluje nabýt status pachatele kyberkriminality každému. Počítače se tak stávají mocnými nástroji, které ve špatných rukou mohou způsobit nedozírné škody.

Kyberprostor jako místo činu

Tento svět sám o sobě se od toho „reálného“ zásadně liší a jako takový skýtá odlišné prostředí páchání kyberkriminality. Typicky jde o poměr jednání a výsledku. Žádné jiné prostředí neumožní způsobit tak značné škody z pohodlí domova jen několika málo pohyby ruky. Útok tedy zpravidla nesměřuje vůči jednomu pachateli, ale je většinou určen neuzavřenému počtu uživatelů. Útok může nastat okamžitě, nebo s odstupem času. Bezprecedentní je též rychlost výměny dat a tedy i pohybu v kyberprostoru, z kterého pachatel může jednoduše zmizet a zanechat jen následky útoku. To znesnadňuje odhalování a vyšetřování. Dalším faktorem je též jeho anonymita. Uživatel zde nemá svou nezaměnitelnou identifikaci, tvář, může se „vytvořit“ dle své vůle, anebo se vydávat za někoho jiného.[25] Také pohled společnosti na toto nehmotné prostředí je odlišný. Některé trestné činy nejsou chápány tak zavrženíhodně jako jejich ekvivalentní protějšky. Například pachatel, který vyloupí banku s pistolí v ruce, je vnímán jinak než pachatel, který neoprávněně převede desítky milionů na svůj účet.[26]

Legislativa

[25] Vydávaní se za jiného se označuje jako tzv. „krádež identity“

[26] Zapletal, J. a kolektiv Aktuální problémy kriminologie pro posluchače magisterského studijního programu, 1. vyd. Praha : PA ČR v Praze, 2009

Podmínkou minimalizace kybernetické kriminality je dostatečně účinná zákonodárná činnost, směřující k definici a ke kriminalizaci těch nejškodlivějších jednání ohrožujících informační bezpečnost. U tradičních trestných činů, které se vyskytují po stovky let v legislativách převážné většiny civilizovaných států, je zákonodárství snadnější a to kvůli možnosti se inspirovat u jiných států, tak čerpat z tradic vlastního. U překotného vývoje informačních technologií, vynalézavosti pachatelů a nutnosti odborných znalostí zákonodárce je legislativní proces o to pomalejší a složitější. To přispívá k výraznému zpoždění legislativy a umožňuje pachatelům beztrestně rozvíjet společensky škodlivé aktivity. Důsledkem pak je mimo jiné nízké právní vědomí občanů ohledně kyberkriminality, kteří některá jednání nepovažují vůbec za trestná, jiná pak alespoň tolerují s omluvou „to přece dělá každý".

Policie a justice

Kybernetická kriminalita, je páchána s použitím velmi specifických technologických nástrojů a specializovaných znalostí. K jejímu odhalení a prokázání je tedy opět potřeba velmi speciálních nástrojů, znalostí a postupů. Je tedy potřeba vysoce kvalifikovaných pracovníků po stránce technologické a také právní. Klasické policejní vyšetřovací metody zde selhávají, je to zejména dáno odlišným charakterem stop v kyberprostoru, jejich trvanlivostí a použitelností v důkazním řízení. Na místě činu nezůstává DNA, fyzické ani pachové stopy, otisky prstů. Kyberprostor je prostředím, které se každou sekundu mění, podléhá technologickým trendům, rychle se rozvíjí a modifikuje. Justice trpí obdobnými problémy jako policie. Přestože je většina projevů kybernality trestná, není vždy snadné takovou činnost odhalit, dokázat a pachatele odsoudit. Soudci se ve velké míře musí z důvodu své nedostatečné technologické odbornosti spoléhat na soudní znalce a znalecké ústavy, kterých je také pomálu. To může vést k prodlužování procesů a k oslabení, případně ztrátě důkazů.[27]

Vysoká míra latence

Z výše uvedených faktů, zejména technické náročnosti odhalování, nutně vyplívá vysoká míra skrytosti, nezjevnosti tohoto druhu kriminality. Důvodem je nedostatečné zabezpečení počítačových systémů uživateli, útok tak mnohdy ani nemůže být zjištěn. Oznamování těchto útoků orgánů činným v trestním řízení z praxe nevede k nápravě, spíše ke ztrátě času.

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

3.2 Pachatel

Ať již je umělá inteligence počítačů jakkoliv vyvinutá, vždy je potřeba ke spáchání kybernetické kriminality alespoň jedné osoby. Fenomén Internetu a informačně komunikačních technologií, jako poměrně nový předmět zájmu kriminologie, s sebou přináší i otázku kdo je pachatelem Internetové a počítačové kriminality a také co je jejich motivem.

3.2.1 Typologie pachatele

Lze říci, že profil pachatele bude tvořit zejména osoba nižší věkové kategorie. Důvodem je, že čím vyšší věková kategorie, tím větší odstup od moderních technologií. Pro starší generace je typické neochota ztotožnění se s novými výdobytky moderní doby, ať již z důvodu jejich odlišného pohledu na jejich využití, tak z důvodu jejich neustálé miniaturizace. Berou je spíše jako doplněk, který je ovšem nutné ovládnout alespoň na uživatelské úrovni. Naopak mladší a střední generaci s počítači řekněme vyrůstali, myšleno z hlediska časového období největšího technologického rozmachu. Jsou tedy nedílnou součástí jejich životů a jejich znalost je hlubší než uživatelská a účel rozmanitější, než jen pracovní. Pachateli budou tedy bezpochyby z větší míry oni. Nicméně Zapletal dle mého názoru správně upozorňuje, že takový závěr není určující a zpochybňuje převážně uváděný věkové rozmezí pachatelů od 17 do 30 let. Záleží na konkrétních typech útoků. Útoků spočívajících v porušování práva autorského se dopouští i osoby trestně neodpovědné. Podvody páchané formou nabízení neexistujícího zboží na Internetu za účelem vylákání peněz jistě páchají i osoby starší 30 let.[28]

Větší zastoupení pachatelů bude z řad odborníků, středoškolsky a vysokoškolsky vzdělaných osob, programátorů, specializujících se právě na informační technologie a mající vyvinutější logické myšlení a v mnoha případech i vyšší inteligenční kvocient. Kriminologicky vnímáno tedy bývá proto kybernetický zločin označován jako trestný čin bílých límečků. To ovšem nebude pravidlem, neboť na samotném Internetu je mnoha diskusních skupin a návodů, jak takovou kriminalitu spáchat. Dle úrovně odborných znalostí a schopností můžeme pachatele kyberkriminality dělit na dvě skupiny – amatéry a profesionály.[29]

---

[28] Zapletal, J. a kolektiv Aktuální problémy kriminologie pro posluchače magisterského studijního programu, Praha 2009

[29] Srov. Madliak, J., Mihaĺov, J., Porada, V., Štefanková, S. Počítačová kriminalita. In Karlovarská právnická revue 1/2008,s. 54.

Pro pachatele kyberkriminality se vžilo označení hacker, zejména co se týče trestných činů proti počítačové integritě. Kyberzločiny vztahující se k obsahu páchají osoby nazývané piráti.

3.2.2 Pachatel a kyberprostor

Z psychologického hlediska je nutno podotknout, že ve zmíněném kyberprostoru si člověk může vytvořit odlišnou identitu od té skutečné. Jen málokdy se setkáváme, že uživatel vystupuje pod svým pravým jménem. Různé přezdívky a pseudonymy jsou takřka pravidlem a při páchání kriminality také účelem. Uživatel se tak může realizovat v tomto virtuálním světě zcela opačně, než v tom reálném.

V kyberprostoru panují jiná pravidla než ve skutečném světě. Je to dáno jak anonymitou uživatelů, tak jeho hmotnou neexistencí. Lze do něj vstoupit z pohodlí domova, ale z jakéhokoliv počítače ve škole, v práci, v knihovně a vlastně bezdrátovým připojením kdekoliv jinde. To způsobuje, že měřítko toho, co je „normální“, je dosti vychýleno. Takový trestný čin pomluvy § 184 TZ[30] je na Internetu rozšířen o mnoho více a to zejména v písemné podobě. Lze obecně říci, že uživatelé Internetu si „dovolí“ mnohem více, než v reálném životě.

3.2.3 Motivy

Motivem pachatelů bývá samozřejmě v první řadě zisk. Na druhou stranu se zde ale objevuje i motiv seberealizační, chtíč zlepšování se například v prolamování bezpečnostních prvků ochrany počítačů u takzvaných hackerů jako koníček. Motivy jsou kategorizovány:[31]

a) Jen tak pro zábavu

Do této kategorie spadají většinou mladí, fascinováni technologiemi, kteří se učí práce se systémem způsobem pokus-omyl. Většinou nepůsobí ani újmu, mohou se chtít jen dostat tam, kam to jiný předtím nedokázal. Mohou to také brát jako hru, kterou hrají proti administrátorovi počítače nebo systému, na který útočí. Charakteristikou takového pachatele je pak onen požitek z takové činnosti.

b) Finanční motiv

30 TZ zkratkou pro zákon č. 40/2009 Sb. ze dne 8. ledna 2009, trestní zákoník
31 Shinder, D. L. Scene of the Cybercrime: Computer Forensics Handbook, Syngress Publishing, 2002

Láska k penězům je důvodem mnoha rozličných jednání v rámci kybernetické kriminality. Není to ovšem jen zisk peněz, ale také získat nějaký požitek bez placení.

c) Hněv, odplata, jiné emocionální důvody

Takové zločiny jsou zejména ty násilné. Z psychologického hlediska je jednání s takovým člověkem srovnatelné, jako by měl duševní poruchu, nebo byl pod vlivem alkoholu či drog. Mohou to být zklamaní milenci, propuštění zaměstnanci. Jejich činy mohou sahat od terorismu po DoS útoky. Motivem může být také přilákání pozornosti na jejich osobu, nebo také projev loajality.

d) Politické motivy

Pachatelé těchto motivů zahrnují členy extrémistických a radikálních organizací na obou koncích politického spektra, kteří používají Internet k šíření propagandy, útokům na Internetové stránky jejich politických protivníků, v extrémních případech kradou prostředky k financování jejich vojenských operací, nebo plánují a koordinují jejich činy ve skutečném světě.

e) Sexuální impulsy

Tyto impulsy a pudy jsou jedny z nejsilnějších u lidí, zvířat. Otázkou je, co způsobuje změnu normálních sexuálních pocitů v ty zvrhlé. Není přitom pochyb, že sexuální odchylky jsou běžné u určitých typů pachatelů. Jsou jimi pedofilové a to jak pasivní, kteří z Internetu stahují materiál zneužívající děti k sexuálním aktivitám, tak aktivní, kteří využívají Internet k získávání důvěry dětí k pozdějšímu osobnímu setkání. Jiní pachatelé používají Internetu k navázání kontaktu s obětí jejich pozdějšího znásilnění.

f) Závažná psychická onemocnění

Osoby, trpící onemocněními jako je schizofrenie, poruchy osobnosti, deprese, jsou považovány za náchylnější, co se páchání trestné činnosti týká. V prostředí Internetu pak mohou snáze skrýt jejich poruchy. Takto motivovaná kriminalita může být složitý ne odhalení, protože se zdá být nelogická a iracionální, na rozdíl od té páchané za účelem zisku.

3.3 Oběť kybernetické kriminality

Poškozeným je ta osoba, která byla zasažena ve sféře ekonomické, sociální, psychické a podobně. Proti ní je čin namířen a jemu je způsobena škoda. Může jím být

samozřejmě jak fyzická (a to nejčastěji), tak právnická osoba, také stát. Tedy kdokoliv využívající počítač a počítačové sítě.

Je třeba mít na mysli, že k tomu, aby se uživatel stal obětí internetové kriminality, stačí pouhé jedno tlačítko myši. Studie, kterou zveřejnil výrobce bezpečnostního softwaru Norton, odhaluje šokující rozmach počítačové kriminality: dvě třetiny (65 %) uživatelů Internetu na celém světě jí bylo postiženo.[32] Mnohdy se totiž stává, že pachatel ani o svém statutu oběti neví, neboť neví, že se stal obětí počítačového útoku.

Přitom kyberzločin patří mezi nejméně ohlašovanou kategorii trestné činnosti a tato nevole ohlašovat tyto orgánům prosazujících právo dále podněcuje následné kybernetické útoky. Experti tvrdí, že je hlášeno méně než 10 % těchto útoků.[33] Důvodem bývá zahanbení obětí, ale též obava ze ztráty věrohodnosti a klientů, zejména u bank. Dále pak to může být v menším či větším rozsahu vlastní obava z odhalení nelegálního obsahu v počítači „oběti“, nebo obava z narušení soukromí dat na něm uchovávaných. Některé útoky mohou být provedeny takovým způsobem, který znemožňuje odhalení z důvodu nezanechání jakýchkoliv stop. Významný v této je vztah pachatele a oběti. Zpravidla zde totiž nedochází k osobnímu kontaktu a vzhledem ke globálnímu rozšíření Internetu mohou pocházet z různých zemí a kontinentů. To vytváří problémy ve výběru práva doléhajícího na takovou kriminalitu. Důvody rozsáhle viktimizace jsou kromě překotného rozvoje ICT je nedostatečné softwarové zabezpečení počítačů pomocí antivirových programů, firewallů, aktualizací.

[32] Symantec, http://www.symantec.com/cs/cz/about/news/release/article.jsp?prid=20100908_02
[33] Kshetri, N. The global cybercrime industry, Springer-Verlag Berlin Heidelberg, 2010

4 Kybernetická kriminalita a legislativa

4.1 Potřeba právní úpravy

S vývojem ICT se vyvinuly kriminální aktivity spojené s jejich využíváním. Stávající trestní právo však nebylo psáno s vědomím on-line společnosti v kybernetickém prostoru. Hlavním problémem tedy byla použitelnost těchto zákonů na kyberzločiny a také její rozsah. Informační struktura kyberprostoru reprezentuje hodnoty, které by měly být dle většinového názorového proudu chráněny prostředky trestního práva. Skutkové podstaty trestních činů se vyvíjely mnohdy stovky let, tak jak se vyvíjelo jednání směřující proti osobám a majetku. Kyberprostor je realitou od 90. let 20. století a jeho dopad byl nebývale rychlý, enormní a trestní právo s ním zpočátku nedrželo krok, navíc u kyberkriminality se projevilo zpoždění legislativy ještě více, než u běžných trestních činů. Některé kybernetické útoky bylo možno subsumovat pod stávající skutkové podstaty, například typicky pod skutkovou podstatu podvodu, otázkou však bylo, zda to bylo vůlí zákonodárce podchytit činy, které v době uzákonění v reálném světě ještě neexistovaly. Místo extensivního výkladu tedy přistoupily novelizace a rekodifikace trestních zákonů v souladu se zásadou prevence, kde potencionální pachatel musí být také v kyberprostoru dostatečně zřetelně varován s adekvátní předvídatelností, že určitá jednání nejsou tolerována.[34]

Opačný názorový proud představuje zastánce svobody jednotlivce a oproštění se od pravidel a regulace americký hudebník a podnikatel John Perry Barlow, který tyto myšlenky aplikoval na prostředí kyberprostoru. Založil též neziskovou společnost Electronic Frontier Foundation[35], která se zabývá ochranou tzv. digitálních práv a svobod a to včetně soudních pří proti vládě Spojených států a velkých korporací, vzděláváním a výzkumem v této oblasti. Jeho dílem je Deklarace nezávislosti kyberprostoru, která se stala všeobecně přijímaným manifestem svobody Internetu. Argumentuje neexistencí společenské smlouvy mezi adresáty právních norem a státem, kterou by se nově vzniklé Internetové společenství vzdalo části své svobody ve prospěch suveréna. Dále je zde vyjádřena nepotřebnost právní a jiné autoritativní

[34] Blíže Schjolberg, S. The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva, 2008, Dostupné z WWW: http://cybercrimelaw.net/documents/cybercrime_history.pdf
[35] Domácí stránka této organizace je www.eff.org

regulace Internetu a schopnost Internetového společenství řešit problémy samo. Také hlásá, že vlády nemají ani nástroje, jak své právo efektivně vynutit.[36]

Pro představu zmíním několik citací této deklarace:

„Nemáme vládu a ani po žádné netoužíme. Mluvím k Vám tedy z pozice autority ne větší, než jakou má sama Svoboda“

„Moc vlád je odvozena ze souhlasu těch, kterým vládnou. Náš souhlas jste však nežádali a nikdy jej neobdržíte“

„Založíme v kyberprostoru novou civilizaci Mysli. Snad bude humánnější a spravedlivější než svět, který Vaše vlády doposud vytvořily.“

4.2 Místní působnost trestně právních norem

Právo je chápáno teritoriálně, geografické hranice rozdělují území, na kterých platí odlišné jurisdikce. Stát může zásadně vykonávat trestní soudnictví jen na svém území. Na principu teritoriality je postaven i český TZ:

§ 4

1) Podle zákona České republiky se posuzuje trestnost činu, který byl spáchán na jejím území.

2) Trestný čin se považuje za spáchaný na území České republiky,

a) dopustil-li se tu pachatel zcela nebo zčásti jednání, i když porušení nebo ohrožení zájmu chráněného trestním zákonem nastalo nebo mělo nastat zcela nebo zčásti v cizině, nebo

b) porušil-li nebo ohrozil-li tu pachatel zájem chráněný trestním zákonem nebo měl-li tu alespoň zčásti takový následek nastat, i když se jednání dopustil v cizině.

To vyjadřuje místní působnost trestněprávních norem, kde místní působnost trestního zákona vymezuje okruh případů, které se posuzují podle trestního zákona se zřetelem k místu, kde byl trestný čin spáchán. Dále se zde uplatňuje zásada registrace (§ 5), zásada personality (§ 6), zásada ochrany a zásada univerzality (§ 7), včetně subsidiární zásady univerzality (§ 8).[37] Princip teritoriality má však vedoucí úlohu. Trestný čin je pak možno stíhat nejen tam, kde byl stíhán, ale také tam, kde nastaly jeho následky. Není tedy vyloučena možnost stíhání pachatele na území více států. To dává prostor k pozitivním právním konfliktům, procesním a administrativním komplikacím,

[36] Blíže Gřivna, T., Polčák, R. (eds.). Kyberkriminalita a právo. Praha: Auditorium, 2008.
[37] Viz. Šámal, P. a kol. Trestní zákoník I. § 1 až 139. Komentář 1. Vydání. Praha : C. H. Beck, 2010, 55s.

které pak nesvědčí nikomu jinému než pachateli. Stěžejní tedy bude pro zákonodárce delimitace jurisdikcí.

Otázkou tedy je místo spáchání trestného činu u kyberzločinů, typických jednání s mezinárodním prvkem, kterým je kyberprostor. Specifický neomezený prostor, který nehledí na státní hranice reálného světa, prostor pro nové nelegální aktivity, případně nové způsoby páchání těch stávajících.[38] Pro pachatele výhodou je efektivita, časová a finanční nenáročnost, místní neomezenost, snížená možnost postihu takových aktů. U kyberkriminality je též zjevný prvek delokalizace, znamenající mj. rozdílné místo jednání pachatele a místo účinků tohoto jednání, kde může být problematické již určení rozhodného práva a příslušného soudu, ale vzhledem k rozdílnosti právních úprav vůbec samotné určení trestnosti i identických skutků a také procesních možností jejich trestního postihu.[39]

K efektivnímu postihu kybernetické kriminality je tedy třeba mnohostranné mezinárodní spolupráce s úmyslem popsat, omezit či zcela vymýtit určitá společensky škodlivá jednání, způsoby jejich postihu, což se jeví jako jediný způsob jak překonat bariéry jurisdikcí jednotlivých států. Snahy harmonizace se ovšem neobejdou bez potíží, z hlediska odlišných postojů k regulaci jednotlivých konkrétních jednání. Příkladem může být Dodatkový protokol k Úmluvě[40], který upravuje opatření týkající se boje proti rasistické a xenofobní propagandě. Tato nebyla obsažena v samotné úmluvě z důvodu předpokládané účasti USA na Úmluvě. Legislativa USA akcentuje svobodu projevu, což by mohlo onu účast ohrozit.

I v případě nalezení řešení v podobě mezinárodních dokumentů však může docházet k jejich rozdílné aplikaci vzhledem k rozdílnosti právních kultur.

4.3 Mezinárodní prameny

Dva nejzásadnější dokumenty byly přijaty na půdě Rady Evropy a jsou jimi:

Úmluva Rady Evropy o kybernetické (počítačové)[41] kriminalitě

[38] Trefně označováno „old wine in new bottles“, neboli staré víno v nových lahvích
[39] Gřivna, T., Polčák, R. (eds.). Kyberkriminalita a právo. Praha: Auditorium, 2008.
[40] Dodatkový protokol č. 189 k Úmluvě Rady Evropy o počítačové kriminalitě ze dne 28.1.2003 týkající se kriminalizace činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů. Dostupný z WWW: http://conventions.coe.int/Treaty/EN/Treaties/html/189.htm, dále jen Dodatkový protokol k Úmluvě
[41] Záleží na překladu autora

Dodatkový protokol k Úmluvě o kybernetické (počítačové) kriminalitě týkající se kriminalizace činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů.

Úmluva byla otevřena k podpisům v Budapešti dne 23. 11. 2001, v platnost vstoupila 1. 7. 2004. K začátku roku 2011 ji podepsalo 47 členských států Rady Evropy a doposud neratifikovalo 17 z nich. Česká Republika Úmluvu podepsala 9. 2. 2005 a doposud neratifikovala.

Úmluva představuje první mezinárodní dohodu týkající se trestných činů páchaných prostřednictvím informačních technologií, zejména využitím Internetu nebo jiných počítačových sítí, vztahujících se k porušování autorských práv, páchání počítačových podvodů, šíření dětské pornografie a k dalším formám útoků proti informační a počítačové bezpečnosti. Jejím hlavním cílem je sjednocení přístupu signatářů Úmluvy v otázkách postihování nejzávažnějších forem kybernetických útoků. Toho se snaží dosáhnout zejména tím, že smluvním stranám ukládá povinnost zařadit do svých národních právních řádů takové instrumenty, které umožní stejný postup proti pachatelům tohoto druhu trestné činnosti bez ohledu na místo spáchání trestného činu. Taktéž stanovuje základní principy pro výběr a ukládání trestů za tyto trestné činy.[42]

Struktura Úmluvy je vystavěna na preambuli a 48 článcích, rozdělených do 4 kapitol. Kapitola první definuje pojmy, které Úmluva používá. Druhá kapitola nazvaná Opatření k přijetí na národní úrovni obsahuje ustanovení hmotného i procesního práva, které jsou uloženy členským státům za účelem sjednocení znaků kybernetických trestných činů a také postupů boje s nimi. Jsou zde zejména znaky devíti skutkových podstat (články 2-10), rozdělené do čtyř kategorií (viz níže), ustanovení o pokusu a pomoci, odpovědnosti právnických osob a sankcích a opatřeních, procesní instituty působnosti, otázky zajišťování a uchovávání počítačových dat a jejich zpřístupňování a vydávání ostatním smluvním stranám. Kapitola třetí nazvaná Mezinárodní spolupráce se zabývá právní pomocí v řízení o kybernetických trestných činech. Kapitola čtvrtá obsahuje Závěrečná ustanovení.

Přínosem Úmluvy a Protokolu k Úmluvě považuji zejména výčet znaků kybernetických trestných činů, který se v zásadě shoduje s definici kyberzločinů uvedenou v této práci. Úmluva upravuje tyto trestné činy:

[42] Volevecký, P. Kybernetická trestná činnost v mezinárodních dokumentech ES/EU. Trestní právo č.7-8/2009

1. Trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů

Čl. 2 Neoprávněný přístup

Čl. 3 Neoprávněné zachycení informací

Čl. 4 Zásah do dat

Čl. 5 Zásah do systému

Čl. 6 Zneužití zařízení

2. Trestné činy související s počítači

Čl. 7 Falšování údajů související s počítači

Čl. 8 Podvod související s počítači

3. Trestné činy související s obsahem

Čl. 9 Trestné činy související s dětskou pornografií

4. Trestné činy související s porušením autorského práva a práv příbuzných k autorskému právu

Čl. 10 Trestné činy související s porušením autorského práva a práv příbuzných k autorskému právu

Protokol k Úmluvě pak upravuje úmyslná protiprávní jednání, která jsou páchána prostřednictvím počítačového systému, a to:

a)šíření rasistických a xenofobních materiálů

b)rasisticky a xenofobně motivovaná pohrůžka

c)rasisticky a xenofobně motivovaná urážka

d)popření, hrubé snižování, schvalování nebo ospravedlnění genocidy nebo zločinů proti lidskosti

e)návod a pomoc k jednání a) až d)

Dalšími dokumenty EU/ES sloužící k harmonizaci právních úprav při potírání kybernetické trestné činnosti jsou pak zejména následující:

- Rozhodnutí rady 92/242/EHS ze dne 31. 3. 1992 o bezpečnosti informačních systémů
- Rámcové rozhodnutí Rady 2000/375/JHA ze dne 29. 5. 2000 o boji proti dětské pornografii na Internetu
- Rámcové rozhodnutí rady 2001/413/SVV ze dne 28. 5. 2001 o potírání podvodů a padělání bezhotovostních platebních prostředků

- Rámcové rozhodnutí Rady 2004/68/SVV ze dne ze dne 22. 12. 2003 o boji proti pohlavnímu vykořisťování dětí a dětské pornografii
- Rámcové rozhodnutí Rady 2005/222/SVV ze dne 24:2:2005 o útocích proti informačním systémům
- Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. 6. 2000 o některých právních aspektech služeb informační společnosti, zejména na elektronickém obchodu na vnitřním trhu (směrnice o elektronickém obchodu)

4.4 Právní úprava z pohledu trestního zákoníku

Dne 1. 1. 2010 nabyl účinnosti zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších přepisů. Oproti jeho předchůdci, zavedl řadu výrazných změn v rozsahu postihování kybernetických trestných činů, které obsahují znaky mající vztah k informačním a komunikačním technologiím. To bylo právě důsledkem výše uvedených mezinárodních dokumentů.

Následuje tabulka, podávající přehled těch typických trestných činů. Volevecký[43] například uvádí, že jejich počet je uzavření a to konkrétně 21. S tím však nelze souhlasit, pomocí počítačových systémů lze jistě spáchat i trestné činy níže neuvedené, nebude to však převažující způsob jejich spáchání.

Třetí a čtvrtý sloupec tabulky rozlišuje, zda se tyto trestné činy dají řadit pod ty,

A) kterých jsou prvky užity při spáchání trestného činu jako nástroj umožňující jejich spáchání
B) kterých jsou prvky informačních a telekomunikačních technologií terčem útoku pachatele, jsou tedy individuálním objektem a předmětem ochrany[44]

[43] Volevecký, P. Kybernetické trestné činy v trestním zákoníku. Trestní právo č.7-8/2010

[44] Volevecký, P. Kybernetické trestné činy v trestním zákoníku. Trestní právo č.7-8/2010

§	Název trestného činu	A	B
180	neoprávněné nakládání s osobními údaji	ano	ne
182	porušení tajemství dopravovaných zpráv	ano	ano
183	porušení tajemství listin a jiných dokumentů uchovávaných v soukromí	ne	ano
184	pomluva	ano	ne
191	šíření pornografie	ano	ne
192	výroba a jiné nakládání s dětskou pornografií	ano	ne
209	podvod	ano	ano
230	neoprávněný přístup k počítačovému systému a nosiči informací	ano	ano
231	opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat	ano	ne
232	poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti-nad rámec mezinárodních závazků	ne	ano
234	neoprávněné opatření, padělání a pozměnění platebního prostředku	ano	ano
236	výroba a držení padělatelského náčiní	ano	ne
270	porušení autorského práva, práv souvisejících s s právem autorským a práv k databázi	ne	ano
287	šíření toxikomanie	ano	ne
311	teroristický útok	ne	ano
345	křivé obvinění	ano	ne
348	padělání a pozměnění veřejné listiny	ano	ne
354	nebezpečné pronásledování	ano	ne
355	hanobení národa, rasy, etnické nebo jiné skupiny osob	ano	ne
356	podněcování k nenávisti vůči skupině osob nebo k omezování práv a svobod	ano	ne
403	založení, podpora, propagace hnutí směřujícího k potlačení práv a svobod člověka	ano	ne
407	podněcování útočné války	ano	ne

Dle Voleveckého lze tyto trestné činy sdružit do těchto kategorií:

4.4.1 Zásahy do počítačového systému a dat

4.4.2 Šíření závadného obsahu

4.4.3 Porušování autorských práv a práv souvisejících

4.4.4 Nakládání se zařízením k páchání kybernetické trestné činnosti

4.4.5 Kybernetické pronásledování

4.4.1 Zásahy do počítačového systému a dat

§ 230 Neoprávněný přístup k počítačovému systému a nosiči informací

Tento paragraf je hlavní skutkovou podstatou kybernetických trestných činů, pojednám o ní tedy na prvním místě a podrobněji. Byl zařazen do TZ na základě Úmluvy po několika neúspěšných pokusech. V roce 2006 nebyla Parlamentem České republiky přijata rekodifikace trestního zákona (sněmovní tisk č. 744), čímž byla ohrožena implementace mezinárodních závazků, vyplívajících z rámcových rozhodnutí přijímaných v rámci spolupráce v policejních a justičních věcech (třetí pilíř EU). Takovým bylo zejména Rámcové rozhodnutí Rady o útocích proti informačním systémům 2005/222/SVV ze dne 24. 2. 2005, které navazuje na dřívější mezinárodní právní úpravu v oblasti ochrany počítačových systémů, reagující zejména na hrozbu organizované trestné činnosti a možné teroristické útoky proti informačním systémům a také na nadnárodní povahu takové trestné činnosti. Sblížení trestních předpisů členských států mělo být dosaženo zejména stanovením výše a druhu sankcí za tyto útoky a dále povinností zavedení skutkových podstat „protiprávní zásah do systému“ a „protiprávní zásah do dat“. O to se pokusila alespoň novela trestního zákona z roku 2007, která sice již obsahovala znění téměř totožné se současnou dikcí § 230 TZ, nicméně přijata nebyla. V platnosti pak nadále zůstávalo ustanovení § 257a Poškození a zneužití záznamu na nosiči informací, které kumulativně k trestnosti požadovalo úmysl způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch a k tomu některé z alternativně uvedených jednání, která však přesahovala pouhý přístup počítačovému systému a v souladu s Úmluvou proto nebyla. Dnešní § 230 se liší zejména záměnou dříve navrhovaného „poruší“ v nyní „překoná“. Logika změny spočívá v zažité odborné terminologii užívané v informační oblasti. Dalším důvodem je obtížnost dokazování dříve navrhovaného „Porušení“ ve vztahu

k softwarovému zabezpečení počítače, a to proto, že případný pachatel do zabezpečovacího programu nemusí nutně zasáhnout destruktivním způsobem a takové bezpečnostní opatření nutně porušit, přestože jej fakticky obejde či jinak eliminuje.

Odst. 1 § 230 byl zaveden do TZ na základě článku 2 Úmluvy nazvaného Protiprávní přístup. Ten vyjadřuje požadavek, že každá smluvní strana přijme legislativní a jiná opatření nezbytná k tomu, aby podle vnitrostátního práva bylo trestným činem jednání spočívající v úmyslném protiprávním přístupu do počítačového systému nebo jeho části. Smluvní strana může stanovit, že ke spáchání tohoto trestného činu dojde jen v případě porušení bezpečnostních opatření, úmyslu získat počítačová data nebo jiného nečestného úmyslu nebo ve vztahu k počítačovému systému, který je propojen s jiným počítačovým systémem.

Objektem tohoto trestného činu je tedy ochrana počítačových systémů a dat. Výrazným prvkem je zejména požadavek trestnosti již pouhého přístupu, průniku do tohoto systému. Není tak zapotřebí jakákoliv manipulace s daty v něm uloženými, ani dokonce seznámení se s nimi. Toto jednání je nutno spáchat úmyslně, pachatelem může být kdokoliv.

K naplnění skutkové podstaty uvedené v odst. 1 § 230 postačí pouhé překonání bezpečnostního opatření počítačového systému nebo jeho části, mající za následek získání neoprávněného přístupu k systému. Jde o rozšíření trestní odpovědnosti vůči předchozí úpravě, již se totiž nevyžaduje úmysl způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch. Soudní judikaturou bude muset být řešen nedostatek definování onoho bezpečnostního opatření. Také byl vyjádřen názor, zda je útok na počítačový systém spojený s překonáním bezpečnostního systému bez vzniku majetkové nebo jiné škody ani prospěchu pachatele natolik závažným problémem, aby byly tyto systémy chráněné prostřednictvím trestního práva.[45] Ustanovením o bezpečnostním opatření tak Česká republika využila možnost omezení trestnosti a to konkrétně požadavkem překonání onoho bezpečnostního opatření. Osoba, která nepřekoná žádné bezpečnostní opatření, ale přesto získá přístup k počítačovému systému, nemůže být stíhána dle tohoto odstavce.

[45] Zejména z hlediska finančních nákladů vydaných ve spojitosti se stíháním těchto osob, jako jsou znalecké posudky podobně. Viz Volevecký, P. Neoprávněný přístup k počítačovému systému v navrhované novele trestního zákona. Trestní právo č.5/2007

Bezpečnostním opatřením bude zřejmě jakékoliv opatření, které je způsobilé plnit ochrannou funkci počítačového systému. Bude se moci jednat například o zabezpečovací software, hardware, užívání vstupních a bezpečnostních hesel, ale taktéž zavedený režim užívání počítačových systémům pracovišti a přístup k nim a k jejich částem, zajištění místnosti s počítačovým systémem pomocí technických zařízení apod. Také to mohou být možnosti operačního systému bránit neoprávněným průnikům a ovládání počítače prostřednictvím sítě Internet, nastavení integrovaného firewallu, který je schopen zamezit ukládání škodlivých programů na pevný disk počítače apod.[46]

V oblasti informační bezpečnosti se pronikání do počítačových systémů označuje jako hacking, o kterém bude pojednáno níže.

Podle odst. 2, který je též základní skutkovou podstatou, se již nevyžaduje pro vznik trestní odpovědnosti překonání bezpečnostních opatření, postačí v podstatě jakékoliv získání (i oprávněného) přístupu k počítačovému systému nebo k nosiči informací.[47] Je zde však požadavek neoprávněného nakládání dle písmen a) až d). Byl tak podstatně zpřesněn způsob spáchání tohoto trestného činu. § 257a odst. 1 obsahoval pouze užití informací, jejich zničení, poškození, změna nebo učinění neupotřebitelnými. Písmeno a) hovoří o neoprávněném užití dat. Je jím jakákoli nedovolená manipulace s daty uloženými v počítačovém systému nebo na nosiči informací, pokud nejde o případy b) až d). Toto jednání bývá označováno jako počítačová špionáž.[48] Neoprávněnost je spatřována v rozporu s právní normou. Uveďme například § 12 odst. 1 Občanského zákoníku nebo § 40 a následující Autorského zákona. Nejčastěji půjde o užití těchto dat bez vědomí a svolení oprávněné osoby.

Písmeno b) je odrazem článku 4 Úmluvy, Zásah do dat. Objektivní stránka spočívá ve vymazání nebo jiném zničení, poškození, změnu, potlačení, snížení kvality dat nebo učinění je neupotřebitelnými. Pod tímto jednáním je spatřováno používání zákeřných programů, tzv. malware, o kterých bude pojednáno níže.

Písmeno c) odráží článek 7 Úmluvy, Falšování údajů související s počítači. Zde se jedná o obdobu padělání listin, ať již veřejných nebo soukromých. Jde zde zejména o

[46] Blíže v Volevecký, P. Neoprávněný přístup k počítačovému systému v navrhované rekodifikaci trestního zákona. Trestní právo č. 7-8/2008

[47] Srov. Smejkal, V., Sokol, T. Postih počítačové kriminality podle nového trestního zákona. Právní rádce, 2009, roč.17, č.7

[48] Šámal, P. a kol. Trestní zákoník II. § 140 až 421. Komentář 1. Vydání. Praha : C. H. Beck, 2010, 2090s.

ochranu pravdivosti dat, a právních vztahů z nich vyplývajících. Paděláním je nutno rozumět úplné vyhotovení nových, nepravých dat vyvolávajících zdání pravosti. Pravostí je pak skutečnost, že data pochází od určitého původce nebo že jsou pravá co do obsahu, tedy správná.

Písmeno d) spočívá v neoprávněném vložení dat do počítačového systému nebo na nosič informací nebo v jiném zásahu, což představuje zbytkové ustanovení. Toto písmeno spolu s tím předcházejícím bývá označováno jako počítačová sabotáž.
Odstavce 3, 4 a 5 pak představují kvalifikované skutkové podstaty.

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

Tento trestný čin je zařazen do TZ nad rámec závazků mezinárodního práva. Individuálním objektem je i zde ochrana počítačového systému, nosičů informací a dat. Objektivní stránka vyjádřená pod písmeny a) a b) odpovídá v zásadě jednání vymezenému v § 230 odst. 2 písm. b) až d). Jedná se zde o nedbalostní poškozovací jednání, způsobující značnou škodu, kterou je 500 000,-Kč.[49] Hrubou nedbalostí se dle TZ rozumí takové zavinění, kdy přístup pachatele k požadavku náležité opatrnosti svědčí o zřejmé bezohlednosti pachatele k zájmům chráněným trestním zákonem.[50] Jde o určitou vyšší míru či stupeň intenzity nedbalosti, a to ať už jde o nedbalost vědomou, či o nedbalost nevědomou.[51] Subjekt je zde speciální, vyžaduje se, aby pachatel spáchal tento trestný čin porušením povinností vyplývajících ze zaměstnání, povolání, postavení nebo funkce nebo uložené podle zákona nebo smluvně převzaté. Půjde o využívání informačních a telekomunikačních technologií tímto subjektem soukromým účelům, což je zakázáno zákoníkem práce.

Jednání naplňující tuto skutkovou podstatu budou mít různé podoby, například vymazání telefonního seznamu obchodní společnosti, mající pro ni fatální dopad. Může to být zanedbání povinnosti správce sítě dostatečně ochránit počítačové systémy bezpečnostními opatření, zejména antivirovými programy. Volevecký[52] popisuje bizarnější situace, kdy například pracovník konzumující kávu u počítače v rozporu s režimem užívání takové výpočetní techniky omylem nalije kávu do počítače, přičemž

[49] Dle výkladového ustanovení TZ, § 138 odst 1
[50] § 16 odst. 2 TZ
[51] Důvodová zpráva k TZ
[52] Volevecký, P. Kybernetické trestné činy v trestním zákoníku. Trestní právo č.7-8/2010

zkratování vede ke ztrátě nebo poškození uložených dat a ke vzniku značné škody. Zamýšlí se, zda měl zákonodárce v úmyslu postihnout takové situace prostředky trestního práva a zda je zde namístě používat termín kybernetický trestný čin.
Odst. 2 představuje kvalifikovanou skutkovou podstatu.

§ 180 Neoprávněné nakládání s osobními údaji

Osobním údajem jakýkoliv údaj týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze na základě jednoho či více osobních údajů přímo či nepřímo zjistit jeho identitu. O osobní údaj se nejedná, pokud je třeba ke zjištění identity subjektu údajů nepřiměřené množství času, úsilí či materiálních prostředků.[53] Ochrana tohoto údaje je tedy individuálním objektem této skutkové podstaty. To je ostatně zajištěno na ústavní úrovni čl. 10 odst. 3 LZPS. Ustanovení § 180 obsahuje dvě samostatné skutkové podstaty.

První skutková podstata je vymezena v odst. 1 a chrání každého před neoprávněným zveřejněním, sdělením, zpřístupněním, jiným zpracováváním nebo přisvojením si osobních údajů shromážděných o jiném v souvislosti s výkonem veřejné moci.

Druhá skutková podstata v odst. 2 sankcionuje neoprávněné zveřejnění, sdělení nebo zpřístupnění třetí osobě osobních údajů získaných v souvislosti s výkonem povolání, zaměstnání nebo funkce pachatele, jestliže tím pachatel porušil státem uloženou nebo uznanou povinnost mlčenlivosti.

Požadavkem je v obou případech způsobení vážné újmy na právech nebo na oprávněných zájmech osoby, jíž se osobní údaje týkají a to i z nedbalosti.

Kybernetický prvek je vyjádřen v odst. 3, který zmiňuje mimo jiné veřejně přístupnou počítačovou síť jako účinný způsob spáchání dvou předchozích odstavců, což je chápáno jako okolnost zvlášť přitěžující. Zákonodárce k tomu vedla masové využívání elektronické komunikace a nakládání s osobními údaji v elektronické podobě. Bude zde možný jednočinný souběh tohoto trestného činu s trestným činem neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 TZ, neboť chrání jiné společenské zájmy.

§ 182 porušení tajemství dopravovaných zpráv

[53] § 4 písm. a) zákona 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů

Tento paragraf představuje ochranu, jejímž předmětem je tajemství dopravovaných zpráv dle článku 13 Listiny základních práv a svobod. Ne tedy tajemství písemností a záznamů chovaných v soukromí nebo již dopravených, na které článek Listiny též dopadá. Dále pak představuje naplnění povinnosti zákonodárce plynoucího z článku 3 úmluvy, nazvaného Neoprávněné zachycení.

Kybernetickým trestným činem je tento v první řadě dle ustanovení odst. 1 písm. b) a c) TZ, podle kterého je trestně odpovědný ten, kdo úmyslně poruší tajemství:
b) datové, textové, hlasové, zvukové či obrazové zprávy posílané prostřednictvím sítě elektronických komunikací a přiřaditelné k identifikovanému účastníku nebo uživateli, který zprávu přijímá, nebo c) neveřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému, přenášejícího taková počítačová data.

Účastníkem elektronické komunikace je každá osoba, která uzavřelas podnikatelem poskytujícím veřejně dostupné služby elektronických komunikací smlouvu na poskytování těchto služeb. Uživatelem pak každý, kdo využívá nebo žádá veřejně dostupnou služby elektronických komunikací. Sítí elektronických komunikací se rozumí přenosové systémy, popřípadě spojovací nebo směrovací zařízení a jiné prostředky, které umožňují přenos signálů po vedení, rádiem, optickými nebo jinými elektromagnetickými prostředky, včetně družicových sítí, pevných sítí s komutací okruhů nebo paketů a mobilních zemských sítí, sítí pro rozvod elektrické energie v rozsahu, v jakém jsou používány pro přenos signálů, sítí pro rozhlasové a televizní vysílání a sítí kabelové televize, bez ohledu na druh přenášené informace.[54]

Textovou zprávou je informace ve formě textu, tedy písmen, slov, vět. Typicky to bude případ Internetové komunikace v reálném čase (chat) pomocí programů jako ICQ, MSN, QUIP, FACEBOOK. Hlasová zpráva přenáší hlas člověka, to umožňují programy jako SKYPE, GOOGLE TALK. Zvuková zpráva je pojem nadřazený tomu předchozímu, zachycuje jakýkoliv zvuk. Obrazovou zprávou je myšlen obrazový záznam přenášený v síti elektronických komunikací, například fotografie, malba, video.
Porušením tajemství je pak jakékoli neoprávněné narušení posílané zprávy nebo neveřejného přenosu počítačových dat. Tajemstvím je zde chráněn jejich obsah.

[54] Srov. § 2 zákona č. 127/2005 Sb. ze dne 22. února 2005 o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)

Zdůrazňuji zde, že se musí jednat o zprávu dopravovanou, ne ještě doručenou, bez ohledu na to, zde se adresát s jejím obsahem seznámil či ne. Pro vznik trestní odpovědnosti pak pachatel nemusí rozumět sdělení této zprávy, pokud je například v jazyce, který neovládá.

Skutková podstata § 182 odst. 2 TZ stanoví, že je trestně odpovědný ten, kdo v úmyslu způsobit jinému škodu nebo opatřit sobě nebo jinému neoprávněný prospěch prozradí tajemství, o němž se dozvěděl z písemnosti, telegramu, telefonního hovoru nebo přenosu prostřednictvím sítě elektronických komunikací, který nebyl určen jemu, nebo takového tajemství využije.

Zde je předmětem ochrany již ono tajemství, obsah, ne pouze přepravovaná zpráva. Prozrazením tajemství se rozumí jeho sdělení třetí osobě. Jeho využitím je myšleno jeho uplatnění jiným způsobem, než právě prozrazením. Subjektivní stránka zde spočívá v úmyslu a to úmyslu přímém, neboť směřuje ke způsobení škody nebo opatření prospěchu.

Kybernetický prvek je dále v odst. 5, kde je kvalifikovaná skutková podstata, ve které je okolností zvlášť přitěžující jiná skutečnost rozvíjející znak subjektu, jímž je zde zaměstnanec provozovatele poštovních služeb, telekomunikační služby nebo počítačového systému anebo kdokoli jiný vykonávající komunikační činnosti, jestliže spáchá čin v odst. 1 nebo 2, jinému úmyslně umožní spáchat takový čin, nebo pozmění nebo potlačí písemnost obsaženou v poštovní zásilce nebo dopravovanou dopravním zařízením anebo zprávu podanou neveřejným přenosem počítačových dat, telefonicky, telegraficky nebo jiným podobným způsobem.

§ 183 porušení tajemství listin a jiných dokumentů uchovávaných v soukromí

Ustanovení tohoto paragrafu chrání tajemství listiny nebo jiné písemnosti, fotografie, filmu nebo jiného záznamu, počítačových dat anebo jiného dokumentu uchovávaného v soukromí. Na rozdíl od § 182 je zde ochrana poskytnuta těmto dokumentům již doručeným. Objekt je chráněn na ústavní úrovni článkem 13 Listiny. Z hlediska objektivní stránky zde o zveřejnění, zpřístupnění třetí osobě nebo použití jiným způsobem v odst. 1, nebo toto jednání v úmyslu získat pro sebe nebo pro jiného majetkový nebo jiný prospěch, způsobit jinému škodu nebo jinou vážnou újmu, anebo ohrozit jeho společenskou vážnost, jak je popsáno v odst. 2.

Z pohledu kybernetické trestné činnosti pak půjde narušení soukromí výše uvedených dokumentů uchovávaných na paměťových mediích, jako je zejména pevný disk počítače, přenosné USB záznamové nosiče (flash disky), informace zapsané na přenosných discích (CD, DVD, Blue-Ray). Typicky zde půjde o zprávy elektronické pošty, ale také SMS (krátké textové zprávy) uchovávané v paměti mobilního telefonu, soukromé fotografie, know-how podnikatelů a jiné dokumenty uchovávané v elektronické podobě.

K provedení spáchání tohoto trestného činu bude docházet zejména v jednočinném souběhu s trestným činem neoprávněného přístupu k počítačovému systému, kdy pachatel nejprve překoná bezpečnostní opatření počítačového systému právě za účelem nakládání se soukromými dokumenty.

§ 311 teroristický útok

Terorismus je jeden s nejnebezpečnějších a nejškodlivějších činů, který ohrožuje ústavní zřízení a obranyschopnost České republiky, demokratické principy, na nichž je republika založena, základní hospodářskou strukturu státu, jakož i zdraví obyvatel republiky. To tvoří objekt tohoto trestného činu.

Tohoto trestného činu se dopustí ten, kdo v úmyslu poškodit ústavní zřízení nebo obranyschopnost České republiky, narušit nebo zničit základní politickou, hospodářskou nebo sociální strukturu České republiky nebo mezinárodní organizace, závažným způsobem zastrašit obyvatelstvo nebo protiprávně přinutit vládu nebo jiný orgán veřejné moci nebo mezinárodní organizaci, aby něco konala, opominula nebo trpěla, zničí nebo poškodí ve větší míře telekomunikační systém, včetně informačního systému, což je jednání popsané v odst. 1 písm. c.[55]

Informačním systémem, který je důležitý z hlediska této práce, se rozumí funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost. Každý informační systém zahrnuje data, která jsou uspořádána tak, aby bylo možné jejich zpracování a zpřístupnění, provozní údaje a dále nástroje umožňující výkon informačních činností. Informační činností získávání a poskytování informací, reprezentace informací daty, shromažďování, vyhodnocování a ukládání dat na hmotné nosiče a uchovávání, vyhledávání, úprava nebo pozměňování dat, jejich předávání,

[55] Dle § 313 je ochrana poskytnuta též mezinárodním organizacím a cizímu státu

šíření, zpřístupňování, výměna, třídění nebo kombinování, blokování a likvidace dat ukládaných na hmotných nosičích. Informační činnost je prováděna správci, provozovateli a uživateli informačních systémů prostřednictvím technických a programových prostředků.[56]

Dle odst. 2 § 311 bude potrestán, kdo jednáním uvedeným v odst. 1 vyhrožuje, nebo kdo takové jednání, teroristu nebo člena teroristické skupiny finančně, materiálně nebo jinak podporuje.

§ 209 podvod

Podvod je jedním z typických klasických trestných činů, u kterého jeho spáchání pomocí informačních technologií představuje jen jeho specifickou formu spáchání. Objektem je zde cizí majetek a v jeho nelegálním získávání se v prostředí Internetu meze nekladou. V prostředí kyberprostoru pak vznikly četné podoby podvodů, z kterých několik pro ilustraci uvedu.

Takovým podvodem bude typicky nějaká podoba bankovního podvodu. Bankovní operace nyní využívají ve stále větší míře Internetu, což je činí zranitelnými. Nicméně hrozbou budou již samotní zaměstnanci bank, kteří mají přístup k účtům a mohou s nimi tak manipulovat, finanční prostředky zaokrouhlovat či si je převádět na vlastní účty. V době používání platebních karet je i tato možnost zneužívána, nazývá se anglickým „carding“. Souvisí zejména s nakupováním na Internetu. Zboží lze z počítače objednat a též zaplatit zadáním identifikačních údajů své karty. Toho může být zneužito zejména tak, že si prodejce strhne více, než mu za prodaný výrobek či službu náleží. Typem bankovního podvodu bude pak i „phishing“, o kterém pojednám v samostatné kapitole.

Za formu podvodu lze považovat i tzv. pyramidy, nebo letadla. Princip je získávání finančních prostředků na základě hierarchie, kdy výše postavení členové těchto skupin získávají více finančních prostředků než ti, kteří se zapojili do struktury později. V prostředí Internetu je pak nábor členů o poznání rychlejší.

[56] § 2 zákona č. 365/2000 Sb. ze dne 14. září 2000 o informačních systémech veřejné správy a o změně některých dalších zákonů

Podvodem jistě bude též spam Nigerijského typu, o kterém bude pojednáno též v samostatné kapitole.

Internet, jako v první řadě prostředí k provádění obchodů, je a bude stále více využíván k obohacování sebe nebo jiných uváděním jeho uživatelů v omyl nebo využíváním omylů nebo zamlčování podstatných skutečností. Pokud tak bude způsobena na cizím majetku škoda nikoliv nepatrná, bude naplněna skutková podstata §

4.4.2 Šíření závadného obsahu

4.4.2.1 Nakládání se zakázanými druhy pornografie

V dnešní informační společnost a digitalizace dala průchod masovému rozvoji a rozšíření šíření a jinému nakládání se zakázanými druhy pornografie, což na ni má zvláště negativní dopad a to zejména pokud se týče pornografie dětské. Pornografické dílo lze charakterizovat tím, že zvláště intenzivním a vtíravým způsobem zasahuje a podněcuje sexuální pud, překračuje podle převládajících názorů ve společnosti uznávané hranice sexuální slušnosti, uráží neakceptovatelným způsobem cit pro sexuální slušnost, vyvolává pocit studu.[57] Význam v této oblasti z hlediska kriminalizace a sjednocení právních úprav má i zde Úmluva. Ta v článku 9, který ukládá kriminalizovat jednání spočívající ve:

a)výrobě dětské pornografie pro účely její distribuce prostřednictvím počítačového systému

b)nabízení nebo zpřístupnění dětské pornografie prostřednictvím počítačového systému

c)distribuci nebo přenášení dětské pornografie prostřednictvím počítačového systému

d)obstarávání dětské pornografie pomocí počítačového systému pro sebe nebo pro jinou osobu

e)držbě dětské pornografie v počítačovém systému nebo na médiu pro ukládání počítačových dat.

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

Dále pak úmluva vykládá, že „dětskou pornografií“ se rozumí pornografické materiály, které zobrazují:

a)nezletilou osobu provádějící viditelný sexuální akt

b)osobu, jež vyhlíží jako nezletilá, provádějící viditelný sexuální akt,

c)realistické zobrazení nezletilé osoby provádějící viditelný sexuální akt.

Nezletilou osobou se pak rozumí osoba mladší 18 let, smluvní strany si však mohou stanovit nižší věkovou hranici, která však nesmí být nižší než 16 let.

Pod pojmem viditelný sexuální akt je třeba spatřovat tyto skutečné nebo simulované situace:

> a)pohlavní styk včetně styku genitálně-genitálního, orálně-genitálního, análně-genitálního nebo orálně-análního, mezi dětmi nebo mezi dospělým a dítětem téhož nebo opačného pohlaví; b)sodomie; c)masturbace; d)sadistické nebo sadomasochistické praktiky v sexuálním kontextu; e)necudné (lascivní) předvádění genitálu nebo pubické krajiny dítěte. Není rozhodné, zda je zobrazené chování skutečné nebo předstírané.[58]

Situace v České Republice proběhla několika změnami. Od roku 2007 byl změněn § 205. Jeho předchozí název „ohrožování mravnosti“ byl nahrazen novým a to „šíření pornografie“ a byly změněny také jeho znaky. Dále byly zavedeny trestné činy § 205a přechovávání dětské pornografie a 205b zneužití dítěte k výrobě pornografie. Tyto však nekriminalizovaly šíření pornografického díla, které zobrazuje osobu, jež se jeví být dítětem. Nyní se zakázané pornografie v kybernetickém kontextu týkají trestné činy popsané v § 192 a § 193.

§ 191 šíření pornografie

Odst. 1 chrání osoby starší 18 let před nežádoucími druhy pornografie. Kdo vyrobí, doveze, vyveze, proveze, nabídne, činí veřejně přístupným, zprostředkuje, uvede do oběhu, prodá nebo jinak jinému opatří fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, v němž se projevuje násilí či neúcta k

[58] Gřivna, T., Polčák, R. (eds.). Kyberkriminalita a právo. Praha: Auditorium, 2008.

člověku, nebo které popisuje, zobrazuje nebo jinak znázorňuje pohlavní styk se zvířetem, bude potrestán. Objektivní stránkou je tedy nakládání s násilnou či neuctivou pornografií a také zoofilní pornografií, které bývají označovány jako tvrdá pornografie.

Počítačovým dílem je dílo, které je zaznamenáno či zobrazeno pomocí počítače. Netvoří tedy samostatný druh, ale formu záznamu děl ostatních (např. filmové dílo zaznamenané v paměti počítače v elektronické podobě nebo na nosiči informací jako multimediální soubor s koncovkou .avi, .mpeg, .vaw, .mov apod., fotografie v podobě souboru s koncovkou .jpg, .jpeg, .bmp apod.). Může to být také počítačový program, který je chráněn jako dílo.[59] Půjde zde například o počítačovou hru. Pojem elektronického díla bude pojmem širším, neboť počítač je druhem elektronického zařízení, avšak ne všechna elektronická zařízení jsou počítače. Počítače nejsou jedinými technickými zařízeními schopnými zaznamenávat a přehrávat výše uvedené multimediální soubory s pornografickou tématikou. Pojem elektronického díla pak bude představovat ta díla, která jsou zaznamenávána v elektronické podobě na technickém zařízení schopném je uskladňovat či přehrávat, přičemž se však nejedná o počítač.[60]

V odst. 2 je druhá základní skutková podstata. Kdo písemné, fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo a) nabízí, přenechává nebo zpřístupňuje dítěti, nebo b) na místě, které je dětem přístupné, vystavuje nebo jinak zpřístupňuje, bude potrestán. Zde se tedy jedná o dovolenou pornografii, ale nakládání ve vztahu k dětem je kriminalizováno.

V odstavci třetím je spáchání činů v předchozích odstavcích prostřednictvím veřejně přístupné sítě, nebo obdobně účinným způsobem zvláště přitěžující okolností. Bude to zejména síť Internet.

§ 192 výroba a jiné nakládání s dětskou pornografií

Tento paragraf se již výlučně týká dětské pornografie. Dítětem se rozumí osoba mladší osmnácti let dle § 124 TZ, což je v souladu s Úmluvou.

[59] § 2 odst. 2 zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon)
[60] Blíže Volevecký, P. Kybernetické trestné činy v trestním zákoníku. Trestní právo č.7-8/2010

Odst. 1 zavazuje potrestat toho, kdo přechovává fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě. Volevecký se zamýšlí nad naplněním znaku „přechovávání“.[61]Klasickým způsobem přechovávání dat je na pevných discích, či CD, DVD apod. Data se již dají ale uchovávat i na Internetových úložištích dat a to mnohdy zcela zdarma. Takovými je například www.uloz.to, nebo www.rapidshare.com , které jsou hojně zneužívány. Otázkou pak je, zda i tzv. uploadování dětské pornografie na tyto servery se dá subsumovat pod pojem přechovávání. Dle mého názoru ano, není totiž podstatné, kde se nachází ono záznamové medium, ale že je má pachatel ve své dispozici.[62]

Trestné není prohlížení dětské pornografie. Na tu může uživatel Internetu náhodně narazit. Pokud si ji však neukládá na nosič informací, nelze trestnost dovodit. Takovým ukládáním není přechodné automatické ukládání webových stránek nebo jiných dat do vyrovnávací paměti počítače, jejich technické kopie (dočasné Internetové soubory) nebo vytváření tzv. cookies. Ani cílené a pravidelné prohlížení stránek s dětskou pornografií nebude trestné, návštěvník je nemá ve své dispozici.

Zákonodárce zde zřejmě učinil výhradu, kterou nabízí Úmluva a nekriminalizoval činy týkající se díla, které zobrazují osobu, jež se jeví být dítětem.

Další spornou otázkou je postih tzv. virtuální pornografie, nezobrazující reálné dítě (např. malba, obrázek, počítačem generovaný obrázek). Například Bartoň se domnívá, že zobrazování takového materiálu není trestní podle tohoto ustanovení.[63]Dle rámcového rozhodnutí Rady 2004/68/SVV je však dle článku 1 dětská pornografie definována jako pornografický materiál, který zobrazuje mimo jiné realistické znázornění neexistujícího dítěte, která se aktivně nebo pasivně účastní jednoznačně sexuálního jednání, a to včetně dráždivého vystavování přirození nebo ohanbí dítěte. Zde ale může působit problém, jak hodnotit onu realističnost, která je otázkou subjektivní.

[61] Volevecký, P. Kybernetické trestné činy v trestním zákoníku. Trestní právo č.7-8/2010
[62] podrobněji v Šámal, P. a kol. Trestní zákoník II. § 140 až 421. Komentář 1. Vydání. Praha : C. H. Beck, 2010, 1704 s.
[63] Bartoň M. Virtuální pornografie, limity svobody umělecké tvorby a svobody projevu a trestní zákon, Právní rozhledy č. 17/2008

Objektivní stránka pak ukládá potrestat toho, kdo vyrobí, doveze, vyveze, proveze, nabídne, činí veřejně přístupným, zprostředkuje, uvede do oběhu, prodá nebo jinak jinému opatří fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě, anebo kdo kořistí z takového pornografického díla. Zde se tak jedná o šíření dětské pornografie, srovnáním trestních sazeb za tento trestný čin a za šíření zakázané pornografie v § 191 odst. 1 pak odvodíme vyšší společenskou škodlivost šíření pornografie dětské.

4.4.2.2 Šíření obsahu, který podněcuje k nenávisti

§ 355 Hanobení národa, rasy, etnické nebo jiné skupiny osob

Toto ustanovení chrání základní lidská práva a klidné soužití proti veřejnému hanobení tak, jak to ukládá například Úmluva o odstranění všech forem rasové diskriminace.

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

„Hanobením“ je každé úmyslné snižování vážnosti. Může se projevovat v jakékoli formě, výslovně nebo zahaleně, tvrzením určitých skutečností nebo bez jejich uvádění; spadá sem i nadávka.[64] Kvalifikovanou skutkovou podstatou je pak způsob spáchání tohoto trestného činu veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem.

Z hlediska požadavku veřejnosti pak půjde zejména o vytváření internetových stránek, blogů, uveřejňování projevů a písní s výše popsaným jednáním.

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

Základním lidským právem, chráněným tímto ustanovením, je rovnost lidí.

[64] Srov R 2963/1927

Kdo veřejně podněcuje k nenávisti k některému národu, rase, etnické skupině, náboženství, třídě nebo jiné skupině osob nebo k omezování práv a svobod jejich příslušníků, bude potrestán. Z hlediska masového využívání moderních informačních a komunikačních technologií je i v tomto jednání kvalifikovanou skutkovou podstatou způsob spáchání tohoto trestného činu veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem.

§ 403 Založení, podpora a propagace hnutí směřujícího k potlačení práv a svobod člověka

I zde je chráněno lidské právo rovnosti lití bez rozdílu národnosti, příslušnosti k etnické skupině, rase, náboženství, třídě či jiné skupině osob. Tímto ustanovením je tak důvodně omezena svoboda projevu a svoboda sdružovací ve smyslu čl. 17 odst. 4 a čl. 20 odst. 3 LZPS.

Kdo založí, podporuje nebo propaguje hnutí, které prokazatelně směřuje k potlačení práv a svobod člověka, nebo hlásá rasovou, etnickou, národnostní, náboženskou či třídní zášť nebo zášť vůči jiné skupině osob, bude potrestán odnětím svobody na jeden rok až pět let. Zde již chybí onen znak veřejnosti, může se tak dít například pomocí elektronické pošty, či jinými způsoby elektronické komunikace. I zde je kybernetický prvek v kvalifikované skutkové podstatě, kde je tento čin spáchán veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem.

§ 407 Podněcování útočné války

Kdo veřejně podněcuje k útočné válce, na které se má podílet Česká republika, takovou válku propaguje nebo válečnou propagandu jinak podporuje, bude potrestán. Kvalifikovaná skutková podstata je zde shodná jako u předchozích. Chráněným zájmem zde bude mír mezi státy a ochrana České republiky. Pojem útočné války lze chápat ve smyslu agrese, jejíž definice byla podána rezolucí OSN v roce1974, podle níž je agresí použití síly státem proti svrchovanosti, územní celistvosti nebo politické nezávislosti jiného státu nebo jakýmkoli jiným způsoben neslučitelným s Chartou OSN. Je to například vpád nebo útok ozbrojených sil jednoho státu na území jiného státu, okupace jako důsledek takového vpádu, anexe s použitím síly, bombardování, apod. I takové

účinky tedy může mít používání počítačových systémů a sítí. Zpravidla půjde o vytváření webových stránek s propagujících tento druh agrese.

4.4.2.3 Šíření pomlouvačných a obviňujících sdělení

§ 184 pomluva

Objektivní stránka tohoto trestného činu spočívá ve sdělení nepravdivého údaje, který je způsobilý značnou měrou ohrozit jeho vážnost u spoluobčanů, zejména poškodit jej v zaměstnání, narušit jeho rodinné vztahy nebo způsobit mu jinou vážnou újmu. Sdělováním pravdivých údajů pak není pomluvou, bez ohledu na způsob, jakým tak bylo učiněno. Individuálním objektem pak je čest a dobrá pověst osoby. Spáchání tohoto veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem je i zde zvláště přitěžující okolností. Hojně se pomluvy vyskytují na diskusních fórech nebo sociálních sítích. Lze si však těžko představit stíhání těchto jednání vzhledem k faktu, že se z takových medií dají jejich uživatelem kdykoliv vymazat.

§ 345 křivé obvinění

I tento trestný čin lze označit jako kybernetický a to na základě kvalifikované skutkové podstaty, která přísněji postihuje pachatele, který křivě obviní veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem. Objektivní stránka spočívá ve lživém obvinění z trestného činu, popřípadě ve lživém obvinění z trestného činu v úmyslu přivodit jinému trestní stíhání. Lživě obvinit znamená nepravdivě tvrdit, že jiný se dopustil jednání, které naplňuje skutkovou podstatu trestného činu, tj. vědomě nepravdivě informovat o skutkových okolnostech, tedy o tom, kdy, kde a jak měl být trestný čin spáchán a kdo je jeho pachatelem. Musí směřovat vůči určité osobě.[65]

4.4.2.4 Šíření toxikomanie

§ 287 šíření toxikomanie

Objektem zde je zájem na ochraně společnosti a lidí, které v sobě skýtá zneužití návykových látek. Kdo svádí jiného ke zneužívání jiné návykové látky než alkoholu nebo ho v tom podporuje anebo kdo zneužívání takové látky jinak podněcuje nebo šíří,

[65] Šámal, P. a kol. Trestní zákoník II. § 140 až 421. Komentář 1. Vydání. Praha : C. H. Beck, 2010, 2954s.

bude potrestán. Přísněji potrestán bude ten, kdo toto spáchá veřejně přístupnou počítačovou sítí. V úvahu zde přicházejí opět diskusní fóra, chaty, aplikace FACEBOOK, internetové stránky.

4.4.3 Porušování autorských práv a práv souvisejících

Na tomto místě zmíním jen trestný čin § 270 Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi, který na toto jednání dopadá. Podrobnější výklad nabídnu v kapitole 6 této práce, kde se na toto téma zaměřím.

4.4.4 Nakládání se zařízením k páchání kybernetické trestné činnosti

Zařazení následujících skutkových podstat trestných činů je implementací článku 6 Úmluvy. Charakteristické pro ně je, že jsou to jednání přípravná k dalšímu páchání kybernetické kriminality a že byly povýšeny na dokonané trestné činy. Ukládá kriminalizovat výrobu, prodej, obstarání k užívání, dovozu, distribuci nebo jiném zpřístupnění nebo držení

> a) zařízení, včetně počítačového programu, určeného nebo přizpůsobeného primárně pro účely spáchání kteréhokoli trestného činu stanoveného v souladu s články 2 až 5 Úmluvy
>
> b)počítačového hesla, přístupového kódu nebo podobného údaji, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části.

Je však výslovně omezena trestní odpovědnost v případech tohoto jednání, které nesleduje účel spáchání trestných činů čl. 2 až 5, jako je tomu například v případě oprávněného testování nebo ochrany počítačového systému. Český TZ obsahuje od počátku roku 2010 následující skutkové podstaty:

§ 231 opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat

Objektem tohoto trestného činu je zájem na ochraně společnosti a osob před možným ohrožením vyplývajícím z nekontrolovaného opatření a přechovávání zařízení, nástrojů a prostředků, jež primárně slouží k spáchání trestných činů porušení dopravovaných zpráv podle § 182 odst. 1 písm. b), c) nebo trestný čin neoprávněného

přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1, 2.[66] Tohoto trestného činu se tak dopustí ten, *kdo vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části, nebo*

b) počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části a to v úmyslu spáchat výše uvedené dva trestné činy, které odpovídají těm uvedeným v článcích 2 až 5 Úmluvy. Bez tohoto specifického úmyslu tedy takové jednání trestné není.

Můžeme tedy rozlišit prostředky vytvořené nebo přizpůsobené k páchání výše popsané kybernetické kriminality, nebo prostředky, které slouží k legálnímu přístupu k počítačovému systému, ale pachatel s nimi neoprávněně nakládá.

§ 234 neoprávněné opatření, padělání a pozměnění platebního prostředku

Toto ustanovení chrání platební prostředky a to jak tuzemské, tak zahraniční. Tento paragraf byl do trestního zákoníku zařazen na základě Rámcového rozhodnutí Rady Evropské unie č. 2001/413/JVV o boji proti podvodům a padělání v oblasti bezhotovostních platebních prostředků. Jde tu o řádné fungování platebního styku, který probíhá pomoví hotových peněz[67], ale z převažující části dnes již bezhotovostními převody. Ty zajišťují pro své klienty zejména banky[68] pod dohledem České národní banky. Za platební prostředky bývají považovány platební karta, elektronické peníze, příkaz k zúčtování, cestovní šek, záruční šeková karta, šek, směnka, dokumentární akreditiv, dokumentární inkaso. Také se sem řadí homebanking, umožňující spravovat svůj účet z pohodlí domova, nebo pomocí telefonu.

Dle odst. 1 bude potrestán ten, kdo sobě nebo jinému bez souhlasu oprávněného držitele opatří, zpřístupní, přijme nebo přechovává platební prostředek jiného. Nevyžaduje se tedy použití takového prostředku ani pokus tohoto.

---

[66] Šámal, P. a kol. Trestní zákoník II. § 140 až 421. Komentář 1. Vydání. Praha : C. H. Beck, 2010, 2097-8s.

[67] Kterými jsou bankovky, státovky, mince

[68] Převody peněz zajišťují též nebankovní instituce jako PayPal, Moneybookers, Neteller, apod.

Dle odst. 2, a zároveň druhé samostatné skutkové podstaty, bude potrestán ten, kdo opatří, zpřístupní, přijme nebo přechovává padělaný nebo pozměněný platební prostředek.

Dle odst. 3 je trestně odpovědný ten, kdo padělá nebo pozmění platební prostředek v úmyslu použít jej jako pravý, respektive kdo takový prostředek jako pravý použije.

Tyto možnosti bývají k důvěřivosti uživatelů zneužívány metodou nazývanou jako phishing, o kterém pojednám později.

§ 236 výroba a držení padělatelského náčiní

I toto ustanovení chrání platební prostředky a to jak tuzemské, tak zahraniční a bylo uvedeno do trestního zákoníku na základě Rámcového rozhodnutí 2001/413/JVV. Je tak zavedena trestní odpovědnost za nakládání s nástroji, zařízením, součástí zařízení, postupem, pomůckou, nebo jakýmkoliv jiným prostředkem, a to včetně počítačového programu, který je vytvořený nebo přizpůsobený k padělání nebo pozměnění peněz nebo prvků sloužících k ochraně peněz proti padělání anebo vytvořený nebo přizpůsobený k padělání nebo pozměnění platebních prostředků.

§ 348 padělání a pozměnění veřejné listiny

Objektem je zde zájem na řádném a zákonném chodu státního aparátu a důvěra v pravost a pravdivost veřejných listin. Veřejnou listinou se rozumí listina vydaná soudem České republiky, jiným orgánem veřejné moci nebo jiným subjektem k tomu pověřeným či zmocněným jiným právním předpisem v mezích jeho pravomoci, potvrzující, že jde o nařízení nebo prohlášení orgánu nebo jiného subjektu, který listinu vydal, anebo osvědčující některou právně významnou skutečnost. Veřejnou listinou je i listina, kterou prohlašuje za veřejnou jiný právní předpis.[69] Je to například občanský průkaz, živnostenský list, koncesní listina. Jsou jimi i listiny naplňující uvedené znaky, které se uchovávají v elektronické podobě, to dává prostor k jejich padělání, pozměňování. Ustanovení tohoto paragrafu tak postihuje padělání a podstavnou změnu v úmyslu užití nebo užití jako pravou. Dále pak opatření, přechovávání v úmyslu užití jako pravé. I zde je ustanovení o nakládání s prostředkem to umožňujícím.

4.4.5 Kybernetické pronásledování

§ 354 nebezpečné pronásledování

[69] Dle § 131 trestního zákona

Nebezpečné pronásledování bývá zahraniční literaturou označováno jako stalking, pokud je spojeno s informačně komunikačními technologiemi, pak se nazývá cyberstalking. Objektem tohoto trestného činu je, jak vyplývá z jeho systematického zařazení v trestním zákoníku, ochrana nerušeného soužití mezi lidmi. Z hlediska objektivní stránky zde jde o dlouhodobé pronásledování jiného tím, že pachatel:

a)vyhrožuje ublížením na zdraví nebo jinou újmou jemu nebo jeho osobám blízkým,

b)vyhledává jeho osobní blízkost nebo jej sleduje,

c)vytrvaleji prostřednictvím prostředků elektronických komunikací, písemně nebo jinak kontaktuje

d)omezuje jej v jeho obvyklém způsobu života,

e)zneužije jeho osobních údajů za účelem získání osobního nebo jiného kontaktu,

přičemž takové pronásledování je způsobilé vzbudit v poškozeném důvodnou obavu o jeho život nebo zdraví nebo o život a zdraví osob jemu blízkých.

Takové jednání bývá motivováno nenávistí, nebo naopak patologickou náklonností, pomstou, apod. Hranice sociální akceptovatelnosti lze bývá jen těžko stanovitelná, tedy až na extrémní případy několikaletého ustavičného pronásledování. Způsoby stalkingu mohou být naprosto legální, jako například kontaktování osoby e-mailem, nebo naopak již jednotlivé jednání může výt v rozporu se zákonem, typicky u vyhrožování.

Znak dlouhodobosti bude znamenat přinejmenším několik vynucených kontaktů nebo pokusů o ně a zároveň musí být způsobilé vyvolat důvodnou obavu. Z klinického hlediska jsou pod stalking zahrnovány jen takové způsoby pronásledování, které představují opakované, trvající nechtěné navazování kontaktů s obětí za použití násilí nebo jiných srovnatelných praktik, přičemž se zde opakováním rozumí více než 10 pokusů o kontakt, trvajícím obdobím pak minimálně doba 4 týdnů.[70]

Pod písmenem c) tedy možno spatřovat různé formy kontaktování a to pomocí e-mailu, SMS, MMS, zveřejňování intimních údajů a záznamů o oběti, také zasílání malwaru, využívání celého spektra elektronické komunikace, které jsou k dispozici, včetně samozřejmě telefonních hovorů.

[70] podrobněji v Šámal, P. a kol. Trestní zákoník II. § 140 až 421. Komentář 1. Vydání. Praha : C. H. Beck, 2010, 3008 s.

4.5 Úvahy de lege ferenda

Budeme-li uvažovat o budoucím vývoji kybernetické kriminality, lze předpokládat, že jí bude přibývat stejnou rychlostí, s jakou bude pokračovat rozvoj informačních a komunikačních technologií. To je třeba mít neustále na paměti a neustále tak sledovat vývoj probíhající v tomto oboru.

Při hodnocení právního stavu práva České republiky bych shrnul, že trestní zákon poskytuje ultima ratio potřebnou právní ochranu společenským zájmům souvisejícím s využíváním počítačových systémů a Internetu a promítá tak do našeho právního řádu četné závazky, které vyplývají z mezinárodního práva. Trestní zákon je v souladu s Úmluvou o kybernetické kriminalitě a v mnohých případech jde dokonce nad rámec. Nevidím však jediný důvod, kvůli kterému jí Česká republika zatím neratifikovala.

Dle mého názoru by měl být kladen důraz zejména na postihování kybernetické kriminality ve vztahu k dětem, tedy § 191, § 192, §193. Újma na mravním vývoji dítěte, která zde hrozí, je o mnoho závažnější a tato jednání o to škodlivější, než jakákoliv újma materiální. Doporučoval bych tedy v rámci prevence vyšší trestní sazby u těchto skutkových podstat.

Dále bych upozornil na důležitost dodržování práv a svobod uživatelů Internetu a ostatních komunikačních technologií v souladu s evropskými a mezinárodními standardy. Mezinárodní dohody týkající se lidských práv musí dopadat na prostředí kyberprostoru ve stejném měřítku, jako na aktivity nevyužívající informační technologie. Počítačové systémy jsou totiž hojně využívány k nezákonným sledováním a odposlechům jak na poli politickém, tak soukromém. Využívány jsou sociální sítě, mobilní telefony, hardwarové i softwarové prostředky.

Je tedy třeba podněcovat mezinárodní diskusi a legislativní aktivity směřující k ochraně společenských zájmů, které jsou narušovány prostřednictvím kybernetického prostoru, zejména sjednocovat terminologii, hledat společné cíle a provádět je pomocí národní legislativy. Tu je pak nutno náležitě aplikovat ve světle evropského a mezinárodního práva.

5 Způsoby páchání kybernetické kriminality

Odhlédněme nyní od právní kvalifikace kybernetických trestných činů a zaměřme se na toto jednání z odborné, technické stránky věci. Následují nejtypičtější způsoby páchání kybernetické trestné činnosti, které naplňují skutkové podstaty výše popsaných trestných činů.

5.1 Hackerství

5.1.1 Pojem hacking

Termín „hacking“ (neboli česky hackerství) byl zřejmě převzat z angloamerického žargonu jezdců na koních, kdy se jím označovala vyjížďka bez zřejmého cíle.[71] Je to ovšem jen jedno z více možných výkladů.[72] V roce 1960 byl tento pojem použit poprvé a za hackera byl považován „opravdový programátor“, ten, kdo plně ovládl počítačové systémy a byl schopen je pozměnit k tomu, aby prováděli více nebo něco jiného, než k čemu byly původně určeny.[73] Pojem byl poprvé použit na MIT (Massachusettský Institut Technologie). Nebylo to tedy nic nezákonného. Hacker, který prováděl onu činnost v úmyslu škodit, byl nazýván pojmem cracker. Dnes se, i když formálně nesprávně, používá pojem hacker v pejorativně, zčásti kvůli masovým sdělovacím prostředkům. Hackerství je dnes, z hlediska počítačové bezpečnosti, považováno na nejznámější a nejvýraznější typ počítačové a internetové kriminality, proto jej uvádím na prvním místě. Znamená pronikání do počítačových a jiných elektronických systémů cestou nikoli předpokládanou, ale naopak obejitím nebo prolomením bezpečnostního systému. Může mít rozličné motivy a důsledky lišícími se podle osoby pachatele, cíle, který svým jednáním sleduje a mnohdy může být jen bránou k páchání jiné nelegální činnosti.

5.1.1 Typologie hackerů:[74]

White hats:[75] Tento hacker prolamuje bezpečnostní opatření z nezlomyslných důvodů, za účelem rozšíření odborných znalostí, poznání, nikoliv za účelem způsobení

[71] Jirovský, V. Kybernetická kriminalita (nejen o hackingu, crackingu, virech a trojských koních bez tajemství). Praha: Grada 2007
[72] Srov. Matějka, M. Počítačová kriminalita, Praha: Computer Press, 2002, s. 20
[73] Shinder, D. L. Scene of Cybercrime, computer forensics handbook, 2002
[74] Wikipedia, http://en.wikipedia.org/wiki/Hacker_(computer_security)

škody. Lze je považovat za hackery v původním slova smyslu, dodržují hackerskou etiku. Někteří, nazýváni „Samurajové“ se nabourají do systému a následně to oznámí jeho správci a navrhnou způsob záplaty bezpečnostní díry. Někdy jsou dokonce za tímto účelem najímáni. To pak není postihováno trestním právem.

Black hats: Jsou to právě oni hackeři, kteří toto jednání nepůsobí v dobré víře. Jejich nelegální aktivita pak může spočívat ve vandalství, tedy poškozování, ničení, překažení práce a úsilí někoho jiného v kyberprostoru. Jiné zneužití přístupu může mít projev v stalkingu, což je případ Internetového obtěžování, pronásledování.

Gray hats: Ti jsou kombinací předchozích hackerů. Mohou prolomit ochranu Internetového serveru, oznámit to administrátorovi a požadovat za to, nebo za nápravu odměnu.

Hacktivisté: Takto jsou označováni hackeři, kteří využívají technologie k prosazování ideologických, náboženských nebo politických poselství. Mohou za tímto účelem pozměňovat Internetové stránky nebo znemožnit jejich funkčnost. K nejzávažnějším případům dochází při kyberterorismu.

Sami hackeři se člení na: rodents (hacking pro ně znamená hru a intelektuální výzvy bez movitu zisku), swappers (využívají hacknuté počítačové systémy k provozování her a výměně informací), crackers (využívají informace získané o slabém bezpečnostním místě počítačového systému, sítě, příp. softwaru k osobnímu prospěchu), carders a travers (jediným motivem hackingu je zisk).[76] Také se sem řadí i skript kiddies (lamers, loosers), kteří využívají nástroje k prolamování bezpečnostních opatření, které sami nevytvořili, nemají k tomu potřebné znalosti. Také se pod pojem hacker může vyjadřovat i příslušnost k určitému myšlenkovému, či dokonce filosofickému směru.[77]

Hackery přitom bývají většinou muži, což plyne ze zahraničních statistik. Důvodem pro to bývají frustrace mladých chlapců, hledajících cesty pro své sklony k dominanci, jako náhražka sexuality. Jiný názor to zdůvodňuje jednoduše faktem, že ženy tolik nezajímá technická dokonalost.

---

[75] „hat“ z anglického klobouk. Kybernetický prostor bývá metaforicky přirovnáván k divokému západu, kde se rozlišovalo mezi těmi hodnými kovboji, nosící bílé klobouky a mezi těmi zlými, kteří měli klobouky černé.

[76] Kuchta, J., Válková, H. a kol. Základy kriminologie a trestní politiky. Praha: C.H.Beck, 2005, s 509

[77] Srov.např. Hackerův manifest z roku 1996, Blankenship,L. dostupné z WWW na: http://www.soom.cz/index.php?name=recenze/show&aid=286

5.1.3 Kazuistika

Uveďme na tomto místě jeden konkrétní případ na demonstraci dopadů hackingu. Případ Citibank je nejznámějším a zároveň prvním bankovním podvodem provedeným pomocí sítě Internet. V roce 1994, Ruský hacker Vladimír Levin převedl peněžní prostředky od klientů banky na účty své a svých kompliců v několika zemích, k čemuž využil bezpečnostních mezer systému banky, kterými získal přístupová hesla k dotčeným bankovním účtům. Přesný způsob získání přístupu do něj nebyl odhalen, spekulovalo se o spolupachateli z řad zaměstnanců banky. Převedeno bylo 10 milionů dolarů. Tři Levinovi pomocníci byli dopadeni při výběru svých částek a pomocí jejich výslechů byl určen i jeho pobyt Sankt Petrsburku. Dopaden byl nakonec na Londýnském letišti Heathrow v roce 1995 a po extradičním řízení byl vydán do Spojených Států. Tiskem byl označen za genia, který stál za prvním Internetovým bankovním podvodem. Někteří bezpečnostní znalci však tvrdí, že použil telekomunikačních systémů a ne Internetu, že byl schopen zachytit telefonické hovory a vyťukávání jejich čísel účtů a PINů. Banka získala, kromě 400.000 amerických dolarů, peníze zpět, Levin byl odsouzen k třem letům odnětí svobody a bylo mu nařízeno zaplatit bance Citibank 240.000 amerických dolarů.[78]

Na důkaz aktuálnosti tématu práce se nabízí kauza společnosti Sony, která je na rozdíl od případu Citibank nejnovějším „úspěchem“ hackerů a též demonstrací zranitelnosti počítačových systémů a sítí. Ve středu 20. 4. 2011 byla z důvodu hackerského útoku odstavena z provozu on-line herní síť PlayStation Network, která zajišťuje přístup k online hraní a přístupu k multimediálním službám Sony na zařízení PlayStation 3 .79 Až po šesti dnech společnost důvod vypnutí sítě oznámila veřejnosti, čehož důvodem mohlo být dle médií zejména představení nového druhu výrobků společnosti Sony krátce před oznámením, tedy marketingový tah. Toto zpoždění vystavilo Sony kritice ze strany uživatelů sítě i zbytku veřejnosti. Společnost se hájí náročností vyšetřování tohoto útoku. Podle analytiků jde o jeden z nejrozsáhlejších nezákonných zásahů do soukromých dat na internetu vůbec. Hackeři ukradli ze 77 milionů zákaznických účtů v síti různá osobní data, mezi kterými mohou být vedle jmen, dat narození, adres a e-mailů také informace o kreditních kartách. Uživatelům

[78] Frontline, http://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/notable.html
[79] PCWorld, Dostupné z WWW:http://pcworld.cz/novinky/sony-priznava-ze-hackeri-ukradli-citliva-data-uzivatelu-konzoli-ps3-20180

bylo doporučeno zkoumat výpisy ze svých bankovních účtů, a aby si ihned vyměnili své kreditní karty, změnili datum použitelnosti, CCV[80] čísla. Zajímavostí je, že útok na Sony byl slibován hackerskou komunitou Anonymous, jako reakce na kauzu, která se týkala prolomení ochrany herní konzole PlayStation3.[81] Téměř 90 procent z uživatelů PlayStation Network se na síť připojovalo z Evropy či Spojených států a potíže Sony by mezi nimi mohly vyvolat zájem o konkurenční herní systémy Wii od společnosti Nintendo a Xbox 360 od Microsoftu. Důsledkem však již dnes je ztráta důvěryhodnosti společnosti Sony a otázka, zda bude síť, která propojuje ji a uživatele herních konzolí, znovu spuštěna a za jakých bezpečnostních opatření.

5.1.4 Modus operandi hackingu

Hacking je v praxi prováděn rozličnými způsoby, literatura uvádí, že jich je více než 50.[82] Pachatel si samozřejmě nejprve zjistí veškeré dostupné informace o systému jeho oběti a o oběti samotné, aby měl dostatek podkladů pro výběr nejúčinnějšího způsobu provedení svého útoku. Navštíví internetovou stránku oběti, telefonickými hovory pod záminkou získání zaměstnání zjišťuje potřebné údaje, zjišťuje, které bezpečnostní systémy jeho potencionální oběti používají. Nabídnu nyní alespoň některé z nich, ty nejběžněji využívané:

Prolamování hesel: Tak se označuje způsob, kde hacker zkrátka získá nějakým způsobem přístupové heslo a tak i přístup do systému. Při dostatečném množství informací o oběti lze heslo odhadnout způsobem pokus omyl, pokud jej například tvoří jméno někoho blízkého nebo datum narození. Chybou uživatelů je též ponechávání tzv. defaultního hesla, tedy hesla přednastaveného pro všechny produkty a aplikace od toho kterého výrobce, dokud nejsou změněny uživatelem. Existují ovšem programy, které využívají metody brute-forcing.[83] Tato metoda spočívá ve vyzkoušení postupně všech možných kombinací písmen, čísel a znaků. To lze kombinovat s využitím seznamů slov, frází, písmen, čísel a symbolů, které uživatelé často používají jako hesla. Metod získání přístupů je více a není potřeba zde zacházet do technických podrobností.

---

[80] CCV číslo bezpečnostní kód, který se používá při internetových platbách. Je to obdoba PINU, který je nutný k výběru hotovosti z bankomatu.

[81] Idnes Bonusweb, Dostupné z WWW: http://bonusweb.idnes.cz/magazin/hackeri-ukradli-data-milionu-lidi-blokujte-kreditni-karty-radi-sony-11j-/clanek.A110427_142142_bw-magazin_oz.idn

[82] Srov. Madliak, J., Mihaĺov, J., Porada, V., Štefanková, S. Počítačová kriminalita. In Karlovarská právnická revue 1/2008

83 Symantec, Dostupné z WWW: http://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password

Keylogging: Metoda keyloggingu, nebo chceme-li Česky odposlouchávání klávesnice, je činnost vedoucí ke zjištění stisknutých kláves na klávesnici a to způsobem skrytým před osobou klávesnici používající. Může se jednat o klávesnici počítačovou, ale též tu u bankomatu nebo jiného přístroje. Pro účely hackingu bude tato metoda využívána zpravidla k získání přístupového hesla, kdy hacker zjistí, které klávesy byly stisknuty, případně v jakém pořadí. Rozpoznáváme keylogging softwarový, což je odposlouchávání pomocí programu, který je umístěn v počítači, ze kterého hodláme odposlouchávat, a který je nainstalovaný způsobem, aby nebyl při běžném používání počítače odhalitelný. Dá se tedy zahrnout pod pojem spyware (druh malwaru, jak bude vylíčeno níže v této práci). Druhým typem je hardwarové odposlouchávání, které lze realizovat například pomocí zařízení vloženého mezi klávesnici a počítač. To vypadá jako součást kabelu připojující klávesnici a dokáže do své paměti zaznamenávat veškeré stisky kláves. Nebezpečím je možnost jeho vizuálního odhalení.[84]

Skenování portů: Hacker zjistí, které porty (neboli vstupní/výstupní) na konkrétním počítači jsou otevřené a tím pádem zranitelné a dovolující přístup k počítači, popřípadě který program či služba port využívá, což vede k získání cenných informací o dírách v bezpečnosti počítačového systému a umožní tak vybrat nejvhodnější možnost dalšího postupu.

Sociální inženýrství: To je charakterizované jako „umění a věda přesvědčení lidí ke splnění vašich požadavků“.[85] Hacker tak použije psychologické triky a přirozené lidské tendence důvěřovat k získání potřebných informací (hesel) k získání přístupu do systému. Může tak učinit osobně, častěji však po telefonu. Tato metoda je založena na specifických způsobech lidského rozhodování známých jako kognitivní chyby úsudku, které jsou založeny na nedokonalosti lidského mozku.

SQL injection: Tak se označuje typ útoku, kde hacker využívá možnosti internetových dotazníků či ukládání informací do databáze serveru, na kterém se internetová stránka nachází. Hacker pak vloží svůj škodlivý kód do svého dotazu a zanese jej tak do databáze poskytovatele.

---

[84] Blíže v Swiatek, D. Metody odposlouchávání klávesnice, bakalářská práce, 2010, Dostupné z WWW: http://dspace.knihovna.utb.cz/bitstream/handle/10563/13694/swiatek_2010_bp.pdf?sequence=1

[85] Symantec, Dostupné z WWW: http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics

Buffer overflow: Tento způsob lze přeložit jako přetečení zásobníku. Tento zásobník je jakýsi úložný prostor pro data. K urychlení výkonu počítače, mnoho programů používá tento zásobník k ukládání změn, poté jsou informace ze zásobníku kopírovány na pevný disk. Když je na zásobník uloženo více, než je schopný udržet, nastane ono přetečení. To může být způsobeno záměrně hackery. Důsledkem může být způsobení nefunkčnosti aplikace, což však hackerovi neumožní proniknout, nebezpečněji to však může vést k vkládání škodlivých kódů do počítačových systémů.[86]

Cross site scripting: Zkráceně je toto jednání označováno jako XSS a znamená skriptování mezi sítěmi. Většina dnešních webových stránek má dynamický obsah, což je činí pro uživatele více atraktivní a právě tyto stránky obsahují XSS. Tento obsah se může chovat a zobrazovat se odlišně v závislosti na nastavení a potřebách uživatelů. To znamená, že webová stránka jako taková nemá kontrolu nad tím, jak se uživateli zobrazí. Pokud je tedy nežádoucí obsah vložen do dynamických stránek, tak webová stránka ani uživatel to nemusí rozpoznat, což je hackery hojně využíváno. Zejména k vkládání nežádoucího vkládání obsahu na cizí stránky, například reklam, nebo přesměrovávání uživatelů na stránky jiné.

Packet Sniffing: Packet znamená balíček nebo svazek a sniffing znamená čichání, čmuchání. K této metodě jsou používány speciální programy, tzv. sniffery, které zachycují ony balíčky jako bloky informací posílané pomocí informačních sítí. Tímto způsobem je možné zachytit citlivé informace, nebo přenášená hesla. Což může vytvářet mnohá bezpečnostní rizika.[87]

Botnety: Tato metoda je z následujících důvodů jak hardwarovou, tak softwarovou. Volně se do Češtiny pro překládají jako zombie. Jsou to systémy jednotlivých botů, neboli softwarových robotů, které se vyskytují bez vůle a kontroly napadených systémů autonomně tak, že tvoří sítě počítačů, které jsou do jisté míry kontrolovány třetí osobou, hackerem. To pak slouží k dalším postupům jako např. k anonymnímu připojení k Internetu, zasílání škodlivých programů, útoky na další cíle.[88]

Rootkity: Rootkit je program, který se snaží zamaskovat vlastní přítomnost počítači, popř. přítomnost jiných aplikací v počítači a to zejména virů a ostatního

[86] Shinder, D. L. Scene of the Cybercrime: Computer Forensics Handbook, Syngress Publishing, 2002
[87] Volevecký, P. Kybernetické hrozby a jejich trestně právní kvalifikace. Trestní právo č.1/2011
[88] Volevecký, P. Kybernetické hrozby a jejich trestně právní kvalifikace. Trestní právo č.1/2011

malwaru.[89] Mohou být však využity k jiným účelům, jak ukázala aféra společnosti Sony BMG Music Entertainment, která v roce 2005 začala umísťovat na jí vydávané disky programy, které se bez vědomí uživatelů instalovaly do počítače uživatele a bránily kopírování disků a vytváření z nich mp3. Bylo tak ve své podstatě rootkity a Sony musela čelit skandálu a četným žalobám.

Backdoors: Jsou to v překladu zadní vrátka, což výstižně vystihuje charakter jejich činnosti. Jsou to kódy, které po instalaci na cílový počítač umožňují jeho vzdálené řízení. Jakmile tedy hacker objeví bezpečnostní díru, pravidelně nainstaluje backdoors. Pomocí takto napadeného stroje pak může podnikat další útoky na cílový stroj, vytvořit tak řetěz mezi strojem hackera cílovým strojem.[90]

Po získání přístupu a provedením útoku hacker, pokud zrovna nepůjde o vandalismus, zahlazuje stopy tak, aby nebyl odhalen, bezpečnostní mezera odstraněna a aby mohl případně vniknutí opakovat.

5.2 Phreaking

Pod pojmem phreaking rozumíme zneužívání telekomunikačních služeb, tj. využívání telefonních linek, bez zaplacení provozovateli.

Toto jednání je vlastně předchůdcem hackingu a bylo vynalezeno Johnem Draperem, který získal svůj věhlas a slávu tím, že jako průkopník hackingu používal dětskou hračku. V 60. letech minulého století našel v krabici od cereálií píšťalku, která vydávala zvuk o frekvenci, která byla shodná s frekvencí používanou telefonními linkami k signalizaci, že tato linka je aktivní. Draper tak vytočil telefonní číslo a v průběhu vyzvánění vyslal tón o té konkrétní frekvenci, aby signalizoval status linky. Imitací konkrétního tonu přiměl telefonní systém, aby si myslel, že již zavěsil. Byl odhalen poskytovatelem jeho telefonních služeb na základě nesrovnalostí v jeho účtech. Vyšetřování a stíhání Drapera trvalo dlouho, protože to bylo poprvé v historii, kdy se právní systém setkal s takovýmto druhem podvodu. John Draper byl nakonec odsouzen ke dvěma měsícům vězení. Dal ovšem podnět ke zrodu hnutí okolo phreakingu, výrobě tzv. věčných čipových telefonních karet, „napíchnutí“ telefonních ústředen či pouličních automatů, ale také k neoprávněnému přístupu k síti Internet.

[89] Rootkit, Dostupné z WWW: http://rootkit.cz/go.php
[90] Blíže Jirovský, V. Kybernetická kriminalita (nejen o hackingu, crackingu, virech a trojských koních bez tajemství). Praha: Grada 2007

Trestně právně je toto jednání možno podřadit pod § 209 TZ neboli podvod. Pachatel totiž uvádí provozovatele sítě v omyl ohledně identifikace uživatele. K tomu je tedy potřeba, aby způsobil poskytovateli škodu nikoliv nepatrnou, tedy vyšší než 5000 Kč.

5.3 DoS útoky

DoS je zkratkou anglického „Denial of Service“, neboli potlačení služby. Útoky s cílem potlačení služby (nebo také odepření služby) tedy vyřazují technické zařízení z provozu, nebo tento alespoň omezují. Tento útok je realizován zahlcením napadeného počítače pomocí opakujících se požadavků na úkony, které má počítač vykonat, dále může též být realizován zahlcením informačních kanálů mezi serverem a počítačem uživatele či zahlcením volných systémových prostředků. Systém napadený DoS útokem se projevuje zejména neobvyklým zpomalením služby, nedostupností části nebo celých webových stránek, extrémním nárůstem spamu apod.[91] K nejznámějším metodám DoS útoku patří zejména:[92]

Zahlcení odesíláním paketů z více strojů, neboli DDoS útok (z anglického distributed denial of service, distribuované odepření služby). Spočívá to v zasílání těchto balíků dat z více počítačů tak, aby byla převýšena přenosová kapacita kanálu cílového počítače, který se tak stane nepoužitelným.

Zahlcení příkazem ping (packet Internet groper), kterým se možné zjistit existenci počítače s danou IP adresou a detekci času odezvy takového počítače. Jestliže je na adresu sítě zaslaný tento příkaz s podvrženou adresou cílového počítače, všechny počítače sítě odpovídají na tento příkaz právě cílovému počítači. Při opakování příkazu ping pak dochází k zahlcení takového počítače.

Zahlcení volných systémových prostředků (SYN-Flood). Zasíláním paketů SYN, což jsou pakety používané pro sestavení spojení v protokolu TCP. Systém, který obdrží paket SYN, odešle odpověď a čeká na potvrzení spojení. Tento čas čekání může dosahovat až několika minut, pokud je tedy odesláno větší množství těchto paketů, vyčerpá volné systémové prostředky a cílový stroj se stane nepřístupným.

[91] Volevecký, P. Kybernetické hrozby a jejich trestně právní kvalifikace. Trestní právo č.1/2011
[92] Jirovský, V. Kybernetická kriminalita (nejen o hackingu, crackingu, virech a trojských koních bez tajemství). Praha: Grada 2007

Toto jednání by se dalo podřadit pod skutkovou podstatu § 228 TZ, poškozování cizí věci za podmínek, že by byl počítač poškozen nebo by byl učiněn neupotřebitelným a zároveň byla způsobena škoda nikoliv nepatrná.

5.4 Spamming

5.4.1 Pojem Spammingu

Tento výraz byl v prostředí informačních sítí tu a tam používán ve významu jako plané řeči nebo kecy, hackeři pak jako spamming označovali techniku, při níž je určitý systém napaden zahlcením vyrovnávací paměti nepotřebnými daty.[93] Jako první byl výraz spam pro označení hromadně zasílané komerční informace použit uživateli sítě USENET, kde byly zasílány zprávy do diskusních fór druhořadými právníky nabízející pomoc imigrantům při získání zelených karet. To dalo vzniku této neetické a později i protiprávní obchodní metodě, spammingu. Pojem spamu je velice obecný a má široký obsah, v právu není nikde vymezen. Lze jej definovat buďto s přihlédnutím ke kvalitativním, nebo kvalitativním. Z kvantitativního hlediska vnímáme hromadnost šíření zpráv a negativní dopad, kvalitativní hledisko zachycuje obsah zpráv a jejich negativní hodnotu.

Spammingem pak bude zasílání sdělení, které je minimálně:

a)elektronické

b)zasílané hromadně

c)zasílané bez vyžádání[94]

Spam můžeme chápat v užším pojetí jako hromadné šíření nevyžádaného sdělení nejčastěji reklamního charakteru pomocí Internetu, nejčastěji pomocí elektronické komunikace. Je tak této komunikace zneužíváno tak, že na množství adres je zasílána jedna a tatáž příjemcem nevyžádaná zpráva. Zasilatele spamu to finančně nijak nezatěžuje, představuje tak pro něj bezplatnou propagaci svých produktů o širokém záběru.[95]

---

[93] Raymond, E., Steele, G. L. (2002) The Jargon File, verze 4.2.2, Project Guttenbergm, Dostupné z WWW: http://www.gutenberg.org/ebooks/3008

[94] Blíže v Polčák, R. Právo na internetu. Spam a odpovědnost ISP. Brno: Computer Press, 2007

[95] Študentová, M. Trestněprávní aspekty související se zasíláním e-mailů a zveřejňováním materiálů na webových stránkách. Trestní právo č.7-8/2007

V širším smyslu se jedná o veškeré nevyžádané zprávy a to i ty, které obsahují viry, trojské koně::[96]

a)Obchodní sdělení

b)Phishing

c)Malware

d)Nigerijský typ

Phishing, malware, Nigerijský typ pak dohromady tvoří souborně největší část spamu a jsou označovány jako scamy (z anglického scam – švindl, podvod). Jejich účelem je pomocí podvodných jednání vylákat finanční prostředky z oklamaných uživatelů informačních technologií.[97]

5.4.2 Obchodní sdělení

Zasílání nevyžádaných obchodních sdělení je legislativně upraveno zákonem č. 480/2004 Sb. o některých službách informační společnosti. Je to implementace Směrnice Evropského parlamentu a Rady 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací. Zákon definuje, co je obchodním sdělením v ustanovení § 2 písm. f takto: *obchodním sdělením jsou všechny formy sdělení určeného k přímé či nepřímé podpoře zboží či služeb nebo image podniku fyzické či právnické osoby, která vykonává regulovanou činnost nebo je podnikatelem vykonávajícím činnost, která není regulovanou činností; za obchodní sdělení se považuje také reklama podle zvláštního právního předpisu. Za obchodní sdělení se nepovažují údaje umožňující přímý přístup k informacím o činnosti fyzické či právnické osoby nebo podniku, zejména doménové jméno nebo adresa elektronické pošty; za obchodní sdělení se dále nepovažují údaje týkající se zboží, služeb nebo image fyzické či právnické osoby nebo podniku, získané uživatelem nezávisle.* Dle § 7 odst. 1 lze toto sdělení šířit elektronickými prostředky jen za podmínek stanovených tímto zákonem. Ze zákona vyplývá, že se za spam považuje nevyžádané sdělení, které musí být obchodní, ne tedy politické nebo náboženské. Dále musí být šířené elektronickými prostředky právnickou osobou nebo fyzickou osobou v rámci její podnikatelské činnosti nebo v souvislosti s ní. Zákon podmiňuje zasílání obchodních sdělení zejména souhlasem příjemce. Naopak zakazuje šíření, pokud není zřetelně označeno jako obchodní, skrývá

[96] Volevecký, P. Kybernetické hrozby a jejich trestně právní kvalifikace. Trestní právo č.12/2010
[97] Lance, J. Phishing bez záhad. 1. Vyd. Praha: Grada Publishing, a.s., 2007

nebo utajuje totožnost odesílatele, je zasláno bez platné adresy, na kterou by mohl adresát přímo a účinně zaslat informaci o tom, že si nepřeje, aby mu byly obchodní informace odesílatelem dále zasílány.

Za nedodržení limitů tohoto zákona hrozí správní postih a to pokuta.[98] Trestním právem by se dalo postihovat toto jednání pouze jako sběr e-mailových adres jako takový, pokud naplní znaky trestného činu neoprávněného nakládání s osobními údaji dle § 180 TZ[99]

5.4.3 Phishing

S rozvojem možností plateb za zboží a služby pomocí Internetu se také rozmohla podvodná jednání toho využívající. K elektronickému platebnímu styku jsou využívány z důvodů bezpečnosti citlivé osobní a identifikační údaje, které dávají svému držiteli přístup k finančním prostředkům. Toho využívá phishing. Slovo údajně vzniklo spojením slov phreaking a fishing.[100] Pojem znamená jednání, které má za cíl podvodně získat citlivé informace, jako přístupová jména a hesla, čísla kreditních karet tím, že se vydává za důvěryhodnou osobu či organizaci, to prostřednictvím elektronické komunikace.

Nejčastěji je k těmto útokům využíván e-mail, v kterém se pachatel vydává za banku, nebo jinou instituci provádějící či vyžadující od oběti platbu. Oběti je tak zaslán e-mail, který je navržen tak, aby nevzbudil žádné podezření. Banka v něm například vyžaduje schválení finanční transakce, nebo ohlašuje bezpečnostní chybu a vyžaduje potvrzení identifikačních údajů oběti. V textovém sdělení e-mailu je obsažen odkaz, na který se má metaforicky řečeno oběť chytnout jako ryba. Stránka, která se po kliknutí na odkaz objeví je navržena tak, aby vyhlížela co možná nejpodobněji té originální, je ovšem podvržena. Po zadání údajů na tuto stránku se tyto dostanou do rukou útočníka, který tak získává přístup k finančním prostředkům oběti. Využívá tedy lidské důvěřivosti a dá se považovat za formu sociálního inženýrství.

Uživatelé českého Internetu se s těmito útoky setkali již mnohokrát. Pro představu uvádím podobu e-mailu, který byl rozšířen 10. 10. 2006 a vyzývá uživatele k

[98] Blíže v Polčák, R. Právo na internetu. Spam a odpovědnost ISP. Brno: Computer Press, 2007
[99] Študentová, M. Trestněprávní aspekty související se zasíláním e-mailů a zveřejňováním materiálů na webových stránkách. Trestní právo č.7-8/2007
[100] Fishing, česky rybaření. Phishing se pak převádí do češtiny jako rhybaření.

přechodu na nový bezpečnostní systém z důvodu množících se případů podvodů. Nabízí také přímý odkaz, na kterém by měl údajný systém běžet. Zde je kompletní text zprávy:

Předmět: Ceska sporitelna – Pozor! Nove bezpecnostni standardy.
Od: „Ceska sporitelna“ <servise@csas.cz>
Datum: Wed, 11 Oct 2006 14:45:52 –0500“
„Dobry den vazeni klienti!“
„Leto roku 2006 bylo pro Banku nejzavaznejsim z hlediska poctu nelegalnich operaci. Cim dal vice maji podvodnici zajem o duvernou informaci nasich zakazniku. Velke mnozstvi lidi se na nas obraci s zadosti zamezit vzniku nebezpeci ztraty peneznich prostredku z uctu.“
„S ohledem na soucasny stav vyhlasuje Banka nasledujici mesic za mesic boje s frodem. Do 1.listopadu musi vsechny nasi klienti aktivovat novy system bezpecnosti vlastnich uctu. Provedli jsme velkou praci pro zlepseni bezpecnosti. System byl zkontrolovan uznavanymi odborniky v oboru elektronickych plateb, a vsechny nezavisli experti potvrdili ucinnost systemu proti frodu. Z duvodu nebezpeci mozneho zneuziti techto udaju podvodniky nejsou tyto data zverejnena v otevrenych zdrojich.“
„Vy jste byl(a) zvolen(a) jako jeden z ucastniku finalniho stadia testovani systemu. V soucasne dobe Vam navrhujeme vyuzit odkaz https://www.servis24.cz/ebanking-s24/ a standardnim zpusobem prihlaseni do Internet bankingu aktivovat novy bezpecnostni system. V aktualnim stadiu provozu jsou mozne nektere nesrovnalosti. Pripoustime jejich existenci, a proto prosim nezasilejte dodatecne popisy vznikajicich potizi, prace na jejich odstraneni jiz probihaji.“
„Musime Vas informovat o bezpodminecnem pouziti noveho systemu od listopadu, v opacnem pripade budou Vase ucty zablokovany do okamziku uplne identifikace Vasi osoby. Proto doporucujeme v nejkratsi mozne dobe prejit na novy bezpecnostni standard.“
„S pozdravem, Oddeleni Banky pro ochranu pred frodem.

Takové útoky bývají úspěšné zejména z důvodu masového rozesílání. Na druhou stranu si nelze nevšimnout chybící diakritiky, což bývá způsobeno překladem těchto mailů strojovými překladači z cizích jazyků.

Dle popsaného způsobu provádění phishingu vyplývá, že se bude dát podřadit pod skutkovou podstatu podvodu, dle § 209 TZ. Pachatel uvádí uživatele Internetu v omyl, získá potřebné informace a údaje a následně je využije tak, že peněžní prostředky odčerpá. Tím je způsobena škoda a pachatel se obohacuje, čímž je tento trestný čin dokonán. Další skutkovou podstatou dopadající na toto jednání je ta uvedená v § 234 TZ, trestný čin neoprávněné opatření, padělání a pozměnění platebního prostředku.

5.4.4 Nigerijský typ

Scam nigerijského typu (označovaný také jako scam 419[101]) je fingovaným dopisem, kterým se jeho pisatel snaží získat od oběti určitou sumu peněz s příslibem sumy mnohonásobně vyšší. Tato suma je vyžadována pro rozličné, většinou chvályhodné účely. Tato částka je pak užita k účelu jinému. I zde je tedy používáno sociální inženýrství, Nigerijský scam bývá považován za předchůdce phishingu.

S tímto spamem jsem měl možnost setkat se na vlastní kůži, uvedu proto tento případ. Kontaktovala mě 23- letá africká dívka z Pobřeží Slonoviny jménem Blesing Coneh. Její otec byl údajně osobní poradce bývalé hlavy státu, než rebelové napadlo její dům a zabili jej i její matku před jejím zrakem. Jediným způsobem, kterým přežila, byl její útěk do Senegalu, odkud mi údajně psala. V Senegalu přežívala v utečeneckém táboře, v kterém to bylo jako ve vězení. Dívka tedy neměla žádné příbuzné, ke kterým by se uchýlila, jediným spřízněným člověkem byl reverend tábora. Dívka neměla právo mít peníze u sebe v táboře, protože to bylo proti zákonům země. Také popisovala její touhu vrátit se ke studiu. Naštěstí však měla přístupové údaje k evropskému účtu jejího otce a jeho úmrtní list. Na účtu se měla nacházet pohádková částka 2,3 milionu dolarů. Ta měla být převedena na můj účet a následně předána při osobním setkání. V dopise byla též vyjádřena obava dívky o její život kvůli nelidským podmínkám, čímž byl vyvíjen psychologický tlak na rychlost celé transakce, dále byla přiložena fotografie této atraktivní slečny. Ze zvědavosti jsem odepsal a trvalo až několik vyměněných mailů, než po mě byla požadována určitá částka z důvodu poplatku africkému advokátovi. Překvapila mě neuvěřitelná promyšlenost příběhu a též trpělivost osoby, která se tohoto podvodu účastnila. I zde tak pisatel útočí na soucit člověka a na vidinu finančního ohodnocení.

[101] To je pro zajímavost číslo paragrafu Nigerijského trestního zákona postihující podvod

Patrně lze toto jednání charakterizovat jako podvod dle § 209 TZ.

5.5 Malware

Tento pojem vznikl složením anglického „malicious“ (záludný, zlomyslný, lstivý) a „software“ (programové vybavení počítače). Je to tedy označení pro veškeré programy, které jsou vytvořeny za účelem poškodit, omezit funkčnost, zneužít počítačový systém nebo data na něm uložená, anebo získat nad takovým počítačovým systémem kontrolu. Někdy bývá malware systematicky zařazen mezi spam, ale elektronická komunikace není výlučným ani převažujícím způsobem šíření malwaru. Převažujícími způsoby jsou zejména škodlivé webové stránky, šíří se i pomocí phishingu anebo zcela samostatně, jako níže popsaný červ. V době vysoce propojené kybernetické infrastruktury propojující mimo jiné medicínské, energetické, telekomunikační a finanční systémy, mohou útoky pomocí malwaru způsobit katastrofické škody na lidských životech, ohrozit poskytování základních služeb a samozřejmě také finanční ztráty. Například virus CodeRed infikoval kolem 359,000 hostitelů, což vedlo ke škodám odhadem 2,6 miliard amerických dolarů.[102] Malware se člení na tyto druhy:[103]

a) viry a červi

b) trojské koně

c) spyware

d) adware

5.5.1 Viry a červi

Virus je typ malwaru a znamená nežádoucí program, který je připojen k nezávadnému programu a který se po spuštění nezávadného programu spustí s ním, nebo se nainstaluje.[104] Je tedy přenášen spolu s nezávadným programem a tedy bez zásahu a vědomí uživatele napadeného počítačového systému. Projevy virů mohou být naprosto neškodné a žertovné, například jen zobrazovat obrázky nebo přehrávat

[102] Moore D., Shannon C., Brown J. Core-Red: a case study on the spread and victims of an internet worm. In Proceedings of the Internet Measurement Workshop 2002, Marseille, France

[103] Volevecký, P. Kybernetické hrozby a jejich trestně právní kvalifikace. Trestní právo č.12/2010

[104] Počítačový virus je inspirován těmi biologickými a to zejména faktem, že nemohou existovat samostatně bez hostitelské buňky (počítačového programu). Přejata je též terminologie, používající pojmů infikování, hostitel, apod.

melodie. Druhým protipólem funkcí virů může být kompletní zničení počítačového systému.

Když pohlédneme do historie virů, v 60. letech 20. stolení se objevit software, který by se jako virus dal označit. V této době totiž skupina programátorů vytvořila hru, která se jmenovala Core Wars. Ta se reprodukovala při každém spuštění a zabírala paměť na počítačích dalších hráčů. Tvůrci této hry/viru se nakonec stali i prvními, kdo přinesl „antivirový“ program. Ten měl název Reeper a sloužil k tomu, aby kopie Core Wars odstranil. Do roku 1983 o Core Wars v podstatě nikdo nevěděl. Tehdy jeden z programátorů oznámil, že program Core Wars existuje, a následně jej popsal v prestižním vědeckém časopisu. Rok 1983 je pak všeobecně považován za začátek éry počítačových virů. Je to dáno také tím, že se začalo rozšiřování operačního systému MS-DOS společnosti Microsoft.[105]Jiný zdroj datuje zrod prvního viru na rok 1986, kdy bratři Basit a Amjat z Pákistánu vytvořili počítačový virus Brain, jenž byl určen pro systém MS-DOS. Byl schopen se sám šířit a infikovat tak další počítače. Důvodem vzniku viru byla ochrana před nelegálním kopírováním medicínského softwaru, který oba Pákistánci vytvořili, ve svých důsledcích však, kromě znepříjemňování života uživatelů, neškodný.[106] Příchod Internetu a rozmach elektronické komunikace pak znamená rozvoj virů ve smyslů spamu, a to z hlediska způsobu jejich šíření. Příkladem mohou být viry Melissa, ILoveYou nebo Černobyl. Virus Melissa je dokonce zařazen do Guinnessovy knihy rekordů, neboť infikoval přes 3,1 milionu počítačů. Od roku 1996 vznikají viry nového typu, tzv. macroviry, které jsou implementovány do textových souborů a nejsou tedy již šířeny pomocí spustitelných souborů jako doposud.[107] Dnes viry již opustily svou výhradní doménu počítačů a jsou konstruovány tak, aby napadali kapesné počítače nebo mobilní telefony.

Jedním z podtypů virů jsou i takzvané „ransomware“ (ransom znamená anglicky výkupné). Takový virus vyhledá v počítači poškozeného soubory, které mu znepřístupní do zaslání požadovaného finančního obnosu na účet pachatele.[108]

---

[105] Technet, Dostupné z WWW: http://technet.idnes.cz/tec_technika.asp?r=bezpecnost&c=A041103_5285981_bezpecnost,

[106] Slunečnice, Dostupné z WWW: http://www.slunecnice.cz/tipy/prvni-pocitacovy-virus-vznikl-pred-25-lety/,

[107] Podrobněji v Šámal, P. a kol. Trestní zákoník II. § 140 až 421. Komentář 1. Vydání. Praha : C. H. Beck, 2010, 2091s

[108] Peníze nebo data. CHIP, 2006, č. 9

Jiným podtypem virů jsou tzv. počítačoví červi (anglicky „worm“). Jinými autory je červ označován za samostatnou kategorii malwaru. Rozdíl je v tom, že červ není závislý na jiném programu, může se tak šířit samostatně. Poté, co infikuje systém, se zmocní prostředků síťové komunikace a využije jich k dalšímu svému šíření. Vysoké nebezpečí tedy spočívá v jejich schopnosti samostatné replikace, například se odešle všem položkám adresáře napadeného počítačového systému a způsobí tak domino efekt. Jedním z prvních počítačových červů, který ke svému šíření využíval celosvětové sítě Internet (obecně je mu připisováno absolutní prvenství), byl Morrisův červ (anglicky Morris worm, někdy označovaný také jako Internet worm). Jednalo se o první počítačovou hrozbu, která přitáhla značný zájem médií. Byl vytvořen tehdy 23-letým studentem Cornellovy univerzity Robertem Tappanem Morrisem. K jeho vypuštění došlo 2. listopadu 1988 za využití počítače institutu MIT. Autor byl prvním člověkem, obviněným v USA z porušení zákona Computer Fraud and Abuse Act z roku 1986, týkajícího se zneužívání výpočetní techniky a s ní spojené podvodné činnosti.[109]

5.5.2 Trojské koně (nebo též Trojany)

Obdobně jako byl mytologický Trojský kůň zdánlivě darem, z kterého následně vyskákali řečtí vojáci, aby se zmocnili Tróji, jsou počítačové trojské koně programy, které se jeví jako užitečné, místo toho však mají nežádoucí funkce. Rozdílem od předchozích je, že se nedokáží sami šířit. Poté, co je trojský kůň v napadeném počítači, může vykonávat funkce typu výše popsaných DoS útoků, key-loggerů, backdoors. Dále pak může přesměrovávat vytáčené připojení k Internetu na připojení dražší (URL trojan), vyřadit z činnosti antivirové programy (security software disable), vytvořit z napadeného počítače centrální server pro rozesílání spamů (spam-server).[110]

Příkladem může být program NetBus, který po jeho umístění na napadený počítač nepozorovaně otevře komunikační port a umožní tak hackerovi tento počítač ovládnout.[111]

[109] Wikipedia, http://cs.wikipedia.org/wiki/Morrisův_červ
[110] Blíže v Šámal, P. a kol. Trestní zákoník II. § 140 až 421. Komentář 1. Vydání. Praha : C. H. Beck, 2010, 2091s
[111] Na Internetu existuje spousta návodů, například http://hackers-play.wgz.cz/navod-na-netbus-pro-2-01, zobrazeno

5.5.3 Spyware

Z anglického „spy“, neboli špion a již vysvětleného software vznikl tento název, který již naznačuje funkci tohoto malwaru. Spyware získává statistická data o provozu počítačového systému a bez vědomí a souhlasu uživatele je odesílá do datové schránky útočníka.[112] Mohou to být informace o osobě poškozeného, o jeho aktivitách a využití jeho počítačového systému, o jím navštívení internetové stránky, apod. Toto monitorování bývá prováděno zejména ze statistických důvodů za účelem cílené reklamy. Bývají často součástí jiných volně šiřitelných programů, ale zůstávají na hostitelském počítači o po odinstalování těchto programů.[113]

5.5.4 Adware

Adware je zkráceninou anglického „advertising supported software“, neboli softwaru podporujícího reklamu. Jeho nežádoucí účinek spočívá zejména v neustálém podsouvání reklamních oken na displej napadeného počítače pomocí vyskakujících oken a mají tak obtěžující charakter. Adware tak velice často využívá statistických výsledků nashromážděných pomocí spyware. Adware se však instaluje do počítače za souhlasu uživatele, ten se tak může rozhodnout, zda k tomu udělí svůj souhlas.

5.5.5 Obrana proti malwaru a trestněprávní kvalifikace

Obrana proti malwaru je zejména prevence a to využitím bezpečnostních programů, kterými jsou zejména antivirové programy, které jsou dnes již volně stažitelné a jsou nezbytnou součástí každého počítačového systému. Pro podnikatelské subjekty bude samozřejmě bezpečnější využití profesionálních placených verzí těchto programů. Pracují na principu průběžně aktualizovaných databází jejich poskytovatelem, takže reagují na denně vznikající nový malware. Dalšími jsou antispamové, antispywarové nebo antiadwarové programy, nebo firewaly, které zjednodušeně řečeno definují pravidla komunikace mezi počítačovým systémem uživatele a okolním prostředím.

Z trestně právního hlediska záleží na tom, k čemu je malware určen. Pokud to bude k získání neoprávněného přístupu k počítačovému systému překonáním bezpečnostního opatření, lze postihnout již jeho držení, výrobu, uvedení do oběhu, dovoz, vývoz, provoz, nabízení, zprostředkování, prodej nebo jiné zpřístupnění a to jako

[112] Požár, J. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeňek, s.r.o., 2005
[113] Volevecký, P. Kybernetické hrozby a jejich trestně právní kvalifikace. Trestní právo č.12/2010

trestný čin opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat podle § 231 TZ. Podmínkou pro to je však úmysl spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) nebo trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1, 2. Dalším stupněm je pak samotné užití malwaru k překonání bezpečnostního opatření k získání přístupu k počítačovému systému nebo k jeho části, respektive získání přístupu a následné v zákoně popsané nakládání s daty, které lze subsumovat pod skutkovou podstatu trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 TZ ve stadiu dokonaného trestného činu, či pokusu dle § 21 TZ.[114]

5.6 Cybersquatting

Tento pojem je opět složeninou dvou anglických slov a to „cybernetic“ (kybernetický) a „squatting“ (protiprávní obsazení domu). Jednání se rozšířilo s internetovým boomem a propagací známých obchodních společností na Internetu. To bylo zneužíváno tak, že se si osoba zaregistrovala doménu známého podniku, instituce nebo produktu a spekulovala s prodejem této domény dotčenému subjektu. Dnes je pochopitelně drtivá většina společností na Internetu propagována a tato činnost ustupuje do pozadí, stále se však může vyskytnout u nově vznikajících společností nebo produktů. Příkladem lze uvést spor o doménu www.oskar.cz, kterou chtěla využít společnost Český mobil pro propagaci své sítě mobilních telefonů. Doména již byla předtím zaregistrována společností Comfor, která za její uvolnění požadovala 10 milionů korun.[115]

Novodobějším projevem cybersquattingu bude nekalosoutěžní jednání, například zaregistrování domény mající název známého produktu a provozování zde svého Internetového obchodu.

S tím souvisí jedna z forem cybersquattingu a to typosquatting, z anglického „typographical“ (typografický) a „squatting“. Zde je záměrně registrováno doménové jméno velice podobné již existujícímu, zpravidla se liší jen jedním písmenkem, mnohdy takovým, které bývá stlačeno v případě překlepu při vyťukávání originální domény. Tím se získává počet návštěv parazitující Internetové stránky, což vede ke zvýšeným

[114] Blíže v Volevecký, P. Kybernetické hrozby a jejich trestně právní kvalifikace. Trestní právo č.1/2011
[115] Matějka, M. Počítačová kriminalita, Computer press, 2002, s.74

ziskům z tam umístěných reklam. Takové jednání bývá klasifikováno jako porušení práv k ochranné známce.[116]

Pokud je výše popsanými jednáními způsobena poškozenému vážná újma na právech tím, že pachatel uvede někoho v omyl nebo využije něčího omylu, tak jej lze charakterizovat jako poškození cizích práv dle § 181 TZ. V případech jednání majícího znaky nekalé soutěže, a to zejména parazitování na pověsti, bude se jednat o trestný čin porušení předpisů o pravidlech hospodářské soutěže.

[116] Volevecký, P. Kybernetické hrozby a jejich trestně právní kvalifikace. Trestní právo č.1/2011

6 Autorské právo a kybernetická kriminalita

6.1 Obecně o tématu

Internet je hromadným sdělovacím prostředkem, masovým médiem, fenoménem, a to patrně nejatraktivnějším a nejužívanějším ze všech. S přihlédnutím k exponenciálnímu růstu jeho významu za dobu jeho nedlouhé historie můžeme s jistotou předvídat, že tomu v budoucnu nebude jinak. Od jeho zrodu a původnímu účelu, pro který byl stvořen, nastal radikální posun v jeho využití směřující k čím dál většímu komerčnímu využití. Spolu se zdokonalováním jeho funkčnosti, zejména kapacitní schopnosti přenášet čím dál tím více dat za kratší a kratší dobu se zdokonalují počítačové systémy z hlediska svých hardwarových dispozic. To umožňuje přenos jakéhokoliv materiálnu v reálném čase, bez ohledu na časová pásma, teritoriální působnost jednotlivých legislativ a mnohdy bez ohledu na zákon jako takový. Ať již je Internet jakkoli specifické prostředí, schopné překlenout hranice států, nestojí nad zákonem. A pokud zvážíme, které právo bývá pomocí Internetu porušováno nejvíce, bude to jistě právo duševního vlastnictví a to konkrétně práv autorských, práv souvisejících s autorským právem a práv k databázi.

Důvodem pro to bude již popsaná charakteristika specifičnosti Internetu, respektive kybernetického prostoru. Znovu bych na tomto místě uvedl možnost anonymity uživatelů této sítě, což jistě zvyšuje míru nelegálního jednání. Dalším faktorem je bezesporu záměrně se zvyšující snadnost a pohodlnost použití Internetu a počítačových systémů. Dostat se do rozporu se zákonem je tak snadné a mnohdy nevědomé. Kdyby však pachateli nestačily jeho znalosti a schopnosti k úmyslnému páchání kybernetické kriminality, na Internetu samotném je spousta návodů a uživatelů připravených podat pomocnou ruku. Samotná kapacita a nenákladnost zpřístupnění Internetového obsahu vzhledem k jeho příjemcům je tak nedozírná a jistě se tak podílí jako jeden z faktorů na vytváření prostoru vhodného k porušování práv duševního vlastnictví.

6.1.1 Autorský zákon a předmět jeho úpravy

Autorské právo je u nás upraveno zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů.[117] Tento upravuje autorské právo komplexně, koncepčně odpovídá kontinentálnímu pojetí práva duševního vlastnictví na rozdíl od toho amerického, copyrightového. Jeho principy jsou zejména:[118]

a) Právo náleží pouze individuálně určené fyzické osobě – autorovi, přičemž na druhé straně stojí povinnost individuálně neurčených osob zdržet se jakýchkoli neoprávněných zásahů do práv nositele autorského práva.
b) Jde o právo nepromlčitelné, neboť to není právo majetkové, ale smíšené, tzv. osobnostně-majetkové. Tato práva jsou však oddělena.
c) Předmětem je jednotlivě určený nehmotný statek, který je hmotně vyjádřen a to v podobě lidskými smysly vnímatelné a sdělitelné.
d) AZ je v poměru speciality k občanskému zákoníku[119] a přebírá zásadu občanského smluvního práva, tj. zásadu smluvní volnosti; zákonná úprava platí teprve tehdy, pokud si strany nesmluvily jinak
e) AZ obsahuje jednotný smluvní typ - licenční smlouva
f) Zapracovává předpisy Evropské Unie. Příkladem může být právo výrobce zvukově obrazového záznamu, právo zveřejnitele k dosud nezveřejněnému dílu, k němuž uplynula doba trvání majetkových práv. Dále je stanovena doba ochrany autorských děl na 70 let po smrti autora.

AZ však neupravuje pouze právo autorské, což vyplívá z § 1, podle kterého jsou předmětem jeho úpravy:

a) práva autora k jeho autorskému dílu,

b) práva související s právem autorským:

1. práva výkonného umělce k jeho uměleckému výkonu,

2. právo výrobce zvukového záznamu k jeho záznamu,

3. právo výrobce zvukově obrazového záznamu k jeho záznamu,

4. právo rozhlasového nebo televizního vysílatele k jeho vysílání,

[117] Dále jen AZ
[118] Smejkal, V. Internet a §§§, 2. Aktualizované vydání, Grada Publishing, 2001
[119] Ten v § 1 odst. 3 říká, že právní vztahy vznikající z výsledků duševní tvořivé činnosti upravují zvláštní zákony, a takovým je zejména AZ

5. právo zveřejnitele k dosud nezveřejněnému dílu, k němuž uplynula doba trvání majetkových práv,

6. právo nakladatele na odměnu v souvislosti se zhotovením rozmnoženiny jím vydaného díla pro osobní potřebu,

c) právo pořizovatele k jím pořízené databázi,

d) ochranu práv podle tohoto zákona,

e) kolektivní správu práv autorských a práv souvisejících s právem autorským.

První skupinu tedy tvoří právo autorské, druhou skupinu pak šest práv souvisejících s právem autorským, třetí skupinu pak právo pořizovatele databáze. Stěžejním a pro tuto práci nejdůležitější však zůstává právo autora k jeho autorskému dílu.

6.1.2 Předmět autorského práva

Na otázku co je předmětem autorského práva pak odpovídá § 2, který definuje autorské dílo. Podle odst. 1 je jím *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 (dále jen "dílo"). Dílem je zejména dílo slovesné vyjádřené řečí nebo písmem, dílo hudební, dílo dramatické a dílo hudebně dramatické, dílo choreografické a dílo pantomimické, dílo fotografické a dílo vyjádřené postupem podobným fotografii, dílo audiovizuální, jako je dílo kinematografické, dílo výtvarné, jako je dílo malířské, grafické a sochařské, dílo architektonické včetně díla urbanistického, dílo užitého umění a dílo kartografické*.

Z hlediska této práce je důležitý také odst. 2, který rozšiřuje pojem díla takto:
Za dílo se považuje též počítačový program, je-li původní v tom smyslu, že je autorovým vlastním duševním výtvorem. Databáze, která je způsobem výběru nebo uspořádáním obsahu autorovým vlastním duševním výtvorem a jejíž součásti jsou systematicky nebo metodicky uspořádány a jednotlivě zpřístupněny elektronicky či jiným způsobem, je dílem souborným. Jiná kritéria pro stanovení způsobilosti počítačového programu a databáze k ochraně se neuplatňují. Fotografie a dílo vyjádřené postupem podobným fotografii, které jsou původní ve smyslu věty první, jsou chráněny jako dílo fotografické.

Zda tedy půjde o dílo ve smyslu AT, musí být kumulativně naplněny následující pojmové znaky:

a) Charakter díla – musí jít o dílo literární, jiné dílo umělecké nebo dílo vědecké
b) Dílo musí být jedinečným výsledkem tvůrčí činnosti autora
c) Dílo je vyjádřeno v jakékoli objektivně vnímatelné podobě
d) Dílo není vyloučeno z ochrany podle ustanovení AZ (např. § 3)[120]

Takto je tedy definováno autorské dílo. Nezákonné nakládání s ním pak dává vzniku odpovědnosti, ať již soukromoprávní nebo veřejnoprávní.

6.1.3 Obsah autorského práva

Ke komplexnímu uchopení problematiky je však třeba alespoň obecně vymezit obsah autorského práva, tedy jaká práva mohou být porušena. Odpověď nám podává § 10 AZ, který stanoví, že *právo autorské zahrnuje výlučná práva osobnostní (§ 11 AZ) a výlučná práva majetková (§ 12 a násl. AZ).*

Mezi osobnostní práva dle § 11 AZ patří autorovo:

1. právo rozhodování o zveřejnění svého díla
2. právo osobovat si autorství, včetně rozhodování o uvedení autorova jména při zveřejnění díla a dalším jeho užití.
3. právo autora na nedotknutelnost svého díla

Pro osobnostní práva pak platí, že se jich autor nemůže vzdát, nemůže je převést a jeho smrtí tato zanikají (§ 11 odst. 4 AZ). Po smrti autora si nikdo nesmí osobovat jeho autorství k dílu, dílo smí být užito jen způsobem nesnižujícím jeho hodnotu a, je-li to obvyklé, musí být uveden autor díla, nejde-li o dílo anonymní (§ 11 odst. 5 AZ).

Mezi majetková práva autora náleží právo dílo užít a tzv. jiná majetková práva (§ 24, 25 AZ).

Právem dílo užít se rozumí (§ 12 odst. 4 AZ):

a) právo na rozmnožování díla (§ 13 AZ),
b) právo na rozšiřování originálu nebo rozmnoženiny díla (§ 14 AZ),
c) právo na pronájem originálu nebo rozmnoženiny díla (§ 15 AZ),
d) právo na půjčování originálu nebo rozmnoženiny díla (§ 16 AZ),
e) právo na vystavování originálu nebo rozmnoženiny díla (§ 17 AZ),
f) právo na sdělování díla veřejnosti (§ 18 AZ), zejména

[120] Smejkal, V., Čermáková-Vlčková, A. Autorská díla v hromadných sdělovacích prostředcích, Linde Praha, 2009

1. právo na provozování díla živě nebo ze záznamu a právo na přenos provozování díla (§ 19 a 20 AZ),
2. právo na vysílání díla rozhlasem či televizí (§ 21 AZ),
3. právo na přenos rozhlasového či televizního vysílání díla (§ 22 AZ),
4. právo na provozování rozhlasového či televizního vysílání díla (§ 23 AZ).

Tento výčet způsobů užití díla však není uzavření (dle § 12 odst. 5 AZ) Jiným majetkovým právem je dle § 24 a § 25 AZ právo na odměnu při opětném prodeji originálu díla uměleckého a na odměnu v souvislosti s rozmnožováním díla pro osobní potřebu a vlastní vnitřní potřebu.

Z hlediska kybernetické kriminality budou z obou kategorií autorských práv porušována zejména právo na rozhodnutí o zveřejnění díla (§ 11 odst. 1 AZ), právo na rozmnožování díla (§ 13 AZ), právo na rozšiřování originálu nebo rozmnoženiny díla (§ 14 AZ), právo na sdělování díla veřejnosti (§ 18 AZ). Neoprávněně zasahovat do práva autorského bude i ten, kdo obchází účinné technické prostředky ochrany práv podle AZ (§ 43 odst. 1 AZ), Do práva autorského neoprávněně zasahuje také ten, kdo vyrábí, dováží, přijímá, rozšiřuje, prodává, pronajímá, propaguje prodej nebo pronájem nebo drží k obchodnímu účelu zařízení, výrobky nebo součástky nebo poskytuje služby, které jsou za účelem obcházení účinných technických prostředků nabízeny, propagovány nebo uváděny na trh, mají vedle obcházení účinných technických prostředků jen omezený obchodně významný účel nebo jiné užití, nebo jsou určeny, vyráběny, upravovány nebo prováděny především s cílem umožnit nebo usnadnit obcházení účinných technických prostředků (§ 43 odst. 2 AZ). Do práva autorského zasahuje též ten, kdo bez svolení autora způsobuje, umožňuje, usnadňuje nebo zastírá porušování práva autorského tím, že odstraňuje nebo mění jakoukoli elektronickou informaci o správě práv k dílu, nebo rozšiřuje, dováží nebo přijímá za účelem rozšiřování, vysílá nebo sděluje veřejnosti, a to i způsobem podle § 18 odst. 2 AZ dílo, ze kterého byla informace o správě práv nedovoleně odstraněna nebo změněna (§ 44 odst. 1 AZ). Jiná porušování autorského práva tím ovšem nevylučuji.

Po obecném úvodu do autorského práva jako takového a výčtu práv, která bývají kybernetickou kriminalitou nejčastěji porušována, se nyní můžeme zaměřit na konkrétní způsoby jeho porušování a to ty, které jsou z hlediska této práce relevantní.

6.2 Zpřístupňování děl pomocí Internetu

Pod tímto jednáním můžeme shledat jakékoliv nahrání (neboli upload) díla v jeho digitální podobě na tzv. server[121], z kterého je toto dílo přístupné veřejnosti. Toto vymezení je obecné a lze pod něj podřadit specifické způsoby zpřístupňování v prostředí Internetu. Ve světle AZ to půjde zřejmě o užití díla dle § 12 a násl. AZ, které slouží primárně autorovi díla a jen na jeho úvaze záleží, jestli své dílo zpřístupní, či nikoliv, nebo jestli dá k takovému zpřístupnění souhlas někomu jinému.

Kdybychom hledali konkrétní způsob užití díla, v úvahu bude jistě přicházet § 13 AZ rozmnožování díla:

> *(1) Rozmnožováním díla se rozumí zhotovování dočasných nebo trvalých, přímých nebo nepřímých rozmnoženin díla nebo jeho části, a to jakýmikoli prostředky a v jakékoli formě.*
>
> *(2) Dílo se rozmnožuje zejména ve formě rozmnoženiny tiskové, fotografické, zvukové, obrazové nebo zvukově obrazové, stavbou architektonického díla nebo ve formě jiné trojrozměrné rozmnoženiny anebo ve formě elektronické zahrnující vyjádření analogové i digitální.*

Rozmnoženinou zde můžeme chápat synonymicky s častěji používanou kopií. Ať již se jedná o fotografii, počítačový program, zvukový záznam nebo jiné dílo, jeho uložením na počítačový server vzniká jeho rozmnožena. Taková rozmnožena vzniká i například při konverzi jednoho datového formátu do druhého (například z formátu .waw, který je identickou kopií zvukového formátu to formátu .mp3, který využívá komprese a tedy i určitou ztrátu kvality). Sice nejde o rozmnoženinu v technickém slova smyslu (soubor je jiný), v právním slova smyslu to tak však bude.[122] S tím je nutno souhlasit, neboť rozmnožováním je dle § 13 odst. 1 AZ i vytváření nepřímých kopií. ¨

Při přenosu dat mezi jednotlivými počítači pomocí Internetu vzniká celá řada rozmnoženin, které vznikají bez vůle subjektů tohoto přenosu. Jedná se o ukládání dat do vyrovnávací paměti (tzv. caching), což umožňuje rychlejší funkci těchto systémů. Dalšími „nechtěnými“ kopiemi pak mohou být dočasně ukládané části internetových stránek v počítači uživatele, což slouží k jejich rychlejšímu opětovnému načtení. To je ošetřeno § 38a AZ, který tak uděluje zákonnou licenci pro dočasné rozmnoženiny. Do

[121] Server znamená počítač, který je určen k poskytování určité služby, například poskytuje www stránky, slouží jako úložiště dat apod.
[122] Čermák, J. Internet a autorské právo, 2. Aktualizované vydání, Linde Praha, 2003

práva autorského tak dle tohoto ustanovení nezasahuje ten, kdo *provádí dočasné úkony rozmnožování děl, které jsou pomíjivé nebo podružné, tvoří nedílnou a nezbytnou součást technologického procesu, nemají žádný samostatný hospodářský význam a jejich jediným účelem je umožnit přenos díla počítačovou nebo obdobnou sítí mezi třetími stranami uskutečněný prostředníkem.*

Jiným konkrétním užití bude sdělování díla veřejnosti dle § 18 AZ:

(1) Sdělováním díla veřejnosti se rozumí zpřístupňování díla v nehmotné podobě, živě nebo ze záznamu, po drátě nebo bezdrátově.

(2) Sdělováním díla veřejnosti podle odstavce 1 je také zpřístupňování díla veřejnosti způsobem, že kdokoli může mít k němu přístup na místě a v čase podle své vlastní volby zejména počítačovou nebo obdobnou sítí.

(3) Sdělováním díla veřejnosti není pouhé provozování zařízení umožňujícího nebo zajišťujícího takové sdělování.

(4) Sdělováním díla veřejnosti podle odstavců 1 a 2 nedochází k vyčerpání práva autora na sdělování díla veřejnosti.

Zde dokonce zákonodárce výslovně ošetřil problematiku v odst. 2 zmíněním počítačové nebo obdobné sítě. Problémem ale je, jaký je vzájemný vztah těchto dvou způsobů užití, tedy rozmnožování a sdělování díla veřejnosti. Dle mého názoru je sdělování díla veřejnosti pojmem širším a zahrnuje v sobě i rozmnožování.

6.2.1 Umísťování děl na Internetových stránkách

Internetové stránky jsou jistě nejužívanější službou Internetu. Jsou tvořeny prvky jako textové pole, ikony, obrázky, zvukové soubory, a další. Tyto prvky jsou pak poskládány pomocí zdrojového kódu dohromady a tvoří tak uživatelsky co nejpřehlednější a nejatraktivnější stránku tak, jak nám ji zobrazí displej počítače. Webová stránka má tak svůj obsah uložen na svém domovském serveru, z kterého se zobrazuje svým uživatelům a z kterého si také uživatelé mohou tento obsah stáhnout. Dochází tak k oběma výše popsaným jednáním, rozmnožování díla a sdělování jej veřejnosti. Pokud k tomu nemají svolení autora či licenci a nejedná-li se o volné dílo (viz níže), jedná se o zásah do majetkových práv autora. O závažnější případ půjde, pokud ono dílo nebylo autorem doposud zveřejněno. Dílo je totiž zveřejněno dle § 4 odst. 1 jeho prvním oprávněným veřejným přednesením, provedením, předvedením, vystavením, vydáním či jiným zpřístupněním veřejnosti. Rozhodnutí o zveřejnění díla je

dle § 11 odst. 2 AZ výhradním osobnostním právem autora, patrně pak půjde i o zásah do osobnostních práv. V praxi se málokdy setkáme s internetovou stránkou, na které by se nenašlo ani jedno dílo na ní neoprávněně umístěné. Může jít o maličkost, jako například obrázek v pozadí, který si amatérský tvůrce stránky stáhne ze stránky jiné, může však jít o záměrné umísťování souborů hudby či filmů za účelem získání zisku za stahování. Je pak na rozhodnutí autora, zda bude svá práva vymáhat, či ne.

6.2.2 Poskytování a využívání odkazu (linking)

Pokud chceme navštívit určitou internetovou stránku, musíme jí nejdříve lokalizovat. Jednou z možností je vypsání jejího URL (Uniform Resource Locator). URL je například http://www.prf.cuni.cz. Na tutéž stránku se ale můžeme dostat pohodlněji jedním kliknutím myši na tzv. odkaz, nebo link či hyperlink. Takový odkaz nám může být odeslán elektronickou poštou, nebo jej častěji nalezneme na jiných Internetových stránkách. To nám umožní přeskakovat mezi jednotlivými stránkami bez nutnosti vypisování URL každé jednotlivé z nich. Můžeme to nazvat surfováním, brouzdáním Internetem a je to jedním z faktorů, který jej činí tak uživatelsky atraktivním a kromě sítě sítí je také sítí těchto odkazů.

Toto jednání jako takové není AZ zakázáno ani jinak ošetřeno, nicméně určitá problematika zde vzniká, i když se týká porušování autorských práv jen nepřímo.

Můžeme rozlišit následující kategorie linkingu:[123]

a) Poskytování odkazů na stránku, na které jsou nelegálně zpřístupněna chráněná díla
b) Poskytování odkazů na stránku, na které jsou legálně zpřístupněna chráněná díla
c) Jiné poskytování odkazu, nejčastěji přímo na jednotlivé části či prvky webových stránek (tzv. deep linking, nebo chceme-li poskytování hloubkových odkazů)
d) Takzvaný „inlinking“ neboli užívání cizího díla ve vlastní webové stránce bez samostatného kopírování tohoto díla, pouze pomocí využití odkazu

a) Poskytování odkazu na webové stránky, které obsahují obsah (nejčastěji hudbu) tam umístěný bez souhlasu autora je nejčastějším případem linkingu. Oprávněná

[123] Čermák, J. Internet a autorské právo, 2. Aktualizované vydání, Linde Praha, 2003

osoba se tak obrací nejen na provozovatele webové stránky, ale také na osobu, která na ní odkazuje a znásobuje tak možnost její navštívení a zásah do práv oprávněné osoby.

b) Poskytování odkazu na stránky s obsahem, který je na nich umístěn v naprostém souladu se zákonem na první pohled neevokuje nic nezákonného. Problémem však může být možnost, že autor stránek si nepřeje, aby na jeho stránky bylo odkazováno.

c) Problematika deep linkingu je následující. Webová stránka má určitou strukturu, zpravidla to není jen plocha k prohlédnutí a obsahuje své podstránky, do kterých je možno se „ponořit". Poskytnutím odkazu již na konkrétní podstránku v této struktuře pak uživateli ulehčuje práci hledáním cíleného obsahu a nasměruje ho přímo k cíli. Tvůrce stránky má však naopak zájem, aby si uživatel prošel strukturou od začátku a to zejména z reklamních důvodů.

d) Charakter inliningu je odlišný od předchozích tří v tom smyslu, že odkaz není poskytován k navštívení stránek, je naopak využíván. Webová stránka pak není sestavená z obsahu, který je umístěn na jejím domovském serveru, ale některý prvek může být „vyvolán" ze serveru jiného. Tento prvek je pak doplněn z jiného prostředí Internetu. Není tak třeba tento prvek ukládat na serveru tvůrce, ale využít jej se stejným výsledkem bez toho.

Poskytování odkazů však dle platného AZ není jednou z forem užití díla dle § 12 a násl., to znamená, že jej přímo neporušuje. Můžeme však připustit nepřímé porušení autorských práv odkázáním na dílo zpřístupnění v rozporu s AZ, což bude případ uvedený pod písmenem a). Půjde pak o posouzení konkrétního případu z hlediska spoluodpovědnosti poskytovatele odkazu. V případě inliningu je to situace jiná, uživatel totiž nemá možnost volby, zda využít odkazu, zda na něj kliknout či ne. Obsah je mu totiž zobrazen přímo. Uživateli se tak zobrazí cílená webová stránka spolu s chráněným obsahem. Čermák[124] zde tvrdí, že se v tomto případě nejedná o užití díla formou sdělování jej veřejnosti s argumentací, že pouze primární akt užití díla, tedy nahrání jej na server, je jeho sdělováním veřejnosti. Zastávám názor opačný, z dikce § 18 AZ zde jde o zpřístupňování díla, což se děje dle mého názoru i jeho zobrazením pomocí inliningu bez ohledu na to, zda osoba odkaz má jeho objekt ve své dispozici či ne.

[124] Čermák, J. Internet a autorské právo, 2. Aktualizované vydání, Linde Praha, 2003

Inliningem lze také rozumět vytvoření nového díla spojením a to spojením cílené webové stránky a vloženého prvku, což se uživateli zobrazí zároveň na displeji jeho počítače. I z toho to úhlu pohledu můžeme vidět porušení autorského práva. Z § 51 AZ totiž můžeme dovodit, že ani nabyvatel licence nesmí dílo spojovat s jiným bez souhlasu autora.

6.2.3 Používání rámování (frames)

Rámování je způsob uspořádání webové stránky do určitých oddílů. Pravidelně bývá horní oddíl věnován provozovateli stránky tak, že je tam umístěno jeho logo. Levý okraj stránky pak je zpravidla navigační a umožňuje se tak lépe orientovat ve struktuře webové stránky. Často je tento oddíl tvořen odkazy na jiné webové stránky a není tak ničím jiným, než výše popsaným poskytováním odkazu. Ve zbytku stránky pak bývá zobrazen obsah, na který je odkazováno, tedy obsah z jiných webových stránek. Pokud je tento obsah neoprávněným užitím autorského díla, pak lze toto jednání právně charakterizovat shodně s inliningem, který je popsán výše.

6.2.4 Výměnné sítě (Peer to peer, P2P)

Výměnné sítě jsou jedním z prostředků výměny dat uživatelů a jejich všeobecně známým artiklem jsou právě díla chráněná AZ. I když mohou být využity k legálním účelům, opak je pravidlem. Z důvodu jejich oblíbenosti a rozšířenosti jim věnuji v této práci více pozornosti.

Výměnná síť je tvořena propojenými počítači svých uživatelů, zejména pomocí Internetu. Na těchto jsou pak nainstalovány aplikace umožňující sdílení souborů. Uživatelé tak ze svého počítače umožňují stahovat[125] jím specifikované soubory a na druhou stranu může stahovat soubory od jiných uživatelů. Je zde proto jiný vztah, než u provozovatele centralizovaného serveru, který zpřístupňuje autorské dílo na jedné straně a uživatelem, který si toto dílo stáhne na straně druhé. Sítě P2P[126] jsou decentralizované a každý článek tak stojí funkčně na stejné úrovni. Z toho též plyne označení „peer to peer“, které lze přeložit jako „rovný rovnému“. Zatímco tedy u centralizovaného systému typu server-uživatel přenosová kapacita při vzrůstajícím počtu uživatelů klesá, u P2P sítí je to právě naopak. Důvodem je možnost stahovat požadovaný soubor od

[125] Pojem „stahování“ rozumějme rozmnožování díla dle § 13 AZ

[126] 2 mezi písmeny P je obvyklou zkráceninou anglického „to“, důvodem je jejich stejná fonetická výslovnost

uživatele, od kterého jej zrovna nikdo nestahuje. Některé sítě však umožňují stahovat jeden a tentýž soubor od různých osob a to i po částech a následně jej „slepit“ v jeden.

P2P sítě můžeme rozdělit do tří kategorií, přitom hlediskem k tomu bude technologie, kterou používají. Z hlediska praxe a soudní judikatury je toto rozlišení důležité zejména k řešení otázky odpovědnosti za zásah do autorského práva. Rozdílné typy těchto sítí tak ovlivňují rozdílný postup proti odpovědným subjektům a rozlišujeme 3 základní typy, jejich princip vysvětlím vždy na nejznámějším představiteli toho kterého typu:[127]

a) Sítě s centrálním vyhledávačem (1. generace)

b) Sítě s decentralizovaným vyhledáváním (2. generace)

c) Sítě s distribuovaným anonymním ukládáním (3. generace)

a) Sítě s centrálním vyhledávačem (1. generace)

Tyto sítě byli prvními peer to peer sítěmi a tou úplně první byl světoznámý Napster. Tato síť fungovala na jednoduchém principu a to tak, že pokud se uživatel chtěl stát členem této komunity, nainstaloval si na svůj počítač software Napster a zaregistroval se. Dále vyčlenil na svém pevném disku určitý prostor, který měl sloužit výhradně k umístění hudebních souborů ve formátu .mp3 za účelem jejich zpřístupnění ostatním takovým členům této komunity. Sdílení pak probíhalo samozřejmě pouze po dobu, po kterou byl ten který člen připojen k síti Internet, neboli on-line. Tento nápad uvedl k životu student Shawn Fanning roku 1999 s úmyslem vytvořit tak úzkou komunitu osob vyměňující si hudební soubory. Tato komunita však nabyla nebývalých rozměrů a to řádově desítek milionů s nespočtem hudebních souborů, které se nacházely nikoliv na centrálním serveru, ale na počítačích koncových uživatelů rozmístěných po celém světě. Tento fakt samozřejmě prakticky znemožňoval směřovat odpovědnost z porušování autorského práva proti jednotlivým poskytovatelům obsahu.

Tato síť však nebyla čistou podobou P2P sítě, neboť prvek decentralizace nebyl zcela naplněn. To již ostatně předesílá zařazení Napsteru do kategorie sítě s centrálním vyhledávačem. Tento systém vyhledávání spočíval v tom, že uživatel položil dotaz na konkrétní nahrávku centrálnímu serveru, který zjistil, kdo ji poskytuje. Poskytovatele pak kontaktoval a byl-li on-line, zkopíroval od něj soubor na disk poptávajícího. To se také Napsteru stalo osudné v následně popsaném soudním sporu.

[127] Čermák, J. Internet a autorské právo, 2. Aktualizované vydání, Linde Praha, 2003

Spor známý jako RIAA(Recording Industry Association of America) vs. Napster byl důsledkem právě úspěchu Fanningova nápadu a také obrat původně neškodné aktivity v lukrativní obchod, který způsobil pokles prodeje nahrávek v hudebním průmyslu. Žaloba na náhradu škody byla podána roku 2000 spolu s návrhem na vydání předběžného opatření, kterým mělo být Napsteru zakázáno poskytování služeb. Soud návrhu vyhověl a i odvolání bylo neúspěšné. Z důvodu decentralizace byla předmětem řízení odpovědnost Napsteru, ale nejprve musela být prokázána přímá odpovědnost uživatelů. Napster zejména argumentoval, že uživatelé stahují soubory oprávněně na základě pravidla „fair use“, které je blízké českému volnému užití díla. Dále pak se snažil zvrátit obvinění tvrzením, že pouze umožňoval stahování vzorků skladeb, které si měl uživatel v případě zájmu zakoupit (tzv. sampling) anebo také tvrzením, že skladby byly komprimované do formátu .mp3 (space-shifting). Neúspěšně. Odpovědnost uživatelů byla prokázána a to zejména na základě nesporného faktu, že 80 % všech děl, s kterými Napster nakládal, bylo chráněno autorským právem a z toho 70 % byly zvukové záznamy vytvořené členy RIAA. Následně pak soud mohl shledat Napster spoluodpovědným za porušování autorských práv uživateli systému (contributory copyright liability). Dále byl shledán tzv. zástupně odpovědným (vicarious copyright liability) z důvodů finančních výhod, které mu plynuly z umísťování reklam v aplikaci a též z důvodu, že vykonával kontrolu nad tímto systémem a proti nelegálnímu jednání nezakročil.

Toto rozhodnutí znamenalo konec Napsateru, který roku 2001 přestal poskytovat služby, což ovšem nebránilo vzniku obdobným sítím, které se vyvarovali jeho chyb a začali používat decentralizované vyhledávání.

b) Sítě s decentralizovaným vyhledáváním (2. generace)

Představitelem tohoto druhu sítě a nástupcem Napsteru se stala síť založená na protokolu Gnutella, nezištně vytvořená programátory společnosti Nullsoft. Byl to otevřený protokol, s nímž umí pracovat několik různých programů, například Morpheus.

Rozdíl spočívá ve vyhledávání, které probíhá výhradně s použitím počítačů koncových uživatelů. Dotaz zde směřuje k minimálně jednomu uživateli sítě, který pokud soubor má, tak jej přímo poskytne. V opačném případě dotaz odešle dalším uživatelům, což znamená lavinovité šíření dotazu a také však výrazně nižší rychlost než

u centrálního vyhledávání. Výhodou je tak roztříštění odpovědnosti mezi koncové uživatele, neboť kromě uživatelů není subjekt mající kontrolu nad obsahem sdělovaných souborů.

Co se týče postihu subjektů, byli ojediněle a exemplárně sankcionováni někteří uživatelé sítí pracující na protokolu Gnutella, kteří porušovali ve větší míře autorská práva. Jejich odpovědnost je nepopiratelná stejně, jako u předchozího případu.

Diskuse probíhá i ohledně odpovědnosti tvůrců protokolu, kterými byl Nullsoft. Většina názorů se však shoduje na tom, že jejich odpovědnost nelze opřít ani o jednu u Napsteru zmíněných doktrín, tedy contributory copyright liability ani vicarious copyright liability.

Třetím subjektem, u něhož je možné zvažovat odpovědnost, jsou tvůrci programů, které pracují právě na protokolu Gnutella. Soudní spor v této věci proběhl v Nizozemí. Byl iniciován kolektivním správcem autorských práv Buma/Stermra roku 2001 a byl veden proti společnosti KaZaA, která vytvořila komunikační software pro sdílení souborů. Soud společnosti nakonec nařídil, aby zastavila užívání svého komunikačního programu. To bylo však prakticky nemožné, neboť již bylo rozšířeno na 20 milionů kopií tohoto programu a společnosti KaZaA nebylo jasné, jak má tomuto užívání zabránit. Rozsudek byl odvolacím soudem zrušen.

c) Sítě s distribuovaným anonymním ukládáním (3. generace)

Představitelem je zde projekt Freenet. Rozdílem je zde nejen způsob vyhledávání, ale též umístění dat. Nejsou umístěny na místní disk uživatele, ale na logický prostor, tvořený místem na discích všech účastníků. Po vložení se tak mohou libovolně přesouvat v závislosti na tom, kde jsou zrovna potřeba. Zjištění subjektu, který autorské právo porušuje, je pak takřka nemožné.[128]

Jak jsem výše nastínil, můžeme odpovědnost směřovat vůči více subjektům participujícím v komunitách výměnných sítí. Na prvním místě přichází přímá odpovědnost koncových uživatelů, která je v případě zpřístupňování autorských děl v P2P sítích shodná se zpřístupňováním těchto pomocí centralizovaného serveru, jak již bylo popsáno. V případě stahování děl koncovými uživateli je tato odpovědnost shodná s tou, o které podám výklad v kapitole 6.3.

[128] Blíže Čermák, J. Internet a autorské právo, 2. Aktualizované vydání, Linde Praha, 2003

Co se týče tvůrců protokolů, na kterých jsou vystaveny výměnné sítě, lze jejich odpovědnost jen těžko dovodit z důvodu nicotné příčinné souvislosti. Ta je vyšší u provozovatelů samotných výměnných sítí, nicméně odpovědnost zde bude možno také hledat jen stěží. Argumentem pro to je fakt, že tyto sítě jsou pouze systémem umožňujícím výměnu dat, nelegální aktivitu pak přinášejí její uživatelé. Nicméně jak bylo uvedeno na případu soudního sporu s Napsterem, je možné spoluodpovědnost dovodit.

6.2.5 Warez fóra

Warez prostředí je pravděpodobně nejnovějším projevem kybernetické kriminality a v drtivé většině se netýká ničeho jiného, než porušování autorských práv. V platném právu tento pojem definován ani jinak upraven není. Původ pojmu je v anglickém slově „wares“, což znamená zboží.[129] Tato činnost spočívá ve zpřístupňování autorských děl na webových stránkách, které se nazývají war/warez fóra. Mají tedy podobu diskusních internetových fór, ale jejich artiklem je nabízení autorských děl k bezplatnému stažení. Díla, která jsou zde nabízena, jsou zejména počítačové programy, filmy, hudba, hry, ale i knihy.

Podstatou této činnosti je zpřístupnění těchto děl veřejnosti co nejdříve a pokud možno dříve, než tak učiní oficiální distributor. To se děje zejména odcizením originálního nosiče při procesu jeho přípravy k jeho oficiálnímu vydání, například při balení CD nosičů osobou, která se na tomto procesu podílí zevnitř (tzv. insider). Takový originál softwaru je pak postoupen zkušeným programátorům, aby obešli účinné technické prostředky ochrany práv, a tento software zbaví bezpečnostních prvků zamezujících jeho kopírování (tzv. cracking, o kterém je pojednáno vzápětí). Následuje pak umístění takového díla na warez fórum, kde si jej může koncový uživatel bezplatně, s podmínkou například pouhé registrace, stáhnout.

U filmů je postup odlišný. Na fórech jsou umísťovány různé „verze“ filmů podle toho, v jaké kvalitě jsou ke stažení. Tou nejméně kvalitní je verze „cam“, což není nic jiného, než film nahraný na kameru při jeho promítání v kině (tzv. camcording). Pokročilejší verze jsou pak získávány například v procesu zpřístupňování filmů recenzentům a kritikům. Takové pak při přehrávání filmu na počítači znázorňují rušivý nápis typu „for your consideration only“, což zdůrazňuje jejich účel. Při vydání filmů na

[129] Wikipedia, http://cs.wikipedia.org/wiki/Warez

DVD nosiče jsou pak filmy komprimovány a ve více či méně kvalitních verzích zpřístupňovány veřejnosti.

Motivací aktérů watez scény není tedy finanční prospěch, i když na většině warez fór jsou pravidelně umístěny reklamy, ale spíše prestiž. Jednotlivé skupiny scény se předhánějí, kdo nabídne publiku dříve co nejkvalitnější podobu autorského díla. Za to například sbírají body a umísťují se v žebříčcích úspěšnosti.

V praxi se díla připravená k distribuci na těchto fórech nahrají na internetový server internetového úložiště, jako je například www.rapidshare.com, www.uloz.to, apod. Po tomto uploadu je odkaz na dílo umístěn na příslušném fóru. Tak je nabídnuto téměř jakékoliv dílo, již připravené k použití, případně opatřené návodem bezstarostného použití, široké laické veřejnosti, která k jeho stažení nepotřebuje takřka žádné hlubší technické vzdělání.

I zde jde o sdělování díla veřejnosti dle § 18 a násl. AZ, které pokud je prováděno bez souhlasu autora nebo oprávněné osoby, je v rozporu se zákonem.

6.2.6 Cracking

V kapitole o hackingu jsem se zmiňoval o pojmu cracker ve smyslu hackera, který je označen jako tzv. black hat a neprovádí svou programátorskou činnost v zájmu posouvání hranic možností programů dále, ale naopak své schopnosti zneužívám. Na tomto místě se zmíním o druhém významu pojmu cracker jako osoby porušující autorská práva. Za cracking, tedy činnost crackerem prováděnou, je v tomto smyslu označováno jednání spočívající v obcházení ochranných prvků, které brání vytváření kopií či nelegálnímu užívání počítačových programů a hudebních nebo filmových produktů.[130] Ve smyslu § 43 odst. 1 zákona 121/2000, autorský zákon, jsou označovány jako účinné technické prostředky ochrany. Jsou jimi:[131]

a) registrační číslo (seriál number), které je nezbytné k úspěšnému nainstalování aplikace

b) časové omezení (time limit), které umožňuje program využívat jen po předem stanovenou dobu, nebo jen se stanovenými funkcemi

c) registrační soubor (key file), který se vkládá k úspěšné instalaci místo registračního čísla

[130] Blíže Matějka, M. Počítačová kriminalita, 1. Vyd. Praha: Computer Press, 2002, s. 73

[131] Blíže Červeň, P. Cracking a jak se proti němu bránit. 1. Vyd. Praha: Vydavatelství a nakladatelství Computer Press, 2001, s. 13

d) samostatný program, který je potřebný k běhu programu jiného

e) hardwarový klíč (dongle), což je technický prostředek, který je připojen ke komunikačnímu portu počítače a bez kterého nelze program spustit

f) kontrola originálního CD/DVD, což je způsob kontroly, zde je v mechanice počítače vložen originální nosič

g) demoverze neboli programy, jejichž jednotlivé části a funkce jsou pro uživatele zablokovány, nebo odstraněny, což je činí nezajímavými pro kopírování

h) další typy ochrany, kombinace předchozích, nebo též metody používané hackery tak, jak jsou zde uvedeny

Cracking bude ve smyslu překonávání technických prvků ochrany charakterizován jako trestný čin porušení autorského práva, práv souvisejících s právem autorským a práv k databázi dle § 270 TZ. Vlastní akt prolomení technické ochrany datového nosiče a následná manipulace s takto zpřístupněnými daty může být trestně právně posouzena též jako trestný čin neoprávněného zásahu k počítačovému systému a nosiči informací podle § 230TZ.[132]

6.3 Stahování děl z Internetu

Stahování autorských děl je párovou kategorií k jejich zpřístupňování, jednáním opačným a smyslem, proč jsou vlastně díla zpřístupňována pomocí internetu. Jestliže jsme zpřístupňování výše charakterizovali dle AZ jako sdělování díla veřejnosti dle § 18 a následujících, stahování bude možno charakterizovat jako jeho rozmnožování dle § 13 AZ. Uživatel zašle požadavek ke stáhnutí počítači, na kterém je cílený soubor uložen. Ten je zašle do počítače uživatele, kde je uložen na nosiči informací, zpravidla na pevném disku. Originální soubor přitom zůstává na počítači, z kterého byl stažen. Je tak vytvořena rozmnoženina. Pro zhodnocení takového jednání musíme nejprve zjistit, zda jde o dílo chráněné AZ a dále charakter zhotovení rozmnoženiny.

Co je dílem, je vyjádřeno v § 2 AZ, jak jsem již výše zmínil. V této souvislosti, a platí to i pro zpřístupňování díla, je samozřejmé, že v kontextu této práce nás nemusí zajímat díla sochařská, architektonická, zkrátka taková, která nejdou rozmnožovat pomocí počítačových sítí. Dle § 2 odst. 6 AZ je omezením pojmu autorské dílo, neboť

[132] Volevecký, P. Kybernetické hrozby a jejich trestně právní kvalifikace. Trestní právo č.1/2011

za něj nepovažuje zejména námět díla sám o sobě, denní zpráva nebo jiný údaj sám o sobě, myšlenka, postup, princip, metoda, objev, vědecká teorie, matematický a obdobný vzorec, statistický graf a podobný předmět sám o sobě. Druhým omezením jsou díla sice způsobilá mít přívlastek autorská, není jim taková ochrana z důvodu veřejného zájmu poskytnuta. Mám na mysli § 3 AZ, který jeho ochranu nevztahuje na úřední díla, právní předpisy, veřejné listiny, úřední dokumentace a jiná taková díla, u nichž je veřejný zájem na vyloučení z ochrany, anebo výtvory tradiční lidové kultury, není-li pravé jméno autora obecně známo a nejde-li o dílo anonymní nebo o dílo pseudonymní (§ 7 AZ).

V otázce pořizování rozmnoženin vyvstává několik otázek. O vytváření technických kopií při procesu přenosu dat mezi počítači jsem se již zmínil a odkazuji proto na tomto místě na kapitolu 6.2, případně na § 38a AZ, který uděluje zákonnou licenci pro dočasné rozmnoženiny.

Obecný princip AZ je takový, že k jakémukoliv užití díla je potřeba souhlasu autora či tento souhlas musí vyplývat z patně uzavřené licenční smlouvy. Výjimkou jsou tzv. volná užití. Dle § 28 odst. 1 AZ lze může každý bez dalšího užít dílo, u kterého uplynula doba trvání majetkových práv, což je obecně 70 let po smrti autora (§ 27 AZ).

Druhou skupinu volných užití zařadil zákonodárce do oddílu 2 AZ: Volná užití a zákonné licence.

6.3.1 Volná užití

Tento institut je z hlediska povahy nakládání s autorskými díly významný a je upraven v § 30 AZ:

(1) Za užití díla podle tohoto zákona se nepovažuje užití pro osobní potřebu fyzické osoby, jehož účelem není dosažení přímého nebo nepřímého hospodářského nebo obchodního prospěchu, nestanoví-li tento zákon jinak.

(2) Do práva autorského tak nezasahuje ten, kdo pro svou osobní potřebu zhotoví záznam, rozmnoženinu nebo napodobeninu díla.

Ustanovení odst. 1 tak uvádí, že užití autorského díla obecně pro osobní potřebu fyzické osoby bez účelu hospodářského nebo obchodního prospěchu, se nepovažuje za užití díla dle AZ. Odst. 2 pak z důvodu právní jistoty stanoví konkrétně, že do autorského práva tak nezasahuje ten, kdo pro svou osobní potřebu zhotoví rozmnoženinu díla, což je případ stahování. Můžeme tak tedy rozlišit mezi užitím díla

nikoliv pro osobní potřebu, pro které je tedy nutno souhlasu autora nebo udělení licence a užití díla pro osobní potřebu.

Podívejme se nyní, co je myšleno onou osobní potřebou. „Osobní potřenou“ se rozumí v soukromí uživatele za účelem např. samostudia, osobní zábavy apod. Získaný zážitek pak může být použit k jakémukoliv účelu, třeba i k podnikání. V soukromí uživatele lze pak chápat užití v rámci domácnosti (§ 115 OZ) jakož i v rámci osob blízkých (§ 116 OZ). Dalšími osobami přítomnými při užití díla pak mohou být pozvaní, individuálně určení hosté domácnosti. Pro představu, volným užitím díla bude stažení filmu z internetu a promítnutí si jej s rodinou.

Podmínka užití díla bez hospodářského prospěchu je vyjádřením základního ústavního principu i zásad evropského komunitárního práva, že užívat cizí majetek bez svolení majitele k vlastnímu hospodářskému prospěchu je zakázáno.

Za připomínku v této souvislosti stojí i diskuse ohledně množstevního rozsahu rozmnožování díla. § 30 odst. 2 AZ dovoluje zhotovit „rozmnoženinu“, což by použitím argumentu ad absurdum znamenalo zhotovení pouze jedné kopie, což by v praxi působilo značné praktické potíže. Uživatel by si mohl např. stáhnout film pro svou osobní potřebu na svůj počítač doma, pokud by si jej chtěl ale zkopírovat (a vytvořit tak druhou rozmnoženinu) na laptop a podívat se na film na pracovní cestě, jednalo by se již o jednání nedovolené. Užití jednotného čísla je však legislativně technickým pravidlem a výklad ad absurdum je zakázaný. Je tedy možno zhotovit si pro osobní potřebu více rozmnoženin. Každý takový konkrétní případ ale bude čelit tzv. tříkrokovému testu, kterým pokud toto jednání neprojde, bude k němu nutný souhlas autora.[133]

Tříkrokový test (three-step test) zavádí § 29 odst. 1 AZ: *Výjimky a omezení práva autorského lze uplatnit pouze ve zvláštních případech stanovených v tomto zákoně a pouze tehdy, pokud takové užití díla není v rozporu s běžným způsobem užití díla a ani jím nejsou nepřiměřeně dotčeny oprávněné zájmy autora.*

Pokud tedy shledáme, že se jedná o dílo volné, musíme brát toto výkladové ustanovení v úvahu při hodnocení míry užití takového díla. Dovolená jsou jen taková užití:

1. která jsou stanovena ve zvláštních případech stanovených v autorském zákoně

[133] Blíže Telec, I.. Tůma, P. Autorský zákon. Komentář. 1. vydání, C. H. Beck, Praha 2007

(Takovým tedy bude volné užití dle § 30)

2. která nejsou v rozporu s běžným způsobem užití díla
3. nejsou jimi nepřiměřeně dotčeny oprávněné zájmy autorů[134]

(Pokud si tedy stáhneme film a podíváme se na něj s rodinou, bude takové jednání v pořádku. Pokud však budeme stahovat každou filmovou novinu a pořádat každý den promítání na veřejném prostranství, půjde již o exces)

Výjimka v podobě § 30 odst. 1, 2 AZ se však nevztahuje na veškerá autorská díla. Dle odst. 3 AZ platí jiný režim pro počítačové programy či elektronické databáze, jejichž užití je stále užitím dle AZ, spadá pod obecný povolovací režim a jejich stahování z Internetu bez autorova povolení porušuje jeho autorská práva. Stejně tak užitím zůstává pořízení záznamu audiovizuálního díla při jeho provozování ze záznamu nebo jeho přenosu (§ 20 AZ, výše zmiňovaný camcording) i pro osobní potřebu fyzické osoby.

S volným užitím díla pak souvisí tzv. bezplatné zákonné licence, které určují případy užití, kterými není zasahováno do práva autorského. Jsou jimi např. citace (§ 31 AZ), katalogová licence (§ 32 AZ), úřední a zpravodajská licence (§ 34 AZ) a další.

6.4 Trestněprávní kvalifikace porušení autorských práv

Kromě trestněprávního postihu porušování autorských práv, který představuje řešení ultima ratio, se nabízejí samozřejmě v první řadě soukromoprávní prostředky ochrany[135], ty ale nejsou z hlediska tématu této práce jejím předmětem. Trestní zákoník chrání autorská práva v blanketní normě § 270 TZ. Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi:

(1) Kdo neoprávněně zasáhne nikoli nepatrně do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, zvukovému či zvukově obrazovému záznamu, rozhlasovému nebo televiznímu vysílání nebo databázi, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.[136]

Předmětem ochrany tohoto ustanovené je ochrana umělecké tvůrčí činnosti a z ní plynoucích požitků. Ústavně právním základ tvoří článek 34 odst. 1 LZPS svou

[134] Telec, I.. Tůma, P. Autorský zákon. Komentář. 1. vydání, C. H. Beck, Praha 2007
[135] V úvahu přicházejí občanskoprávní žaloby s nároky uvedenými v dílu 5 samotného AZ
[136] Další odstavce pak upravují kvalifikované skutkové podstaty

formulací „*Práva k výsledkům tvůrčí duševní činnosti jsou chráněna zákonem*“ a také článek 15 odst. 2 „*Svoboda vědeckého bádání a umělecké tvorby je zaručena*“.

Oproti předcházejícímu znění skutkové podstaty § 270 TZ byla do jejího znění vložena slova „nikoli nepatrně“. Bude třeba zkoumat okolnosti konkrétního případu a to zejména intenzitu zásahu, způsob provedení činu, jeho následky, závažnost zasažení osobnostních a majetkových práv, zkušenost pachatele a další faktory. Přitom způsobů zásahu do autorských práv je nespočet. U osobnostních práv to bude zejména přivlastnění si autorství k dílu, zveřejnění díla bez jeho souhlasu. U majetkových práv pak neoprávněné zhotovování rozmnoženin mnou výše popsanými jednáními.

Z hlediska subjektivní stránky je vyžadován úmysl. Pachatel musí vědět, že jde o autorské dílo, tedy výsledek tvůrčí činnosti autora. Pachatelem samotným pak může být kdokoli.

Závěr

V mé diplomové 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 nejporušovanějšímu, a to autorskému.

V úvodu uvedenou hypotézu o nemožnosti úplné eliminace počítačové a internetové kriminality považuji za potvrzenou. To musíme mít na vědomí při úvahách o potírání tohoto druhu kriminality. 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. Je tedy potřeba, kromě již zmíněných legislativních aktivit, zejména dbát na ochranu informací z hlediska fyzického přístupu k nim. 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. Na jedné straně je nutno zajistit dostatečně kvalifikované pracovníky veřejného sektoru a to zejména orgány činné v trestním řízení, soudce, zákonodárce, na druhé straně je nutností dostatečné povědomí koncových uživatelů počítačů, soukromého sektoru. Každý takový uživatel by měl dbát základních pravidel jako používání dostatečně bezpečných hesel a používat pro každou používanou službu jiné heslo. Důležité je také zálohovat si data, aktualizovat bezpečnostní software počítače, nestahovat data od nevěrohodných a neznámých původců, nenavštěvovat podezřelé stránky a neposkytovat své osobní údaje pokud to není nezbytně nutné. 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.

Seznam použitých zkratek

AZ – Autorský zákon

ES – Evropská společenství

EU - Evropská unie

ICT – informačně komunikační technologie

LZPS – Listina základních práv a svobod

OZ – Občanský zákoník

PC – osobní počítač, nepřenosný (z anglického „personal computer“)

PPC – pocket personal computer (v překladu kapesní osobní počítač)

TZ – trestní zákoník

Úmluva – Úmluva o kybernetické (počítačové) kriminalitě

WWW – world wide web (v překladu celosvětová síť)

Seznam použitých pramenů

Seznam použité literatury

- Bartoň M. Virtuální pornografie, limity svobody umělecké tvorby a svobody projevu a trestní zákon, Právní rozhledy č. 17/2008
- Čermák, J. Internet a autorské právo, 2. Aktualizované vydání, Linde Praha, 2003
- Červeň, P. Cracking a jak se proti němu bránit. 1. Vyd. Praha: Vydavatelství a nakladatelství Computer Press, 2001
- Gibson, W. Burning Chrome. HarperCollins Publishers, 2003
- Gřivna, T., Polčák, R. (eds.). Kyberkriminalita a právo. Praha: Auditorium, 2008
- Jedlička, P. Internetová společnost: Sociální a ekonomické důsledky rozšíření internetu. Praha: FSV UK, 2001
- Jirovský, V. Kybernetická kriminalita (nejen o hackingu, crackingu, virech a trojských koních bez tajemství). Praha: Grada 2007
- Kshetri, N. The global cybercrime industry, Springer-Verlag Berlin Heidelberg, 2010
- Kuchta, J., Válková, H. a kol. Základy kriminologie a trestní politiky. Praha: C.H.Beck, 2005
- Madliak, J., Mihaĺov, J., Porada, V., Štefanková, S. Počítačová kriminalita. In Karlovarská právnická revue 1/2008
- Matějka, M. Počítačová kriminalita, Praha: Computer Press, 2002
- Moore D., Shannon C., Brown J. Core-Red: a case study on the spread and victims of an internet worm. In Proceedings of the Internet Measurement Workshop 2002, Marseille, France
- Musil S. (ed.) Počítačová kriminalita. Nástin problematiky. Kompendium názorů specialistů. Praha: IKSP, 2000
- Novotný O., Vokoun, R. a kol. Trestní právo hmotné – II. Zvláštní část. Praha : Aspi, 2007
- Peníze nebo data. CHIP, 2006, č. 9
- Polčák, R. Právo na internetu. Spam a odpovědnost ISP. Brno: Computer Press, 2007
- Požár, J. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeňek, s.r.o., 2005
- Shinder, D. L. Scene of the Cybercrime: Computer Forensics Handbook, Syngress Publishing, 2002
- Smejkal, V., Sokol, T., Vlček, M. Počítačové právo. Praha: C. H. Beck. 1995
- Smejkal, V., Sokol, T. Postih počítačové kriminality podle nového trestního zákona. Právní rádce, 2009, roč. 17
- Smejkal, V. Internet a §§§, 2. Aktualizované vydání, Grada Publishing, 2001
- Smejkal, V., Čermáková-Vlčková, A. Autorská díla v hromadných sdělovacích prostředcích, Linde Praha, 2009
- Sterling, B. Introduction to The Hacker Crackdown. London: Penguin, 1994

- Šámal, P. a kol. Trestní zákoník II. § 140 až 421. Komentář 1. vydání. Praha: C. H. Beck, 2010
- Študentová, M. Trestněprávní aspekty související se zasíláním e-mailů a zveřejňováním materiálů na webových stránkách. Trestní právo č. 7-8/2007
- Telec, I. Tůma, P. Autorský zákon. Komentář. 1. vydání, C. H. Beck, Praha 2007
- Volevecký, P. Neoprávněný přístup k počítačovému systému v navrhované novele trestního zákona. Trestní právo č.5/2007
- Volevecký, P. Neoprávněný přístup k počítačovému systému v navrhované rekodifikaci trestního zákona. Trestní právo č. 7-8/2008
- Volevecký, P. Kybernetická trestná činnost v mezinárodních dokumentech ES/EU. Trestní právo č. 7-8/2009
- Volevecký, P. Kybernetické trestné činy v trestním zákoníku. Trestní právo č. 7-8/2010
- Volevecký, P. Kybernetické hrozby a jejich trestně právní kvalifikace. Trestní právo č.12/2010
- Volevecký, P. Kybernetické hrozby a jejich trestně právní kvalifikace. Trestní právo č.1/2011
- Wall, D. S. Cybercrime: The Transformation of Crime in the Information Age. Policy press, 2007
- Webster, F. Theories of information society. London: Routledge, 2006
- Zapletal, J. a kolektiv Aktuální problémy kriminologie pro posluchače magisterského studijního programu, 1. vyd. Praha: PA ČR v Praze, 2009

Seznam zákonů České republiky

- zákon č. 2/1993 Sb. ze dne 16. prosince 1992 o vyhlášení Listiny základních práv a svobod (Listina základních práv a svobod)
- zákon č. 106/1999 Sb. ze dne 11. května 1999 o svobodném přístupu k informacím
- zákon č. 123/1998 Sb. ze dne 13. května 1998 o právu na informace o životním prostředí
- zákon č. 40/2009 Sb. ze dne 8. ledna 2009, trestní zákoník
- zákon č. 40/1964 Sb. ze dne 26. února 1964, občanský zákoník
- zákon č. 121/2000 ze dne 7. dubna 2000 o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon)
- zákon č. 127/2005 Sb. ze dne 22. února 2005 o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)
- zákon č. 365/2000 Sb. ze dne 14. září 2000 o informačních systémech veřejné správy a o změně některých dalších zákonů
- zákon č. 480/2004 ze dne 29. července 2004 o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti)

(zákony České republiky citované v této práci jsou v jejich původním označení, ale chápány jsou ve znění pozdějších předpisů)

Seznam právních předpisů ES/ EU

- Úmluva Rady Evropy č. 185 ze dne 23. 11. 2001 o kybernetické (počítačové) kriminalitě
- Dodatkový protokol č. 189 k Úmluvě Rady Evropy o počítačové kriminalitě ze dne 28. 1. 2003 týkající se kriminalizace činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů
- Rozhodnutí rady 92/242/EHS ze dne 31. 3. 1992 o bezpečnosti informačních systémů
- Rámcové rozhodnutí Rady 2000/375/JHA ze dne 29. 5. 2000 o boji proti dětské pornografii na Internetu
- Rámcové rozhodnutí rady 2001/413/SVV ze dne 28. 5. 2001 o potírání podvodů a padělání bezhotovostních platebních prostředků
- Rámcové rozhodnutí Rady 2004/68/SVV ze dne ze dne 22. 12. 2003 o boji proti pohlavnímu vykořisťování dětí a dětské pornografii
- Rámcové rozhodnutí Rady 2005/222/SVV ze dne 24:2:2005 o útocích proti informačním systémům
- Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. 6. 2000 o některých právních aspektech služeb informační společnosti, zejména na elektronickém obchodu na vnitřním trhu (směrnice o elektronickém obchodu)

Seznam internetových zdrojů

- About.com, http://inventors.about.com/od/estartinventions/a/Eniac.htm
- Český statistický úřad, Informační společnost v číslech 2008 , http://www.czso.cz/csu/redakce.nsf/i/informacni_spolecnost_v_cislech_2008_o
- České vysoké učení technické v Praze, Ústřední knihovna, http://knihovny.cvut.cz/vychova/vychova2/internet_zdroj_informaci/historie.html
- Electronic Frontier Foundation, www.eff.org
- Frontline, http://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/notable.html
- Hackerův manifest z roku 1996, Blankenship,L. http://www.soom.cz/index.php?name=recenze/show&aid=286
- Howe, D. The Free On-line Dictionary of Computing. http://foldoc.org/data
- Idnes Bonusweb, http://bonusweb.idnes.cz/magazin/hackeri-ukradli-data-milionu-lidi-blokujte-kreditni-karty-radi-sony-11j-/clanek.A110427_142142_bw-magazin_oz.idn
- Internet Society (ISOC), History of the internet, http://www.isoc.org/internet/history
- Internet users, Update for 2010, http://www.internetworldstats.com
- PCWorld, http://pcworld.cz/novinky/sony-priznava-ze-hackeri-ukradli-citliva-data-uzivatelu-konzoli-ps3-20180
- Schjolberg, S. The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva, 2008, http://cybercrimelaw.net/documents/cybercrime_history.pdf

- Raymond, E., Steele, G. L. (2002) The Jargon File, verze 4.2.2, Project Guttenbergm, http://www.gutenberg.org/ebooks/3008
- Rootkit, http://rootkit.cz/go.php
- Slunečnice, http://www.slunecnice.cz/tipy/prvni-pocitacovy-virus-vznikl-pred-25-lety/,
- Symantec, http://www.symantec.com/cs/cz/about/news/release/article.jsp?prid=20100908_02
- Symantec, http://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password
- Symantec, http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics
- Swiatek, D. Metody odposlouchávání klávesnice, bakalářská práce, 2010, , http://dspace.knihovna.utb.cz/bitstream/handle/10563/13694/swiatek_2010_bp.pdf?sequence=1
- Technet,http://technet.idnes.cz/tec_technika.asp?r=bezpecnost&c=A041103_5285981_bezpecnost
- Tim09 blog, http://tim09.blog.cz/0912/5-vyvoj-a-definice-konceptu-kybernetickeho-prostoru
- Wikipedia, otevřená encyklopedie, http://cs.wikipedia.org/wiki/Internet

Computer and Internet criminality

Keywords: Internet, computer, criminal law

Klíčová slova: Internet, počítač, trestní právo

Résumé (EN):

In my thesis I have tried to analyze questions connected to information in general, as in my opinion the most valuable articles of our days. Information society, of which we are part of, is surrounded with information and has developed certain mechanisms, procedures and technology. My aim has been to consecrate a usage of information and communications technology.

We can say that nowadays advanced world is almost perfectly linked and networked. It is done by virtue of increasing availability of computers and other communication instruments; another reason is constantly escalating technological ingenuity of their interconnection. Crucial role in this matter plays Internet, the net of nets, offering still faster, cheaper and more variable connection of its segments. It enables receiving and providing for information without any territorial, contentual, quantity limitation. Technological progression, which information sector shows, is unusually dynamic and also blond our control. Advances of the development go hand in hand with its disadvantages, to be specific with exploitation of computers and Internet. The question therefore is, if the proportion of benefits information and communications technology and its misuse stays the same and only the quantity extent rises. The answer is unfortunately impossible to find, because the area of Internet, computers and information is changing with every moment and is difficult to estimate, which way it proceeds.

In writing this paper I have considered as the most important to approach the topic from the lay readers point of view and to define the basic terms related to it in the first place. That was the cornerstone to more detailed research of the subject. The next

step was to specify computer and internet criminality and capture its distinctions as regards to the area of its activity, the cyberspace, and also to the subjects involved. The fight against criminality has to be fought in multiple levels, from which the most important for us will be sufficiently effective legislative cooperation between states mainly due to its cross-border effect. I have closely focused on the new criminal code, which regulates cyber crimes more complexly. Those crimes and the ways of theirs realization are described in following chapter with accent on the most typical, hacking. Significant part of the paper was devoted to the copyright, which is being infringed the most.

While debating the computer and internet criminality we have to realize the fact, that it can never be completely eliminated. The only way of fighting it is to establish as effective measures of reducing risks as possible. That is the task for discipline of computer security, which places emphasis on the protection from unauthorized manipulation with computer systems, data, secure communication and data transfer and other aspects. In addition to legislative measure, it is necessary to protect our data from physical violation, which means to keep our CD´s, hard-drives, other media safe stored. On the other hand, the software protection of our computers is needed. It is a purpose of antivirus, antispyware, firewall software. If we take in account technical complexity of information technology, inevitable component of fighting cybercrime will be educational training of law enforcing subjects as well as the computer end-users. The toughest task in my eyes will be to exterminate the disillusion, that cybercrime is something less dangerous and harmful, which is probably given by its immaterial character and nonviolent way of committing. I also claim, that cybercrime is not taken in public properly, which would surely raised awareness of its often astronomical financial impacts.

Despite of all measures we have to realize, that all technology has been created by a man and no security measure has been invented so far, which would be impossible to break. It is therefore good to notice, that the basic element of technology progression and also misusage of our information society is a man himself. It is required to begin here and realize the dangers and a possible damage of seemingly such harmless activity, as using computers is.