POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY

V PRAZE

Fakulta bezpečnostně právní

Katedra kriminologie

Mládež a kyberkriminalita

Diplomová práce

Younth and Cybercrime

Diploma thesis

VEDOUCÍ PRÁCE

PhDr. Alena Marešová Ph. D.

AUTOR PRÁCE

Miroslav Dušek

PRAHA

2023

Čestné prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracoval pod vedením vedoucí diplomové práce samostatně a uvedl jsem všechny použité prameny a literaturu.

V Kutné Hoře, dne 09.03.2023 Miroslav DUŠEK

Poděkování

Děkuji vedoucí diplomové práce PhDr. Aleně Marešové Ph. D. za cenné rady, trpělivost a profesionální přístup.

ANOTACE

DUŠEK, Miroslav. *Mládež a kyberkriminalita.* Praha: Policejní akademie České republiky v Praze, 2023. 63 s. Diplomová práce.

Diplomová práce se zabývá problematikou mládeže a kyberkriminality, zejména povědomím mládeže o rizicích spojených s užíváním internetu, neboť se jedná o aktuální a velmi závažné téma.

V teoretické části jsou představena dosavadní zjištění a fakta v oblasti kyberkriminality se zvláštním zřetelem na problematiku kyberkriminality mládeže, která představuje cílovou skupinu diplomové práce.

V empirické části práce je prezentován průběh realizace a výsledky výzkumného šetření, jehož cílem bylo zjistit, jaké povědomí má mládež v oblasti kybernetické kriminality.

Klíčová slova: mládež, kyberkriminalita, internet

ANNOTATION

DUŠEK, Miroslav. *Youth and cybercrime*. Prague: Police Academy of the Czech Republic in Prague, 2023. 63 p. Diploma thesis.

This diploma thesis deals with the issue of youth and cybercrime, especially the awareness of youth about the risks associated with the use of the Internet, as it is a topical and very serious topic.

In the theoretical part, the existing findings and facts in the field of cybercrime are presented, with special attention to the issue of youth cybercrime, which represents the target group of the thesis.

In the empirical part of the thesis, the course of implementation and results of a research investigation are presented, the aim of which was to find out the awareness of youth in the field of cybercrime.

Keywords: youth, cybercrime, internet

Obsah

1 Úvod

Kyberkriminalita je velmi závažným celospolečenským problémem, který se projevuje setrvalým nárůstem počtu případů, každoročně se podíl trestných činů páchaných v kyberprostoru zvyšuje. Policisté na obvodních odděleních i na odděleních služby kriminální policie a vyšetřování denně řeší případy internetových podvodů, neoprávněných přístupů k počítačovým systémům, kyberstalkingu, kyberšikany, mravnostních deliktů a dalších případů páchaných v kybernetickém prostoru. Na nárůst počtu případů musí společnost reagovat. Je proto nutné přijmout řadu opatření, která mají pomoci v boji proti kyberkriminalitě. Vzhledem k tomu, že kyberprostor je anonymní prostředí a technologie se každým dnem zdokonalují, není vůbec snadné tyto případy odhalit a vyšetřit. V loňském roce začala proto vznikat v rámci policie nová oddělení, v nichž jsou policisté zaměřeni právě na problematiku trestné činnosti páchané ve virtuálním prostoru a na tento druh trestné činnosti jsou speciálně školeni.

Vzhledem k tomu, že moderní technologie hojně využívají nejen dospělí, ale rovněž děti a mladiství, objevuje se ve statistikách obětí i pachatelů kyberkriminality bohužel i tato věková skupina. Je to způsobeno tím, že mládež není o kyberkriminalitě dostatečně informována a stává se tak snadnou obětí internetových predátorů? Nebo bere rizika a hrozby na lehkou váhu a počíná si ve virtuálním světě neopatrně? Jakým způsobem vůbec mládež tráví na internetu volný čas? Na uvedené otázky se zaměřuje výzkumné šetření této diplomové práce. Diplomová práce se věnuje problematice mládeže a kyberkriminality, jejím hlavním cílem bylo zjistit, jaké povědomí má mládež o rizicích spojených s užíváním internetu. Tyto informace jsou velmi důležité při tvorbě preventivních programů a opatření, neboť je potřeba co nejrychleji zasáhnout, a to jak případnou represí, tak i preventivně proti dalšímu šíření jevu. Cílená prevence je v této oblasti velmi důležitá, neboť může výrazně napomoci snížení počtu obětí kybernetické kriminality.

2 Kyberkriminalita

Kyberkriminalita se stala součástí naší společnosti v době, kdy se začaly používat počítače. Dalším mezníkem byl vznik počítačových sítí, především sítě Internet a možnosti vzdáleného přístupu k počítačům. K dalšímu rozmachu kyberkriminality napomohl příchod mobilních telefonů, které přináší ještě vyšší míru rizika při páchání trestné činnosti.[1] Mobilní technologie způsobily revoluci ve způsobu, jakým přistupujeme k internetu. Mobilní telefon rychle přestal být nástrojem, který by sloužil pouze k telefonování, ale stal se sám o sobě počítačem.[2] Za poslední desetiletí došlo ke strmému nárůstu kyberkriminality. V roce 2020 bylo prostřednictvím internetu i jiných sociálních sítí spácháno 8 073 skutků. Oproti předchozímu roku tak došlo k poklesu o 344 skutků (- 4,1 %). Nejčastěji dochází k páchání podvodů mezi soukromými osobami (3 368 skutků), zde byl zaznamenán meziroční pokles o 45 skutků, následuje poškození a zneužití záznamu na nosiči informací, kdy bylo registrováno 1 160 skutků, přičemž meziročně došlo k navýšení o 230 případů. Dále bylo evidováno 709 skutků spáchaných v oblasti úvěrových podvodů, i zde byl zaznamenán meziroční pokles o 112 skutků. Nezanedbatelnou měrou se na kyberkriminalitě podílí také mravnostní trestné činy, evidováno bylo 709 skutků, přičemž rovněž došlo k meziročnímu poklesu a to o 87 skutků. Přestože, rok 2020 ve statistikách vykazuje pokles trestné činnosti spáchané v prostředí internetu, je nutné uvést, že tato trestná činnost měla do 31.8.2020 stoupající tendenci. V období do srpna roku 2019 bylo spácháno 5 080 skutků, v témže období v roce 2020 to bylo 5 600 skutků. Pokles trestné činnosti na internetu v posledním čtvrtletí tak lze zřejmě přičítat skutečnosti, že došlo ke změně výše škody, pro trestně právní posouzení

[1] *Bezpečný středočeský kraj*. [online]. [cit. 2022-12-03]. Dostupné z: Bezpečný Středočeský Kraj | Kyberkriminalita | PČR - Bezpečný Středočeský Kraj (bezpecnystredoceskykraj.cz).

[2] GILLESPIE A. *Alisdair. Cybercrime: Key Issues and Debates*. [online]. [cit. 2022-12-03]. Dostupné z: https://books.google.cz/books?id=0N4sCgAAQBAJ&pg=PA3&dq=cybercrime&hl=cs&sa=X&ved=2ahUKEwjGr6-q4sf8AhX-gP0HHedpCSoQ6AF6BAgGEAI#v=onepage&q=cybercrime&f=false.

z 5 na 10 tisíc korun.[3]

V oblasti kyberkriminality je značná latence, i když do statistik jsou zahrnovány skutky napříč všemi úrovněmi Policie ČR. Kybernetické útoky byly také zaměřeny do oblasti zdravotnictví, kde bylo provedeno několik útoků na nemocniční zařízení. Příkladem je útok z března roku 2019 na Fakultní nemocnici Brno, při kterém vznikla škoda v desítkách milionů korun a toto zařízení přišlo o některá administrativní a ekonomická data. Takovéto útoky probíhají na vysoce profesionální úrovni a jsou prováděny tzv. kombinovaným útokem. V první fázi je napaden vlastní počítačový systém aplikací malware, následně ve druhém kroku dochází k zašifrování dostupných počítačových systémů. Při vyžadování výkupného pachatelé v převážné většině požadují platby v kryptoměně bitcoin.[4]

Lze předpokládat, že s rozvojem současných a vývojem nových informačních technologií bude kybernetická trestná činnost prostupovat všemi kriminálními problematikami, jelikož řada činností probíhá v kyberprostoru. V dalších letech, stejně jako v těch minulých lze očekávat kybernetické útoky s jednoznačným cílem majetkového prospěchu. I nadále přetrvává trend trestněprávních aktivit v prostředí darknetu. Odhalování této trestné činnosti je velice náročné, nejen z hlediska času, ale také z hlediska finančních i lidských zdrojů. Systém darknetu je rozsáhlý, umožňující anonymní komunikaci např. v souvislosti s vydíráním subjektů. Na území ČR jsou na tzv. tržištích nabízeny různé služby sloužící k objednání průniku do počítačového systému třetích osob, případně je možné nelegálně získaná data vystavit na uvedeném marketu k prodeji. Anonymní komunikace a platby realizované ve virtuální měně v prostředí darknetu tak představují velmi významné hrozby.[5] V roce 2021 již bylo evidováno přes 9 500 skutků spáchaných v kyberptostoru,[6] ani toto číslo nemusí být konečné, jelikož

---

[3] *ZPRÁVA O SITUACI V OBLASTI VNITŘNÍ BEZPEČNOSTI A VEŘEJNÉHO POŘÁDKU NA ÚZEMÍ ČESKÉ REPUBLIKY V ROCE 2020*. [online]. [cit. 2023-02-03]. Dostupné z: https://prevencekriminality.cz/zprava-o-situaci-v-oblasti-vnitrni-bezpecnosti-a-verejneho-poradku-.na-uzemi-cr-v-roce-2020/.

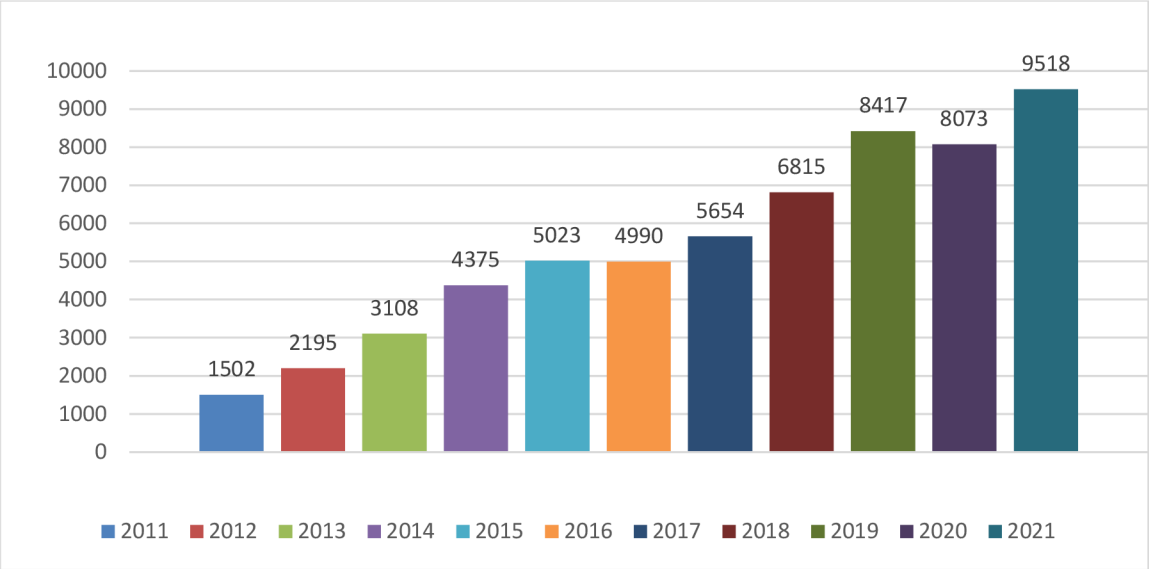
[4] Tamtéž.

[5] Tamtéž.

[6] *Kyberkriminalita na vzestupu*. [online]. [cit. 2022-12-03]. Dostupné z: https://echo24.cz/a/SiF29/hackeri-kyberneticka-kriminalita-zlociny-policie-ncoz-internet.

trestná činnost páchaná v kyberprostoru může být až z 90 procent latentní.[7]

Graf 1: Vývoj kybernetické kriminality 2011–2021.



Zdroj: https://www.policie.cz/clanek/statistika-kyberkriminality.aspxs.

2.1 Pojem kyberkriminalita

Pojem kyberkriminalita je odvozen od pojmu kyberprostor. Kyberprostorem se rozumí virtuální prostředí, jež nemá začátek ani konec, není omezen na hranice států a jeho rozsah nelze určit. Dříve byla kyberkriminalita označována jako počítačová kriminalita.[8]

Počítačová kriminalita byla v roce 1995 definována jako „*páchání trestné činnosti, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení včetně dat, nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď: a) jako předmět této trestné činnosti, ovšem s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité, nebo*

[7] *Bezpečný středočeský kraj*. [online]. [cit. 2022-12-03]. Dostupné z: Bezpečný Středočeský Kraj | Kyberkriminalita | PČR - Bezpečný Středočeský Kraj (bezpecnystredoceskykraj.cz)
[8] *Rozcestník kyberkriminality* [online]. [cit. 2022-12-02]. Dostupné z:Rozcestník kyberkriminality – Prevence kriminality.

b) jako nástroj trestné činnost".[9]

V současnosti je počítačový zločin popsán českou technickou normou jako *„zločin spáchaný pomocí systému zpracování dat nebo počítačové sítě nebo přímo s nimi spojený".* Tato definice směřuje k novému označení této trestné činnosti jako kybernetické kriminalitě. V současné době již nejsou útoky omezeny na jeden či více počítačů fixně propojených mezi sebou, ale probíhají v kyberprostoru tvořeném počítačovými sítěmi a jednotlivými prvky těchto sítí, které mají přidělenou svoji IP adresu. Komunikace probíhá prostřednictvím TCP/IP nebo jiného protokolu v kyberprostoru.[10] Obecně můžeme kyberkriminalitu chápat jako jednání namířené proti počítačovému systému, počítačové síti, uživatelům či datům, při kterém počítačový systém slouží jako nástroj pro spáchání trestného činu. Aby bylo možné uplatnit definici kyberkriminality, je zde fakt, že kyberprostor je prostředím, ve kterém se tato činnost odehrává. Kybernetická trestná činnost představuje nejširší množinu veškeré trestné činnosti, ke které dochází v prostředí informačních a komunikačních technologií. Často je běžná trestná činnost přenášena do kyberprostoru, jelikož zde je možné tuto činnost páchat rychleji a efektivněji (např. podvody). Ne každý kybernetický útok musí být trestným činem, avšak každý kybernetický trestný čin musí být rovněž kybernetickým útokem. Díky absenci trestněprávní normy je možné řadu kybernetických útoků subsumovat pod jednání, které bude mít povahu správně právního či občanskoprávního deliktu, může se také jednat o jednání, které není postižitelné jakoukoliv právní normou, tedy se může jednat pouze o nemorální, či netolerované jednání.[11]

Kybernetický útok (CyberAttack) lze chápat jako jakékoliv úmyslné jednání útočníka v kyberprostoru směřující proti zájmům jiného. Také je možné jej definovat jako jednání útočníka či celé skupiny útočníků, kteří využívají informační a komunikační technologie k útoku na jinou komunikační a informační infrastrukturu s cílem narušit dostupnost, důvěrnost nebo integritu dat. Je třeba

---

[9] VÁLKOVÁ Helena, Josef KUCHTA, Jana HULMÁKOVÁ a kol. *Základy kriminologie a trestní politiky*. 3. vydání 2019, 664 s. Praha: Nakladatelství C. H. Beck, ISBN 978-80-7400-732-3, str. 542.

[10] Tamtéž, 542.

[11] KOLOUCH Jan, Pavel Bašta. *CyberSecurity*. Praha: CZ.NIC,2019. ISBN 978-80-88168-31-7 str. 83.

také rozlišovat mezi kybernetickým bezpečnostním incidentem a kybernetickým útokem, který spočívá v zavinění. Ke kybernetickému bezpečnostnímu incidentu může dojít jak úmyslným, tak nedbalostním jednáním člověka, popřípadě zásahem vyšší moci. Kybernetický útok je vyvolán úmyslným jednáním člověka.[12]

Pojem kyberprostor (angl. cyberspace) původem z literární tvorby, umělecké pojetí však nemá nic společného se současným chápáním kyberprostoru, intuitivně jej chápeme jako nehmotný svět informací, vznikající vzájemným propojením komunikačních a informačních systémů. V tomto prostředí je možné vytvářet, uchovávat, využívat a vzájemně si vyměňovat informace a je uskutečňováno prostřednictvím počítačů připojených do komunikačních sítí v celosvětovém formátu, zejména v rámci sítě Internet.[13]

Zákon o kybernetické bezpečnosti č. 181/2014 Sb. v § 2 písm. a) uvádí, že „*kybernetickým prostorem se rozumí digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací*“.[14]

Kybernetickou bezpečností se rozumí proces, schopnost či způsobilost chránit informační a komunikační systémy a informace v nich obsažené před poškozením či neoprávněným použitím.[15]

Viry, trojští koně a červi, představují škodlivý software, kterému mnoho jedinců z široké veřejnosti nerozumí. Problém bývá v identifikaci různorodého spektra malwaru. Pomocí virů, trojských koní a červů nejčastěji dochází ke změnám funkcí počítačových programů, poškození dat, či jejich krádeži.[16]

---

[12] KOLOUCH Jan, Pavel Bašta. *CyberSecurity*. Praha: CZ.NIC,2019. ISBN 978-80-88168-31-7 str. 82.

[13] VÁLKOVÁ Helena, Josef KUCHTA, Jana HULMÁKOVÁ a kol. *Základy kriminologie a trestní politiky*. 3. vydání 2019, 664 s. Praha: Nakladatelství C. H. Beck, ISBN 978-80-7400-732-3, str. 543.

[14] Zákon č. 181/2014 Sb. *Zákon o kybernetické bezpečnosti* v posledním znění § 2.

[15] NAM H Nguyen. *Essential Cyber Secutity Handbook*. 2018. [online] [cit. 2022-12-03] Dostupné z: Essential Cyber Security Handbook In Slovak - Nam H Nguyen - Knihy Google.

[16] HOLT J. Thomas and Adam M. Bossler. *Cybercrime and Digital Forensics: An Introduction*. [online]. [cit. 2022-12-03]. Dostupné z: Cybercrime and Digital Forensics: An Introduction - Thomas J. Holt, Adam M. Bossler, Kathryn C. Seigfried-Spellar - Knihy Google.

2.2 Druhy kyberkriminality

Mezi nejzávažnější trestnou činnost páchanou v kyberprostoru patří dětská pornografie. Pro mnoho lidí je dětská pornografie synonymem k Internetu. Není to zcela na místě, neboť zneužívání dětí pro výrobu pornografie se dělo dávno před vznikem Internetu, avšak díky Internetu je možné její šíření účinným a do jisté míry anonymním způsobem. Z tohoto důvodu vzniklo propojení těchto pojmů, ovlivňující konstrukci právních norem Evropské unie i České republiky. Proto trestní zákoník obsahuje § 192 – 193b ve tvaru, jak je uvedeno níže:[17]

§192 Výroba a jiné nakládání s dětskou pornografií

1) Kdo přechovává fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě nebo osobu, jež se jeví být dítětem, bude potrestán odnětím svobody až na dva roky.
2) Stejně bude potrestán ten, kdo prostřednictvím informační nebo komunikační technologie získá přístup k dětské pornografii.
3) Kdo vyrobí, doveze, vyveze, proveze, nabídne, činí veřejně přístupným, zprostředkuje, uvede do oběhu, prodá nebo jinak jinému opatří fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě nebo osobu, jež se jeví být dítětem, anebo kdo kořistí z takového pornografického díla, bude potrestán odnětím svobody na šest měsíců až tři léta, zákazem činnosti nebo propadnutím věci.
4) Odnětím svobody na dvě léta až šest let nebo propadnutím majetku bude pachatel potrestán, spáchá-li čin uvedený v odstavci 3
a) jako člen organizované skupiny,
b) tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem, nebo
c) v úmyslu získat pro sebe nebo pro jiného značný prospěch.
5) Odnětím svobody na tři léta až osm let nebo propadnutím majetku bude pachatel potrestán, spáchá-li čin uvedený v odstavci 3

---

[17] SMEJKAL Vladimír. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015. ISBN 978-80-7380-501-2, str. 192.

a) jako člen organizované skupiny působící ve více státech, nebo
b) v úmyslu získat pro sebe nebo pro jiného prospěch velkého rozsahu.

§ 193 Zneužití dítěte k výrobě pornografie

1) Kdo přiměje, zjedná, najme, zláká, svede nebo zneužije dítě k výrobě pornografického díla nebo kořistí z účasti dítěte na takovém pornografickém díle, bude potrestán odnětím svobody na jeden rok až pět let.
2) Odnětím svobody na dvě léta až šest let bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1
a) jako člen organizované skupiny, nebo
b) v úmyslu získat pro sebe nebo pro jiného značný prospěch.
3) Odnětím svobody na tři léta až osm let bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1
a) jako člen organizované skupiny působící ve více státech, nebo
b) v úmyslu získat pro sebe nebo pro jiného prospěch velkého rozsahu.

§ 193a Účast na pornografickém představení

Kdo se účastní pornografického představení nebo jiného obdobného vystoupení, ve kterém účinkuje dítě, bude potrestán odnětím svobody až na dvě léta.

§ 193b Navazování nedovolených kontaktů s dítětem

Kdo navrhne setkání dítěti mladšímu patnácti let v úmyslu spáchat trestný čin podle § 187 odst. 1, § 192, 193, § 202 odst. 3 nebo jiný sexuálně motivovaný trestný čin, bude potrestán odnětím svobody až na dvě léta.[18]

Pornografickým dílem zobrazujícím dítě (to znamená osobu mladší osmnácti let), se rozumí např. snímky obnažených dětí v polohách vyzývavě předvádějících pohlavní orgány za účelem sexuálního uspokojení, rovněž také snímky dětí v polohách skutečného či předstíraného pohlavního styku s nimi, nebo i jiné obdobně sexuálně dráždivé snímky dětí. Aby dílo zobrazující dítě mohlo být podle

[18] Zák. č. 40/2009 Sb., *trestní zákoník* v posledním znění § 192 – 193b.

trestního zákoníku považováno za pornografické, je třeba, aby byly kumulativně splněny dvě základní charakteristiky, zaprvé musí u normálního jedince vyvolávat aktualizaci sexuálního pudu, zadruhé překračovat uznávané morální normy příslušné společnosti. Jak již bylo uvedeno výše, za takové jsou považovány snímky obnažených dětí v polohách vyzývavě předvádějících pohlavní orgány za účelem sexuálního uspokojení, rovněž také snímky dětí v polohách skutečného či předstíraného pohlavního styku s nimi, nebo i jiné obdobně sexuálně dráždivé snímky dětí.[19]

Mezi další trestné činy páchané v kyberprostoru, jejichž účastníky jsou děti, patří nebezpečné vyhrožování a nebezpečné pronásledování.

§ 353 Nebezpečné vyhrožování

1) *Kdo jinému vyhrožuje usmrcením, těžkou újmou na zdraví nebo jinou těžkou újmou takovým způsobem, že to může vzbudit důvodnou obavu, bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti.*
2) *Odnětím svobody až na tři léta nebo zákazem činnosti bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1*
a) *jako člen organizované skupiny,*
b) *vůči dítěti nebo těhotné ženě,*
c) *se zbraní,*
d) *na svědkovi, znalci nebo tlumočníkovi v souvislosti s výkonem jejich povinnosti, nebo*
e) *na zdravotnickém pracovníkovi při výkonu zdravotnického zaměstnání nebo povolání směřujícího k záchraně života nebo ochraně zdraví nebo na jiném, který plnil svoji obdobnou povinnost při ochraně života, zdraví nebo majetku vyplývající z jeho zaměstnání, povolání, postavení nebo funkce nebo uloženou mu podle zákona.*[20]

---

[19] SMEJKAL Vladimír. *Kybernetická kriminalita.* Plzeň: Aleš Čeněk, 2015. ISBN 978-80-7380-501-2, str. 198.
[20] Zákon č. 40/2009 Sb., *trestní zákoník* v posledním znění.

K vyhrožování dochází za fyzické přítomnosti fyzické osoby a také distančním způsobem, např. poštou, nástroji elektronických komunikací, případně nápisy na budovách, plotech apod. Elektronické vyhrožování dnes neprobíhá pouze přes email, ale také přes SMS a MMS zprávy či jiné nástroje pro internetovou komunikaci Facebook, WhatsApp apod. Vyhrožování musí způsobit důvodnou obavu, kterou se rozumí vyšší stupeň tísnivého pocitu z jednání, kterým je vyhrožováno. Důvodná obava vzniknout nemusí, ale její vznik musí být reálný, proto je třeba maximálně hodnotit povahu a závažnost vyhrožování, jelikož je třeba odlišit nebezpečné vyhrožování od jednání, při kterém bylo pouze použito silných slov. Vždy je třeba posuzovat konkrétní okolnosti případu, zejména k povaze výhružky, k fyzickým a charakterovým vlastnostem pachatele ve srovnání s fyzickými a povahovými vlastnostmi poškozeného a jejich vzájemném vztahu. Zda se jedná o výhružky způsobilé vzbudit důvodnou obavu lze posoudit na základě kompletního zhodnocení situace.[21]

§ 354 Nebezpečné pronásledování

1) Kdo jiného dlouhodobě 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,
d) omezuje jej v jeho obvyklém způsobu života, nebo
e) 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.
2) Odnětím svobody na šest měsíců až tři roky bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1
a) vůči dítěti nebo těhotné ženě,

---

[21] SMEJKAL Vladimír. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015. ISBN 978-80-7380-501-2, str. 272.

b) se zbraní, nebo
c) nejméně se dvěma osobami.

Pro nebezpečné pronásledování je v současné době často užívaným výrazem stalking. Pojem stalking byl poprvé použit v 90. letech v USA k označení určitého komplexu charakteristik lidského jednání. Tento pojem se v odborné, zejména pak v psychiatricky a psychologicky zaměřené literatuře vžil, rozumí se jím způsob chování pachatele, který se zaměřuje na jiného člověka, po kterém vyžaduje kontakt, obtěžuje a pronásleduje jej, vyhrožuje mu, často dochází i k fyzickému napadání a ve výjimečných případech jej i usmrtí. Pachatel svým jednáním vyvolává u oběti pocity strachu. Stalking lze rozdělit na dvě kategorie, zaprvé, zda se jedná o pronásledování vyvolané v důsledku předchozího, nebo stále trvajícího intimního partnerského vztahu, zadruhé o jednání, kde objektem se stane víceméně cizí člověk. V první skupině stalkerů je motivem pronásledování snaha udržet kontrolu a moc nad obětí za každou cenu, pro druhou skupinu je charakteristická neschopnost reálného úsudku a utkvělá představa o vztahu s prominentní osobou, která však nemá se skutečností nic společného a jedná se pouze o výplod chorobné posedlosti a z ní vyplývající fixace na povrchně známou osobu. Specifickým druhem stalkingu je jeho nová virtuální podoba nazývaná cyberstalking, která zahrnuje aktivity, kterými mohou být nevyžádané e-maily, rozesílání negativních zpráv přes chat, blog apod., jenž poškozují dobrou pověst oběti, zasílání spamů a záměrné útoky na data v počítači oběti (zavirování, nepřípustné získávání osobních dat atd.). Může dojít také ke kombinaci forem stalkingu např. telefonní a virtuální teror, což může zapříčinit devastující dopad na psychiku oběti.[22]

2.3 Kybernetické útoky na sociálních sítích

Co je sociální síť? Sociální sítí (anglicky social network) rozumíme propojenou skupinu lidí. V širším smyslu sociální sítí rozumíme každou skupinu lidí, která

[22] SMEJKAL Vladimír. *Kybernetická kriminalita.* Plzeň: Aleš Čeněk, 2015. ISBN 978-80-7380-501-2, str. 273.

spolu komunikuje různými prostředky.[23] V užším významu sociální sítí rozumíme internetovou službu, umožňující svým členům vytvářet veřejné, uzavřené nebo firemní profily, prezentace, diskusní fóra, a dále poskytuje prostor pro sdílení fotografií, videí a další aktivity. Převážnou část obsahu na sociálních sítích tvoří uživatelé prostřednictvím svých příspěvků, veřejnou komunikací apod. Mezi oblíbená patří tematická diskusní fóra, tematické skupiny, kde si lidé vyměňují názory na různá témata (koníčky, politika, sex).[24] Mezi neuživateli sociálních sítí je rozšířen názor, že sociální sítě jsou používány převážně generací teenagerů, což neodpovídá skutečnosti. V současné době, převažuje skupina dospělých uživatelů.[25] Mezi první sociální síť se řadí projekt Sixdegres, který byl spuštěný v roce 1997. Uživatelé zde měli možnost vytvořit si svůj osobní profil a dále seznám přátel. Později bylo možné procházet i seznamy přátel svých přátel. Služba byla ukončena v roce 2000. Dle zakladatele této služby nebyl projekt úspěšný, a to z důvodu, že předběhl svou dobu. Na konci 90 let byl počet uživatelů internetu nízký.[26] K rozmachu sociálních sítí došlo v období tzv. „neomezeného internetu“, který do té doby byl drahý a nedostupný.[27] Mezi nejznámější sociální sítě patří Facebook, který byl založen v roce 2004, a dále Twitter založený v roce 2006. Na sociálních sítích je možné páchat většinu kybernetických útoků (např. malware, phishing, spam atd.) Mezi specifické útoky, které se odehrávají právě v prostředí sociálních sítí, patří kyberšikana, kybergrooming, sexting, kyberstalking.

2.3.1 Kyberšikana

Klasická šikana spočívá v úsilí útočníka ublížit, ponížit, zesměšnit či urazit jiného fyzicky, nebo jen psychicky, s kyberšikanou je tak nerozlučně spjata, neboť sdílí stejné základní rysy a projevy, které však v online světě nabývají jiných forem. Definice kyberšikany podle Priecové a Dalgleishe zní: „*Kyberšikana je kolektivní*

[23] BURIAN Pavel. *Internet inteligentních aktivit*. Praha: Grada, 2014. ISBN 978-80-247-5137-584, str. 84.
[24] KOŽÍŽEK M. *Bezpečně na internetu*. Praha: Grada, 2016. ISBN 978-80-247-5595-3, str. 24.
[25] BURIAN Pavel. *Internet inteligentních aktivit*. Praha: Grada, 2014. ISBN 978-80-247-5137-584, str. 84.
[26] Tamtéž.
[27] KOŽÍŽEK M. *Bezpečně na internetu*. Praha: Grada, 2016. ISBN 978-80-247-5595-3, str. 24.

označení forem šikany prostřednictvím elektronických médií, jako je internet a mobilní telefony, která slouží k agresivnímu a záměrnému poškození uživatele těchto médií.“ [28] Kyberšikana převádí klasickou šikanu do virtuálního světa a dovoluje útočníkovi použít takové prostředky a nástroje, které mohou mít mnohem větší dopad na oběť. Kyberšikana umožňuje díky používání informačních a komunikačních technologií a trvanlivosti dat v kyberprostoru opakované útoky na oběť i přesto, že se oběť v reálném světě geograficky značně vzdálila od původního místa, kde byla šikanována. Rovněž dochází k propojení „klasické“ šikany s kyberšikanou, při které je např. oběť fyzického napadení nahrávána a následně je tento útok umístěný na web. Abychom mohli hovořit o kyberšikaně, je nutné, aby k šikanování byly použity informační a komunikační technologie či služby nabízené v kyberprostoru.[29]

Mezi základní znaky kyberšikany patří zejména pocit anonymity, útočník se domnívá, že je díky Internetu nedohledatelný, dále neomezenost útoků, je možné šikanovat kdykoliv, odkudkoliv a kohokoliv. Neomezený okruh útočníků ve virtuálním světě nezáleží na věku, pohlaví, fyzické síle. Šikanujícím může být v podstatě jakákoliv osoba. Internet poskytuje útočníkovi neomezený prostor a prostředky pro šikanování. Ze strany útočníka mohou být opakovaně vyvěšovány urážlivé komentáře, fotografie a videa na různých portálech, sociálních sítích atd., které může neustále vylepšovat a zdokonalovat. Kyberšikana je obtížně zjistitelná, chybí zde vnější projevy jako u šikany klasické, kterými mohou být podlitiny, chybějící peníze a jiné. Dalším znakem je trvalost. U klasické šikany dochází k jednotlivým útokům, které se opakují, ale dílčí útok vždy skončí. U kyberšikany stačí např. jedna SMS, e-mail apod., přičemž oběť se k nim stále vrací. Útočné SMS, e-maily, fotografie mají trvalejší ráz než jednotlivé fyzické útoky. Mezi nejčastější projevy kyberšikany patří pomlouvání, zastrašování, urážení, pořizování zvukových záznamů či videí s cílem vybranou osobu zesměšnit. Dále pak natáčení videí, při kterých je vybraná osoba fyzicky napadána či jinak psychicky týrána, provokování a napadání uživatelů v diskuzních fórech,

[28] ČERNÁ Alena. *Kyberšikana*. Praha: Grada, 2013. ISBN 978-80-247-4577-0, str. 20.
[29] KOLOUCH Jan. *CyberCrime*. Praha: CZ.NIC, 2016. ISBN 978-80-88168-15-7, str. 309.

vydírání pomocí internetu nebo obtěžování a pronásledování voláním či psaním zpráv.[30]

Příkladem je příběh Anny Halman,14 let, z Polska, kterou pět spolužáků podrobilo před celou třídou sexuální šikaně, tím způsobem, že z ní strhali šaty a předstírali, že ji znásilňují. Celou scénu si přitom natočili na mobil a dívce poté vyhrožovali, že video zveřejní na internetu, což později také udělali. Nahrávku umístili na stánku YouTube. Mělo se jednat o pomstu Anně za to, že s jedním z chlapců nechtěla chodit. Anna následně spáchala sebevraždu.[31]

Kyberšikana obdobně jako klasická šikana není sama o sobě trestným činem ani přestupkem. Záleží na jednání, kterým pachatel šikanoval. V případě, že jednání naplní všemi obligatorními znaky skutkovou podstatu některého z činů vyjmenovaných v trestním zákoníku, jedná se o trestný čin. V úvahu pak přichází např. § 146 Ublížení na zdraví, § 354 Nebezpečné pronásledování a další.[32]

2.3.2 Kybergrooming

Jedná se o jednání, při kterém dochází k psychické manipulaci s osobou za použití sociálního inženýrství, které je realizováno prostřednictvím Internetu či informačních a komunikačních technologií. Účelem kybergroomingu je vyvolání falešné důvěry v oběti a přimět ji k osobní schůzce, na které může dojít k fyzickému, sexuálnímu či jinému útoku na oběť. Obětí mohou být děti i dospělí. Ze statistik však vyplývá, že nejčastějšími obětmi jsou dívky ve věku 13–17 let.[33]

Kybergrooming má různé etapy, nejprve dochází ke vzbuzení důvěry a snaze izolovat oběť od okolí, poté přichází ze strany útočníka podplácení dárky či jinými službami, budování kamarádského vztahu, které přechází ve vyvolání emoční závislosti oběti na osobě útočníka. Následně na řadu přichází osobní setkání, které vyvrcholí sexuálním obtěžováním, zneužitím dítěte či jiným útokem. Rizikovou skupinu tvoří adolescenti/teenageři, kteří se zajímají o lidskou sexualitu,

---

[30] KOLOUCH Jan. *CyberCrime*. Praha: CZ.NIC, 2016. ISBN 978-80-88168-15-7, str. 310.
[31] Tamtéž.
[32] Tamtéž.
[33] Tamtéž, str. 313.

děti s nízkou sebeúctou nebo nedostatkem sebedůvěry, děti s emocionálními problémy a děti naivní a přehnaně důvěřivé.[34] Osoba, která se dopouští kybergroomingu, může svým jednáním naplnit skutkovou podstatu některých trestných činů uvedených v trestním zákoníku, zejména se může jednat o § 175 Vydírání, § 353 Nebezpečné vyhrožování, § 354 Nebezpečné pronásledování.[35]

Jedna z definic kybergroomingu uvádí, že jde o jednání uživatelů internetu, které má v dětské oběti vyvolat falešnou důvěru a tuto přimět k osobní schůzce. Výsledkem může být sexuální zneužití oběti, fyzické násilí či zneužití oběti pro dětskou prostituci, nebo k výrobě dětské pornografie. Zde přichází v úvahu využití speciálního ustanovení uvedeného v § 193b Navazování nedovolených kontaktů s dítětem.[36]

2.3.3 Sexting

V prostředí sociálních sítí číhá spousta nebezpečí, jednou z podob je tzv. sexting. Tento pojem vznikl spojením slov sex a texting, z něhož vyplývá i jeho význam. Jedná se o elektronické rozesílání textových zpráv, fotografií či videí se sexuálním podtextem. Takovýto materiál je nahráván na sociální sítě či jiná uložiště přímo jeho samotnými autory, nebo jiným uživatelem, který získal k takovému materiálu přístup. Nejčastěji k tomuto dochází při dobrovolném posílání souborů se sexuálním obsahem, pořízeným samotným odesílatelem. Po ukončení komunikace použije útočník získaný choulostivý materiál k vyhrožování či vydírání. V některých případech útočník pod pohrůžkou zveřejnění takového materiálu může požadovat zaslání dalších fotografií či videí a psychickým nátlakem tak nutí oběť k výrobě a pořizování dalších materiálů s choulostivím obsahem, které útočník požaduje buď pro vlastní potřebu, nebo se záměrem je sdílet na Internetu. V případě dětí jsou tyto materiály sdíleny v komunitách zaměřených na dětskou pornografii. Další variantou útočníkova jednání může být užití získaného materiálu k jinému nátlaku, např. k obnově partnerského vztahu, provozování sexuálních aktivit, zaslání finanční částky atp. Podíl oběti na činu je

[34] KOLOUCH Jan. *CyberCrime*. Praha: CZ.NIC, 2016. ISBN 978-80-88168-15-7, str. 313.
[35] Tamtéž, str. 314.
[36] Tamtéž.

neoddiskutovatelný, neboť právě tato vytvořila předmětnou fotografii či video, avšak po odeslání ztrácí naprostou kontrolu nad daty.[37] Specifické jsou situace, kdy jsou získávány a zneužívány audiovizuální materiály zobrazující dítě. V případě, že útočník vyzývá dítě k vytvoření a následnému zaslání fotografií, videí či online streamování před web kamerou, kde je zachyceno dítě nahé, obnažené, či jinak vzbuzující sexuální vzrušení, může se dopustit trestného činu Zneužití dítěte k výrobě dětské pornografie § 193 trestního zákoníku. Jedním z projevů sextingu je také situace, kdy pachatel nutí oběť posílat další materiály, případně live stream pod pohrůžkou zveřejnění již zaslaných materiálů na Internetu, nebo zpřístupnění těchto materiálů rodině či přátelům, čímž se dopouští trestného činu Vydírání § 175 trestního zákoníku.[38]

2.3.4 Kyberstalking

Kyberstalking vznikl složením slov kyber a stalking. Původně slovo stalking používali lovci divoké zvěře, znamenalo stopování zvěře až k jejímu uštvání. V podobě, v jaké je slovo chápáno dnes, bylo použito v 90.letech 20.století v rámci studie Meloye, který za stalking označil nebezpečné pronásledování známým či neznámých pachatelem, který pronásleduje oběť takovým způsobem, že v ní vyvolá pocit nebezpečí či strachu, jedná se o dlouhodobé pronásledování.[39] Kyberstalking je jednání spočívající v opakovaném kontaktování oběti přes SMS zprávy, e-maily, telefonáty, messengery aj. Jednání pachatele se zpravidla stupňuje a vyvolá v oběti obavy o svoje soukromí, zdraví či život. Kyberstalkeři jsou vytrvalí, systematičtí. Kyberstalker demonstruje svoji moc a sílu zejména tím, že zveřejní informace ze života oběti, které může získat z různých online zdrojů. Kyberstalking je možné subsumovat pod trestný čin Nebezpečné pronásledování § 354 trestního zákoníku. Mezi základní podmínky naplnění skutkové podstaty trestného činu Nebezpečné pronásledování však patří vytrvalé kontaktování oběti ze strany útočníka prostřednictvím prostředků elektronických komunikací, kdy toto

[37] KOLOUCH Jan. *CyberCrime*. Praha: CZ.NIC, 2016. ISBN 978-80-88168-15-7, str. 315.
[38] Tamtéž, str. 317.
[39] Tamtéž, str. 318.

jednání je způsobilé vzbudit v oběti důvodnou obavu o její život nebo zdraví nebo o život a zdraví osob jí blízkých.[40]

2.4 Legislativní základ kybernetické bezpečnosti

Existuje celá řada důvodů, pro které je třeba zavést a implementovat kybernetickou bezpečnost. Mezi hlavní důvody patří např. negativní ekonomický dopad v případě úspěšného kybernetického útoku, při němž jsou odcizena citlivá data. Při úspěšném kybernetickém útoku může dojít k ohrožené fungování organizace tím, že může být omezen přístup k počítačovým systémům nebo datům pomocí ransomware. Dalším důvodem pro zavedení kybernetické bezpečnosti může být ztráta kredibility napadené společnosti. Posledním, avšak stejně významným důvodem je respektování právních norem a práv a povinností vyplývajících z těchto norem. Pro mnoho subjektů tento legislativní důvod vyplývá ze zákona o kybernetické bezpečnosti, nejedná se však o jediný právní předpis, který souvisí s problematikou kybernetické bezpečnosti. Obzvlášť v posledních letech dochází k rozrůstání primárně mezinárodní právní úpravy, zaměřující se na činnost subjektů (fyzických, právnických osob, států a organizací) v kyberprostoru.[41]

2.4.1 Legislativní vývoj kybernetické bezpečnosti v České republice

Poprvé byla kybernetická bezpečnost řešena státem v roce 2000. V Uvedeném roce byla na Ministerstvu vnitra vytvořena Koncepce boje proti trestné činnosti v oblasti informačních technologií včetně Harmonogramu opatření. Tato koncepce se primárně zaměřila na problematiku potírání trestné činnosti v oblasti informačních technologií, avšak je možné sledovat snahu státu, která spočívá ve vytvoření podmínek pro systémový přístup státu k této trestné činnosti. Tento dokument se vyjadřuje k otázkám potírání kybernetické trestné činnosti a též k otázkám kybernetické bezpečnosti, neboť uvádí, že „*je zapotřebí vytvořit prostředí pro vzájemnou osvětu a informační výměnu mezi*

[40] KOLOUCH Jan. *CyberCrime.* Praha: CZ.NIC, 2016. ISBN 978-80-88168-15-7, str. 318.
[41] KOLOUCH Jan, Pavel Bašta. *CyberSecurity*. Praha: CZ.NIC,2019. ISBN 978-80-88168-31-7, str. 87.

subjekty, získávajícími poznatky o jednotlivých bezpečnostních aspektech, spojených s používáním nových technologií. Je úlohou státních orgánů vytvářet stabilní a bezpečné prostředí, které dává občanům oprávněně pocit právní jistoty při využívání moderních informačních a komunikačních prostředků. K získaným poznatkům o jednotlivých obecných i konkrétních bezpečnostních rizicích by měla mít bezprostřední přístup o veřejnost. K tomuto úkolu je třeba přistoupit aktivně, tedy průběžně provádět preventivně cílenou informační kampaň ve spolupráci všech odpovědných resortů a za účinné participace zainteresovaných subjektů."[42]

Další dokument s názvem Státní informační a komunikační politika e-Česko 2006 byl představen v roce 2004, tento definoval následující priority z pohledu státu:

1) dostupné a bezpečné komunikační služby
2) informační vzdělanost
3) moderní veřejné služby on-line (např. e-zdravotnictví aj.)
4) dynamické prostředí pro elektronické podnikání.[43]

V roce 2005 došlo ke vzniku dokumentu Národní strategie informační bezpečnosti ČR, který navázal na dokument Státní informační a komunikační politiky e-Česko a dokument Bezpečnostní strategie ČR. Cílem této strategie bylo:

1) zlepšení řízení informační bezpečnosti a řízení rizik,
2) rozvoj znalostí o informační bezpečnosti,
3) podpora národní a mezinárodní spolupráce v oblasti informační bezpečnosti,
4) podpora používání nejlepší praxe v oblasti informační bezpečnosti,
5) podpora ochrany lidských práv a svobod,
6) podpora konkurenceschopnosti české ekonomiky.[44]

V roce 2008 byl dokument Koncepce boje proti trestné činnosti v oblasti informačních technologií včetně Harmonogramu opatření nahrazen Koncepcí boje

---

[42] KOLOUCH Jan, Pavel Bašta. *CyberSecurity*. Praha: CZ.NIC,2019. ISBN 978-80-88168-31-7l, str. 88.
[43] Tamtéž.
[44] Tamtéž, str. 89.

proti organizovanému zločinu. Aktualizovaná koncepce reagovala na nárůst kybernetické trestné činnosti a kybernetických hrozeb. V roce 2011 Vláda ČR zřídila Radu pro kybernetickou bezpečnost a schválila tak vznik Národního centra kybernetické bezpečnosti, jakž to součásti NBÚ. V témže roce byla přijata Strategie pro oblast kybernetické bezpečnosti České republiky na období let 2011–2015. Předložená strategie měla vytýčené následující cíle a opatření:

1) vytvoření legislativního rámce,
2) vybudování Národního centra kybernetické bezpečnosti a vládního pracoviště CERT (Central Emergency Response Team)
3) ochrana kritických informačních infrastruktur
4) posilování kybernetické bezpečnosti informačních a komunikačních systémů veřejné správy
5) zefektivnění potírání kriminality v kybernetickém prostoru
6) koordinace aktivit k zajištění kybernetické bezpečnosti v Evropě
7) používání spolehlivých a důvěryhodných informačních technologií
8) zvyšování povědomí o kybernetické bezpečnosti
9) odezva na kybernetické útoky.[45]

V červnu roku 2013 byl ze stran NBÚ předložen návrh zákona o kybernetické bezpečnosti Vládě ČR. Tento byl následně schválen a zák. č. 181/2014 Sb., o kybernetické bezpečnosti vstoupil v platnost dne 29. srpna 2014 s účinností od 1. ledna 2015.[46] Od tohoto roku prošel dvěma novelizacemi, první byla provedena zákonem č. 104/2017 Sb., který nabyl účinnosti 1. července 2017. Obsahem novely bylo rozšíření okruhu povinných osob spadajících pod zákon o kybernetické bezpečnosti o provozovatele informačních systémů a také došlo k úpravě některých sankcí. Druhá a významnější novela byla provedena zákonem č. 205/2017 Sb., jehož účinnost nabyla dne 1. srpna 2017. Tato novela zahrnovala implementaci Směrnice Evropského parlamentu a Rady EU 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii a také byl zřízen národní úřad pro kybernetickou

[45] KOLOUCH Jan, Pavel Bašta. *CyberSecurity*. Praha: CZ.NIC,2019. ISBN 978-80-88168-31-7I, str. 91.
[46] Tamtéž, str. 92.

a informační bezpečnost, který převzal od NBÚ práva a povinnosti v oblasti kybernetické bezpečnosti včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany.[47]

2.4.2 Právní normy ČR

V současnosti je problematika kybernetické bezpečnosti řešena zákonem o kybernetické bezpečnosti (zákon č. 181/2014 Sb.). Další dílčí aspekty ochrany České republiky před kybernetickými útoky lze nalézt také v dalších právních předpisech, mezi které patří:

Ústavní zákony:

Ústavní zákon č. 1/1993 Sb., Ústava české republiky, ve znění pozdějších předpisů.
Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod, ve znění pozdějších předpisů.
Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky.

Zákony:

Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.
Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.
Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským ve znění pozdějších předpisů.
Zákon č. 240/2000Sb., o krizovém řízení ve znění pozdějších předpisů.
Zákon č. 365/2000Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů.
Zákon č. 480/2004 Sb., o některých službách informační společnosti, ve znění pozdějších předpisů.

---

[47] KOLOUCH Jan, Pavel Bašta. *CyberSecurity*. Praha: CZ.NIC,2019. ISBN 978-80-88168-31-7I, str. 93.

Zákon č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů.
Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.
Zákon č. 69/2006 Sb., o provádění mezinárodních sankcí, ve znění pozdějších předpisů.
Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů.
Zákon č. 40/2009Sb., trestní zákoník, ve znění pozdějších předpisů.
Zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.
Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim.
Zákon č. 89/2012 Sb., občanský zákoník.
Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů.
Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.[48]

2.5 Odhalování a vyšetřování kybernetické kriminality

Z kriminologického hlediska jsou pod pojmem pachatelé chápány nejen osoby, které se dopustily zákonem označených trestných činů, ale také další osoby, které nejsou orgány činnými v trestním řízení stíhány. Věnuje se i jedincům, kteří věkem (děti), nebo stavem vědomí (nepříčetnost) překračují rámec trestního práva.[49]

Trestní zákoník uvádí, že pachatelem trestného činu je také ten, jenž trestný čin připravuje, nebo se o něj pokusí (§ 22 odst. 1 trestního zákoníku). Dále se ve smyslu trestního zákoníku za pachatele považuje také osoba spolupachatele (§ 23 trestního zákoníku) a účastníka (§ 24 trestního zákoníku). Trestně odpovědným pachatelem je fyzická osoba, která je starší 15 let a je příčetná.[50]

---

[48] KOLOUCH Jan, Pavel Bašta. *CyberSecurity*. Praha: CZ.NIC,2019. ISBN 978-80-88168-31-7l, str. 98,99.
[49] NOVOTNÝ, O., M. ŠTIKA a Z. BOLELOUCKÝ. *Kriminologie*. Praha: ASPI, 2004. ISBN 80-735-7026-2, str. 113.
[50] NOVOTNÝ, F. *Trestní právo hmotné*. Plzeň: Aleš Čeněk, 2017. ISBN 978-80-7380-651-4, str. 79, 80.

V oblasti kyberkriminality lze předpokládat, že pachatelé budou nejen z osob mladistvých (ten, kdo v době spáchání dovršil patnáctý rok a nepřekročil osmnáctý rok věku), ale také z osob, které podle § 25 tr. zákoníku nejsou trestně odpovědné, neboť nedovršily 15 let věku.[51]

Způsoby páchání trestné činnosti, ale i motivace pachatelů budou záviset především na jejich věku, osobní vyspělosti a případné příležitosti. Daleko méně bude záviset na technických vědomostech a dovednostech pachatele. „Klasická" kriminalita se v průběhu historie prakticky nemění, moderní technologie přináší i nové druhy trestné činnosti. Vražda zůstane vraždou, i přes použití laserové pistole namísto sekery. Nový fenomén se objevil s dematerializací některých předmětů (informací, financí), který bychom mohli nazvat dematerializovaným zločinem. Jeho kořeny pochází z nepoctivosti ve světě obchodu, podnikání, bankovnictví a pojišťovnictví. Jeho živnou půdu tvoří počítačové systémy, které obsahují databáze plné informací, jejichž znalost nebo manipulovatelnost poskytuje nemalé výhody. Důsledkem nepoctivosti lidí s vysokou odpovědností, pravomocí, v důvěryhodném postavení, a to buď z vlastní iniciativy či na objednávku, je dematerializovaný zločin. Tento druh kriminality neobsahuje prvky násilí, ale jeho základem je nezákonná manipulace a podvod. V případě některých pachatelů se dá říci, že pokud by stejnou energii, vynalézavost a inteligenci věnovali podnikání, mohli by být velmi úspěšní, u většiny však jsou základními předpoklady příležitost a dostatečná odvaha nebo i omezenost.[52]

Pro tipování pravděpodobného pachatele je třeba zjistit motiv kybernetického trestného činu. Zjištění motivu spáchání trestného činu je úzce spjaté s otázkou, kdo má nebo může mít z důsledků činu prospěch. Dále má značný význam zjištění a dokázání motivu kybernetického trestného činu pro právní kvalifikaci skutku a určení společenské škodlivosti tohoto jednání.[53]

---

[51] SMEJKAL Vladimír. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015. ISBN 978-80-7380-501-2, str. 486.
[52] Tamtéž, str. 487.
[53] Tamtéž.

2.6 Pachatelé kybernetické kriminality

Podmínka páchání kybernetické kriminality je schopnost pracovat s počítačem či jiným zařízením na zpracování dat. Avšak představa, že kyberkriminalitu budou páchat pouze špičkoví odborníci, profesionálové či amatéři je zcela mylná. V dnešní době pachatelé kybernetické kriminality pochází z nejrůznějších vrstev, tříd či skupin, přičemž jejich počítačové vzdělání a dovednosti mohou být omezeny pouze na schopnost na Internetu najít, stáhnout a spustit nějaký škodlivý program generující viry. Takoví útočníci se nazývají „script kiddies“, pouze „odpálí“ vhodný script bez hlubšího poznání této problematiky. Další skupina pachatelů počítačových trestných činů pochází z řad zaměstnanců poškozené organizace, či zaměstnanců jejich dodavatelů. Do třetí skupiny se řadí tzv. průnikáři (hackeři). Tato skupina má anarchistické rysy, čemuž odpovídají i jejich činy, zejména se jedná o zavirování počítačů či průniky do vládních počítačových sítí. Do čtvrté skupiny lze zařadit organizovaný zločin. Tito pachatelé používají počítače zejména ke skryté komunikaci, výrobě padělků, (např. software, či platebních karet), obchodování s nelegálním zbožím (drogy, zbraně apod.), výrobě a distribuci pornografie všeho druhu. Pátou kategorii ovládají profesionálové, kteří se živí hackerstvím. Provádí průniky za účelem odhalování státních a obchodních utajovaných informací či útoky na infrastruktury jiných států. Převážně se jedná o žoldáky, kteří pracují za peníze, nebo v rámci služby v ozbrojených složkách a výzvědných službách. V neposlední řadě máme skupinu kyberteroristů, kdy jejich chování může, ale nemusí mít charakter jednání organizovaného zločinu. Do poslední kategorie se řadí pachatelé, jejichž věk je blízký věku dětí a mladistvých. Tito pachatelé nepřemýšlí o svém jednání a následcích. Nenapadne je, že jejich jednání by mohlo být trestné a v případě, že je odhaleno, hájí se zcela naivně. Typickou obhajobu je tvrzení, že nevěděli o tom, že jejich jednání je trestné, případně, že k předmětné situaci došlo omylem.[54]

[54] VÁLKOVÁ Helena, Josef KUCHTA, Jana HULMÁKOVÁ a kol. *Základy kriminologie a trestní politiky*. 3. vydání 2019, 664 s. Praha: Nakladatelství C. H. Beck, ISBN 978-80-7400-732-3, str. 551.

3 Mládež a kyberkriminalita

V dnešní době je využívání internetu dětmi nezbytné. Jejich znalosti v oblasti informačních a komunikačních technologiích převyšují nad znalostmi jejich rodičů. Často tedy dochází k tomu, že rodiče vzhledem k této skutečnosti na ochranu svých dětí v tomto prostředí nedbají, tedy nedrží nad dětmi v online prostředí žádný dozor. Důvěřivost, naivita a nedostatek životních zkušeností může vést k tomu, že se dítě snadno stane obětí virtuálního predátora. Proto je potřeba se mnohem více věnovat ochraně těch nejzranitelnějších. Rodiče často vštěpují svým dětem do paměti, že je třeba pozdravit staršího, nebo že před přechodem pro chodce je třeba se rozhlédnout. Obdobným způsobem je třeba vést ze strany rodičů své děti k bezpečnému chování v online prostředí.[55]

Můžeme říci, že sociální sítě v posledních 20 letech ve velké míře napomáhají dětem k socializaci ve společnosti. Prostřednictvím sociálních sítí a chatů navazují kontakty s dalšími vrstevníky, přičemž si neuvědomují rizika, která jim při této činnosti hrozí.[56]

Zpravidla okolo třetí třídy bývá vysloveno dětmi přání mít účet na sociálních sítích. Před rokem 2018 se jednalo o účet na sociální síti Facebook, v dnešní době však převládá touha mít účet na Instagramu, Snapchatu, či Tik Toku. Zde může vyvstat mnoho problémů, pokud dítěti účet rodiče zakážou, založí si ho nejspíše samo, nebo mu pomohou spolužáci a rodiče tak nebudou o účtu vědět, tudíž nebudou moci účet nastavit tak, aby nebylo ohroženo soukromí dítěte. Účet na sociálních sítích lze založit od 13 let, děti jsou však s tímto srozuměny a v případech, kdy je dítě mladší 13 let, při registraci uvádí věk nepravdivý. Důležité je nastavit zabezpečení účtu, výchozí stavy bývají veřejné a viditelné pro kohokoliv, což zejména pro děti může být nebezpečné.[57]

---

[55] *Ochrana dítěte v online prostředí.* [online]. [cit. 2022-12-02]. Dostupné z:Ochrana dítěte v online prostředí - INTERNETEM BEZPEČNĚ (internetembezpecne.cz).
[56] *Kyberkriminalita*. [online]. [cit. 2022-12-03]. Dostupné z: Zneužívání dětí na internetu - Policie České republiky.
[57] DOČEKAL Daniel a kol. *Dítě v síti*. Preface 2019. ISBN 978-80-204-5145-3, str. 50,51.

3.1 Mládež

Pod pojem mládež lze zahrnout osoby, které jsou v současnosti označovány také jako mileniové, narozené na přelomu století a tisíciletí, Net-generace, iGen – internetová generace, generace Z apod. Mládež je takto označována z důvodu, že se narodila do doby, kdy světu vévodí internetové technologie a vyznačuje se životem online, což znamená okamžité sdílení myšlenek, poznatků, názorů pomocí různých médií.[58]

Z kriminologického hlediska je pojmu mládež přisuzován obsah užívaný v sociologii, to znamená, že se jedná o osoby společensky nezralé, nesamostatné ve věkovém rozmezí 12–24 let. V případě užití statistických údajů o kriminalitě mládeže je vymezení a trestněprávní členění užito s tím, že existuje skupina blízká věku mladistvých (starší 18 a mladší 21 let) a skupina mladých dospělých, která začíná jednotně dosažením věku 18 let, konečná hranice může být do 24 let.[59]

Pojem nezletilí používá trestní zákoník ČR, česká trestní justice a stejně tak i Úmluva o právech dítěte OSN. Nezletilými se rozumí skupina osob omezená vrchní věkovou hranicí 18 let. Pod pojmem děti rozumíme osoby ve věku do 15 let, a mezi mladistvé řadíme osoby s věkovým rozpětím 15–18 let.[60]

3.2 Delikvence mládeže

Delikvence, slovo pochází z latinského delinquere, což znamená provinit se. Z hlediska společensky nepřijatelného chování se jedná o širší pojem, pod který je zahrnována nejen kriminalita, ale rovněž také činy, které nejsou tzv. jinak trestné. Jedná se například o přestupky a také o trestnou činnost osob mladších 15 let, kterým z důvodu věku nelze trest uložit. Často je pojem delikvence používán v souvislosti s nežádoucím a nepřijatelným chováním dětí a mládeže. V případě mladistvých může být také použit pojem juvenilní delikvence. Ve své podstatě se jedná o právnické hodnocení společensky nepřijatelného činu, který

[58] MAREŠOVÁ Alena. *Kriminalita mládeže v podmínkách současné české společnosti*. Praha 2018.ISBN 978-80-7251-483-0, str. 15.
[59] Tamtéž.
[60] Tamtéž, str. 16.

spočívá v porušování právních norem určitého státu, přičemž toto jednání je posléze sankcionováno. Hranice mezi delikvencí a tím, co není delikvence, je dána následným trestem. Nelze sem zařadit jednání, které není pro společnost nebezpečné, např. disociální chování, do kterého lze zahrnout např. drobné lži, vzdorovitost apod. Toto může být označováno jako poruchy chování, ale mezi sociálně patologické jevy nepatří. Kriminální chování a delikvenci lze označit jako projev poruchy sociálně adaptačních schopností a dovedností. Odchylku od společenské normy můžeme definovat jako neschopnost plnit požadavky a očekávání společnosti. Řada delikventních osob není schopna či ochotna společenskou nepřijatelnost svého chování zhodnotit, proto o změnu svého společensky nepřijatelného chování ani neusilují. Vznik a rozvoj kriminality a delikvence je multifaktoriální. Podstatný význam vyšší pravděpodobnosti vzniku kriminálního jednání mají následující biopsychosociální faktory, které působí ve vzájemné interakci.[61]

3.2.1 Biologické faktory

První biologický faktor ovlivňující vyšší pravděpodobnost kriminality je pohlaví. Muži se kriminálního i delikventního chování dopouští mnohem častěji než ženy. Vzájemný poměr se pohybuje 10 : 1. Důvodem je větší agresivní a sociálně dravé jednání pro dosažení seberealizace u mužů. Další důvodem je větší tendence k agresivitě u mužů vzhledem k mužskému pohlavnímu hormonu testosteronu. Velký význam pro vznik a rozvoj kriminálního chování má věk, většinou se jedná o mladé jedince. Značnou část vězeňské populace tvoří muži do 26 let. Mezi další biologické faktory patří vrozené dispozice k určitým způsobům reagování. Vyšší tendenci k delikventnímu jednání a kriminalitě mají jedinci, kteří jsou zvýšeně dráždiví. Toto je dáno geneticky. Zejména se jedná o poruchy související s tzv. minimální mozkovou dysfunkcí, dále pak problémy související s hyperaktivitou (ADHD).

---

[61] FISCHER Slavomil, Jiří ŠKODA. *Sociální patologie*. 2 vydání. Praha: Grada. ISBN 978-80-247-5046-0, str. 170.

3.2.2 Psychické faktory

Dlouhodobě je pozornost věnována úrovni mentálních schopností. Mezi delikventy můžeme nalézt osoby s inteligencí na škále od mentální retardace až po genialitu. Obecně se však kriminálního jednání dopouští jedinci, jejichž rozumové schopnosti jsou nižší. S tím souvisí nižší schopnost jedince posoudit danou situaci, zvážit důsledky vlastního jednání. Mezi delikventy se vyskytuje vyšší počet osob trpících poruchou osobnosti.[62]

3.2.3 Sociální faktory

Významným sociálním faktorem ovlivňujícím vyšší pravděpodobnost vzniku kriminality a delikvence je rodina. Jedinec si zde utváří vzorce chování. Mezi nejvýznamnější aspekty související s vyšší pravděpodobností budoucího negativního vývoje jedince patří otázka anomálie rodičů. Jedná se o různé příčiny vedoucí k tomu, že rodiče nejsou schopní vychovávat a pečovat o své děti. Velký význam v případě kriminality a delikvence má jednání, kdy rodiče se sami dopouštěli asociálních a antisociálních forem chování (závislost na alkoholu, drogách, páchání trestné činnosti apod.). V případě, že rodina je z hlediska funkčnosti dysfukční či dokonce afunkční, má to pro vývoj dětí velmi negativní důsledky.[63]

3.3 Druhy kyberkriminality páchané na mládeži

Mezi nejvíce závažnou trestnou činností páchanou přes internet na mládeži patří online sexuální zneužívání dětí. Vzhledem k tomu, že internet je především anonymní, není problém vydávat se za někoho jiného. Pachatel oběť (převážně děti) kontaktuje přes sociální sítě či v online hrách. Potencionální oběti v kyberprostoru ztrácí zábrany a nedochází jim míra rizika. Samy nedokáží rozeznat riziko, jenž jim v internetové síti hrozí. Často se nechají snadno přesvědčit k zasílání erotických fotografií. Těmto projevům říkáme sexting.

[62] FISCHER Slavomil, Jiří ŠKODA. *Sociální patologie*. Závažné sociálně patologické jevy, příčiny, prevence, možnosti řešení. 2 vydání. Praha: Grada. ISBN 978-80-247-5046-0, str. 170.
[63] Tamtéž.

Převážně se jedná o děti, které dobrovolně zasílají citlivý materiál, který bývá následně použit proti nim. Tímto se stávají snadno vydíratelnými- *„jestli nepošleš další a ještě odvážnější, tak pošlu tvé rodině, kamarádům a spolužákům ze školy fotky, které už mám*“. Často se stává, že se děti nafotí či natočí v erotických pozicích a choulostivý materiál bez znalosti základních pravidel chování na internetu odesílají protějšku, který převážně znají pouze z internetového prostředí. Takovýto materiál poté koluje v síti Internet a jeho definitivní odstranění není prakticky možné. Zde přichází v úvahu trestný čin Výroba a jiné nakládání s dětskou pornografií § 192 trestního zákoníku, Zneužití dítěte k výrobě pornografie § 193 trestního zákoníku, Ohrožování výchovy dítěte § 201 trestního zákoníku, Svádění k pohlavnímu styku § 202 trestního zákoníku.[64]

Dalším neméně závažným druhem kyberkriminality páchané na mládeži je kybešikana. Jde o specifický druh šikany, využívající elektronické prostředky jako nástroj pro její páchání. Cílem kybešikany je stejně jako u té klasické někomu ublížit, či ho zesměšnit. Převážná část případů je kvalifikována jako přestupek, případně se může jednat o jiný správní delikt (např. porušení školního řádu). Výjimečně dochází jednáním pachatele kyberšikany k naplnění skutkové podstaty trestného činu, kdy se může jednat například o trestný čin Účast na sebevraždě § 144 trestního zákoníku, Vydírání § 175 trestního zákoníku, Nebezpečné vyhrožování § 353 trestního zákoníku apod.[65]

Policie v roce 2019 zaregistrovala celkem 469 skutků spáchaných prostřednictvím internetu na osobě mladší 18 let. Nejčastěji se jednalo o trestný čin ohrožování výchovy dítěte, sexuální nátlak a šíření pornografie.[66]

---

[64] *Kyberkriminalita*. [online]. [cit. 2022-12-03]. Dostupné z: Zneužívání dětí na internetu - Policie České republiky.
[65] Tamtéž.
[66] *Statistika kybernetické kriminality za rok 2019*. [online]. [cit. 2022-12-04]. Dostupné z: https://www.e-bezpeci.cz/index.php/z-jinych-webu/1749-statistika-kyberneticke-kriminality-za-rok-2019.

3.4 Druhy kyberkriminality páchané mládeží

Kriminalita mládeže je typická vysokou mírou latence, zejména to platí u méně závažných forem kriminality. Zde je zřejmá vyšší tolerance společnosti vůči mladistvým pachatelům méně závažné trestné činnosti.[67] Mezi mládeží se kriminality dopouštějí ve větší míře chlapci. Podíl obžalovaných mladistvých dívek v letech 2010–2016 se pohyboval mezi 6–11,8 %.[68] Z hlediska struktury kriminality u mládeže převažují méně závažné majetkové trestné činy (činy jinak trestné) zejména krádeže.[69] Je třeba také poukázat na to, že část kriminality se přenesla do oblasti kyberprostoru, ve kterém lze předpokládat vyšší míru latence. Z výzkumu ISRD 2 vyplývá, že např. nelegální stahování z internetu je u mládeže běžným jevem.[70]

Celkově trestná činnost spáchaná v kyberprostoru zaznamenala v roce 2021 nárůst na 9 518 skutků, oproti roku 2020 tedy přibylo 1 445 skutků, což znamená meziroční nárůst o 17,8 %. Mezi nejčastěji páchané trestné činy v kyberprostoru patří podvody. V tomto odvětví bylo zaregistrováno celkem 4 087skutků, dále se jedná o neoprávněný přístup a poškození záznamu v počítačovém systému, opatření a přechovávání přístupového zařízení a hesla, kdy bylo zaregistrováno celkem 1 682, a úvěrové podvody, celkem 645 záznamů. Platí, že nejrozšířenější trestnou činností páchanou v kyberprostoru je majetková trestná činnost, dále pak jednání v oblasti mravnostních trestných činů, v oblasti neoprávněného držení platebního prostředku a trestných činů páchaných v oblasti porušování autorského práva a porušování práv k autorské známce.[71]

Mezi další větší skupinu protiprávního jednání dlouhodobě patří trestná činnost mravnostního charakteru,[72] u které roste počet pachatelů do 18 let věku v poměru k pachatelům zletilým. Pachatelů ve věku do 18 let bylo u mravnostních trestných

---

[67] VÁLKOVÁ Helena, Josef KUCHTA, Jana HULMÁKOVÁ a kol. *Základy kriminologie a trestní politiky*. 3. vydání 2019.. Praha: Nakladatelství C. H. Beck, ISBN 978-80-7400-732-3, str. 284.
[68] Tamtéž, str. 285.
[69] Tamtéž, str. 286.
[70] Tamtéž, str. 304.
[71] *ZPRÁVA O SITUACI V OBLASTI VNITŘNÍ BEZPEČNOSTI A VEŘEJNÉHO POŘÁDKU NA ÚZEMÍ ČESKÉ REPUBLIKY V ROCE 2021.* [online]. [cit. 2022-12-03]. Dostupné z: https://www.mvcr.cz/clanek/statistiky-kriminality-dokumenty.aspx.
[72] Tamtéž.

činů zaregistrováno více, než v ostatních druzích kybernetické kriminality dohromady.[73]Nejčastějšími případy jsou šíření nebo držení dětské pornografie, navazování kontaktu s dětmi s cílem od nich vylákat erotické materiály a v malé míře se jedná o sexuální nátlak.[74] Mezi druhy kyberkriminality páchané mládeží můžeme zařadit např. Výrobu a jiné nakládání s dětskou pornografií § 192 trestního zákoníku, Zneužití dítěte k výrobě pornografie § 193 trestního zákoníku, neboť děti, které šíří dál své vlastní intimní fotografie nebo videa, svým jednáním naplňují skutkové podstaty uvedených trestných činů[75]

K dalšímu jednání, které je rozšířeno zejména mezi spolužáky, patří kyberšikana. Jak bylo popsáno výše, úkolem kyberšikany je někomu ublížit či ho ztrapnit skrze prostředky elektronické komunikace. Z takového to jednání může vyvstat trestně právní jednání, kterým může být naplněna skutková podstata trestného činu např. Účast na sebevraždě § 144 trestního zákoníku, Vydírání § 175 trestního zákoníku, Nebezpečné vyhrožování § 353 trestního zákoníku apod.[76]

Z výzkumu realizovaného projektem Kraje pro bezpečný internet pod záštitou Asociace krajů České republiky 2018, kterého se zúčastnili žáci ve věku od 11 do 16 let, vyplývá, že se na internetu dopouští různých druhů neoprávněných přístupů k informačnímu systému, což je samo o sobě trestným činem. Celkem 15,2 % respondentů přiznalo, že se dopustilo neoprávněného přístupu k cizí Wifi síti, neoprávněný přístup k cizímu facebookovému účtu přiznalo 11,3 % respondentů. Dalším v pořadí je porušování autorských práv, ke kterému se doznalo 9,6 % respondentů. Dále 9,1 % respondentů uvedlo, že přes internet poslalo výhružnou zprávu a 6,6 % šířilo přes internet erotickou fotografii zachycující osobu mladší 15 let.[77]

---

[73] *Statistika kybernetické kriminality za rok 2019.* [online]. [cit. 2022-12-04]. Dostupné z: https://www.e-bezpeci.cz/index.php/z-jinych-webu/1749-statistika-kyberneticke-kriminality-za-rok-2019.

[74] *ZPRÁVA O SITUACI V OBLASTI VNITŘNÍ BEZPEČNOSTI A VEŘEJNÉHO POŘÁDKU NA ÚZEMÍ ČESKÉ REPUBLIKY V ROCE 2021*. [online]. [cit. 2022-12-03]. Dostupné z: https://www.mvcr.cz/clanek/statistiky-kriminality-dokumenty.aspx.

[75] *Policie CZ, Zneužívání dětí na internetu*. [online]. [cit. 2022-12-03]. Dostupné z:Zneužívání dětí na internetu - Policie České republiky.

[76] *Kyberkriminalita*. [online]. [cit. 2022-12-03]. Dostupné z: Zneužívání dětí na internetu - Policie České republiky.

[77] *Vnímání kyberkiminality mezi dětmi*. [online]. [cit. 2022-12-03]. Dostupné z :Vnímání kyberkriminality mezi dětmi | Zájmové a neformální vzdělávání (npi.cz).

4 Prevence kriminality

Pod pojmem prevence kriminality se skrývá soubor různých společenských aktivit, které směřují k odstranění, oslabení či neutralizaci kriminogenních faktorů. Jejich úkolem je zastavit nebo alespoň potlačit růst kriminality. Především se jedná o působení na faktory doprovázející vznik kriminality a podněty směřující k páchání trestné činnosti. Také se jedná o působení na potencionálního pachatele a potencionální oběť. Podle zaměření prevenci dělíme na sociální, situační a viktimologickou. Podle okruhu adresátů, kterým je určena, třídíme prevenci na primární, sekundární a terciární.[78]

4.1 Sociální prevence

Sociální prevence má nejširší zaměření, jelikož jejím účelem je překonávat či neutralizovat kriminogenní faktory. Sociální prevence je orientována na sociální kriminogenní faktory, kterými jsou alkoholismus, prostituce, nezaměstnanost, chudoba, záškoláctví, bezdomovectví apod., dále pak na deformace v oficiální politice a v právním řádu či na působení médií, které mohou mít kriminogenní vliv, a dále na otázky vlivu rodiny, školy, sociálních služeb a jiných institucí v oblasti kriminálně preventivní či socializační.[79]

Sociální prevence se dále zabývá ovlivňováním užitečných a žádoucích rolí ohrožených osob. Lidé chtějí něčím být, někam patřit či zastávat nějakou směsici rolí, proto je třeba ohroženým jedincům dopřát sociální role a vymanit je z okruhu abnormních sociálních vazeb a kontaktů.[80]

---

[78] GŘIVNA, T., M. SCHEINOST, I. ZOUBKOVÁ a kol. *Kriminologie*. Praha: WoltersKluwer, 2014. ISBN 978-80-7478-614-3, str. 142.
[79] NOVOTNÝ, O., M. ŠTIKA a Z. BOLELOUCKÝ. *Kriminologie*. Praha: ASPI, 2004. ISBN 80-735-7026-2, str. 173.
[80] GŘIVNA, T., M. SCHEINOST, I. ZOUBKOVÁ a kol. *Kriminologie*. Praha: WoltersKluwer, 2014. ISBN 978-80-7478-614-3, str. 150.

4.2 Situační prevence

Situační prevence má za úkol odstranit kriminogenní situace, omezit příležitost k páchání trestné činnosti a zvýšit rizika dopadení pachatele. Kriminologické a kriminalistické poznatky uvádí, že k páchání trestné činnosti jsou příhodná určitá místa, doba dne, týdne, měsíce a určité situace.[81]

Některé kriminogenní situace vznikají v souvislosti s životními zvyklostmi a stereotypy obyvatel daného místa. Opatření situační prevence jsou v zásadě technického, organizačního a administrativního charakteru. Kriminalitu snižují pomocí technických prostředků, kterými trestnou činnost znemožní či znesnadní.[82]

4.3 Viktimologická prevence

Viktimologická prevence se zaměřuje na ochranu potencionální oběti, v určité míře se překrývá s prevencí sociální i situační. Její činnost je orientována na osvětu, poradenství a na vštěpování obecných a speciálních zásad ochrany ohrožených osob. Osvětová činnost poučuje potencionální oběti o způsobu chování, tak aby se zbytečně nevystavovaly vyšší míře nebezpečí. Také uvádí, jak se lze útoku bránit, chovat se během něj i po něm.[83]

4.4 Prevence primární, sekundární a terciární

Primární prevence je určena veškerému obyvatelstvu, ať již celého státu, některého území, či některým skupinám obyvatel (mládeži, ženám). Působí na každého, bez ohledu na stupeň kriminálního ohrožení či kriminální rizikovosti jedince.[84]

Sekundární prevence směřuje proti potenciálním pachatelům, potenciálním obětem a na kriminogenní situace. Sekundární sociální prevence je zaměřena na

[81] GŘIVNA, T., M. SCHEINOST, I. ZOUBKOVÁ a kol. *Kriminologie*. Praha: WoltersKluwer, 2014. ISBN 978-80-7478-614-3, str. 153.
[82] Tamtéž, str. 154.
[83] Tamtéž, str. 160
[84] Tamtéž.

kriminálně rizikové skupiny, jako jsou děti, mladiství a mladí dospělý. Je potřeba zacílit preventivní aktivity přesně tak, aby nedocházelo ke stigmatizaci jedinců.[85]

Terciární prevence je spojena s předcházením kriminální recidivě u pachatele a viktimologické recidivě u oběti. U oběti se jedná o nápravu následků vzniklých v souvislosti s trestnou činností a o poskytnutí potřebné pomoci. U zločinců se jedná o jejich sociální integraci.[86]

4.5 Prevence kyberkriminality

Současná doba vede k rostoucí závislosti civilizace na informačních a komunikačních technologiích. Zranitelnost těchto technologií přináší významnou hrozbu. Vhledem k tomu, že hlavním nástrojem obrany proti kyberútokům a kyberzločninu je prevence, je nutné informační systémy vytvářet zabezpečené, čímž dojde ke snížení zranitelnosti a zábraně hrozeb pocházejících z řad pachatelů kybernetické kriminality. Rovněž je třeba mít nástroje pro zjišťování možných kybernetických útoků tak, aby na ně mohlo být včas reagováno a stejně tak je potřeba mít nástroje, které umožní rozkrýt co konkrétně se v sytému odehrálo, aby bylo možné zajistit důkazy, které slouží nejen pro usvědčení pachatele, ale také pro zlepšování bezpečnostních opatření.

Jak již bylo uvedeno v předchozí kapitole, můžeme rozlišit několik úrovní prevence. Primární prevencí v oblasti kybernetické kriminality se zabývá zejména výzkum kriminologický, kriminalistický a bezpečnostní. Úkolem primární prevence v oblasti kyberkriminality je předcházení vzniku bezpečnostních incidentů pomocí všeobecného bezpečnostního povědomí uživatelů a utvářením legislativní podpory pro kybernetickou bezpečnost. Sekundární prevence v oblasti kyberkriminality se zabývá předcházením vzniku, rozvoji a přetrvávání rizikového chování u osob, jež jsou ohroženy již na základě toho, že se pohybují v kyberprostoru, např. chování na sociálních sítích. Terciální prevence má za úkol

[85] NOVOTNÝ, O., M. ŠTIKA a Z. BOLELOUCKÝ. *Kriminologie*. Praha: ASPI, 2004. ISBN 80-735-7026-2, str. 190.
[86] Tamtéž, str. 191.

zabránit opakování kyberútoků, a to budováním zabezpečených informačních systémů a také vytvářením maximálních předpokladů pro odhalování trestných činů v kyberprostoru a opatřováním důkazů.[87]

Trestná činnost páchaná v prostředí internetu narůstá zejména v posledních 10 letech. Nejčastějšími online trestnými činy jsou různé druhy podvodů, dále pak trestné činy mravnostního a násilného charakteru. Policie věnuje velkou pozornost osvětové činnosti a informování o nových trendech kyberkriminality. Policie České republiky mimo vlastních preventivních aktivit, které zastřešuje jeden z pilířů policejní prevence „*Tvoje cesta onlinem*" se spolupodílí na dalších projektech na regionální i mezinárodní úrovni.[88]

Preventivní projekt s názvem Tvoje cesta onlinem má za úkol ukázat dětem na konkrétních případech formy, kterými internetoví predátoři kontaktují své potencionální oběti, způsoby, jakými s nimi manipulují, a z jakých veřejně dostupných informací čerpají. Dále policejní preventisté upozorňují na riziková jednání při komunikaci s osobou na internetu. Tento projekt je rovněž zaměřen i na rodiče dětí, neboť právě oni mohou poskytnou nejefektivnější prevenci, a proto je důležité, aby rodiče věděli, co děti na sociálních nejčastěji sítích dělají, jak komunikují, jaké jsou jejich preference a jaká rizika na děti v síti číhají.[89]

Další projekt, který se zabývá prevencí kyberkriminality, má název Kraje pro bezpečný internet. Na tomto projektu se rovněž spolupodílí Policie České republiky s Radou Asociace krajů ČR. Projekt je zaměřen zejména na žáky a studenty základních a středních škol, pedagogy, sociální pracovníky, dále na policisty, strážníky, rodiče a seniory. Výstupem jsou didaktické a metodické materiály pro jednotlivé cílové skupiny. Na mezinárodní úrovni je nejvíce rozšířená kampaň Europolu zaměřená na problematiku zneužívání dětí online#SayNo!, která v České republice byla realizována pod názvem „*Řekni Ne*!"Součástí

---

[87] VÁLKOVÁ Helena, Josef KUCHTA, Jana HULMÁKOVÁ a kol. *Základy kriminologie a trestní politiky*. 3. vydání 2019, 664 s. Praha: Nakladatelství C. H. Beck, ISBN 978-80-7400-732-3, str. 552-554.

[88] *Prevence kyberkriminality.* [online]. [cit. 2022-12-04]. Dostupné z: https://www.policie.cz/clanek/prevence-kyberkriminality.aspx.

[89] *Tvoje cesta onlinem*. [online]. [cit. 2022-12-05]. Dostupné z: https://www.policie.cz/clanek/tvoje-cesta-onlinem.aspx.

kampaně je video spot, který patří mezi nejsledovanější preventivní videa Policie České republiky na kanálu YouTube.[90]

[90] Prevence kyberkriminality. [online] [cit. 2022-12-05] Dostupné z: https://www.policie.cz/clanek/prevence-kyberkriminality.aspx.

5 Výzkumné šetření

Předchozí kapitoly diplomové práce tvoří teoretický rámec pro výzkumné šetření vedoucí k realizaci výzkumu. V této kapitole bude stanoven problém, cíle výzkumného šetření, dále bude zvolena výzkumná metoda a charakteristika výzkumného souboru, v závěru práce budou prezentována získaná data.

5.1 Stanovení problému

Tato diplomová práce se zabývá problematikou mládeže a kyberkriminality, která představuje velmi aktuální problém současné doby. Internet často využívají děti, které nemají tušení o nástrahách a rizicích internetového prostředí a může tak dojít k situaci, kdy se stanou obětí různých internetových útoků. Povědomí o bezpečném chování na internetu by mělo být základem před vstupem dětí do světa internetového prostředí, bohužel tyto informace však většina z nich od nikoho nezíská.

5.2 Cíl výzkumného šetření

Hlavním cílem výzkumného šetření je zjistit, jaké povědomí má mládež o rizicích spojených s užíváním internetu.

Vedlejšími cíli je zjistit:

- kolik času tráví denně mládež v internetovém prostředí a co na internetu nejčastěji dělá
- zda na aktivity mládeže v internetovém prostředí má vliv pohlaví respondentů
- zda mládež v internetovém prostředí někdy komunikuje i s lidmi, které ve skutečnosti nezná
- zda by mládež měla zájem dozvědět se o kyberkriminalitě více informací

5.3 Výzkumná metoda

Vzhledem k výše stanoveným výzkumným cílům byla zvolena výzkumná metoda dotazníku. Jedná o nejčastěji používaný nástroj v kvantitativní výzkumné strategii, který umožní na velkém počtu respondentů zjistit potřebné údaje. Výhodou této metody je rychlé a ekonomické shromáždění dat.

Výzkumné šetření bylo realizováno pomocí dotazníku vlastní konstrukce, který je zaměřen na zjišťování názorů a zkušeností mládeže spojených s problematikou kyberkriminality. Dotazník je sestaven ze 13 položek, obsahuje celkem 7 uzavřených, 4 polouzavřené a dvě otevřené položky. Kompletní znění dotazníku je součástí přílohy této diplomové práce.

K ověření srozumitelnosti a funkčnosti výzkumného nástroje došlo realizací předvýzkumů na celkovém počtu 10 respondentů, kteří odpovídali kritériím cílové výzkumné skupiny. K předvýzkumu byli vybráni respondenti ve věku 10 a 11 let, tedy na spodní věkové hranici cílové skupiny, aby bylo zřejmé, že uvedeným otázkám porozumí. Šetřením bylo zjištěno, že respondenti všem otázkám porozuměli, výsledky předvýzkumu nebyly zahrnuty do výsledků výzkumu.

5.4 Charakteristika výzkumného souboru

Výzkumné šetření se zaměřuje na cílovou skupinu dětí druhého stupně základních škol, tedy na děti ve věku 10–15 let. V tomto věkovém období začínají být děti na internetu již plně aktivní, průměrný věk, kdy děti začínají používat internet, klesl pod 10 let. Jak uvádí článek Ochraňme své děti před nebezpečím internetu, nejnáchylnější na ovlivnění nevhodným obsahem jsou děti v pubertálním věku v rozmezí 9–16 let.[91]

[91] *Ochraňme své děti před nebezpečím internetu*. [online]. [cit. 2023-01-03]. Dostupné z: https://www.zenax.cz/ochranme_sve_deti_pred_nebezpecim_internetu_14237.htm.

Respondenty tvoří celkem 363 osob ve věku 10–15 let, s průměrným věkem M = 12,52. Výzkumný soubor se skládá ze 189 chlapců (52 %) a 174 dívek (48 %), poměr obou pohlaví je tedy téměř vyrovnaný.

V případě výběru prvků výzkumného souboru pro tento výzkum se jedná o záměrný výběr, kdy bylo rozhodnuto, že respondenti budou z řad druhého stupně základních škol. Výzkum byl realizován na dvou základních školách ve Středočeském kraji.

V tabulce č. 1 je znázorněno konkrétní věkové rozdělení respondentů včetně podílu v procentech, v tabulce č. 2 rozdělení respondentů podle pohlaví a věku.

Tabulka 1: Podíl respondentů podle věku

Věk respondentů	Celkový počet respondentů	Podíl respondentů podle věku (%)
10	39	10,7
11	60	16,5
12	82	22,5
13	66	18,2
14	84	23,2
15	32	8,9

Zdroj: Vlastní zpracování v programu MS Word

Z tabulky je zřejmé, že nejpočetněji zastoupenou skupinou jsou 14 letí respondenti, kteří tvoří 23,2 % z celkového počtu, druhou nejpočetnější skupinou jsou 12 letí, kterých je 22,5 %. Nejmenší podíl tvoří děti ve věku 15 let (pouze 8,9 %).

Tabulka 2: Podíl respondentů podle věku a pohlaví

Věk respondentů	Chlapci	Dívky
10	15	24
11	34	26
12	44	38
13	42	24
14	35	49
15	19	13

Zdroj: Vlastní zpracování v programu MS Word

Nejvíce zastoupenou skupinou ve výzkumu jsou čtrnáctileté dívky, kterých je celkem 49, druhou nejpočetnější skupinou jsou dvanáctiletí chlapci v počtu 44 jedinců.

Výzkum byl realizován v období od 21.11.2022 do 16.12.2022 na dvou základních školách v České republice ve Středočeském kraji. Celkem bylo rozdáno 400 dotazníků. Na vyplnění dotazníku byl vymezen časový limit 15 minut. Při dotazníkovém šetření je důležité, aby měli respondenti záruku, že zjištěné skutečnosti nebudou proti nim zneužity, je tedy vhodné použití anonymních dotazníků. V úvodní části dotazníku byli proto respondenti upozorněni na to, že se jedná o anonymní dotazník a odpovědi budou využity pouze pro účely výzkumného projektu.

5.5 Vyhodnocení dotazníků

Každá položka dotazníku byla vyhodnocena samostatně, pro každé pohlaví zvlášť.

Položka č. 1 a položka č. 2 spolu souvisí, pokud respondenti uvedli u první položky kladnou odpověď, byli v další položce dotazováni na zabezpečení svého účtu na sociální síti.

Položka č. 1: Máš účet na sociálních sítích? Pokud ano, označ na kterých: K této položce byly na výběr odpovědi Ne / Ano: Messenger, WhatsApp, Snapchat, Instagram, Tik Tok, Facebook, YouTube a možnost doplnění další odpovědi, která nebyla součástí výběru.

Položka č. 2: Pokud máš účet na některé ze sociálních sítích, máš ho veřejně přístupný pro všechny, nebo zabezpečený, že informace vidí pouze lidé, které máš v přátelích? Jako odpovědi byly nabízeny varianty: veřejný / zabezpečený.

Na uvedené položky odpověděli všichni respondenti. Kladnou odpověď na položku č. 1 uvedlo celkem 349 respondentů, 169 dívek a 180 chlapců. Na sociálních sítích nemá účet celkem 14 respondentů, 3 dívky a 11 chlapců. Nejvíce využívanou sociální sítí je dle sdělení respondentů mezi oběma pohlavími WhatsApp, kdy tuto síť využívá celkem 166 chlapců a 163 dívek. Mezi druhou nejpočetněji využívanou sociální síť mezi chlapci patří YouTube, které označilo celkem 148 chlapců. Mezi dívkami je YouTube rovněž na druhém místě, o které se dělí se sociální sítí Tik Tok. Tyto sítě shodně označilo 127 dívek. Tik Tok je mezi chlapci třetí nejvíce zastoupená sociální síť, označilo ji celkem 137 chlapců. Na třetí pozici mezi dívkami se umístila sociální síť Snapchat, kterou označilo 123 dívek. Mezi chlapci se o čtvrtou pozici dělí Messenger, Snapchat a Instagram. Tyto sociální sítě shodně obdržely 114 hlasů. Mezi dívkami se na čtvrté pozici umístil Instagram, který označilo celkem 114 dívek. Na páté pozici se u chlapců umístil Facebook, který označilo celkem 91 chlapců. Celkem 97 dívek označilo sociální síť Messenger, kterému připadá 5 místo mezi dívkami. Z nabízených sociálních sítí má u obou pohlaví nejmenší zastoupení Facebook, který uvedlo, že používá 91 chlapců a 74 dívek. Mezi nejvíce zastoupenou sociální sítí, kterou respondenti uváděli v položce další sociální sítě patří Discord, který používá celkem 23 chlapců a 14 dívek.

Co se týče zabezpečení profilů, tak celkem 51 dívek uvedlo, že svůj profil má veřejně přístupný, zabezpečený profil má 105 dívek, 18 dívek nebylo hodnoceno z důvodu nezapsání odpovědi. Celkem 60 chlapců uvedlo, že má veřejně přístupný profil, 111 chlapců uvedlo, že má profil soukromý. Nehodnoceno bylo 18 respondentů z řad chlapců, kteří na uvedenou položku neodpověděli.

Podíl respondentů dle pohlaví na odpovědích u položek č. 1 a č. 2 znázorňují tabulky č. 3 a č. 4.

Tabulka 3: Máš účet na sociálních sítích? Pokud ano, označ na kterých:

Sociální síť	Chlapci	Dívky
Messenger	113	97
WhatsApp	166	163
Snapchat	114	123
Instagram	114	114
Tik Tok	137	127
Facebook	91	74
YouTube	148	127
Discord	23	14

Zdroj: Vlastní zpracování v programu MS Word

Tabulka 4: Pokud máš účet na některé ze sociálních sítích, máš ho veřejně přístupný pro všechny, nebo zabezpečený

	Chlapci	Dívky
Veřejný profil	61	49
Zabezpečený profil	112	107
Nehodnoceno	16	18

Zdroj: Vlastní zpracování v programu MS Word

Následující položkou bylo zjišťováno kolik času tráví děti na internetu. Položka č. 3: Kolik hodin denně trávíš na internetu? U této otázky byl zvolen uzavřený okruh odpovědí a to: méně než 1 hodinu, 1–2 hodiny a více jak 2 hodiny. Vyhodnocením položky č. 3 bylo zjištěno, že nejčetnější odpovědí mezi oběma pohlavími byla odpověď více než 2 hodiny. Tuto odpověď uvedlo celkem 123 chlapců a 83 dívek. Druhá nejpočetnější odpověď zněla 1–2 hodiny, kdy tuto možnost zvolilo celkem 59 chlapců a 81 dívek. Méně než 1 hodinu denně

strávenou na internetu zvolilo pouze 8 chlapců a 7 dívek. U této otázky byly vyřazeni celkem 3 respondenti, kdy se jednalo pouze o dívky. Důvodem vyřazení z vyhodnocení bylo nezaškrtnutí odpovědi. Odpovědi na položku č. 3znázorňuje tabulka č. 5.

Tabulka 5: kolik hodin denně trávíš na internetu?

	Chlapci	Dívky
Méně než 1 hodinu	8	7
1-2 hodiny	59	81
Více než 2 hodiny	123	83
Nehodnoceno	0	3

Zdroj: Vlastní zpracování v programu MS Word

Další položkou byla zjišťována nejčastější aktivita dětí na internetu. Položka č. 4: Co nejčastěji děláš na internetu? U této otázky bylo předem definováno pět možných odpovědí a to: hraji hry, píšu si s přáteli, vyhledávám různé informace, seznamuji se s novými lidmi, sleduji videa. Dále byla dána možnost uvést vlastní nejčastější aktivitu mimo definovaný výběr. U této položky bylo možné uvést pouze jednu odpověď. Vyhodnocením položky č. 4 bylo zjištěno, že mezi nejčastější aktivitu na internetu u chlapců patří hraní her, kdy tuto možnost zvolilo celkem 79 chlapců. Zde je patrný výrazný rozdíl mezi chlapci a dívkami, kdy hraní her jako nejčastější aktivitu prováděnou na internetu označily pouze 4 dívky. Na druhém místě se mezi chlapci umístilo sledování videí, kdy tuto možnost zvolilo celkem 51 respondentů, následuje dopisování s přáteli, které označilo celkem 20 chlapců. Vyhledávání informací jako nejčastější aktivitu na internetu uvedli pouze 3 chlapci. Z odpovědí na tuto položku je zřejmé, že u chlapců jednoznačně převládá hraní her jako nejčastější aktivita provozovaná na internetu. Nejčastější aktivitou dívek na internetu je sledování videí, kdy tuto možnost označilo 68 respondentů, následuje dopisování s přáteli, které označilo celkem 51 respondentů. Ostatní položky mají zanedbatelné hodnoty. Odpověď vyhledávám si různé informace uvedlo 6 respondentů, hraní her, jak již bylo uvedeno výše, označily 4 dívky a 3 dívky uvedly, že jejich nejčastější aktivita na internetu je

poslouchání hudby. Možnost seznamuji se s novými lidmi neuvedl žádný z dotazovaných respondentů z řad dívek, stejně tak mezi chlapci nebyla ani v jednom případě zvolena možnost poslouchám hudbu. Položku uvést vlastní nejčastější aktivitu prováděnou na internetu nevyužil žádný respondent. U této otázky bylo vyřazeno celkem 78 respondentů, kdy se jednalo o 36 chlapců a 42 dívek. Nejčastějším důvodem vyřazení z vyhodnocení bylo zaškrtnutí několika odpovědí, v některých případech pak nedošlo k zaškrtnutí odpovědi žádné. Odpovědi na položku č. 3 jsou znázorněny v tabulce č. 6.

Tabulka 6: Co nejčastěji děláš na internetu?

	Chlapci	Dívky
Hraju hry	79	4
Píšu si s přáteli	20	51
Vyhledávám informace	3	6
Seznamuji s lidmi	0	0
Sleduji videa	51	68
Poslouchám hudbu	0	3
Jiné	0	0
Nehodnoceno	36	42

Zdroj: Vlastní zpracování v programu MS Word

Položkou č. 5 v dotazníku bylo zjišťováno, zda děti někdy komunikují na internetu s neznámými lidmi. Na výběr byly u této otázky uzavřené odpovědi ANO/NE. U této otázky nebylo hodnoceno 5 chlapců, kteří nezaškrtli žádnou z nabízených odpovědí. Vyhodnocením položky č. 5 bylo zjištěno, že téměř polovina dotazovaných chlapců na internetu komunikuje s neznámými lidmi, konkrétně tuto možnost zvolilo 84 dotazovaných, celkem 100 chlapců uvedlo, že na internetu s neznámými lidmi nekomunikuje. Dívky jsou v tomto ohledu obezřetnější, dvě třetiny dotazovaných dívek uvedly, že na internetu s neznámými lidmi nekomunikuje, konkrétně tuto možnost uvedlo 121 dívek. Zbylých 53 dívek,

uvedlo, že má zkušenost s komunikací s neznámými lidmi. Odpovědi respondentů na položku č. 5 jsou znázorněny v tabulce č. 7.

Tabulka 7: Komunikuješ na internetu s neznámými lidmi?

	Chlapci	Dívky
ANO	84	53
NE	100	121
Nehodnoceno	5	0

Zdroj: Vlastní zpracování v programu MS Word

Položka č. 6: Slyšel/a si někdy pojem KYBERKRIMINALITA? K této položce byly na výběr odpovědi ANO/NE. Na tuto otázku odpovědělo všech 363 respondentů. Mezi chlapci jsou odpovědi na tuto otázku téměř vyrovnané. Převažuje však odpověď ANO, kterou uvedlo 97 chlapců. Odpověď NE pak uvedlo 92 chlapců. U dívek je situace zcela opačná, kdy 118 dotazovaných dívek uvedlo, že pojem kyberkriminalita nikdy neslyšely. Zbylých 56 dívek uvedlo, že o tomto pojmu již slyšely. Odpovědi respondentů na položku č. 6 znázorňuje tabulka č. 8.

Tabulka 8: Slyšel/a si někdy pojem KYBERKRIMINALITA?

	Chlapci	Dívky
ANO	97	56
NE	92	118

Zdroj: Vlastní zpracování v programu MS Word

Položkou č. 7 bylo zjišťováno, co si respondenti představují pod pojmem kyberkriminalita? Jednalo se o otevřenou otázku, a tak odpovědi respondentů byly velmi různorodé. Z tohoto důvodu byly vybrány 3 nejčastější odpovědi uváděné respondenty. Vyhodnocením této položky bylo zjištěno, že nejčastější odpovědi na tuto otázku byly u obou pohlaví shodné, a to kriminalita spáchaná na internetu, šikana a nevím. Zásadní rozdíl je v počtu jednotlivých odpovědí mezi chlapci a dívkami. Nejvíce chlapců, celkem 50 si pod pojmem kyberkriminalita představuje

kriminalitu spáchanou na internetu, zatímco nejvíce dívek, celkem 58 si pod tímto pojmem vybaví šikanu. Šikanu si pod pojmem kyberkriminalita představilo celkem 21 chlapců, totožný počet dívek si pod tímto pojmem představilo kriminalitu spáchanou na internetu. Shodný počet respondentů obou pohlaví, tedy 32 chlapců a 32 dívek uvedlo, že neví, co si má pod uvedeným pojmem představit. U této otázky bylo vyřazeno celkem 42 respondentů, kdy se jednalo o 17 chlapců a 25 dívek. Důvodem vyřazení z vyhodnocení bylo neuvedení odpovědi. Odpovědi na položku č. 7jsou vyobrazeny v tabulce č. 9.

Tabulka 9: Co si představuješ pojmem kyberkriminalita?

	Chlapci	Dívky
Kriminalita spáchaná na internetu	50	21
Šikana	21	58
Nevím	32	32
Nehodnoceno	17	25

Zdroj: Vlastní zpracování v programu MS Word

Položka č. 8 je rovněž otevřenou otázkou, která zní: Jaké je podle tebe největší riziko na internetu? V tomto případě byly odpovědi respondentů také různorodé, a proto byly pro účely hodnocení vybrány 3 nejčastější odpovědi chlapců a 3 nejčastější odpovědi dívek. U této otázky bylo vyřazeno celkem 43 respondentů, kdy se jednalo o 18 chlapců a 25 dívek. Důvodem vyřazení z vyhodnocení bylo neuvedení odpovědi. Vyhodnocením položky č. 7 bylo zjištěno, že více než polovina všech dotazovaných chlapců, celkem 97 největší riziko na internetu spatřuje v možnosti odcizení dat. Na druhém místě se u chlapců nejčastěji objevila odpověď vydírání, kterou uvedlo 22 ze všech dotazovaných chlapců a na třetím místě se umístila odpověď nevím. Dívky také vidí největší riziko na internetu v krádeži dat, avšak tuto odpověď uvedlo pouze 41 všech dotazovaných, mezi další nejčastěji uváděné riziko na internetu podle dívek patří šikana, takto odpovědělo 28 všech dotázaných dívek. Na třetí pozici se dle dívek umístilo vydírání. Odpovědi na položku č. 8jsou znázorněny v tabulce č. 10.

Tabulka 10: Jaké je podle tebe největší riziko na internetu?

	Chlapci	Dívky
Krádež dat	97	41
Vydírání	22	19
Nevím	19	0
Šikana	10	28
Nehodnoceno	18	25

Zdroj: Vlastní zpracování v programu MS Word

Další položkou bylo zjišťováno, zda děti od někoho slyšely o rizicích internetu. Položka č. 9: Bavil se s tebou někdo o rizicích internetu? U této položky byl předem stanoven výběr odpovědí: NE, rodiče, spolužáci/kamarádi, beseda ve škole a beseda mimo školu. U této položky byla dána možnost označit více odpovědí. Vyhodnocením dotazníku bylo zjištěno, že nejvíce chlapců celkem 101 získalo informace o rizicích internetu od svých rodičů. Jako druhá nejvíce označovaná odpověď ze strany chlapců zněla beseda ve škole, kterou označilo celkem 68 chlapců, následuje odpověď spolužáci/kamarádi, kterou označilo 35 chlapců. Celkem 27 chlapců uvedlo, že se s nimi nikdo o rizicích internetu nebavil. Na poslední příčce se umístila odpověď beseda mimo školu, kterou označilo 18 chlapců. Umístění odpovědí dívek koresponduje s umístěním odpovědí chlapců. Nejvíce dívek, celkem 139 uvedlo, že o rizicích internetu slyšely od svých rodičů. Následuje odpověď beseda ve škole, kterou označilo celkem 58 dívek, mírný pokles zaznamenala odpověď spolužáci/kamarádi, kterou označilo celkem 53 dívek. Variantu, že se s dívkami o rizicích nikdo nebavil uvedlo celkem 22 dívek a 6 jich uvedlo, že o této problematice se dozvěděly na besedě mimo školu. U této položky nebylo hodnoceno celkem 10 respondentů, 8 chlapců a 2 dívky, důvodem bylo neuvedení žádné odpovědi. Odpovědi na položku č. 9 uvádí tabulka č. 11.

Tabulka 11: Bavil se s tebou někdo o rizicích internetu?

	Chlapci	Dívky
NE	27	22
Rodiče	101	139
Spolužáci/kamarádi	35	53
Beseda ve škole	68	58
Beseda mimo školu	18	6
Nehodnoceno	8	2

Zdroj: Vlastní zpracování v programu MS Word

Znění položky č. 10: Stal/a ses někdy obětí útoku na internetu? U této položky byl zvolen předem definovaný okruh odpovědí: NE, ANO – jednou, ANO – vícekrát. Na tuto otázku odpovědělo všech 363 respondentů. Nejčastější odpovědí u této otázky byla NE. Tuto označilo celkem 164 chlapců a 135 dívek. Odpověď ANO – jednou zvolilo celkem 21 chlapců a 26 dívek a ANO – vícekrát uvedli 4 chlapci a 13 dívek. Vyhodnocením této položky bylo zjištěno, že obětmi útoků na internetu se častěji stávají dívky. Odpovědi respondentů na položku č. 10 jsou vyobrazeny v tabulce č. 12.

Tabulka 12: Stal/a ses někdy obětí útoku na internetu?

	Chlapci	Dívky
NE	164	135
Ano – jednou	21	26
Ano – vícekrát	4	13

Zdroj: Vlastní zpracování v programu MS Word

Další položkou bylo zjišťováno, jaký druh útoku byl na dětech spáchán. Položka č. 11: Pokud jsi na předchozí otázku odpověděl/a ANO, uveď, o jaký útok se jednalo. U této položky byly předem stanoveny možnosti odpovědí a to: vydírání,

šikana, vyhrožování, podvod a dále byla možnost uvést jednání, jenž není uvedeno v seznamu odpovědí. Počet možných odpovědí nebyl omezený. Z odpovědí je patrné, že chlapci se nejčastěji stali obětí podvodu, kdy tuto možnost zvolilo 22 respondentů. Celkem 7 chlapců uvedlo, že se stalo obětí šikany a totožný počet chlapců označilo vyhrožování. Možnost vydírání zvolili celkem 4 chlapci. Dívky se v nejvyšší míře staly obětí vyhrožování, kdy tuto možnost označilo 21 dívek. Následuje šikana, která byla označena celkem 10 ti dívkami. Obětí podvodu se dle dotazníkového šetření stalo celkem 9 dívek, 5 dívek uvedlo, že se stalo obětí vydírání. Mezi jinými útoky na internetu bylo ze strany dívek ve 4 případech uvedeno posmívání. Chlapci se s jiným, než uvedeným jednáním v dotazníku nesetkali. Ve dvou případech nebyla položka č. 11 u dívek hodnocena, a to z důvodu neoznačení odpovědi. Odpovědi respondentů na položku č. 11 jsou vyobrazeny v tabulce č. 13.

Tabulka 13:Pokud jsi na předchozí otázku odpověděl/a ANO, uveď, o jaký útok se jednalo.

	Chlapci	Dívky
Vydírání	4	5
Šikana	7	10
Vyhrožování	7	21
Podvod	22	9
Posmívání	0	4
Nehodnoceno	0	2

Zdroj: Vlastní zpracování v programu MS Word

Další položkou bylo zjišťováno, zda se dětské oběti s útokem někomu svěřily. Položka č. 12: Pokud jsi se stal obětí útoku na internetu, uveď, zda jsi o útoku někomu řekl? Odpovědi na uvedenou otázku byly polootevřené, NE – proč? Ano – komu? Vyhodnocením této položky bylo zjištěno, že v případě útoku se děti v drtivé většině svěří. U obou pohlaví převládá rodina, kdy tuto odpověď uvedlo celkem 13 chlapců a 31 dívek. U chlapců se mezi odpověďmi objevili také kamarádi, kterým se s útokem na internetu svěřili 4 chlapci a 2 chlapci v dotazníkovém šetření uvedli, že se svěřili, avšak neuvedli komu. V případě

odpovědi NE – a proč? dva chlapci uvedli jako důvod strach, další 4 chlapci u odpovědi NE neuvedli důvod. Celkem 4 dívky u odpovědi NE jako důvod svého počínání uvedly nepochopení, další 2 pak strach a zbylé 2 neuvedly důvod. Odpovědi respondentů jsou zobrazeny v tabulkách č. 14 a 15.

Tabulka 14: Pokud jsi se stal obětí útoku na internetu, uveď, zda jsi o útoku někomu řekl?

ANO	Chlapci	Dívky
Rodina	13	31
Kamarádi	4	0
Neuvedeno	2	0

. Zdroj: Vlastní zpracování v programu MS Word

Tabulka 15: Pokud jsi se stal obětí útoku na internetu, uveď, zda jsi o útoku někomu řekl?

NE	Chlapci	Dívky
Nepochopení	0	4
Strach	2	2
Neuvedeno	4	2

Zdroj: Vlastní zpracování v programu MS Word

Poslední položka dotazníku č.13 má znění: Měl/a bys zájem dozvědět se o kyberkriminalitě více informací v rámci besedy nebo přednášky ve škole? U této otázky byly na výběr pouze dvě možnosti ANO/NE. Převážná většina všech dotazovaných respondentů projevila zájem dozvědět se více informací v rámci přednášky nebo besedy ve škole. Odpověď ANO uvedlo celkem 281 respondentů, z toho 138 chlapců a 143 dívek. O informace vztahující se ke kyberkriminalitě nemá zájem celkem 79 respondentů, 49 chlapců a 30 dívek. U této položky nebyly hodnoceny celkem 3 respondenti, 2 chlapci a 1 dívka, a to z důvodu neoznačení žádné z odpovědí. Odpovědi na položku č. 13 jsou vyobrazeny v tabulce č. 16.

Tabulka 16: Měl/a bys zájem dozvědět se o kyberkriminalitě více informací v rámci besedy nebo přednášky ve škole?

	Chlapci	Dívky
ANO	138	143
NE	49	30
Nehodnoceno	2	1

Zdroj: Vlastní zpracování v programu MS Word

5.6 Shrnutí výsledků dotazníku

Výzkumné šetření bylo zaměřené na děti druhého stupně základních škol a týkalo se zjišťování jejich názorů a zkušeností s internetovým prostředím v souvislosti s kyberkriminalitou. Provedeným šetřením bylo zjištěno, že v současné době jsou žáci na sociálních sítích stále aktivnější. Pouze 14 respondentů (3,9 %) z celkového počtu 363 respondentů uvedlo, že neužívá žádné sociální sítě. Nejvíce užívanou sociální sítí je WhatsApp, kde má svůj účet 329 respondentů (90,6 %), následuje YouTube, na kterém má svůj účet celkem 275 žáků (75,7 %). Na třetím místě se umístila sociální síť Tik Tok, kterou užívá 264 žáků (72,7 %). Dále následuje Snapchat s 237 uživateli (65,2 %), Instagram, který používá 228 žáků (62,8 %), Messenger, na kterém je registrováno 210 žáků (57,8 %). Na sociální síti Facebook má svůj účet méně než polovina dotazovaných, konkrétně 165 žáků (45,5 %).

Co se týče zabezpečení profilů, více než polovina dotazovaných uvedla, že má své profily zabezpečené. Zabezpečený profil má cekem 219 respondentů (60,3 %). Podíl nezabezpečených profilů mezi chlapci a dívkami je obdobný 32,2 % chlapců a 28,1 % dívek. Z výzkumného šetření dále vyplývá, že děti tráví na internetu velkou část svého volného času. Více než 2 hodiny denně stráví na internetu 206 respondentů (56,7 %), pouze 15 respondentů (4,1 %) z řad dívek i chlapců tráví na internetu denně méně než hodinu. Chlapci nejčastěji internet využívají ke hraní her, což uvedlo 79 chlapců (41,8 %), následuje sledování videí 51 chlapců (27 %). Dívky nejčastěji tráví čas na internetu sledováním videí, což

uvedlo 68 dívek (39 %), na druhé pozici se umístilo dopisování s přáteli, které označilo jako nejčastější činnost na internetu 51 dívek (29,3 %). Zde je patrný značný rozdíl mezi činností chlapců a dívek. V komunikaci s neznámými lidmi na internetu jsou opatrnější dívky, 121 dívek (69,5 %) uvedlo, že s cizími lidmi na internetu nekomunikuje, u chlapců je tento počet nižší, konkrétně se takto vyjádřilo 100 chlapců (52,9 %).

Výsledky provedeného výzkumu ukázaly, že žáci mají nedostatečné znalosti v oblasti kyberkriminality – celkem 210 respondentů (57,8 %) nikdy neslyšelo o pojmu kyberkriminalita. Na otázku, co si respondenti představují pod pojmem kyberkriminalita, byla nejčastější odpovědí šikana, kterou uvedlo celkem 79 dotazovaných (21,8 %), následovala odpověď kriminalita spáchaná na internetu, kterou uvedlo 71 respondentů (19,6 %). Celkem 64 respondentů (17,6 %) odpovědělo, že neví a 42 respondentů (11,6 %) v této otázce nebylo hodnoceno z důvodu neuvedení odpovědi, z čehož lze usuzovat, že rovněž nevěděli, co mají odpovědět. Největší riziko na internetu žáci spatřují v krádeži dat – takto se vyjádřilo 138 respondentů (38 %), následuje možnost vydírání, kterou uvedlo 41 dotazovaných (11,3 %).

Informace o rizicích internetu získávají žáci nejčastěji od rodičů (44,7 % respondentů), dále na školních besedách (23,5 % respondentů) a od svých kamarádů (16,4 % respondentů). Obětí útoku na internetu se stalo 64 respondentů (17,6 %), z toho 47 (73,4 %) bylo obětí útoku na internetu více než jednou. Nejčastěji se jednalo o podvod, který byl uveden v 31 případech (34 %), následovalo vyhrožování v 28 případech (30,8 %). Z provedeného výzkumu dále vyplývá, že 78,1 % žáků, kteří se stali obětí útoku na internetu, se v převážné většině s útokem svěřili, a to zejména své rodině, což uvedlo 68,8 % respondentů. Naopak s útokem se nesvěřilo 21,9 % respondentů, kdy mezi hlavní důvody patří nepochopení a strach. V poslední řadě bylo v dotazníkovém šetření zjišťováno, zda by žáci měli zájem dozvědět se více informací o kyberkriminalitě v rámci besedy či přednášky ve škole. Z dotazníkového šetření jednoznačně vyplynulo, že žáci mají zájem získat další informace o kyberkriminalitě. Takto se vyjádřilo 77,4 % respondentů.

6 Závěr

Diplomová práce se zabývá problematikou mládeže a kyberkriminality, neboť právě skupina dětí a dospívajících patří mezi nejvíce ohroženou část populace ve vztahu k tomuto druhu trestné činnosti. Mladí lidé tráví na internetu velké množství svého volného času a často si vůbec neuvědomují rizika, která se s jeho užíváním pojí. Internet často využívají už i děti v předškolním věku, školní děti pak berou toto prostředí jako samozřejmou součást svých životů, přičemž množství času, které v kyberprostoru denně tráví, je alarmující.

Je proto velmi důležité zacílit prevenci rizikového chování v kybernetickém prostoru již na děti na prvních stupních základních škol, neboť jak z výsledků výzkumu této diplomové práce vyplynulo, téměř všechny děti na druhém stupni základní školy vlastní účty na sociálních sítích a denně tráví na internetu velkou část svého volného času. Z výzkumu rovněž vyplývá, že ačkoliv více jak polovina dětí si počíná ve virtuálním světě opatrně a chrání si své soukromí, téměř 40% dotazovaných dětí sdílí obsah svých účtů na sociálních sítích veřejně a komunikuje s neznámými osobami. Problémem je skutečnost, že s některými dětmi se nikdo o rizicích a hrozbách, které se pojí s internetovým prostředím, nikdy nebavil, většina dětí má informace od rodičů nebo učitelů ze školy. Otázkou je, do jaké míry jsou rodiče či učitelé schopni dětem poskytnout adekvátní informace o této problematice, moderní technologie jdou každým dnem kupředu a praktiky internetových podvodníků a predátorů se velmi rychle mění, to, co platilo včera, nemusí platit dnes. Nejaktuálnější a nejpřesnější informace mohou veřejnosti poskytnout tedy pouze osoby zabývající se problematikou kyberkriminality na profesní úrovni, které však bohužel kvůli svému pracovnímu vytížení nemají na tyto aktivity čas.

Výsledky diplomové práce, které zahrnují postoje, názory a zkušenosti dětí ve vztahu ke kybernetickému prostředí, by mohly sloužit jako podklad pro tvorbu preventivních opatření a programů na základních školách, významné by mohly být rovněž pro policejní preventisty, kteří se uvedené problematice při besedách ve školách rovněž okrajově dotýkají.

7 Seznam použité literatury

Monografie

BURIAN Pavel. *Internet inteligentních aktivit*. Praha: Grada, 2014. ISBN 978-80-247-5137-5.

ČERNÁ Alena. *Kyberšikana.* Praha: Grada, 2013. ISBN 978-80-247-4577-0.

DOČEKAL Daniel a kol. *Dítě v síti*. Preface 2019. ISBN 978-80-204-5145-3.

FISCHER Slavomil, Jiří ŠKODA. *Sociální patologie*. Závažné sociálně patologické jevy, příčiny, prevence, možnosti řešení. 2 vydání. Praha: Grada. ISBN 978-80-247-5046-0

GŘIVNA, T., M. SCHEINOST, I. ZOUBKOVÁ a kol. *Kriminologie*. Praha: WoltersKluwer, 2014. ISBN 978-80-7478-614-3.

KOLOUCH Jan, Pavel Bašta. *CyberSecurity.* Praha: CZ.NIC,2019. ISBN 978-80-88168-31-7.

KOLOUCH Jan. *CyberCrime*. Praha: CZ.NIC, 2016. ISBN 978-80-88168-15-7.

KOŽÍŽEK M. *Bezpečně na internetu*. Praha: Grada, 2016. ISBN 978-80-247-5595-3.

MAREŠOVÁ Alena. *Kriminalita mládeže v podmínkách současné české společnosti*. Praha 2018. ISBN 978-80-7251-483-0.

NOVOTNÝ, F. *Trestní právo hmotné*. Plzeň:Aleš Čeněk, 2017. ISBN 978-80-7380-651-4.

NOVOTNÝ, O., M. ŠTIKA a Z. BOLELOUCKÝ. *Kriminologie*. Praha: ASPI, 2004. ISBN 80-735-7026-2.

SMEJKAL Vladimír. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015. ISBN 978-80-7380-501-2.

VÁLKOVÁ Helena, Josef KUCHTA, Jana HULMÁKOVÁ a kol. *Základy kriminologie a trestní politiky*. 3. vydání 2019, 664 s. Praha: Nakladatelství C. H. Beck, ISBN 978-80-7400-732-3.

Právní předpisy a interní akty řízení

Zákon č. 181/2014 Sb., *zákon o kybernetické bezpečnosti* v posledním znění.

Zák. č. 40/2009 Sb., *trestní zákoník* v posledním znění.

Elektronické zdroje

Bezpečný středočeský kraj. [online]. [cit. 2022-12-03]. Dostupné z: Bezpečný Středočeský Kraj | Kyberkriminalita | PČR - Bezpečný Středočeský Kraj (bezpecnystredoceskykraj.cz).

GILLESPIE A. Alisdair. *Cybercrime: Key Issues and Debates*. [online]. [cit. 2022-12-03]. Dostupné z: https://books.google.cz/books?id=0N4sCgAAQBAJ&pg=PA3&dq=cybercrime&hl=cs&sa=X&ved=2ahUKEwjGr6-q4sf8AhX-gP0HHedpCSoQ6AF6BAgGEAI#v=onepage&q=cybercrime&f=false.

HOLT J. Thomas and Adam M. Bossler. *Cybercrime and Digital Forensics: An Introduction*. [online]. [cit. 2022-12-03]. Dostupné z: Cybercrime and Digital Forensics: An Introduction - Thomas J. Holt, Adam M. Bossler, Kathryn C. Seigfried-Spellar - Knihy Google.

Kyberkriminalita na vzestupu. [online]. [cit. 2022-12-03]. Dostupné z: https://echo24.cz/a/SiF29/hackeri-kyberneticka-kriminalita-zlociny-policie-ncoz-internet.

Kyberkriminalita [online]. [cit. 2022-12-03]. Dostupné z: Zneužívání dětí na internetu - Policie České republiky.

NAM H Nguyen. *Essential Cyber Secutity Handbook*. 2018. [online]. [cit. 2022-12-03]. Dostupné z: Essential Cyber Security Handbook In Slovak - Nam H Nguyen - Knihy Google.

Ochrana dítěte v online prostředí. [online]. [cit. 2022-12-02]. Dostupné z: Ochrana dítěte v online prostředí - INTERNETEM BEZPEČNĚ (internetembezpecne.cz)

Ochraňme své děti před nebezpečím internetu. [online]. [cit. 2023-01-03]. Dostupné z: https://www.zenax.cz/ochranme_sve_deti_pred_nebezpecim_internetu_14237.htm.

Policie CZ, Zneužívání dětí na internetu. [online]. [cit. 2022-12-03]. Dostupné z: Zneužívání dětí na internetu - Policie České republiky.

Prevence kyberkriminality. [online]. [cit. 2022-12-04]. Dostupné z: https://www.policie.cz/clanek/prevence-kyberkriminality.aspx.

Rozcestník kyberkriminality. [online]. [cit. 2022-12-02]. Dostupné z: Rozcestník kyberkriminality – Prevence kriminality.

Statistika kybernetické kriminality za rok 2019. [online]. [cit. 2022-12-04]. Dostupné z: https://www.e-bezpeci.cz/index.php/z-jinych-webu/1749-statistika-kyberneticke-kriminality-za-rok-2019.

Tvoje cesta onlinem. [online]. [cit. 2022-12-05]. Dostupné z: https://www.policie.cz/clanek/tvoje-cesta-onlinem.aspx.

Vnímání kyberkiminality mezi dětmi. [online]. [cit. 2022-12-03]. dostupné z: Vnímání kyberkriminality mezi dětmi | Zájmové a neformální vzdělávání (npi.cz).

ZPRÁVA O SITUACI V OBLASTI VNITŘNÍ BEZPEČNOSTI A VEŘEJNÉHO POŘÁDKU NA ÚZEMÍ ČESKÉ REPUBLIKY V ROCE 2020. [online]. [cit. 2023-02-03]. Dostupné z: https://prevencekriminality.cz/zprava-o-situaci-v-oblasti-vnitrni-bezpecnosti-a-verejneho-poradku-na-uzemi-cr-v-roce-2020/.

ZPRÁVA O SITUACI V OBLASTI VNITŘNÍ BEZPEČNOSTI A VEŘEJNÉHO POŘÁDKU NA ÚZEMÍ ČESKÉ REPUBLIKY V ROCE 2021. [online]. [cit. 2022-12-03]. Dostupné z: https://www.mvcr.cz/clanek/statistiky-kriminality-dokumenty.aspx.

8 Seznam grafů, tabulek a příloh

Seznam grafů

Seznam tabulek

Seznam příloh

Jmenuji se Miroslav Dušek a studuji obor Policejní management a kriminalistika na Policejní akademii v Praze. Tento dotazník byl vytvořen za účelem zjištění, jaké povědomí mají děti a mladiství o problematice kyberkriminality a slouží jako podklad k mé diplomové práci. Dotazník je anonymní, odpovědi budou využity pouze pro účely mého výzkumného projektu. Za vyplnění dotazníku předem velmi děkuji.

Zakroužkuj prosím vždy pouze jednu odpověď, se kterou nejvíce souhlasíš nebo doplň svou odpověď do prázdného řádku.

Označ svůj věk: 10 11 12 13 14 15

Pohlaví: chlapec dívka

1.) **Máš účet na sociálních sítích? Pokud ano, označ, na kterých:.**

- Ne
- Ano

Messenger Instagram Facebook

Whatsapp Tik Tok Youtube

Snapchat Na dalších (jakých) ……

2.) **Pokud máš účet na některé ze sociálních sítí, máš ho veřejně přístupný pro všechny, nebo zabezpečený tak, že informace vidí pouze lidé, které máš v přátelích?**

Veřejný Zabezpečený

3.) Kolik hodin denně trávíš na internetu?

Méně než 1 hodinu 1 – 2 hodiny Více jak 2 hodiny

4.) Co nejčastěji děláš na internetu? (Vyber pouze jednu odpověď)

Hraju hry Seznamuji se s novými lidmi

Píšu si s přáteli Sleduji videa

Vyhledávám si různé informace Jiné ……..

5.) Komunikuješ někdy na internetu s lidmi, které ve skutečnosti neznáš?

ANO NE

6.) Slyšel/a jsi někdy pojem KYBERKRIMINALITA?

ANO NE

7.) Co si představíš pod pojmem KYBERKRIMINALITA?

……..

8.) Jaké je podle tebe největší riziko na internetu?

…….

.

9.) Bavil se s tebou někdo o rizicích internetu? (Zde můžeš zakroužkovat více odpovědí.)

NE rodiče spolužáci/kamarádi beseda ve škole beseda mimo školu

10.) Stal/a ses někdy obětí útoku na internetu?

NE ANO – jednou ANO – vícekrát

11.) Pokud jsi na předchozí otázku odpověděl/a ANO, uveď, o jaký útok se jednalo:

vydírání šikana vyhrožování podvod jiné ……..……

12.) Měl/a bys zájem dozvědět se o kyberkriminalitě více informací v rámci besedy nebo přednášky ve škole?

ANO NE