Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra práva

Bakalářská práce

Právní úprava kybernetické kriminality v ČR

Veronika Srbová

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Veronika Srbová

Veřejná správa a regionální rozvoj

Název práce

Právní úprava kybernetické kriminality v ČR

Název anglicky

The legal regulation of cybercrime in Czech Republic

Cíle práce

- Rešerše základních pojmů kybernetické kriminality, analýza vybraných druhů kybernetické kriminality a postupu při jejím vyšetřování
- Analýza platné právní úpravy oblasti trestné činnosti páchané proti informačním a komunikačním technologiím a objasnění cest vedoucích k prevenci kybernetické kriminality
- Návrh na zlepšení platné právní úpravy se zvláštním zřetelem ke kybernetické šikaně
- Analýza konkrétního případu kybernetické kriminality a zjištění povědomí žáků na základní škole o kybernetické kriminalitě

Metodika

Bakalářská práce bude rozdělena na část teoretickou a část praktickou. V teoretické části bude použita zejména rešerše literatury, metoda deskripce k vysvětlení základních pojmů kybernetické kriminality a metoda analytická, která bude použita u vybraných ustanovení platných právních předpisů upravujících kybernetickou kriminalitu v ČR.

V praktické části bude na základě poznatků a zjištění dosažených analýzou v teoretické části vypracován návrh na zlepšení platné právní úpravy. Dále bude provedeno dotazníkové šetření o vědomí žáků na základní škole o kybernetické kriminalitě. V praktické části bude též využito případové studie konkrétního případu kybernetické kriminality a budou uskutečněny řízené rozhovory s pachatelem a obětí kybernetické kriminality.

Doporučený rozsah práce

30-40

Klíčová slova

kriminalita, kybernetická kriminalita, šikana, kybernetická šikana, trestná činnost, počítač, oběť, pachatel, právní úprava, prevence

---

Doporučené zdroje informací

ECKERTOVÁ, Lenka a Daniel DOČEKAL. Bezpečnost dětí na internetu: rádce zodpovědného rodiče. 1. vyd. Brno: Computer Press, 2013, 224 s. ISBN 978-80-251-3804-5.

GŘIVNA, Tomáš; POLČÁK, Radim. Kyberkriminalita a právo, nakladatelství Auditorium, Praha 2008 (první vydání), ISBN 978-80-903786-7-4

HULANOVÁ, Lenka. Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality. Praha: Triton, 2012, 217 s. ISBN 978-80-7387-545-9.

JANSA Lukáš, OTEVŘEL Petr, ČERMÁK Jiří, MALIŠ Petr, HOSTAŠ Petr, MATĚJKA Michal a MATEJKA Ján. Internetové právo. 1. vydání. Brno: Computer Press, 2016, 432 s. ISBN 978-80-251-4664-4

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

KOLÁŘ Michal, Nová cesta k léčbě šikany, Vyd. 1. – Praha: Portál, 2011. -336 s. ISBN 978-80-7367871-5

KRČMÁŘOVÁ, Barbora. Děti a online rizika: sborník studií. Praha: Sdružení Linka bezpečí, 2012, 178 s. ISBN 978-80-904920-2-8

MATĚJKA, M.: Počítačová kriminalita. Praha : Vydavatelství a nakladatelství Computer Press, 2002, ISBN: 80–7226–419–2

SMEJKAL Vladimír, Kybernetická kriminalita, nakladatelství Aleš Čeněk, s.r.o., Plzeň 2015, ISBN 978-80-7380-501-2

WALDEN, Ian. Computer Crimes and Digital Investigations, Oxford University Press, New York 2007 ISBN-13: 978-0198705598

Předběžný termín obhajoby

2019/20 ZS – PEF (únor 2020)

Vedoucí práce

JUDr. Jitka Mráčková, CSc.

Garantující pracoviště

Katedra práva

Elektronicky schváleno dne 27. 11. 2017

JUDr. Jana Borská, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 28. 11. 2017

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 25. 11. 2019

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Právní úprava kybernetické kriminality v ČR" jsem vypracovala samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autorka uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušila autorská práva třetích osob.

V Praze dne 26.11.2019 _____

Poděkování

Ráda bych touto cestou poděkovala JUDr. Jitce Mráčkové, CSc. za vedení a odborné rady při zpracování bakalářské práce. Připomínky, kterých se mi dostalo, byly pro vypracování bakalářské práce nejcennější. Dále děkuji všem, kteří mě během práce podporovali.

Právní úprava kybernetické kriminality v ČR

Abstrakt

Bakalářská práce rozdělená na teoretickou a praktickou část se zabývá kybernetickou kriminalitou a její právní úpravou v České republice. Objasňuje problematiku kybernetické kriminality, historií vzniku a její rozšíření. Dále jsou v práci rozebrány vybrané druhy kybernetické kriminality a její účastníci. Pozornost je věnována právní úpravě kybernetické kriminality v české legislativě, zejména se zřetelem na trestní zákoník. Práce obsahuje také formy objasňování kybernetické kriminality a její prevenci. Součástí práce je návrh na zlepšení platné právní úpravy v oblasti kybernetické kriminality. Dále je v bakalářské práci provedeno dotazníkové šetření o povědomí kybernetické kriminality na 2. stupni základní školy, šetření případovou studií a řízené rozhovory s pachatelem a obětí kybernetické kriminality.

Klíčová slova: kriminalita, kybernetická kriminalita, šikana, kybernetická šikana, trestná činnost, počítač, oběť, pachatel, právní úprava, prevence

The legal regulation of cybercrime in the Czech Republic

Abstract

Bachelor thesis is dividend into the toretical and practical part deals with cybercrime and its legal regulation in the Czech Republic. It explains the issue of cybercrime, its history and its spread. Furthermoreis in the thesis analyzes selected types of cybercrime and its participants. Attention is paid to the legal regulation of cybercrime in the Czech legislation, especially with regard to the Criminal Code. The work also contains forms of clarification of cybercrime and its prevention. Part of the work is a proposal to improve the current legislation in the field of cyber crime. Furthermore, the thesis is conducted a questionnaire survey on awareness of cyber crime at the high school, a case study and controlled interviewswiththeoffender and thevictim of cyber crime.

Keywords: crime, cybercrime, bullying, cyberbullying, criminalactivity, computer, victim, offender, legislation, prevention

Obsah

Seznam obrázků

Seznam tabulek

Seznam grafů

1 Úvod

Žijeme v době, kdy je střet s informačními technologiemi každodenní součástí života. Tak, jako bylo 19. století nazývané stoletím páry by se dalo 21. století nazvat jako století digitalizace. Na přelomu 20. a 21. století se informační technologie masově rozšířily, už nebylo výjimkou, že domácnost vlastnila počítač nebo mobilní telefon. Pokrok umožnil dostupnost těchto zařízení větší sortě uživatelů. Dnes už je vývoj informačních technologií na takové úrovni, kdy je prakticky nemožné se jim vyhnout. Mnozí mohou namítat, že pokud nevlastní mobilní telefon nebo počítač, nejsou součástí této digitalizace, avšak pomocí informačních technologií dnes funguje drtivá většina úřadů, společností a služeb, se kterými přijdeme denně do styku. Veškeré databáze se transformují do digitální podoby, ať už se jedná o klientelu v bankách, občanské a cestovní průkazy, nabídky bydlení nebo například e-shopy.

Globální rozmach informačních a komunikačních technologií spolu s sebou však nese i negativní stránku, kterou je kybernetická kriminalita. Jedná se o protiprávní jednání ve virtuálním světě, který svými možnostmi anonymity a volnosti vyjadřování vytváří prostor pro páchání kybernetických trestných činů.

Účelem této bakalářské práce je analyzovat problematiku kybernetické kriminality a poukázat na její úskalí. Na začátku práce je vysvětlen pojem kybernetická kriminalita, její rozdělení a vysvětlení pojmů, které jsou důležité k pochopení virtuálního světa a kriminality v něm. Dále je práce zaměřena na historii a rozšíření kybernetické kriminality. Ačkoli je označována jako relativně nový pojem, její počátky lze najít už na konci 60. let minulého století.

V další části práce jsou vysvětleny některé pojmy kybernetické kriminality. Je to nebezpečný fenomén zejména proto, že si mnoho lidí spojí kybernetickou kriminalitu s páchání trestné činnosti zaměřené proti osobám, ale už ne s o nic méně nebezpečnou kriminalitou páchanou proti počítačovým systémům. Nechrání si dostatečně informace uložené na svém nosiči dat a často ani nevědí, že se stali obětí kybernetické kriminality. Dále je v práci rozebrána platná právní úprava, zejména se zřetelem na trestní zákoník č. 40/2009 Sb. Závěrem práce jsou uvedeny cesty prevence a návrhy na zlepšení právní úpravy v oblasti kybernetické kriminality.

2 Cíl práce a metodika

2.1 Cíl práce

Tématem bakalářské práce je kybernetická kriminalita se zřetelem na její právní úpravu v ČR. Práce je rozdělena na teoretickou a praktickou část.

Hlavní cílem práce je analyzovat platnou právní úpravu v oblasti trestné činnosti páchané s využitím informačních a komunikačních technologií, zejména v zákoně č. 40/2009 Sb., trestní zákoník a zákoně č. 181/2004 Sb., o kybernetické bezpečnosti. Dalším cílem bakalářské práce je navrhnout zlepšení platné právní úpravy se zřetelem ke kybernetické šikaně a analýza konkrétního případu kybernetické kriminality.

Dílčími cíli této práce pro správné pochopení kontextu kybernetické kriminality je objasnění jejího vzniku, rešerše základních pojmů kybernetické kriminality, analýza jejích vybraných druhů kybernetické kriminality a vysvětlení profilu jejich účastníků. Cílem bakalářské práce je také vysvětlit vyšetřování kybernetické kriminality a objasnění cest vedoucích k prevenci kybernetické kriminality.

2.2 Metodika

V rámci teoretické části práce je použita zejména metoda rešerše literatury, metoda srovnávací, metoda deskripce a metoda analytická.

Základním východiskem pro rešerši literatury jsou publikace týkající se této problematiky uvedené v závěru práce. Na základě rešerše a srovnávání těchto publikací jsou vyhodnoceny závěry k jednotlivým kapitolám teoretické části, zejména u vysvětlení pojmu kybernetická kriminalita, jejího rozdělení a vzniku

Metoda deskripce byla použita na vysvětlení pojmu kyberprostor, vybraných druhů kybernetické kriminality, vysvětlení pojmu pachatel a oběť kybernetické kriminality a zejména na objasňování a vyšetřování kybernetických trestných činů.

Dále je v teoretické části využita analýza platných právních předpisů a jejich vybraných ustanovení, které upravují kybernetickou kriminalitu v České republice. V práci je analýza zaměřena zejména na právní úpravu a jednotlivá ustanovení trestního zákoníku a na právní úpravu a jednotlivá ustanovení zákona o kybernetické bezpečnosti, ve kterých je ukotvena základní právní úprava pro kybernetickou kriminalitu.

V praktické části je použita metoda srovnávací, dotazníkové šetření, případová studie a řízený rozhovor.

Na základě syntézy teoretických východisek, znalostí a poznatků získaných z analýzy právních předpisů je vypracován návrh na zlepšení právní úpravy. V praktické části je s využitím dotazníkového šetření zjišťováno u žáků 2. stupně základní školy jejich povědomí o kybernetické kriminalitě, její prevenci a způsobu, jak takové jednání řešit.

Součástí práce jsou i případová studie konkrétního případu kybernetické kriminality a řízený rozhovor s pachatelem a obětí trestné činnosti z oblasti kybernetické kriminality.

3 Teoretická část

3.1 Kybernetická kriminalita

3.1.1 Úvod do problematiky

Jakkoli lze informační a komunikační technologie vnímat jako přínosné, nelze opomíjet jejich možné zneužití. Tento druh kriminality se v současném prostředí stále označuje jako nový, a to z toho důvodu, že tato společensky škodlivá jednání nelze ve většině případů zařadit pod současné skutkové podstaty trestných činů.[1] Z toho následně vychází novelizace stávajících právních předpisů, popřípadě přijímání předpisů nových.

Problematika kybernetické kriminality je rovněž upravena mezinárodními smlouvami a legislativou Evropské unie.[2]

Kybernetická kriminalita, rovněž označována jako kriminalita informačních technologií za účelem zkrácení často využívá pojem kybernalita. V médiích a zahraničních pramenech se v tomto ohledu lze rovněž setkat s anglickými ekvivalenty původního pojmu – cybercrime, IT crime nebo v neposlední řadě také computercrime. Jednoznačně definovaný obsah pojmu kybernetická kriminalita bychom však hledali marně. Odborná veřejnost totiž v tomto ohledu přináší celou řadu odlišných pojetí.

V nejširším pojetí je počítačová kriminalita „*trestná činnost, v níž figuruje určitým způsobem počítač jakou souhrn technického a programového vybavení (včetně dat), nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět této trestné činnosti (s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité), nebo jako nástroj trestné činnosti*.“[3]Problém této definice však spočívá v tom, že si pod ním lze představit téměř veškerou trestnou činnost, k jejímu vykonání byl potřeba počítač, přestože zde hrál minimální roli a nelze proto hovořit o kybernetickém zločinu.

O kybernetické kriminalitě můžeme v nejširším pojetí mluvit jako o činnosti páchané proti informačním a komunikačním technologiím, nebo o činnosti páchané s využitím informačních a komunikačních technologií. Lepší využitelnost této definice

[1] Viz ustanovení § 13 Trestního zákoníku „*Trestným činem je protiprávní čin, který trestní zákon označuje za trestný a který vykazuje znaky uvedené v takovém zákoně.“*
[2] Jedna z nejdůležitějších je Úmluva o počítačové kriminalitě (Budapešť, 23. listopadu 2001)
[3]JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007s. 271

spočívá v tom, že o kybernetické kriminalitě uvažuje v souvislosti s existencí a permanentním využíváním internetové sítě.

Ani toto rozdělení se však nemusí jevit jako zcela vhodné, jelikož velké množství jednání může spadat do obou kategorií najednou.

3.1.2 Trestná činnost páchaná proti informačním a komunikačním technologiím

Kybernetickou kriminalitu páchanou proti počítačům lze označit jako druh kriminality, kde je počítač, nebo jeho hardware[4], software[5], data sítě atd. přímo terčem útoku. Dochází zde k narušení systému spuštěním neoprávněného software za účelem například krádeže dat, špionáže, bankovního podvodu, zneužití osobních údajů apod.[6] Do této kategorie lze zařadit i hacking a spamming, které jsou zmíněny v pozdější části práce.

3.1.3 Trestná činnost páchaná s využitím informačních a komunikačních technologií

Druhá kategorie kybernetické kriminality se pak označuje jako druh kriminality, v níž vystupuje počítač jako nástroj pro páchání trestného činu, případně počítačová síť a k ní připojená zařízení, která se tak stávají prostředím, v níž se tato trestná činnost odehrává. Sem lze zařadit například problematiku phisingu a pharmingu, problematiku dětské pornografie či cyberstalking, které jsou rovněž zmíněny v pozdější části práce.

3.2 Kyberprostor

Abychom mohli dále objasňovat pojem kybernetická kriminalita, je důležité definovat pojem kyberprostor.

Podle zákona č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů je dle § 2 písm. a) „*kybernetickým prostorem digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.*“[7]

---

[4] Vše v počítači, na co si můžeme sáhnout. Jsou to tedy veškeré části počítače, které jsou potřebné pro jeho fungování. Hardware může být například grafická karta, paměť RAM, pevný disk nebo základní deska. [online] IT SLOVNÍK.cz [cit. 2018-03-7] Dostupné z.https://it-slovnik.cz/pojem/hardware

[5] Programové vybavení počítače – tedy programy a aplikace v počítači. [online] IT SLOVNÍK.cz [cit. 2018-03-7] Dostupné z.https://it-slovnik.cz/pojem/software

[6] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015., s.20

[7] MAISNER, Martin, VLACHOVÁ, Barbora. Zákon o kybernetické bezpečnosti: komentář. Praha: Wolters Kluwer, a. s. 2015. s.63

Pojem kyberprostor se dostal do povědomí díky knize Williama Gibsona „Neuromancer“.[8]Výkladů kyberprostoru ale je ale možné najít mnohonásobně víc a neexistuje jasná a přesná definice, na které by se všichni bez rozdílu shodli.

Dle mého laického názoru lze kyberprostor vysvětlit jako nekončící realitu, která ovšem nemá hmotnou podstatu a proto na ní nelze praktikovat stejná pravidla, jako fungují ve světě reálném.

3.3 Historie kybernetické kriminality

Je otázkou, od kdy mluvit o trestných činech jako o činech kybernetické kriminality. V takovém pojetí, v jakém známe kybernetickou kriminalitu dnes, je jedním z nejstarších příkladů případ Johna Drapera na přelomu 60. a 70. let 19. století.[9] Tento muž objevil přístroj s názvem blue-box, který umožňoval telefonovat zdarma. Tím oklamával telefonní síť AT&T, která byla tehdy jedinou telefonní sítí v USA. O největší rozmach kybernetické kriminality se však zasloužila 80. léta a technologie BBS.[10] Z toho pramenil vznik prvních hackerských spolků.

Největší kybernetickou událostí konce 80. let 20. století byl podvod na Národní banku v Chicagu, kdy se stala obětí počítačového útoku spáchaného dosud neznámých pachatelem a přišla tak o velké množství peněz.

Nelze se však na hackery dívat pouze negativně. Mnozí z těchto lidí se stali doslova hvězdami v oblasti ICT. Zdárným příkladem je v tomto směru Bill Gates, který založil společnost Microsoft[11] a je rovněž jedním z nejbohatších lidí na světě. Tento muž byl za dob svých studií na Harvardské univerzitě známy pro svůj zájem o počítače a hackerské schopnosti, kterých využíval v prostorách univerzity.

---

[8] "*Konsensuální halucinace každý den zakoušená miliardami oprávněných operátorů všech národů, dětmi, které se učí základy matematiky… Grafická reprezentace dat abstrahovaných z bank všech počítačů lidského systému. Nedomyslitelná komplexnost. Linie světla seřazené v neprostoru mysli, shluky a souhvězdí dat. Jako světla města ..*"JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007s. 17

[9] PTÁČEK, David. Problematika počítačové kriminality. Praha, 2010. Bakalářská práce. Bankovní institut vysoká škola Praha, Katedra práva, 2018 [online] is.ambis.cz [cit.2018-03-07] Dostupné z.https://is.ambis.cz/th/b9j7y/Problematika_pocitacove_kriminality..pdf?so=nx

[10] Počítače, ze kterých mohl uživatel standardizovanými dotazy získávat informace z databáze uložené v počítači

[11] „zabývá se výrobou, vývojem, licencováním a podporou široké škály produktů a služeb, které jsou spjaty především s počítači“ [online] wikipedia.org [cit.2018-03-07]Dostupné z. https://cs.wikipedia.org/wiki/Microsoft

Vzhledem k tématu práce se však jeví jako vhodné pozastavit se u vývoje kybernetické kriminality i v této zemi. V České republice se jedná o poměrně nový obor, neboť kvůli komunistickému režimu u nás byly počítače veřejně nedostupné až do konce 80. let. Přesto bychom však první počítačový zločin našli již na konci 70. let20. století. Za první čin provedený pomocí výpočetní techniky byl odsouzen pracovník[12] Úřadu důchodového zabezpečení, který cíleně znehodnotil data na magnetických páskách. Výsledkem bylo jeho odsouzení k více než 10 letům vězení podle Části druhé hlavy prvé tehdejšího trestního zákona[13].

O největší technologický rozvoj v České republice a potažmo i prostor pro rozvoj kybernetické kriminality se zasadily dva důležité milníky. Prvním bylo otevření hranic po roce 1989 pro zahraniční trh a tím druhým byl rok 1992, kdy došlo k připojení tehdejší ČSFR k internetu.[14]

3.3.1 **Rozšíření kybernetické kriminality**

Rozšíření kybernetické kriminality do podoby, v jakém je známá dnes, bylo následkem dvou důležitých technologických pokroků. Prvním z nich bylo masivní rozšíření osobních počítačů mezi spotřebitele, už nebylo výjimkou, že běžná domácnost vlastnila počítač. Tím druhým mezníkem byl vznik počítačových sítí a možnost vzdáleného přístupu. Vytvořily se tak zcela nové možnosti pro páchání trestných činů, které však v kyberprostoru nabyly úplně nových rozměrů.[15]

Přelom 20. a 21. století se dá současně považovat i za jakýsi přelom mezi různými formami kybernetické kriminality.[16] Dříve většina trestného jednání zahrnovala útoky na počítačové systémy a telefonní sítě, podvody a neoprávněné používání osobních údajů. Dnes se kybernetická kriminalita posunula už do státní sféry a infrastruktury, kdy

[12] Podle neověřených informací byl tento pracovník souzen za sabotáž.
[13] „Zde byly uvedeny tzv. trestné činy proti zakladatelům republiky, které byly postrachem pro každého občana tehdejšího socialistického státu, neboť byly – zejména v 50.letech, ale i později – rozsáhle zneužívány pro postih odpůrců tehdejšího režimu. Tato právní kvalifikace byla nicméně spíše projevem totalitního státu než reálnou právní kvalifikací jednání.“SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, s 73
[14] K oficiálnímu připojení k internetu došlo 13. února 1992 na pražském ČVUT. Šlo o jednu mezinárodní linku Praha – Linz.
[15]SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2.vyd.Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015., s 103
[16] DIBLÍKOVÁ, Simona. Analýza trendů kriminality v České republice v roce 2015. In: *Institut pro kriminologii a sociální prevenci* [online]. 2016 [cit. 2018-10-15]. Dostupné z: http://www.ok.cz/iksp/docs/437

pachatelé pomocí informačních a komunikačních technologií mohou útočit na bankovní instituce, energetické systémy, dopravu nebo na obranné systémy jiných zemí.[17]

3.4 Vybrané druhy kybernetické kriminality

3.4.1 Cyberstalking

Pojem cyberstalking je složení slov „cyber“ a „stalking“. Pojem stalking[18] byl poprvé použit v 90. letech v USA[19] a rychle se zafixoval jako pojem odborné literatury.[20]Jednoduše lze stalking vysvětlit jako promyšlené, dlouhodobé a opakované[21] pronásledování. Pachatel se zaměří na svou oběť, kterou pronásleduje, vyhrožuje jí a vyvolává v ní pocit strachu. Není výjimkou, že by toto obtěžování mohlo skončit i fyzickým násilím nebo smrtí oběti.

Cyberstalking je potom specifický druh stalkingu, kdy stalker obtěžuje svou oběť pomocí informačních a komunikačních technologií. Tento druh stalkingu můžeme rozdělit na 2 části:

1. Přímý cyberstalking – stalker pronásleduje svou oběť neustálými telefonáty, SMS zprávami, e-maily nebo například nevyžádanými komentáři na sociálních sítích.[22] Takový útočník často používá ke kontaktování své oběti hned několik falešných internetových profilů nebo telefonních čísel.

2. Nepřímý cyberstalking – stalker vyhrožuje oběti prostřednictvím internetu – zveřejňováním negativních zpráv[23], krádeži dat nebo vyvěšení falešného inzerátu se sexuálním podtextem. V případě takového inzerátu může zveřejnit

[17]SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2.vyd.Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015., s 103

[18]Viz § 354 z. č. 40/2009 Sb., trestního zákoníku

[19]MELOY Reid J. STALKING (OBSESSIONAL FOLLOWING): A REVIEW OF SOME PRELIMINARY STUDIES.[online].[cit.15.10.2018]. Dostupné z: http://forensis.org/PDF/published/1996_StalkingObsessi.pdf

[20] Zejména literatura psychologická a psychiatrická.

[21] Opakovaným pronásledováním se podle ministerstva vnitra rozumí 4 – 6 týdnů a více než 10 pokusů o kontakt.

[22]*„Za vytrvalý kontakt prostředky elektronické komunikace je považováno zejména opakované zasílání e-mailových zpráv (často s vulgárním nebo agresivním obsahem), zahlcování elektronické pošty spamy, záměrná distribuce počítačových virů, opakované vzkazy, nevyžádané volání jak na mobilní telefon, tak na pevnou linku, textové zprávy, tradiční písemné formy komunikace, jakými jsou dopisy, pohlednice, lístky apod.“* SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015., s.280

[23] Takové zprávy mohou poškodit pověst oběti (např. soukromý nebo pracovní život)

i osobní informace oběti, jako je telefonní číslo nebo adresa a ta je potom obtěžována nevyžádanými nabídkami potencionálních zájemců.[24]

Žijeme v době, kdy díky sociálním sítím může kdokoli komentovat cokoli a je jednoduché prostřednictvím internetu někomu ublížit. Aby se jednalo o trestný čin pronásledování, musí cyberstalker splňovat určité podmínky:

1. Kdo jiného pronásleduje tím, že:

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

    b) vyhledává jeho osobní blízkost nebo jej sleduje,

    c) vytrvale jej prostřednictvím prostředků elektronických komunikací, písemně nebo jinak kontaktuje, omezuje jej v jeho obvyklém způsobu života

    d) zneužije jeho osobních údajů za účelem získání osobního nebo jiného kontaktu, a toto jednání je způsobilé vzbudit v něm důvodnou obavu o jeho život nebo zdraví nebo o život a zdraví osob jemu blízkých, bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti.[25]

Podrobnější rozbor těchto podmínek provedl Nejvyšší soud ČR.[26]

Proti cyberstalkingu je třeba se bránit. V první řadě je důležité si hlídat svá osobní data, dbát na doporučení sociálních sítí a nezveřejňovat na nich fotky nebo informace, kterých by mohl někdo zneužít.

3.4.2 **Hacking**

Hacking je jednou z nejvýznamnějších činností kybernetické kriminality. V odborné literatuře je hacking vysvětlován jako přístup do systému jinou než legální cestou.[27] Novináři si tuto definici zjednodušují a označují hacking jako činnost, která spočívá ve vyhledávání bezpečnostních děr v počítačových systémech a jejich využívání.

[24]Cyberstalking. In: *Epravo.cz*[online]. 2013 .[cit.2018-01-15]. Dostupné z: https://www.epravo.cz/top/clanky/cyberstalking-91552.html

[25] Viz § 354 Trestního zákoníku „Nebezpečné pronásledování“

[26] Usnesení Nejvyššího soudu ČR, sp. Zn. 8Tdo 1082/2011 ze dne 8.9.2011. Dále pak také usnesení Nejvyššího soudu ČR, sp. Zn. Tdo 1378/2011 ze dne 11.11.2011

[27]*„proniknutí do počítačového nebo řídícího systému, jinou než standardní cestou při obejití nebo prolomení jeho bezpečnostní ochrany“*JIROVSKÝ, Václav. Kybernetická kriminalita, nejen o hackingu, crackingu, virech a trojských koních bez tajemnství. Praha: Vydavatelství Grada Publishing, a. s., 2007. s. 102

Na čem se však oba principy shodnou je fakt, že motivace hackerů nemusí být finanční, jde také o reputaci, zábavu a překonávání výzev.

Hacking má opravdu dlouhou historii, jejíž počátky začínají ještě dlouho předtím, než počítače začaly být vůbec populární. Nejranější forma hackingu využívala telefonů a byla označována jako phreaking a váže se k období 70. let 20. století. Phreaking[28] je kriminální činnost, při které phreaker využívá neoprávněně telefonní linku bez její úhrady zaměstnavateli.[29]

Právní úprava hackingu se jeví jako velice obtížná. Zásahem do počítačového systému zcela jistě dochází k porušení základních lidských práv a svobod – zejména článek 7 odst.1[30]a článek 13 Listiny.[31] Pokud pachatel překoná bezpečnostní opatření systému, a získá tak neoprávněný přístup k počítači nebo k jeho části, bude souzen podle § 230 odst. 1 Trestního zákona.[32] V tomto případě závisí naplnění skutkové podstaty faktu, že pachatel jednal v úmyslu získat neoprávněný prospěch, nikoli na tom, zda byl trestný čin dokonán.

Pokud bychom chtěli provést hrubou klasifikaci hackerů, poslouží nám tzv. kloboukové dělení[33], na jehož základě jsou hackeři členěni na:[34]

- whitehats - tito hackeři uznávají hackerskou etiku a často pracují ve firmách zaměřených na bezpečnost systémů. Provádějí útoky, které se sice podobají těm, kterými jsou napadány systémy, ale tyto útoky jsou prováděny na žádost majitele, kdy je cílem najít bezpečnostní chyby v systému.
- blackhats - činnost těchto hackerů se podobá útokům, které provádí skupina první, avšak s tím rozdílem, že jejich cílem je systém napadnout a díky

[28] z anglického freak = ztřeštěnec a phone = telefon

[29] „*phreaking přináší phreakerovi řadu velkých výhod a kromě volání zadarmo či spíše na účet nebohé oběti, mohou být technikou phreakingu odposlouchávány cizí telefonní hovory, což může vést k efektivnímu získání jistého druhu citlivých a osobních informací.*“ sprava-site.eu. *Phreaking* [online].[cit.15.10.2018]. Dostupné z: https://www.sprava-site.eu/phreaking/

[30] „*Nedotknutelnost osoby a jejího soukromí zaručena. Omezena může být jen v případech stanovených zákonem.“*

[31] „*Nikdo nesmí porušit listovní tajenství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon. Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením“*

[32] Viz § 230 Trestního zákoníku *„ Neoprávněný přístup k počítačovému systému a nosiči informací“*

[33] Klasifikace je odvozena od klobouků, které měli hlavní hrdinové ve westernech. Zatímco kladný hrdina míval tradičně bílý nebo světlý klobouk, záporný hrdina se vyznačoval tmavou (obyčejně černou) barvou klobouku.

[34] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007 s. 54-55

prolomení ochranných prvků se snaží získat určité výhody pro sebe nebo pro svého zaměstnavatele. Zařadili bychom sem i hackery, kteří slouží průmyslové špionáži mezi velkými konkurenty.

- greyhats – ti jsou jakýmsi průnikem mezi oběma výše zmíněnými skupinami, Obvykle se jedná a začínající hackery, kteří si ještě nejsou jisti svým budoucím úkolem.

K lepšímu pochopení toho, jak hackeři vnímají společnost, nám poslouží Levyho principy hackerské etiky:

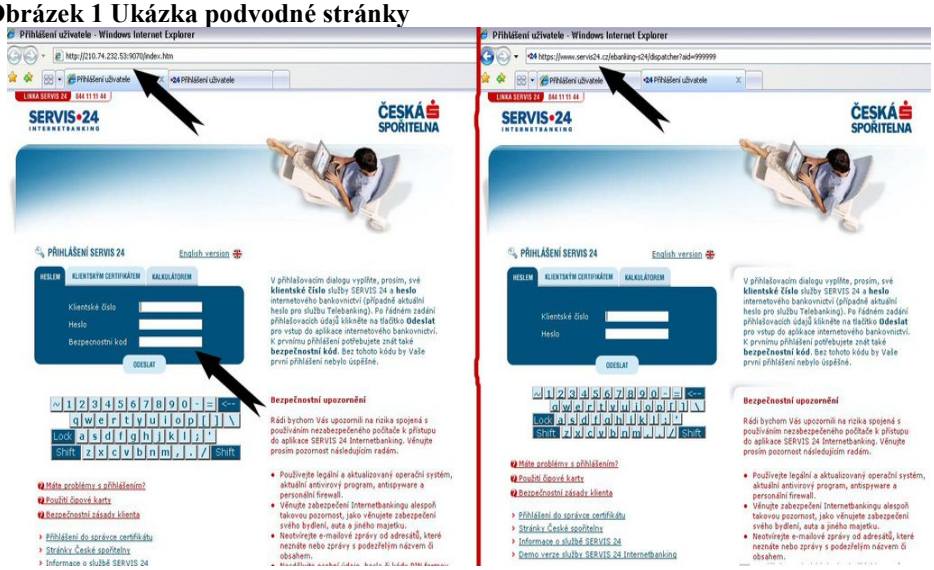
1. Přístup k počítači a čemukoliv dalšímu, co tě může naučit o tom, jak svět funguje, by měl být neomezený a absolutní. Vždy respektuj pravidlo osobní zkušenosti.
2. Veškeré informace by měly být bezplatné,
3. Nevěř autoritám, podporuj decentralizaci.
4. Hackeři by měli být souzeni podle svých činů a nikoliv podle scestných kritérií jako jsou věk, rasa a pohlaví.
5. Na počítači můžeš vytvářet krásu.
6. Počítače mohou změnit tvůj život k lepšímu.[35]

3.4.3 **Phising**

Phisingem[36] lze nazvat nelegální činnost, kdy pachatel podvodně získává citlivé informace o jiných osobách, jakou jsou čísla kreditních karet, přístupová hesla či e-mailové adresy. V tomto kontextu dochází k rozesílání e-mailů, které na první pohled vypadají jako žádosti zaslané bankami, nebo jinými institucemi, za účelem získání identifikačních údajů klientů. Na první pohled tyto stránky nevypadají nijak škodlivě a od originálu se skoro neliší (viz Obrázek 1). Oběti jsou ale ve skutečnosti přesměrovány na falešné stránky a jimi dále zadávané údaje jsou zasílány rovnou pachateli.[37] Oběti oklamané tímto trestným jednáním poskytnou své identifikační údaje a výsledkem následně může být kupříkladu vykradení bankovního účtu.

[35] LEVY, Steven. Hackers: Heroes of the ComputerRevolution Sebastopol, CA: O'Reilly, edia, s. 32-41
[36] Česky někdy označováno jako „rybaření".
[37] JAMES, Lance. Phishing bez záhad. 1. vyd. Praha: Grada, 2007, s. 281

Obrázek 1 Ukázka podvodné stránky



Zdroj : notebook.cz [online].[cit. 15. 10. 2018]. Dostupné z: https://notebook.cz/clanky/kratke-zpravy/2006/061011-Servis24-phishing

Odhalení pachatelů je ale velmi složité, neboť při páchání phisingu používají tzv. spoofing, který má za následek skrytí identity počítače.[38]

Trestní jednání phisingu v ČR je možné postihnout trestným činem podvodu dle § 209 Trestního zákoníku, pokud dojde k majetkové škodě. Jestliže pachatel při svém jednání pronikne do systému nebo zneužije data, bude souzen dle § 230 Trestního zákoníku.[39]Dále pak phising v některých případech může naplňovat znaky skutkové podstaty trestného činu dle § 234 Trestního zákoníku.[40]

3.4.4 Pharming

Pharming[41] je nebezpečnější a škodlivější forma výše uvedeného phisingu. Motivem jednání pachatele je získání důležitých osobních a identifikačních informací od oběti. Principem tohoto jevu je napadení DNS[42], v důsledku čehož je klient zpravidla přesměrován na stránky internetového bankovnictví.

Trestněprávní úprava u tohoto druhu jednání je obdobná jako u výše zmiňovaného phisingu.

---

[38] „*dochází k využití počítačů a identity (e-mailu) nic netušících osob*“JANSA, L., OTEVŘEL, P., ČERMÁK, J., MALIŠ, P., HOSTAŠ, P., MATĚJKA, M., MATEJKA, J., Internetové právo, Brno: Computer Press, 2016. s. 395

[39] viz § 230 Trestního zákoníku „ Neoprávněný přístup k počítačovému systému a nosiči informací“

[40] viz § 234 Trestního zákoníku „ Neoprávněné opatření, padělání a pozměnění platebního prostředku“

[41] Jedná se o kombinaci slov farming (farmaření, hospodaření) a phreaking.

[42] DNS je databáze, které obsahuje systém internetových doména příslušných adres – slouží tedy k převodu doménových adres na IP adresy.

3.4.5 **Šíření dětské pornografie**

Šíření dětské[43] pornografie se stalo postupně díky rozvoji internetu poměrně hodně rozšířenou nelegální aktivitou. Toto prostředí totiž skýtá ideální podmínky pro získávání i další šíření těchto záležitostí.[44]Šíření dětské pornografie se stalo celosvětovým problémem[45] a je o to závažnější zejména proto, že děti obvykle neví, jak se bránit. Současný trestní zákoník ve svých ustanoveních obsahuje závazky vyplývající z mezinárodních smluv a práva EU.[46]

Zda se jedná o dětskou pornografii nezávisí podle zákona[47]na tom, jakém pocity dílo (např. fotografie) přináší osobám se sexuální deviací. Tím se odliší pornografický materiál například od fotek dětí pořízených rodiči z dovolené apod. To ale neznamená, že šíření takových fotografií na sociálních sítích nebo sdílených webech[48] nemůže potencionálního útočníka přilákat a lidé by tak měli při vkládání souborů dbát základních pravidel.[49]

Z hlediska českého trestního práva je otázka šíření pornografie řešena v § 191 až §193 trestního zákoníku. Jedná se o trestné činy šíření pornografie, výroby a jiného nakládání s dětskou pornografií a zneužití dítěte k výrobě pornografie:

- § 191 TZ 40/2009 –„*Šíření pornografie"* - trestní zákoník uvádí jednotlivé podoby nabízení závadné pornografie a stanovuje předpoklady pro to, aby se toto šíření stalo trestným dle českého trestního práva.
- § 192 TZ 40/2009 – „*Výroba a jiné nakládání s dětskou pornografií*" – dle tohoto paragrafu se považuje za trestné také přechovávání dětské pornografie

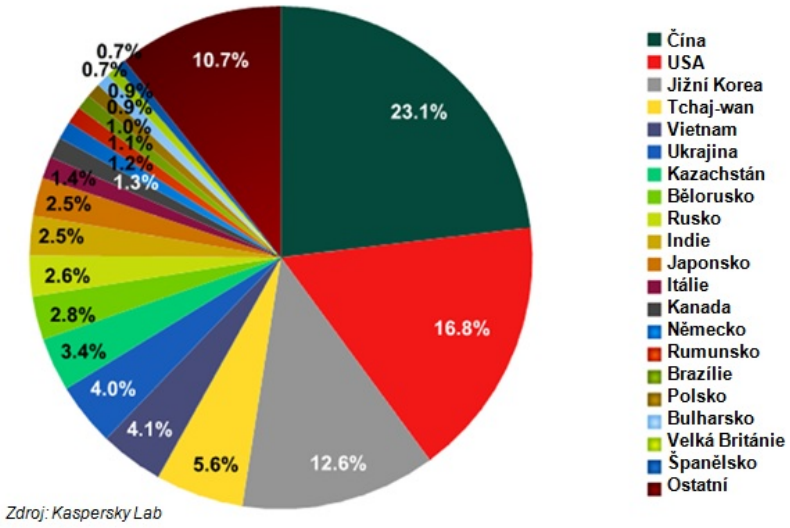
[43] Dítětem se rozumí osoba mladší 18 let vz § 126 a § 192 odst. 1 a 3 Trestního zákoníku.
[44] Nutno však podotknout, že zneužívání dětí k pornografickým účelům bylo značně rozšířeno již před vznikem internetu, který ovšem otevřel zcela nové možnosti k nelegálnímu šíření těchto materiálů.
[45]*„k jejímuž stíhání se zavázala většina států světa, bez ohledu na to, zda ratifikovala či neratifikovala Úmluvu o kyberkriminalitě"*KOLOUCH, Jan. Cybercrime. Praha: CZ. NIC, z. s. p. o., 2016., s. 305
[46] Jedná se zejména o úmluvu o Ochraně dětí před sexuálním vykořisťováním a zneužíváním a Úmluvu o kybernetické kriminalitě.
[47] Dle rozhodnutí Nejvyššího soudu ČR ze dne 12.2.2012, sp. zn. 8 Tdo 1002/2012: „*Aby mohlo být nějaké dílo zobrazující dítě podle trestního zákoníku považováno za pornografické, je třeba, aby kumulativně splňovalo dvě základní charakteristiky: musí jednak u normálního jedince vyvolávat aktualizaci sexuálního pudu a za druhé překračovat uznávané morální normy příslušné společnosti, a tedy u většiny jejích členů vzbuzovat stud."*
[48] Tím může být například portál www.rajce.net určený ke sdílení fotografií.
[49] např. základní pravidla serveru www.rajce.net, který uvádí:„*Obsah zobrazující nahé osoby, zejména mladší 18 let, je na Rajče povoleno umisťovat pouze do soukromých alb s heslem, ostatní ustanovení těchto pravidel, zejména zákaz umisťovat na Rajče pornografický obsah nebo obsah neoprávněně zasahující do práva na ochranu osobnosti třetích osob, zůstává i v takovém případě nedotčena*."

- § 193 TZ 40/2009 – „*Zneužití dítěte k výrobě pornografie*“–tento paragraf považuje za trestné i účast na pornografickém nebo obdobném vystoupení, ve kterém účinkují děti.[50]

3.4.6 Spamming

Vznik spammingu jde ruku v ruce se vznikem elektronické pošty, kdy pachatelé[51] získávají nejrůznějšími způsoby e-mailové adresy (diskuzní fóra, SMS, sociální sítě atd.), na které jsou potom spamy zasílány. Spamem se v užším slova smyslu rozumí zasílání nevyžádané, reklamně laděné elektronické pošty. V širším pojetí se potom jedná o všechny nevyžádané zprávy zahrnující i trojské koně, viry apod.[52]

Obrázek 2 Rozdělení spamů podle zemí původu.



Zdroj: Itbiz.cz [online].[cit. 15. 10. 2018]. Dostupné z: https://www.itbiz.cz/zpravicky/spamu-opet-pribyva

Charakteristickým znakem spamu je hromadný a podbízivý charakter a hlavně jeho nevyžádanost adresátem. Jeho obdržení může elektronickou komunikaci omezit nebo zcela znemožnit, neboť může dojít k jejímu přehlcení a celkově má negativní vliv na infrastrukturu sítě.

Společně s rozšiřováním spammingu vzniká i celá řada programů, která dokáže tyto spamy filtrovat, ale není však žádným překvapením, že se pachatelé dokážou tomuto pokroku přizpůsobit a hledají cesty, jak ochranné programy obejít. Prevencí proti spamům může být i chování uživatelů, kteří nebudou zveřejňovat své e-mailové adresy na

[50] Zákon 40/2009 Sb., Trestní zákoník, Tiskárna Ministerstva vnitra, částka 11, 2009
[51] V této souvislosti označováni také pojmem „spammeři“.
[52] KOLOUCH, Jan. Cybercrime. Praha: CZ. NIC, z. s. p. o., 2016., s. 231

neověřených serverech a pokud nějaký spam obdrží, nebudou ho otevírat ani na něj odpovídat.

Pokud se nyní opět zaměříme na problematiku právního postihu tohoto druhu kybernetické kriminality, lze konstatovat, že samotný sparing podle českého práva patrně postižitelný není. Jednou z prvních směrnic, která se zabývá problematikou spamu je Evropská směrnice č. **2000/31/ES** o elektronickém obchodu, která označuje spam jako obchodní sdělení. Další směrnicí upravující problematiku sparingu je směrnice Evropského parlamentu a Rady č. **2002/58/ES**o soukromí a elektronické komunikaci. Tato směrnice se zabývá ochranou osob proti nedovolenému vniknutí do jejich soukromého života pomocí elektronických služeb.

V ČR tuto problematiku v souladu s výše uvedenými směrnicemi upravuje zákon č. 480/ 2004 Sb.[53], ve kterém jsou podmínky upravující zasílání a přenos obchodních sdělení. Pokud bude možno z adresy dostatečným způsobem identifikovat příjemce spamu, mohla by za určitých okolností být naplněna skutková podstata podle § 180 trestního zákoníku.[54]

[53] viz zákon č. 480/2004 Sb.“*Zákon o některých službách informační společnosti“*
[54] viz § 180 trestního zákoníku „*Neoprávněné nakládání s osobními údaji*“

3.5 Šikana

V tato část práce bude věnována šikaně, znakům šikany a jejímu rozdělení na tradiční a kybernetickou, jelikož je to velice závažný problém a pro pochopení jedné části šikany je důležité vysvětlit i část druhou. Zároveň bude tato část zaměřena i na jejich porovnání, neboť vždy není jasné, do které části šikana spadá a jaké bude naplnění její skutkové podstaty.

3.5.1 Tradiční šikana

Tradiční šikana v reálném (offline) světě je chování, jehož cílem je ublížit, zesměšnit, ponížit nebo ohrozit oběť ať už fyzicky, nebo psychicky.

Je důležité vysvětlit, co šikana zahrnuje a umět rozpoznat její znaky, které nám pomohou posoudit, zda se jedná o šikanu, nebo pouze a popichování, které nemá ani pro jednu stranu negativní dopady.

Upřesnění těchto znaků lze najít na stránkách Policie ČR, kde uvádějí, že šikana je:

- *„jakékoliv chování, jehož záměrem je opakovaně ubližovat, ohrožovat nebo zastrašovat jiného člověka, případně skupinu lidí,*
- *zahrnuje jak fyzický útok v podobě bití, poškozování věcí druhé osobě, tak i útok slovní v podobě vydírání, nadávek, pomluv, vyhrožování či ponižování,*
- *většina případů šikany mezi dětmi se odehrává ve škole, na cestě do školy nebo ze školy, případně v okolí bydliště,*
- *nebezpečí šikany spočívá především v závažnosti, dlouhodobém působení a s tím souvisejících následcích v oblasti duševního a fyzického zdraví“*[55]

Pro lepší a praktičtější vysvětlení šikany nám může posloužit tzv. trojdimenzionální mapa, podle které můžeme šikanu a její projevy členit na:

1. přímé a nepřímé
2. fyzické a verbální
3. aktivní a pasivní

Kombinováním těchto tří rozdělení nám vzniká osm druhů šikany (viz Tabulka 1).

[55] [online] policie.cz [cit 25-09-2018] Dostupné z: https://www.policie.cz/clanek/vite-co-je-kybersikana.aspx

Tabulka 1 Mapa vnějších projevů šikany

Fyzické aktivní přímé	*Útočníci oběť věší, škrtí, kopou, fackují.*
Fyzické aktivní nepřímé	*Kápo pošle nohsledy, aby oběť zbili. Oběti jsou ničeny věci.*
Fyzické pasivní přímé	*Agresor nedovolí oběti, aby si sedla do lavice. Fyzické bránění oběti k dosahování jejích cílů.*
Fyzické pasivní nepřímé	*Agresor odmítne oběť na její požádání pustit ze třídy na záchod (odmítnutí splnění požadavků)*
Verbální aktivní přímé	*Nadávání, urážení, zesměšňování.*
Verbální aktivní nepřímé	*Rozšiřování pomluv. Patří sem i tzv. symbolická agrese, která může být vyjádřena v kresbách, básních apod.*
Verbální pasivní přímé	*Neodpovídání na pozdrav, otázky apod.*
Verbální pasivní nepřímé	*Spolužáci se nezastanou oběti, je-li nespravedlivě obviněna z něčeho, co udělali její trýznitelé.*

[56]

3.5.2 **Kybernetická šikana**

Kybernetická šikana[57] převádí tradiční šikanu do online podoby. Je to v podstatě forma psychické šikany a jedná se o opakovanou záměrnou činnost využívající informační a komunikační technologie, kdy hlavním cílem tohoto jednání je způsobit psychickou újmu či jinak poškodit oběť. Tento druh šikany je v mnoha znacích podobný s výše zmiňovaným cyberstalkingem, je však mnohem zákeřnější.

Mezi nejčastější znaky kybernetické šikany patří:

- zasílání výhružných, zesměšňujících nebo urážlivých zpráv přes sociální sítě, SMS, e-mail apod.,
- natáčení videí a zvukových záznamů nebo pořizování fotografií a jejich následné zveřejnění s cílem oběť zesměšnit nebo jinak poškodit,

[56] KOLÁŘ, Michal, Nová cesta k léčbě šikany, Praha: nakladatelství Portál, s. r. o., 2011, s. 37
[57] Termín převzatý z anglického „cyberbully".

- vytváření různých internetových stránek a sociálních profilů, na kterých je oběť zesměšňována a urážena,
- krádeže kybernetické identity – zneužívání e-mailových nebo jiných sociálních účtů
- provokování obětí na diskuzních fórech , např. chatovací místnosti,
- vydírání nebo obtěžovaní pomocí internetu nebo mobilního telefonu[58].

Kybernetická šikana (stejně tak šikana tradiční) není trestným činem nebo přestupkem. Vždy se to odvíjí od toho, jak útočník jednal. Například vydírání či zastrašování bude klasifikováno podle § 175[59], na pronásledování a obtěžování by přicházel v úvahu § 354[60] a u některých extremistických projevů může být aplikován např. § 356[61] nebo § 355[62].

3.5.3 Srovnání tradiční a kybernetické šikany

Při zaměření na charakteristiky, které mají oba druhy šikany společné, je nevyvratitelné, že v obou případech se jedná o vztahy mezi lidmi. Obě formy šikany jsou nesporně zraňující a záměrné.

Prvním zásadním a zřejmým rozdílem, který ostatně plyne již ze samotných názvů, je fakt, že zatímco tradiční šikana probíhá tváří v tvář, šikana kybernetická využívá k tomuto účelu informační a komunikační technologie. V tomto ohledu je kybernetická šikana psychicky o to náročnější, neboť může trvat 24 hodin denně a nekončí tím, že oběť uteče před svým útočníkem. Ani v případě, že se oběť útokům brání (například útočníka zablokuje), není výsledek zaručen, jelikož online prostředí oproti reálnému světu skýtá různé možnosti, jak si oběť znovu vyhledat.[63]

Dalším podstatným rozdílem mezi tradiční a kybernetickou šikanou je anonymita. Zatím co při tradiční šikaně je útočník známý, často fyzicky i verbálně zdatnější než oběť, kybernetická šikana nabízí útočníkovi prostor, kde může skrýt svou identitu a schovat se tak za anonymitu internetu. S kyberprostorem je spojena i jakási možnost předstírat falešnou identitu. Anonymita internetu zkrátka snižuje odpovědnost jedince za své činy.

[58] [online] policie.cz [cit 25-09-2018] Dostupné z: https://www.policie.cz/clanek/vite-co-je-kybersikana.aspx
[59] viz ustanovení § 175 Trestního zákoníku „ *vydírání“*
[60] viz ustanovení § 354 Trestního zákoníku „ *nebezpečné pronásledování“*
[61] viz ustanovení § 356 Trestního zákoníku „ *podněcování k nenávisti vůči skupině osob nebo omezování jejich práv a svobod“*
[62] viz ustanovení § 355 Trestního zákoníku „ *hanobení národa, rasy, etnické nebo jiné skupiny osob“*
[63] KOLÁŘ, Michal, Nová cesta k léčbě šikany, Praha: nakladatelství Portál, s. r. o., 2011, s. 86

Neopomenutelná je také síla publika. Při tradiční šikaně jsou svědci pouze útočníci popřípadě přihlížející tomuto jednání, kdežto u kybernetické šikany může mít přístup k zesměšňujícím stránkám každý, kdo má internet.

Offline agresor pracuje s fyzickou a obyčejně i sociální převahou, kdežto v kyberprostoru si vystačí se znalostí informačních technologií.

Jak už bylo výše zmíněno, tradiční ani kybernetická kriminalita nejsou trestným činem. Z důvodu ochrany osobních práv a svobod a svobody projevu je aplikace trestněprávních ustanovení v takovém případě obzvlášť obtížná. Přesto si však myslím, že s ohledem na dnešní dobu by bylo vhodné toto jednání právně upravit a to jak u dospělých, tak u nezletilých osob. Agresivita mezi dětmi stálé stoupá a považuji za nezbytné, aby za takové jednání nesly následky.

3.6 Účastníci kybernetického zločinu

Lze říci, že ať už je umělá inteligence jakkoliv rozvinutá, vždy je bezesporu potřeba ke spáchání kybernetického zločinu dvou aktérů. Fenomén internetu a informačně komunikačních technologií s sebou neodmyslitelně přináší i otázku, kdo je obětí a pachatelem kybernetické kriminality a také co je jejich motivem.

Faktem zůstává, že z právního pohledu je vztah oběť a pachatel nerovná dvojice. Legislativa je zaměřena zejména na práva pachatele. Existují sice hlavní zásady pro jednání policistů s obětí, ale dle mého názoru je tato úprava s ohledem na oběť nedostatečná a bylo by vhodné ji upravit.

3.6.1 **Pachatel**

Pachatelem kybernetické kriminality se stává ten, kdo spáchal trestný čin, tedy kdo svým jednáním naplnil znaky skutkové podstaty trestného činu podle § 22.[64]

Dalo by se říci, že pachateli trestné činnosti budou z větší části osoby nižších věkových kategorií, jelikož vyrůstali v době největšího rozvoje informačních a komunikačních technologií, zatímco osoby starší generace se museli tomuto fenoménu přizpůsobit.

Dle kriminologické klasifikace lze trestný čin kybernetické kriminality označit jako trestný čin tzv. bílých límečků, tedy lidí s určitou technickou znalostí, výše postavené a

[64] viz ustanovení § 22 odst.1 Trestního zákoníku „*Pachatelem trestného činu je, kdo svým jednáním naplnil znaky skutkové podstaty trestného činu nebo jeho pokusu či přípravy, je-li trestná.*

s vysokou důvěryhodností. To ovšem není zcela ideální označení, protože v dnešní době už je kybernetická kriminalita tak rozšířená, že se jejím pachatelem může stát kdokoli, kdo jen trochu ovládá informační a komunikační technologie.

Typologii pachatelů můžeme rozdělit do 6 skupin:

1. První skupina jsou zaměstnanci. Mnohdy si nikdo ani neuvědomuje riziko toho, že zaměstnanci mají dostatečné možnosti a přístup k informacím a mohou s nimi dále operovat.
2. Druhou skupinou jsou hackeři. Jejich trestná činnost zahrnuje průniky do softwarových programů, zavirování sítí apod.
3. Třetí skupinou rozumíme organizovaný zločin. Spadá sem zejména výroba různých druhů padělků, šíření pornografie nebo praní špinavých peněz.
4. Do čtvrté kategorie můžeme zařadit profesionály, kteří tuto činnost provádí na něčí popud – zpravidla jde o osoby najaté ozbrojenými silami nebo výzvědnou službou.
5. Pátá kategorie potom zahrnuje kyberteroristy – jedná se o teroristické útoky, které probíhají v kyberprostoru.
6. Šestou a poslední skupinou se v tomto ohledu rozumí osoby neznalé práva, které nad svým jednáním příliš neuvažují a často je ani nenapadne, že by mohli jednat v rozporu s právem.[65]

Dle mého názoru by do této typologie měla patřit ještě skupina sedmá a to pachatelé kybernetické šikany, cyberstalkingu, spammingu a podobně, které nejsou ve stávajících šesti skupinách přímo zahrnuty.

Odhalování pachatele je v kybernetické kriminalitě velice složité, protože kyberprostor skýtá možnost anonymity a je nezbytné ztotožnit pachatele s prostředkem páchání trestného činu.[66]

3.6.2 **Oběť**

Obětí kybernetického zločinu se stává osoba, proti které byla trestná činnost namířena. V dnešní době se jí tak může stát každý, kdo využívá informační a komunikační technologie a nezáleží na tom, zda je to právnická osoba, fyzická osoba nebo stát. Podle

[65] SMEJKAL, Vladimír. *Kybernetická kriminalita.* 2. vyd. Plzeň: Aleš Čeněk, 2018 s 689
[66] Počítač, IP adresa apod.

některých studií bylo kybernetických zločinem postihnuto až 65% uživatelů internetu po celém světě.[67]

Faktem ale zůstává, že tento druh kriminality je nejméně ohlašovanou trestnou činností. U některých druhů kybernetické kriminality se může stát, že oběť o svém napadení ani neví. Dalším faktorem, proč oběti své napadení nenahlašují je, že se bojí o narušení soukromí dat uchovávaných na jejich nosiči dat nebo odhalení nelegálního obsahu na jejich počítači.[68]To ale může podněcovat pachatele k dalšímu páchání této trestné činnosti.

Podle Ministerstva vnitra České republiky přináší rozšiřující se digitalizace soukromé i veřejné sféry v kyberprostoru i vyšší intenzitu útoků. Roste počet útoků na informační systémy, e-mailové či bankovní účty i dalších případů kybernetické kriminality. Ministerstvo v této souvislosti uvádí, že tento trend se bude rozšiřovat i v budoucnosti, a to i včetně hrozby kybernetické špionáže.

V prostředí kyberprostoru je velmi aktivní také mládež, a to již od velmi raného věku. Například v souvislosti se sociální sítí Facebook je možná aktivita na něm až od 12 let, ale i děti v mladším věku si vytvářejí profily nebo se na síti pohybují přes účet starších sourozenců apod. S tím je spojena vysoká míra důvěřivosti v online prostředí, bez uvědomění si rizik, která jsou s tím spojena. Rozšiřujícím se problémem v České republice stoupající počet obětí trestných jednání páchaným prostřednictvím sociálních sítí, což souvisí s životním stylem dnešní mládeže a jejich přílišnou otevřeností, důvěřivostí a sdělováním informací neznámým osobám bez domýšlení následků.[69]

Nejenom děti jsou však pro pachatele kybernetických zločinů vhodnou cílovou skupinou. I přílišná důvěra a otevřenost starších lidí ve virtuálním světě se stává stále větším problémem, který se projevuje mimo jiné ve stále častějším citovém vydírání seniorů přes internet. Jelikož má stále větší počet seniorů přístup k internetu, případy, ve kterých vystupují senioři v roli oběti podvodů, každoročně narůstají.[70]

---

[67] ZEMAN, Daniel. *Internetová kriminalita*. Praha, 2012. Rigorózní práce. Univerzita Karlova v Praze, Katedra trestního práva, Právnická fakulta [online] is.cuni.cz [cit.2018-03-07] Dostupné z.https://is.cuni.cz/webapps/zzp/detail/124482/

[68] „*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 snižovalo důvěru veřejnosti*“ GŘIVNA, Tomáš, POLČÁK, Radim. *Kyberkriminalita a právo*. Praha. Vydavatelství Auditorium. 2008. s. 36

[69] [online] policie.cz [cit 25-09-2018] Dostupné z: https://www.policie.cz/clanek/vite-co-je-kybersikana.aspx

[70] [online] novinky.cz [cit 25-09-2018] Dostupné z:https://www.novinky.cz/domaci/454447-duverivi-seniori-se-na-internetu-stavaji-koristi-smejdu.html

V každém případě je ale nutné, aby uživatelé informačních a komunikačních technologií kladli důraz na vhodná preventivní opatření, kterými se budu podrobněji zabývat v části 3.9.Hledání cest prevence kybernetické kriminality

3.7 Analýza platné právní úpravy

Následující kapitola je zaměřena úpravu kybernetické kriminality na území České republiky. Úvodem je nezbytné podotknout, že právní úprava v současné době není v rámci legislativy České republiky, dokonce ani v rámci evropské legislativy koncepční. Nyní se společnost nachází spíše v tom stadiu, kdy jsou jednotlivé díry systému postupně „zadělávány". Tato situace je vyvolána více příčinami, k nimž patří velká dynamika kyberprostoru a jeho specifičnost. Není proto divu, že v takto dynamicky se rozvíjejícím prostředím je aplikace právních předpisů více než obtížná.

3.7.1 Úvod do problematiky

Jak již bylo naznačeno, kyberprostor je poměrně novým kriminálním prostředím a rovněž vykazuje řadu specifik, na která je potřeba zvláštní právní úprava. Česká právní úprava v tomto ohledu prošla mnoha změnami v návaznosti na přijetí nového trestního zákoníku. Jedním z faktorů pro úpravu v trestním zákoníku byla Úmluva o kybernetické kriminalitě z roku 2004, kterou Česká republika podepsala a která se stala stěžejním pilířem pro úpravu kybernetické kriminality v trestním zákoníku.[71] Oproti zákonu č. 140/1961 Sb. používá trestní zákoník č. 40/2009 Sb. odpovídající terminologii.[72]

Předpisů, které se dotýkají právní úpravy kybernetické kriminality, je na našem území celá řada. Mezi základní prameny právní úpravy v boji s kybernetickou kriminalitou v českém právním řádu patří:

- zákon č. 40/2009 Sb., Trestní zákoník
- zákon č. 141/1961 Sb., Zákon o trestním řízení soudním (Trestní řád)
- zákon č. 127/2005 Sb., Zákon o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)
- zákon č. 205/2017 Sb., Zákon, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o

[71] BARTŮNĚK, Jan. *Kybernetická kriminalita*. Praha. 2014. Dipolomová práce. Univerzita Karlova v Praze. Právnická fakulta. Katedra trestního práva. s.18
[72] SMEJKAL, Vladimír. Internet a §§§, druhé vydání, Grada Publishing, Praha 2001, s. 14.

kybernetické bezpečnosti, ve znění zákona č. 104/2017 Sb., a některé další zákony

3.7.2 Právní úprava kybernetické kriminality v novém trestním zákoníku

Česká republika dne 1. 1. 2009 přijala nový trestní zákoník č. 40/2009 Sb., který je nástupce trestního zákoníku č. 140/1961 Sb. Na první pohled je jasné, že právní úprava v novém trestním zákoníku je mnohem rozsáhlejší a popisnější, co se týče popisu trestných jednání.

Mezi časté příklady trestných činů týkajících se kybernetické kriminality patří:

§ 175 vydírání – *„Objektem trestného činu je zde svobodné rozhodování člověka v nejširším slova smyslu.“*

§ 180 neoprávněné nakládání s osobními údaji – „*Objektem trestného činu neoprávněného nakládání s osobními údaji podle § 180 je právo na ochranu před neoprávněným zveřejňováním osobních údajů a jejich zneužíváním ,jakož i ochrana dalších práv a oprávněných zájmů, které zveřejněním osobních údajů mohou být poškozeny.“*

§ 181 poškození cizích práv – „*Ustanovením § 181 jsou chráněna jiná než majetková práva jednotlivce, v oblasti vztahů rodinných, pracovních, podnikatelských apod., ale i práva právnických osob (v podnikatelských i jiných vztazích), kolektivních orgánů apod., a také státu.“*

§182 porušení tajemství dopravovaných zpráv – „*Objektem tohoto trestného činu je tajemství dopravovaných zpráv, zaručené čl. 13 LPS. Článek 13 LPS zahrnuje ochranu listovního tajemství i tajemství jiných písemností a záznamů zasílaných poštou nebo jiným způsobem i tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením, s výjimkou případů a způsobem, které stanoví zákon“*

§ 183 porušení tajemství listin a jiných dokumentů uchovávaných v soukromí - „*Objektem tohoto trestného činu je listovní tajemství a tajemství jiných písemností, záznamů a dokumentů uchovávaných v soukromí, zaručené čl. 13 LPS. Článek 13 LPS zahrnuje ochranu listovního tajemství i tajemství jiných písemností a záznamů bez ohledu na to, zda jsou uchovávány v soukromí nebo jsou zasílány poštou nebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon.“*

§ 184 pomluva – *„Ustanovení § 184 poskytuje ochranu cti a dobré pověsti člověka před pomluvou, která může vážným způsobem narušit jeho rodinný a společenský život. Lidská důstojnost, osobní čest a dobrá pověst jsou mravními hodnotami člověka ve společnosti, které požívají ochrany i čl. 10 LPS, podle kterého každý má právo, aby byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a chráněno jeho jméno. Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života.“*

§ 191 šíření pornografie – „*Objektem u trestného činu podle odstavce 1 je zájem na ochraně mravopočestnosti dospělých před útoky (obtěžováním) určitého druhu (tvrdá pornografie). Objektem trestného činu podle odstavce 2 je zájem na ochraně*

mravního rozvoje a výchovy mládeže proti negativnímu působení pornografie. Tímto ustanovením se omezuje právo na svobodu projevu a vyhledávat a šířit informace (čl. 17 LPS, čl. 10 EÚLP).“

§ 192 výroba a jiné nakládání s dětskou pornografií – „*Objektem § 192 je zájem společnosti na ochraně mravního vývoje dětí a ochraně před jejich sexuálním zneužíváním.“*

§ 205 krádež – *„Objektem trestného činu krádeže je především vlastnictví věci, dále i držba věci, ale i jen faktické držení věci. Rozhodující je faktický stav, v rámci kterého má poškozený nebo jiný faktický držitel věc ve své moci (vlastník, nájemce, vypůjčitel, schovatel, dopravce, zástavní věřitel, ale i předchozí zloděj atd.).“*

§ 207 neoprávněné užívání cizí věci – *„Objektem trestného činu neoprávněného užívání cizí věci je především vlastnictví věci, pokud jde o výkon některých oprávnění s vlastnictvím věci spojených. Jde především o oprávnění věc užívat (ius utendi, popř. ius utendi et fruendi) a věc držet (ius possidendi).“*

§209 podvod – *„Objektem trestného činu je tu cizí majetek. Ochrana majetkových práv se poskytuje bez ohledu na druh a formu vlastnictví.“*[73]

3.7.2.1 Ustanovení § 230, § 231 a § 232 trestního zákoníku

Při neoprávněném zásahu do počítačových systémů a dat dochází obvykle k naplnění skutkových podstat trestných činů:

- § 230 Neoprávněný přístup k počítačovému systému a nosiči informací
- § 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat
- § 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti

§ 230 trestního zákoníku – Neoprávněný přístup k počítačovému systému a nosiči informací

(1) Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Kdo získá přístup k počítačovému systému nebo k nosiči informací a

a) neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,

[73] ŠÁMAL, P. a kol. *Trestní zákoník.*1.vydání, Praha: C.H.Beck, 2009

b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými,

c) padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo

d) neoprávněně vloží data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(3) Odnětím svobody na šest měsíců až tři léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 nebo 2

a) v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch, nebo

b) v úmyslu neoprávněně omezit funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat. (4) Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 nebo 2 jako člen organizované skupiny,

b) způsobí-li takovým činem značnou škodu,

c) způsobí-li takovým činem vážnou poruchu v činnosti orgánu státní správy, územní samosprávy, soudu nebo jiného orgánu veřejné moci,

d) získá-li takovým činem pro sebe nebo pro jiného značný prospěch, nebo

e) způsobí-li takovým činem vážnou poruchu v činnosti právnické nebo fyzické osoby, která je podnikatelem.

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

c) způsobí-li činem uvedeným v odstavci 1 nebo 2 škodu velkého rozsahu, nebo

d) získá-li takovým činem pro sebe nebo pro jiného prospěch velkého rozsahu.

Ustanovení § 230 zahrnuje dle trestního zákoníku 2 základní skutkové podstaty:

- V 1 odstavci je chráněna důvěryhodnost počítačových dat a systémů a jejich částí.
- Ve 2 odstavci je ochrana primárně zaměřena na integritu a dostupnost počítačových dat a systémů

Nová právní úprava trestního zákoníku je v souladu se závazky, které vyplývají z Úmluvy o kybernetické kriminalitě a lze ji tak použít při výkladu trestního zákoníku.

Podle Úmluvy o kybernetické kriminalitě v sobě trestný čin podle § 230 zahrnuje jednání rozdělené do 5 odstavců:

1. V prvním odstavci rozděleným na 7 částí je upravován neoprávněný přístup[74] a překonávání bezpečnostních opatření[75] počítačových systémů nebo nosičů informací. V tomto případě není k naplnění skutkové podstaty trestného činu podstatné to, jestli pachatel jednal za účelem získat prospěch nebo způsobit škodu, ale postačí už samotný fakt, že pachatel překonal bezpečností opatření.

2. Druhý odstavec rozdělený na 9 částí je zaměřený na postihy případného dalšího jednání pachatele, který získal přístup k počítačovému systému nebo nosiči informací. K naplnění skutkové podstaty trestného činu zde není podstatné, zda získal pachatel přístup neoprávněně, jako tomu bylo v prvním odstavci. Důležité zde je, že pachatel

   - *„neoprávněně užije uložená data*
   - *neoprávněně vymaže uložená data nebo je jinak zničí, poškodí, změní, potlačí, sníží jejich kvalit, případně je učiní neupotřebitelnými*
   - *padělá nebo pozmění uložená data tak, aby byla považována za pravá*
   - *neoprávněně vloží data do systému.“*[76]

[74] Též označován anglickým pojmem „hacking“ zmiňovaným v části 3.4.2 mé práce.

[75] *„Bezpečnostním opatřením je třeba rozumět každé opatření, jehož cílem je zabránit volnému přístupu k počítačovému systému nebo nosiči informací (např. heslo nebo použití firewallu).“*ŠÁMAL, P. a kol. *Trestní zákoník.*1.vydání, Praha: C.H.Beck, 2009, s.2088

[76] [online] pravniradce.ihned.cz [cit 25-09-2018] Dostupné z:https://pravniradce.ihned.cz/c1-37865090-postih-pocitacove-kriminality-podle-noveho-trestniho-zakona

3. Ve třetím odstavci rozděleným na tři části je kvalitativně postihován úmysl pachatele. Jednou věcí je překonání bezpečnostního opatření systému a druhou je motiv pachatele. Podle tohoto odstavce bude pachatel, který se dopustil některého z výše uvedených trestných činů souzen přísněji, pokud tak jednal s úmyslem získat prospěch nebo způsobit škodu.

4. Odstavec čtvrtý rozdělený na 6 částí je zaměřený na skutkovou podstatu trestných činů uvedených výše, pokud jsou provedeny organizovanou skupinou.[77]

   Mnoho autorů se však shoduje, že právní úprava specifických subjektů je v tomto ohledu mírně rozporuplná, protože podle dané úpravy bude přísněji potrestán pachatel, který způsobí vážnou škodu orgánům veřejné moci, právnické osobě či podnikatelům.[78]

5. V pátém odstavci rozděleným na 3 části je zahrnuto způsobení škody velkého rozsahu, tedy větší než 5 000 000 Kč. [79]

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

> *(1) Kdo v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) nebo trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1, 2 vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává*

[77] *„Organizovanou skupinou se rozumí sdružení více osob, v němž je provedena určitá dělba úkolů mezi jednotlivé členy sdružení a jehož činnost se v důsledku toho vyznačuje plánovitostí a koordinovaností, což zvyšuje pravděpodobnost úspěšného provedení trestného činu, a tím i jeho nebezpečnost pro společnost"*ŠÁMAL, P. a kol. *Trestní zákoník.*1.vydání, Praha: C.H.Beck, 2009, s.2126

[78] „*Nejsme si jisti, zda tato speciální právní úprava obstojí v ústavním testu rovnosti všech před zákonem, protože si lze představit námitky kupříkladu neziskové organizace nebo sportovního klubu, že získání přístupu k jejich počítačovému systému je vnímáno jako méně nebezpečné než získání k přístupu k počítačovému systému vedle sídlícího ševce*" SOKOL, T., SMEJKAL,V., Postih počítačové kriminality podle nového trestního zákona. Právní rádce, XVII., 2009. č.7, s.43

[79] *„: NS 20/2003-T 494. Subjektivní stránka trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 2 písm. a), odst. 3 písm. a) TrZ nespočívá jen v tom, že úmyslným zaviněním pachatele je zahrnuto získání přístupu k nosiči informací a neoprávněné užití takových dat. Subjektivní stránka tohoto trestného činu je širší, protože do ní spadá také to, že pachatel jedná s úmyslem způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch. Objektivně však takový následek nemusí nastat."* Trestní zákoník (EVK), 2009, s. 2097 - 2102

a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části, nebo

b) počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části,

bude potrestán odnětím svobody až na jeden rok, propadnutím věci nebo jiné majetkové hodnoty nebo zákazem činnosti.

(2) Odnětím svobody až na tři léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny, nebo

b) získá-li takovým činem pro sebe nebo pro jiného značný prospěch.

(3) Odnětím svobody na šest měsíců až pět let bude pachatel potrestán, získá-li činem uvedeným v odstavci 1 pro sebe nebo pro jiného prospěch velkého rozsahu.

„Objektem tohoto trestného činu je zájem na ochraně společnosti a osob před možným ohrožením vyplývajícím z nekontrolovaného opatření a přechovávání zařízení, nástrojů a prostředků, jež primárně slouží ke spáchání trestných činů porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) nebo neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1, 2.“[80]

Ustanovení § 231 trestního zákoníku nám říká, že k naplnění skutkové podstaty tohoto trestného činu není důležité jako v případě § 230 prolomit bezpečnostní opatření systému, popřípadě následná manipulace s daty na něm uložených. Trestným činem v tomto případě je i samotné obstarání[81] počítačového hesla nebo nástroje, kterým lze přístup k počítačovému systému získat,[82]kdy pachatel jedná s úmyslem spáchat trestný čin neoprávněného přístupu k počítačovému systému a nosiči dat.

[80] ŠÁMAL, P. a kol. *Trestní zákoník.*1.vydání, Praha: C.H.Beck, 2009, s.2097-2098

[81] *„kdo vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části“*ŠÁMAL, P. a kol. *Trestní zákoník.*1.vydání, Praha: C.H.Beck, 2009, s.2130

[82] *„počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části“*ŠÁMAL, P. a kol. *Trestní zákoník.*1.vydání, Praha: C.H.Beck, 2009, s.2130

Hlavním úmyslem tohoto ustanovení je ochrana majetku se zřetelem na trestní právo, protože nesvědomité zacházení s počítačovými systémy může zapříčinit újmu na majetku.

§ 232 trestního zákoníku – poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti

> *(1) Kdo z hrubé nedbalosti porušením povinnosti vyplývající ze zaměstnání, povolání, postavení nebo funkce nebo uložené podle zákona nebo smluvně převzaté*
>
> *a) data uložená v počítačovém systému nebo na nosiči informací zničí, poškodí, pozmění nebo učiní neupotřebitelnými, nebo*
>
> *b) učiní zásah do technického nebo programového vybavení počítače nebo jiného technického zařízení pro zpracování dat,*
>
> *a tím způsobí na cizím majetku značnou škodu, bude potrestán odnětím svobody až na šest měsíců, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.*
>
> *(2) Odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 škodu velkého rozsahu.*

Tento paragraf byl do trestního zákoníku č. 40/2009 Sb. zařazen nad rámec Úmluvy o kybernetické kriminalitě na žádost poznatků orgánu, které se pohybují v oblasti práva. Některým pachatelům bylo náročné dokázat úmysl, ačkoli jim muselo být jasné, že svými činy způsobí škodu a že jsou si takových následků vědomi.

Objektem tohoto trestného činu je „*ochrana dat a technického či programového vybavení počítače (jiného technického zařízení pro zpracování dat) před nedbalostním poškozovacím jednáním, pokud je těmito zásahy způsobena značná škoda.*“[83]

Zákon se v tomto ustanovení omezuje pouze na hrubou nedbalost[84] a na škody vysokého rozsahu, tedy škody nad částku 500 000 Kč.[85]

[83] ŠÁMAL, P. a kol. *Trestní zákoník.*1.vydání, Praha: C.H.Beck, 2009, s.2136
[84] viz ustanovení § 16 odst. 2 trestního zákoníku „*trestný čin je spáchán z hrubé nedbalosti, jestliže přístup pachatele k požadavku náležité opatrnosti svědčí o zřejmé bezohlednosti pachatele k zájmům chráněným trestním zákonem*“
[85] Dle výkladového ustanovení TZ, § 138 odst 1

3.7.3 **Zákon o kybernetické bezpečnosti**

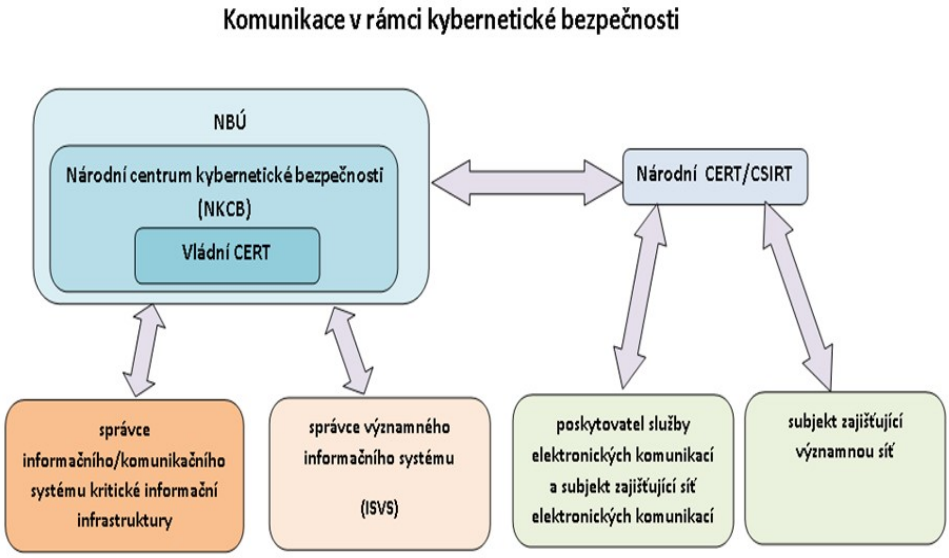
> *(1) Tento zákon upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti.*
>
> *(2) Tento zákon zapracovává příslušné předpisy Evropské unie a upravuje zajišťování bezpečnosti sítí elektronických komunikací a informačních systémů.*
>
> *(3) Tento zákon se nevztahuje na informační nebo komunikační systémy, které nakládají s utajovanými informacemi.*

Národní bezpečnostní úřad připravil v roce 2014 návrh zákona o kybernetické bezpečnosti a o změně souvisejících zákonů. Účinnosti nabyl dne 1.1.2015. Jeho smyslem je zlepšit ochranu proti kybernetickým útokům a to nejen proti útokům zaměřeným na klíčovou infrastrukturu. Tento zákon přináší minimální požadavky na standardní zabezpečení kritické informační struktury a významných informačních systémů. Na jeho základně budou mít vybrané úřady a společnosti[86]povinnost nahlásit kybernetický útok. Tento nahlášený útok bude dále posuzovaný příslušnými institucemi.[87]

[86] Například velké banky nebo energetické podniky.

[87] Dvě dohledové pracoviště - národní a vládní CERT. „*Základním smyslem fungování obou dohledných pracovišť je vyhodnocování informací o výskytu kybernetických bezpečnostních incidentů z pokud možno co největšího množství informačních a komunikačních systémů.*“MAISNER Martin, VLACHOVÁ, Barbora. *Zákon o kybernetické bezpečnosti, Komentář*. Praha, Wolters Kluwer, a. s., 2015. s.49

Obrázek 3Komunikace v rámci kybernetické bezpečnosti



Zdroj: [online] tsoft.cz [cit 25-09-2018] Dostupné z:http://www.tsoft.cz/zakon-o-kyberneticke-bezpecnosti/

Tento zákon byl v roce 2017 novelizován zákonem č. 205/2017 Sb. Hlavní cílem bylo prostřednictvím této novely do české právní úpravy zanést evropskou směrnici **2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.** Změn je nové úpravě zákona celá škála. Mezi nejvýznamnější změny lze zařadit zřízení nového Národního úřadu pro kybernetickou a informační bezpečnost v Brně, který „*je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany*“.[88]nebo rozšíření osobní působnosti.

Národní centrum pro kybernetickou bezpečnost, že zákon je postavený na **dvou zásadách:**

1. minimalizovat zásahy do práv soukromoprávních subjektů
2. větší individuální odpovědnost za ochranu vlastních informačních systémů

a na třech pilířích:

1. zavádění bezpečnostních opatření (prevence)
2. zřízení systému pro hlášení kybernetických bezpečnostních incidentů

[88] [online] nukib.cz [cit 03-10-2018] Dostupné z:https://www.nukib.cz/cs/o-nukib/

3. reakce na kybernetické incidenty – protiopatření.[89]

3.7.3.1 Vybrané pojmy definované zákonem o kybernetické bezpečnosti

Kybernetická bezpečnostní událost[90]– touto událostí rozumíme událost, která může narušit bezpečnost informací, služeb a integrity v informačních systémech a v sítích elektronické komunikace.

Stav kybernetického nebezpečí[91]– jedná se o stav, kdy je ve velkém rozsahu ohrožena bezpečnost informací nebo služeb v informačních systémech a v sítích elektronické komunikace a tím by mohlo dojít k ohrožení zájmu České republiky v souladu se zákonem upravujícím ochranu utajovaných informací.[92]

Opatření[93]- opatřením rozumíme úkony, které mají za úkol zabezpečit ochranu informačních systémů, služeb a sítí elektronické komunikace před kybernetickými hrozbami nebo řešit kybernetické bezpečnostní incidenty. Mezi taková opatření patří:

a) *Varování*[94] – varování vydává úřad[95], pokud se dozví o hrozbě v oblasti kybernetické bezpečnosti. Takové varování bude zveřejněno na internetových stránkách Národního bezpečnostního úřadu[96], aby se s hrozbou mohla seznámit i veřejnost. Součástí varování bývá i doporučení, jak takové kybernetické hrozbě čelit.

b) *Reaktivní opatření*[97] - účelem reaktivního opatření je okamžitá reakce na výskyt kybernetického bezpečnostního incidentu. Úřad toto opatření vydá a doručí ho povinné osobě. Pokud se to nepodaří doručit povinné osobě do vlastních rukou, vyvěsí se rozhodnutí na úřední desce Úřadu a od toho okamžiku je vykonatelné. Pokud kvůli rychlému vývoji nebo složitosti

---

[89] [online] govcert.cz [cit 03-10-2018] Dostupné z:https://www.govcert.cz/download/Zpravy-KB-vCR/Zprava-oKB-2014.pdf
[90] viz § 7 zákona o kybernetické bezpečnosti
[91] viz § 21 zákona o kybernetické bezpečnosti
[92] viz zákon č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti
[93] viz § 11 zákona o kybernetické bezpečnosti
[94] viz § 12 zákona o kybernetické bezpečnosti
[95] Národní bezpečnostní úřad.
[96] *„respektive jeho součásti – vládního CERT“*MAISNER Martin, VLACHOVÁ, Barbora. *Zákon o kybernetické bezpečnosti, Komentář*. Praha, Wolters Kluwer, a. s., 2015. s.110
[97] viz § 13-15 zákona o kybernetické bezpečnosti

kybernetického incidentu nelze přesně určit adresáta[98], má reaktivní opatření formu obecné povahy.[99]

c) *Ochranná opatření*[100] - Ochranné opatření, které má stejně jako reaktivní opatření formu obecné povahy, Úřad vydává za účelem zvýšení ochrany informačních systémů, služeb nebo sítí elektronických komunikací. Takové opatření je vydáno na základě analýzy již vyřešeného kybernetického bezpečnostního incidentu.

3.8 Objasňování kybernetické kriminality

Objasňování trestných činů kybernetické kriminality se zabývá zvláštní část kriminalistiky[101]. Kybernetická kriminalita se v současné době nezadržitelně rozšiřuje a je důležité, aby kriminalisté udrželi krok s pachateli, kteří jsou často velmi znalí v oblasti informačních a komunikačních technologií a stále své znalosti v této oblasti rozvíjejí.

Při vyšetřování kybernetické kriminality hraje důležitou roli **čas**. Kriminalisté musí postupovat rychle, aby tak měl pachatel co nejméně času na případnou likvidaci stop. Největším problémem v praxi zůstává, že řada kybernetických útoků zůstane nenahlášena a velká většina pachatelů tak zůstane nepotrestána.

3.8.1 Vyšetřování kybernetické kriminality

Plán vyšetřování bychom mohli rozdělit do dvou částí:

1. V první části je zahrnuto získávání a vyhodnocování informací. Je třeba určit, o jaký trestný čin z oblasti kybernetické kriminality se jedná, kdo se bude podílet na vyšetřování tohoto trestného činu a určení potencionálního pachatele.

---

[98] Orgán nebo osoba.

[99] „*budou v něm specifikovány, povinnosti k jeho odvrácení neurčitému okruhu orgánů a osob definovanému za užití generických znaků odpovídajících jeho charakteru*“MAISNER Martin, VLACHOVÁ, Barbora. *Zákon o kybernetické bezpečnosti, Komentář*. Praha, Wolters Kluwer, a. s., 2015. s.111

[100] viz § 13-15 zákona o kybernetické bezpečnosti

[101] „*Kriminalistika je samostatný vědní obor, který zkoumá a objasňuje zákonitosti vzniku, zániku, vyhledávání, zajišťování, zkoumání a využívání kriminalistických stop, jiných soudních důkazů a kriminalisticky významných skutečností. Vypracovává podle trestního zákona a trestního řádu metody, postupy, prostředky a operace v zájmu úspěšného odhalování, vyšetřování a předcházení trestné činnosti .“*STRAUS, J. VAVERA, F. *Slovník kriminalistických pojmů a osobností*. 1. vydání. Plzeň: Aleš Čeněk, 2010, s.108

2. Ve druhé části je zahrnuta domovní prohlídka, ohledání místa činu, zajištění kriminalistických počítačových stop a výslech svědků a obviněného.[102]

Vyšetřovací tým musí vždy počítat s tím, že pachatelem trestných činů nemusí být jen jedinec, ale i organizovaná skupina, která má často velice dobrou organizaci bezpečnostní opatření zabraňující jejímu odhalení.

Jednotlivé vyšetřovací úkony musí být prováděny v souladu s trestním řádem České republiky a musí být prováděny tak, aby nenarušily průběh vyšetřování.[103]

3.8.2 **Metodika vyšetřování a dokazování**

Samotné vyšetřování trestného činu v oblasti kybernetické kriminality můžeme rozdělit na 7 částí uvedeny sestupně podle jejich důležitosti:

1. *Zjištění způsobu, kterým pachatel prolomil ochranná opatření systému a pochopení jednotlivých kroků tohoto prolomení.*
2. *Analýza získaných informací a určení okamžiku, kdy k vyšetřování přizvat orgány činné v trestním řízení.*
3. *Obstarání informací nezbytných pro nastražení tzv. „pasti" na pachatele – zejména odhalení místa, ze kterého pachatel do systému proniká.*
4. *Najít motiv pachatele – proč si pro svůj čin vybral ten konkrétní systém.*
5. *Shromáždit co nejvíce důkazů o průniku do systému.*
6. *Získání dalších informací, které pomohou zúžit seznam dalších podezřelých subjektů – součástí toho může být i zabavení počítače dalšího možného pachatele, neboť v něm mohou být uloženy usvědčující informace.*
7. *Vypočtení výše škody, která byla trestným jednáním způsobena, a to i včetně nákladů na vyšetřování a na vrácení postiženého systému zpět do původního stavu.*

Z výše uvedených částí jsou z hlediska objasňování nejdůležitější kroky 2 a 3.[104]

---

[102] GŘIVNA, Tomáš, POLČÁK, Radim. *Kyberkriminalita a právo*. Praha. Vydavatelství Auditorium. 2008. s. 88

[103] „*Cílem vyšetřovacích a pátracích úkonů kriminalistů je zajištění dostatečného množství důkazů, které umožní orgánům činným v trestním řízení poznání skutečností, důležitých pro rozhodnutí. Problematika důkazních prostředků je podrobně upravena v ust. § 89 odst. 2 TŘ. který stanoví, že za důkaz může sloužit vše, co může přispět k objasnění věci, zejména výpovědi obviněného a svědků, znalecké posudky, ohledání, věci a listiny důležité pro trestní řízení a ohledání.*"GŘIVNA, Tomáš, POLČÁK, Radim. *Kyberkriminalita a právo*. Praha. Vydavatelství Auditorium. 2008. s. 89

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

3.8.3 **Domovní prohlídka**

Domovní prohlídka je jeden z možných úkonů podniknutých k zajištění věcí nebo důkazů, které mohou prokázat trestné jednání pachatele. Lze ji nařídit jen tehdy, pokud je v souladu s ustanovením § 80 odst. 1 TŘ[105]. Jedná se tak o jeden z největších zásahů do nedotknutelnosti obydlí, který je však při zákonném dodržení všech podmínek v čl. 12 odst. 2 Listiny základních práv a svobod povolený.

Příkaz k domovní prohlídce musí být zdůvodněn a mít písemnou formu. Může ji nařídit jen soudce nebo předseda senátu[106] a následně ji pak zrealizovat policejní orgán a to i přes případný zákaz majitele nebo zletilého člena domácnosti. To však neznamená, že by policejní orgán nemohl bez příkazu k domovní prohlídce na soukromý pozemek vstoupit.[107]V takovém případě však trestní řád stanovuje, že po vstupu do obydlí nesmějí být provedeny žádné jiné úkony, než které jsou nezbytné k odvrácení naléhavého nebezpečí.[108]

O provedené domovní prohlídce musí být sepsán protokol, ve kterém musí být uvedeny všechny okolnosti prohlídky a to včetně odebrání věcí a nejdéle do 24 hodin musí policejní orgán osobě, u které byla domovní prohlídka provedena, předat písemné potvrzení o provedených úkonech.

Je nezbytné, aby domovní prohlídka proběhla rychle a systematicky, aby nikdo z osob neměl možnost s daty manipulovat.[109]

3.8.4 **Digitální stopy a důkazy**

Zajištění důkazů při vyšetřování trestných činů kybernetické kriminality mají specifický charakter. Na rozdíl od hmotných důkazů je digitální důkazy mnohem obtížnější

---

[105] viz ustanovení § 82 odst.1 TŘ „*Domovní prohlídku lze vykonat, je-li důvodné podezření, že v bytě nebo jiné prostoře sloužící k bydlení nebo v prostorách k nim náležejících (obydlí) je věc nebo osoba důležitá pro trestní řízení.“*

[106]viz ustanovení § 83 odst. 1 TŘ „*Nařídit domovní prohlídku je oprávněn předseda senátu a v přípravném řízení na návrh státního zástupce soudce. V neodkladných případech tak může namísto příslušného předsedy senátu nebo soudce (§ 18) učinit předseda senátu nebo soudce, v jehož obvodu má být prohlídka vykonána. Příkaz k domovní prohlídce musí být vydán písemně a musí být odůvodněn. Doručí se osobě, u níž se prohlídka koná, při prohlídce, a není-li to možné, nejpozději do 24 hodin po odpadnutí překážky, která brání doručení.*

[107] viz ustanovení § 83 TŘ odst. 1 písm. c „*Policejní orgán může vstoupit do obydlí, jiných prostor nebo na pozemek jen tehdy, jestliže věc nesnese odkladu a vstup tam je nezbytný pro ochranu života nebo zdraví osob nebo pro ochranu jiných práv a svobod nebo pro odvrácení závažného ohrožení veřejné bezpečnosti a pořádku*.“

[108] V kybernetickém okruhu se bude jednat například o hrozící nebezpečí teroristického útoku.

[109] GŘIVNA, Tomáš, POLČÁK, Radim. *Kyberkriminalita a právo*. Praha. Vydavatelství Auditorium. 2008. s. 92

získat a zaznamenat. Pro pachatele je snadnější je ovlivnit nebo úplně zničit. Z kriminalistického hlediska je každé informační zařízení digitální stopou.[110]

S ohledem na komplikovanost výpočetní techniky je zajišťování digitálních důkazů velmi choulostivý úkon a musí při něm být dodrženo přísné opatření, jelikož neopatrné zacházení s ní může zapříčinit nenávratné vymazání dat. Je tedy důležité, aby takovou činnost vykonával odborník nebo soudní znalec

Pachatelé mohou mít také námitky, že usvědčující data byla do počítače nahrána až při zajišťování důkazů a musí proto být během expertizy za účasti odborníků a znalců pořízena dokumentace, která by případně vyvrátila pochybení orgánu činného v trestním řízení.[111]

3.9 Hledání cest prevence kybernetické kriminality

Na čem se snad všichni autoři současné literatury v oblasti kybernetické kriminality shodují je fakt, že preventivní opatření proti kybernetické kriminalitě musí jít ruku v ruce s jejím vývojem. Jako prevenci proti kriminalitě můžeme brát všechna opatření, jejichž cílem je snížení rizika trestných činů. Důležitým faktorem prevence je subjektivní ochrana soukromých dat uložených na nosiči informací. Jako nejzákladnější ochranu dat můžeme jmenovat například instalaci a pravidelnou aktualizaci antivirových programů. U větších firem se jeví jako vhodná také investice do technického vybavení a na IT pozice dosazovat personál, který je v tomto oboru dostatečně kvalifikovaný.

Důležitá je i masová osvěta o působnosti takového druhu kriminality v kyberprostoru napříč všemi generacemi. V dnešní době existuje mnoho projektů a seminářů, které pomáhají vysvětlit, jak proti kybernetické kriminalitě bojovat.

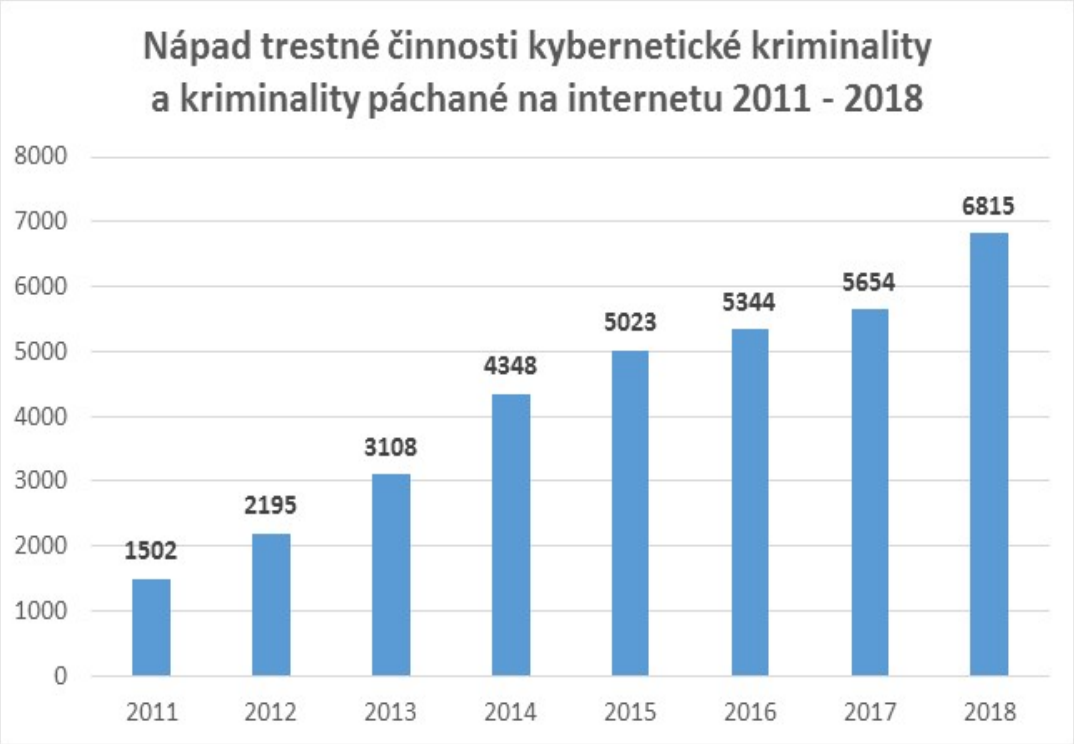
Jak můžeme vidět na stránkách Policie ČR, kybernetická kriminalita každým rokem stoupá a je důležité se jí bránit.

---

[110] *„Kriminalistickou počítačovou stopu lze v užším slova smyslu chápat jako digitalizovanou informaci, která je dočasně či trvale uchována na záznamovém médiu, nosiči informací a kterou je možno zpětně získat zpravidla týmiž nebo obdobnými technickými a programovými prostředky, kterými byla vytvořena“*.GŘIVNA, Tomáš, POLČÁK, Radim. *Kyberkriminalita a právo*. Praha. Vydavatelství Auditorium. 2008. s. 93

[111] GŘIVNA, Tomáš, POLČÁK, Radim. *Kyberkriminalita a právo*. Praha. Vydavatelství Auditorium. 2008. s. 94

Obrázek 4 Trestná činnost kybernetické kriminality v letech 2011-2018



Zdroj: [online] govcert.cz [cit 03-10-2018] Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx

Podle Policie ČR byl největší nárůst kybernetické kriminality zaznamenán v oblasti mravnostních trestných činů, zejména šíření dětské pornografie nebo navazování nedovolených kontaktů s dítětem. Kvůli takovým případům vznikla v České republice celá řada organizací, kam se můžou oběti takového jednání obrátit, jako například:

- www.linkabezpeci.cz
- www.onlinehelpline.cz
- www.poradna.e-bezpeci.cz
- www.bezpecnyinternet.cz

To jsou jen příklady stránek, na které se mohou děti, případně jejich rodičem obrátit v případě, že se stanou oběťmi kybernetické kriminality. Na stránkách působí uživatel anonymně a jejich cílem je postiženému pomoci nebo poradit, kam a na koho se má poškozený případně obrátit.

3.10 Dílčí závěr teoretické části práce

V teoretické části bakalářské práce je objasněn fenomén kybernetická kriminalita, její historie a rozšíření mezi veřejnost. Zároveň je provedena analýza vybraných druhů kybernetické kriminality a platné právní úpravy, která je zpracována v kontextu s trestním zákoníkem. Závěr teoretické části je věnován objasňování kybernetické kriminality v České republice s cílem vysvětlit metodiku objasňování kybernetické kriminality a vysvětlit cesty vedoucí k prevenci.

Teoretická část na základě rešerše literatury odhalila, že neexistuje jednotná definice kybernetické kriminality, která by byla schopna odborně a věcně shrnout celou problematiku (viz. kapitola 3.1.1.). Útoky mířené proti informačním a komunikačním technologiím jsou stále sofistikovanější a technicky dokonalejší.

S určitostí nelze říci, od kdy datovat trestné jednání jako činy kybernetické kriminality (viz. kapitola 3.3.). V České republice se o největší rozmach této problematiky zasloužil rok 1989, kdy došlo k otevření hranic pro zahraniční trh a následné připojení k internetu. To vše mělo za následek rozšíření tohoto druhu kriminality do takového rozsahu, v jakém je dnes. Vybrané druhy kybernetické kriminality rozebrané v kapitole 3.4.jsou jen nepatrnou ukázkou tak globálního problému, který kybernetická kriminalita představuje. Dále je věnována pozornost účastníkům kybernetické kriminality (viz kapitola 3.6), kde je rozebrán profil oběti a pachatele, jelikož ke kybernetickému zločinu je potřeba účast alespoň obou z nich.

Kapitola 3.7. odhaluje nedostatky platné právní úpravy a nutnost její novelizace s ohledem na dynamicky se rozvíjející možnosti, které kyberprostor nabízí. V České republice je kybernetická kriminalita právně upravena zejména trestním zákoníkem a zákonem o kybernetické bezpečnosti. V návaznosti na právní úpravu je proveden rozbor objasňování a vyšetřování kybernetické kriminality (viz kapitola 3.8). Při objasňování kybernetických zločinů je velkým problémem prostor pro anonymitu, kterou virtuální svět umožňuje. Je důležité správně naplánovat metodiku a postup při vyšetřování, neboť čas je významným faktorem, který může hrát ve prospěch pachatele.

Součástí teoretických východisek je prevence proti kybernetické kriminalitě (viz kapitola 3.9). Na základě rešerše literatury by se měla prevence rozvíjet duplicitně s vývojem informačních a komunikačních technologií, jelikož je důležitější než represivní postihy.

4 Praktická část

Praktická část je nejprve věnována návrhu na zlepšení právní úpravy kybernetické kriminality. Jak už bylo výše zmíněno, kybernetická kriminalita je velmi dynamicky rozvíjena a bylo by dle mého názoru na místě, aby byla právní úprava častěji novelizována vzhledem k počtu nových trestných činů.

Další částí je analýza a grafické znázornění výsledků dotazníkového šetření, které jsem provedla na základní škole na téma povědomí o kybernetické kriminalitě.

V praktické části je rovněž provedena případová studie cyberstalkingu.

Závěr praktické části je věnován řízenému rozhovoru s pachatelem a obětí kybernetického trestného činu.

4.1 Návrh na zlepšení platné právní úpravy

Při boji s kriminalitou je v bakalářské práci vybrán poměrně úzký výsek sociálního jevu, a to kybernetickou kriminalitu. Jedná se o jev relativně nový a velmi moderní. I když zneužívání telefonu či telegrafu (např. výhrůžky po telefonu) jsou reálné po více než jedno století zpětně. Ale bezbřehý kybernetický prostor je realita až posledních padesáti let.

Kybernetická kriminalita je závislá na existenci kybernetického prostoru. Pokud bychom zrušili kybernetický prostor, tak by tato kriminalita zcela vymizela. To je první radikální řešení, které však není možné z ekonomických důvodů, neboť by přineslo takové národohospodářské ztráty, které by naprosto nevyvažovaly přínos z neexistence tohoto druhu trestné činnosti.

Pokud je kybernetická kriminalita velice mladým jevem, pak i prostředky boje proti ní jsou velice nevyzkoušené, nevyladěné a do velké míry neznámé. Jen velice obtížně se v toku dat rozliší naprostá většina nezávadných informací od malého procenta škodlivých vlivů a degenerací. Není v možnostech lidstva, každou stranu zasílané korespondence nejdříve přečíst, vyhodnotit a povolit či nepovolit její další šíření.

Je tedy otázkou, jak by se tedy dal boj proti kybernetické kriminalitě zefektivnit do budoucna. Jistě je zde možnost vsadit na represi a podstatně zvýšit trestní sazby hrozící za tuto trestnou činnost. Ale zkušení kriminologové již dávno vypočítali, že zvýšení trestních sazeb u jakéhokoliv druhu kriminality, nevede k jejímu potlačení či dokonce vymýcení. Například počet vražd na milion obyvatel není v jednotlivých státech závislý na tom, zda

se v tomto konkrétním státě realizuje trest smrti či nikoliv. A to trest smrti působí hodně silným dojmem na potencionálního pachatele.

U kybernetické kriminality se samozřejmě nikdy nenastane trest smrti či výjimečný trest. Tato trestná činnost nepatří k nejzávažnějším, co do následků. To se ale v blízké budoucnosti může podstatně změnit, neboť různí počítačoví hackeři mohou vážně narušit chod elektráren, záchranného systému, nemocnic či dokonce vojenského velení. Ve stále propojenějším světě je tato hrozba velmi aktuální a v budoucnu bude spíše stoupat.

Pro lepší úpravu kybernetického prostoru lze tedy navrhnout:

- užší a propracovanější nadnárodní spolupráce při vyšetřování kybernetické kriminality, čímž by se zvýšila šance při odhalování pachatelů,
- častější novelizace právních úprav v oblasti kybernetického prostoru
- větší efektivnost vymáhání práva v kyberprostoru. Zákony by na jedné straně měly zahrnovat všechny formy trestního jednání spolu s dostatečnými postihy, ale jejich porušení musí být zároveň dostatečně účinně vynucováno, jinak nebude žádná norma dostatečně plnit svou funkci.

Kromě zlepšování příslušných zákonů při boji s kybernetickou kriminalitou, což je činnost vysoce odborná a bez velké historické zkušenosti, lze s tímto jevem bojovat hlavně prevencí a výchovou.

Stěžejní případy porušování práva v této oblasti je třeba zveřejnit pro výchovu celé společnosti. Jeden odhalený pachatel anonymních výhrůžek po e-mailu může desítky dalších obdobných pachatelů od této trestné činnosti odradit. Dále by měly být pravidelně zveřejňovány osudy obětí této trestné činnosti. Zde se jedná o velice citlivou oblast, takže oběti by byly chráněny proti identifikaci, pouze jejich příběhy by byly zveřejněny pro poučení společnosti. Pokud se vyskytlo již několik případů, kdy nezletilé dítě spáchalo sebevraždu po zdánlivě nevinném šikanování ze strany kamarádů, pak tento alarmující jev je třeba co nejvíce „zpopularizovat“ a vysvětlit společnosti jeho negativní a hrůznou podobu. To může působit více preventivně na život společnosti, než udělované vysoké tresty za tuto protizákonnou činnost.

Jak vyšlo z analýzy, kybernetická šikana, potažmo i šikana tradiční v právní úpravě nejsou dostatečně upraveny, stávající aplikace práva se odvíjí až na základě příslušného jednání. Návrhem by mohlo být zakotvení tohoto jednání v právu jako samostatný trestný čin, zařazen do trestního zákoníku č 40/2009 Sb. zvláštní části HLAVA II – Trestné činy proti svobodě a právům na ochranu osobnosti, soukromí a listovního tajemství jako trestný

čin kybernetické šikany. Tradiční šikanu by dle mého názoru mohla být vyšetřována jako přestupek.

Je také důležité, aby s oběťmi této trestné činnosti nadále intenzivně pracoval zkušený psycholog či psychiatr. Tím by se předešlo mnoha krutým osudům, kdy se oběť nesmíří s touto potupou a poškodí sama sebe či pachatele nebo domnělého pachatele. Tím by se ve společnosti pouze prohluboval řetězec násilí a odplaty. Mimo snížení latentní kriminality ve společnosti by tito odborníci velice přispěli k duševní hygieně celé společnosti.

Avšak nejlépe se proti kybernetické kriminalitě bojuje vyšším vzděláním celé společnosti a především podtržením jejích morálních zásad. Každá kybernetická kriminalita je nejenom nebezpečná, ale i vysoce nemorální, takže by zlepšení morálních zásad všech jedinců velice přispělo k eliminaci tohoto jevu na okraj společnosti.

4.2 Dotazníkové šetření povědomí žáků 2. stupně základní školy o kybernetické kriminalitě

K výzkumu byla zvolena množinu žáků základní školy v Mladé Boleslavi, kteří byli podrobeni dotazníkové akci na téma „Co víte o šikaně, konkrétně o kybernetické šikaně“.

Cílem dotazníkového šetření bylo zjistit, zda mají děti už od raného věku povědomí o kybernetické šikaně a zda vědí, jak toto jednání případně řešit. V souvislosti s prevencí bylo cílem zjistit, zda fungují nějaké preventivní opatření a výchova v tomto ohledu už na základní škole.

Zvolena byla skupina 100 žáků z 2. stupně základní školy. Jednalo se o žáky ve věku 11-15 let s tím, že jsem si vybrala konkrétní žáky v počtu 25 z 6 třídy, 25 ze sedmé třídy, 25 z 8 třídy a 25 z 9 třídy.

Dotazník byl nejprve předložen třídním učitelkám ke kontrole, aby věděly, jaké otázky budou dětem položeny. Ty pak samy vybraly skupinu 25 žáků, kteří byli ochotni dobrovolně a zodpovědně na položené otázky odpovědět.

Žáci byli taktéž srozuměni se smyslem této akce, nejprve byli trochu překvapení, ale postupně se osmělovali a dobře spolupracovali. Bylo jim zdůrazněno, že je důležitý jejich vlastní názor a nebudou za to hodnoceni.

Všechny dotazníky byly anonymní, takže všechny podmínky ochrany GDPR byly dodrženy.

Odpovědi na otázky v mém dotazníku byly nastaveny tak, že každý žák měl odpovídat pouze jednoduchými odpověďmi „ANO, NE“. Nebyly tedy žádné popisné odpovědi.

Otázky byly připraveny tyto:

1. Víš co to je šikana?
2. Víš, co to je kybernetická šikana?
3. Setkal ses někdy s kybernetickou šikanou?
4. Znáš někoho, kdo někoho jiného kyberneticky šikanoval?
5. Byl jsi poučen/na o rizicích psaní osobních údajů (adresa, věk) na internet?
6. Pokud se ti spolužák svěří, že ho někdo přes internet šikanuje, víš, za kým ho máš poslat?
7. Měly jste ve škole přednášku na téma „ Nebezpečí přicházející z internetu“?

Celkově se dá zhodnotit dotazníková akce za úspěšnou. Děti odpovídaly ochotně, rychle a zodpovědně. Nebyl, kdy by všechno nějaký žák jen proškrtal, pomaloval či jinak akci bojkotoval.

Vyhodnocení dotazníkového šetření přineslo pozitivní výsledky ve smyslu prevence a výchovy. Téma kybernetické kriminality není na základních školách tabu a je snaha seznámit děti s nebezpečím, které kyberprostor přináší. Naopak negativním výsledkem bylo velké procento dětí, které se již s kybernetickou šikanou setkaly.

Dle mého názoru by obdobných akcí a to s ještě podrobnějším dotazníkem mohlo být mezi žáky základních a středních škol více, jistě by zde našli hodnotné výsledky i psychologové, sociologové, pedopsychiatři a další specialisté.

4.3 Případová studie

4.3.1 Kybernetická šikana - cyberstalking

Pro zpracování případové studie na téma kybernetická šikana byla oslovena slečna, z důvodu ochrany osobních údajů bude v bakalářské práci jmenována jako Adéla, která má za sebou zkušenost s kybernetickou šikanou, konkrétně s cyberstalkingem (viz kapitola 3.4.1.). Adéla pasivně souhlasila se zveřejněním jejího příběhu pod podmínkou anonymity a byla seznámena se zpracováním jejího příběhu bakalářské práce.

Počátek kyberšikany

Vše začalo, když bylo Adéle 22 let. Do té doby vedla normální společenský život, měla dva dlouhodobé partnery, spoustu přátel a řešila jen klasické problémy všedního

života. Jednou se v baru seznámila se s klukem, říkejme mu Petr, se kterým začala randit a později udržovat intimní vztah. Jejich vztah trval cca 3 měsíce, když Adéla náhodou, přes společného známého přišla na to, že je Petr ženatý. To pro ni byla naprosto nečekaná informace, jelikož s ní trávil hodně času a okamžitě vztah ukončila, jelikož Petr nejen že byl ženatý, ale měl se svoji manželkou i dvě děti.

Petr se ovšem s rozchodem nechtěl smířit a začal Adélu obtěžovat každodenními telefonáty, SMS a zprávami na sociálních sítích. Adéla ale nereagovala a nechtěla s ním být v jakémkoli kontaktu. Přestože byl odmítán, stále více se snažil o kontakt a začal na ní dokonce čekat před prací.

Intenzita útoků

Na několika nepříjemných střetnutích mu Adéla dala jasně najevo, že si nepřeje mít s ním dál nic společného, ale to Petra pouze vyprovokovalo a jeho zprávy začaly být více agresivní. Začal dokonce kontaktovat její kamarády a svěřovat se jim s vymyšlenými příběhy o tom, jak mu Adéla pomotala hlavu, citově ho vydírala a nutila ho do rozvodu. To se začalo podepisovat na jejích soukromém životě, jelikož někteří její známý v ní přestali mít důvěru. Celá situace se už začalo podepisovat na doteď psychicky silné Adéle, začala mít nepříjemný pocit pokaždé, když vyšla z domu a na každé pípnutí telefonu se šla podívat s obavou, že to bude zase výhrůžná zpráva od Petra.

Obranný útok proti agresorovi

Adéla se tedy uchýlila k tomu, že kontaktovala Petrovu manželku a všechno jí vylíčila, včetně jejich vztahu a následnému teroru z Petrovy strany. Dokonce jí ukázala výhružné zprávy od něj i nespočetné množství telefonátů. Přestože se k tomu Petrova manželka stavěla pasivně, tvrdila Adéle, že jí nevěří, z následných zpráv, co Adéla od Petra dostala, bylo patrné, že mezi nimi došlo k nějaké konfrontaci. Po této situaci se Petr uchýlil k zoufalému kroku a začal Adéle vyhrožovat, že zveřejní její intimní fotky a videa z dob, kdy se ještě scházeli. To už Adélu psychicky zlomilo, jelikož se bála, že to zničí její osobní život. Její okolí si začalo všímat, že s ní není něco v pořádku, je stále nervózní a uzavřená do sebe. I přes to však nechtěla hnát tento příběh na povrch, jelikož se styděla se s tím svěřit a stále doufala, že Petra ta posedlost přejde.

On však na její prosby, ať jí už nechá být a žije si svůj vlastní život nereagoval a tak Adéla stále čelila každodennímu kybernetickému teroru. Jednoho dne už Adéla tento tlak psychicky nevydržela a po další výhružné zprávě se psychicky zhroutila, čehož si všiml jeden se spolumajitelů stavební firmy, kde Adéla pracovala. Ten se Adély zeptal a

ona, jelikož to byl pro ni blízký člověk už nátlak nevydržela a celý příběh mu odvyprávěla. Na dotaz spolumajitele firmy, proč s celou věcí už nešla na policii odpověděla, že jí bylo trapně a ač ji několik měsíců terorizoval, nechtěla mu vzhledem k tomu, že má dvě malé děti dělat potíže. Spolumajitele firmy tedy napadlo, ať ho pod záminkou schůzky pozve na parkoviště před firmu. Petr souhlasil, ale když na místo setkání dorazil, místo Adély na něj čekala parta dělníků z firmy vyzbrojených pracovním náčiním a ti důrazně Petrovi vysvětlili, že toto chování je nadále nepřípustné a pokud v tom bude dál pokračovat, bude mu to vysvětleno fyzickým násilím. A jako výhrůžku a důkaz toho, že to myslí vážně mu urazili zrcátko u auta.

Život bez kybernetické šikany

Petr, který si doteď dovoloval jen na jednu ženu, si vzal doporučení dělníků k srdci a už nikdy Adélu nekontaktoval ani se nesnažil o jakýkoli způsob komunikace.

Adéla postupně celou situaci vytěsnila z hlavy, v 25 letech si našla partnera, za kterého se vdala a nyní s ním čeká již druhé dítě.

4.3.2 Závěr případové studie kybernetické šikany – cyberstalking

Případová studii je rozdělena na čtyři období, na kterých je, i když ne až tak markantně vidět změna Adélina psychického rozpoložení. Na výzkumu je vidno, že obětí kybernetické šikany se může stát každý, protože ačkoli je Adéla podle mě psychicky silný jedinec, dlouhodobý kybernetický teror se znaky nebezpečného pronásledování a výhrůžky se na ní postupem času podepsaly a Adéla začala vykazovat jeden z charakteristických rysů obětí kybernetické šikany – uzavírání se do sebe. Podle odborníků je v takových životních situacích důležité o svých problémech mluvit alespoň s přáteli, když už se oběť prozatím nechce obrátit na odbornou pomoc.

Naštěstí po skončení tohoto teroru se s tím Adéla dokázala sama poměrně rychle vyrovnat a nepotřebovala návštěvu psychologa nebo jinou odbornou pomoc. Bohužel ne všechny případy mají takový konec a proto existuje spoustu poraden a sdružení, kde se zaměřují na pomoc lidem s traumatickými zážitky.

Bohužel Adélin problém nebyl vyřešen úplně nejšťastnějším způsobem, jelikož výhrůžkami fyzického násilí se Adéla dostala na stejnou úroveň řešení problému, jako Petr. Sama říká, že v zoufalých chvílích lidé dělají zoufalé věci, ale s odstupem času ví, že teď už by podobnou situaci řešila jinak. Nestyděla by se svým problémem svěřit a vše by

nahlásila policii. Při takovém postupu by bylo důležitým aspektem uchování všech zpráv a jiných důkazů, které by mohly sloužit k usvědčení pachatele.

4.4 Řízený rozhovor

V rámci praktické části bakalářské práce byl vypracován rozhovor s pachatelem trestného činu kyberšikany a s obětí kyberšikany. Oba dotazovaní po několika konzultacích svolili k vytvoření rozhovoru na toto citlivé téma pod podmínkou jejich úplné anonymity.

Oba rozhovory byly předem připraveny v tom, jak budou oba dotazováni a jaká bude osnova těchto rozhovorů. Připraveno bylo asi 30 otázek s tím, že dotazovaní budou nejprve požádáni, aby nastínili svůj případ vlastními slovy a spontánně, a poté jim budou položeny další otázky.

4.4.1 Řízený rozhovor s pachatelem trestného činu

Při rozhovoru nebylo opomněno, že se jedná o muže, který by mohl mít před studentkou určité rozpaky. Otázky byly tedy pokládány tak, aby dotazující nebyl uveden do nepříjemné situace.

Celý rozhovor byl zachycen v poznámkách a poté pečlivě přepsán do přehledného zápisu, především s ohledem na jeho autenticitu.

Rozhovor měl také vliv na můj názor, jak bych do budoucna navrhla změny v právním řádu ČR tak, aby obětí kybernetické šikany bylo co nejméně. Cílový stav by směřoval k absenci těchto obětí, což je sice stěží dosažitelné, ale je třeba se o to alespoň pokusit.

Rozhovor s pachatelem kyberšikany:

Praktikantka: **Dovoluji si Vás poprosit, abyste mi vlastními slovy popsal Vaši zkušenost s kyberšikanou a s jejími následky ve Vašem životě.**

Rád Vám to všechno vypovím, ale nejsem moc dobrý řečník, tak se mě raději ptejte. Na vše Vám odpovím.

Praktikantka: **Děkuji za důvěru. Pokud Vám budou připadat mé dotazy příliš osobní, tak mi to ihned sdělte a já se pokusím Vás dotazovat jinak.**

Už mám za sebou výslech na Policii ČR, u soudu i u psychiatra. Mám tedy nějakou zkušenost, takže se tohoto rozhovoru nebojím. Klidně se ptejte.

Praktikantka: **Ráda bych začala Vaším dětstvím. Bylo v něm něco nezvyklého?**

Ani bych neřekl. Měl jsem oba rodiče a starší sestru. Rodiče se o nás starali dobře. Sestra byla starší o osm let, takže jsme si moc nerozuměli. Já jako mladší jsem byl asi trochu rozmazlován.

Praktikantka: **Pokud se podíváte na své dětství z dnešního pohledu, scházelo Vám něco?**

Ani bych neřekl. Rád jsem hrál fotbal, chodil mezi lidi, měl jsem dost přátel.

Praktikantka: **Naznačovalo něco Vaše pozdější chování?**

Nic to nenaznačovalo, občas jsem se popral, ale tak normálně, jako ostatní kluci.

Praktikantka:**A co vztah s děvčaty, jak se u Vás vyvíjel?**

Měl jsem o děvčata vždycky zájem, ale neřekl bych, že to bylo nějak nezdravé

Praktikantka:**Měla jsem na mysli Váš vztah s děvčaty v dospívajícím věku.**

Ano, dokonce jsem v šestnácti začal chodit do tanečních. Tam se zájem o dívky přímo vyžadoval.

Praktikantka: **Připadal Vám Váš vztah k ženám nějaký abnormální?**

Ne, vůbec ne. Měl jsem starší sestru, takže jsem byl zvyklý na přítomnost žen u nás doma i na určité ženské móresy.

Praktikantka: **Týrala Vás sestra jako starší a silnější?**

Jako malý jsem ji musel poslouchat. Ale zase se o mě starala, takže jsem si nepřipadal hloupě. V patnácti letech jsem ji dorostl. Už se na mě nedívala jako na malého, docela jsme si rozuměli. Ale rychle se vdala a odešla z domu.

Praktikantka: **A co jiná děvčata, jaké jste s nimi měl zkušenosti?**

Na základní škole žádné. Měl jsem partu kluků, takže jsme holky ani nepotřebovali. To přišlo až na střední škole.

Praktikantka: **Ublížila Vám někdy nějaká dívka v těchto citlivých letech?**

To nevím. Dostával jsem kopačky ne úplně hezky, třeba na taneční zábavě, ale to asi většina mých kamarádů. Kvůli tomu jsem proti ženám nic neměl.

Praktikantka: **Musím se zeptat i kdy jste navázal první intimní kontakt, nevadí Vám to?**

Ne, opravdu ne. Ptali se na to již policisté i psychiatr. Jsme na to zvyklý.

Praktikantka: **Pokud by Vám nějaká otázka nesedla, ráda ji vynechám.**

Ničeho se nebojím, jen se ptejte.

Praktikantka: **Tak bych se tedy ráda zeptala tu intimní zkušenost.**

Docela jsem se styděl, tak mám první intimní zkušenost až z osmnácti let.

Praktikantka: **To snad není pozdě. Dnes jsou ty statistiky ještě vyšší.**

Asi ano. Ale tenkrát to bylo nějaké rychlejší. V osmnácti se již někteří kluci ženili.

Praktikantka: **Bylo to poprvé nějaké nepříjemné?**

Nepříjemné asi ne, ale hodně trapné. Ale to asi mnoho kluků zažije. Ta holka byla o rok starší, tak jsem si připadal jako pitomec.

Praktikantka: **Myslíte si, že to nějak ovlivnilo Váš další život?**

Asi ne. Potom jsem navázal tři další vztahy a ty byly docela normální

Praktikantka: **Vystupoval jste vůči ženám nějak dominantně?**

To asi ne, ale nenechal jsem si nic líbit. Měl jsem dobrý trénink s různými spory s mojí sestrou. Nebyl jsem tedy nějaká ušlápnutá chudinka.

Praktikantka: **Co se tedy stalo, že jste se dostal před soud?**

S tou poslední dívkou jsem chodil skoro tři roky a pak mi ji přebral kamarád. Nějak jsem to nevydejchal a posílal jsem jí výhružné maily a SMS. Dostal jsem podmínku za pronásledování.

Praktikantka: **To jste to tedy vzal velice rychle. Co bylo příčinou tohoto incidentu?**

Dnes už to vím, že to byla špatná komunikace. Ale to mi řekli až psychiatři. Sám bych na to nepřišel. Kdyby mi to ten psychiatr řekl předem, asi by se to nestalo. Choval jsem se jako blázen.

Praktikantka: **Proč jste tu dívku pronásledoval?**

To vůbec nedokážu vysvětlit. Ani po léčení u psychiatra. Asi jsem ji moc miloval a nedovedl jsem se smířit s tím, že mi utekla. Asi zhrzená pýcha.

Praktikantka: **Ale zhrzená pýcha většinou nedostane lidi před soud.**

Ano,to máte pravdu. Nevím, co na to říct, choval jsem se jako blázen, měl úplné zatmění.

Praktikantka: **Myslíte si, že ta dívka se Vás mohla bát?**

Z počátku se mi vysmívala do očí. Po mých výhrůžkách se ale jistě bála. Choval jsem se jako psychopat.

Praktikantka: **Jak se to projevovalo?**

Volal jsem ji třeba ve tři hodiny ráno pětkrát za sebou, že s ní nutně potřebuju mluvit. Až si pak vypnula telefon. Dnes bych si za to sám nafackoval!

Praktikantka: **Nerada se ptám, ale vyhrožoval jste jí také smrtí?**

Bohužel i to, cítil jsem se bezmocně.

Praktikantka: **Co Vám policie nejvíc vytýkala? Že jste jí vyhrožoval smrtí?**

Je to divné, ale to mi ani nevyčítali. Asi to nebrali moc vážně. Vyčítali mi hlavně to, že jsem ji pronásledoval skoro dva roky a neustále se jí montoval do života. Od jejího nového přítele jsem dostal několikrát na hubu, ale ani to mě nezastrašilo. Já jsem útočil stále jen na ni.

Praktikantka: **Připadá Vám toto chování zbabělé?**

Ano, dneska už mi to připadá velice zbabělé. Ale k tomu jsem dospěl až po několika letech. Mezitím jsem si vzal jinou dívku, která již měla ročního chlapce, kterého dodnes spolu vychováváme. Kdyby ji dnes někdo takto pronásledoval, určitě by mi to nebylo jedno a chtěl bych tomu nějak zamezit.

Praktikantka: **Bál jste se, že Vás zavřou?**

Toho jsem se vůbec nebál. V tu chvíli mi bylo všechno úplně jedno.

Praktikantka: **Chtěli Vás zavřít?**

Chtěli, ale do blázince! To je snad ještě horší než vězení! Byl jsem tam zavřen tři týdny a už bych tam nikdy nechtěl. Pak jsem dalších pět let docházel k psychiatrovi ambulantně a snad už jsem teď vyléčen. Po tolika letech se na to dívám jako na mladickou nerozvážnost. Nechápu, jak jsem se mohl takhle chovat.

Praktikantka: **Mohl byste mi poradit, co bych měla do své práce napsat, aby se v budoucnu takovýmto případům předešlo?**

To jste mě tedy dostala! Stokrát jsem přemýšlel o svém životě a už vím, co bych v životě nikdy neopakoval. Ale co bych poradil ostatním?

Praktikantka: **Zkuste mi, prosím, poradit. Vaše zkušenost je pro mě velice přínosná. Co byste poradil dnešním mladým lidem, aby se jim třeba toto již nestalo?**

Jak mi psychiatr vysvětlil, bylo to selhání komunikace. S mojí bývalou dívkou jsme si některé problémy nevysvětlili, a takhle to dopadlo. Dovedlo mě to skoro až do kriminálu.

Praktikantka: **Myslíte si, že takovýchto případů bude v budoucnu méně?**

Se všemi možnostmi dnešní doby myslím, že toho bude spíš více.

Praktikantka: **Máme tedy špatné zákony?**

To se vůbec neodvážím posoudit. Prošel jsem si vyšetřováním na policii i u soudu, ale nemám nějaké strašné zkušenosti. Jsem ale přesvědčen, že mi pomohl až ten psychiatr. Ten první se mnou mluvil jako s člověkem, ne jako s psychopatem.

Praktikantka: **Takže prevence v tomto případě by Vám pomohla?**

Tohle se asi nedá předpovědět. Ale člověk by se v každé situaci měl chovat jako člověk. života. Dokonce ani moje maminka ani sestra mě za to neodsoudily. Toho si velice vážím.

Praktikantka: Moc děkuji za rozhovor a musím Vám vyslovit uznání, že jste se nebál ani velmi nepříjemných otázek. Ještě jednou děkuji.

4.4.2 Řízený rozhovor s obětí (poškozenou) kybernetické kriminality

Při rozhovoru bylo využito toho, že se jednalo o mladou ženu, které se nestyděla o svém zážitku mluvit před stejně starou studentkou.

Celý rozhovor byl zachycen v poznámkách a poté pečlivě přepsán do přehledného zápisu, především s ohledem na jeho autenticitu. Rozhovor nebyl nijak zkracován ani upravován. Cílem bylo zachytit opravdový příběh jedné ženy a vliv této trestné činnosti na život konkrétního člověka.

Rozhovor praktikantky s obětí:

Praktikantka: **Zkuste mi, prosím, popsat, jakou zkušenost jste Vy osobně zažila s kybernetickou šikanou.**

Jako většina mladých lidí jsem si i před deseti lety založila FB účet. Bylo to doslova proti přání mých rodičů, oni mi to nejenom nedoporučovali, ale přímo zakazovali. Přesto jsem si tento účet založila.

Praktikantka: **Jak se to rodiče dozvěděli?**

Mohla jsem si za to sama, byla jsem stále „přilepená‘‘ na obrazovce, až si toho rodiče všimli. Stále se opakují ty samé příběhy, rodiče zakazují dětem FB, ony si ho stejně zařídí a pak to v mnoha případech dopadne špatně.

Praktikantka: **Co Vám ten FB v tak mladém věku přinášel?**

Určitě je to pocit, že máte blízko kamarády, že jste pořád s nimi.

Praktikantka: **Psychologové tomu říkají virtuální svět. Jak to Vy osobně vnímáte?**

Je to hezký pojem. Je to takový pocit, jakože máte kamarády na dosah ruky ve dne i v noci.

Praktikantka: **Co Vám ten FB vzal?**

Z počátku jsem si myslela, že nic, jako většina. Naopak mi přišlo, že mi všechno dává. Ten virtuální svět vás zcela pohltí, připadá vám to tak, že ten normální svět vůbec k životu nepotřebujete.

Praktikantka: **Tušila jste něco, že Vám hrozí z FB ve smyslu kybernetické šikany?**

To v žádném případě. Domnívala jsem se, že mi z této strany nemůže nic hrozit. Že případy, o kterých se mluví v televizi, jsou lživé nebo nafouklé a mně by se to přece nikdy nemohlo stát.

Praktikantka: **Co Vás osobně potkalo?**

Jako malá jsem byla spíš podvyživená, ale v pubertě jsem začala poměrně rychle nabírat, takže jsem brzy byla holka „krev a mlíko‘‘. Ve čtrnácti letech jsem již měla velké prsa i boky. Některé děti se do mě začaly navážet.

Praktikantka:**Jak se do Vás navážely?**

Bylo to takové nenápadné. Třeba mi na Facebook k fotkám psaly, jestli si nemusím půjčovat podprsenku od babičky, zveřejňovaly různé upravené fotky a podobné posměšky.

Praktikantka:**To Vám působilo nějaké duševní trauma?**

Trošku. V tom věku jsem to brala až moc citlivě. To si ale člověk uvědomí až v dospělosti.

Praktikantka:**Jak dále Vás děti šikanovaly?**

Stále se naválely do mé váhy, že prý musím nakupovat v obchodě s nadměrnými velikostmi a tak.

Praktikantka:**Nerozumím tomu, proč jste si to s těmi děvčaty nevyřídila při osobním setkání tváří v tvář?**

Dnes už bych jim to řekla naplno. Ale v těch letech člověk stále o všem moc přemýšlí.

Praktikantka:**Zažila jste podobné narážky taky ze strany chlapců?**

To ne, těm moje předčasná vyspělost nevadila. Ale problém byl v tom, že většina těch kluků měla FB taky a všechny ty urážky viděli. Do očí mi ale nikdo nic neřekl.

Praktikantka: **Jaký to mělo dopad do Vašeho duševního života?**

Styděla jsem se chodit mezi vrstevníky, po škole jsem šla rovnou domů. Výsledek byl ten, že jsem ještě více byla na Facebooku a pročítala si všechny ty komentáře pořád a pořád. Začala jsem se utápět v sebelítosti.

Praktikantka: **Jak jste se tuto šikanu snažila vyřešit? Radila jste se s učiteli nebo s rodiči?**

To určitě ne! Bála jsem se jim to říct. V těchto letech si každý chce vyřešit všechno sám. Bylo mi trapně.

Praktikantka: **Tyto útoky na Vás se stupňovaly nebo jste si na to časem „zvykla‘‘?**

Ano, narážky se stupňovaly a stále mi byly méně příjemné.

Praktikantka: **Měla tato šikana ve Vašem životě nějaké nepříznivé následky?**

Ano, nerada o tom mluvím, ale pokusila jsem se o sebevraždu.

Praktikantka: **Mělo to souvislost s šikanou na FB?**

Bohužel, tehdy jsem si myslela, že tímto všechno vyřeším. Měla jsem deprese. Bylo to zkratkovité jednání, dnes už to vím. Ale děti umí udeřit na to nejcitlivější místo.

Praktikantka: **A jak to vidíte po téměř deseti letech?**

Byla jsem hloupá. Potom se mi to již nelíbilo, ale bála jsem se s někým poradit. Můžu si za to sama.

Praktikantka: **Za těch deset let, pomohl Vám nějaký odborník, třeba psychiatr nebo psycholog?**

Ano, ale pozdě. Potom pokusu o sebevraždu jsem strávila tři měsíce v psychiatrické léčebně. Tam to bylo hrozné, ale lékaři byli na mě moc hodní a teprve tam jsem si uvědomila, že mám problém.

Praktikantka: **Léčili Vás pomocí léků nebo nějaké jiné terapie?**

Ano, pomocí léků i pomocí skupinové terapie, kdy jsme si v kruhu s ostatními pacienty povídali o svých problémech.

Praktikantka: **Jak byste se dnes zachovala v takovémto případě?**

Dnes bych se chovala již úplně jinak. Ale čas se vrátit nedá. Na jednu stranu mě to posilnilo, získala jsem nadhled. Dokonce teď spolupracuji s jednou organizací, která pomáhá obětem šikany.

Praktikantka: **Moc Vám děkuji za rozhovor a omlouvám se, pokud nějaké dotazy na Vás byly příliš osobní.**

4.4.3 Vyhodnocení rozhovorů

Jak z obou rozhovorů vyplývá, nejdůležitějším faktorem pro oba dotazované byla následná práce s psychiatrem a psychologem. Z rozhovoru s pachatelem kybernetické kriminality nic nenasvědčuje tomu, že by jeho chování směřovalo k násilí od mladého věku. Jak on sám řekl, jednalo se o zkratkovité jednání, které mu psycholog pomohl zpracovat a pochopit tak, aby nedošlo k recidivě.

Rozhovor s obětí kybernetické kriminality rovněž ukázal, že největší pomocí pro ni byla práce s psychologem. Oběť měla tendenci se uzavírat do sebe a bohužel až moc pozdě se svým případem svěřila psychologovi, který ji pomohl.

I zde se potvrdilo, jak důležitá je osvěta a šíření povědomí o problematice kybernetické kriminality, jak důležité je mezi lidi dostat informace, kam a na koho se mají v takových případech obrátit.

4.5 Dílčí závěr praktické části

Úvodem praktické části je námět na zlepšení právní úpravy v boji proti kybernetické kriminalitě (viz kapitola 4.1). Z námětu se jeví jako vhodné ustanovit

kybernetickou kriminalitu trestným činem. Dále z námětu vychází závěr, který kromě zlepšování a novelizací stávajících právních norem klade důraz na prevenci a osvětu o kybernetické kriminalitě mezi širokou veřejností napříč celou společností.

Součástí praktické části je dotazníkové šetření o povědomí o kybernetické kriminalitě u žáků 2. stupně základní školy (viz kapitola 4.2.). Výsledky šetření byly uspokojivé, neboť na otázku „ Měli jste ve škole přednášku na téma nebezpečí přicházející z internetu“ odpovědělo kladně 96 ze 100 dotázaných. To potvrzuje hypotézu z kapitoly 4.1., kde je stěžejním pilířem pro boj s kybernetickou kriminalitou je uvedena právě osvěta.

Další součástí praktické části je případová studie. Šetření bylo provedeno na konkrétním případu kybernetické šikany z pohledu oběti, která byla pod útokem cyberstalkingu (viz kapitola 3.4.1.). Případová studie byla provedena zejména jako doplňková metoda této práce, aby přiblížila problém kybernetické šikany v reálném životě. Výsledkem tohoto šetření byla rovněž osvěta (viz kapitola 4.1.)

Závěrem praktické části jsou řízené rozhovory s obětí a pachatelem kybernetické kriminality. Z obou rozhovorů vyplývá, že důležitým faktorem pro oba dotazované byla práce s odborníkem. To rovněž potvrzuje hypotézu z kapitoly 4.1., kde je navrženo, aby s oběťmi této trestné činnosti a potažmo i pachateli nadále pracoval zkušený psycholog či psychiatr. Zároveň by se s ohledem na oběť jevilo jako vhodné zlepšit právní úpravu chránící její práva, jak bylo zmíněno v kapitole 4.1.

5 Diskuze a výsledky

Vyhodnocením teoretických východisek byla zjištěná absence jednoznačně definovaného pojmu kybernetická kriminalita, jelikož odborná veřejnost v tomto ohledu přináší celou řadu odlišných pojetí. Ačkoli se na první pohled jeví jako vhodné pro tuto problematiku vytvořit jednotnou definici, z rešerše odborné literatury vyplynulo, že takové řešení je neefektivní, neboť by nebylo možné do jedné definice správně zakomponovat celou podstatu fungování kybernetické kriminality. Jde tudíž považovat za dostatečné několik opakujících se definičních kritérií (viz kapitola 3.1.1.).

V rámci analýzy platné právní úpravy (viz kapitola 3.7) bylo zjištěno, že v současné době není legislativa v rámci České republiky koncepční. Je to však z velké části pochopitelné, jelikož kybernetická kriminalita je relativně nový pojem a více než u jiných typů kriminality zde platí, že právní úprava se vytváří až na základě předešlých událostí. Může se proto stát, že pachatel kybernetického trestného činu nebude zapadat do žádné stávající skutkové podstaty. Přesnější a lépe terminologicky vysvětlené úpravy se kybernetická kriminalita na základě Úmluvy o kybernetické kriminalitě dočkala v novém trestním zákoníku č. 40/2009 Sb., avšak vzhledem k neustálému rozvoji informačních technologií a specifičnosti kyberprostoru je aplikace právních předpisů stále obtížná. Hlavním cílem právní úpravy by tedy mělo být zabránění situace, aby nějaký kybernetický trestný čin nebyl právně upraven nebo aby nebyla možnost ho objasnit.

Rozbor objasňování kybernetické kriminality (viz kapitola 3.8.) poukazuje na nepoměr mezi nahlášenými kybernetickými útoky a jejich skutečným počtem. Mnoho poškozených z důvodu udržení své důvěryhodnosti útok nenahlásí a tím se zvyšuje počet nepotrestaných pachatelů. S tím souvisí zákon o kybernetické bezpečnosti (viz kapitola 3.7.3.), na jehož základě mají některé instituce povinnost nahlásit kybernetický útok, který je následně posuzován příslušnými institucemi. Při objasňování kybernetických zločinů je velkým problémem prostor pro anonymitu, kterou virtuální svět umožňuje. Vyšetřovatelé musí vždy počítat s variantou, že trestný čin kybernetické kriminality nemusí být proveden jen jedincem ale i organizovanou skupinou. Je důležité odborníky v tomto odvětví kriminalistiky neustále zdokonalovat v jejich dovednostech, jelikož vynalézavost a technické

schopnosti pachatelů se také zdokonalují. Jednotlivé vyšetřovací úkony však musí být prováděny v souladu se zákonem.

Návrh na zlepšení právní úpravy v kapitole 4.1. je kompatibilní s prevencí (viz kapitola 3.9.). Samozřejmě je zde možnost vsadit na represi a podstatně zvýšit trestní sazby hrozící za tuto trestnou činnost, ale z kriminalistických statistik vychází, že zvýšení trestních sazeb u jakéhokoliv druhu kriminality nevede k jejímu potlačení či dokonce vymýcení. Prevence naproti tomu dokáže kybernetické kriminalitě a jejímu potencionálnímu rozšiřování zabránit. S prevencí je nerozdělitelně spjatá i osvěta. Návrhem na zlepšení právní úpravy by mělo být ustanovit kybernetickou šikanu, potažmo tradiční šikanu jako trestný čin, jelikož její rozšíření hlavně mezi dětmi nezadržitelně stoupá a je třeba toto jednání právně upravit i mezi nezletilými.

Pozitivní výsledek v tomto ohledu přineslo dotazníkové šetření (viz kapitola 4.2.), neboť ukázalo, že taková osvěta se praktikuje už od útlého věku. Již na základních školách fungují semináře a přednášky objasňující hrozby, které s sebou informační technologie a kyberprostor přinášejí. Naopak negativním výsledkem dotazníkového šetření bylo vysoké procento dětí, které se již s kybernetickou kriminalitou setkaly. I zde však byla znát působící prevence, jelikož na otázku „pokud se ti spolužák svěří, že ho někdo přes internet šikanuje, víš, kam ho máš poslat“ odpovědělo kladně 85 ze 100 dětí. Pro takové případy je zřízeno hned několik institucí, které mají obětem kybernetické kriminality pomáhat (viz kapitola 3.9.)

Šetřením případovou studií (viz kapitola 4.3.) byl rozebrán případ Adély, která se stala obětí kybernetické kriminality se znaky nebezpečného pronásledování (viz kapitola 3.4.1.). Adéla si ale tyto znaky neuvědomovala, nechtěla se svěřit policii a její případ tedy nebyl řešen jako trestný čin nebezpečné pronásledování. I v tomto případě se ukazuje, že je důležité povědomí o kybernetické kriminalitě stále šířit, aby oběti věděly, že jsou instituce, které jim mohou pomoc a není důvod cítit stud této pomoci využít.

Námětem na zlepšení byla rovněž užší spolupráce s psychology a psychiatry. Tuto hypotézy potvrdily řízené rozhovory s pachatelem a obětí kybernetické kriminality, neboť v obou případech byla návštěva takového odborníka nejdůležitější pomocí pro vyřešení jejich problému.

6 Závěr

Cílem této bakalářské práce bylo analyzovat kybernetickou kriminalitu a její právní úpravu v České republice. Informační a komunikační technologie jsou stále jeden z nejvíce dynamicky se rozvíjejících oborů a je třeba si uvědomit, že kromě různých pozitiv s sebou nesou i svou stinnou stránku.

Kybernetická kriminalita nemá dlouhou historii, avšak formy kybernetických trestných zločinů prošly značnou transformací. Od různých sabotáží a útoků na telefonní linky se dostaly až ke kyberterorismu a nebezpečnému pronásledování. Rozbor vybraných druhů kybernetické kriminality v teoretické části práce byl jen pouhou ukázkou toho, s jakými formami trestných zločinů je možné se v kyberprostoru setkat. Rešerše odborné literatury odhalila, že neexistuje jednotná definice pro tento druh kriminality. Je proto třeba pracovat s několika obecnými definičními kritérii, které objasňují chápání kybernetické kriminality jak se zřetelem na trestné činy páchané proti informačním technologiím, tak i trestné činy páchané s jejich využitím.

Právní úprava kybernetické kriminality je v České republice zakotvena zejména v trestním zákoníku a v zákoně o kybernetické bezpečnosti. Analýzou právní úpravy byla zjištěna nedokonalost koncepce legislativy v rámci České republiky. Je to zapříčiněné tím, že kybernetická kriminalita je stále relativně nový pojem a vzhledem k vysoké dynamice zdokonalování informačních a komunikačních technologií a potažmo i zdokonalování pachatelů se trestněprávní úprava formuje až v návaznosti na již vykonané činy. Aktualizace v oblasti kybernetické kriminality se právní úprava v České republice dočkala v roce 2009, kdy byl po téměř padesáti letech zaveden nový trestní zákoník. Kybernetické trestné činy jsou v něm upraveny na základě Úmluvy o kybernetické kriminalitě, kterou Česká republika podepsala v roce 2005. Trestní zákoník přesněji a s dokonalejší terminologií upravuje jednání v oblasti kybernetické kriminality, ale s ohledem na specifikaci a vysokou individualitu kyberprostoru je třeba zákony a vyhlášky stále novelizovat.

Rozbor objasňování kybernetické kriminality ukázal, že při vyšetřování trestných činů týkajících se této problematiky je potřeba tým specialistů, kteří jsou trénováni a školeni v oboru informačních a komunikačních technologií. Zásadním faktorem při objasňování je čas, je proto důležité, aby kriminalisté správně rozfázovali vyšetřovací plán a dali tak pachateli co nejmenší časový prostor k zametání stop. Zároveň byla odhalena

neúměrnost mezi ohlášenými a skutečně provedenými trestnými činy. V některých případech postižená osoba ani neví, že se stala obětí kybernetického trestného činu, nebo ho neohlásí, aby si zachovala svou důvěryhodnost. Takové jednání bylo časté například u velkých firem. Na to se zaměřil zákon o kybernetické bezpečnosti, který uvádí, že některé podniky mají povinnost kybernetické útoky hlásit příslušným institucím.

Z návrhu na zlepšení právní úpravy se jeví jako ustanovit kybernetickou šikanu, potencionálně šikanu tradiční trestným činem. Dále by byla vhodná rychlejší novelizace zákonů v tomto oboru a větší nadnárodní spolupráce. Návrhem byla i užší spolupráce s psychology a psychiatry, neboť jak vyznělo z řízených rozhovorů, právě oni byli důležitým článkem při práci s oběťmi a pachateli trestných činů. Dalším východiskem vyplývajícím z návrhu je prevence a výchova. Mohlo by se zdát efektivnější vsadit na represi a podstatně zvýšit trestní sazby hrozící za tuto trestnou činnost, ale jak bylo již dříve zjištěno z kriminalistických statistik, zvýšení trestních sazeb u jakéhokoliv druhu kriminality nevede k jejímu potlačení nebo vymícení. Prevence naproti tomu pomáhá s kybernetickou kriminalitou bojovat nebo se jí úplně vyhnout. Jedním z nejdůležitějších kroků k prevenci je výchova a osvěta. Pozitivní zprávu přineslo vyhodnocení z dotazníkového šetření, kde bylo zjištěno, že je snaha rozšířit povědomí o existenci kybernetické kriminality už od mladších generací. Fungují různé přednášky a semináře, které mají za cíl seznámit posluchače s možnostmi nebezpečí, které s sebou kyberprostor přináší a jak se takovému nebezpečí bránit.

7 Seznam použitých zdrojů

7.1 Monografie, publikace, sborníky

- BARTŮNĚK, Jan. *Kybernetická kriminalita*. Praha, 2014. Diplomová práce. Univerzita Karlova v Praze.
- BOCIJ, Paul. *Cyberstalking: harassment in the Internet age and how to protectyourfamily*. Westport, Conn.: Praeger, 2004. ISBN 0-275-98118-5.
- ČERNÁ, Alena. *Kyberšikana: průvodce novým fenoménem*. Praha: Grada, 2013. Psyché (Grada). ISBN 978-80-247-4577-0.
- ČÍRTKOVÁ, L. *Moderní psychologie pro právníky.* Praha: GradaPublishing, 2008. ISBN 978-80-247-2207-8
- ERIKSON, Erik. *Identity: Youth and crisis*. New York: W. W. Norton&Company, 1968.
- GŘIVNA, Tomáš; POLČÁK, Radim. *Kyberkriminalita a právo*, Vyd. 1. Praha: Nakladatelství Auditorium, Praha, 2008.
- GŘIVNA, Tomáš, Miroslav SCHEINOST a Ivana ZOUBKOVÁ. *Kriminologie*. 4., aktualiz. vyd. Praha: WoltersKluwer, 2014. ISBN 978-80-7478-614-3.
- JELÍNEK, Jiří. *Trestní právo hmotné: obecná část, zvláštní část*. Praha: Leges, 2009. Praktik (Leges). ISBN 9788087212240.
- JELÍNEK, Jiří. *Trestní právo hmotné: obecná část, zvláštní část*. Vyd. 2. Praha: Leges, 2010. Student (Leges). ISBN 978-80-8721-249-3.
- JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007. ISBN 978-80-247-1561-2.
- KAVALÍR, Aleš, ed. *Kyberšikana a její prevence: příručka pro učitele*. Plzeň: Pro město Plzeň zpracovala společnost Člověk v tísni, pobočka Plzeň, 2009. ISBN 978-80-86961-78-1.
- KOLÁŘ, Michal. *Nová cesta k léčbě šikany*. Praha: Portál, 2011. ISBN 978-80-7367-871-5.
- KOPECKÝ, K. *Stalking a kyberstalking*. Nebezpečné pronásledování. Olomouc: NET Universi-TY, s. r. o., 2010.
- KOPECKÝ, Kamil a Veronika KREJČÍ. *Rizika virtuální komunikace*. Olomouc: Net University, 2010. ISBN 978-80-254-7866-0.
- LEPIČOVÁ, Zuzana. *Kybernetická šikana jako fenomén nových médií*. České Budějovice, 2015. Diplomová práce. Jihočeská univerzita v Českých Budějovicích.
- MATĚJKA, Michal. *Počítačová kriminalita*. 1. vydání. Praha: ComputerPress, 2002.

- MCQUADE, Samuel C. *Encyclopediaofcybercrime*. Westport, Conn.: GreenwoodPress, 2009. ISBN 978-0-313-33974-5.
- MINÁRIK, Tomáš. *Trestněprávní aspekty počítačové kriminality*. Praha, 2007. Diplomová práce. Univerzita Karlova v Praze.
- PINKAVA, Jan. Počítačová kriminalita a softwarové pirátství z pohledu kriminalistiky a trestního práva. Olomouc, 2010. Diplomová práce. Univerzita Palackého v Olomouci.
- PTÁČEK, David. *Problematika počítačové kriminality*. Praha, 2010. Bakalářská práce. Bankovní institut vysoká škola.
- RAK, Roman. *Digitální stopy a jejich vlastnosti*. Data security management. Roč. XIV, 2010, č. 1.
- SAXENA, Dr. Manish. *Web Spamming - A Threat*. ResearchmaGma, 2017. ISBN 9781387015818.
- SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. Pro praxi. ISBN 978-80-7380-501-2.
- STEUER, Petr. *Počítačová kriminalita*. Brno, 2009. Bakalářská práce. Masarykova univerzita.
- ŠÁMAL, Pavel. *Trestní zákoník: komentář*. Praha: C.H. Beck, 2010. Velké komentáře. ISBN 978-80-7400-178-9.
- ŠEVČÍKOVÁ, Anna. *Děti a dospívající online: vybraná rizika používání internetu*. Praha: Grada, 2014. Psyché (Grada). ISBN 978-80-247-5010-1.
- VAŠUTOVÁ, Maria. *Proměny šikany ve světě nových médií*. Ostrava: Filozofická fakulta Ostravské univerzity v Ostravě, 2010. ISBN 978-80-7368-858-5.
- VITAL, Stan. *PhonePhreaking*. CreateSpace Independent PublishingPlatform, 2016. ISBN 9781537608471.
- VOLEVECKÝ, Petr. Kybernetické trestné činy v trestním zákoníku. Trestní právo č.7-8/2010
- WILLARD, Nancy E. Cyberbullying and cyberthreats: responding to thechallengeof online socialaggression, threats, and distress. Champaign, Ill.: ResearchPress, c2007. ISBN 978-0-87822-537-8.
- ZAPLETAL, J. a kolektiv Aktuální problémy kriminologie pro posluchače magisterského studijního programu, Praha, 2009.
- ZEMAN, Daniel. *Internetová kriminalita*. Praha, 2012. Rigorózní práce. Univerzita Karlova v Praze.

7.2 Právní předpisy

- Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších přepisů
- Zákon č. 121/2000 Sb., zákon o právu autorském, o právech souvisejících s právem autorskýma o změně některých zákonů (autorský zákon)
- Zákon č. 141/1961 Sb., zákon o trestním řízení soudním (trestní řád)
- Zákon č. 205/2017 Sb., zákon, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony

7.3 Elektronické prameny

- Agrese a šikana - osobnost agresora. In: *Portál prevence rizikového chování* [online]. 2017 [cit. 2018-01-14]. Dostupné z: http://www.prevence-praha.cz/agrese-a-sikana?start=3
- Co je to phreaking. In: *Správa sítě: slovník pojmů* [online]. 2016 [cit. 2018-01-14]. Dostupné z: https://www.sprava-site.eu/phreaking/
- Cyberstalking. In: *Epravo.cz* [online]. 2013 [cit. 2018-01-15]. Dostupné z: https://www.epravo.cz/top/clanky/cyberstalking-91552.html
- Česká republika po osmi letech ratifikovala Úmluvu o počítačové kriminalitě. In: *Právní rádce* [online]. 2013 [cit. 2018-01-14]. Dostupné z: https://pravniradce.ihned.cz/c1-60516560-ceska-republika-po-osmi-letech-ratifikovala-umluvu-o-pocitacove-kriminalite
- DIBLÍKOVÁ, Simona. Analýza trendů kriminality v České republice v roce 2015. In: *Institut pro kriminologii a sociální prevenci* [online]. 2016 [cit. 2018-01-15]. Dostupné z: http://www.ok.cz/iksp/docs/437
- Dodatkový protokol k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů. In: *CouncilofEurope* [online]. 2017 [cit. 2018-01-14]. Dostupné z: https://rm.coe.int/16804931bf
- DONÁT, Josef. Zákon o kybernetické bezpečnosti a navazující prováděcí předpisy. In: *Česká společnost pro systémovou integraci* [online]. 2015 [cit. 2018-01-13]. Dostupné z: http://www.cssi.cz/cssi/z%C3%A1kon-o-kybernetick%C3%A9-bezpe%C4%8Dnosti-navazuj%C3%ADc%C3%AD-prov%C3%A1d%C4%9Bc%C3%AD-p%C5%99edpisy
- Důvěřiví senioři se na internetu stávají kořistí šmejdů. In: *Novinky.cz* [online]. 2017 [cit. 2018-01-14]. Dostupné z: https://www.novinky.cz/domaci/454447-duverivi-seniori-se-na-internetu-stavaji-koristi-smejdu.html

- GLOGAR, Martin. Novela zákona o kybernetické bezpečnosti. In: *Právní prostor* [online]. 2017 [cit. 2018-01-13]. Dostupné z: https://www.pravniprostor.cz/zmeny-v-legislative/vyslo-ve-sbirce-zakonu/novela-zakona-o-kyberneticke-bezpecnosti
- GŘIVNA, Tomáš. Úmluva o kybernetické kriminalitě (soulad české právní úpravy s ustanoveními Úmluvy). In: *Europen.cz* [online]. 2010 [cit. 2018-01-14]. Dostupné z: https://www.europen.cz/Proceedings/32/Umluva%20o%20kyberneticke%20kriminalite.pdf
- Hacking. In: *Živě* [online]. 2017 [cit. 2018-01-14]. Dostupné z: https://www.zive.cz/hacking/sc-381/default.aspx
- Kriminalita v Česku klesla. Policie dokáže objasnit 97 procent vražd. In: *Deník.cz* [online]. 2017 [cit. 2018-01-15]. Dostupné z: https://www.denik.cz/z_domova/kriminalita-v-cr-loni-klesla-o-12-pct-na-217-927-trestnych-cinu-20170124.html
- KUCHTA, Josef. Aktuální problémy počítačové kriminality včetně její prevence. Časopis pro právní vědu a praxi. [Online]. 2016, č. 1, s. 5-19. [cit. 2018-01-14]. Dostupné z: https://journals.muni.cz/cpvp/article/view/5260
- MAREŠOVÁ, Alena. Analýza trendů kriminality v roce 2014. In: *Institut pro kriminologii a sociální prevenci* [online]. 2015 [cit. 2018-01-15]. Dostupné z: http://www.ok.cz/iksp/docs/425.pdf
- NEIDERMEIEROVÁ, Jana. Česko je první zemí na světě, kde začne platit zákon o kyberbezpečnosti. In: *Hospodářské noviny* [online]. 2014 [cit. 2018-01-13]. Dostupné z: https://domaci.ihned.cz/c1-62638370-cesko-je-prvni-zemi-na-svete-kde-zacne-platit-zakon-o-kyberbezpecnosti
- Pharming je zpět a silnější. In: *Lupa.cz* [online]. 2007 [cit. 2018-01-14]. Dostupné z: https://www.lupa.cz/clanky/pharming-je-zpet-a-silnejsi/
- Právo být zapomenut a rovnoprávnost v kyberprostoru. In: *RadioWave* [online]. 2016 [cit. 2018-01-14]. Dostupné z: https://wave.rozhlas.cz/pravo-byt-zapomenut-a-rovnopravnost-v-kyberprostoru-5209935
- Policie přiznává, že v boji proti kyberkriminalitě mají navrch hackeři. In: *Právní rádce* [online]. 2016 [cit. 2018-01-15]. Dostupné z: https://pravniradce.ihned.cz/c1-65479680-policie-priznava-ze-v-boji-proti-kyberkriminalite-maji-navrch-hackeri
- SMEJKAL, Vladimír. Kybernetická kriminalita - fenomén dneška. In: *Právní prostor* [online]. [cit. 2018-01-15]. Dostupné z: https://www.pravniprostor.cz/clanky/trestni-pravo/kyberneticka-kriminalita-fenomen-dneska

- SMEJKAL, Vladimír. Současné formy kybernetické kriminality a možnosti jejich postihu. In: *Institut pro kriminologii a sociální prevenci* [online]. 2017 [cit. 2018-01-14]. Dostupné z: http://www.ok.cz/iksp/docs/2016X_Smejkal.pdf
- ŠOSTÝ, Zbyněk. Autorský zákon - legislativa a bezpečnost v kyberprostoru. In: *Metodický portál* [online]. 2015 [cit. 2018-01-14]. Dostupné z: https://digifolio.rvp.cz/artefact/file/download.php?file=74218&view=11751
- VIČAR, Radim. Kybernetická kriminalita: Vybrané skutkové podstaty trestných činů ve vztahu k kybrnetické kriminalitě. In: *Univerzita obrany* [online]. 2017 [cit. 2018-01-15]. Dostupné z: https://moodle.unob.cz/pluginfile.php/20126/mod_resource/content/1/skutky.pdf
- Zákon o kybernetické bezpečnosti: co v něm stojí? In: *ROOT.cz* [online]. 2013 [cit. 2018-01-13]. Dostupné z: https://www.root.cz/clanky/zakon-o-kyberneticke-bezpecnosti-co-v-nem-stoji/
- Zpráva o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky v roce 2016. In: *Ministerstvo vnitra České republiky* [online]. 2017 [cit. 2018-01-14]. Dostupné z: http://www.mvcr.cz/clanek/zprava-o-situaci-v-oblasti-vnitrni-bezpecnosti-a-verejneho-poradku-na-uzemi-ceske-republiky-v-roce-2016.aspx

8 Přílohy

Příloha č. 1 – Dotazník – Povědomí žáků 2. stupně základní školy o kybernetické kriminalitě

Dobrý den,

ráda bych vás požádala o vyplnění následujících otázek, které mi pomůžou s mou bakalářskou prací. Dotazník je zcela anonymní, odpovídejte tedy prosím na otázky pravdivě. Zaškrtněte vždy jen jednu odpověď.

1. Víš, co je to šikana?

☐ Ano

☐ Ne

2. Víš co je to kybernetická šikana?

☐ Ano

☐ Ne

3. Setkal ses někdy s kybernetickou šikanou?

☐ Ano

☐ Ne

4. Znáš někoho, kdo někoho jiného kyberneticky šikanoval?

☐ Ano

☐ Ne

5. Byl jsi poučen/a o psaní osobních údajů (adresa, věk) na internet?

☐ Ano

☐ Ne

6. Pokud se ti spolužák svěří, že ho někdo šikanuje, víš, za kým ho máš poslat?

☐ Ano

☐ Ne

7. Měli jste ve škole přednášku na téma „Nebezpečí přicházející z internetu“?

☐ Ano

☐ Ne

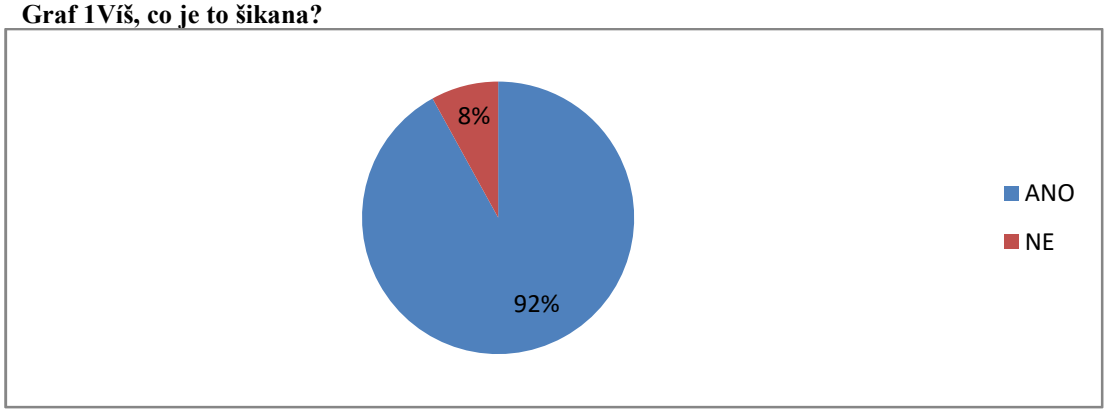
Děkuji vám za pomoc a přeji vám krásný zbytek dne.

Příloha č. 2 – Vyhodnocení dotazníku

Víš, co je to šikana?

Na první otázku odpovědělo kladně 20 dětí z 6 třídy, 23 ze 7 třídy, 24 dětí z 8 třídy a 25 dětí z 9 třídy. Opět při této odpovědi bylo kladných odpovědí velké množství, téměř všechny děti se setkaly s výrazem „šikana“. Byl by ale třeba podrobnější průzkum, zda žáci opravdu pojmu „šikana“ rozumí či jen ho zaslechly ve sdělovacích prostředcích.

Graf 1Víš, co je to šikana?

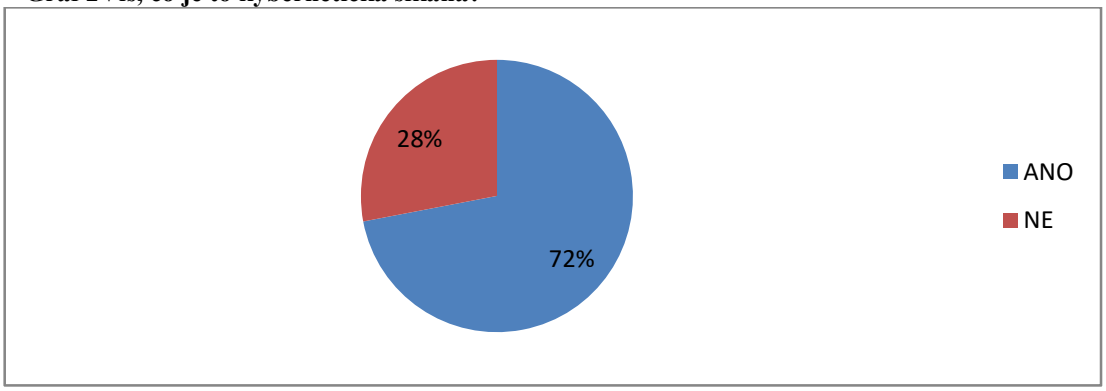


Zdroj: vlastní práce

Víš, co to je kybernetická šikana?

Na druhou otázku odpovědělo kladně 15 dětí z 6 třídy, 18 dětí ze 7 třídy, 19 dětí z 8 třídy a 20 dětí z 9 třídy. U této odpovědi již bylo podstatně méně kladných odpovědí, jednalo se zde o otázku na odborný výraz, který již děti základních škol neznají ze sdělovacích prostředků, a proto si z velké části nebyly jisté.

Graf 2Víš, co je to kybernetická šikana?

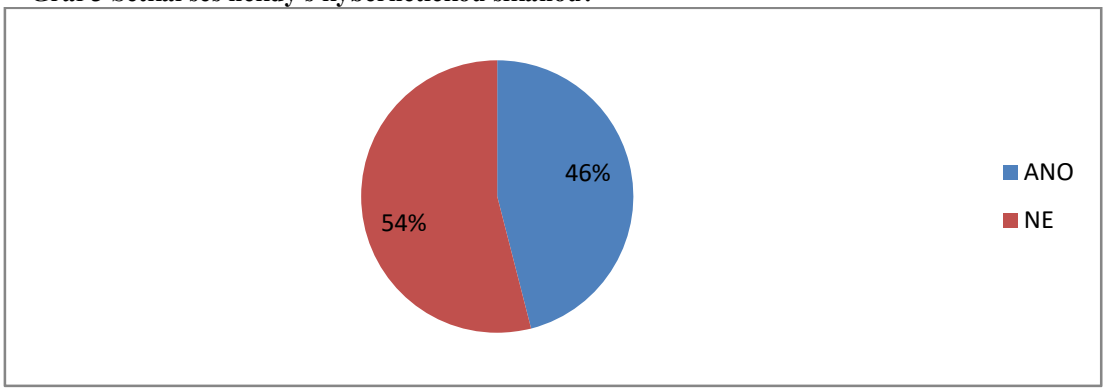


Zdroj: vlastní práce

Setkal ses někdy s kybernetickou šikanou?

Na třetí otázku odpovědělo kladně 10 dětí z 6 třídy, 11 dětí ze sedmé třídy, 13 dětí z 8 třídy a 12 dětí z 9 třídy. Je zde problematické, zda by takto staré děti v praxi dovedly rozlišit, co je to kybernetická šikana od běžného pošťuchování mezi spolužáky. Opět by zde byl na místě podrobnější dotazník, aby žáci třeba třemi větami popsali, jak taková kybernetická šikana v jejich životě vypadala.

Graf 3 Setkal ses někdy s kybernetickou šikanou?

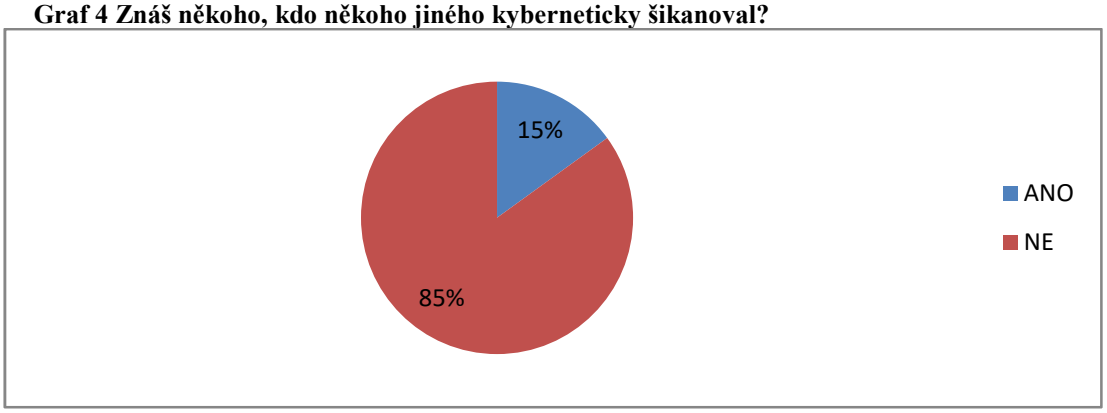


Zdroj: vlastní práce

Znáš někoho, kdo někoho jiného kyberneticky šikanoval?

Na čtvrtou otázku odpovědělo kladně 2 děti z 6 třídy, 4 děti ze 7 třídy, 3 děti z 8 třídy a 6 dětí z 9 třídy. Zde se projevila velká solidarita mezi dětmi, pravděpodobně nechtěli žáci udávat své kamarády, nebo se s takovou činností mezi sebou vzájemně nechlubí. Opět by zde bylo na místě položit podrobnější otázku při jiném typu dotazníkové akce.

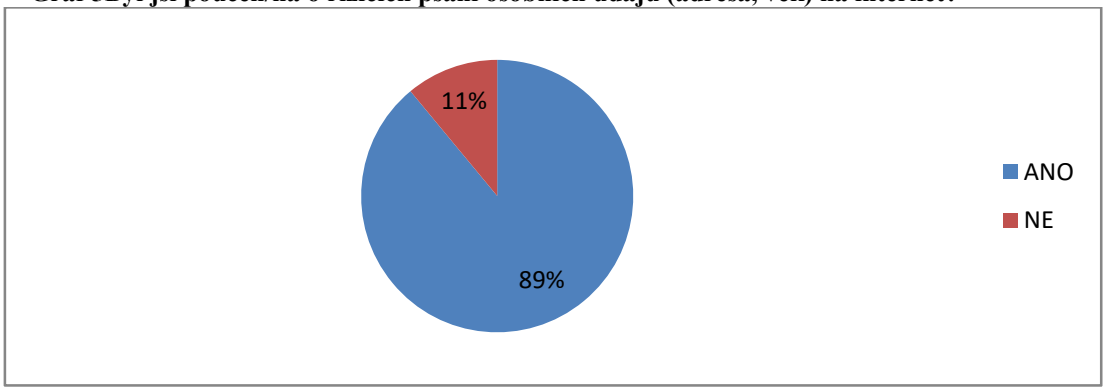
Graf 4 Znáš někoho, kdo někoho jiného kyberneticky šikanoval?



Byl jsi poučen/na o rizicích psaní osobních údajů (jména, adresy, věk) na FB

Na pátou otázku odpovědělo kladně 19 dětí z 6 třídy, 21 dětí ze 7 třídy, 24 dětí z 8 třídy a 25 dětí z 9 třídy. V těchto odpovědích byla opravdu znát působící prevence mezi dětmi základních škol i ze strany rodičů.

Graf 5Byl jsi poučen/na o rizicích psaní osobních údajů (adresa, věk) na internet?

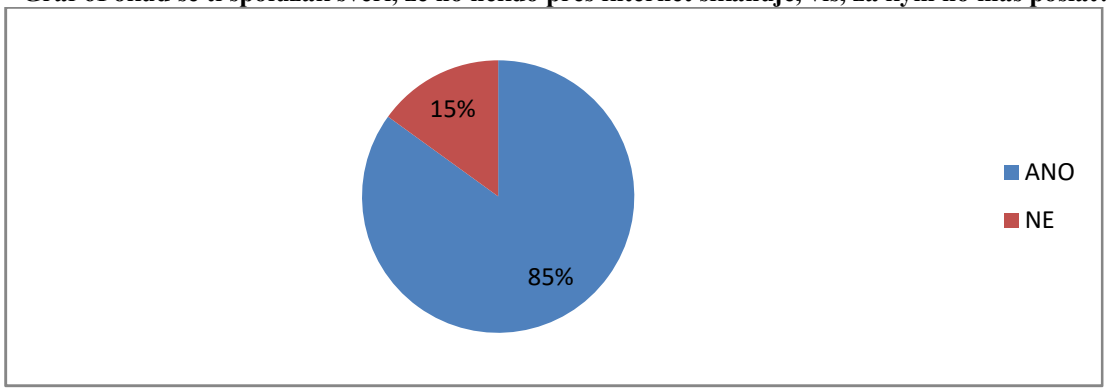


Zdroj: vlastní práce

Pokud se ti spolužák svěří, že ho někdo přes internet šikanuje, víš, za kým máš poslat?

Na šestou otázku odpovědělo kladně 18 dětí z 6 třídy, 20 dětí ze 7 třídy, 23 dětí z 8 třídy a 24 dětí z 9 třídy. Opět by zde byl třeba podrobnější typ dotazníku, abych mohla vyhodnotit, zda by žáci poslali svého spolužáka za tou pravou osobou, která by mu mohla pomoci.

Graf 6Pokud se ti spolužák svěří, že ho někdo přes internet šikanuje, víš, za kým ho máš poslat?



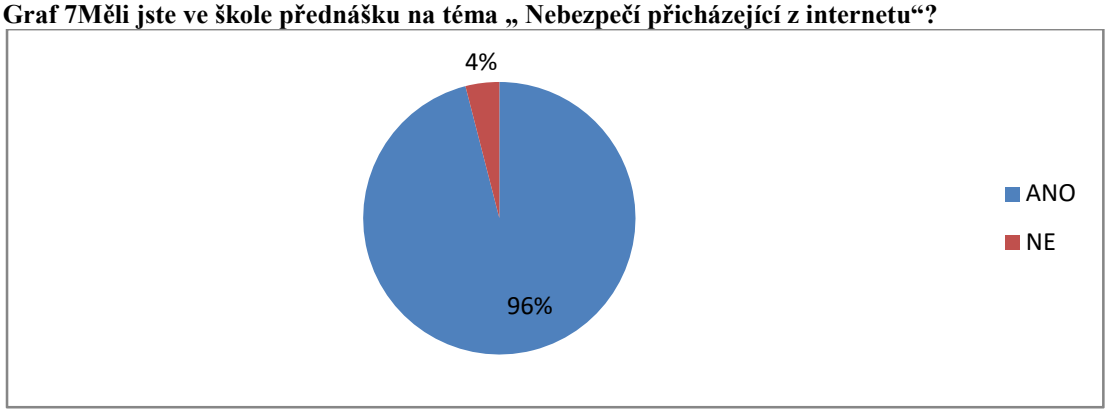
Zdroj: vlastní práce

Měly jste ve škole přednášku na téma „ Nebezpečí internetu“?

Na sedmou otázku odpovědělo kladně 24 dětí z 6 třídy, 22 dětí ze 7 třídy, 25 dětí z 8 třídy a 25 dětí z 9 třídy. S radostí jsem se dozvěděla, že základní školy neberou nebezpečí hrozící dětem na lehkou váhu a opravdu děti školí ohledně rozeznávání

nebezpečí přicházející z internetu. Měli jste ve škole přednášku na téma „ Nebezpečí přicházející z internetu“?

Graf 7Měli jste ve škole přednášku na téma „ Nebezpečí přicházející z internetu“?



Zdroj: vlastní práce

Příloha č. 3 – Poučení oběti o jejích právech

Základní informace pro oběť trestného činu

podle zákona **č. 45/2013 Sb.** o obětech trestných činů a změně některých zákonů

Jako oběť máte právo prohlásit, že nechcete informace podle tohoto zákona, ledaže jsou nutné k plnému uplatnění Vašich práv poškozeného v trestním řízení. Toto prohlášení můžete kdykoliv vzít zpět.

Oběť trestného činu: (§ 2)
Obětí je pouze fyzická osoba, které bylo nebo mělo být trestným činem

- ublíženo na zdraví,
- způsobena majetková i nemajetková újma,
- nebo na jejíž úkor se pachatel obohatil,
- byla-li trestným činem způsobena smrt oběti, považují se, utrpěli-li v důsledku smrti oběti újmu, za oběť též její příbuzný v pokolení přímém, sourozenec, osvojenec, osvojitel, manžel nebo registrovaný partner, druh nebo osoba, které oběť ke dni své smrti poskytovala nebo byla povinna poskytovat výživu.

Zvlášť zranitelná oběť: (§ 2)

a) dítě (osoba mladší 18 let)
b) osoba, která je vysokého věku nebo je postižena fyzickým, mentálním nebo psychickým handicapem nebo smyslovým poškozením,
c) oběť trestného činu obchodování s lidmi (§ 168 trestního zákoníku) nebo trestného činu teroristického útoku (§ 311 trestního zákoníku)
d) oběť trestného činu, který zahrnoval nátlak, násilí či pohrůžku násilím, trestného činu spáchaného pro příslušnost k některému národu, rase, etnické skupině, náboženství, třídě nebo jiné skupině osob nebo oběť trestného činu spáchaného ve prospěch organizované zločinecké skupiny, jestliže je v konkrétním případě zvýšené nebezpečí způsobení druhotné újmy.

Základní informace pro oběť (§ 8)

Prvotní informace důležité pro okamžitou pomoc a Vaše bezpečí.

A) Kontakt na policejní orgán (nebo státní zastupitelství), který je pro Vás nejvhodněji dostupný, pro účely podání trestního oznámení

.....
.....

Trestní oznámení bude potvrzeno:
- písemně s vyznačením: spisové značky, času a místa ohlášení trestného činu a základními okolnosti trestného činu, jako je jeho druh, čas a místo a způsobená škoda či újma,
- poskytnutím opisu protokolu o trestním oznámení.

Na stav řízení se můžete informovat u orgánu, kde jste podali trestní oznámení, nebo budete vyrozuměni o postoupení věci na jinou součást policie (státního zastupitelství), včetně konkrétní adresy a telefonního čísla.

B) Potřebujete-li odbornou pomoc psychologického a sociálního poradenství, právní pomoc, právní informace nebo informace o restorativních programech, obraťte se na subjekty zapsané v registru poskytovatelů pomoci obětem s žádostí o odbornou pomoc. Kontakt na tyto subjekty je přístupný na internetu (www.justice.cz), nebo Vám bude předán.
Kontakt:

……

……

Zvlášť zranitelná oběť může žádat o bezplatnou odbornou pomoc.

C) Je-li pachatel na svobodě, podle stupně nebezpečí budou přijata opatření k Vaší ochraně (§ 14):

- Policie ČR provede vykázání osoby ze společného obydlí, nebo Vám poskytne krátkodobou ochranu,
- soud vydá na Vaši žádost předběžné opatření v občanském soudním řízení,
- podle zvláštního předpisu Vám bude poskytnuta zvláštní ochrana svědka,
- podle trestního řádu (zákon č. 141/1961 Sb.) Vám bude poskytnuto utajení totožnosti i podoby svědka,
- podle trestního řádu bude vydáno předběžné opatření obviněnému v trestním řízení,
- justiční orgán vydá evropský ochranný příkaz a to ještě předtím, než odjedete do členského státu, v němž zamýšlíte pobývat.

Další informace si pozorně přečtěte, ústně Vám budou na Vaši žádost vysvětleny.

D) Po podání trestního oznámení obecně následují fáze:
Přípravné řízení - jeho úkolem je zadokumentovat případ tak, aby vedl k podání obžaloby nebo k jinému rozhodnutí. Dozor vykonává státní zástupce. Oběť většinou podává vysvětlení, vystupuje jako svědek, je poškozeným s nárokem na náhradu škody, kterou musí alespoň přibližně vyčíslit, může se zúčastnit znaleckého zkoumání. Po celou dobu má práva oběti.
Hlavní líčení - probíhá před soudem. Zde probíhá dokazování a rozhodování o vině a trestu; státní zástupce má roli žalobce, práva obžalovaného zajišťuje zpravidla, *ne vždy*, obhájce. Oběť bývá předvolána jako svědek a uplatňuje nárok na náhradu škody.
Vykonávací řízení - vykonání pravomocného rozsudku. Oběť může podat dovolání proti rozhodnutí soudu.

E) Informace v trestním řízení:
a) Policejní orgán, státní zástupce nebo soudce na **Vaši žádost** poskytne:

- informaci, že trestní řízení nebylo zahájeno,
- informaci o stavu trestního řízení,
- informaci o skutku, ze kterého byl pachatel obviněn,
- informaci o době a místě konání veřejného projednání věci v řízení před soudem,
- pravomocné rozhodnutí, kterým se trestní řízení končí.

b) Chcete-li být informováni o pobytu pachatele na svobodě (bude propuštěn, uprchne, bude změněn způsob jeho léčby nebo bude předán do cizího státu), Věznice, poskytovatel zdravotních služeb pro výkon ústavní ochranné léčby pachatele, nebo ústav pro výkon zabezpečovací detence pachatele Vám na **žádost** poskytnou informace a to do 24 hod od doby, kdy nastala oznamovaná skutečnost. **Žádost** se podává v přípravném řízení policejnímu orgánu, státnímu zástupci nebo soudu.

Pokud si žádost nepodáte, ale hrozilo by Vám nebezpečí, policejní orgán přijme opatření k zajištění Vašeho bezpečí.

F) Máte za podmínek stanovených zákonem právo na peněžitou pomoc poskytnutou Ministerstvem spravedlnosti (24), jste-li
a) obětí, které bylo v důsledku trestného činu ublíženo na zdraví,
b) osoba pozůstalá po oběti, která v důsledku trestného činu zemřela, byla-li osobou blízkou a současně v době jeho smrti s ním žila v domácnosti, nebo osoba, které zemřelý poskytoval nebo byl povinen poskytovat výživu,
d) oběť trestného činu v sexuální oblasti a dítě, které je obětí trestného činu týrání svěřené osoby (§ 198 trestního zákoníku), kterým vznikla nemajetková újma,
Více informací se dozvíte na kartě: Peněžitá pomoc podle zákona o obětech trestných činů.

G) Vyžaduje-li to situace, obraťte se na nejbližší azylové domy, intervenční centra či jiná zařízení sociálních služeb poskytující pobytové služby.
Kontakt:
……
……

H) Vyžaduje-li to situace, obraťte se na nejbližšího poskytovatele zdravotních služeb s žádostí o poskytnutí zdravotních služeb.
Kontakt:
……
……

I) Pokud Vám byla rozhodnutím nebo nesprávným úředním postupem orgánu veřejné moci způsobena škoda nebo nemajetková újma, uplatněte nárok na její náhradu (zákon č. 82/1998 Sb.). Újmu způsobenou Policií ČR nebo úřadem ve správním řízení řeší Ministerstvo vnitra; újmu způsobenou státním zastupitelstvím nebo soudem řeší Ministerstvo spravedlnosti.

J) **Oběť** má dále právo na

- respektování osobnosti a důstojnosti oběti a na zdvořilý a šetrný přístup (§ 3 odst. 2),
- opakované poskytnutí informací (§ 3 odst. 4),
- informace od subjektů zapsaných v registru poskytovatelů pomoci obětem trestných činů (§ 9),
- informace od orgánů veřejné moci a zdravotnických zařízení (§ 10),
- poskytnutí informací v jazyce, o němž oběť prohlásí, že mu rozumí, nebo v úředním jazyce státu, jehož je občanem (§ 12),
- ochranu před zveřejněním informací umožňujících zjištění totožnosti oběti (§ 15),
- ochranu osobních údajů oběti, tedy aby byly osobní údaje vedeny tak, aby se s nimi mohly seznamovat pouze oprávněné osoby (§ 16),
- učinění potřebných opatření k zabránění Vašeho kontaktu a osob Vám blízkým s podezřelým (§ 17),
- šetrné kladení otázek směřujících do intimní oblasti, popř. podání námitek proti takové otázce (§ 18 odst. 1),
- výslech osobou stejného nebo opačného pohlaví v přípravném řízení (§ 19),
- doprovod důvěrníkem (§ 21),
- prohlášení o dopadu trestného činu na Váš život (§ 22).

Zvlášť zranitelná oběť má dále právo na

- bezplatnou odbornou pomoc (§ 5 odstavec 1)
- na tlumočníka stejného nebo opačného pohlaví (§ 19 odstavec 2)
- právo na výslech provedený zvlášť citlivě s ohledem na konkrétní okolnosti, které Vás činí zvlášť zranitelnou obětí (§ 20 odstavec 1)
- v přípravném řízení právo na výslech osobou vyškolenou za tímto účelem (§ 20 odstavec 2)
- takové provedení výslechu, aby nemusel být později opakován (§ 20 odstavec 3)
- výslech stejnou osobou pro případ dalšího výslechu před týmž orgánem (§ 20 odst. 3),
- přijetí potřebných opatření k zabránění bezprostředního vizuálního kontaktu oběti s podezřelým (§ 20 odstavec 4)

Potvrzení
o převzetí poučení oběti trestného činu – základní informace

Byla mi předána základní informace pro oběť trestného činu a ústně sděleny prvotní informace ano - ne

.....

jméno, příjmení