Univerzita Karlova v Praze
Právnická fakulta

Štičková Věra

Kriminologické aspekty kybernetické kriminality

Diplomová práce

Vedoucí diplomové práce: doc. JUDr. Bc. Tomáš Gřivna, Ph.D.
Katedra trestního práva

Datum vypracování práce: 27. června 2016

Čestné prohlášení

Prohlašuji, že předloženou diplomovou práci jsem vypracovala samostatně a že všechny použité zdroje byly řádně uvedeny. Dále prohlašuji, že tato práce nebyla využita k získání jiného nebo stejného titulu.

V Praze dne 27. června 2016

.....

Věra Štičková

Poděkování

Ráda bych touto cestou poděkovala vedoucímu své práce, panu doc. JUDr. Bc. Tomáši Gřivnovi, Ph.D. za jeho ochotu a rady, které mi pomohly práci dokončit. Dále také děkuji svým rodičům, kteří mne po celou dobu mého studia podporovali a poskytli mi skvělé zázemí pro rozvoj. Také děkuji svému příteli, a to nejen za to, že je mi vždy oporou, ale především za jeho trpělivost, kterou semnou hlavně v posledních měsících měl.

OBSAH

Úvod **1**

1. Úskalí vývoje **3**

2. Terminologie **3**

2.1 Počítačová, informační a internetová kriminalita 3

2.2 Kybernetická kriminalita 6

3. Pojem Kyberprostoru **6**

4. Specifika kybernetické kriminality **7**

4.1 Dostupnost 7

4.2 Nízké náklady 8

4.3 Globálnost 8

4.4 Anonymita 8

4.5 Latence 9

4.6 Nevyrovnanost 9

5. Právní regulace **10**

5.1 Vnitrostátní právo 11

5.1.1 Trestní zákoník 11

5.1.2 Zákon o kybernetické bezpečnosti 13

5.2 Mezinárodní právo 14

5.2.1 Úmluva Rady Evropy o kybernetické kriminalitě 14

6. Kriminalita v kyberprostoru **15**

6.1 Útoky proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů 17

6.1.1 Průnik do systému a oklamání uživatele 17

6.1.1.1 Prolamování hesel 17

6.1.1.2 Keylogger 18

6.1.1.3 Phishing 19

6.1.1.4 Pharming 20

6.1.1.5 Další techniky a nástroje 21

6.1.2 Malware 21

6.1.2.1 Počítačové viry a červy 22

6.1.2.2 Trojské koně 22

6.1.2.3 Spyware 23

6.1.3 DoS, DDoS útoky 24
6.2 Útoky spočívající ve vytváření a šíření škodlivého obsahu 24
6.2.1 Dětská pornografie 25
6.2.2 Extremismus a násilí 26
6.2.3 Kybergrooming 27
6.2.4 Kyberšikana 27
6.2.5 Hoax 28
6.2.6 Ostatní 29
6.3 Útoky spočívající v porušování práv duševního vlastnictví 29
6.3.1 Práva duševního vlastnictví 30
6.3.2 Průmyslové vlastnictví 31
6.3.3 Autorské právo 31
6.3.3.1 Předmět autorského práva 32
6.3.3.2 Obsah autorského práva 33
6.3.3.3 Porušení autorského práva a trestněprávní kvalifikace 35
6.3.3.4 Autorské dílo v kyberprostoru 36
6.3.3.5 Filehosting 38
6.3.3.6 Peer-to-Peer 41
6.3.3.7 Warez, warez fóra, linking 42
6.3.3.8 Embedded linky 43
6.3.3.9 Shrnutí 45
6.4 Tradiční kriminalita v novém kabátě 46
6.4.1 Podvodná jednání 46
6.4.2 Zneužívání platebních karet 47
6.4.3 Kyberterorismus 48
6.4.4 Kyberstalking 49
7. Pachatel a oběť kyberkriminality 50
7.1 Jaký je pachatel kyberkriminality a kdo je hacker? 50
7.1.1 Hacker (a Cracker) 52
7.2 Existuje typologie pachatelů kyberkriminality? 53
7.2.1 Dělení na amatéry a profesionály 54
7.2.2 Dělení dle Smejkala 54
7.2.3 Dělení dle znalosti a vybavenosti pachatele 55
7.2.4 Shrnutí 56
7.3 Pachatel kybernetické kriminality a jeho motiv 56
7.4 Oběť kybernetické kriminality 57
8. Současný stav kybernetické kriminality 59

9. Boj proti kybernetické kriminalitě 60
9.1 Prevence 61
9.2 Represe 62
10. Vybrané zahraniční přístupy k řešení kybernetické kriminality 62
10.1 Německo a dětská pornografie 63
10.2 Francie a autorské právo 65
Závěr 68
Seznam zkratek 71
Seznam použitých pramenů 72
Abstrakt 77
Abstract 78

ÚVOD

Od dob, kdy byl pro většinu společnosti počítač a Internet něco nepochopitelného, mnohdy nechtěného a často také nedosažitelného, se hodně změnilo. Dnes už máme malé a lehké mobilní telefony, které jsou schopné nám nahradit počítač, a život bez připojení k Internetu si skoro neumíme představit.

Internet je nyní zcela běžnou součástí našich životů a co víc, podle OSN je dokonce připojení k Internetu lidským právem, které státy musí svým občanům garantovat.

Ale co je to vlastně Internet? Není to snad jedno a to samé jako kyberprostor? A proč se tato práce nejmenuje "Internetová kriminalita"? To jsou základní otázky, na které ve své práci odpovím.

Předně je ale třeba uvést, že kybernetická kriminalita je poměrně nový společenský jev, který se ovšem stává větším a větším nebezpečím. Lidé už si zvykli na užívání informačních a komunikačních technologií (dále také jako "ICT") ve velkém, čím dál tím víc se naše životy a aktivity stávají virtuálními. Na druhé straně ale uživatelům ICT chybí obezřetnost a uvědomění si nebezpečí, které se s jejich používáním pojí.

Smyslem této práce je proto vysvětlit, co pojem kybernetické kriminality obnáší. Chci se zabývat nejen vývojem tohoto fenoménu, ale především jeho podstatou, tedy škodlivými aktivitami a činnostmi, které jsou jeho obsahem. Kladu si za cíl nashromáždit maximum aktuálních informací, které se kybernetické kriminality týkají, a vytvořit o ní jasný a ucelený výklad. Tato práce by se tak mohla stát základním přehledem rizik, která na nás v kyberprostoru číhají.

V úvodních kapitolách se budu věnovat především otázce terminologie. Jak jsem uvedla shora, je třeba jasně odlišit pojmy kyberprostor a Internet, a objasnit, proč dnes mluvíme o kybernetické kriminalitě.

Dále se budu zabývat i jednotlivými specifiky kybernetické kriminality. Tedy tím, čím je odlišná od ostatních druhů kriminality, tím, co z ní dělá tak speciální jev.

Pojem kybernetické kriminality se v poslední době mnohokrát objevil i v médiích, a spolu s ním i pojem kyberzločinci, kteří páchají kyberzločiny. Máme ale nějaké

kyberzločiny v naší české právní úpravě? Této otázce se budu věnovat v kapitole týkající se právní úpravy, která je samozřejmě nezbytnou součástí každé kriminality a také každé práce, která se tím kterým druhem kriminality zabývá.

Jádro celé mé diplomové práce leží v kapitole, která se zabývá škodlivým jednáním v kyberprostoru. Záměrně nepoužívám termín "trestná činnost", protože ne vždy je popsané jednání trestným činem. Jako třeba v případě šikany. Ta se díky ICT mnohem snáz provádí, ba dokonce může mít mnohem větší dopad, ale nejde o trestný čin. Toto je zásadní pro uvědomění si, jakou sílu kyberprostor má a také proto, abychom pochopili, že se stal místem, kam přesouváme náš život, a to jak se vším dobrým, tak i s tím špatným. To znamená, že tam můžeme narazit na stejně nepříjemné věci, na které jsme zvyklí v reálném světě. Proto je nutné být obezřetní a přijímat podobná opatření, jako přijímáme v běžném životě pro to, abychom byli v bezpečí.

Zvláštní pozornost pak věnuji autorskému právu, které je mi osobně blízké a jehož porušování je jedním z nejčastějších projevů kybernetické kriminality vůbec.

Dále se budu zabývat i osobou pachatele a oběti kybernetické kriminality, což jsou základní aktéři celé problematiky.

V závěru své práce se budu věnovat také aktuálnímu stavu kybernetické kriminality v České republice, kde chci upozornit především na rostoucí trend tohoto fenoménu. V souvislosti s tím zmíním i to, jaká jsou preventivní a represivní východiska, kde chci poukázat zejména na korelaci činnosti Policie ČR se zvyšujícím se počtem trestných činů v oblasti kybernetické kriminality.

V poslední kapitole se pak budu zabývat tím, jak také jiné státy vybrané problémy z kybernetické kriminality řeší. Jak ještě mnohokrát zmíním, kybernetická kriminalita je problémem celosvětovým. Já jsem se proto rozhodla zaměřit na to, jak s ním bojují v zahraničí.

1. ÚSKALÍ VÝVOJE

Počítače, chytré telefony, připojení k Internetu. Vymoženosti dnešní doby, které nás obklopují na každém kroku. Jsou prostředkem k práci i zábavě, vytvářejí prostor k realizaci a vůbec jsou každodenní součástí našich životů.

Informační a komunikační technologie mají vedle kladů bohužel i svou stinnou stránku. Naše závislost na nich roste a to spolu s globálním připojením a množstvím sdílených dat vytváří dokonalé prostředí k páchání trestné činnosti.

Zdá se, že čím víc jde pokrok vpřed, tím horší se situace stává. Kybernetická kriminalita je totiž celosvětově rostoucí fenomén.[1] A přestože není nikde přesně definován, je možné, a vlastně i žádoucí, se vzhledem k jeho rozsahu věnovat jeho dílčím aspektům.

2. TERMINOLOGIE

Než přistoupím k výkladu celé problematiky týkající se kybernetické kriminality, je nezbytné tento pojem odlišit od ostatních pojmů, které mají podobný, či stejný význam.

2.1 Počítačová, informační a internetová kriminalita

Termín počítačová kriminalita se objevil současně s příchodem prvních počítačů (v druhé polovině 20. století).[2] Vzhledem k tehdejším možnostem bylo takové označení logické, neboť trestná činnost spočívala v protiprávní manipulaci s počítačem. Jednalo se o jeho ničení (sabotáže), neoprávněné užívání, nebo o změny údajů v počítači (tzv. dokladové delikty).[3]

Musil v roce 2000 definoval počítačovou kriminalitu obecně jako *každou nekalou činnost páchanou s pomocí počítače.*[4] To je ale definice velice obecná, a tak (i

[1] Studie OSN o kyberzločinu, dostupné online: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf), s. 6
[2] CLOUGH, J. *Principles of cybercrime*. New York: Cambridge University Press, 2010, s. 4
[3] SMEJKAL, V. *Internet a §§§*. 1. vyd. Praha: Grada, 2001, s. 154-155
[4] MUSIL, S. *Počítačová kriminalita: nástin problematiky : kompendium názorů specialistů.* Vyd. 1. Praha: Institut pro kriminologii a sociální prevenci, 2000, s. 6

vzhledem k výše uvedeným rozličným jednáním) bylo nutné podrobnějšího rozlišení. Například Matějka později uvádí, že existují dvě základní kategorie počítačové kriminality a to jsou protiprávní jednání směřující proti počítači a protiprávní jednání spáchaná s využitím počítače.[5] Taková definice byla vhodnější proto, že lépe postihovala situace, kdy byl počítač buď předmětem trestné činnosti, anebo jejím prostředkem.

Na tomto místě se musím pozastavit nad úvahou Jiřího Krupičky, kterou uvádí ve své disertační práci. A sice, že *obecné definice počítačové kriminality se potýkají s problémem, a to že zahrnují i jednání, která s počítačovou kriminalitou nemají nic společného, například pokud pachatel počítačem udeří oběť trestného činu do hlavy a způsobí jí tak těžké zranění.*[6] Taková myšlenka mi přijde absurdní. Ne proto, že by někdo nemohl určitou součástí počítače (například klávesnicí) druhému ublížit, ale proto, že takové jednání bychom přeci nezařazovali pod počítačovou kriminalitu a naopak by se jednalo o trestnou činnost namířenou proti životu a zdraví a popřípadě proti majetku.

Zpětně se tedy vracím k podrobnějšímu dělení Matějky a dodávám, že ani on nepovažoval za "prostředek trestné činnosti" to, že by pachatel použil počítač, nebo jeho část jako nástroj k fyzickému ublížení na zdraví. Jednoduše je jím počítač chápán jako cíl trestné činnosti, anebo nástroj, který jí usnadňuje.

Co se týká proměn terminologie, tak je třeba se dále zaměřit na vývoj techniky. Postupně totiž docházelo k propojování počítačů mezi sebou a vznikly první počítačové sítě a mezi nimi ta nejznámější, Internet.

Internet je tzv. "síť sítí", je to systém celosvětově propojených počítačových sítí, díky nimž mezi sebou počítače mohou komunikovat. Internet je pro většinu obyvatel synonymem pro tzv. "www" (world wide web, web), což je ale systém pro prohlížení, ukládání a odkazování dokumentů. Je ale pouze jednou ze služeb, které Internet nabízí, např. vedle známé "e-mail" služby a dalších.[7]

Příchodem Internetu se také transformovala počítačová kriminalita. Připojení k síti totiž vytvořilo nové možnosti páchání trestné činnosti.

---

[5] MATĚJKA, M. *Počítačová kriminalita*. Vyd. 1. Praha: Computer Press, 2002, s. 6

[6] KRUPIČKA, J. *Trestněprávní a kriminologické aspekty internetové kriminality*. Praha 2012. Disertační práce, s. 10

[7] https://cs.wikipedia.org/wiki/Internet, https://cs.wikipedia.org/wiki/World_Wide_Web, (zobrazeno 24.1.2016)

V zahraniční literatuře je trestná činnost spojená s počítačem a sítí (resp. Internetem a dalšími sítěmi) označována jako "kyberzločin" (cybercrime) nebo "kyberkriminalita" (cybercriminality).[8] V České republice se ale v průběhu času vytvořily zvláštní kategorie tzv. "informační" nebo také "internetové" kriminality.

Tak například Smejkal v jedné ze svých starších publikací uvedl, že vedle počítačové kriminality existují ještě nové druhy kriminality, tedy "informační trestná činnost" a "internetová trestná činnost".

V prvním případě je pozornost zaměřena na informaci, která je prostřednictvím Internetu šířena, shromažďována, prezentována atd., a to v rozporu se zákonem. Internetovou trestnou činností pak autor označuje páchání trestné činnosti v internetovém prostředí.[9] V tehdejší době zřejmě mělo takové rozlišení význam, podle mne už je dnes ale bezpředmětné. Nemyslím si, že můžeme izolovat problematiku týkající se informací od další trestné činnosti, která v kyberprostoru probíhá a už vůbec ne Internet a počítač, jakožto hlediska pro rozlišení různých druhů kriminálního jednání.

Nicméně Policie ČR ve své zprávě o stavu vnitřní politiky pro rok 2014 užívá taktéž termín "informační kriminalita" a to pro *trestnou činnost páchanou v prostředí informačních technologií včetně počítačových sítí, kdy předmětem útoku je samotná oblast informačních technologií nebo je tato trestná činnost páchána za výrazného využití informačních technologií. Zejména se jedná o zneužívání internetu.*[10]

Na téma "internetová" kriminalita byla také sepsána nejedna akademická práce.[11]

Kuchta se rovněž zabývá zvlášť počítačovou a internetovou kriminalitou, ale také zmiňuje, že internetová kriminalita je součástí té počítačové, neboť *trestná činnost na internetu se děje výlučně prostřednictvím výpočetní techniky nebo je výpočetní technika sama o sobě cílem této trestné činnosti, kdežto ne všechna kriminalita spáchaná výpočetní technikou je spáchána na internetu nebo jeho prostřednictvím.*[12]

---

[8] např. MOORE, R. *Cybercrime: investigating high-technology computer crime*. 2nd ed. Amsterdam: Elsevier, 2011, s. 4

[9] SMEJKAL, V. (2001).: op. cit., s. 176- 184

[10] Zpráva MV o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky v roce 2014 (dále jen "Zpráva MV"), dostupné online http://www.mvcr.cz/clanek/statistiky-kriminality-dokumenty.aspx, s. 61

[11] např. práce Jiřího Krupičky na téma Trestněprávní a kriminologické aspekty internetové kriminality, nebo práce Daniela Zemana na téma Internetová kriminalita, obě z r. 2012

[12] KUCHTA, J., VÁLKOVÁ H. a kol. *Základy kriminologie a trestní politiky*. Vyd. 1. Praha: C.H. Beck, 2005, s. 515

Toto je dle mého neměnný fakt, který popírá rozlišování počítačové, informační nebo internetové kriminality a odkazuje tak k univerzálnímu pojmu "kybernetické kriminality", který nejlépe postihuje celou problematiku trestné činnosti v oblasti informačních a komunikačních technologií.

2.2 Kybernetická kriminalita

Z doposud uvedeného vyplývá, že termíny "počítačová", "informační" a "internetová" kriminalita se více či méně překrývají. Smejkal ve své nejnovější publikaci zabývající se kybernetickou kriminalitou sám uvádí, že dnes se spíše než počítačová kriminalita užívá pojem kybernetická, protože k útokům dochází v tzv. kyberprostoru, který je tvořen počítačovými sítěmi.[13] *Je to obdobný příměr, jako když se mluví o organizované kriminalitě, kde je specifickým prvkem pro změnu právě organizovanost.*[14]

Já jsem se ve své práci rozhodla užívat současně termíny "kybernetická kriminalita" a "kyberkriminalita". Toto pojmenování vnímám jako nejvhodnější nejen vzhledem k dané problematice (kriminalita, která se odehrává v kyberprostoru), ale také proto, že je to v souladu se zahraniční literaturou. Byť je pravda, že se tato označení objevují stabilně už i v té české.[15] Myslím si, že "převzetí" zahraniční terminologie odstraňuje problematická dělení a složité definice, které tuto oblast trestné činnosti provázely.

3. POJEM KYBERPROSTORU

Pokud má kyberkriminalita svá zvláštní specifika, tak je to bez pochyb dáno tím, kde k ní dochází. Je to místo, které označujeme jako kyberprostor, což je pojem, který pochází z anglického "cyberspace", a který je definován různě.

Například zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů rozumí kybernetickým prostorem digitální prostředí, umožňující

[13] SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, s. 15
[14] TAUCOVÁ, Z. Kyberkriminalita a další kyberhrozby, *Policista*. 2015, č. 1, s. 6
[15] např. GŘIVNA, T., POLČÁK R.**.** *Kyberkriminalita a právo*. Vyd. 1. Praha: Auditorium, 2008., nebo JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007 a SMEJKAL, V. (2015).: op. cit.

vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.

Kyberprostor lze chápat jako pomyslné prostředí, ve kterém probíhá komunikace v počítačových sítích.[16] Jinými slovy je to virtuální svět, tvořený informačními a komunikačními technologiemi.[17] Existuje díky kybernetické infrastruktuře, čímž můžeme rozumět PC, notebooky, chytré telefony, routery, servery, kabeláže atd. A díky tomu pak může být zaplňován daty uživatelů, jakožto jejich projekcí do tohoto paralelního světa.[18]

Zásadní je, jakou měrou jsou s ním spjaty naše životy. Běžně jej využíváme ke komunikaci, např. skrze e-mail, sociální sítě a video-hovory, také k vyhledávání či shromažďování informací a obecně pro zábavu.[19] Takové prostředí, kde sdílíme svá data, jež pro nás mají pochopitelně svou hodnotu, a které je navíc celosvětově propojené, je lákavým místem pro páchání trestné činnosti.[20]

S ohledem na podstatu kyberkriminality je třeba mít na paměti, že kyberprostor nerovná se Internet nebo jiná počítačová síť (např. zaměstnanecká), ale soubor sítí a zařízení, vytvářející interaktivní prostředí, v němž mohou jeho uživatelé komunikovat.

4. SPECIFIKA KYBERNETICKÉ KRIMINALITY

Teď když je zřejmé, že se kyberkriminalita od ostatních druhů kriminality určitým způsobem odlišuje, je na místě uvést ony dílčí prvky, které jsou pro ni charakteristické, a které jsou často také důvodem jejího vzniku a neustálého růstu.

4.1 Dostupnost

Můžeme jí vnímat jednak dostupnost finanční ale i praktickou. Počítače, chytré telefony aj. se dnes dají pořídit za velmi přívětivou cenu, a i když to nejsou a priori prostředky k páchání trestné činnosti, svou dostupností jí značně usnadňují.

[16] Volně přeloženo z http://www.oxforddictionaries.com/us/definition/american_english/cyberspace (25.1.2016)
[17] GŘIVNA, T., SCHEINOST M., ZOUBKOVÁ I.. *Kriminologie*. 4., aktualiz. vyd. Praha: Wolters Kluwer, 2014, s. 334
[18] http://www.businessit.cz/cz/kyberneticka-kriminalita-i-co-se-deje-v-kyberprostoru.php (25.1.2016)
[19] GŘIVNA, T., SCHEINOST M., ZOUBKOVÁ I.: op. cit., s. 334
[20] WALL D. S. *Cybercrime: the transformation of crime in the information age.* Reprint. Cambridge, UK: Polity, 2008., s. 32

Vývoj informačních a komunikačních technologií posledních let, který rozhodně neustává, spolu s jejich oblibou a vlastně i potřebou zapříčinily, že se ICT rychle rozšířily mezi obyvatelstvo celého světa. Z původně drahých a těžkých zařízení, která vlastnili v podstatě jen ti nejbohatší, se stala výkonná a oproti dřívějšku levná a snadno přenosná technika.

A tak jsou dnes trestné činy v kyberprostoru páchány v pohodlí domova, nebo vlastně kdekoliv a prakticky kýmkoliv. A také vůči komukoliv. Dostupností ICT totiž vzrůstá obecně počet jejich uživatelů, tedy i potenciálních obětí.

4.2 Nízké náklady

Spolu s dostupností moderních technologií se pojí také nízké náklady pachatelů kyberkriminality. Vzhledem k tomu, že tato trestná činnost vyžaduje, vedle schopností pachatele, pouze vybavení (a občas stačí opravdu jen to základní) a poté případně připojení k té které síti, tak je to, ve srovnání s ostatními druhy trestné činnosti, skutečně jedna z těch nejméně nákladných v poměru ke škodám, které může způsobit.

4.3 Globálnost

Zatímco běžná trestná činnost se zpravidla odehrává na témž místě, kde působí pachatel, pro kyberkriminalitu je spíše charakteristický její přeshraniční charakter. Díky propojenosti sítí je dosah pachatelů v podstatě bezbřehý. Jejich působnost je celosvětová, a z domova tak mohou páchat trestnou činnost, jejíž následky nastávají klidně na zcela jiném kontinentu. Taková propojenost zkracuje nejen vzdálenosti, ale i čas, který je k provedení trestného činu obvykle nezbytný.

4.4 Anonymita

V prostředí kyberprostoru je snadné svou identitu skrýt, nebo vystupovat pod falešným jménem, což může být pro některé pachatele okolnost, která je podporuje v trestné činnosti. Především fakt, že nemusí stát své oběti tváří tvář, může jejich úmysl jiného poškodit značně usnadnit. Anonymita kyberprostoru dodává lidem kuráž páchat trestné činy, kterých by se třeba v reálném světě nedopustili, typicky např. krádeže.

Nicméně pravda je taková, že pachatel za sebou v kyberprostoru jisté stopy zanechává (např. IP a MAC adresy zařízení, s nímž útok provádí)[21] a je možné jej při technické zdatnosti vypátrat.

4.5 Latence

V oblasti kyberkriminality se setkáváme s vysokou latencí. Tedy situací, kdy přesně nevíme, jakého rozsahu kriminalita skutečně dosahuje. Obecně nám v tom brání především chybějící údaje o obětech trestné činnosti. Je běžné, že ty kolikrát ani netuší, že jsou cílem útoku, třeba proto, že neví, že dané jednání (např. to, že má ve svém PC spyware[21]) je trestné.[22] To znamená, že trestný čin pak ani neohlásí. Anebo v případě že o trestném činu ví, tak je může od jeho ohlášení odrazovat fakt, že si uvědomují vlastní protiprávní chování, např. že sami využívají nelegální software.

4.6 Nevyrovnanost

Posledním a důležitým znakem kybernetické kriminality je nevyváženost mezi jednotlivými státy světa jednak v jejich technické vyspělosti, ale také možnostech jak se proti kyberkriminalitě bránit.

Kyberkriminalita je celosvětový fenomén, ale celý svět není připravený proti ní současně efektivně postupovat. Brání tomu rozdíly mezi stupněm vývoje daných zemí (například USA vs. státy severní Afriky).

Může jít předně o problém nedostatečné úrovně technologického zázemí dané země. To má důsledek v tom, že je snadné některé země využít pro páchání trestné činnosti a především proto, že takové zemi chybí účinné nástroje jak proti kyberkriminalitě zasáhnout. Také může být potíž v chybějící právní úpravě, neboť každá země má odlišný katalog trestných činů. U méně vyspělých států mohou chybět účinné prostředky k potírání trestné činnosti obecně.

[21] GŘIVNA, T., SCHEINOST M., ZOUBKOVÁ I.: op. cit., s. 337
[22] Idem., s. 338; Spyware je software určený ke sledování aktivity uživatele (např. navštívené internetové stránky) nebo obsahu jeho zařízení (např. nainstalované programy, přístupová hesla atp.).

5. PRÁVNÍ REGULACE

Jak jsem v předešlém dílu naznačila, existence kvalitní právní úpravy je jedním z předpokladů pro úspěšný boj s kyberkriminalitou. Právo je dynamický nástroj, který umožňuje státu reagovat na nové společenské jevy, jedním z nichž kybernetická kriminalita bezpochyby je.

Cílem státu je pomocí zákonů a jiných předpisů regulovat chování společnosti. Pokud se týká konkrétně prostředí kyberprostoru, tak se může nabízet otázka, zda je taková regulace potřeba.

Například J. Barlow, prostřednictvím Electronic Frontier Foundation, kterou založil, *prosazuje svobodu jedince na internetu a zpochybňuje legitimitu jakékoli jeho právní regulace.* [23] Tato organizace vydala v roce 1996 Deklaraci nezávislosti kyberprostoru[24], která promlouvá k vládám a autoritám světa a vymezuje se proti jejich snahám regulovat kyberprostor. Říká, že vlády nedostaly souhlas uživatelů k tomu, aby v kyberprostoru uplatňovaly svou moc.

Ovšem vzhledem ke kriminálním aktivitám v kyberprostoru většina uživatelů usměrňování státu, respektive jeho ochranu, spíše vítá. I když je pravda, že hranice mezi vítaným a nechtěným je tenká. Mohlo by velice snadno dojít k tomu, že regulace zpřísní a najednou z Internetu nebude svobodné médium, jak jsme na něj dnes víceméně zvyklí. A to je třeba říci, že už nyní ve státech světa běžně funguje cenzura[25]. Takovým příkladem je například Čínská lidová republika, jejíž vláda mohutně blokuje služby společnosti Google.[26]

V souvislosti s rostoucí kybernetickou kriminalitou tak státy začaly přijímat příslušná opatření. A to nejen v rámci své vlastní vnitrostátní úpravy, ale i mezi sebou, na mezinárodní úrovni.

Zde je třeba upozornit na rozmanitost jednotlivých národních úprav. Ty se liší nejen svým obsahem, ale i tím, které právní odvětví se kyberkriminalitou zabývá.

I když trestní právo je jako odpověď na kybernetickou kriminalitu vnímáno jako nejvhodnější, je možné užít i jiné obory práva, např. právo civilní (které řeší právní

[23] GŘIVNA, T., SCHEINOST M., ZOUBKOVÁ I.: op. cit., s. 334
[24] A Declaration of the Independence of Cyberspace, dostupné online: https://www.eff.org/cyberspace-independence
[25] https://cs.wikipedia.org/wiki/Cenzura_na_internetu
[26] http://byznys.ihned.cz/c1-63309180-cina-zablokovala-gmail-jde-o-dalsi-cenzuru-tvrdi-organizace-greatfire (zobrazeno 3.2.2016)

vztahy mezi osobami) anebo správní (které řeší právní vztahy mezi osobami a státem).[27]

Já se v následujícím oddílu budu zabývat pouze právní úpravou českou a mezinárodní.

5.1 Vnitrostátní právo

V České republice se ke kyberprostoru váže hned několik právních předpisů. *Kybernetickou bezpečností se zabývá především zákon č. 480/2004 Sb., o některých službách informační společnosti, zákon č. 127/2005 Sb., o elektronických komunikacích, a zákon č. 1011/2000 Sb., o ochraně osobních údajů*.[28]

Důležité místo má také zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále v textu jen "zákon o kyb. bezpečnosti" nebo "ZKB"). Kriminálním chováním v prostředí kyberprostoru jako takovým se pak pochopitelně zabývá zákon č. 40/2009 Sb., Trestní zákoník (dále jen "trestní zákoník" nebo "TZ"). Jejich rozboru se budu věnovat v následujících pododdílech.

5.1.1 Trestní zákoník

O trestním zákoníku, který vstoupil v účinnost 1. ledna 2010, se dnes už moc nehodí mluvit jako o novém, nicméně je třeba uvést, že zákon skutečně reaguje na potřeby doby a při jeho přípravě nebyla opomenuta ani kybernetická kriminalita.

Zákonodárce sice v trestním zákoníku nevytvořil "zvláštní" skutkové podstaty, které by měly před svým názvem předponu "kyber" nebo přímo kategorii TČ s názvem "kyberzločiny". A proto je trochu zavádějící mluvit v ČR o "kyberzločinech", byť se to pro zjednodušení i s ohledem na zahraniční literaturu nabízí (anglicky "cybercrime" = kyberzločin). Ale za to se na trestněprávní jednání v oblasti kyberprostoru myslelo jiným způsobem.

U některých kvalifikovaných skutkových podstat trestných činů je uvedena jako zvlášť přitěžující okolnost pokud budou spáchány prostřednictvím "veřejně přístupné počítačové sítě"[29]. Čímž se myslí *funkční propojení počítačů do sítí s cílem vytvořit informační systém pracující s tzv. dálkovým přístupem, jakým je především internet*

[27] Studie OSN o kyberzločinu.: op. cit. s. 52
[28] GŘIVNA, T., SCHEINOST M., ZOUBKOVÁ I.: op. cit., s. 351
[29] např. TČ Pomluvy- §184 odst. 1, 2 trestního zákoníku; nebo TČ Šíření pornografie podle §191 odst. 1, 3 písm. b) trestní zákoníku.

a jiné podobné informační systémy (např. francouzský Minitel). Z technického hlediska je veřejně přístupná počítačová síť soustavou serverů, datových komunikací a k nim připojených počítačů.[30]

Dále v trestním zákoníku najdeme některé trestné činy, které už ve svém názvu operují s pojmy počítačový systém[31] a nosič informací[32] čímž jasně evokují souvislost s kyberprostorem. Mohli bychom je nazvat kategorií "počítačových trestných činů". Jde o následující trestné činy: § 230 TZ Neoprávněný přístup k počítačovému systému a nosiči informací, § 231 TZ Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat a § 232 TZ Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti. K jejich zavedení nás zavazuje Úmluva o kybernetické kriminalitě, které se budu věnovat později. Předmětem ochrany těchto trestných činů jsou víceméně shodně počítačová data, počítačový systém a nosič informací, zejména jejich bezpečnost, důvěrnost a integrita.

Poslední varianta trestných činů, které mohou mít souvislost s kyberprostorem, jsou již známé trestné činy, respektive skutkové podstaty běžné v reálném světě, pod něž dané protiprávní jednání, k němuž však dochází v kyberprostoru, subsumujeme. Tak tomu je například u Phishingu[33] který bychom mohli podřadit pod TČ podvodu podle § 209 odst. 1 trestního zákoníku.

Je tedy patrné, že možnosti trestněprávní kvalifikace protiprávního jednání v oblasti kyberprostoru jsou široké. A zároveň, že jsou samotným trestním zákoníkem omezené. Dle zásady "nullum crimen sine lege scripta" je to totiž jediný právní předpis, který označuje jednání, za něž je možné uložit trest.

---

[30] ŠÁMAL, P. *Trestní zákoník: komentář*. 2. vyd. Praha: C.H. Beck, 2012. s. 1300

[31] jímž se myslí *jakékoli zařízení nebo skupina vzájemně propojených nebo souvisejících zařízení, z nichž jedno nebo více provádí na základě programu automatické zpracování dat. Počítačovým systémem je tedy zařízení sestávající z technického (hardware) a programového (software) vybavení, které je určené k automatickému zpracování digitálních dat. Automatickým zpracováním se rozumí zpracování bez přímého lidského zásahu. Zpracování dat znamená, že na data se v počítačovém systému působí prováděním počítačového programu.* (ŠÁMAL, P.: op. cit., s. 2306)

[32] *se rozumí jakýkoli nosič dat v informační technice, tedy materiál, do kterého nebo na který lze zaznamenávat („zapsat“) data a z kterého lze data zpět získat („přečíst“).* (ŠÁMAL, P.: op. cit., s. 2308)

[33] Podvodná technika sloužící k získání citlivých údajů o uživatelích, zejména přístupových hesel a kódů.

5.1.2 Zákon o kybernetické bezpečnosti

Další zákon z ostatních právních předpisů (mimo trestní zákoník), který považuji za nutné zmínit, je zákon o kyb. bezpečnosti, který vstoupil v účinnost 1. ledna 2015. Problematika kybernetické bezpečnosti doposud nebyla českým právním řádem specificky řešena. Až na základě mezinárodních závazků ČR došlo k přijetí ZKB, jehož cílem je ochrana kyberprostoru, o němž tato práce v podstatě pojednává.

Zajištění kybernetické bezpečnosti státu je jednou z klíčových výzev současné doby.[34] Týká se to nejen České republiky, ale vzhledem ke globálnosti kyberprostoru, respektive kybernetické kriminality, i ostatních států světa. Otázka zabezpečení kyberprostoru se tak řeší i na mezinárodní úrovni, například v NATO nebo EU. Toto jen podporuje argument, že útoky v kyberprostoru jsou každodenní reálnou hrozbou a je nezbytné se jimi zabývat.

Kybernetickou bezpečností rozumíme souhrn prostředků směřujících k zajištění ochrany kybernetického prostoru. Tyto prostředky mohou být různého charakteru- právní, organizační, vzdělávací, technické apod. Pro účely zákona o kybernetické bezpečnosti je však nutno termín "kybernetická bezpečnost" chápat především ve smyslu právních prostředků zajišťujících ochranu kybernetického prostoru, které jsou obsaženy v ZKB. Jeho hlavním smyslem je ochrana funkčnosti kybernetického prostoru.[35]

V České republice je ochrana kybernetického prostoru prováděna především osobami soukromého práva a jejich činnost je nyní díky ZKB regulována státní mocí. ZKB vymezil role jednotlivých subjektů zainteresovaných v ochraně kybernetického prostoru, jejich povinnosti a také sjednotil pojmy užívané v oblasti kybernetické bezpečnosti.[36]

ZKB tak zlepšuje efektivitu řešení kybernetických bezpečnostních incidentů a zrychluje reakce na kybernetické hrozby.[37]

---

[34] Důvodová zpráva k zákonu č. 181/2014 Sb., o kybernetické bezpečnosti, sněmovní tisk č. 81/0 ze dne 10.1.2014. s. 18

[35] MAISNER, M., VLACHOVÁ B. *Zákon o kybernetické bezpečnosti: komentář*. Praha: Wolters Kluwer, 2015, s. 62

[36] Důvodová zpráva k zákonu č. 181/2014 Sb., o kybernetické bezpečnosti, sněmovní tisk č. 81/0 ze dne 10.1.2014. s. 19, 20

[37] Zpráva MV: op. cit., s. 63

5.2 Mezinárodní právo

Přeshraniční charakter kyberprostoru nutně vyžaduje, aby spolu jednotlivé státy světa v boji s kybernetickou kriminalitou spolupracovaly. To může být ale problematické zejména v okamžiku, kdy jsou právní úpravy jednotlivých států, ale i úroveň jejich vyspělosti, zcela rozdílné. Nicméně za účelem harmonizace jednotlivých úprav byla vytvořena řada mezinárodních dokumentů, z nichž nejvýznamnějším je Úmluva o kybernetické kriminalitě (dále v textu jen "Úmluva"), která vznikla na půdě Rady Evropy.

Kybernetickou kriminalitou se pak zabývají i jiné mezinárodní organizace a instituce, například NATO, Interpol, EU, OSN a další.

5.2.1 Úmluva Rady Evropy o kybernetické kriminalitě[38]

Úmluva sice vznikla už v listopadu roku 2001 v Budapešti, ale ratifikována prezidentem České republiky byla až v srpnu roku 2013, kdy se pro nás také stala závaznou.

Úmluvu doposud celosvětově ratifikovalo celkem 48 států světa.[39] Jejím cílem je sblížit právní úpravy jednotlivých států, zlepšit vyšetřovací techniky a také mezinárodní spolupráci v oblasti boje s kybernetickou kriminalitou.

Obsah Úmluvy tvoří 48 článků, které se vedle preambule člení do 4 kapitol. V první kapitole najdeme vymezení některých pojmů, které se v Úmluvě objevují. Druhá kapitola s názvem "opatření, která mají byt přijata na vnitrostátní úrovni" obsahuje hmotněprávní a procesně-právní závazky, které státy musí implementovat do svých úprav. Především zde nalezneme výčet jednání, které mají státy trestněprávně stíhat. Dále ustanovení týkající se procesního práva, jako jsou povinnosti v oblasti vyšetřovacích postupů a pravomocí a pak také ustanovení o působnosti vnitrostátních norem. Třetí kapitola se týká mezinárodní spolupráce států a obsahuje její zásady a také postupy. Čtvrtá kapitola je věnována závěrečným ustanovením.

[38] Jindy také v českém překladu jako "Úmluva o počítačové kriminalitě".

[39] http://www.coe.int/cs/web/conventions/full-list/-/conventions/treaty/185/signatures (zobrazeno 13.3.2016)

K Úmluvě byl také později vydán tzv. "Dodatkový protokol k Úmluvě" (dále jen Dodatek), který zařazuje mezi trestněprávní jednání další skutky a to rasistické a xenofobní povahy.

6. KRIMINALITA V KYBERPROSTORU

V následující kapitole se budu věnovat tomu, jakým způsobem je kybernetická kriminalita páchána, respektive k jakým útokům v kyberprostoru dochází. Pro jejich rozlišení jsem se rozhodla užít dělení podle Úmluvy a to na:

a) Útoky proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů
b) Útoky spočívající ve vytváření a šíření škodlivého obsahu
c) Útoky spočívající v porušování práv duševního vlastnictví
d) Tradiční kriminalita v novém kabátě.[40]

Nejde však o popis a vysvětlení jednotlivých škodlivých jednání uvedených v Úmluvě, ani o jejich trestněprávní kvalifikaci, ale o výčet kriminálních aktivit, které se v kyberprostoru objevují.

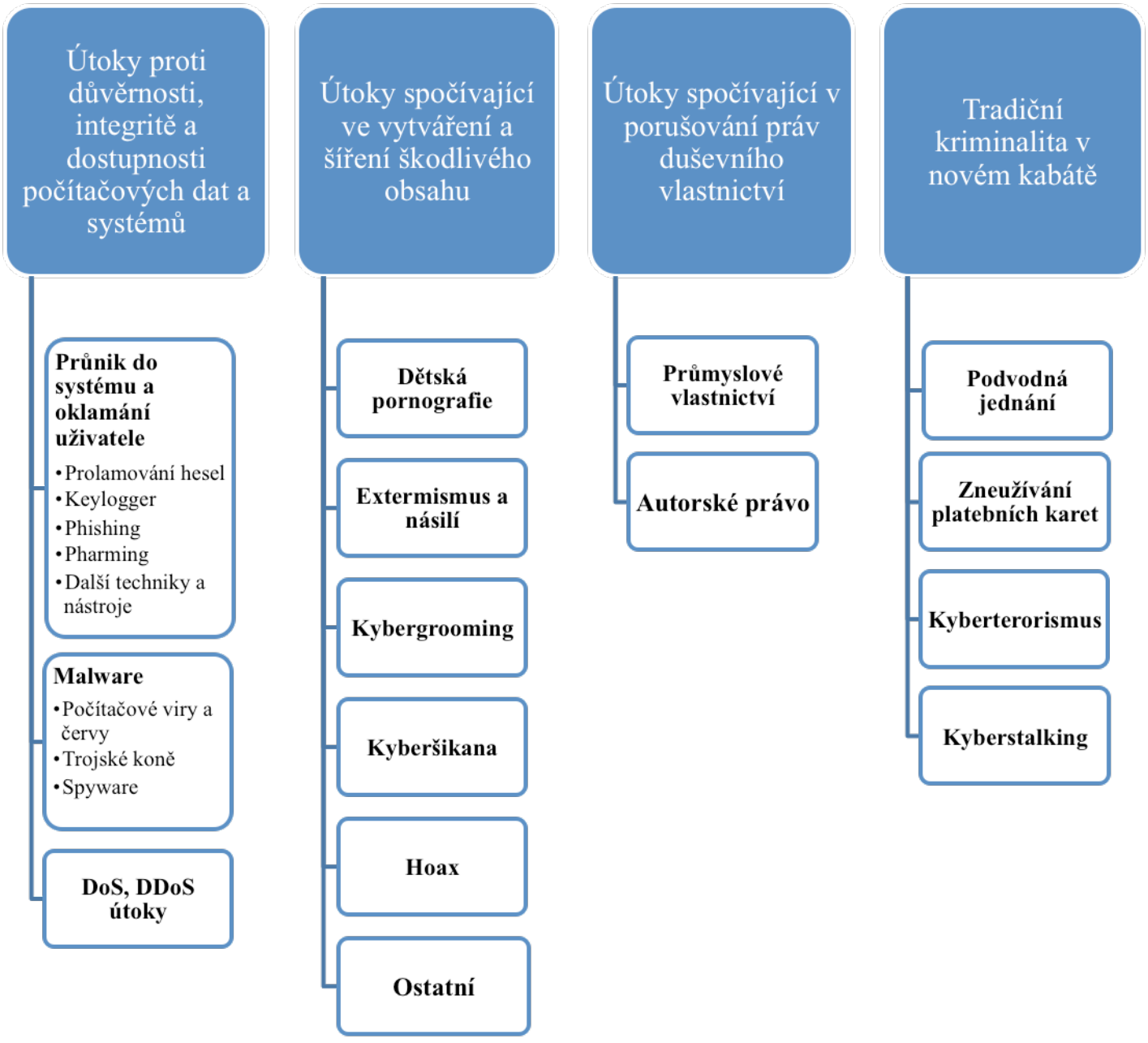
Dělení lze samozřejmě zvolit jiné, nebo žádné a dané činnosti pouze vyjmenovat a popsat. Vzhledem k aktuálnosti kyberkriminality a existencí Úmluvy, která se jí zabývá myslím, že má smysl s touto pracovat a porovnávat její osnovu a samotný obsah s reálným stavem.

Mým cílem je zařadit pod zvolené členění co nejvíce pojmů, jednání. A protože jich není málo a většina z názvů má anglický původ, tak se chci také maximálně věnovat popisu a vysvětlení jejich podstaty.

Zvláštní pozornost pak budu věnovat právům duševního vlastnictví, jejichž ochranu považuji za nezbytnou, a zejména pak autorskému právu, neboť jeho porušování patří mezi nejčastější projevy kyberkriminality[41] vůbec.

Pro přehlednost celé kapitoly jsem na úvod vytvořila tabulku, která by měla usnadnit porozumění a orientaci v dané problematice.

[40] GŘIVNA, T., SCHEINOST M., ZOUBKOVÁ I.: op. cit., s. 339
[41] Zpráva MV: op. cit., s. 61


Útoky proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů
Průnik do systému a oklamání uživatele
• Prolamování hesel
• Keylogger
• Phishing
• Pharming
• Další techniky a nástroje
Malware
• Počítačové viry a červy
• Trojské koně
• Spyware
DoS, DDoS útoky
Útoky spočívající ve vytváření a šíření škodlivého obsahu
Dětská pornografie
Extermismus a násilí
Kybergrooming
Kyberšikana
Hoax
Ostatní
Útoky spočívající v porušování práv duševního vlastnictví
Průmyslové vlastnictví
Autorské právo
Tradiční kriminalita v novém kabátě
Podvodná jednání
Zneužívání platebních karet
Kyberterorismus
Kyberstalking

6.1 Útoky proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů

Počítače a vůbec veškeré informační technologie, včetně svého obsahu, by měly být nedotknutelné. Přesto velká část kybernetické kriminality spočívá právě v jejich poškozování (prostřednictvím malwaru) anebo v tzv. sociálním inženýrství[42], tedy *manipulaci lidí za účelem provedení určité akce nebo získání určité informace.*[43]

Jinými slovy, v první kategorii útoků je cílem cizí ICT poškodit, narušit, nebo do nich proniknout a potažmo to zužitkovat ve vlastní prospěch.

6.1.1 Průnik do systému a oklamání uživatele

Obvyklým způsobem jak zasáhnout do integrity ICT je tzv. "průnikaření", což je český výraz pro "hacking". V této souvislosti se zde proto pro pachatele užívá označení "hacker" či "cracker". Oběma těmto výrazům se ve své práci budu věnovat později a vysvětlím jaký je skutečně jejich význam. A i když některé mnou užité zdroje hovoří o "hackerech", já budu pro útočníka souhrnně užívat pojem pachatel.

Průnik do systému může být cílem nebo prostředkem ke spáchání TČ.[44] Jeho smysl tkví v tom, že pachatel se snaží překonat ochranu počítačového systému. Ať už jde o získání hesla, prolomení softwarové ochrany anebo jiné oklamání uživatele. K tomu může pachatel využít různé techniky, jejichž výčet a popis bude následovat. Pokud do systému pronikne, může pokračovat v další trestné činnosti (např. použít informace o uživateli k získání online půjčky).

6.1.1.1 Prolamování hesel

Tato technika je zřejmě tím nejběžnějším způsobem, jak získat cizí uživatelské heslo a případně i celý přístup do systému, nebo ke konkrétnímu uživatelskému účtu. Jedná se o jednoduché zadávání a zkoušení hesla, které si uživatel při zakládání účtu zvolil, anebo o prolomení hesla pomocí tzv. prolamovače hesel.

---

[42] Nebo také "sociotechnika" má stejně jako mnoho jiných aktivit původ v reálném světě a nyní se v závislosti na rozvoji ICT objevuje i v kyberprostoru

[43] JIRÁSEK P., NOVÁK L., POŽÁR J. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze, 2013, s. 93

[44] GŘIVNA, T., SCHEINOST M., ZOUBKOVÁ I.: op. cit., s. 340

Zatímco technika prostého "zkoušení hesla" bude doménou pachatelů - laiků, kteří mají různou motivaci k tomu, aby se k uživatelskému účtu oběti dostali. Druhá technika, která pomocí speciálního softwaru, tzv. prolamovače hesel heslo zjistí tzv. hrubou silou[45], bude užívána zkušeným pachatelem, který má jasný cíl heslo získat.

Často se upozorňuje, aby uživatelé neměli jedno heslo pro více svých uživatelských účtů a také aby při jejich volbě využívali co nejvíce možných druhů znaků, od číslic po velká písmena. Pro tento účel existují i tzv. "generátory hesel", které uživateli vygenerují "bezpečné" heslo.

Lidé tzv. "sílu hesla" často podceňují a zadávají např. svá čísla narození, nebo pouze za sebou jdoucí číslice, kombinace jména a roku narození apod. Pak stačí skutečně jen málo informací o dané osobě, chvíle času a trpělivosti a pachatel má vyhráno.

Samotný prolamovač hesel je ovšem legální program, který může použít každý z nás, pokud zapomněl své přístupové heslo k vlastnímu účtu. Prolamovač zná tolik slov, čísel a jejich kombinací a generuje jich tisíce za sekundu, až se jednoduše "trefí" a uživatelské heslo tak vyluští. Ovšem v okamžiku, kdy někdo program zneužije k získání cizího hesla, vzniká problém.

Některé webové stránky však už fungují tak, že pokud je heslo zadáno několikrát za sebou špatně, dojde k zablokování účtu. Standard to ale není.

6.1.1.2 Keylogger

Další způsob jak zjistit uživatelovo heslo je použití tzv. keyloggeru. Jedná se o zařízení, které je nainstalované nebo připojené k PC a které zaznamenává všechny úhozy do klávesnice, které uživatel udělá, a snímá tak veškerý psaný text.[46] Zejména se ale používá k zjišťování hesel a dalších citlivých údajů.

Může mít formu softwarovou a tak se někdy řadí mezi tzv. malware (tzv. škodlivý software, jemuž bude prostor věnován později), kdy jde tedy o program nainstalovaný v PC. Nebo může mít formu hardwarovou, kdy se jedná o součástku nacházející se mezi klávesnicí a skříní PC, což v praxi vypadá tak, že USB kabel od klávesnice není

[45] tzv. Brute force attack
[46] JIRÁSEK P., NOVÁK L., POŽÁR J.: op. cit., s. 52

zapojený přímo do PC skříně, ale právě do této "mezisoučástky" vypadající jako USB paměť.

Každá z forem keyloggeru má své výhody a nevýhody. Zatímco softwarový může být jako malware snadno zjistitelný, tak hardwarové součástky si nemusíme vůbec všimnout. Nainstalovat softwarový keylogger může být ovšem mnohem snadnější, než se fyzicky dostat k počítači oběti a "namontovat" keylogger hardwarový.

Zajímavé je, že většina moderních keyloggerů je považována za legitimní software nebo hardware a jsou volně prodejné. Mohou být totiž dost dobře užitečné v běžném životě. Například pro rodiče, kteří chtějí mít větší kontrolu nad svými dětmi, nebo pro společnosti, které si hlídají, aby jejich zaměstnanci nevyzradili obchodní tajemství, které by mohlo společnost poškodit.[47] Ovšem ve chvíli, kdy někdo pomocí keyloggeru zjistí vaše přihlašovací údaje k bankovnímu účtu a díky tomu z něj potom "vybere" peníze, to už rozhodně legální činnost není.

6.1.1.3 Phishing

Homofon anglického slova "fishing" česky proto překládaného jako "rybaření", nebo "rhybaření", je podvodná metoda, která usiluje o získání osobních aj. citlivých údajů za účelem jejich dalšího zneužití.[48]

Účelem phishingu je nalákat uživatele do pasti, která je tvořená zejména podvodným emailem a podvodnou webovou stránkou. Celý systém funguje tak, že uživateli přijde email, který se na první pohled tváří, že je od instituce, jež například poskytuje veřejnosti běžné služby (typicky banka). Obsahem emailu je pak žádost o zadání přihlašovacích údajů adresáta a to na níže uvedené webové adrese. Email včetně webové stránky jsou ale uměle vytvořené s cílem zmást uživatele a získat jeho přihlašovací údaje, pro vlastní potřeby.

Pachatelé takto rozešlou tisíce emailů a záleží pak jen na adresátech, zda jsou při čtení emailu pozorní. Byť email obsahuje řadu rádoby důvěryhodných údajů, ať už jde o jméno společnosti, která je skutečně všeobecně známá, její logo a strukturu emailu samotného, lze při podrobnějším zkoumání odhalit, že jde o podvod. Zejména proto, že

[47] https://securelist.com/analysis/publications/36138/keyloggers-how-they-work-and-how-to-detect-them-part-1/ (zobrazeno 18.3.2016)
[48] JIRÁSEK P., NOVÁK L., POŽÁR J.: op. cit., s. 70

společnosti nikdy o kompletní přihlašovací údaje nežádají. Dále jde o gramatické chyby, anebo emailovou adresu odesílatele, která není ze skutečné domény společnosti, či výhružky týkající se následků, pokud adresát nevyhoví.

Phishing je problémem nejen běžných uživatelů, ale i velkých společností, na jejichž zaměstnance pachatelé útočí. V takovém případě bývá útok sofistikovaný, zaměřený pouze na jednu konkrétní osobu, o níž si útočník nastřádá co nejvíce údajů, tak aby jeho email a žádost v něm byly co nejvíce důvěryhodné.[49] Jedná se o formu tzv. "spear phishingu" (z anglického oštěp). Pokud pak míří útok na nejvyšší management společnosti, je lidově nazýván jako "whaling" (z anglického velryba).[50]

Podvodné žádosti o sdělení osobních a jiných údajů mohou být vynucovány také na náhodně navštívené webové stránce, nebo prostřednictvím telefonního hovoru. V takovém případě se hovořící osoba představí např. jako pracovník softwarové společnosti, s nabídkou řešení problému, anebo nabízí produkt společnosti. Pod touto záminkou pak vyžadují přihlašovací údaje volaných.[51] Opět však platí, že softwarové společnosti takto při své práci nepostupují.

6.1.1.4 Pharming

Technika pharmingu je svou podstatou podobná předešlému Phishingu. Opět je zde cílem získat důvěrné údaje o oběti a to jejich zadáním na podvodné webové stránce. Na tu se ale oběť dostane přesměrováním z webové adresy, byť byla zadána správně a je důvěryhodná. V tomto případě se nevyužívá návnada v podobě emailu, či telefonátu.[52]

V případě pharmingu pachatel napadne DNS[53] a přepíše IP adresu čím je uživatel přesměrován na falešnou stránku např. internetbankingu, e-mailu, či sociální sítě, potom, co zadá do vyhledávače webovou adresu. Stránka na kterou je přesměrován je obvykle k nerozeznání od těch pravých a záměnu je těžké zpozorovat.[54]

Pachatel tímto mění provoz v určité oblasti Internetu a žene jeho uživatele na

[49] http://www.webopedia.com/TERM/S/spear_phishing.html (zobrazeno 23.3.2016)
[50] https://en.wikipedia.org/wiki/Phishing (zobrazeno 23.3.2016)
[51] https://www.microsoft.com/en-us/security/online-privacy/phishing-symptoms.aspx (zobrazeno 23.3.2016)
[52] http://us.norton.com/cybercrime-pharming (zobrazeno 23.3.2016)
[53] tzv. "domain name server" což je překladová služba, která zprostředkovává náš požadavek na otevření webové stránky. Zdroj: https://napoveda.active24.cz/idx.php/0/308/article/ (zobrazeno 23.3.2016)
[54] JIRÁSEK P., NOVÁK L., POŽÁR J.: op. cit., s. 69

falešné stránky. Tím toto jednání získalo svůj název, který můžeme přeložit jako "farmaření".

Přestože se jedná o hůř rozpoznatelný podvod, lze se proti němu bránit. Především je třeba mít důvěryhodného poskytovatele Internetu (kterých je většina) a který na prvním místě detekuje takové falešné stránky. Dále je třeba dávat si pozor na to, zda stránka po načtení nezměnila svůj název (například o jedno písmenko). A dále, aby se v případě přesměrování na platební bránu "http" změnilo na "https" kdy "s" indikuje "secure", tedy zabezpečený.[55]

6.1.1.5 Další techniky a nástroje

Vedle uvedených metod jak proniknout do systému uživatele existují i další techniky a způsoby, jak tak učinit. Zvláště pro ně je typické, že jsou s ostatními kombinovány. Teprve při jejich spojení je "útok" úspěšný. Dále pro ně platí, že jejich užití vyžaduje už poměrně pokročilé zkušenosti s ICT.

Patří sem například *skenování portů, SQL injection, Buffer overflow, Cross site scripting, sniffing,* nebo *IP spoofing.* Podrobněji se těmto metodám věnují ve své práci například Krupička nebo Čikovský.

6.1.2 Malware

Další způsob, kterým dochází k narušení ICT je malware, neboli škodlivý software. *Výraz "malware" vznikl složením anglických slov "malicious" (zákeřný) a "software" a používá se pro programy, jejichž cílem je někomu nějak uškodit. Pod označení malware zahrnujeme v prvé řadě počítačové viry, trojské koně, spyware a adware, ale jde pouze o příklady a prakticky tak lze označit každý program, který někomu způsobí škodu či jinému získá neoprávněný prospěch. Naopak malwarem nejsou programy, které mají legální a legitimní cíle a jen vykazují chyby.*[56]

Malware se do zařízení dostane instalací, kterou nejčastěji provede sám uživatel a to tak, že klikne například na odkaz na internetu, nebo otevře přiložený soubor v e-mailu. Součástí takových odkazů, souborů, nebo programů je pak i malware, který je otevřením nainstalován a to bez vědomí uživatele.

[55] http://us.norton.com/cybercrime-pharming (zobrazeno 25.3.2016)
[56] SMEJKAL, V. (2015).: op. cit., s. 138

Pro účely své práce jsem se rozhodla uvést ty nejznámější a nejčastější druhy malwaru, jejichž charakteristiku uvádím níže.

6.1.2.1 Počítačové viry a červy

Hlavní rozdíl mezi počítačovými viry a červy je ten, že viry vyžadují aktivní hostitelský program nebo již infikovaný program a k tomu aktivně fungující systém. Toto spojení umožní viru fungování, může tak působit škodu a infikuje další soubory nebo dokumenty. Zatímco červy jsou samostatně stojící škodlivé programy, které se mohou samy duplikovat a šířit se počítačovou sítí bez pomoci člověka.[57]

Viry se tedy chovají jako viry biologické, šíří se v napadeném zařízení samy.[58] *A to prostřednictvím Internetu (elektronickou poštou, stahováním programů, nespolehlivými zdroji,) nebo pomocí přenosných paměťových médií apod.*[59]

Červi pak rozesílají kopie sebe samých na další zařízení, např. v podobě e-mailu zaslaného všem kontaktům zjištěným v e-mailové schránce dostupné v napadeném zařízení.[60]

Cílem virů i červů je narušení či poškození ICT. To může spočívat ve zcizení dat, poškození hardwaru či softwaru počítače, znepřístupněním dat atp.[61] Lze se proti nim však účinně bránit. Především tím, že uživatelé pravidelně aktualizují svůj operační systém a mají nainstalovaný anti-virový software, který viry, červy aj. detekuje.

6.1.2.2 Trojské koně

Trojský kůň je takovým druhem programu, který je často maskovaný jako legitimní a neškodný software, opak je však pravdou. Princip jeho fungování je stejný, jak u trojského koně, známého z řecké mytologie, po němž se také shodně nazývá. Uživatel je v tomto případě obelstěn, s tím, že poté, co si stáhne a nainstaluje na první pohled bezproblémový program, přijdou více či méně viditelné nepříjemnosti. Program začne působit ke svému skrytému škodlivému účelu, který může spočívat ve špehování,

[57] https://usa.kaspersky.com/internet-security-center/threats/computer-viruses-vs-worms#.VwZ18MffRbU (zobrazeno 7.4.2016)
[58] GŘIVNA, T., SCHEINOST M., ZOUBKOVÁ I.: op. cit., s. 341
[59] JIRÁSEK P., NOVÁK L., POŽÁR J.: op. cit., s. 73
[60] GŘIVNA, T., SCHEINOST M., ZOUBKOVÁ I.: op. cit., s. 342
[61] Idem

přisvojení si citlivých dat uživatele, anebo umožní jeho autorovi, pachateli přístup do napadeného systému. Toto všechno může také obnášet ničení, blokování, změnu i kopírování dat a narušení výkonu počítače nebo počítačové sítě.[62]

Na rozdíl od počítačových virů a červů se trojský kůň nemnoží infikováním ostatních souborů ani se dál sám nereprodukuje.[63] Stejně jako u virů a červů platí, že se proti nim lze bránit používáním antivirového programu.

6.1.2.3 Spyware

Spyware je program, který skrytě sleduje činnost uživatele a mapuje obsah jeho uložených souborů, aby pak mohl nastřádaná data odeslat pachateli, který je dále podle svého využije. Jedná se například o informace týkající se toho, jaké internetové stránky uživatel navštívil, ale také o citlivé údaje jako jsou hesla, přihlašovací údaje, čísla platebních karet a další jiné soubory.[64]

Je to takový program, který je často na cílový počítač nainstalován spolu s jiným programem (utilitou, nebo počítačovou hrou), s jehož funkcí však nesouvisí.[65] Opět tedy platí, že jde o škodlivý software, který *na počítači běží bez vědomí uživatele a nějakým způsobem poškozuje nebo zhoršuje jeho funkci.*[66]

Spyware se projevuje především tak, že při zadání domovské stránky přesměrovává uživatele na jinou webovou stránku, zpomaluje počítač i internet a také zvyšuje výskyt reklam (tzv. pop-up okna, která sama od sebe vyskakují při prohlížení webu).[67] Jeho účelem je především zisk citlivých údajů, nebo poškození PC.

---

[62] https://usa.kaspersky.com/internet-security-center/threats/trojans#.VwbamMffRbU (zobrazeno 7.4.2016)
[63] http://www.webopedia.com/DidYouKnow/Internet/virus.asp (zobrazeno 7.4.2016)
[64] GŘIVNA, T., SCHEINOST M., ZOUBKOVÁ I.: op. cit., s. 342
[65] JIRÁSEK P., NOVÁK L., POŽÁR J.: op. cit., s. 96
[66] https://cs.wikipedia.org/wiki/Spyware (zobrazeno 7.4.2016)
[67] Idem

6.1.3 DoS, DDoS útoky

Denial of service a distributed denial of service (česky odepření služby) jsou dvě techniky útoku, které míří na omezení funkčnosti konkrétního serveru.[68] Útok probíhá tak, že na jeden konkrétní systém (cíl útoku) je kladeno mnoho požadavků, čímž dojde k jeho zahlcení a následnému zhroucení.[69]

Rozdíl mezi DoS a DDoS spočívá pouze v počtu útočníků. V prvním případě útočí na systém pouze jeden počítač, ve druhém pak několik počítačů, které jsou navíc ve své činnosti koordinované. Výsledkem útoků (zahlcení) je pak nefunkčnost a nedostupnost systému.[70]

Takovým způsobem byly například v roce 2013 napadeny webové stránky několika českých bankovních institucí. Útoky pocházející ze zahraničí tehdy způsobily, že internetové bankovnictví, internetové stránky a mobilní aplikace byly několik hodin nefunkční.[71]

6.2 Útoky spočívající ve vytváření a šíření škodlivého obsahu

Na rozdíl od předešlé kategorie útoků, jsou v tomto případě ICT spíše prostředkem, nežli cílem.

Úmluva se z hlediska šíření škodlivého obsahu zabývá především dětskou pornografií. Dodatek k Úmluvě pak mezi škodlivé jednání, které je třeba stíhat, přidává i šíření obsahu, který má rasistickou a xenofobní povahu. To ale nejsou jediná nežádoucí jednání, ke kterým v souvislosti s šířením závadného obsahu v kyberprostoru dochází.

[68] GŘIVNA, T., SCHEINOST M., ZOUBKOVÁ I.: op. cit., s. 342
[69] http://www.webopedia.com/TERM/D/DoS_attack.html (zobrazeno 8.4.2016)
[70] JIRÁSEK P., NOVÁK L., POŽÁR J.: op. cit., s. 33
[71] http://www.patria.cz/zpravodajstvi/2282801/dalsi-utok-hackeru-v-cr-tercem-internetove-bankovnictvi-velkych-bank-cnb-i-web-burzy.html (zobrazeno 8.4.2016)

6.2.1 Dětská pornografie

I když podle českého trestního zákoníku lze trestně stíhat šíření pornografického díla projevující násilí či neúctu k člověku, nebo které popisuje, zobrazuje nebo jinak znázorňuje pohlavní styk se zvířetem (tzv. tvrdá pornografie), Úmluva se zabývá pouze pornografií dětskou.

To že Úmluva klade důraz na dětskou pornografii je pochopitelné, neboť ta má oproti ostatním druhům pornografie vyšší společenskou závažnost.[72] To lze dovodit například z toho, že šíření dětské pornografie je v ČR trestáno vyšší trestní sazbou[73] a z toho, že trestní zákoník dokonce stíhá její pouhé přechovávání.[74] Obecně také společnost vnímá dítě jako něco křehkého a nevinného a tudíž jakékoliv zacházení s ním s postranními úmysly, natož zacházení necitlivé, násilné, či ponižující, snáší velice špatně.

Okolnosti, za kterých dětská pornografie vzniká a její specifika nejsou předmětem této práce. Je ale třeba uvést, že informační a komunikační technologie zjednodušují její výrobu a distribuci. Přičemž jedním z problémů je vůbec všeobecná dostupnost fotografií obnažených dětí, které jejich matky hojně sdílejí na sociálních sítích ale i na diskuzních fórech a které si lze snadno stáhnout.

Za pozornost stojí také další aspekt, který nové technologie přináší, a tím je tvorba dětské pornografie. Úmluva řadí mezi pornografický materiál znázorňující dítě i "realistické zobrazení dítěte"[75] a trestní zákoník zase "osobu, jež se jeví být dítětem"[76]. Tím můžeme rozumět i *vyobrazení dítěte, které vzniklo zcela za pomoci počítače*.[77] A tak je možné díky vyspělosti ICT vytvářet i pouhé animace, které budou vyobrazovat dítě v erotických pozicích.

---

[72] ŠÁMAL, P.: op. cit., s. 1892

[73] Srovnej §191 odst. 1 TZ: *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 člověku, nebo které popisuje, zobrazuje nebo jinak znázorňuje pohlavní styk se zvířetem, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty* a § 192 odst. 1 TZ: *Kdo přechovává fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě nebo osobu, jež se jeví být dítětem, bude potrestán odnětím svobody až na dva roky*.

[74] §192 odst. 1 trestního zákoníku

[75] Kapitola II, část 1, článek 9, odst. 2, písm. c) Úmluvy

[76] §192 trestního zákoníku, odst. 1, 2

[77] ŠÁMAL, P.: op. cit., s. 1892

Kyberprostor poskytl zakázaným formám pornografie obecně nový rozměr a usnadnil jejich šíření. To si ale pachatelé, uvědomují a soustřeďují se proto v uzavřených komunitách, kde zdokonalují své techniky, jejichž součástí je i prověřování svých členů.[78]

Nesmíme také zapomenout na naivitu dětí samotných, které mohou být samy původci potenciálně erotického materiálu. Jsou známé případy, kdy na různých chatovacích platformách děti sdílely fotografie či videa sebe samých, kde byly obnažené. V tomto případě platí, že nelze pomíjet charakter kyberprostoru a dostupnost ICT a věnovat dostatečný prostor osvětě dětí ohledně nástrah internetové komunikace.

6.2.2 Extremismus a násilí

Další nevhodný obsah, který se v kyberprostoru šíří se týká násilí a extremismu. *Pojmem extremismus jsou označovány vyhraněné ideologické postoje, které vybočují z ústavních, zákonných norem, vyznačují se prvky netolerance, a útočí proti základním demokratickým ústavním principům, jak jsou definovány v českém ústavním pořádku.*[79] Násilný obsah se může týkat osob, zvířat, ale i majetku. Často bývá ale spojován právě s extremistickými myšlenkami. Úmluva se vymezuje proti šíření *"rasistického a xenofobního" materiálu, který obhajuje, podporuje nebo podněcuje nenávist, diskriminaci nebo násilí proti jednotlivci nebo skupině jednotlivců, na základě rasy, barvy pleti, rodového nebo národního nebo etnického původu, jakož i náboženství.*[80]

Opět není mým cílem zde oba dva kriminologické jevy popisovat. Nýbrž vysvětlit jejich spojitost s kyberprostorem. Stejně jako tomu bylo u dětské pornografie, i zde platí, že ten značně usnadňuje šíření tohoto nevhodného obsahu. To je nežádoucí nejen proto, že k němu získávají přístup děti, které takový obsah může ovlivnit v jejich vývoji, ale i osoby, které se dál na praktickém šíření extremistických myšlenek a samotného násilného jednání mohou podílet.

Zvlášť v současném období tzv. uprchlické krize a ve stínu teroristických útoků (Paříž leden a listopad 2015, Brusel březen 2016) se jedná o velmi aktuální otázku. Společnost je rozpolcená a především na Internetu, prostřednictvím sociálních sítí jejich

[78] Zpráva MV: op. cit., s. 61
[79] http://www.policie.cz/clanek/prevence-informace-o-extremismu-co-je-extremismus.aspx (zobrazeno 10.4.2016)
[80] Dodatek, Kapitola I, čl. 2, odst. 1

uživatelé vyjadřují své názory na současnou situaci. V dubnu 2016 byl například, za své výroky uveřejněné na sociální síti, namířené proti muslimům[81] obžalován[82] Martin Konvička, předseda hnutí Blok proti Islámu.

6.2.3 Kybergrooming

Kybergrooming je psychická manipulace oběti prostřednictvím informačních a komunikačních technologií s cílem jejího sexuálního využití[83] a týká se zejména nezletilých.

Pachatel v tomto případě využívá anonymity kyberprostoru a vydává se za jinou osobu, než kterou skutečně je. Za tímto účelem má například zřízený falešný profil na sociální síti, jejímž prostřednictvím oběť náhodně kontaktuje. Snaží se s ní navázat důvěrný vztah, tak aby od ní později získal pornografický materiál.

V případě dětí, které často nedokážou situaci vyhodnotit, anebo podezřelou osobu odhalit je situace o to závažnější. *Pachatel totiž zpravidla později změní rétoriku a tvrdě vyžaduje další fotografie, svlékání před webkamerou, anebo dokonce osobní setkání, kde dochází ke zneužití a násilnostem.*[84]

Může následovat také vydírání dítěte, kdy mu pachatel vyhrožuje zveřejněním doposud zaslaných fotografií, pokud mu oběť nepošle další, nebo neudělá, oč jej žádá. Tak tomu bylo i v nejznámějším případě kybergroomingu v ČR, v kauze Pavla Hovorky, který byl v roce 2008 odsouzen za 7x za pohlavní zneužití dítěte a 13x vydírání dítěte.[85]

6.2.4 Kyberšikana

Jedná se o šikanu, která probíhá ve virtuálním prostředí, prostřednictvím moderních komunikačních technologií a která se může prolínat s tradiční šikanou v reálném světě.[86]

---

[81] Jeden z jeho výroků zněl: „Pokud vstoupíme do politiky, vyhrajeme volby, vás muslimové nameleme do masokostní moučky.“ Zdroj: http://www.lidovky.cz/konvicka-je-obzalovan-kvuli-podnecovani-k-nenavisti-a-hrozi-mu-vezeni-1e0-/zpravy-domov.aspx?c=A160408_105356_ln_domov_ele (zobrazeno 10.4.2016)
[82] Z trestného činu podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod
[83] GŘIVNA, T., SCHEINOST M., ZOUBKOVÁ I.: op. cit., s. 344
[84] ECKERTOVÁ, L., DOČEKAL D. *Bezpečnost dětí na internetu: rádce zodpovědného rodiče*. Brno: Computer Press, 2013, s. 40
[85] http://www.ceskaskola.cz/2009/05/kamil-kopecky-kybergrooming-aneb-kdo.html (zobrazeno 9.4.2016)
[86] ECKERTOVÁ, L., DOČEKAL D.: op. cit., s. 64

Kyberprostor poskytuje pachateli anonymitu a díky své "velikosti" navíc znásobuje účinek šikany. Oběť může být vystavena permanentnímu útoku, o kterém její okolí navíc nemusí vůbec vědět, především proto, že nenese fyzické známky útoku.[87]

Pachatel zde *využívá elektronické prostředky, jako jsou mobilní telefony, e-maily, Internet, blogy aj. k zasílání obtěžujících, urážejících či útočných e-mailů a SMS, vytváření stránek a blogů, které dehonestují vybrané jedince nebo skupiny lidí*.[88]

Opět zde mezi nejnáchylnější oběti patří právě děti, pro něž je obecně problém šikanu řešit. V minulosti ve světě dokonce několikrát došlo k tomu, že děti reagovaly na kyberšikanu sebevraždou.[89]

6.2.5 Hoax

Anglické slovo hoax v překladu do češtiny znamená falešnou zprávu, mystifikaci, novinářskou kachnu atd. Jedná se zpravidla o e-mailovou zprávu, která se snaží tvářit důvěryhodně, ačkoliv je nepravdivá.

V počítačovém světě tak nejčastěji označujeme poplašnou zprávu, která varuje před neexistujícím nebezpečným virem. Jako hoax můžeme také označit šířenou zprávu, která obsahuje nepřesné, zkreslující informace, účelově upravené polopravdy nebo směsku polopravd a lží.[90]

Hoax se snaží adresáty svým obsahem přimět k dalšímu šíření zprávy. Byť se tak často děje pro pobavení, může být hoax i nebezpečný. Například v poslední době se v ČR opět v souvislosti s migrační vlnou objevilo několik lživých zpráv, týkajících se chování uprchlíků, za něž dokonce hrozilo obvinění z přečinu šíření poplašné zprávy[91]. Takové smyšlené zprávy pak mohou hýbat celým míněním společnosti a negativně se tak podepsat na stavu morálky a přístupu k řešení aktuálních problémů.

---

[87] GŘIVNA, T., SCHEINOST M., ZOUBKOVÁ I.: op. cit., s. 345
[88] JIRÁSEK P., NOVÁK L., POŽÁR J.: op. cit., s. 72
[89] *Například čtrnáctiletá polka Anna Halman, která spáchala sebevraždu poté, co se za přihlížení celé své třídy stala terčem sexuální šikany a kyberšikany ze strany pěti spolužáků.* Zdroj: https://cs.wikipedia.org/wiki/Anna_Halman (zobrazeno 10.4.2016)
[90] http://www.hoax.cz/hoax/co-je-to-hoax (zobrazeno 12.4.2016)
[91] Což je asi nejznámější případ, kdy žena z jižních čech prostřednictvím sociální sítě Facebook zveřejnila zprávu o tom, že v jedné vesnici v pohraničí skupina arabských "uprchlíků" bezdůvodně podřezala veškerá hospodářská zvířata. Zdroj: http://www.lupa.cz/clanky/policie-resi-hoax-o-imigrantech-na-facebooku-jako-sireni-poplasne-zpravy/ (zobrazeno 12.4.2016)

6.2.6 Ostatní

Na internetu lze nalézt z hlediska škodlivého obsahu také návody nejrůznějšího druhu. Například jak spáchat určitý útok, vyrobit zločinný nástroj apod.[92] Může jít o návody na výrobu výbušnin, nebo návody na to jak si co nejlépe ublížit (tzv. sebepoškozování). Tento obsah může být profesionální, či amatérský, nebo dokonce úmyslně špatně popsaný. Pak záleží na koncovém uživateli, jak jej vyhodnotí. V každém případě platí, že Internet je místem neomezeného poznání a jeho vliv na společnost je enormní.

Dalším škodlivým obsahem na Internetu může být obchod s nežádoucími artikly, jako jsou zbraně, drogy informace, zejména vytěžené citlivé údaje, nebo také nájemnými zabijáky. Takový obchod může probíhat například prostřednictvím tzv. "dark webu" (jedním z nejznámějších obchodů na dark webu je Silk Road). Jedná se o zvláštní síť přístupnou pouze skrze tzv. systém "tor" ("the onion router").[93] Tento systém umožňuje uživateli skrýt svou IP adresu a to díky víceúrovňovému zabezpečení[94], čímž se pak obchodování zde stává anonymním.

6.3 Útoky spočívající v porušování práv duševního vlastnictví

Internet jako médium umožňující sdílení obsahu mezi širokým spektrem uživatelů skýtá velký prostor pro porušování práv duševního vlastnictví.[95] Zejména autorské právo, jak už jsem zmínila, patří mezi ta vůbec nejvíce ohrožená práva v kyberprostoru.

Informační a komunikační technologie a zejména Internet se od svého vzniku neustále vyvíjí a zdokonalují. Internetové pokrytí je širší, jeho rychlost je vyšší. Zařízení mají větší kapacitu a jsou více mobilní. Služby, které jsou s nimi spojeny, jsou stále propracovanější a uživatelsky příjemnější. To vše je ku prospěchu jejich uživatelům, včetně těch, kteří vytvářejí obsah, jež se dá prostřednictvím moderních technologií konzumovat.

Bohužel existuje i stinná stránka celého rozvoje a tou je mnohem jednodušší možnost, jak z vytvořeného obsahu nelegálně profitovat. Zejména pokud jde o hudbu,

[92] GŘIVNA, T., SCHEINOST M., ZOUBKOVÁ I.: op. cit., s. 345
[93] http://www.forbes.com/sites/realspin/2014/03/25/insider-trading-on-the-dark-web/#308876893d3b (zobrazeno 12.4.2016)
[94] Anglické slovo onion v překladu do češtiny znamená cibule. Stejně jako má cibule více vrstev, tak zde má zabezpečení více úrovní. Víceúrovňové zabezpečení probíhá opakovaným přesměrováváním.
[95] GŘIVNA, T., SCHEINOST M., ZOUBKOVÁ I.: op. cit., s. 346

filmy a software. Považuji za nezbytné se touto problematikou zabývat, a to především kvůli morálce, která v naší společnosti panuje a pocitu, že lidé často berou obsah dostupný na Internetu, ať už je jakéhokoliv původu, za samozřejmost.

Neustále totiž pokračuje trend uploadu nelegálních souborů na datová úložiště, čímž se umožňuje volné šíření a sdílení nahraných souborů. Pokračuje fenomén přesunu kriminality v oblasti duševního vlastnictví do kyberprostoru.[96]

Byť se chci věnovat především problematice porušování autorského práva, dovolím si začít stručným úvodem do problematiky práv duševního vlastnictví, kam autorské právo spadá. Zejména se chci zabývat typickými případy, se kterými se pravidelně setkáváme. A sice stahováním filmů, hudby, či softwaru z veřejně přístupných úložišť, zejména pomocí filehostingu a takzvaných peer-to-peer sítí, kterým se budu věnovat později.

6.3.1 Práva duševního vlastnictví

Vyčerpávající výčet toho, co jsou práva "duševního vlastnictví" najdeme v čl. 2 Úmluvy o zřízení Světové organizace duševního vlastnictví[97]. Rozumí se jimi *práva k literárním, uměleckým a vědeckým dílům, k výkonům výkonných umělců, zvukových záznamů a rozhlasovému vysílání, k vynálezům ze všech oblastí lidské činnosti, k vědeckým objevům, k průmyslovým vzorům a modelům, k továrním, obchodním známkám a známkám služeb, jakož i k obchodním jménům a obchodním názvům, práva na ochranu proti nekalé soutěži a všechna ostatní práva vztahující se k duševní činnosti v oblasti průmyslové, vědecké, literární a umělecké.*

Především je třeba říci, že se jedná o výsledky procesu lidského myšlení a zkoumání, které mají jako takové nehmotnou povahu. Předmětem společenských vztahů jsou ale práva k nim a proto hovoříme o právu duševního vlastnictví. To se dělí do dvou hlavních kategorií a to na průmyslové vlastnictví (průmyslová práva) a autorská práva.[98]

[96] Zpráva MV: op. cit., s. 33
[97] Vyhláška ministra zahraničních věcí č. 69/1975 Sb., o Úmluvě o zřízení Světové organizace duševního vlastnictví podepsané ve Stockholmu dne 14.7. 1967, ve znění vyhlášky č. 80/1985 Sb.
[98] SMEJKAL, V. (2015).: op. cit., s. 333

6.3.2 Průmyslové vlastnictví

Průmyslovým právem rozumíme ochranu výsledků technické tvůrčí činnosti (vynálezy a užitné vzory), předměty průmyslového výtvarnictví (průmyslové vzory), jakož i práva na označení (ochranné známky a označení původu) a v neposlední řadě také konstrukční schémata polovodičových výrobků (tzv. topografie polovodičových výrobků) a další.[99]

Proti porušování průmyslových práv týkajících se vynálezů, průmyslových vzorů, užitných vzorů a topografií polovodičových výrobků[100] nám poskytuje ochranu trestní zákoník v § 269 TZ. Uvedenými právy se zabývají předpisy: zákon č. 527/1990 Sb. o vynálezech a zlepšovacích návrzích, ve znění pozdějších předpisů, zákon č. 207/ 2000 Sb. o ochraně průmyslových vzorů, ve znění pozdějších předpisů, zákon č. 478/1992 Sb. o užitných vzorech, ve znění pozdějších předpisů a zákon č. 529/1991 Sb. o ochraně topografií polovodičových výrobků, ve znění pozdějších předpisů.

Zajímavým způsobem, jak lze uvedená průmyslová práva v souvislosti s ICT porušit, je 3D tisk. Ten je prováděn 3D tiskárnou, která z vhodného materiálu pomocí jeho vrstvení trojrozměrně "vytiskne" hmotný předmět dle návrhu, například zbraň, součástku počítače apod.[101] Takový návrh věci, respektive její technická konstrukce, ale mohou být chráněny průmyslovým právem.

6.3.3 Autorské právo

Porušování autorských práv je často vnímáno jako synonymum pro kybernetickou kriminalitu. Jedná se o celosvětový problém, který si společnost velmi dobře uvědomuje. Na jedné straně máme autory, pro většinu z nichž je jejich dílo současně jejich živobytím. Na druhé straně máme řadu uživatelů informačních a komunikačních technologií, kteří konzumují to, co jim kyberprostor nabízí, včetně obsahu legálního a nelegálního. Někteří uživatelé v tomto ohledu tvrdí, že Internet je svobodné médium a dokud na něm obsah bude dostupný, ať už je jakéhokoliv původu, budou jej konzumovat.

---

[99] http://www.upv.cz/cs/prumyslova-prava.html (zobrazeno 12.4.2016)

[100] *Pouze tyto čtyři druhy předmětů práv průmyslových jsou výslovně uvedeny v § 269 Porušení chráněných průmyslových práv v TZ. A contrario tedy nelze podle tohoto ustanovení TZ stíhat zásah do práv k jiným předmětům průmyslového práva.* SMEJKAL, V. (2015).: op. cit., s. 335

[101] http://www.pravniprostor.cz/clanky/trestni-pravo/kyberneticka-kriminalita-fenomen-dneska (zobrazeno 14.4.2016)

A tak přestože chápeme, že je třeba práva autorů chránit, a že je nutné zajistit, aby za svou práci měli výdělek, tak se často chováme úplně opačně. Toto téma je obecně zajímavé a já jsem se mu proto rozhodla věnovat ve své práci větší prostor.

Během úvodního výkladu budu čerpat hlavně ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (dále jen jako "autorský zákon" nebo "AZ"), který nám poskytuje komplexní úpravu autorského práva a který je v poměru speciality vůči občanskému zákoníku.

Hned na úvod můžeme uvést, že *neoprávněného užívání autorských děl v oblasti ICT se dopouštějí pachatelé zásadně dvěma způsoby:*

a) neoprávněným užíváním (a/nebo šířením) počítačových programů,

b) neoprávněným užíváním (a/nebo šířením) jiných autorských děl, zejména pak audiových a audiovizuálních děl (hudba, filmy).[102]

Nás zajímají především případy, kdy k neoprávněnému užití autorského díla (porušení autorského práva) dochází prostřednictvím dálkového přístupu. Jedná se například o sdílení nelegálního díla e-mailem, přes filehostingový server, nebo skrze link, který nás na nelegální obsah odkazuje. Mimo to také samozřejmě rozeznáváme i neoprávněné užití autorského díla pomocí fyzického kontaktu, kdy např. dochází k opakovanému prodeji nelegální kopie hudebního CD.

6.3.3.1 Předmět autorského práva

Prvním pojmem, který je třeba vyložit, je autorské dílo, jakožto předmět autorského práva, čili to, co podléhá ochraně dle AZ. Co to je předmět autorského práva nám říká § 2 odst. 1, 2 AZ:

(1) Předmětem práva autorského je 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

[102] SMEJKAL, V. (2015).: op. cit., s. 342

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.

(2) 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.

Pod těmito pojmy si představíme zejména umělecká díla, jako jsou např. básně, povídky, romány, hudební díla, obrazy, fotografie, filmy a počítačové programy.[103]

Já se ve své práci budu zabývat zejména hudbou, filmy, literaturou a počítačovými programy, které jsou nejčastěji předmětem porušování autorských práv v kyberprostoru. Právě v souvislosti s nimi hovoříme o tzv. "počítačovém pirátství". Tím myslíme kopírování, distribuci a používání autorsky chráněného softwaru, filmů, hudby nebo elektronických knih bez povolení jejich vlastníka a za využití výpočetní techniky.[104]

6.3.3.2 Obsah autorského práva

Obsahem autorského práva, jak uvádí § 10 AZ jsou výlučná práva osobnostní a práva majetková.

Práva osobnostní jsou uvedená v § 11 AZ a patří sem právo autora:

(1) právo rozhodnout o zveřejnění svého díla.

(2) právo osobovat si autorství, včetně práva rozhodnout, zda a jakým způsobem má být

[103] Problematika počítačových programů, čili software je ještě o něco složitější. U software v zásadě platí, že při jeho koupi uživatel kupuje tzv. licenci. Tedy právo na užívání nějakého softwaru/ programu a právě to je chráněno autorskými právy Taková licence pak určuje, jak lze se softwarem nakládat, například kolikrát lze software nainstalovat. Proto stažení software z Internetu ještě nemusí trestněprávní důsledky mít, zadání licenčních údajů (zpravidla e-mail a tzv. "klíč") už ano. Obráceně to samozřejmě platí i pro upload.

[104] http://www.stoppiratstvi.cz/cs/o-piratstvi/co-je-piratstvi.shtml (zobrazeno 20.6.2016)

jeho autorství uvedeno při zveřejnění a dalším užití jeho díla...
(3) právo na nedotknutelnost svého díla...

Pro osobnostní práva platí, že se váží konkrétně k osobě autora a tudíž se jich nelze vzdát, autor je nemůže převést a jeho smrtí zanikají (§ 11 odst. 4 AZ).

Mezi majetková práva pak patří právo dílo užít a jiná majetková práva. Než ale uvedu co je jejich obsahem, objasním, komu náleží právo dílo užít. O tom pojednává § 12 odst. 1 AZ:

(1) Autor má právo své dílo užít v původní nebo jiným zpracované či jinak změněné podobě, samostatně nebo v souboru anebo ve spojení s jiným dílem či prvky a udělit jiné osobě smlouvou oprávnění k výkonu tohoto práva; jiná osoba může dílo užít bez udělení takového oprávnění pouze v případech stanovených tímto zákonem.

Zásadně tak platí, že dílo může užít pouze autor a dále ten, komu dá autor souhlas k užití jeho díla (kdy hovoříme o udělení tzv. "licence"). V zákonem stanovených případech lze ale dílo užít i bez souhlasu autora. Této výjimce se budu věnovat později.

O tom, co znamená právo užít dílo nám říká více ustanovení § 12 odst. 4 AZ:

(4) Právem dílo užít je

a) právo na rozmnožování díla (§ 13),

b) právo na rozšiřování originálu nebo rozmnoženiny díla (§ 14),

c) právo na pronájem originálu nebo rozmnoženiny díla (§ 15),

d) právo na půjčování originálu nebo rozmnoženiny díla (§ 16),

e) právo na vystavování originálu nebo rozmnoženiny díla (§ 17),

f) právo na sdělování díla veřejnosti (§ 18), zejména

1. právo na provozování díla živě nebo ze záznamu a právo na přenos provozování díla (§ 19 a 20),

2. právo na vysílání díla rozhlasem či televizí (§ 21),

3. právo na přenos rozhlasového či televizního vysílání díla (§ 22),

4. právo na provozování rozhlasového či televizního vysílání díla (§ 23).

Jiná majetková práva jsou pak uvedená v § 24 AZ právo na odměnu při opětném prodeji originálu díla uměleckého a § 25 AZ právo na odměnu v souvislosti s rozmnožováním díla pro osobní potřebu a vlastní vnitřní potřebu.

Pokud bychom měli uvést ta nejčastěji porušovaná autorská práva v rámci kyberkriminality, půjde určitě o právo na rozhodnutí o zveřejnění díla (§ 11 odst. 1 AZ), dále právo na rozmnožení díla (§13 AZ), právo na rozšiřování originálu nebo rozmnoženiny díla (§ 14 AZ) či právo na sdělování díla veřejnosti (§ 18 AZ).

6.3.3.3 Porušení autorského práva a trestněprávní kvalifikace

Autor, do jehož práv bylo neoprávněně zasaženo se může předně domáhat ochrany před soudem prostřednictvím soukromoprávní žaloby, a to dle nároků uvedených v pátém díle autorského zákona. V závažnějších případech, kdy bude třeba takové škodlivé jednání potrestat, a tam kde nebude stačit postih dle jiného právního předpisu, tedy posouzení případu jako přestupku (§ 105a AZ), či správního deliktu právnických a podnikajících fyzických osob (§ 105b AZ), lze tedy jako ultima ratio použít trestního práva.

Trestní zákoník pro tyto případy postihu upravuje tuto skutkovou podstatu:

§ 270

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.

(2) Odnětím svobody na šest měsíců až pět let, peněžitým trestem nebo propadnutím věci bude pachatel potrestán,

a) vykazuje-li čin uvedený v odstavci 1 znaky obchodní činnosti nebo jiného podnikání,

b) získá-li takovým činem pro sebe nebo pro jiného značný prospěch nebo způsobí-li tím jinému značnou škodu, nebo

c) dopustí-li se takového činu ve značném rozsahu.

(3) Odnětím svobody na tři léta až osm let bude pachatel potrestán,

a) získá-li činem uvedeným v odstavci 1 pro sebe nebo pro jiného prospěch velkého rozsahu nebo způsobí-li tím jinému škodu velkého rozsahu, nebo

b) dopustí-li se takového činu ve velkém rozsahu.

Zde je třeba zdůraznit několik věcí. Předně to, že se jedná o blanketní normu. První odstavec nás totiž odkazuje na "zákonem chráněná práva k autorskému dílu", čímž se myslí právě autorský zákon. Zásah musí mít také určitou intenzitu, neboť jak je uvedeno, musí být "nikoliv nepatrný". Proto budeme vždy posuzovat konkrétní okolnosti případu. Nepatrné zásahy by pak byly řešeny jako přestupky, či jiné správní delikty. Z hlediska subjektivní stránky je vyžadován úmysl pachatele. Ten se *musí vztahovat i na pachatelovo vědomí, že jde o dílo jako výsledek tvůrčí činnosti autora.*[105] Také je třeba upozornit na fakt, že pachatelem může být s ohledem na § 7 ZTOPO[106] vedle fyzické osoby i osoba právnická.

6.3.3.4 Autorské dílo v kyberprostoru

Po vysvětlení základních pojmů z autorského práva a vyložení trestní sankce, která se k porušování autorského práva v kyberprostoru váže mohu přistoupit k další části výkladu.

Hudba, filmy, literatura a software, které jsou autorským dílem (předmětem autorského práva) jsou dnes běžně dostupné on-line. Lze je bez problému po zaplacení stáhnout, ať už do PC nebo do mobilních zařízení. Tímto způsobem získávají autoři z prodeje určitý zisk.

Vedle toho ale existuje ještě možnost si vše zmíněné díky Internetu stáhnout bez placení. A skoro všichni jsme tak pravděpodobně někdy učinili. Z takového stažení už samozřejmě autorům žádný zisk neplyne. Pokud tedy nebyl autorův záměr své dílo zpřístupnit veřejnosti on-line bezplatně, vzniká problém.

Zjednodušeně lze říci, že nelegální kopie filmů, hudby, literatury atd. které jsou na Internetu dostupné, způsobují autorům ztráty. Jak je ale možné, že jsou vůbec

[105] ŠÁMAL, P.: op. cit., s. 2753

[106] Zákon č. 418/2011 Sb., Zákon o trestní odpovědnosti právnických osob a řízení proti nim v odst. 7 obsahuje taxativní výčet trestných činů, jichž se právnická osoba může dopustit, kde je uveden i trestný čin dle § 270 TZ Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi.

nelegální kopie filmů na Internetu dostupné? Kdo nese odpovědnost za takové zpřístupnění? A jaké právní postavení má ten, kdo si poté takovou kopii stáhne? Pokusím se co nejsrozumitelněji vysvětlit technickou i právní stránku věci a vše doplním související judikaturou.

Předně je nutné zabývat se tím úplně nejdůležitějším, a tedy vytvořením kopie autorského díla. To samo o sobě ovšem není nelegální. Právo vytvořit si kopii díla, tedy jej rozmnožit (§ 13 AZ) náleží sice pouze autorovi, případně osobě, které udělí souhlas. Jak ale víme z § 12 odst. 1 AZ, v zákonem stanovených případech může bez souhlasu autora dílo užít i jiná osoba. To znamená, že je možné si bez souhlasu autora udělat např. kopii hudebního CD. Tyto zákonem stanovené případy, kdy může bez souhlasu autora užít dílo někdo jiný, jsou taxativně vymezeny v § 30 AZ a jsou označeny jako tzv. "volná užití".

Institut "volných užití" je upraven v §30 odst. 1, 2, 3 AZ, který zní následovně:
(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.
(3) Nestanoví-li tento zákon dále jinak, užitím podle tohoto zákona je užití počítačového programu či elektronické databáze i pro osobní potřebu fyzické osoby či vlastní vnitřní potřebu právnické osoby nebo podnikající fyzické osoby včetně zhotovení rozmnoženiny takových děl i pro takovou potřebu...

Je třeba zdůraznit, že tento režim "volných užití" platí pro autorská díla, s výjimkou počítačových programů. Z třetího odstavce daného ustanovení jasně plyne, že vytvořit kopii PC programu si nemůžeme za žádné situace. Nejedná se o výjimku z autorského práva.

Když se ale vrátím k zpět k výjimce, kdy není třeba souhlasu autora k užití díla, můžeme na základě uvedeného konstatovat, že vytvořit si kopii hudebního CD, které si budu pouštět pro radost u sebe doma je v pořádku a autorské právo tím neporušuji.

Mělo by ale moje jednání nějaké limity? Ano, autorský zákon chrání autora důkladně a upravuje i tzv. "tříkrokový test" (dále jen "test"), který stanovuje tři

podmínky, které musí být splněny, aby bezesmluvní užití díla (bez souhlasu autora) bylo dovolené. Test najdeme v ustavení § 29 odst. 1 AZ:

1) 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.

To znamená, že pokud bych si původně pouze pro svou potřebu vytvořila kopii hudebního CD (volná užití), ale později bych jej přehrávala ve své kavárně, jednalo by se už o užití nedovolené. Přehrávání hudby (z kopie originálu CD) návštěvníkům kavárny určitě není v souladu se zájmy autora a ani to není běžný způsob užití díla. Takové situace se ale vždy musí porovnávat individuálně a podle konkrétních okolností případu.

Obdobně si pak můžeme představit situaci, kdy je taková kopie hudebního CD umístěna volně ke stažení na Internet tak, že k ní má přístup nespecifikovatelný počet osob (sdělování díla veřejnosti §18 AZ, jedno z práv "užít dílo"). I v tomto případě se jedná o nelegální jednání a porušení autorských práv. Podrobněji se touto otázkou budu zabývat dále.

Musíme si nejprve uvědomit základní fungování mechanismu sdílení skrze Internet, ať už se týká jakéhokoliv obsahu. Rozlišujeme zde osobu tzv. uploadera, tedy toho, který obsah nahrává, dává k dispozici druhému, tzv. downloaderovi, který si jej stahuje. Internet jim umožňuje přenos uskutečnit a k tomu lze využít různé způsoby, jako je např. filehosting, peer to peer síť, či linking.

6.3.3.5 Filehosting

Filehosting neboli webové úložiště je úplně základní a snad všem známý způsob jak na Internetu sdílet prakticky cokoliv. Filehostingová služba, umožňuje hostování (nahrávání) uživatelských souborů na webový server poskytovatele. Jedná se o tzv. on-line úložiště souborů. Mezi nejznámější patří zahraniční Mega, Rapidshare anebo třeba

české uloz.to či uschovna.cz. Motivací pro vznik takových úložišť je například zisk z reklamy.[107]

Soubory, které lze na úložiště nahrát, mohou být jakéhokoliv charakteru. Mohou to být dokumenty, fotografie, videa atd. K těmto souborům může mít poté přístup více či méně neomezený počet uživatelů, což ovlivňuje uploader svou volbou při nahrávání. Ten má možnost soubor zaheslovat, takže k němu mají přístup pouze osoby, které znají heslo, anebo jej také nechat skrýt a přístup k němu zná jen on díky vygenerovanému odkazu.

Zcela běžně se zde nachází volně ke stažení filmy či seriály, hudba a další. Vyvstává zde tedy otázka, jak právně posoudit právní postavení jednotlivých aktérů kteří se sdílení účastní. Jak víme, patří sem uploader, downloader, ale také ten, který webové úložiště spravuje.

Jak už jsem předestřela dříve, nahrát (upload) kopii autorsky chráněného obsahu (sdělování díla veřejnosti dle § 18 AZ), například film na webové úložiště tak, že k němu má přístup neomezené množství osob je jasným porušením autorských práv. Takovým jednáním se uživatel podle intenzity zásahu vystavuje trestnímu stíhání podle § 270 TZ.

Naproti tomu, stahuji-li (download) si takovýto soubor do svého PC, rozmnožuji tím autorské dílo (§ 13 AZ) a musíme se ptát, zda jednám v rozporu s autorským právem, či nikoliv. Pokud tak totiž činím pro vlastní potřebu (§ 30 odst. 2 AZ) a nikoliv v rozporu s běžným způsobem užití díla a ani tím nejsou nepřiměřeně dotčeny oprávněné zájmy autora (tříkrokový test dle § 29 odst. 1 AZ), mělo by být moje jednání v souladu se zákonem.

Pokud se ale zamyslíme nad tím, že je např. kopie filmu umístěná na úložiště nelegálně, pak není splněna podmínka tříkrokového testu, tedy že se nejedná o běžné užití díla. Dílo bylo totiž na Internet umístěno nelegálně. Dalo by se argumentovat, že každé jeho stažení je pak také nelegální.

Naproti tomu existuje i názor opačný, tedy že každé stažení, byť nelegální kopie autorského díla, je v pořádku. To proto, že § 30 AZ (volná užití) výslovně neřeší zda je

[107] Na webových stránkách úložiště je umístěna reklama (např. na nový mobilní telefon nejmenované značky), za kterou bylo provozovateli zaplaceno. Společnost, která za umístění takové reklamu platí, vsází na to, že si jí díky návštěvnosti webu všimne velké množství uživatelů.

zdroj, z nějž má být kopie pro osobní potřebu vytvořena, legální, či nikoliv. To pak znamená, že by naopak podmínky tříkrokového testu byly dodrženy.

Nejvyšší soud ve svém usnesení ze dne 25. 3.2009, sp. zn. 5 Tdo 234/2009 konstatuje, že: *ze znění ustanovení § 30 odst. 1 písm. a) AZ nelze dovozovat, že se omezení autorského práva pro pořizování rozmnoženiny díla pro osobní potřebu vztahuje pouze na pořízení rozmnoženiny z originálu díla nebo z jeho legálně zakoupené kopie pořizovatelem rozmnoženiny, neboť v rámci omezení autorského práva pro pořizování rozmnoženin pro osobní potřebu nestanoví toto ustanovení nic o právní povaze zdroje, ze kterého je možno rozmnoženinu díla pro osobní potřebu pořizovat.*

Může se tedy jednat jak o originál, tak i o rozmnoženinu díla, přičemž není bez dalšího nikterak vyloučeno, aby zdrojová rozmnožena, ze které si zhotovitel pořídí vlastní rozmnoženinu pro osobní potřebu, byla pořízena i na základě jednání, které je v rozporu s autorským zákonem.

Z toho dovozujeme, že *kopírování z ilegálního zdroje automaticky nezakládá autorskoprávní (resp. trestněprávní) odpovědnost.*[108]

Nezbývá než připomenout § 30 odst. 3 AZ a fakt, že stahovat se dá prozatím legálně z Internetu jakýkoliv autorský obsah s výjimkou softwaru.

Na posledním místě se musíme zabývat provozovateli filehostingových serverů. Jejich právní postavení je upraveno v zákoně č. 480/2004 Sb., o některých službách informační společnosti. Ten upravuje jejich odpovědnost v § 5 a omezuje ji na 3 případy:

- *pokud provozovatel mohl vzhledem k okolnostem vědět o tom, že obsah je závadný,*
- *pokud se provozovatel prokazatelně dozvěděl o protiprávní povaze obsahu uživatele a neprodleně neučinil veškeré kroky, které lze po něm požadovat k odstranění nebo znepřístupnění takovýchto informací,*
- *pokud provozovatel vykonával přímo či nepřímo rozhodující vliv na činnost uživatele.*

Provozovatel tak není primárně odpovědný za protiprávní obsah, jeho odpovědnost nastupuje jen ve výše uvedených třech případech. Toto omezení má sloužit k tomu, aby nebylo bráněno poskytování služeb prostřednictvím internetu.[109]

[108] http://www.lupa.cz/clanky/je-stahovani-piratskeho-obsahu-z-webu-legalni/ (zobrazeno 14.4.2016)
[109] http://finance.idnes.cz/odpovednost-provozovatelu-internetovych-ulozist-fxr-/pravo.aspx?c=A130509_233027_pravo_vr (zobrazeno 23. 6. 2016)

Ostatně sama důvodová zpráva k zákonu o některých službách informační společnosti říká, že *není rozumné požadovat od poskytovatelů, aby při vysokém počtu uživatelů a vysokém objemu uložených dat zjišťovali a posuzovali legálnost či nelegálnost veškerého obsahu uložených informací. Je věcí a odpovědností samotných uživatelů, jaký obsah ukládají na poskytnutém serverovém prostoru. Poskytovatelé proto nemají povinnost aktivně monitorovat materiály, které jsou na jejich serverech uloženy.*[110]

6.3.3.6 Peer-to-Peer

Peer-to-peer (nebo také "P2P") znamená v překladu do češtiny "rovný s rovným". Jedná se o typ počítačové sítě, v níž mezi sebou komunikují počítače uživatelů (klienti) přímo mezi sebou, nikoliv počítač uživatele se serverem, jako tomu bylo u filehostingu.

Jako P2P označujeme především výměnné sítě, jejichž prostřednictvím si uživatelé mohou vyměňovat soubory (data) jakéhokoliv charakteru, tedy dokumenty, obrázky, videa apod. Jedná se tak o legální způsob, jak spolu uživatelé "komunikují". Momentálně nejznámější P2P sítí je BitTorrent.

Jednou ze základních výhod P2P sítí je to, že s rostoucím množstvím uživatelů celková dostupná přenosová kapacita roste. Přenos souboru přes P2P síť funguje tak, že soubor se stahuje po částech z více zdrojů najednou. Naopak pokud stahuji ze serveru (filehosting), dělím se o konstantní kapacitu serveru, takže pokud je stahujících uživatelů více, pak průměrná přenosová rychlost klesá.[111]

V případě P2P máme osobu tzv. seedera (uploader) a leechera (downloader). Seeder má soubor již kompletně stažený a umožňuje ostatním uživatelům - leecherům jednotlivé části souboru stahovat. Leecher ovšem v okamžiku stahování, tím že kumuluje jednotlivé části souboru, tyto zároveň umožňuje stahovat dalším leecherům (laicky řečeno stahuje a nahrává zároveň). Soubor je pak kompletní stažením všech dílčích částí.

[110] Vláda: Důvodová zpráva k zákonu č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti), č. 480/2004 Dz
[111] https://cs.wikipedia.org/wiki/Peer-to-peer (zobrazeno 23.6.2016)

Ke stahování souborů (dat) skrze P2P sítě je ještě nezbytný speciální program, např. uTorrent a tzv. "torrent" soubor (soubor s koncovkou .torrent), který obsahuje metadata o tom, co přesně má být sdíleno. [112,113]

P2P sítě představují noční můru všech umělců. Jsou zřejmě nejpoužívanějším způsobem, jak uživatelé ve velkém sdílí nelegální kopie jejich výtvorů, zejména pokud jde o filmy a hudbu.

Nás stejně jako u filehostingu zajímá, jaké je právní postavení aktérů celého procesu sdílení. Přestože se jedná o jiný systém sdílení souborů, tak postavení seedera, tedy uploadera bude stejné jako v případě filehostingu. Seeder tedy může být potenciálně trestněprávně odpovědný za nelegální šíření kopie autorského díla. Opět zde totiž máme kopii autorského díla, která je zpřístupněná veřejnosti (§ 18 AZ) a to bez souhlasu autora tak, že k dílu má přístup neomezený okruh osob.

Právní postavení leechera, tedy downloadera bude podobné seederovi. Je zde tedy změna oproti postavení downloadera v případě filehostingu, kde jsem došla k závěru, že stahování není protiprávní.

Jak jsem uvedla v technickém popisu fungování sdílení pomocí P2P sítě, soubor (dílo) se zde sdílí po částech. Leecher tak v okamžiku vlastního stahování současně umožňuje dalším leecherům stahovat své, již stažené, části dosud nekompletního souboru. Zjednodušeně řečeno se tak částečně dostává do pozice seedera. Pak nezbývá než konstatovat, že se na něj uplatní stejná pravidla jako na seedera a uploadera u filehostingu, tedy že může být za stahování autorsky chráněného obsahu trestněprávně odpovědný.

Uzavírám, že sdílením filmů, hudby, literatury apod. resp. jejich nelegálních kopií přes P2P sítě se ti, kteří je využívají, vystavují v každém případě nebezpečí trestního stíhaní.

6.3.3.7 Warez, warez fóra, linking

Warez je termín počítačového slangu označující autorská díla, se kterými je nakládáno nelegálně, zejména v rozporu s autorským právem. K jeho šíření je dnes

[112] https://cs.wikipedia.org/wiki/BitTorrent (zobrazeno 23.6. 2016)
[113] http://www.lupa.cz/clanky/peer-to-peer-site-od-a-do-z-bittorrent-a-edonkey/#ic=serial-box&icc=text-title (zobrazeno 23.6.2016)

využíván hlavně Internet. Uživatelé, kteří s warezem nakládají, jsou často označováni jako počítačoví piráti a jsou zároveň určitou komunitou.[114]

Komunikují spolu především na tzv. warez fórech. Ty slouží sice jako prostředek, díky kterému je warez šířen, ale také obecně jako diskuzní fórum s různými tématy.

Nás ale zajímá jeho význam právě pro autorské právo, respektive pro jeho případné porušování. Zde se dostáváme k problematice tzv. linkingu. Jím rozumíme umístění tzv. linku (odkazu na soubor) na webových stránkách.

Link může mít dvojí charakter. V prvním případě dojde k tomu, že po jeho prokliknutí uživatele přesměruje na jiné stránky, tedy skutečně odkazuje jinam. Právě takové "obyčejné" linky (odkazy) se obvykle vyskytují na warez fórech.

V druhém případě link po prokliknutí automaticky daný obsah (na který je odkazováno) na původní stránce otevře. Prakticky to vypadá například tak, že se kliknutím přímo na původní stránce (kde je link umístěn) spustí film, ale k přenosu dat dochází z linkovaného serveru. V tomto případě tedy k přesměrování nedochází. Mluvíme o tzv. embedded (zapuštěných) lincích.

Obecně lze říci, že linkingem se uživatelé snaží obejít autorské právo. Ani v jednom z uvedených případů se totiž obsah (např. nelegální kopie filmu) nenachází na původních stránkách.

Zatímco u obyčejných linků právní problém nevyvstává, neboť tyto odkazují z původních stránek jinam (link je pouhou informací, kde obsah najít a ten se sám o sobě na původních stránkách vůbec neobjeví), v případě druhém už je situace odlišná.

6.3.3.8 Embedded linky

Tzv. Embedding je *technický způsob umístění obsahu na internetových stránkách vložením připraveného kódu, odkazujících na obsah umístěný na jiné internetové stránce tak, že je tento obsah možné zpřístupnit na té stránce, kde je embeddovaný link umístěn, bez nutnosti uživatele přejít na internetovou stránku, kde je umístěn obsah.*[115]

V případě embeddingu máme opět několik subjektů. Předně je zde osoba uploadera, tedy osoby, která soubor, ať už se jedná o cokoliv (v našem případě kopie

[114] https://cs.wikipedia.org/wiki/Warez (zobrazeno 24.6.2016)
[115] http://docplayer.cz/3912001-Kyberneticka-kriminalita-v-judikature-ceskych-soudu-doc-judr-tomas-grivna-ph-d-pravnicka-fakulta-uk-v-praze.html (zobrazeno 23.6.2016)

autorského díla) nahrála na Internet (např. webové úložiště). Na jeho právním postavení se proto, jak už jsem uvedla v kapitole 6.3.3.5, nic nemění (porušuje autorská práva a může být trestněprávně odpovědný),.

Druhým aktérem je downloader u kterého můžeme také dojít ke stejnému závěru jako v případě filehostingu, tedy že autorská práva svým jednáním neporušuje a trestněprávní odpovědnost zde nehrozí.

Nejzajímavější je zde postavení provozovatelů webových stránek, na kterých se embedded linky objevují. Nejvyšší soud v jednom ze svých rozhodnutí dovodil, že provozovatelé jsou za umístění embedded linků na svých webových stránkách odpovědní.

V kauze tzv. "libereckého piráta" se Nejvyšší soud zabýval trestní odpovědností za neoprávněné užití díla jeho "embeddováním" na webovou stránku. *Mladý muž v tomto případě po dobu 10 měsíců provozoval webové stránky, na kterých shromažďoval a zveřejňoval tzv. "embedded linky", které umožňovaly návštěvníkům jím provozovaných stránek shlédnout nejméně 2470 audiovizuálních děl a to bez souhlasu nositelů majitelů autorských práv.*[116]

Mladík svým jednáním zpřístupňoval uvedená díla veřejnosti ve smyslu § 18 odst. 2 AZ. Na protiprávnost svého jednání byl dokonce upozorněn Českou protipirátskou unií. V návaznosti na toto upozornění sice webové stránky smazal, avšak založil současně jiné, které fungovaly úplně stejně jako ty původní. Jeho obhajoba spočívala v tom, že tvrdil, že na své webové stránky neumístil žádné audiovizuální dílo, ale pouze embed kódy, které odkazují na jiný server odlišný od jeho. Tím pádem pak také nemohl naplnit skutkovou podstatu § 270 TZ.[117]

Nejvyšší soud však ve svém rozhodnutí ze dne 27. 2. 2013 sp. zn. 8 Tdo 137/2013 ale shledal, že: *"Za neoprávněný zásah do zákonem chráněných práv ve smyslu § 270 odst. 1 TZ lze považovat i takové jednání pachatele, který na Internetu v prostoru vyhrazeném pro své internetové stránky umístí odkazy (tzv. embedded linky) umožňující neoprávněný přístup k rozmnoženinám děl (např. filmových a televizních) umístěných*

[116] MYŠKA, M. Odkaz není zločin? Embedding, užití díla a trestný čin porušování autorského práva, *Revue pro právo a technologie*. 2013, č. 7 s. 42, dostupné z: https://journals.muni.cz/revue/article/viewFile/4368/pdf (zobrazeno 24.6.2016)
[117] Rozhodnutí NS sp.zn. 8 Tdo 137/2013, dostupné z: http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/763AE1D4853A3985C1257B5C004F46EE?openDocument&Highlight=0, (zobrazeno 24.6.2016)

na externích serverech tak, že kdokoli k nim může mít prostřednictvím takové internetové stránky přístup, aniž by k tomu měl souhlas nositelů autorských práv, a využije tzv. hostingu s možností uložení dat na serveru. V takovém případě totiž pachatel (umístěním tzv. embedded linku) umožnil přístup k rozmnožení díla, a to jako osoba odlišná od osoby, která je vlastníkem této rozmnoženiny nebo jinou oprávněnou osobou, což je činnost, jíž je nutné považovat za porušení autorských práv k jednotlivým dílům a porušení práva na sdělování díla veřejnosti ve smyslu § 18 odst. 1, 2 AZ."

Mladistvý tak popsaným činem porušil ustanovení § 18 odst. 2 AZ a naplnil tak znak neoprávněného zásahu do zákonem chráněných práv ve smyslu § 270 odst. 1 TZ. Znak nikoliv nepatrného zásahu do zákonem chráněných práv, jak vyžaduje ustanovení § 270 odst. 1 TZ byl taktéž naplněn, neboť pachatel uvedenou činnost provozoval po dobu 10 měsíců způsobem, který umožňoval téměř neomezený zásah do uvedených autorských práv, tudíž nemůže být pochyb o tom, že se jedná o zásah vyšší než nepatrný.[118]

Můžeme tak sledovat odlišný přístup než v případě filehostingu, kde jsem uvedla, že provozovatel webového úložiště není primárně za obsah na svém webu odpovědný (odpovědnost nastupuje ve vymezených případech). Podle mého názoru je ale přístup Nejvyššího soudu správný. Je třeba odlišit situaci, kdy někdo pro uživatele spravuje sdílecí službu, která může být potenciálně zneužita, a to, když někdo spravuje webové stránky s přímým úmyslem parazitovat na práci jiných. Motivací pro provozování takových webových stránek může být opět zisk z reklamy. Takové jednání nemůže zůstat bez odpovídající reakce.

6.3.3.9 Shrnutí

Můžeme sledovat, že problematika autorských práv v kyberprostoru je skutečně složitá. Přesto si myslím, že zákonodárce i judikatura pružně reagují na aktuální problémy.

Bohužel pro autory - umělce ale musíme konstatovat, že jejich možnosti ochrany jsou omezené. Skutečně není možné zajistit, aby nelegální kopie nevznikaly a nešířily

[118] Idem

se. Kyberprostor je fenomén, kterému se nelze postavit. Myslím že klíčové by pro umělce mělo být naopak přizpůsobit se mu a poskytovat prostřednictvím kyberprostoru konzumentům služby, které je od sdílení nelegálních kopií odradí.

6.4 Tradiční kriminalita v novém kabátě

Poslední kategorie útoků, která shromažďuje již známá škodlivá jednání, která díky ICT získala jinou formu.

6.4.1 Podvodná jednání

Jak uvádí zpráva Ministerstva vnitra, podvodná jednání v kyberprostoru celé oblasti kybernetické kriminality dominují.[119]

Nejobvyklejší formou je zřejmě podvod ve spojení s internetovým obchodováním v různých podobách, zejména při platbě předem.[120] Zpravidla se tak děje prostřednictvím tzv. podvodném e-shopu, či jiného webu, který nabízí nějaké zboží. Na první pohled se e-shop tváří jako normální obchod, ale po zaplacení zboží (předem) přijde problém a zboží není prodejcem odesláno. Případně je zasláno zboží jiné, a to buď úplně (např. balíček mouky), anebo jen dané zboží v horší kvalitě, či jiném množství. Na výzvu k vrácení peněz zpravidla obchodník nereaguje. Takové e-shopy bývají zakládány krátkodobě, pod falešným jménem provozovatele a nemají zpravidla žádné reference od jiných zákazníků[121]. Podvodný e-shop je ale možné při větší obezřetnosti odhalit, zejména přezkoumáním informací, které je obchodník ze zákona je povinen na webových stránkách e-shopu uveřejnit. Tam patří identifikační údaje, nákupní řád, obchodní a reklamační podmínky.[122]

Mezi další podvodná jednání můžeme řadit tzv. letadla, a další způsoby, kterými se podvodníci snaží z uživatelů ICT vylákat peníze, například za neexistující služby.[123] *A dále podvody spojené s účtováním jiné výše hodnot než jaké jsou ve skutečnosti. Stává se tak u účtování mzdy, v účetnictví, v elektronickém bankovnictví, pohybu skladových*

[119] Zpráva MV: op. cit., s. 61
[120] GŘIVNA, T., SCHEINOST M., ZOUBKOVÁ I.: op. cit., s. 347
[121] Například na webu heureka.cz
[122] http://finance.idnes.cz/podvodny-e-shop-u-slona-0v1-/viteze.aspx?c=A131209_110502_viteze_sov (zobrazeno 13.4.2016)
[123] MATĚJKA, M.: op. cit., s. 60-61

zásob apod.[124]

Za specifický podvod můžeme označit tzv. nigerijské dopisy, s nimiž má zkušenost řada uživatelů ICT. Vzhledem k rozvoji se forma dopisu přeměnila na e-mail, jehož prostřednictvím někdo neznámý prosí o zaslání finančního obnosu, za účelem darování charitě, půjčky, příspěvku na živobytí apod. Obsahem sdělení je současně dojemný příběh, který hraje na city adresáta, tak aby jej přesvědčil k zaslání finanční částky. Svůj úspěch nigerijské dopisy měly především s nástupem informačních a komunikačních technologií, dnes už se jedná spíše o historickou záležitost, která však stojí za připomenutí.

6.4.2 Zneužívání platebních karet

Placení prostřednictvím platební karty (debetní či kreditní) je dnes zcela běžné a to nejen fyzicky, ale i na Internetu. V obou případech ovšem existuje riziko jejího zneužití.

Prvním způsobem, jak lze platební kartu zneužít je tzv. skimming. *Skimmingem se označuje podvodný způsob fyzického okopírování magnetického proužku platební karty a následné odčerpání peněz prostřednictvím internetového platebního portálu, případně výběru z bankomatu. V praxi to funguje tak, že pachatelé umístí na bankomat zařízení na zkopírování údajů z karty. Jedná se o dvoudílné zařízení, kdy jedním jsou získávány údaje z magnetického proužku karty a druhým údaje o kódu PIN*.[125] Tyto údaje jsou pak nahrány na novou padělanou kartu, kterou lze dál užívat.

Další způsob jak může dojít ke zneužití platební karty je skrze platbu na Internetu. K takovým platbám jsou využívány veškeré údaje na kartě, včetně trojmístného kódu CVC/CVV který se nachází na její zadní straně a který je alternativou PIN kódu. Tyto informace by měly být po zadání do formuláře předávány bezpečnými kanály mezi bankou obchodníka a bankou držitele karty (tzv. systém "3D Secure"[126]). Přesto se může stát, že budou tyto údaje zneužity, nejčastěji neseriózním obchodníkem. Informace mohou být totiž zadány do formuláře, který obchodníkovi nepatří, a tak

[124] GŘIVNA, T., SCHEINOST M., ZOUBKOVÁ I.: op. cit., s. 347
[125] http://www.policie.cz/clanek/pozor-na-zneuziti-platebni-karty.aspx (zobrazeno 13.4.2016)
[126] Tento systém zajistí, že údaje jsou poskytovány bance a ne obchodníkovi. Bezpečnostní opatření dále spočívá v autorizaci dané platby zadáním jednorázového kódu, který přijde v SMS. S ohledem na bezpečnost internetových transakcí tento systém neposkytují všechny bankovní instituce. Také si jeho aktivaci (pro možnost plateb na internetu) zpravidla musí držitel karty sám vyžádat.

dojde k jejich úniku a později zneužití.[127] Obranou proti takovému zneužití platební karty je především obezřetnost a také třeba nastavení limitů pro platby na Internetu pro danou kartu.

6.4.3 Kyberterorismus

Stejně jako v jiných případech, tak i u terorismu došlo k jeho přesunu do kybernetického prostředí.

Na to, jaký je mezi terorismem a kyberterorismem vztah mají různí autoři různý názor. *Jedna skupina autorů a odborníků považuje za „kybernetický terorismus" široké spektrum aktivit, které zpravidla alespoň nějak souvisí s terorismem nebo kyberprostorem. Jedná se tak o aktivity velmi různorodé a často velice vzdálené od terorismu samotného. Druhá skupina se naopak snaží kyberterorismus co nejpřesněji vymezit a zabránit dalšímu rozmělňování již nyní velmi abstraktních konceptů.*[128] Já se přikláním k užšímu vymezení a tedy, že kyberterorismus je podmnožinou terorismu a tedy jde o poddruh terorismu, který je páchán za pomoci informačních a komunikačních technologií.

Smyslem takových teroristických útoků je vyvolat strach, či neadekvátní reakci za účelem dosažení nějakého politického cíle. Útoky jsou tak nejčastěji extremisticky, nacionalisticky a politicky motivované.[129]

Je třeba říci, že klasický terorismus útočí fyzicky a dochází při něm pravidelně ke ztrátám na životech. Na většinu společnosti takové útoky působí velmi negativně, protože soucítí s oběťmi a pozůstalými.

Vzhledem k povaze kyberprostoru je jen velice obtížné zde páchanými teroristickými útoky způsobit skutečné násilí ve smyslu poškození zdraví lidí, ztrát na životech nebo rozsáhlého zničení majetku, jako je tomu u terorismu.

Elektronické útoky jsou však velmi dobře schopny způsobit rozsáhlé ekonomické škody, poškodit prestiž a image nebo nepřímo vést i k fyzickému násilí. V každém

[127] http://www.penize.cz/platebni-karty/18567-platebni-karty-jaka-zneuziti-cihaji-a-jak-se-jim-branit (zobrazeno 13.4.2016)
[128] DRMOLA, J. Konceptualizace kyberterorismu. *Vojenské rozhledy*. 2013, č. 2., s. 96
[129] JIRÁSEK P., NOVÁK L., POŽÁR J.: op. cit., s. 59

případě musí být útokem (nebo hrozbou útoku) generován intenzivní strach či podobný silný psychologický účinek.[130]

Podle Dorothy Denning, která se problematikou kyberterorismu zabývá, ale teroristické skupiny stále preferují bombové útoky, než kybernetický terorismus. Naopak kyberprostor využívají k šíření svých myšlenek a jiným aktivitám, které směřují k dosažení jejich cílů.[131]

Mezi zatím nejznámější a teroristické útoky v kyberprostoru se řadí DDoSové útoky na Estonsko v roce 2007 a na Gruzii v roce 2008. Obě země měly v tomto období s Ruskou federací problematický vztah a také jí označují jako útočníka. V Estonsku došlo k přemístění sovětského válečného památníku, což Kremlin odsoudil.[133] Mezi Gruzií a Ruskem se schylovalo k válečnému konfliktu (Válka v Jižní Osetii). V obou případech byly útoky nasměrovány na webové sránky vlády, politických stran, médií a bank, které byly vyřazeny z provozu.[134]

Dále jsou také známé hacktivistické útoky skupin Anonymous nebo LulzSec.[136] Ty působí celosvětově a prostřednictvím kyber útoků vyjadřují svůj názor (většinou nesouhlasný) s činností vlád a různých společností.

6.4.4 Kyberstalking

Takzvané nebezpečné pronásledování, neboli stalking je *způsob chování, kdy se pachatel zaměří na nějakého člověka, po kterém slídí, obtěžuje a pronásleduje jej, vyhrožuje mu a může jej i fyzicky napadat či dokonce usmrtit.*[137] Taková nevyžádaná pozornost je pro oběť velmi nepříjemná. Omezuje jí v jejím osobním životě a vyvolává pocity strachu.

Kyberprostor dal tomuto škodlivému jednání novou podobu. Stalking lze tak provádět za využití informačních a komunikačních technologií. Pachatel, tzv. stalker tak svou oběť může obtěžovat prostřednictvím e-mailů a jiných zpráv, nebo komentováním příspěvků oběti, ať už na sociálních sítích, nebo na blogu, dále také vytvářením vlastního obsahu, který se oběti týká, anebo telefonicky, prostřednictvím SMS, MMS

[130] DRMOLA, J.: op. cit., s. 97
[131] http://essays.ssrc.org/10yearsafter911/whither-cyber-terror/ (zobrazeno 20.6.2016)
[133] http://news.bbc.co.uk/2/hi/europe/6665145.stm (zobrazeno 20.6.2016)
[134] http://essays.ssrc.org/10yearsafter911/whither-cyber-terror/ (zobrazeno 20.6.2016)
[136] http://www.businessit.cz/cz/kyberneticka-kriminalita-iii-hacktivismus-a-kyberterorismus.php (zobrazeno 13.4.2016)
[137] SMEJKAL, V. (2015).: op. cit., s. 273

nebo telefonních hovorů.

V souvislosti s přesunem našich životů do kyberprostoru se nachází řada více či méně osobních informací na různých webových stránkách (například zaměstnaneckých) nebo diskuzních fórech, které může pachatel snadno o své oběti střádat a využívat k dalšímu obtěžování.

Bohužel pro oběť informační a komunikační technologie znásobily účinek, který stalking má. Přibyla totiž další možnost, jak jí může stalker kontaktovat a obtěžovat. Přesto si myslím, že pachatel bude nadále vyhledávat osobní kontakt s obětí a kombinovat tak možnosti jak se s ní spojit.

7. PACHATEL A OBĚŤ KYBERKRIMINALITY

Mezi další aspekty, kterými se kriminologie zabývá, patří i osoba pachatele a oběti. Statistiky a další kriminologická zkoumání, které se na ně soustředí, nám o nich poskytují řadu údajů. Ty nám poté umožňují porozumět konkrétnímu druhu kriminality a tím na ní i reagovat.

V případě kybernetické kriminality, která je souborem více druhů protiprávního jednání, respektive různých trestných činů, je ale těžké takové údaje získat. Znamenalo by to pro každou dílčí trestnou činnost zvlášť vytěžit ty informace, které mají spojitost s kyberprostorem.

7.1 Jaký je pachatel kyberkriminality a kdo je hacker?

Jak jsem naznačila, získat dostatečné množství informací o pachateli kybernetické kriminality, tak abychom sestavili jeho specifický profil, je velmi složité a dle mého dokonce nemožné.

Jde o to, že nelze vytvořit medián z údajů o pachatelích, kteří šíří dětskou pornografii, o majitelích falešných e-shopů a o kyberstalkerech. Každý z nich má jinou motivaci, jinou osobnost atd. Museli bychom proto vytvořit několik profilů zvlášť, pro každý trestný čin, a ty by potom zkoumaly motivace, příležitosti a uživatelské

schopnosti pachatelů atd.[138] To je jen těžko proveditelné a tak nyní uvádím pro základní přehled spíše obecnější fakta.

Pachatel kyberkriminality už nemusí disponovat zvláštními schopnostmi, a vzhledem k dostupnému škodlivému softwaru ani technikami. A přestože pachatelé bývají odborně vzdělaní (především v oblasti IT), jsou naproti tomu tací, kteří žádné odborné vzdělání nemají.[139]

Z hlediska věku pachatele nebude překvapením, že se spodní věková hranice posouvá spíše níže. Je to dáno především vývojem ICT, kterému se starší generace zcela nepřizpůsobila. Naučit osoby vyššího věku využívat nové prostředky, nebo postupy, ať už se to týká čehokoliv, je vždy problematické. Proto není divu, že počítače, chytré telefony atd. jsou doménou spíše mladších osob včetně těch nejmladších, tedy dětí.[140] Tato generace se také mj. označuje jako generace Z.[141] Studie OSN o kyberzločinu uvádí, že nejčastěji jsou pachatelé kyberkriminality ve věku mezi 18 - 30 lety.

Co se týká pohlaví pachatele, tak studie dále uvádí, že převážná většina pachatelů je pohlaví mužského.

Odhaduje se, že 80% útoků pochází z některé z forem organizované trestné činnosti. A ať už jde o malé nebo velké kriminální skupiny, svou typologií se podobají organizovaným skupinám v běžném světě.[142]

K úplnosti výkladu ještě uvádím, že pachatelem může být vedle fyzické osoby i osoba právnická. A to na základě zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim. Ten zavedl s účinností od 1. 1. 2012 trestní odpovědnost právnických osob.

V následující kapitole se budu věnovat možným typologiím, nebo spíše dělení pachatelů kybernetické kriminality. Předtím ale ještě objasním pojem "hacker", s nímž si veřejnost často (chybně) pachatele kyberkriminality spojuje.

---

[138] WALDEN, I. *Computer crimes and digital investigations*. 1st pub. Oxford: Oxford University Press, 2007, s. 62
[139] Studie OSN o kyberzločinu.: op. cit., s. 39
[140] KUCHTA, J., VÁLKOVÁ H. a kol.: op. cit., s. 507
[141] Jde o osoby narozené po roce 1990, pro něž je charakteristické, že využívaly internet ve velkém již od dětství, zdroj: https://en.wikipedia.org/wiki/Generation_Z, (zobrazeno 5.2.2016)
[142] Studie OSN o kyberzločinu.: op. cit. s. 39-41

7.1.1 Hacker (a Cracker)

Tyto pojmy jsou sice většině společnosti známé, ale myslím, že méně už jejich opravdový význam.

Termín "hacker" se v teorii a běžném jazyce vyvinul k označení pachatele počítačové trestné činnosti.[143] Přitom dříve, v druhé polovině 20. století, kdy se termín objevil, neměl s protiprávní činností nic společného. V té době vznikaly první obrovské počítače a pracovat s nimi mohla jen úzká část lidí. Mezi ně patřila i skupina studentů[144], kteří se díky práci s počítačem naučili programovat.[145] Byli to oni, kdo vymyslel pojem "hacking". Tak tehdy svou činnost s počítačem pojmenovali. Pro ně byl hacker někdo, "*kdo dělá... zajímavou a kreativní práci na vysoké úrovni*". Jejich hacking byla původně důmyslná a skutečná legrace, jako třeba hackování výtahu, kdy přepojili tlačítka ve výtahu a tím pádem tlačítko pro druhé podlaží poslalo osobu do dvacátého.

Od těchto začátků se hacking rozrůstal, nejen sám o sobě, ale i jako činnost praktikovaná po celé zemi.[146] *Byl vnímán jako technicky vyspělá aktivita, která byla prováděna na účet velkého technologického systému*[147] a nikdo si jej tehdy s kriminální činností nespojoval.

Postupem času hackeři vytvořili komunitu s vlastní jasně definovanou etikou, odpovídající tehdejším sociálním a politickým hodnotám[148]. Hackeři té doby běžně zkoumali ostatní počítačové systémy, což vyplývalo nejen ze zvědavosti, ale také z touhy se učit, objevovat a svobodně sdílet s ostatními, co zjistili. Naproti tomu ničení a jiné zásahy do takových systémů během průzkumů, ať už úmyslně či jinak, bylo shledáváno jak neschopné a neetické.

Ono dřívější pojetí hackingu a jeho charakter tak byly znevářeny svým negativním protějškem, průniky, poruchami, krádežemi a sabotážemi. Hackeři ze staré

[143] GŘIVNA, T., POLČÁK R.: op. cit., s. 38
[144] Z Massachusetts Institute of Technology's (MIT)
[145] např. dokázali přimět počítač "dělat věci", jako třeba převádět arabské číslice do římských.
[146] BRENNER, S. W. *Cybercrime and the Law: Challenges, Issues, and Outcomes*. Boston: University Press of New England, 2012, s. 16-17
[147] GŘIVNA, T., POLČÁK R.: op. cit., s. 39
[148] Tato etika mimo jiné vyzdvihovala právo na svobodný přístup a výměnu znalostí a informací, víru ve schopnosti vědy a technologií (zejména počítačů) podpořit životy jednotlivců, nedůvěru v politiku, války a korporátní autority, a odolnosti vůči "konvenčním" a "mainstreamovým" životním stylům, zvykům a sociálním hierarchiím.

školy rázně odmítali, aby byli takto negativně vnímáni a začali využívat pojem "cracker" k odlišení zlomyslného počítačového nadšence od opravdového hackera.[149]

Byť jsou Crackeři koexistující subkulturou hackerů[150], laická veřejnost mezi nimi rozdíl nedělá a užívá pro obojí jednotný název hacker.[151] Tím pádem je jasné, proč tento pojem získal postupem času pejorativní význam.

Pro zajímavost uvádím dvě definice hackera dostupné na internetu. První jej popisuje jako *osobu, která využívá počítač k tomu, aby získala neoprávněný přístup k datům.*[152] Druhá jako *někoho, kdo hledá a využívá slabost počítačového systému, nebo počítačové sítě.* [153] Zatímco první formulace je jasně negativní (s protiprávním charakterem), druhá už je neutrální (protiprávní prvek v ní chybí). Bude tak vždy záležet na úhlu pohledu, jak budeme hackera vnímat.

V každém případě je nutno připomenout, že pachatel kyberkriminality nerovná se hacker a naopak. I když můžeme říct, že hacker je někdo, kdo se zajímá o počítače a má k tomu příslušné znalosti, neznamená to, že každý takový činí při práci s počítačem něco protiprávního. A naproti tomu někdo s minimálními znalostmi s PC (například pachatel šířící dětskou pornografii prostřednictvím Internetu) rozhodně není automaticky hacker.

7.2 Existuje typologie pachatelů kyberkriminality?

V kriminologii, respektive u jednotlivých druhů trestné činnosti se objevují různá dělení, kategorie, a typologie pachatelů. Na základě určitého kritéria jsou tak pachatelé rozděleni do několika skupin, které je poté možné zkoumat jako celek, zaobírat se např. motivy, osobnostními rysy pachatelů atd.

Jenže kyberkriminalita je natolik rozmanitá, že vybrat vhodné kritérium, které by jí postihovalo jako celek je velmi složité. Anebo lépe řečeno, vytvořit dělení, které by bylo skutečně smysluplné a reprezentativní není jednoduché.

Přesto jsem se ve své práci rozhodla vyjádřit ke kategoriím a dělením pachatelů, které mne zaujaly nejvíce.

---

[149] YAR, M. *Cybercrime and society: crime and punishment in the information age*. 1st ed. Thousand Oaks, CA: SAGE Publications, 2006, s. 23
[150] GŘIVNA, T., POLČÁK R.: op. cit., s. 39
[151] Shodně SMEJKAL, V. (2015).: op. cit., s. 91
[152] http://www.oxforddictionaries.com/definition/english/hacker (zobrazeno 7.2.2016)
[153] https://en.wikipedia.org/wiki/Hacker_(computer_security) (zobrazeno 7.2.2016)

7.2.1 Dělení na amatéry a profesionály

V literatuře se objevuje dělení pachatelů na "amatéry" a "profesionály". Kuchta tak pachatele dělí *z hlediska jejich vztahů k informacím.*

Do první skupiny se řadí osoby, které náhodně nebo cílevědomě pronikají do informačních systémů a to tak, že vyhledávají zranitelná místa. Jsou to zpravidla osoby s vyšší jednostranně rozvinutou inteligencí, plně si uvědomující své počínání. Snadno se učí pracovat s počítači, jsou schopni se jim dále učit. Jsou flexibilní, vynalézaví a řešení nových problémů je pro ně osobní výzva.

Do druhé skupiny patří ti, jejichž náplň práce dána informačním procesem. K počítačovým prostředkům mají v rámci zaměstnavatele prakticky neomezený přístup. Jsou to např. programátoři, nebo pracovníci managementu.[154]

Jinými slovy rozhodujícím faktorem uvedeného dělení je to, zda má pachatel v oblasti IT zaměstnání či nikoliv. Myslím si, že to je ale pro profil pachatele a určení jeho vlastností, nepodstatné.

IT profesí je totiž celá řada a tak se úroveň uživatelských dovedností každého zaměstnance liší. Naproti tomu někdo, kdo se živí úplně jinou prací, může svými znalostmi takového zaměstnance předčit. Zaměstnání tak o schopnostech pachatele kyberkriminality ještě vůbec nic nevypovídá.

Podstatné jsou tedy faktické znalosti a zkušenosti, které může kdokoliv nabýt bez ohledu na zaměstnání, či vysokoškolské vzdělání.

7.2.2 Dělení dle Smejkala

Další rozřazení do skupin uvádí ve své knize Smejkal. Nabízí celkem pět různých skupin, přičemž *do první skupiny se rekrutují zaměstnanci poškozené organizace, případně zaměstnanci jejích dodavatelů.*

Do další skupiny patří průnikáři (hackeři), kyberpunkoví počítačoví desperáti. Mají spíše anarchistické rysy a tomu odpovídají jejich činy: zavirovávají počítače, pronikají do vládních počítačových sítí, provádí útoky DoS/ DDoS apod.

Třetí skupina patří organizovanému zločinu, jehož příslušníci využívají počítač zejména ke skryté komunikaci, výrobě padělků, nebo distribuci pornografie.

[154] KUCHTA, J., VÁLKOVÁ H. a kol.: op. cit., s. 508

Čtvrtou skupinu tvoří profesionálové, kteří se živí činností, jako jsou průniky, odhalování státních a obchodních utajovaných informací atd. Jde převážně o žoldáky pracující za peníze, nebo v rámci služby v ozbrojených silách a výzvědných službách.

Poslední skupinu tvoří lidé, obvykle ve věku dětí a mladistvých, kteří o svém jednání a jeho následcích příliš nepřemýšlejí. Vůbec je nenapadne, že by se mohlo jednat o trestnou činnost- a pokud se na to přijde, hájí se zcela naivně.[155]

U tohoto členění předně postrádám hledisko, kterým se autor řídil. Je sice pravda, že takoví pachatelé existují, ale podle nich sestavené kategorie mi nedávají smysl, a to hlavně proto, že nám stejně neumožňují sledovat motiv pachatele, jeho osobnostní stránku, nebo například typ trestného činu aj.

Takto vytvořené skupiny vnímám jen jako prázdné kategorie, pouze jako určité seřazení, protože je žádoucí nějakou kategorizaci vytvořit.

7.2.3 Dělení dle znalosti a vybavenosti pachatele

Jako poslední jsem se rozhodla uvést jedno z dělení, které nabízí Požár, a to podle znalosti a vybavenosti pachatele, které rozeznává tři následující skupiny:

Skupinu slabé síly, kam řadí amatéry a náhodné útočníky využívající náhodně objevená zranitelná místa při běžné páci. Útoky jsou náhodné/ neúmyslné, útočníci mají omezené znalosti, příležitosti i prostředky. Stačí vůči nim přijmout relativně slabá, ale zato levná protiopatření.

Skupinu střední síly, kam patří hackeři, koumáci, hračičkové, typicky VŠ/SŠ studenti, "psychopati", jejichž krédem je dostat se k tomu, na co nejsou autorizovaní. Jedná se o běžné úroky. Útočníci mívají mnohdy hodně znalostí. Na ochranu se přijímají protiopatření střední síly.

A nakonec skupinu velké síly, což jsou profesionální zločinci, kteří mají původ obvykle mezi počítačovými profesionály. Je pro ně typická neomezenost znalostí, mají dostatek prostředků (peněz) a mnohdy i dost času. Provádějí útoky vymykající se běžné praxi a je nutno proti nim přijímat silná protiopatření.[156]

Jak je patrné, ani toto dělení nepostihuje celou oblast kyberkriminality. Těžko říct, kam bychom měli zařadit pachatele, který na Internetu šíří xenofobní či rasistické texty

[155] SMEJKAL, V. (2015).: op. cit., s. 488
[156] POŽÁR, J. *Základy teorie informační bezpečnosti*. 1. vyd. Praha: Vydavatelství PA ČR, 2007, s. 40-41

anebo pachatele, který provozuje fiktivní internetový obchod, jehož prostřednictvím podvodně jedná. Uvedené členění je totiž zaměřeno pouze na pachatele "informační kriminality", o níž autor ve své publikaci pojednává. Pro účely dělení pachatelů kyberkriminality je tím pádem nepoužitelné.

Myšlenka takového vzestupného dělení mi ale nepřijde špatná, ovšem za užití jiného kritéria. Vedla jsem úvahu, zda by bylo možné dělit pachatele podle toho, jak náročné je spáchat trestný čin.

To znamená, že umístit nevhodný příspěvek na internetovém fóru nebo šířit dětskou pornografii je snadné. Provést podvod, nebo nelegálně šířit software je už náročnější. A zásahy do počítačových sítí (hacking) nebo počítačová špionáž jsou těmi nejnáročnějšími trestnými činy.

V těchto kategoriích bychom poté mohli sledovat psychologii pachatele. Spáchal by takový trestný čin i v reálném světě? Jaká je souvislost jeho protiprávního jednání s jeho uživatelskými schopnostmi s PC?

V každém případě by se asi jednalo o mravenčí práci a je otázka, zda by poté bylo možné vzešlé výsledky zužitkovat v boji s kyberkriminalitou.

7.2.4 Shrnutí

Sledování a studium chování jednotlivých druhů pachatelů by jistě přispělo k prevenci a represi kyberkriminality. Přesto jsem došla k závěru, že rozdělit pachatele do skupin, které bychom poté mohli zkoumat, je prozatím nemožné.

Brání nám v tom především variabilita trestných činů, kterých se pachatelé dopouštějí a také náročnost sběru dat, které s kyberkriminalitou souvisí. A tak nezbývá než se spokojit s obecnou charakteristikou pachatele a zaměřit se efektivní sběr informací, které se jej týkají.

7.3 Pachatel kybernetické kriminality a jeho motiv

Vedle otázky "kdo" je nezbytné ptát se i "proč". Co vede pachatele kyberkriminality k protiprávnímu jednání? A proč bychom to měli zjišťovat?

Motiv sám o sobě umožňuje trestněprávní kvalifikaci jednání a určuje stupeň jeho společenské škodlivosti. Odpovídá nám ale také na otázku kdo má, nebo by mohl mít ze

spáchaného činu prospěch. To je užitečné v okamžiku, kdy tipujeme pravděpodobného pachatele z vymezeného okruhu podezřelých osob.[157]

Jak už jsem naznačila, motivy jsou různé a pachatel jich může mít hned několik najednou. *Převažujícím motivem pachatelů kyberkriminality je obvykle bezpracný zisk, osobní obohacení, často zdůvodňované nízkým finančním oceněním pachatele, zejména ve srovnání se zisky firmy, nebo jejich majitelů.* [158]

Existují ale i další motivy, například zvědavost, pomsta, touha po moci a po dobrodružství a také chuť vymezit se proti ostatním. S motivem si pak více či méně umíme představit, jaký by pachatel mohl být. Třeba znechucený zaměstnanec, který chová zášť vůči svému zaměstnavateli a mstí se mu škodlivými aktivitami v zaměstnanecké síti. Či mladý teenager, který zkouší možnosti Internetu. Anebo nevyrovnaný jedinec s touhou vymezit se proti světu svými názory.

Motiv je další údaj, který nám pomáhá dotvářet obraz pachatele. Jeho zjištěním získáváme přehled o psychickém stavu pachatele a také jeho vztahu ke spáchanému trestnému činu. Je to další věc, která nám pomáhá na kybernetickou kriminalitu reagovat, čili jí úspěšně předcházet a eliminovat.

7.4 Oběť kybernetické kriminality

Při zkoumání etiologie trestné činnosti je stejně žádoucí střádat poznatky o obětech jako o pachatelích trestných činů.

Už dříve jsem ale uvedla, že v rámci kyberkriminality se často stává, že oběti dílčích trestných činů protiprávní jednání, kterého se proti nim někdo dopustil, neoznámí. Buď proto, že neví, že jsou obětí trestného činu, anebo to ví, ale nechtějí na sebe upozorňovat v obavě, že by mohly být samy stíhány za trestný čin.

V této souvislosti je zajímavé co uvádí Gřivna, a to že *většina postižených subjektů (podniky a organizace) nemá zájem na zveřejnění útoku, který utrpěla, protože by to odhalilo jejich zranitelnost a omylnost. Zveřejnění by mohlo poškodit ekonomický úspěch těchto obětí, protože by zvýšilo nedůvěru v bezpečnost jejich služeb a tím snížilo důvěru veřejnosti.*[159]

[157] SMEJKAL, V. (2015).: op. cit. s. 487
[158] Idem
[159] GŘIVNA, T., POLČÁK R.: op. cit., s. 36

Pokud ale oběti trestný čin neohlásí, údaje nám chybí a to jen brzdí vyšetřování trestné činnosti a akademický výzkum jako takový. V případě kyberkriminality je přitom obzvlášť žádoucí informace o obětech shromažďovat a analyzovat je. Vzhledem k současným možnostem připojení a technické vybavenosti společnosti totiž existuje permanentní riziko, že se každý uživatel ICT může obětí kyberkriminality skutečně stát.

Takovým uživatelem může být jedinec, společnost nebo stát aj. korporace. Oběť může být jak fyzická, tak právnická osoba. Jediným předpokladem je jednoduše spojení s kyberprostorem.

Co se týče charakteristiky oběti, tak bude pochopitelně, stejně jako u pachatelů, záležet na tom, kterého trestného činu jsou obětí. Je třeba si uvědomit, že typické studie o obětech těch kterých trestných činů, bude měnit právě povaha kyberprostoru.

Jak uvádí Zpráva MV, *internetoví podvodníci se čím dál častěji zaměřují na seniory. Kontaktují je pomocí inzerátů, nevyžádaných e-mailů a sociálních sítí a nabízejí jim různé zboží a nevýhodné smlouvy. Stále častější je také citové vydírání seniorů přes internet. Stále větší počet seniorů má totiž přístup k internetu a počet těch, kteří se stávají terčem podvodů tak každý rok strmě narůstá.*[160]

Ohroženou skupinou jsou pak z podobného důvodu i děti, které mají k Internetu sice běžně přístup, ale většinou ještě nejsou schopné rozeznat podvodná jednání, anebo se bránit proti šikaně.

Proto je v každém případě třeba, aby uživatelé ICT dbali na vhodná preventivní opatření. Jak uvádí společnost Norton (Symantec) ve svém přehledu za rok 2015, celosvětově bylo v tomto roce obětí "online" zločinu 594 milionů osob přičemž uživatelé pro svou ochranu stále nepodnikají příslušné kroky.[161]

Ve Velké Británii, kde vzrůstá počet útoků v oblasti kybernetické kriminality, konkrétně v rámci hospodářské kriminality, už přišli s tím, že oběti, které nepřijaly dostatečná preventivní opatření, budou mít ve vyšetřování nižší prioritu, než ostatní.[162] Toto jen poukazuje na fakt, jakou práci s vyšetřováním této, navíc rostoucí, trestné činnosti policejní složky mají.

---

[160] Zpráva MV: op. cit., s. 62

[161] https://us.norton.com/cyber-security-insights#expander-content-4709169d1ad49c49183a3b7038cddc7 (zobrazeno 28.2.2016)

[162] http://www.telegraph.co.uk/news/uknews/crime/11931958/Victims-of-cyber-crime-should-be-low-priority-if-they-fail-to-take-security-steps-says-report.html (zobrazeno 28.2.2016)

8. SOUČASNÝ STAV KYBERNETICKÉ KRIMINALITY

Stav kyberkriminality by se dal sledovat pomocí nejrůznějších statistik. Jak už jsem ale uvedla, kyberkriminalita je škodlivé jednání čítající řadu trestných činů. V policejních a justičních statistikách není vykazována samostatně[163] a tak se u každého trestného činu musí zkoumat jeho souvislost s kyberprostorem. Identifikovat takové trestné činy není jednoduché, a tak je náročné i vytvořit statistiku, která se jich týká.

Jak už ale vyplývá ze zprávy OSN, kyberkriminalita je na vzestupu.[164] *Z původně zanedbatelného počtu trestných činů souvisejících s kyberprostorem jejich množství v ČR každoročně stoupá.*[165]

Nejužitečnější informace ohledně trestné činnosti páchané v prostředí informačních technologií včetně počítačových sítí, nabízí Zpráva MV[166]. Jednoznačně z ní také vyplývá nárůst této trestné činnosti, když uvádí, že v roce 2014 bylo řešeno 4348 případů, což je o 48% víc než předešlý rok.

Trestná činnost v kyberprostoru v roce 2014 podle zprávy MV spočívala zejména v porušování autorských práv, výhružkách, vydírání a podvodném jednání, u kterého je navíc zaznamenáván trvalý meziroční nárůst. Zejména rostou útoky formou phishingu (kapitola 6.1.1.4.). Roste také počet podvodných jednání souvisejících s vyváděním finančních prostředků do virtuálních měn.

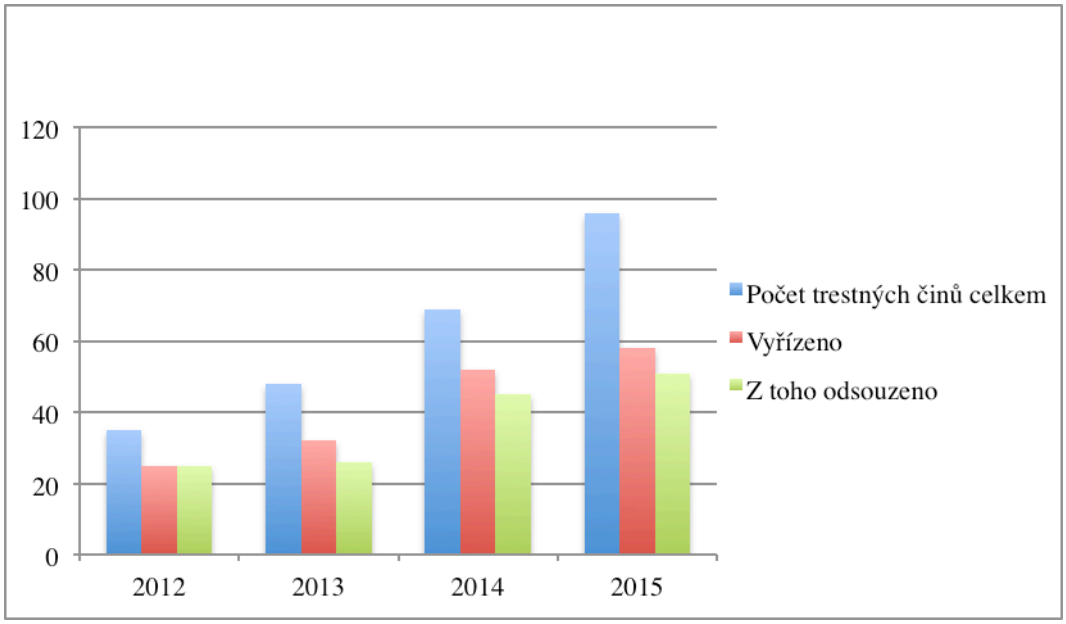
Zajímavé informace se dále týkají autorského práva. V lednu 2014 byl za šíření nelegálních kopií softwaru v ČR odsouzen k nepodmíněnému trestu odnětí svobody v délce 20 měsíců první Čech. V ČR se přitom pirátsky užívá až 38% softwaru, který má hodnotu 3,8 miliardy korun. A jak správně zpráva dodává, *autorské právo v tomto případě neporušují jen ti, kteří takový software nabízí, ale i ti, kteří si jej koupí a nainstalují.*[167]

Konkrétní trestné činy, které můžeme spolehlivě sledovat v rámci statistik, jsou tzv. počítačové trestné činy, kam se řadí neoprávněný přístup k počítačovému systému a nosiči informací, opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat a poškození záznamu v počítačovém systému a na nosiči

[163] GŘIVNA, T., SCHEINOST M., ZOUBKOVÁ I.: op. cit., s. 349
[164] Studie OSN o kyberzločinu.: op. cit. s. 6
[165] GŘIVNA, T., SCHEINOST M., ZOUBKOVÁ I.: op. cit., s. 349
[166] Zpráva MV hovoří o informační kriminalitě, jedná se pouze o jiné použití terminologie pro kriminalitu páchanou v kyberprostoru.
[167] Zpráva MV: op. cit., s. 62

informací a zásah do vybavení počítače z nedbalosti. Níže uvedený graf znázorňuje počet "počítačových" trestných činů, které byly v letech 2012 až 2015 evidovány, a dále počet osob, které stanuly před soudem na základě obžaloby z některého z nich (vyřízené) a současně počet skutečně odsouzených. V každém ohledu je zde patrný rostoucí trend.

Graf č. 1 Statistika počítačových trestných činů - § 230- 232 trestního zákoníku



Pramen: Justiční statistiky. *Přehled o pravomocně vyřízených osobách podle paragrafů - právní předpis TRZ2009* za roky 2012, 2013, 2014 a 2015 (dostupné online).

9. BOJ PROTI KYBERNETICKÉ KRIMINALITĚ

Stejně jako u jiných druhů kriminality i zde je nutné škodlivému jednání předcházet anebo na ně zpětně reagovat těmi nejúčinnějšími dostupnými prostředky. Prevence a represe jdou ruku v ruce spolu a jsou nezbytné pro to, aby kontrola, v tomto případě kybernetické kriminality, byla co nejúspěšnější.

9.1 Prevence

Vzhledem k povaze kyberprostoru není snadné útokům, k nimž zde dochází, předcházet. Tím základním předpokladem jak se primárně bránit je vlastní obezřetnost. Je třeba, aby si uživatelé ICT uvědomili svou zranitelnost, kterou jako takoví mají.

Bránit se lze především fyzicky, tedy chránit svá zařízení, ať už jde o PC, telefon, úložný disk, nebo připojení k wifi routeru. Předně zařízení nepůjčovat neznámým lidem a nenechávat je bez dohledu. Také je nutné hlídat svá přístupová hesla, nesdělovat je dalším osobám a nezaznamenávat si je tam, kde je lze snadno dohledat- v PC samotném, v telefonu či v diáři.

Téměř samozřejmostí dnes bývá instalace ochranného softwaru (který se zpravidla sestává z antiviru[168], firewallu[169] a případně i antispywaru[170]), který brání zařízení před útoky, k nimž v kyberprostoru dochází.

V neposlední řadě je také nezbytná osvěta uživatelů, a to zejména pokud jde o děti a seniory, kteří se vyznačující neopatrností a velkou důvěřivostí. V tomto ohledu mají v ČR zásluhu především Národní centrum kybernetické bezpečnosti (dále jen "NCKB"), Národní centrum bezpečnějšího internetu (dále jen "NCBI").

NCKB které je zřízené pod gescí Národního bezpečnostního úřadu je především státním orgánem, který dohlíží na bezpečí českého internetu. Zabývá se kybernetickými hrozbami a útoky, o kterých shromažďuje informace, tak aby na ně mohl co nejlépe reagovat a především o nich informovat veřejnost a stát. V tomto ohledu se věnuje také mezinárodní spolupráci a pořádá přednášky, které se zabývají kybernetickou bezpečností, čímž jednoznačně přispívá k vyšší informovanosti laické i odborné veřejnosti.

Naopak NCBI je nevládní a neziskové sdružení, které se zabývá bezpečností užívání Internetu a ICT. Pořádá konference, semináře, přednášky a školení, jejichž prostřednictvím šíří osvětu právě v oblasti nebezpečí, které může kyberprostor skrývat a dále se také zabývá etikou v oblasti online prostředí.

[168] Program, který kontroluje přítomnost virů v PC. Je pravidelně aktualizovaný tak, aby znal ty nejnovější. Na jejich přítomnost uživatele upozorní a případně provede i jeho smazání.
[169] Tzv. "bezpečnostní brána" provádí ochranu oběma směry. Umí vyhodnotit škodlivá data, které nedovolí propustit do PC (směr dovnitř) a opačně nedovolí určitým datům PC opustit (směr ven).
[170] Který detekuje a odstraňuje spyware.

9.2 Represe

Odpovědí na škodlivé jednání v kyberprostoru jsou především zákonné normy. Pro trestní represi je zásadní trestní zákoník, ve kterém najdeme skutkové podstaty tzv. "počítačových trestných činů" a další. Trestní zákoník je nástrojem státních orgánů-policie, soudů aj., který jim umožňuje vyšetřovat a především stíhat ta nejzávažnější škodlivá jednání, k nimž v kyberprostoru dochází.

Zásadní úlohu má ve vyšetřování má samozřejmě Policie ČR, která kybernetické kriminalitě věnuje velkou pozornost. Na základě útoku proti premiéru Bohuslavu Sobotkovi z ledna 2016, který spočíval v krádeži jeho e-mailové komunikace, se Policie ČR rozhodla posílit své stavy o specialisty z oblasti IT tak, aby její práce byla co nejefektivnější.[171] Mimo jiné Policie ČR na svých webových stránkách umožňuje veřejnosti od srpna 2012 nahlásit závadný obsah a aktivity, které se na internetu objevují. Jedná se o tzv. formulář "Hlášení kyberkriminality" po jehož vyplnění bude podaný podnět zpřístupněn policistům odboru informační kriminality Policie ČR a následně prošetřen.

Těmito kroky dává ČR jasně najevo, že boj proti kybernetické kriminalitě je jednou z jejích současných priorit s tím, že kriminální jednání v kyberprostoru rozhodně nebude tolerováno.

10. VYBRANÉ ZAHRANIČNÍ PŘÍSTUPY K ŘEŠENÍ KYBERNETICKÉ KRIMINALITY

V předchozích kapitolách jsem mnohokrát zdůraznila mezinárodní charakter kybernetické kriminality a také to, jak je mezistátní spolupráce v této oblasti nezbytná. Jedině společnými silami mohou státy efektivně proti škodlivému jednání v kyberprostoru působit.

Jednotlivé národní úpravy se sice liší, ale dá se říci, že vzhledem k mezinárodním závazkům (např. Úmluva o kybernetické kriminalitě) se daří, aby státy trestněprávně stíhaly shodná protiprávní jednání.

[171] http://zpravy.idnes.cz/internet-bude-hlidat-nova-pocitacova-policie-fnf-/domaci.aspx?c=A160513_214736_domaci_fka (zobrazeno 14.5.2016)

Přesto v některých státech můžeme sledovat odlišné přístupy v tom, jak reagovat na škodlivé jednání v kyberprostoru. Příkladem může být Německo, které se snažilo zavést blokaci webových stránek, které obsahovaly dětskou pornografii, a Francie, která měla v úmyslu odpojovat uživatele internetového připojení v případě porušení autorských práv.

10.1 Německo a dětská pornografie

Na první pohled efektivní řešení problematiky šíření dětské pornografie na Internetu, jakožto trestné činnosti s vysokou společenskou nebezpečností, měli v úmyslu zavést v Německu.

V dubnu roku 2009 tamní ministryně pro rodinné záležitosti vyjádřila záměr přijmout právní úpravu, která by umožnila blokovat internetové stránky s obsahem dětské pornografie. Jejím cílem tak bylo bojovat proti zneužívání dětí na všech úrovních, což se týká i obrázků na Internetu. Takovéto blokování webových stránek mělo být jednou částí plánu, jak potírat dětskou pornografii.[172]

Německá veřejnost se tehdy proti připravovanému zákonu tvrdě ohradila a více než 130 000 občanů, což bylo v té době nejvíce v historii Německa, podepsalo on-line petici. která vyjadřovala nesouhlas s navrhovaným opatřením.[173] Myšlenka cenzury a omezení základních svobod se německé veřejnosti nezamlouvala.

Nicméně později v červnu roku 2009 Německý spolkový sněm nakonec zákon přijal. Zákon vyžadoval aby federální vyšetřovací úřad vedl seznam webových stránek obsahujících dětskou pornografii, který měl dále postoupit poskytovatelům internetového připojení. Ti měli poté za úkol blokovat cestu uživatelů na tyto webové stránky.[174]

Tato právní úprava budila od počátku diskuzi. Blokování internetových stránek bylo shledáváno jako neefektivní a také jako počátek cenzury. Mnoho právních expertů jej považovalo za porušení Německé ústavy.[176]

---

[172] http://www.spiegel.de/international/germany/family-minister-vs-freedom-of-speech-anti-child-pornography-law-flounders-a-627447.html (zobrazeno 20.6.2016)

[173] https://opennet.net/blog/2009/06/germany-passes-legislation-block-child-pornography (zobrazeno 20.6.2016)

[174] http://www.theinquirer.net/inquirer/news/1356941/german-parliament-passes-internet-censorship (zobrazeno 20.6.2016)

[176] https://en.wikipedia.org/wiki/Zugangserschwerungsgesetz (zobrazeno 15.5.2016)

Kritici také poukazovali na fakt, že existují efektivnější, méně obtěžující cesty jak potlačit dětskou pornografii, jako třeba výzva e-mailem web-hostingové společnosti, aby nevhodný obsah smazala. Navíc se pro menší poskytovatele internetového připojení ukázalo jako problematické dodržovat podmínky, které zákon zavedl. Největší obava se ale týkala cenzury. Jak by totiž jednou byla cenzura takto schválena, mohla by být dále rozšířena i na jiné oblasti. Právo na svobodu projevu, odpor a svobodu přístupu k informacím by bylo narušeno.[177]

Situace se pak zkomplikovala v září roku 2009, kdy po volbách došlo k novému rozložení politických sil a zákon se stal předmětem jednání nově vzniklé koalice. Ta se nakonec shodla, že odstoupí od záměru blokovat internetové stránky a spíše přistoupí k mazání nevhodného obsahu. Než však došlo k vytvoření nového zákona namířeného proti dětské pornografii, prezident Německa předchozí zákon podepsal s tím, že v únoru roku 2010 vstoupil v účinnost. Německá vláda se tak ocitla v nezáviděníhodné situaci, když měla v účinnosti zákon, který vlastně nechtěla.[178]

A tak se nakonec v prosinci roku 2011, po více než dvou letech diskuzí, Německý spolkový sněm rozhodl zákon umožňující blokování stránek s dětskou pornografií zrušit.

Jeden z členů tamní Pirátské politické strany označil blokování internetových stránek za zbytečné. Obejít toto opatření podle něj zabere 5 minut. Především ale upozornil, že bojovat proti dětské pornografii by se mělo tam, kde tento problém začíná. Obrázky a videa přeci mají nějaký původ, dětská pornografie přeci není problémem Internetu.[179]

Já se domnívám, že byť měla tehdejší vládnoucí koalice dobrý úmysl, původně zvolené prostředky skutečně nebyly vhodné. Svoboda, ať už se týká čehokoliv, je křehká a je dobře, že si němečtí zákonodárci nakonec uvědomili své pochybení a zákon zrušili. Nemůžu jinak, než se ztotožnit s tím, že blokování přístupu na webové stránky není vhodné řešení a jednou povolené blokování je výzvou pro blokování další.

[177] http://www.theinquirer.net/inquirer/news/1356941/german-parliament-passes-internet-censorship (zobrazeno 20.6.2016)
[178] http://www.spiegel.de/international/germany/the-law-that-nobody-wanted-new-internet-legislation-embarrasses-german-government-a-678782.html (zobrazeno 20.6.2016)
[179] http://www.dw.com/en/bundestag-looks-to-delete-child-pornography-websites/a-15575254 (zobrazeno 20.6.2016)

10.2 Francie a autorské právo

Mnohem ráznější přístup v oblasti porušování autorských práv na Internetu měli ve Francii, kde jako možnou sankci zavedli přerušení pachatelova připojení k Internetu. Nakonec ale bylo od tak razantního řešení ustoupeno.

V červnu roku 2009 tamní zákonodárce přijal zákon, označovaný jako "tvorba a internet", nebo také jako "Hadopi 1". Jeho cílem bylo zejména zamezit sdílení souborů skrze P2P. Pro tento účel zákon zřídil nezávislou státní instituci HADOPI (Haute autorité pour la diffusion des oeuvres et la protection des droits sur Internet), tzv. Vrchní úřad pro šíření děl a ochranu práv na Internetu (dále také jako "úřad").[183] Tento úřad i přes řadu reforem funguje dodnes a jeho úkolem je *zejména kontrolovat zneužívání Internetu pro porušování autorských práv.*[185]

Zákon Hadopi 1 počítal se zavedením systému tzv. "stupňující se odpovědi" ("la riposte graduée"), označovaný také jako "třikrát a dost", na jehož dodržování by dohlížel zmíněný úřad. Systém měl fungovat tak, že pokud by byl někdo přistižen při stahování autorsky chráněného obsahu skrze sítě peer-to-peer (nikoliv např. přes filehosting), tak byl identifkován skrze užitou IP adresu a poté mu byl zaslán varovný e-mail. Pokud by uživatel tomuto varování nevěnoval pozornost a nadále pokračoval v nelegálním stahování, byl by upozorněn na rizika svého počínání doporučeným dopisem. Po této druhé výzvě už měl totiž následoval trest ve formě odpojení od internetového připojení v délce od 3 měsíců do jednoho roku s tím, že by uživatel nemohl ani přejít k jinému poskytovateli internetového připojení.[186]

Cílem tohoto mechanismu bylo odradit uživatele od stahování autorsky chráněného obsahu z Internetu. Měl ale určité nedostatky. Tak například ten, že uživatel byl identifikován pomocí IP adresy. Co když pod danou IP adresou ale funguje celá rodina? Nebo dokonce společnost? To by pak kvůli nezákonnému stahování jedné osoby byli odpojeni všichni?

Mnohem zásadnější problém se ale objevil v působnosti úřadu samotného. Měl to být totiž úřad sám, který rozhodoval o tom, zda bude uživatel odpojen. To vše bez

[183] https://fr.wikipedia.org/wiki/Loi_favorisant_la_diffusion_et_la_protection_de_la_création_sur_internet (zobrazeno 21.6.2016)
[185] HERCZEG, J., GŘIVNA, T., Právo na přístup k Internetu, blokace stránek a digitální gilotina, Trestněprávní revue. 2009, č. 5, s. 143
[186] http://www.lepoint.fr/actualites-societe/2008-11-02/telechargement-illegal-que-dit-la-nouvelle-loi-hadopi/1597/0/288089 (zobrazeno 21.6.2016)

projednání před soudem. Naopak s tím, že by hrozila dvojí sankce. Uživatel by mohl být za zasažení do autorského práva obžalován z trestného činu a hrozil by mu trest odnětí svobody v délce až tří let a pokuta ve výši až 300 000 euro.[187]

Zákonem se proto zabýval Francouzský ústavní soud, který shledal činnost úřadu v *rozporu s (i) presumpcí neviny,*

> *(ii) s principem, že rozhodovat o vině a ukládat tresty může pouze soud (HADOPI není soud) a*
>
> *(iii) s právem na svobodu slova.*[188]

Soud ve svém rozhodnutí především zdůraznil, že Deklarace práv člověka a občana ve svém článku čl. 11 zaručuje svobodu sdělování myšlenek a názorů. Pokud tedy stát umožňuje občanům toto právo uplatňovat on-line, musí jim také zaručit právo na přístup k tomu "být on-line".[189]

Z toho důvodu byl v září roku 2009 přijat zákon "Hadopi II", který na výtky soudu reagoval a zavedl v systému několik drobných, za to důležitých změn. V platnosti zůstaly dvě výzvy (e-mailem a doporučeným dopisem), s tím že na potřetí následuje odpojení od Internetu (v délce max. 1 roku). O sankci už ale nerozhoduje úřad, nýbrž nezávislý soud. Navíc přibyla vedle sankce odpojení od Internetu možnost uložit pachateli pokutu do výše 1500 euro (v případě recidivy až 3000 euro). Úřad tak získal jistou policejní výsadu s tím že mohl označit určité stahování jako ilegální a poté postoupit věc soudu.[190]

Můžeme sledovat, že počáteční úmysl francouzského zákonodárce razantně trestat uživatele ICT, kteří porušují autorská práva na Internetu, postupně oslaboval. Nakonec byla sankce odpojování od připojení k Internetu v červnu roku 2013 zrušena úplně a zůstala v platnosti (jako třetí stupeň odpovědi) pouze pokuta až do výše 1500 euro. Tamní vláda shledala, že odpojování od Internetu nebylo účinné a tato sankce by neměla mít v našem světě místo. Prioritou se stal boj proti komerčnímu pirátství a proti webům, které profitují z autorsky chráněného obsahu, aniž by z toho něco měli autoři

[187] http://www.agoravox.fr/actualites/technologies/article/hadopi-pour-les-nuls-explications-54212 (zobrazeno 21.6.2016)
[188] HERCZEG, J., GŘIVNA, T.: op. cit., s. 143
[189] http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/2009/decisions-par-date/2009/2009-580-dc/decision-n-2009-580-dc-du-10-juin-2009.42666.html (zobrazeno 16.5.2016)
[190] http://www.lemonde.fr/technologies/article/2009/09/15/que-contient-hadopi-2_1240913_651865.html (zobrazeno 21.6.2016)

samotní. Došlo zde ke změně filozofie, neboť přístup k Internetu je pro obě strany, jak pro tvůrce (autory), tak pro jejich konzumenty zásadní a nemá smysl přístup omezovat.[191]

Zajímavé jsou v tomto ohledu statistiky týkající se činnosti úřadu a vlivu, který měl. Předně je třeba říci, že i přes velké množství výzev (e-mailů a dopisů), které byly odeslány neustále pokračoval klesající trend prodeje hudby. Bylo tak jen otázkou času, kdy se politici začnou ptát, k čemu se platí tak nákladný chod instituce, jejíž účel není naplněn.[192]

Nejzajímavější je ale fakt, že za celou dobu činnosti úřadu byl k odpojení od Internetu na dobu 15 dní odsouzen (nepravomocně) pouze jeden člověk a to v červnu roku 2013, jen měsíc předtím, než došlo k samotnému zrušení sankce v zákoně. S ohledem na pokračující soudní řízení se nakonec podle zásad trestního práva procesního užilo pozdější výhodnější právní úpravy a původně uložený trest spočívající v odpojení od Internetu nebyl nikdy vykonán. Ke květnu roku 2016 bylo celkem zasláno 6,8 milionu e-mailových výzev, více než 622 500 tisíc doporučených dopisů a 972 případů bylo řešeno před soudem.[193]

Také Francie měla původně zajímavou, ale podle mě utopickou myšlenku, že bude-li vyhrožovat odpojením uživatelů ICT od Internetu, povede to ke zvýšení prodejů hudby, filmů aj. Představa, že výzvy, pokuty a původně i odpojení, odradí uživatele ICT od stahování hudby a filmů a naopak je nasměrují do obchodů, kde si toto všechno budou řádně kupovat, je dle mého názoru mylná.

[191] http://www.culturecommunication.gouv.fr/Presse/Communiques-de-presse/Publication-du-decret-supprimant-la-peine-complementaire-de-la-suspension-d-acces-a-Internet (zobrazeno 21.6.2016)
[192] https://www.techdirt.com/articles/20130603/00362223289/france-ready-to-shut-down-hadopi-as-its-incompatible-with-digital-economy.shtml (zobrazeno 21.6.2016)
[193] http://www.numerama.com/politique/129728-hadopi-faq-savoir.html (zobrazeno 21.6. 2016)

ZÁVĚR

Ve své diplomové práci jsem se věnovala především pojmu kyberprostoru a zejména pak škodlivému jednání, k němuž v něm dochází. Mou snahou bylo obzvláště srozumitelně vysvětlit základní souvislosti a hlavně podstatu kybernetické kriminality jako takové.

Předně bylo nutné věnovat se, byť krátce, historii vývoje počítačů. Myšlenka, že by kdysi obří počítače mohly komunikovat mezi sebou, dala vzniknout Internetu a tím i kyberprostoru jako takovému.

Tento virtuální svět, existující souběžně vedle každodenní reality ale nelze přirovnávat pouze k Internetu, nebo světu počítačů. Naopak Internet a veškerá technická zařízení, která nám jej umožňují používat, ať už jde o počítače, chytré telefony, routery, nebo kabeláže, atd. tvoří kyberprostor, jakožto interaktivní prostředí, v němž můžeme díky uvedenému komunikovat.

Poměrně krátká evoluce výpočetní techniky měla vliv i na terminologii, a tak jsme se postupně od počítačové, informační a internetové kriminality dostali ke kriminalitě kybernetické, jakožto trestné, nebo spíše škodlivé činnosti, k níž dochází právě v onom kyberprostoru.

Kyberkriminalita se značně odlišuje od ostatních druhů trestné činnosti. Mezi její hlavní specifika patří to, že díky dostupnosti ICT je to prakticky nenákladná činnost. Tím pádem také může být páchána širokým spektrem pachatelů, protože počítačem, či chytrým mobilním telefonem a připojením k Internetu dnes disponuje téměř každý.

Pokud jde o právní úpravu, tak v České republice máme řadu zákonů, které s kyberprostorem nějak souvisí. Pokud se pak týká konkrétně kybernetické kriminality, tak je pro nás zásadní samozřejmě trestní zákoník. Tam ale nenajdeme žádný výčet "kyberzločinů", jak se s oblibou trestným činům, k nimž dochází v kyberprostoru, říká. V trestním zákoníku máme tři pomyslné kategorie trestných činů, k nimž dochází v kyberprostoru: "počítačové trestné činy", dále trestné činy, kde je přitěžující okolností jsou-li spáchány prostřednictvím "veřejně přístupné počítačové sítě" a na závěr ostatní trestné činy, čili běžné skutkové podstaty, které pouze aplikujeme na případy, odehrávající se v kyberprostoru. Typicky jde například o TČ podvodu.

Protože je kybernetická kriminalita problémem celosvětovým, není překvapením, že se jí zabývá i řada mezinárodních institucí a zejména pak Úmluva o kybernetické kriminalitě, která je po několika letech od svého vzniku konečně závazná i v České republice a která je zásadní pro harmonizaci jednotlivých národních úprav pokud jde právě o boj proti kybernetické kriminalitě.

Hlavní částí mé práce je pak popis škodlivého jednání, k němuž v kyberprostoru dochází. Mým cílem bylo shrnout ty činnosti, nebo chceme-li nebezpečí, s nimiž se můžeme setkat při běžné práci s ICT, nikoliv je však trestněprávně kvalifikovat. Aby se nejednalo jen o bezmyšlenkovitý seznam, rozhodla jsem se pro dělení útoků podle Úmluvy a to na čtyři základní kategorie: (i) útoky proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů, kde je cílem útoku narušit, poškodit nebo proniknout do ICT, (ii) útoky spočívající ve vytváření a šíření škodlivého obsahu, kde jsou ICT spíše prostředkem k šíření škodlivého obsahu, (iii) útoky spočívající v porušování práv duševního vlastnictví a (iv) na útoky tradiční, kde škodlivá aktivita známá z reálného světa přechází do virtuálního, např. kyberšikana.

V každé z uvedených kategorií pak byly případné podkategorie anebo přímo popis jednotlivých škodlivých jednání. Těch se ukázala být celá řada, ale myslím, že se mi podařilo uvést ty skutečně nejznámější, s nimiž má bohužel mnoho z nás zkušenost. Ať už jde o phishing, nebo malware v podobě počítačových červů a virů, dětskou pornografii, či třeba kyberstalking.

Zvláštní pozornost jsem pak věnovala právům duševního vlastnictví, respektive porušování autorského práva v kyberprostoru. Zde bylo zapotřebí čerpat a uvést mnoho informací z autorského zákona, který obsahuje komplexní úpravu autorského práva a bez nějž by nebylo možné pochopit veškeré souvislosti. Teprve poté bylo možné tento exkurs propojit s existencí kyberprostoru a věnovat se problematice sdílení autorského obsahu na Internetu. Právní posouzení uploadera a downloadera vždy bude záležet na tom, jakým způsobem k sdílení dochází. Zatímco uploader autorsky chráněného obsahu (bez souhlasu autora) jedná v podstatě vždy v rozporu s právem, u downloadera situace tak jednoznačná není. Zabývala jsem se i otázkou právního postavení provozovatelů webových úložišť a webových stránek, které obsahují tzv. embedded linky. Ač by se mohlo zdát, že jejich postavení bude stejné, je tomu právě naopak.

V kapitole, která se zabývala osobami oběti a pachatele kybernetické kriminality jsem došla k závěru, že ani jednu z nich nelze jasně charakterizovat. Byť se také řada autorů snažila vytvořit určitá členění, která by pak shrnovala jejich společné znaky, já jsem ani jedno neshledala jako uspokojivé. Naopak zastávám názor, že v tomto případě je lepší užít charakteristiku obecnou a zejména pak neužívat automaticky pro pachatele označení hacker.

Abych popsala současný stav kybernetické kriminality, čerpala jsem především ze studie OSN o kyberzločinu a ze zprávy MV o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky v roce 2014. Z těchto dokumentů jasně vyplývá, že trestná činnost, k níž dochází v kyberprostoru, každoročně narůstá. V České republice je pak nejpalčivějším problémem v kyberprostoru porušování autorských práv a podvody. Z přiložené tabulky týkající se tzv. "počítačových trestných činů" můžeme taktéž sledovat meziroční nárůst výskytu těchto trestných činů, které se díky své konkrétní skutkové podstatě dají ve statistikách vykázat.

Boji proti kybernetické kriminalitě můžeme rozložit na etapu prevence (předběžná činnost) a represe (následná činnost). V případě prevence hraje roli hlavně obezřetnost uživatelů samotných, kteří by měli využívat jednak ochranný software a jednak být pozorní při uživatelské činnosti s ICT. A dále v osvětě veřejnosti, které se věnuje zejména Národní centrum kybernetické bezpečnosti a Národní centrum bezpečnějšího internetu. V případě represe je zásadní hlavně činnost policejních složek. Zde můžeme sledovat neustálou snahu o profesionalizaci aparátu Policie ČR, která posiluje své řady o odborníky z oblasti IT, tak aby její činnost byla co nejefektivnější, což hodnotím jednoznačně jako přínosné a žádoucí.

Poslední kapitola je věnovaná vybraným způsobům jak chtěly jiné státy kybernetickou kriminalitu řešit. Rozebrala jsem zde na příkladu Německa problematiku postihu šíření dětské pornografie a na příkladu Francie zase postih za porušování autorských práv na Internetu. Zatímco v Německu prosazovali jako řešení přímou blokaci internetových stránek se závadným obsahem, ve Francii měli v úmyslu uživatele Internetu v případě porušení autorského práva za určitých podmínek rovnou odpojit. Oba dva státy ale musely nakonec od takto razantních řešení ustoupit a to v zásadě proto, že se to neslučuje s právem na přístup k Internetu, které je dle OSN jedním z lidských práv.

SEZNAM ZKRATEK

ICT- Informační a komunikační technologie[201]

IT- Informační technologie

PC- Osobní počítač[202]

TČ- Trestný čin

MV- Ministerstvo vnitra

ZKB- Zákon o kybernetické bezpečnosti

TZ- Trestní zákoník

AZ- Autorský zákon

ZTOPO- Zákon o odpovědnosti právnických osob

P2P- Peer-to-peer

[201] Z anglického "Information and Communication Technologies"
[202] Z anglického "Personal computer"

SEZNAM POUŽITÝCH PRAMENŮ

KNIŽNÍ PUBLIKACE

BRENNER, Susan W. *Cybercrime and the Law: Challenges, Issues, and Outcomes*. Boston: University Press of New England, 2012, 263 s. ISBN 1555537995.

CLOUGH, Jonathan. *Principles of cybercrime*. New York: Cambridge University Press, 2010, 449 s. ISBN 0521728126.

ECKERTOVÁ, Lenka, DOČEKAL Daniel. *Bezpečnost dětí na internetu: rádce zodpovědného rodiče*. Brno: Computer Press, 2013, 224 s. ISBN 978-80-251-3804-5.

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

GŘIVNA, Tomáš, SCHEINOST Miroslav, ZOUBKOVÁ Ivana. *Kriminologie*. 4., aktualiz. vyd. Praha: Wolters Kluwer, 2014, 536 s. ISBN 978-80-7478-614-3.

JIRÁSEK, Petr, NOVÁK Luděk, POŽÁR Josef. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze, 2013, 200 s. ISBN 978-80-7251-397-0.

JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007, 284 s. ISBN 978-80-247-1561-2.

KUCHTA, Josef, VÁLKOVÁ Helena. a kol. *Základy kriminologie a trestní politiky*. Praha: C.H. Beck, 2005, 546 s. ISBN 80-7179-813-4.

MAISNER, Martin, VLACHOVÁ Barbora. *Zákon o kybernetické bezpečnosti: komentář*. Praha: Wolters Kluwer, 2015, 232 s. ISBN 978-80-7478-817-8.

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

MOORE, Robert. *Cybercrime: investigating high-technology computer crime*. 2nd ed. Amsterdam: Elsevier, 2011, 318 s., Anderson publishing. ISBN 978-1-4377-5582-4.

MUSIL, Stanislav. *Počítačová kriminalita: nástin problematiky : kompendium názorů specialistů*. Praha: Institut pro kriminologii a sociální prevenci, 2000, 281 s. ISBN 80-86008-80-0.

POŽÁR, Josef. *Základy teorie informační bezpečnosti*. 1. vyd. Praha: Vydavatelství PA ČR, 2007, 219 s. ISBN 978-80-7251-250-8.

SMEJKAL, Vladimír. *Internet a §§§*. Praha: Grada, 2001, 284 s. ISBN 80-247-00581.

SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. ISBN 978-80-7380-501-2.

ŠÁMAL, Pavel. *Trestní zákoník: komentář*. 2. vyd. Praha: C.H. Beck, 2012. 3614 s. ISBN 978-80-7400-428-5.

WALDEN, Ian. *Computer crimes and digital investigations*. Oxford: Oxford University Press, 2007, 491 s. ISBN 978-0-19-929098-7.

WALL, David S. *Cybercrime: the transformation of crime in the information age*. Cambridge, UK: Polity, 2008, 276 s. ISBN 9780745627366.

YAR, Majid. *Cybercrime and society: crime and punishment in the information age*. Thousand Oaks, CA: SAGE Publications, 2006, 185 s. ISBN 1412907543.

ODBORNÉ ČASOPISY

TAUCOVÁ, Zuzana. Kyberkriminalita a další kyberhrozby, *Policista*. 2015, č. 1

DRMOLA, Jakub. Konceptualizace kyberterorismu. *Vojenské rozhledy*. 2013, č. 2

HERCZEG, Jiří, GŘIVNA, Tomáš. Právo na přístup k Internetu, blokace stránek a digitální gilotina, *Trestněprávní revue*. 2009, č. 5

MYŠKA, Matěj. Odkaz není zločin? Embedding, užití díla a trestný čin porušování autorského práva, *Revue pro právo a technologie*. 2013, č. 7

JUDIKATURA

Usnesení Nejvyššího soudu ze dne 25. 3.2009, sp. zn. 5 Tdo 234/2009

Usnesení Nejvyššího soudu ze dne 27. 2. 2013 sp. zn. 8 Tdo 137/2013

KVALIFIKAČNÍ PRÁCE

KRUPIČKA, Jiří. *Trestněprávní a kriminologické aspekty internetové kriminality.* Praha 2012. Disertační práce. Univerzita Karlova, Právnická fakulta. Vedoucí práce prof. JUDr. Jiří Jelínek, CSc.

ZEMAN, Daniel. *Internetová kriminalita*. Praha 2012. Rigorózní práce. Univerzita Karlova, Právnická fakulta. Vedoucí práce doc. JUDr. Tomáš Gřivna, Ph.D.

ČIKOVSKÝ, Jan. *Internetová a počítačová kriminalita.* Praha 2013. Diplomová práce. Univerzita Karlova, Právnická fakulta. Vedoucí práce doc. JUDr. Tomáš Gřivna, Ph.D.

ELEKTRONICKÉ ZDROJE

http://www.mvcr.cz/clanek/statistiky-kriminality-dokumenty.aspx
http://www.oxforddictionaries.com/us/definition/american_english/cyberspace
http://www.businessit.cz/cz/kyberneticka-kriminalita-i-co-se-deje-v-kyberprostoru.php
http://www.oxforddictionaries.com/definition/english/hacker
https://us.norton.com/cyber-security-insights#expander-content-e4709169d1ad49c49183a3b7038cddc7
https://www.eff.org/cyberspace-independence
http://byznys.ihned.cz/c1-63309180-cina-zablokovala-gmail-jde-o-dalsi-cenzuru-tvrdi-organizace-greatfire
http://www.coe.int/cs/web/conventions/full-list/-/conventions/treaty/185/signatures
https://securelist.com/analysis/publications/36138/keyloggers-how-they-work-and-how-to-detect-them-part-1/
http://www.webopedia.com/TERM/S/spear_phishing.html
https://www.microsoft.com/en-us/security/online-privacy/phishing-symptoms.aspx
http://us.norton.com/cybercrime-pharming
https://napoveda.active24.cz/idx.php/0/308/article/
https://usa.kaspersky.com/internet-security-center/threats/computer-viruses-vs-worms#.VwZ18MffRbU
https://usa.kaspersky.com/internet-security-center/threats/trojans#.VwbamMffRbU
http://www.webopedia.com/DidYouKnow/Internet/virus.asp
http://www.webopedia.com/TERM/D/DoS_attack.html
http://www.patria.cz/zpravodajstvi/2282801/dalsi-utok-hackeru-v-cr-tercem-internetove-bankovnictvi-velkych-bank-cnb-i-web-burzy.html
http://www.policie.cz/clanek/prevence-informace-o-extremismu-co-je-extremismus.aspx
http://www.lidovky.cz/konvicka-je-obzalovan-kvuli-podnecovani-k-nenavisti-a-hrozi-mu-vezeni-1e0-/zpravy-domov.aspx?c=A160408_105356_ln_domov_ele
http://www.ceskaskola.cz/2009/05/kamil-kopecky-kybergrooming-aneb-kdo.html
http://www.hoax.cz/hoax/co-je-to-hoax
http://www.lupa.cz/clanky/policie-resi-hoax-o-imigrantech-na-facebooku-jako-sireni-poplasne-zpravy/
http://www.forbes.com/sites/realspin/2014/03/25/insider-trading-on-the-dark-web/#308876893d3b
http://www.upv.cz/cs/prumyslova-prava.html

http://finance.idnes.cz/podvodny-e-shop-u-slona-0v1-/viteze.aspx?c=A131209_110502_viteze_sov
http://www.policie.cz/clanek/pozor-na-zneuziti-platebni-karty.aspx
http://www.penize.cz/platebni-karty/18567-platebni-karty-jaka-zneuziti-cihaji-a-jak-se-jim-branit
http://www.pravniprostor.cz/clanky/trestni-pravo/kyberneticka-kriminalita-fenomen-dneska
http://www.stoppiratstvi.cz/cs/o-piratstvi/co-je-piratstvi.shtml
http://www.lupa.cz/clanky/je-stahovani-piratskeho-obsahu-z-webu-legalni/
http://finance.idnes.cz/odpovednost-provozovatelu-internetovych-ulozist-fxr-/pravo.aspx?c=A130509_233027_pravo_vr
http://www.lupa.cz/clanky/peer-to-peer-site-od-a-do-z-bittorrent-a-edonkey/#ic=serial-box&icc=text-title
http://docplayer.cz/3912001-Kyberneticka-kriminalita-v-judikature-ceskych-soudu-doc-judr-tomas-grivna-ph-d-pravnicka-fakulta-uk-v-praze.html
http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/763AE1D4853A3985C1257B5C004F46EE?openDocument&Highlight=0,
http://zpravy.idnes.cz/internet-bude-hlidat-nova-pocitacova-policie-fnf-/domaci.aspx?c=A160513_214736_domaci_fka
http://www.lemonde.fr/technologies/article/2009/09/15/que-contient-hadopi-2_1240913_651865.html
http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/2009/decisions-par-date/2009/2009-580-dc/decision-n-2009-580-dc-du-10-juin-2009.42666.html
http://essays.ssrc.org/10yearsafter911/whither-cyber-terror/
http://news.bbc.co.uk/2/hi/europe/6665145.stm
http://www.spiegel.de/international/germany/family-minister-vs-freedom-of-speech-anti-child-pornography-law-flounders-a-627447.html
http://www.theinquirer.net/inquirer/news/1356941/german-parliament-passes-internet-censorship
https://opennet.net/blog/2009/06/germany-passes-legislation-block-child-pornography
http://www.spiegel.de/international/germany/the-law-that-nobody-wanted-new-internet-legislation-embarrasses-german-government-a-678782.html
http://www.dw.com/en/bundestag-looks-to-delete-child-pornography-websites/a-15575254
http://www.lepoint.fr/actualites-societe/2008-11-02/telechargement-illegal-que-dit-la-nouvelle-loi-hadopi/1597/0/288089

http://www.agoravox.fr/actualites/technologies/article/hadopi-pour-les-nuls-explications-54212
http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-

Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001,

- https://cs.wikipedia.org/wiki/Internet
- https://cs.wikipedia.org/wiki/World_Wide_Web
- https://en.wikipedia.org/wiki/Generation_Z
- https://en.wikipedia.org/wiki/Hacker_(computer_security)
- https://cs.wikipedia.org/wiki/Cenzura_na_internetu
- https://en.wikipedia.org/wiki/Phishing
- https://cs.wikipedia.org/wiki/Spyware
- https://cs.wikipedia.org/wiki/Anna_Halman
- https://cs.wikipedia.org/wiki/Peer-to-peer
- https://cs.wikipedia.org/wiki/BitTorrent
- https://cs.wikipedia.org/wiki/Warez
- https://en.wikipedia.org/wiki/Zugangserschwerungsgesetz
- https://fr.wikipedia.org/wiki/Loi_favorisant_la_diffusion_et_la_protection_de_la_création_sur_internet

ABSTRAKT

Cílem této diplomové práce je seznámit čtenáře s problematikou kybernetické kriminality, fenoménem, který v posledních letech nabývá na významu.

V úvodní kapitole je nastíněn základní problém, a sice že masově užívané informační a komunikační technologie mohou mít i svou stinnou stránku.

Následně se čtenář v krátkosti dozví o vývoji počítačů, který měl za následek vznik Internetu. Zejména pak to, jaký tato krátká evoluce měla vliv na terminologii, pokud se týká kriminality související s informačními technologiemi. Zásadní je pak v tomto ohledu pojem "kyberprostor", od kterého odvozujeme termín "kybernetická kriminalita". Tento virtuální svět je totiž místem pro zábavu, ale bohužel i pro škodlivé jednání.

Dále se práce zabývá i specifiky kybernetické kriminality. Zvláštnostmi, které ji odlišují od ostatních druhů trestné činnosti.

Pátá kapitola se zabývá právní regulací, a to jak vnitrostátní tak mezinárodní. Nalezneme zde výčet zásadních právních předpisů, které se ke kybernetické kriminalitě vztahují. Zejména je zde věnován prostor rozboru trestního zákoníku, zákonu o kybernetické bezpečnosti a Úmluvě o kybernetické kriminalitě.

Následuje hlavní kapitola celé práce zabývající se kriminalitou v kyberprostoru. Zde je uveden popis těch nejčastějších škodlivých aktivit, k nimž v kyberprostoru dochází. Pro přehlednost celé věci je v úvodu přiložena tabulka napomáhající orientaci. Zvláštní pozornost je pak věnována autorskému právu, jehož porušování na Internetu je momentálně nejčastějším projevem kybernetické kriminality.

Sedmá kapitola rozebírá dva nezbytné elementy kybernetické kriminality a tím jsou oběť a pachatel. Zde je vysvětleno, proč není možné ani jednoho z nich jasně charakterizovat.

Dále je čtenář seznámen se současným stavem kybernetické kriminality. A také s tím, jaká jsou preventivní a represivní opatření.

Poslední kapitola se pak věnuje tomu, jak řeší vybrané druhy kyberkriminality jiné státy. Na příkladu Německa a Francie je poukázáno na neúspěšné snahy o regulaci škodlivých aktivit na Internetu.

ABSTRACT

The purpose of this thesis is to introduce the issue of cyber crime, a phenomenon which is gaining importance in recent years.

The first chapter outlines the basic problem: Mass use of information and communications technologies may have downsides.

Consequently, the reader learns briefly about development of computers, which resulted in the emergence of the Internet. Especially, how this short evolution affected the terminology regarding crimes related to information technology. The term "cyberspace", from which we derive the term "cyber crime", becomes crucial. This virtual world is not only a place of fun but unfortunately also full of malicious behavior.

Further, the work deals with the specifics of cybercrime and its differences that distinguish it from other types of crime.

The fifth chapter deals with the legal regulation, both domestic and international. It lists major legislation related to the cyber crime and is especially dedicated to analysis of the Criminal Code, the law on cyber security and the Convention on Cybercrime.

Next comes the main section of the thesis dedicated to crime in cyberspace. It describes the most common malicious activities which occur in cyberspace. A table of individual crimes is included to ease orientation. Particular attention is paid to copyright violations on the Internet which are currently the most common type of cyber crime.

The seventh chapter discusses two essential elements of a cyber crime, the offender and the victim. It is explained here why it is impossible for either of them to be clearly described.

Furthermore, the reader will become familiar with the current state of cybercrime and also with the latest preventive and repressive measures.

The last chapter is devoted to foreign legislation, where, using the example of Germany and France, unsuccessful efforts to control harmful Internet activities are explained.

KLÍČOVÁ SLOVA

KLÍČOVÁ SLOVA

Kybernetická kriminalita/ Kyberprostor/ Kriminologie

KEY WORDS

Cybercrime/ Cyberspace/ Criminology