Ohrožení mládeže v kyberprostoru a jeho prevence

Tomáš Mička

Bakalářská práce
2024

Univerzita Tomáše Bati ve Zlíně
Fakulta humanitních studií

Univerzita Tomáše Bati ve Zlíně
Fakulta humanitních studií
Ústav pedagogických věd

Akademický rok: 2023/2024

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Tomáš Mička**
Osobní číslo:	**H20482**
Studijní program:	**B0111A190011 Sociální pedagogika**
Forma studia:	**Kombinovaná**
Téma práce:	**Ohrožení mládeže v kyberprostoru a jeho prevence**

Zásady pro vypracování

Zpracování rešerše a studium odborné literatury.
Vymezení terminologie a teoretických východisek z oblasti vývojových specifik dospívajících, současné kyberkriminality a možností sociální pedagogiky v její prevenci.
Příprava metodiky empirické části, zpracování projektu výzkumu a stanovení výzkumného problému.
Realizace kvantitativního výzkumu formou obsahové analýzy.
Zpracování a vyhodnocení získaných dat, včetně jejich interpretace.
Prezentace výsledků výzkumu, jejich shrnutí a doporučení pro praxi.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

ABU-TAIEH, Evon, 2020. Cyberspace. London: Intechopen. ISBN 978-1-78985-857-0.
BAŠTA, Pavel, 2020. Cybersecurity. Praha: CZ.NIC. ISBN 978-80-88168-34-8.
MARTÍNEK, Zdeněk, 2015. Agresivita a kriminalita školní mládeže. Praha: Grada. ISBN 978-80-247-9760-1.
SMEJKAL, Vladimír, 2022. Kybernetická kriminalita. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 978-80-7380--849-5.
VOJTÍŠEK, Petr, 2012. Výzkumné metody. Praha: Vyšší odborná škola sociálně právní. ISBN 978-80-905109-3-7.

Vedoucí bakalářské práce: **PhDr. Hana Včelařová, Ph.D.**
Ústav pedagogických věd

Datum zadání bakalářské práce: **10. ledna 2024**
Termín odevzdání bakalářské práce: **26. dubna 2024**

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta humanitních studií
L.S.

Mgr. Libor Marek, Ph.D.
děkan

doc. Mgr. Jakub Hladík, Ph.D.
ředitel ústavu

Ve Zlíně dne 10. ledna 2024

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že

- odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby [1];
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k nahlédnutí;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3 [2];
- podle § 60 [3] odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 [3] odst. 2 a 3 mohu užít své dílo - bakalářskou práci - nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům.

Prohlašuji, že

- elektronická a tištěná verze bakalářské práce jsou totožné;
- na bakalářské práci jsem pracoval(a) samostatně a použitou literaturu jsem citoval(a). V případě publikace výsledků budu uveden(a) jako spoluautor.

Ve Zlíně .....

1) zákon č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, § 47b Zveřejňování závěrečných prací:

(1) Vysoká škola nevýdělečně zveřejňuje disertační, diplomové, bakalářské a rigorózní práce, u kterých proběhla obhajoba, včetně posudků oponentů a výsledku obhajoby prostřednictvím databáze kvalifikačních prací, kterou spravuje. Způsob zveřejnění stanoví vnitřní předpis vysoké školy.

(2) Disertační, diplomové, bakalářské a rigorózní práce odevzdané uchazečem k obhajobě musí být též nejméně pět pracovních dnů před

konáním obhajoby zveřejněny k nahlížení veřejnosti v místě určeném vnitřním předpisem vysoké školy nebo není-li tak určeno, v místě pracoviště vysoké školy, kde se má konat obhajoba práce. Každý si může ze zveřejněné práce pořizovat na své náklady výpisy, o pisy nebo rozmnoženiny.
(3) Platí, že odevzdáním práce autor souhlasí se zveřejněním své práce podle tohoto zákona, bez ohledu na výsledek obhajoby.

2) zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, § 35 odst. 3:
(3) Do práva autorského také nezasahuje škola nebo školské či vzdělávací zařízení, užije -li nikoli za účelem přímého nebo nepřímého hospodářského nebo obchodního prospěchu k výuce nebo k vlastní potřebě dílo vytvořené žákem nebo studentem ke splnění školních nebo studijních povinností vyplývajících z jeho právního vztahu ke škole nebo školskému či vzdělávacího zařízení (školní dílo).

3) zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, § 60 Školní dílo:
(1) Škola nebo školské či vzdělávací zařízení mají za obvyklých podmínek právo na uzavření licenční smlouvy o užití školního díla (§ 35 odst. 3). Odpírá-li autor takového díla udělit svolení bez vážného důvodu, mohou se tyto osoby domáhat nahrazení chybějícího projevu jeho vůle u soudu. Ustanovení § 35 odst. 3 zůstává nedotčeno.
(2) Není -li sjednáno jinak, může autor školního díla své dílo užít či poskytnout jinému licenci, není -li to v rozporu s oprávněnými zájmy školy nebo školského či vzdělávacího zařízení.
(3) Škola nebo školské či vzdělávací zařízení jsou oprávněny požadovat, aby jim autor školního díla z výdělku jím dosaženého v souvislosti s užitím díla či poskytnutím licence podle odstavce 2 přiměřeně přispěl na úhradu nákladů, které na vytvoření díla vynaložily, a to podle okolností až do jejich skutečné výše; přitom se přihlédne k výši výdělku dosaženého školou nebo školským či vzdělávacím zařízením z užití školního díla podle odstavce 1.

ABSTRAKT

Bakalářská práce se zaměřuje na kyberkriminalitu u mladistvých a dospívajících dětí. První kapitola zvaná Vývojová specifika dospívajících skupin pojednává o jejich vývinu. Druhá kapitola zavede čtenáře do podoby kyberkriminality a jejímu vývoji. Ve třetí kapitole s názvem možnosti sociální pedagogiky při prevenci páchání kyberkriminality se práce zabývá prevencí u mladistvých osob.

Cílem praktické části práce bylo zjistit, zda a v jakých oblastech dochází k ohrožení mládeže v kyberprostoru a jaké jsou zkušenosti s efektivní prevencí těchto konkrétních ohrožení. Pro naplnění výzkumných cílů byl použit kvantitativní přístup a nashromážděná data Policií České republiky.

Klíčová slova: kyberkriminalita, prevence kyberkriminality, sociální pedagogika

ABSTRACT

The bachelor's thesis focuses on cybercrime in adolescent and teenage children. The first chapter, Developmental Specifics of Adolescents, discusses the development of adolescents. The second chapter introduces the reader to cybercrime and its development. In the third chapter, entitled Social Pedagogy's Options for Preventing Cybercrime, the thesis discusses prevention in adolescents.

The aim of the practical part of the thesis was to find out whether and in what areas youth are threatened in cyberspace and what experiences there are in effectively preventing these particular threats. A quantitative approach and data collected by the Police of the Czech Republic were used to meet the research objectives.

Key words: cybercrime, cybercrime prevention, social pedagogy

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Uherské Hradiště 2024 Tomáš Mička

OBSAH

ÚVOD

Kybernetická kriminalita je v oblasti informačních technologií stále častějším jevem. S rozvojem digitálního prostředí a internetu vznikají nové možnosti páchání trestné činnosti prostřednictvím počítačových sítí a elektronických zařízení. Počítačová kriminalita zahrnuje širokou škálu trestných činů, jako jsou hackerské útoky, podvody, šíření škodlivého softwaru a kyberšikana.

Práce je rozdělena na část teoretickou a část praktickou. Teoretická východiska práce se skládají ze tří kapitol, a to Specifika dospívajících skupin, Kyberkriminalita a její vývoj, Možnosti sociální pedagogiky při prevenci páchání kyberkriminality.

V praktické části je prezentován vývoj kyberkriminality u mladistvých od roku 2019 až do roku 2023. Data jsou vyhodnocena za celou ČR a za jednotlivé kraje.

Věřím, že tato práce přispěje k lepšímu popsání problematiky kyberkriminality u mladistvých.

I. TEORETICKÁ ČÁST

1 VÝVOJOVÁ SPECIFIKA DOSPÍVAJÍCÍCH SKUPIN

„Vývojové změny v daném věku lze očekávat, ale vývoj nelze zobecňovat, protože lidský jedinec je jedinečný a neopakovatelný“ (Šimíčková-Čížková, 2003).

Definice

Vývojové skupiny jsou skupiny jedinců v různých věkových obdobích, které mají společné zkušenosti a úkoly spojené s jejich vývojem a růstem. Tato koncepce byla poprvé prezentována psychologem Erikem Eriksonem, který identifikoval různá věková období a specifické úkoly, které jedinci v každé fázi svého života musí splnit pro dosažení psychického zdraví a celkového rozvoje osobnosti. Mezi vývojové skupiny patří kojenci, batolata, dospívající nebo dospělí (Erik Erikson, 2002).

1.1 Období adolescence

Do dospívání vstupujeme ve věku od deseti let a zakončujeme toto období přibližně ve věku dvaceti let. Tomu se říká přechod mezi dětstvím a dospíváním. Během tohoto období člověk zažívá mnoho změn, ale to je fyzická, psychologická a sociální sféra. Dospívání je období, kdy se konkrétní jedinec snaží měnit v závislosti na společenském postavení, zkoumá a přehodnocuje svou osobnost, takže hlavním úkolem vývoje souvisejícího s obdobím, kdy se formuje jeho identita, je objevit sám sebe. Identita nám umožňuje vidět svět autonomně, důsledně a zodpovědně. Identita není dokončený proces puberty, je spojena pouze s nepřetržitým procesem sebepoznání. Je důležité být schopen řídit svůj život způsobem, který kombinuje minulé a současné zkušenosti a nápady do jednoho celku. Ale způsob, jakým člověk dosahuje autonomie, identity a odpovědnosti dospělých, je velmi osobní a každý to může dělat v různých věkových kategoriích. Dnešní mladí lidé se snaží toto období urychlit, aby se co nejdříve zbavili dětských vlastností a tzv. dětských návyků. Sociálně závislí a dospělí požadují stejná práva a nadřazenost, ale málokdy mají stejné povinnosti. Ve srovnání s minulým stoletím začíná dospívání o něco dříve a jeho trvání se ještě prodloužilo. V důsledku toho se dospívající většinou vzdělávají, žení a vdávají a vychovávají děti v pozdějším věku. Moderní definice dospívání odpovídá věku 10-24 let. V této fázi vývoje se lidé nezařazují do žádné skupiny, protože se liší jak od dospělých, tak od dětí. Například oblečením, účesem, barvou vlasů a výrazem obličeje. Tyto detaily mohou vytvořit subkulturu, která se zcela liší od dospělých i dětí. Tyto způsoby chování mohou také vést k nebezpečným způsobům posilování vlastní identity. Během dospívání se objevují individuální stavy. Tyto stavy nejsou trvalé a jsou vyvolány

reakcemi na určité situace. Člověk může snadno zažít všechny čtyři identity. V době dosažení prvního stavu identity již dospívající zažil krizi identity a má určité zkušenosti, které přispívají k posílení identity. Prvního stavu identity je dosaženo, když člověk neprožívá krizi identity a přijímá identitu, která může být dána pouze s pomocí druhých. Stav identity je moratorium, které nastává u lidí, kteří prožívají krizi identity, mají stále se měnící přesvědčení a postoje, mají za sebou dlouhé zkušenosti a nesou si je, jako by si je nepamatovali. Čtvrtým stavem identity je difúze, kdy se člověk chová nezrale a nezískává přesvědčení a postoje. Dospívající potřebuje najít cíl, kterého by chtěl dosáhnout. Takovým cílem je volba povolání. Je to proto, že někteří nemají zcela oddělené zájmy, někteří pracují, někteří nemají plně rozvinuté rozhodovací schopnosti a někteří si v 18 letech povolání vůbec nevybírají. Zde se obvykle dostávají do konfliktu zájmy rodičů a zájmy mladého člověka, když si mladý člověk zvolí povolání a jde za ním podle požadavků rodičů. Je to proto, že v této fázi ještě neví, co chce dělat. Případně si někteří mladí lidé vybírají z několika možností a rozhodují se na poslední chvíli, kdy jsou pod největším tlakem. Jen menšina mladých lidí má jasnou představu o tom, co chtějí v budoucnu dělat. Dalším faktorem tlaku je očekávání, že ve své profesi uspějí. Chlapci zažívají větší stres kvůli očekávání rodičů ohledně jejich profesní dráhy a nesplněným snům. Na druhé straně ženy často hrají roli matek. Očekává se od nich málo. Dospívání lze rozdělit do dvou fází. První fáze se nazývá puberta. Prvních pět let probíhá u každého člověka jinak. Nejčastější změny se týkají fyzického zrání, myšlení a citových prožitků. Druhou fází je pozdní dospívání, které trvá 10 měsíců. Během prvních pěti let po předpubertálním období se změny u jednotlivých lidí liší. V tomto období často dochází k prvnímu pohlavnímu styku. Pozdní adolescence je náročným obdobím psychosociální transformace, kdy dochází k prvním změnám osobnosti a sociálních rolí (Vágnerová, 2012; Sobotková, 2009; Šimíčková-Čížková, 2010).

1.2 Změny u adolescentů

Dospívající v tomto věku kombinují svou jedinečnost a výjimečnost, základ, který získali v dětství, se vším ostatním. V tomto období objasňují svůj postoj a názor. Dospívající neví, jak se se změnami vypořádat, a někdy ho překvapí i náhlé změny, které se odehrávají s jeho tělem. Někteří se s tím chtějí smířit, zatímco jiní chtějí klást dostatečně silný odpor. Vnímání přeměny je subjektivní a závisí na představě dospívajících o přitažlivosti vzhledu dospělých. Pozitivní nebo negativní vnímání nového vzhledu také závisí na reakci na změny v prostředí.

Tělesný a emocionální vývoj u adolescentů

Na konci puberty je tělesný vývoj dokončen a dochází k pohlavnímu rozmnožování. V tomto období dospívající věnují pozornost svému tělu a snaží se přijmout všechny změny. Porovnávají se s ostatními vrstevníky a snaží se přizpůsobit svůj styl oblékání, aby odpovídal jejich stylu. Ikonami pro dospívající jsou často modelky s dokonalým štíhlým tělem a dětskou postavou, které se objevují v časopisech a na sociálních sítích. Vnitřně se tyto dívky chtějí takovým modelkám přiblížit. Protože to je ideální obraz krásy, který je jim předkládán. Většina středoškolaček je se svým tělem nespokojená a chce zhubnout. Chlapci v tomto věku naopak prezentují ideální obraz mužské krásy s dobře proporcionálním tělem, které se skládá z dobře vyvinutých svalů a vypracované postavy (Thorová, 2015).

Emoční vývoj v období dospívání je do značné míry ovlivněn hormonálními změnami, které mají vliv na změny v emočním prožívání. Dospívající jsou obvykle velmi citliví na různá témata v důsledku zvýšeného emočního napětí. Dospívající věnují svým emocím a prožitkům větší pozornost, analyzují je a hlouběji o nich přemýšlejí. Emoce také souvisejí se sebeúctou a sebehodnocením. Jako primární prostředek sebeúcty jsou důležitými zkušenostmi, kterým musí dospívající čelit, i když v tomto věku není dostatek informací, abychom jim mohli důvěřovat. Emoční nevyrovnanost dospívajících ovlivňuje také jejich sebeúctu. Proto je negativní postoje lidí vůči nim, často ne přímé nebo nepřátelské urážky, mohou velmi poškodit (Vágnerová, 2012).

Kognitivní vývoj

Kognitivní vývoj v tomto období naznačuje, že dospívající dosáhl poslední fáze zrání a učení. Plně zralí a zkušení adolescenti mohou v tomto období dále rozvíjet své kognitivní schopnosti. Adolescenti tedy v tomto období nejen přemýšlejí o reálném světě, ale chtějí o něm také vědět nebo alespoň přemýšlet o tom, jaký by mohl nebo měl být. Dospívající proto mohou nejen hypoteticky uvažovat o různých možnostech, ale také reálně přemýšlet a uvažovat o tom, co neexistuje nebo je nepravděpodobné, že by existovalo. V tomto období si adolescenti také rozvíjejí tzv. schopnost hypotetického řešení problémů a jsou schopni „hledat správné řešení bez ohledu na realitu a původní hypotézu“. V tomto období si dospívající také rozvíjejí schopnost argumentovat a zdůvodňovat své myšlenky. Jsou tedy schopni navrhnout více řešení problému, který se snaží vyřešit. Dospívající jsou

schopni vyjádřit svůj názor, zejména v konfrontaci s dospělými, a dokáží si poradit v situacích, kdy je východisko okamžitě zřejmé. Často však nedokážou předvídat důsledky svých činů nebo výroků. Proto jsou adolescenti ve všem, co dělají, odvážní a svobodomyslní. Pociťují určitou míru samostatnosti a nezávislosti na dospělých. Stávají se například závislejšími, nesnášejí kritiku, nemají vlastní názor na druhé a uchylují se k nálepkování. V tomto období se dospívající často izolují. Své myšlenky si nechávají pro sebe. V důsledku toho se mohou zdát lhostejní ke světu kolem sebe. Cítí potřebu realizovat se odděleně od okolního světa. Proto se dospívající zaměřují na techniku, přípravu na budoucí povolání a životní zkušenosti. V tomto období dochází také k morálnímu vývoji a dospívající přijímají morální normy společnosti V tomto období se dospívající začínají zajímat o různé morální zásady. Účastní se různých aktivit, jako jsou demonstrace a charitativní akce. Nemusí však mít vyhraněné názory omezené konkrétními životními zkušenostmi. Někteří dospívající se v tomto období potýkají s reálnými životními obtížemi, jako je rozvod rodičů, smrt blízké osoby, sexuální nebo fyzické zneužívání. Pro tyto mladé lidi je svět od počátku nespravedlivý a nejdůležitější je postarat se o sebe a přežít v tomto světě bez starostí o druhé (Šimíčková-Čížková, 2010; Vágnerová, 2012; Thorová 2015).

1.3 Vztahy v období dospívání

Od narození člověk prochází procesem socializace. V tomto celoživotním procesu nepřetržitého zespolečnění, vytváří člověk různé mezilidské vztahy. V rámci sociální interakce má myšlenky nejen na sebe a sebeúctu, ale také na svět ostatních lidí. Mezilidské vztahy jsou velmi dynamické a transformují se, jejich intenzita a hloubka se zvyšují nebo snižují. V dospívání probíhá proces budování a integrace vztahů velmi intenzivně. Adolescenti hledají sebe a své místo ve společnosti mezi svými vrstevníky. Vztahy získávají nové dimenze a formy. Během tohoto obtížného období mají tendenci způsobovat nedorozumění a konflikty.

Socializační a emoční vývoj

Vztahy a nová spojení navázaná v tomto období mají pro jedince velký význam. Přispívají nejen k osobnímu rozvoji, ale jsou důležité i pro učení se sociálním rolím, které budou hrát v budoucnu jako dospělí – manželé, rodiče, přátelé a rodina. Vztahy a nové vazby získané během tohoto období jsou pro jedince velmi důležité. To platí i pro pracovní role. Tyto vztahy také pomáhají při rozvoji komunikačních dovedností. Být zdvořilý, pozorně

naslouchat druhým, nabídnout pomoc nebo sám požádat o pomoc, vyjádřit vlastní názor. Dospívající v této věkové skupině mají také silnou potřebu vytvářet skupiny. Mladí lidé v této věkové skupině dělají mnoho věcí. A bojují s jinými skupinami s odlišnými názory a představami, zejména s dospělými (Šimíčková-Čížková, 2010; Macek, 2003).

Vztahy s rodiči a sourozenci

Vztah s rodiči má na socializaci dospívajícího důležitý vliv. V minulosti se věřilo, že konflikt mezi rodiči a dospívajícími je přirozený a že jeho prostřednictvím dospívající získávají autonomii. Od té doby se však ukázalo, že rodiče mohou toto období dospívání vnímat jako proces vyhýbání se otevřenému konfliktu a ničení vztahu mezi rodiči a dětmi. Zvýšený konflikt ve vztazích mezi dospívajícími může vést k rizikovému chování, jako je delikvence, útěky z domova, záškoláctví a užívání drog. Vztah mezi rodiči a dospívajícími v tomto období by měl být takový, aby i přes možnost konfliktu mohli dospívající vyjádřit své názory a měli pocit, že je rodiče berou v úvahu. Autorita rodičů je nezbytná, ale stejně jako v případě konfliktů jsou nutné určité hranice. Hodnotové orientace dospívajících vůči rodičům jsou však podobné jako jejich hodnotové orientace vůči kamarádům. V každodenních činnostech a záležitostech se mohou nechat ovlivnit vrstevníky, ale pokud jde o důležitá rozhodnutí, obvykle se před konečným rozhodnutím ptají na názor rodičů. V průběhu dospívání se závislost na rodičích postupně snižuje a stávají se finančně nezávislými. Malý věkový rozdíl mezi sourozenci znamená, že patří ke stejné generaci a sdílejí stejné potřeby, postoje a zájmy. Sourozenecká blízkost je silnější u dívek (Macek, 2003).

Vztahy se současníky

V raném dospívání jsou vztahy s vrstevníky klíčové a pomáhají rozšiřovat a legitimizovat vlastní názory, pocity a chování. Vrstevníci pomáhají potvrzovat a utvářet identitu člověka. Ve vrstevnických vztazích se pozice člověka rychle mění ze soupeře na spoluhráče, z protivníka na kolegu. Dospívající dávají přednost tomu, aby je vrstevníci chválili a naslouchali jim. Dospívající si vybírají přátele, kteří mají stejné chování, zájmy a studijní výsledky jako jejich vrstevníci. Důležité jsou také vztahy s vrstevníky. Vrstevníci nahrazují rodinu a někteří vědí, že když dojde k fyzickým, sociálním nebo psychickým změnám, jsou to právě vrstevníci, kdo jim může pomoci se s nimi vyrovnat. V tomto období je mnoho mladých lidí odloučeno od své rodiny a ztrácí její lásku a náklonnost. Mladí lidé se cítí osamělí a hledají podporu u svých vrstevníků, zejména u těch, kteří zažili totéž co oni. Často nacházejí bezpečí ve skupinách vrstevníků. Touha být přijat ve skupině

je pro dospívající v tomto období velmi důležitá, protože jim pomáhá budovat sebeúctu a identitu. Aby dosáhli určitého statusu, tedy aby byli více přijímáni, jsou dospívající ochotni zajít až do krajnosti. Míra, do jaké se dospívající přizpůsobují ostatním, závisí na jejich vývojové úrovni. Mladší, méně sebevědomé děti jsou méně náročné než starší, sebevědomější děti. Vrstevníci mohou na dospívající vyvíjet sociální tlak, aby změnili své chování. Vrstevníci mohou člověka instruovat nebo motivovat k dobrému chování, nebo naopak podporovat negativní chování. Tato náročnost se u jednotlivých dospívajících liší. Někteří například preferují určitý životní styl, jiní vyžadují určité vnější změny. Vytvářejí si vlastní pravidla, aby se odlišili od světa dospělých. V této fázi jsou pravidla jasná a jejich dodržování jim dodává sebedůvěru. Protože požadavky vrstevníků a rodičů nejsou vždy stejné, dospívající se ocitají v nejistotě a v některých případech jsou nuceni se rozhodnout. V tomto věku začínají dospívající obdivovat idoly, s nimiž se ztotožňují. Často se jedná o herce, zpěváky, hudební skupiny, sportovce nebo o něco starší dospívající. Nejdůležitějším aspektem výběru idolu je, že musí být zajímavý pro ostatní členy jejich skupiny. Mladí lidé se často snaží co nejvíce přiblížit svým idolům tím, že mění svůj vzhled jednoduchými způsoby, například se oblékají jako jejich idoly nebo si stříhají či barví vlasy. Pokud se však skupina na mladého člověka dívá svrchu, stává se mrzutým, šaškovským, třídním klaunem nebo otrokem svého idolu (Thorová, 2015; Vágnerová, 2012; Macek, 2003).

Mladí lidé se mohou sblížit s kýmkoli, i když o takové přátelství nestojí, často ho přijímají jako důsledek osamělosti. Ve většině případů ti, kteří nemají o nikoho zájem, přijímají lidi se stejnými problémy. Dospívající osamělost je nepřijatelná a v tomto věku už nestačí pouze rodinné vztahy. Přátelství v tomto období se často dělí na přátelství s dívkami a přátelství s chlapci. Je to proto, že intimní vztahy mezi dívkami a chlapci jsou v období dospívání méně časté. I když k intimním vztahům dochází, chlapci je často využívají ke sdílení tajemství. Častěji se svěřují osobám opačného pohlaví než svým kamarádům mužského pohlaví. Dívky častěji důvěřují kamarádkám než kamarádům. To může být důležitější, pokud nemají sourozence opačného pohlaví. Rozvíjení blízkých přátelství je pro dospívající velmi důležité. Nejenže je to důležitý citový vztah, ale je to také příležitost k sebepoznání a podpora při zvládání růstových obtíží. Ve srovnání s chlapci, kteří měli v tomto období pět blízkých přátel, mají dívky méně blízkých přátel, ale jejich vztahy jsou hlubší než u chlapců. To může být způsobeno tím, že dívky jsou vyspělejší než chlapci, mají méně přátel a potřebují s nimi navázat hlubší vztahy, zatímco chlapci jsou na svých

přátelích méně závislí a přátelé často hrají v jejich životě důležitou roli. Aby bylo přátelství úspěšné, musí se obě strany shodnout na řadě věcí. Tím se podpoří vzájemné porozumění a vztah bude pro obě strany příjemnější. Pokud dva lidé nemají dobrý vztah, neznamená to, že si nerozumějí s ostatními mladými lidmi, ale znamená to, že není zajímavé si s nimi povídat. Nedokážou se podělit o své problémy a upřímně si důvěřovat. To nepřispívá k budování charakteru. Je proto důležité, aby se tyto dva typy komunikace alespoň částečně překrývaly. Například mladí lidé mají málokdy blízké přátele na jiných školách (Vágnerová, 2012; Macek, 2003).

Partnerské a sexuální vztahy

Takzvaný binární vztah je velmi důležitý ze dvou hledisek. Prvním je intimní přátelství mezi osobami stejného pohlaví, které je založeno na vzájemné sexuální a citové přitažlivosti. Intimní přátelství vzniklá v dospívání často trvají léta a často jimi zůstávají i v dospělosti. Partnerské vztahy jsou naproti tomu vztahy letmé první lásky, vzájemné náklonnosti a romantických setkání. Obvykle se prohlubují až po pubertě, kdy osobnost jako celek dozraje a je dosaženo rovnováhy mezi fyzickou (sexuální) a psychickou zralostí. Tyto vztahy, zejména jejich rozpad a opakované neúspěšné pokusy o chození, však mohou mít pro některé lidi fatální následky, dokud není dosaženo žádoucí rovnováhy. Citově nejistí a labilní jedinci vnímají odchod partnera jako zradu, přičemž rozchod může být provázen nesnesitelnou frustrací a úzkostí. Takové rozrušení a frustrace mohou u některých dospívajících vést k vážným krizím a dokonce k sebevražednému chování. Dospívající se se svými zážitky těžko vyrovnávají a považují je za výjimečné. Ve většině případů jsou tyto zážitky dočasné, ale pro dospívající mohou být skutečným utrpením. Konflikty mezi dospívajícími a úspěšnějšími kamarády mohou způsobit citové strádání a ohrozit jejich sebeúctu. Nejčastějšími spouštěči jsou rodinné konflikty, narušené vztahy, problémy ve škole a sexuální problémy. V těchto případech, i když dospělí v tomto těžkém období přemýšlejí nad maličkostmi a nedělají vše důležité, potřebují dospívající někoho, kdo jim bude naslouchat a poskytne jim citovou odezvu, které se jim při ztrátě vztahu nedostane (Šimíčková-Čížková, 2010; Macek, 2003).

2 KYBERKRIMINALITA A JEJÍ PODOBA

2.1 Definice a struktura kyberkriminality

Pojem kyberkriminalita je velmi obtížné definovat. Definice je obvykle buď příliš úzká a nezahrnuje konkrétní typy trestných činů, které by mohly být klasifikovány jako kyberkriminalita, nebo naopak příliš obecná a zahrnuje trestné činy, které by měly či neměly být klasifikovány jako kyberkriminalita. Často dochází k záměně kyberkriminality a jiných trestných činů. Je proto velmi obtížné zachytit tento jev v jednoduché a stručné definici.

Jako výchozí můžeme použít jedno z nejčastěji užívaných tvrzení Claye Wilsona ve znění:

„Kybernetický zločin je takový čin, který je páchaný s pomocí počítače nebo je zaměřen proti počítači. Mnoho lidí nesouhlasí s touto definicí kybernetického zločinu, protože se domnívá, že kyberprostor je pouze novým prostředím, které napomáhá k páchání trestných činů, které vůbec nejsou nové. Nicméně kyberkriminalita v sobě zahrnuje i útoky, které jsou vedeny proti počítači s cílem narušit jeho proces zpracování, nebo dochází ke zkopírování důležitých dat, nebo je využit jako nástroj špionáže.“ (Wilson, 2008)

Kyberkriminalita je jakýkoli čin spáchaný počítačem nebo proti počítači. Jelikož se však jedná o poměrně obecnou a širokou definici, bude v této části použito několik dalších definic a nezávislé pomocné kritérium. Při rozhodování o tom, zda určitý trestný čin klasifikovat jako kybernetický trestný čin, se zohledňuje další důležitý faktor. Tímto faktorem je odpověď na otázku, zda je trestný čin spáchán bez použití počítače nebo podobné technologie. Pokud je trestný čin spáchán jiným způsobem než za použití počítače, není pro účely této studie považován za kyberkriminalitu. Kyberkriminalitou se rozumí také trestné činy, které mohou být spáchány jinými prostředky, ale jejich odhalení nebo prokázání je výrazně snazší nebo obtížnější díky použití počítače. Předměty, kterými lze páchat kyberkriminalitu, jsou: Počítač, Mobilní telefon, Tablet, USB flashdisk, Externí harddisk, Wi-Fi router, Webová kamera, Chytrá televize, Digitální fotoaparát, Cloud storage úložiště (PČR, 2024).

Typy kyberkriminality

Jedním z nejčastěji hlášených trestných činů v oblasti kyberkriminality je podvod (**podvodná jednání)**. Patří sem i falešné e-shopy, které se otevírají pod záminkou fundraisingu a po krátké době zmizí. Někdy jsou finanční prostředky přesouvány mimo

Českou republiku nebo se k anonymizaci toku finančních prostředků používá virtuální měna.

Mezi podobné taktiky patří podvodná inzerce (prodej automobilů, bílé techniky, hospodářských zvířat a pronájem bytů), inkaso a nigerijské podvody (nigerijské podvody jsou známé také jako podvody 419, jedná se o typ podvodu, který je obvykle páchán prostřednictvím e-mailu, dopisu nebo telefonu). Tyto podvody obvykle zahrnují falešné a podvodné nabídky finanční pomoci, dědictví nebo investic s cílem získat osobní údaje, peníze nebo jiné cennosti oběti. Tento typ podvodu upravuje § 419 nigerijského trestního zákoníku (tento typ podvodu existuje po celém světě, ale obecně se uznává, že se vyskytuje v Nigérii). Patří sem také krádeže z bankovních účtů prostřednictvím falešných e-mailů a phishingu.

Jako další typ se uvádí **hacking**, tedy neoprávněný přístup k počítačovým systémům a paměťovým médiím. Může být použit pro většinu činností označovaných jako hacking, narušení dat, sabotáž systému a zneužití zařízení. Nejtypičtějším příkladem, který je často vyšetřován, je chování útočníka, který prolomí zabezpečení počítačového systému, získá přístup k datům oběti a pokračuje v jejich libovolném používání. Takové chování zahrnuje mimo jiné šíření škodlivého kódu nebo zavádění tzv. zadních vrátek do volně dostupného softwaru. Stále častěji dochází k hackerským útokům na e-maily, sociální sítě a bankovní účty, které mají za následek nejen porušení důvěrnosti, ztrátu nebo zničení citlivých informací, ale také finanční zisk. To zahrnuje i další související trestné činy (vydírání, nebezpečné pronásledování, krádeže z účtů, podvody). Do tohoto typu trestného činu spadají také kybernetické útoky (např. DDoS) a vydírání pomocí ransomwaru (Ransomware je typ malwaru, který zašifruje soubory uživatele a za jejich dešifrování požaduje výkupné (Kolouch & Bašta, 2020; PČR, 2023).

Tento typ malwaru se často šíří prostřednictvím příloh e-mailů, infikovaných webových stránek nebo zneužitím softwaru. Po úspěšném zašifrování dat zobrazí ransomware požadavek na výkupné, obvykle ve formě kryptoměny, například bitcoinu. Často hrozí, že pokud oběť nezaplatí výkupné do určité doby, budou data nenávratně zničena. Ransomware může vést ke ztrátě osobních údajů a finančním ztrátám, proto je pro ochranu před tímto typem útoku důležité mít spolehlivý antivirový software a pravidelně zálohovat důležitá data). Nejběžnější formou tohoto trestného činu je sniffing, Útočníci zachycují probíhající síťovou komunikaci, aby získali citlivý obsah a provozní údaje. Často se tak děje proniknutím do nezabezpečených připojení Wi-Fi, e-mailových serverů a v poslední

době i do domácích routerů. Útočníci pak získávají přístup k citlivým údajům, jako jsou hesla, platební údaje, osobní a soukromé informace, a vyvíjejí na oběti nátlak s cílem získat peníze nebo se alespoň pokusit poškodit jejich pověst (Kolouch & Bašta, 2020; PČR, 2023).

Jako další oblast trestné činnosti si můžeme uvést **blagging**. Tento typ útoku využívá sociální inženýrství, phishing nebo jiné strategie k získání neoprávněného přístupu k citlivým údajům nebo osobním informacím-(Kolouch & Bašta, 2020; PČR, 2023).

Phishing je způsob, jakým kyberzločinci získávají informace, které mohou být použity k různým činnostem, včetně krádeže identity, podvodů s penězi a zákeřného sociálního inženýrství), jelikož se na internetu masivně šíří podvody sociálního inženýrství. Ohroženi jsou jak jednotlivci, tak obchodní společnosti. Jeden z nejčastějších sociálních podvodů na internetu se týká tzv. generálních ředitelů společností, kteří jsou oprávněni činit důležitá rozhodnutí týkající se transakcí a investic. Takové podvody jsou téměř vždy založeny na velmi dobré znalosti trhů, struktur a zákazníků společnosti. Získané informace jsou často využívány k manipulaci s oběťmi a vytváření přesvědčivých argumentů, které je mají přimět k provedení požadované akce. Typickým scénářem je, že pachatel kontaktuje vedoucího pracovníka společnosti (např. prezidenta, generálního ředitele, finančního ředitele) nebo důvěryhodného partnera (např. právníka, notáře, auditora, účetního) tak, že se za ně vydává. Pod touto záminkou pachatel kontaktuje určité zaměstnance společnosti a tvrdí, že obdržel telefonát např. od generálního ředitele ohledně načasování žádosti nebo smlouvy, a přesvědčí je, aby se podíleli na požadované transakci (Kolouch & Bašta, 2020; PČR, 2023).

Obliba online nakupování prostřednictvím e-shopů stále roste. Bohužel tomto případě se jedná o **podvodné e-shopy.** Počet a obrat zákazníků využívajících online nakupování neustále roste. Nakupování online je rychlé, často nabízí lepší ceny než kamenné obchody a je doručováno na adresu uvedenou kupujícím. Je však třeba být obzvláště opatrný při nákupu v neověřených internetových obchodech nebo při nákupu za neobvykle nízké ceny, zejména pokud internetový obchod vyžaduje platbu předem (což je v případě podvodných obchodů často jediný způsob platby) (PČR, 2023).

Mezi nejspolehlivější oběti podvodníků v dnešní době patří ti, kterým je nabízena práce na částečný úvazek v oblasti reklamy a převodů peněz. Takový spolupachatel je také někdy označován jako takzvaně bílý kůň. Tímto způsobem se podílejí na praní výnosů z trestné

činnosti tím, že si zakládají zločinecké bankovní účty a převádějí platby za podvodné internetové transakce (PČR, 2023).

Do kategorie **mravnostní trestné činy** spadají všichni jedinci, kteří v takových případech kontaktují děti mladší 18 let, snaží se získat jejich intimní fotografie či videa nebo je zvou na návštěvu. Nejčastějšími místy kontaktu jsou chatovací místnosti, sociální sítě a online hry. Do této kategorie spadají také trestné činy proti nezletilým, jako je kuplířství, sexuální nátlak, obchodování s dětskou pornografií, výroba pornografie s využitím dětí a nezákonný styk s dětmi (PČR, 2023).

Kategorie trestných činů **proti autorskému právu** zahrnuje porušení autorského práva, práv souvisejících s autorským právem a práv k databázím, zejména sdílení hudby, filmů a softwaru porušujících autorské právo na síťových paměťových zařízeních a v sítích P2P (PČR, 2023).

Mezi další kategorie dělení se řadí **násilné projevy a hate crime.** Tato kategorie zahrnuje trestné činy, jako je vydírání, nebezpečné vyhrožování, nebezpečné pronásledování (známé také jako obtěžování či stalking) a šíření varovných zpráv, které jsou anonymizovány pomocí informačních technologií. K tomu slouží anonymní servery a služby (např. proxy servery, tor sítě, VPN). Mezi tyto trestné činy patří hanobení národnostních, rasových, etnických nebo jiných skupin, podněcování k nenávisti vůči skupině osob nebo extremistické projevy omezující práva a svobody. Na zahraničních serverech se objevily krajně pravicové a levicové webové stránky, které podněcují k nenávisti a diskriminaci etnických menšin a politických skupin, a dokonce vyzývají k násilí. Objevily se také fiktivní profily na sociálních sítích a diskuse v různých médiích (PČR, 2023).

Pozornost musíme věnovat také dalším kategoriím jako je **Dark Web a Deep Web**. Jsou to dvě části internetu, které se často zaměňují, ale mají odlišné charakteristiky. Deep Web, neboli Hluboký web, je část internetu, která je nepřístupná běžným vyhledávačům a obsahuje osobní informace, jako jsou bankovní účty a firemní intranety. Dark Web (či také Temný web) je ještě skrytější a zahrnuje nelegální aktivity, jako je obchod s drogami a zbraněmi. Dark web je často spojován s anonymitou a bezpečností, ale také s nelegální činností. Na dark webu se odehrává mnoho trestné činnosti, protože je obtížné sledovat jeho uživatele. Naproti tomu deep web je rozšířenější a obsahuje legální a legitimní informace, které jsou obvykle pouze skryté. Zde můžeme najít všechnu nezahrnutou kybernetickou kriminalitu (PČR, 2023).

2.2 Pachatelé jednotlivých druhů kyberkriminality a jejich motivační faktory

Kyberkriminality se mohou dopouštět jak fyzické, tak právnické osoby a podmínky trestní odpovědnosti právnických osob jako aktérů kyberkriminality jsou zakotveny v českém i unijním právu. Vzhledem k omezenému rozsahu této studie jsou za pachatele kyberkriminality považovány pouze fyzické osoby. Pokud je pachatelem fyzická osoba, předpokládá se, že se jedná o osobu zletilou, nezletilou nebo osobu, která není trestně odpovědná z důvodu věkového omezení (např. v případě trestných činů kyberšikany). Vzhledem k různorodosti kyberkriminálního chování se motivace kyberzločinců liší a často závisí na jejich věku, osobnosti a schopnostech. Naopak technické dovednosti a znalosti jsou pro motivaci méně důležité. Je velmi pravděpodobné, že u jednoho pachatele existuje několik typů motivace současně. Například kyberzločinec, který při své činnosti získá pornografický materiál a rozhodne se jej šířit, je pravděpodobně motivován jak vlastním sexuálním uspokojením, tak vyhlídkou na finanční zisk (Smejkal, 2018).

Předpokládá se, že hlavní motivací pachatelů je zisk, pomsta (např. kyberstalking), pocit beztrestnosti nebo euforie z toho, že nebyli nalezeni, a pocit dobrodružství, který přináší anonymita internetu. Sexuální pachatelé jsou motivováni vlastním sexuálním uspokojením. Pachatelé působící u výše uvedených kategorií trestných činů mají specifické motivace. K páchání trestných činů souvisejících s prací jsou motivováni také tím, že jejich kriminální chování je vyvoláno možnostmi, které nabízí jejich zaměstnání, např. pocitem nadřazenosti vůči zaměstnavateli nebo přesvědčením, že malá ztráta nemůže firmu poškodit. Vzhledem k tomu, že největší riziko kyberkriminality pochází z důvěrných informací a skupin, které k nim mají přístup, zejména zaměstnanců, manažerů a jim podobných osob, je třeba do vnitřní struktury podniků zabudovat preventivní opatření (Smejkal, 2018; Požár, 2015).

Motivace pachatelů pirátských trestných činů (nelegální stažení, sdílení nebo distribuce chráněného obsahu, kybernetický podvod, zločinný software, síť počítačů, která je infikována škodlivým softwarem a umožňuje útočníkovi vzdáleně ovládat tyto počítače pro útoky, pokusy proniknout do zabezpečených sítí, získání osobních informací uživatele, distribuce virů a jiné...) je rovněž specifická. Ve většině případů jsou motivováni zisky, které mohou ze své nezákonné činnosti získat, a velmi konkrétními cíli, které se v jejich očích zdají být ušlechtilé, a ani se nepovažují za zločince. Hackerská kultura ve prospěch

svobodného softwaru a základních lidských práv na svobodu komunikace a používání softwaru (Završnik, 2017; Hamuddin, Syahdan, Rahman, Rianita, 2019).

2.3 Oběti kyberkriminality

Jednotlivci jsou často oběťmi kyberkriminality prostřednictvím phishingu, ransomwaru, hackingu nebo identity theftu. Mohou být cílem útoků kvůli osobním informacím, financím nebo citlivým údajům (Smejkal, 2018; Požár, 2015; Završnik, 2017).

Také **firmy** bývají terčem kyberkriminality kvůli citlivým obchodním informacím, finančním údajům nebo osobním údajům zaměstnanců a zákazníků. Útoky na firmy mohou mít za následek finanční ztráty, škody na pověsti či dokonce únik citlivých informací (Smejkal, 2018; Požár, 2015; Završnik, 2017).

Vládní instituce jsou také často terčem kyberkriminality, protože mají přístup k důvěrným informacím a důležitým systémům. Útoky na vládní instituce mohou mít vážné důsledky pro národní bezpečnost a stabilitu (Smejkal, 2018; Požár, 2015; Završnik, 2017).

Zdravotnická zařízení jsou cílem kyberútoků kvůli citlivým zdravotním informacím pacientů a důležitým systémům pro poskytování zdravotní péče. Útoky na zdravotnická zařízení mohou ohrozit zdraví pacientů a způsobit finanční ztráty (Smejkal, 2018; Požár, 2015; Završnik, 2017).

Finanční instituce bývají terčem kyberkriminality kvůli finančním údajům a transakcím. Útoky na finanční instituce mohou mít za následek ztrátu peněz pro banky i klienty, a mohou ohrozit důvěru ve finanční systém (Smejkal, 2018; Požár, 2015; Završnik, 2017).

Průmyslová odvětví, jako například energetika, výroba nebo doprava, mohou být terčem kyberútoků s cílem sabotovat výrobu, způsobit havárie nebo odcizit duševní vlastnictví (Smejkal, 2018; Požár, 2015; Završnik, 2017).

Další možné oběti kyberkriminality mohou zahrnovat mediální organizace, občanská sdružení, vzdělávací instituce nebo jednotlivce s dětmi veřejně prezentovanými online. Jednotlivé oběti mohou být také charakterizovány podle zranitelnosti, důležitosti jejich dat, finanční hodnoty či politické nebo sociální relevance. Ale tato práce je zaměřena zejména na **nezletilé subjekty** a pojednání o všech obětech nelze zpracovat do bakalářské práce požadovaného rozsahu (Smejkal, 2018; Požár, 2015; Završnik, 2017).

Kyberkriminalita páchaná na nezletilých obětech

Násilná trestná činnost je v kriminologii chápána jako útok na fyzickou nebo psychickou integritu člověka ve smyslu úmyslného fyzického násilí nebo pohrůžky násilím vůči člověku. Násilná trestná činnost je spíše kriminologický než právní pojem. Násilí může být prvkem trestného činu nebo pouze alternativním či omezeným prvkem trestného činu. Příčiny násilné trestné činnosti jsou různé, vyskytují se ve všech společnostech a jsou ovlivněny kulturou, politickým vývojem, ekonomickou stabilitou, úrovní vzdělání, užíváním drog a vlivem médií. Informační trestné činy proti dětem jsou klasifikovány jako trestné činy proti mravnosti (Novotný, Zapletal, 2004).

Sexuální trestné činy jsou takové, které vyjadřují pudy společensky nepřijatelným způsobem. Nebezpečí sexuálních trestných činů spočívá v jejich latenci a v jejich vztahu k jiným trestným činům, zejména k organizovanému zločinu. Latence je usnadněna tím, že k trestným činům dochází „za zavřenými dveřmi“ a úzkými mezilidskými vztahy mezi účastníky (Novotný, Zapletal, 2004).

Sexuální trestné činy, organizovaná kriminalita

Sexuální trestné činy se dotýkají lidské důstojnosti, zejména zdravého vývoje obětí. Škodlivé následky se objevují bezprostředně po trestném činu, ale často dochází i k dalším škodlivým následkům v podobě fyzických zranění. S tímto problémem úzce souvisí fenomén prostituce, který v České republice není sám o sobě trestným činem, ale je sociálně patologickým jevem a je spojen s mnoha trestnými činy. Dětská prostituce je velmi nebezpečná a často vede k obchodování s lidmi a organizovanému zločinu. Je to jeden z nejnebezpečnějších trestných činů podkopávajících stabilitu a rozvoj občanské společnosti. Postupné uvolňování hraničních a celních kontrol a otevírání hranic vedlo k nárůstu migrace a organizovaného zločinu. Poloha země poskytuje zahraničním skupinám výhodné tranzitní body, místa působení a cíle (Novotný, Zapletal, 2004).

Další druhy kybernetické kriminality páchané na dětech

Kyberkriminalita zahrnuje širokou škálu oblastí, jako je phishing, pharming, sniffing, cracking, hacking, pirátství, šíření falešných nebo znepokojivých zpráv, hacking a skimming. Mezi nejčastější kyberkriminalitu páchanou na dětech patří kyberšikana, obtěžování a kyberstalking (Kopecký, 2010).

Tento článek se však zaměří na sexuální a související trestné činy páchané prostřednictvím internetu, zejména na kyberšikanu a dětskou pornografii. Kyberšikana má obvykle podobu slovních útoků a opakování. Zahrnuje slovní útoky, výhrůžky, urážky a obtěžování zaměřené na konkrétní oběti. Ke kyberšikaně často dochází po výrazném odhalení soukromého života pachatele, zejména po spontánním zveřejnění erotických fotografií nebo sdílení intimních informací. V nejhorších případech vede k sebevraždě oběti. Happy slapping je forma kyberšikany, při níž je oběť vystavena nevybíravým fyzickým útokům. Vyznačuje se zveřejňováním fotografií nebo videoútoků na internetu (Kopecký, 2010).

Další formou kyberšikany je kyberstalking, technologicky vyspělá forma obtěžování. Kyberstalker využívá k obtěžování své oběti osobní údaje zveřejněné na internetu nebo na internetu. Jedná se o dlouhodobou a opakovanou snahu kontaktovat oběť všemi dostupnými prostředky. Oběť má důvodnou obavu o svůj život, zdraví nebo zdraví blízké osoby (Kopecký, 2010).

2.4 Vývoj kyberkriminality jako sociálně patologického jevu a její formování do současné podoby

Kyberkriminalita se postupně vyvíjí a formuje do současné podoby jako sociálně patologický jev. S rostoucím využitím internetu a digitálních technologií se stávají kyberútoky stále sofistikovanějšími a nebezpečnějšími. Tento trend je způsoben nejen technologickým pokrokem, ale také změnami ve společnosti, jako je závislost na internetu, nedostatečná informovanost o bezpečnosti online prostředí nebo absence legislativy adekvátní k potřebám digitální éry. Kyberkriminalita představuje vážné ohrožení pro jednotlivce, firmy i státy a je třeba se jí aktivně bránit a hledat efektivní způsoby, jak ji zamezit a potírat.

Zdokumentované případy

K jednomu z největších kybernetických zločinů v bankovnictví došlo během tří let na počátku 70. let. Teller, tehdejší ředitel newyorské pobočky Union Dime Savings Bank (UDSB), zpronevěřil více než 1,5 milionu dolarů ze stovek účtů. Heckerova skupina si říkala MOD (Masters of Deception) a údajně ukradla hesla a technické údaje z telekomunikačních společností, jako jsou Pacific Bell a Nynex, několika úvěrových organizací a dvou velkých univerzit (WEITZER, 2003).

V roce 1983 se devatenáctiletý student Kalifornské univerzity v Los Angeles (UCLA) pomocí svého počítače naboural do mezinárodního komunikačního systému ministerstva obrany (WEITZER, 2003).

V letech 1995 až 1998 společnost Newscorp platila za šifrované služby SKY-TV; v březnu 1999 červ Melissa infikoval dokumenty v počítačích obětí; v roce 2000 byly dokumenty rozeslány a červ je automaticky rozesílal dalším uživatelům prostřednictvím e-mailu; v únoru 2000 bylo zjištěno, že osoba pod přezdívkou Mafioso používala tuto službu k rozesílání červa dalším uživatelům prostřednictvím e-mailu. V únoru 2000 byla řada známých webových stránek, včetně Yahoo, Amazon.com, Dell Inc, E*TRADE, eBay a CNN, zasažena útoky typu DoS (denial-of-service). Bylo napadeno 50 počítačů na Stanfordově univerzitě a několik počítačů na Kalifornské univerzitě v Santa Barbaře, které byly použity jako „zombie“ v rámci distribuovaného útoku na odepření služby (DDoS). Výsledkem útoku bylo 54 případů neoprávněného přístupu a 10 případů poškození dat (Economist.com, 2007).

Russian Business Network (RBN) byla zaregistrována jako webová stránka v roce 2006. Ačkoli její činnost byla zpočátku legální, její zakladatelé si brzy uvědomili, že bude výhodnější poskytovat hosting pro nelegální činnosti, a začali své služby pronajímat kyberzločincům. Společnost Verisign brzy prohlásila RBN za nejhorší z nejhorších. (Economist.com, 2007).

RBN je tvůrcem MPacku (balíčku malwaru) a provozovatelem botnetu Storm. Dne 2. března 2010 španělští výzkumníci zjistili, že z více než tří milionů počítačů jich byl infikován více než milion (Homelad Security, 2011).

V srpnu 2010 odhalil 600členný mezinárodní vyšetřovací tým Derego Office ministerstva vnitřní bezpečnosti přibližně 123 terabajtů dětské pornografie (což odpovídá přibližně 16 000 DVD) a uzavřel mezinárodní pedofilní distribuční web. Jednalo se o dosud nejrozsáhlejší stíhání obchodování s dětskou pornografií ve Spojených státech, jehož výsledkem bylo celkem 52 zatčení po celém světě (Homelad Security, 2011).

2.5 Předpoklad dalšího vývoje trestné činnosti v kyberprostoru

Kybernetické útoky a kybernetická kriminalita jsou v Evropě stále častější a sofistikovanější. Do roku 2025 se očekává, že k internetu bude na celém světě připojeno 41 miliard zařízení, a tento trend bude pokračovat. Stroje, senzory, sítě a další zařízení připojená k internetu budou hrát důležitou roli: V prosinci 2020 Evropská rada konstatovala, že zvýšené používání spotřebitelských a průmyslových výrobků připojených k internetu vytvoří nová rizika pro soukromí, bezpečnost informací a kybernetickou bezpečnost. V závěrech byly stanoveny priority založené na maximálních standardech odolnosti, bezpečnosti a zabezpečení s cílem řešit tento klíčový problém a posílit mezinárodní konkurenceschopnost odvětví internetu věcí v EU (European Council, 2021).

Ministerstvo vnitra ČR vydalo varování před používáním umělé inteligence k vydávání se za jiné osoby, jejich zneužívání nebo deepfake. Ministerstvo rovněž vydalo brožuru shrnující základní pravidla a rizika používání umělé inteligence. Kyberkriminalita je dlouhodobě nejrychleji rostoucím druhem trestné činnosti, a to nejen v České republice: V roce 2016 tvořila přibližně 2 % evidovaných trestných činů, do roku 2023 se však očekává nárůst na zhruba 11 %. Nejčastějším typem podvodů zůstávají podvody zaměřené na finanční prostředky uživatelů internetu, ale postupem času přibývá i charitativních trestných činů (charitativní trestné činy jsou činy spáchané za účelem podvodného získávání peněz nebo majetku ve jménu charitativních organizací nebo účelů). Ministerstvo vnitra bylo proto jedním ze spoluorganizátorů letošní preventivní iniciativy Den bezpečnějšího internetu, která se konala 6. února (MVCR, 2024).

Vedle tradičních útoků typu ransomware, DoS/DDoS a trojských koní se stále častěji objevují útoky založené na spoofingu, zneužívání umělé inteligence a podvodech typu deepfake (Scharre, 2020; Bocetta, 2020).

Na ministerstvu vnitra působí pracovní skupina, která se zabývá bezpečnostními otázkami souvisejícími s rozvojem umělé inteligence. Vzhledem k tomu, že s umělou inteligencí může pracovat kdokoli, je však užitečné porozumět možným rizikům a základním

pravidlům. Brožura ministerstva je určena všem, kteří chtějí získat základní informace o umělé inteligenci. Ministerstvo vnitra plánuje tento materiál využít při preventivních aktivitách. Umělá inteligence zažívá v současné době obrovský rozmach. Společnosti se předhánějí v tom, která z nich dokáže vytvořit efektivnější a lepší systémy (MVCR, 2024).

Umělá inteligence se využívá také v klíčových státních strukturách, jako je zdravotnictví, doprava a výroba. To vše s sebou nese značná rizika, protože tyto systémy jsou zranitelné a mohou být předmětem sofistikovaných hackerských útoků. Jednou z oblastí AI je strojové učení a hluboké učení. Útočník může do systému určeného pro stroje přímo vložit záměrně pozměněná vstupní data, která mohou dělat chyby. Útočník nepotřebuje přístup ke vstupním datům ani k algoritmům systému. V poslední době se začaly objevovat útoky založené na umělé inteligenci. Opět je obtížné určit, kdo útok provedl. Nejčastějším typem útoku jsou botnety, kdy umělá inteligence provádí útoky DDoS na servery (Scharre, 2020; Bocetta, 2020).

Umělá inteligence se často používá v oblasti autoringu. Může fungovat jako speciální software používaný přímo při tvorbě díla nebo může být začleněna jako součást interaktivní platformy. Zde je třeba se zabývat otázkou odpovědnosti za UI (umělou inteligenci) z hlediska trestního práva; není snadné definovat, co UI je. Pokusilo se o to mnoho autorů, přičemž existují tři modely odpovědnosti za UI: zaprvé odpovědnost prostřednictvím jiných osob; zadruhé odpovědnost podle možnosti přirozeného vzniku; a poslední model přímá odpovědnost. Tyto tři modely lze použít samostatně nebo v kombinaci (Smejkal, 2022; Završnik, 2017).

V modelu odpovědnosti za jiné osoby je UI strojem, nikoli člověkem, a funguje pouze jako nástroj pro programátora nebo uživatele UI k provedení trestného činu. Tento model nelze použít, pokud se UI sama rozhodne spáchat trestný čin na základě znalostí, které získala. Je však vhodný v případě, kdy jsou použity méně schopné UI a za provedení trestného činu je odpovědný programátor nebo uživatel (Smejkal, 2022; Završnik, 2017).

V důsledku toho je přirozeně pravděpodobnější, že programátor se podílí na každodenních činnostech UI, ale nemá v úmyslu spáchat trestný čin. Model počítá se dvěma různými scénáři: prvním je situace, kdy programátor jednal z nedbalosti, ale neměl v úmyslu spáchat trestný čin. Druhým je situace, kdy programátor úmyslně naprogramoval nebo použil UI s úmyslem spáchat trestný čin, ale samotná UI se dopustila jiného trestného činu. Například pokud byla UI naprogramována k vykrádání bank, ale ne k zabíjení lidí. Přesto UI stále zabíjí lidi. V tomto případě by programátor odpovídal za činy spáchané UI, tj. jak

za loupež, tak za vraždu. A to navzdory skutečnosti, že takové činy vyžadují úmyslnou nedbalost. V tomto případě by měla být trestně odpovědná i samotná UI (Smejkal, 2022; Završnik, 2017).

Poslední model představuje přímou odpovědnost UI, která se výrazně neliší od odpovědnosti lidí a musí splňovat jak subjektivní, tak objektivní hledisko. K naplnění objektivní stránky trestného činu je třeba, aby došlo k jednání jako projevu úmyslu ve vnějším světě a k jeho následkům, tj. k porušení nebo poškození právem chráněného zájmu. Jednání má kombinaci psychologických a fyzických prvků a je otázkou, zda UI může mít psychologický úmysl: UI analyzuje každý podnět na základě svých naučených znalostí. Pokročilé algoritmy UI se snaží napodobit lidské kognitivní procesy. Například v případě robotů je to proto, že se části jejich těla pohybují. Trestní odpovědnost je vyžadována za subjektivní stránku trestného činu. Jedná se o vnitřní psychologický vztah mezi konkrétními skutečnostmi, které způsobily trestný čin, a pachatelem. Takové psychologické vztahy lze naprogramovat a umělá inteligence se je může sama naučit. V současné době je proto za jednání umělé inteligence odpovědná fyzická nebo právnická osoba, ať už tvůrce algoritmu, vlastník umělé inteligence nebo jiná osoba, která na stroj dohlíží (Smejkal, 2022; Završnik, 2017).

Kyberkriminalita týkající se odcizování se mládeže je velkým problémem v dnešní digitální době. S nárůstem používání internetu a sociálních sítí mládeží dochází k postupnému snižování osobních kontaktů a komunikace ve skutečném světě. Tím vzniká prostor pro manipulaci a zneužívání mladých lidí prostřednictvím online komunikace. V důsledku snížení osobních kontaktů a přímé interakce může u mládeže docházet ke zvýšení sexuální frustrace a touhy po osobním propojení. Tuto frustraci mohou někteří jedinci využít k sexuálně motivovaným útokům v kyberprostoru. Těmito útoky může být například získávání intimních fotografií, vydírání nebo grooming, což je proces manipulace mladých lidí s cílem získat jejich důvěru a nakonec je zneužít. Abychom snížili riziko kyberkriminality spojené s odcizováním se mládeže, je důležité, aby rodiče, učitelé a další důležité osoby v životě mladých lidí byli obeznámeni s tímto problémem a uměli je chránit. Je také nutné vzdělávat mládež o bezpečnosti online prostředí, důležitosti zachování soukromí a správném chování na internetu. Prevence je klíčem k ochraně mladých lidí před kyberkriminalitou a nebezpečnými situacemi online (Smejkal, 2022; Završnik, 2017).

3 MOŽNOSTI SOCIÁLNÍ PEDAGOGIKY PŘI PREVENCI PÁCHÁNÍ KYBERKRIMINALITY

3.1 Prostředí ovlivňující výchovu jedince

Prostředí člověka lze definovat jako část světa, která ho obklopuje, působí na něj svými podněty a ovlivňuje jeho vývoj. Lidé na tyto podněty reagují a přizpůsobují se jim. Z širšího společenského hlediska je prostředí historicky vyvinutý systém společenských a přírodních vztahů. Kromě materiálních vztahů zahrnuje lidské prostředí také vztahy nezbytné, tj. materiální systémy, a duchovní systémy, tj. vědu, umění a morálku. Je proto důležité, že prostředí jako konkrétní prostor obsahuje podněty nezbytné pro rozvoj osobnosti. Člověk může žít v určité zemi, regionu, městě nebo na venkově, ve zdravém nebo znečištěném prostředí, patřit do určité rodiny, chodit do určité školy, být bohatý nebo chudý, vzdělaný nebo nevzdělaný, mít přátele nebo spolužáky atd. V literatuře je možné se setkat s různými typologiemi. Zatímco první typologie se dělí na přírodní a sociální prostředí, druhá typologie se dělí na makro, mezo a mikro prostředí v závislosti na různých kritériích a velikosti území (Kraus, 2001).

Mikroprostředí je bezprostřední okolí, tj. sociální skupina, která člověka obklopuje. Patří sem rodina, spolužáci, sousedé, přátelé a vrstevníci. Jedním z nejdůležitějších socializačních faktorů je rodina a škola, protože tato prostředí ovlivňují růst, výchovu a vzdělávání člověka. Pojem „meziprostředí“ v sociálně psychologickém smyslu odkazuje na vztahy mezi mikroprostředími, představuje přenos hodnot mezi prostředími a abstrahuje od schopnosti lidí přizpůsobit se změnám v jejich prostředí. Makroprostředí se skládá ze sociálních faktorů. Každá rodina nevyhnutelně patří do určité společenské vrstvy a náš osobní a profesní život je ovlivněn ekonomickou, politickou a právní kulturou dané společnosti nebo země. Právě v kontextu makroprostředí náhle objevujeme skutečný význam slov (a často i politických termínů), jako jsou lidská práva, rovnost příležitostí a náprava porušování práv. Příkladem takového prostředí jsou církve a politické strany. Církve a politické strany jsou prostředí, která sdružují lidi z určitých důvodů a zájmů (Procházka, 2012).

3.2 Prevence kyberkriminality

Slovo „prevence“ pochází z latinského slova praeventus. V širším slova smyslu znamená ochranu a prevenci nežádoucích událostí. Zahrnuje také postupy a činnosti, jejichž cílem je zabránit vzniku společensky nežádoucích událostí. Zatímco lékaři chápou prevenci jako opatření, která mají zabránit vzniku nemoci, právníci chápou prevenci jako právní opatření na ochranu společnosti před protiprávními činy. V užším slova smyslu je prevence předcházením jednotlivým konkrétním negativním událostem, jako je například kriminalita. Prevence kriminality označuje soubor mimotrestních opatření zaměřených na odstranění, snížení nebo neutralizaci faktorů, které způsobují kriminalitu, s cílem předcházet kriminalitě a snižovat ji (Novotný & Zapletal, 2001).

Modely prevence

Nejběžnějšími modely prevence kriminality dětí a mládeže jsou primární, sekundární a terciární model. Liší se podle okruhu pachatelů a stadia vývoje kriminálního chování. Primární prevence je zaměřena především na předcházení trestné činnosti dětí a mládeže. Cílovou skupinou je celá populace dětí a mladých lidí. Zahrnuje zvyšování povědomí a vzdělávání na různých úrovních, zejména doma, ve škole, v dalších sociálních institucích a v médiích. Obsahuje také přímé poradenství. Primární prevence zařazuje ovlivňování a pozitivní ovlivňování hodnot dětí a mladých lidí. Tato prevence se vyznačuje také snahou o pozitivní ovlivňování přátel, volnočasových aktivit a volby životního stylu. Pokud jde o trestnou činnost, cílí na děti a mladé lidi, kteří dosud nespáchali trestný čin (Kaise, 1994).

Sekundární prevence se zaměřuje na rizikové skupiny, tj. na děti a mladé lidi s vysokým rizikem sociálně patologických jevů nebo s vyšší pravděpodobností spáchání trestného činu. V modelu sekundární prevence hrají velmi důležitou roli školy. Cílem není prevence celé populace dětí a mládeže, ale prevence malých a středních skupin. Na prevenci se zaměří i sektor volného času. Zaměřuje se také na rizika v sociálním prostředí a sociálních vztazích dítěte. Cílem je co nejdříve identifikovat postižení a další obtíže. Jakmile jsou tyto problémy identifikovány, lze přijmout opatření, která zabrání dalším negativním dopadům. Důležitou roli zde hrají poradenské služby (Kaise, 1994).

Terciární prevence se týká policejních aktivit zaměřených především na kriminální chování a opakování trestné činnosti. Jejím cílem je bojovat proti opakovanému páchání trestné činnosti a společensky nepřijatelnému chování. V obou případech je cílem zabránit páchání nových trestných činů na základě předchozích trestných činů. Vzhledem k tomu, že programy jsou zaměřeny na děti a mladistvé, kteří opakovaně páchají trestnou činnost, klade se důraz na prevenci jako na předstupeň před systémem trestního soudnictví. Terciární prevence je často označována jako rozšíření sekundární prevence. Jejím cílem je zabránit zhoršení současné situace osoby prostřednictvím opatření nezbytných pro její vlastní blaho. Záměrem je také pomoci osobě najít nejvhodnější cestu z nejhorší situace. V rámci resocializace je úkolem podat pomocnou ruku mentálně postiženým dětem a mladým pachatelům trestných činů, pomoci jim dokončit vzdělání, vstoupit na trh práce, najít bydlení atd. (Kaise, 1994).

Sociální prevence

Sociální prevence zahrnuje velmi širokou oblast. Jejím cílem je předcházet všem sociopatickým jevům, a tedy i kriminalitě. Snaží se tyto jevy překonat a odstranit. Zaměřuje se také na negativní aspekty politického a právního systému a vliv médií. Společnost a stát dosahují žádoucího chování svých členů tím, že kontrolují chování cizích osob. Využívají přitom především normativní systémy, které ve společnosti existují (Novotný & Zapletal, 2001).

Normativní systémy regulující lidské chování zahrnují právo a řád, morálku, náboženství, zvyky a tradice. Zvláštní místo ve vnější kontrole lidského chování zaujímá právo a pořádek, kdy společnost stanovuje pravidla chování v podobě právních norem a sankcí za jejich porušení. V případě kriminality mladistvých je to především trestní právo a příslušné právní předpisy (Novotný & Zapletal, 2001).

Jednou z hlavních podmínek prevence kriminality mladistvých je existence propracovaného a především správně definovaného právního řádu a jeho kvalifikovaná aplikace. Právní předpisy upravující kriminalitu mladistvých se netýkají pouze výkonu spravedlnosti, trestů, výchovy a sociální nápravy. Vedle dohledu nad mladistvými pachateli byla zřízena řada institucí, kterým společnost svěřuje řízení této oblasti, včetně preventivní a výchovné role rodiny a školy. Mezi tyto orgány patří orgány ochrany, orgány péče o mládež a výchovní poradci (Novotný & Zapletal, 2001).

Dalším prostředkem prevence je vnitřní kontrola chování jedince. Hlavním úkolem společnosti je vytvářet optimální podmínky pro socializaci jedinců. Proces socializace je ovlivňován nejen bezprostředním prostředím, v němž člověk žije, ale také společností jako celkem. Proces socializace by měl zejména umožnit, aby si jedinec co nejpřirozeněji a nejsamostatněji vytvořil žádoucí systém vnitřních zábran (Novotný & Zapletal, 2001).

Policejní prevence

Důležitou součástí prevence trestné činnosti páchané na dětech a mládeži je policejní prevence kriminality, kterou provádí Policie ČR a příslušné obecní policie. Policisté se často setkávají s dětmi a mladistvými, kteří se dopustili trestné činnosti nebo jiného protiprávního či sociálně patologického jednání, poprvé. Policie ČR hraje v prevenci kriminality dětí a mladistvých velmi důležitou roli (Otevrenaspolecnost, 2024).

Policie ČR má na všech úrovních, od policejních stanic a místních správ až po okresní a městské úřady, preventivní a zpravodajské skupiny, které mají dva hlavní úkoly. Prvním úkolem je spolupráce s médii a druhým je prevence. V rámci svých povinností organizují policisté pověření těmito úkoly různé preventivní aktivity zaměřené na předcházení trestné činnosti dětí a mládeže. Příkladem jsou besedy s dětmi od předškolního do středoškolského věku a aktivity v oblasti prevence kriminality, kterých se děti aktivně účastní. Mohou také poskytovat poradenství v oblasti prevence kriminality přímo dětem. Spolupracují také s policisty z oddělení bezpečnosti silničního provozu, kteří se na těchto preventivních aktivitách podílejí (Otevrenaspolecnost, 2024).

V České republice je policie dětmi vnímána jako represivní složka. Důležitou roli v aktivitách prevence kriminality ve školách hrají uniformovaní policisté, kteří dětem vysvětlují hranice zákonného chování a informují je o důsledcích překročení těchto hranic. Takové vysvětlování je obvykle doprovázeno ukázkami policejních technik a zásahových metod a provádí se na žádost vedení základních a středních škol, učitelů a nověji i obecních úřadů, které jsou zřizovateli škol. Takové preventivní aktivity provádí nejen Policie ČR, ale i strážníci městské policie. Policie ČR v současné době realizuje projekty community policing v rámci mobilní a dopravní policie. Jedná se o projekt aktivní komunikace a spolupráce s občany, partnery, institucemi a školami s využitím různých metod. Cílem projektu je nejen zvýšit efektivitu běžné policejní práce, ale také promítnout výsledky spolupráce do oblasti prevence. Zjednodušeně řečeno, cílem projektu je přeměna Policie ČR z čistě represivní instituce na instituci, která účinně využívá preventivní opatření v boji proti kriminalitě. Byli vybráni a proškoleni odborníci z různých policejních

útvarů zabývajících se kriminalitou mladistvých a mládeže a trestnými činy páchanými na mládeži (Otevrenaspolecnost, 2024).

Prevence, odhalování a evidence trestných činů páchaných na dětech vyžaduje úzkou spolupráci se sociálními, zdravotnickými, školskými a dalšími orgány. Kromě přetrvávající a opakující se kriminality mladistvých, problémových dětí a trestných činů páchaných na dětech je pozornost věnována dětem, u nichž se před školní docházkou nebo v jejím průběhu objevuje závažné problémové chování, s důrazem na zjišťování příčin takového chování a upozorňování rodičů na problémové chování jejich dětí. Zákon o ochraně dětí se zabývá zejména těmito otázkami (Otevrenaspolecnost, 2024).

Prevence na místní úrovni

Prevence kriminality na místní úrovni a podle místních reálií se stala hlavním cílem systémů prevence, protože může vycházet z místní znalosti konkrétních problémů, může být přizpůsobena místním reáliím a může snadněji reagovat na konkrétní problémy, které se objeví. Z těchto důvodů se v současné době stále více upouští od jednotlivých preventivních intervencí ve prospěch preventivních intervencí na úrovni komunit. Nejúčinnější preventivní opatření jsou ta, která jsou integrována do prostředí jednotlivce (Nikl, 2000).

V některých městech je kriminalita mladistvých obvykle upravena obecně závaznými vyhláškami. Tyto vyhlášky mohou regulovat chování dětí a mladistvých tím, že určité chování povolují a jiné zakazují. Na místní úrovni mohou být z iniciativy starosty nebo městské rady zřízeny výbory pro prevenci kriminality, které se skládají ze sociálních pracovníků a zástupců vládních i nevládních organizací, jež mají zájem na snižování kriminality a účinné práci s ohroženými mladistvými. Města a obce mohou nejefektivněji pracovat s těmi, kteří jsou ohroženi a potřebují zvýšenou pozornost (Nikl, 2000).

Různé preventivní experimenty lze provádět ve školách, v obytných čtvrtích, ve sportovních klubech mládeže, na letních táborech apod. Velký význam zde má také vzdělávání a profesní rozvoj pracovníků (učitelů, školních vychovatelů, pracovníků pedagogicko-psychologických poraden, diagnostických ústavů, policie, věznic, komunitních sdružení, klubů a dalších zainteresovaných skupin a institucí) v oblasti prevence všech sociopatických jevů (Nikl, 2000).

3.3 Subjekty vykonávající preventivní činnosti v dané oblasti

Výchovné a preventivní působení školy a pedagoga

Škola je do jisté míry, při nezbytné spolupráci s rodinou, prostředím, v němž si děti mohou upevňovat své postoje a dovednosti, které jsou předpokladem pro prosociální cestu bez kriminality. V nových, náročnějších kolektivech získávají všichni žáci sociální zkušenosti a rozvíjejí návyky společenského chování. Nedostatky ve vzdělávacím procesu mohou oslabit potenciální pozitivní vliv školy a v určitých fázích způsobit nebo přispět k nepříznivým podmínkám pro osobnostní rozvoj (Novotný & Zapletal, 2001).

Úloha škol v prevenci kriminality dětí a mládeže

Vzdělávání zaujímá důležité místo v prevenci kriminality dětí a mládeže. Rozsah jeho činností je velmi široký. Začíná primární prevencí ve školách, následuje sekundární prevence zaměřená na jednotlivce a rizikové skupiny a terciární prevence zaměřená na eliminaci recidivy nežádoucího chování mladistvých pachatelů ve výchovných ústavech (Matoušek & Kroftová, 1998).

Ve školách jsou realizovány různé preventivní programy. Za prevenci lze považovat již vzdělávání v mateřských školách. Pokud je dětem, které ve škole neprospívají a zaostávají za ostatními dětmi, věnována v mateřských školách náležitá pozornost a je učiněno vše pro to, aby mohly školu navštěvovat, je to jeden ze způsobů prevence trestné činnosti. Děti, kterým se ve škole nedaří, se častěji chovají špatně. Školy mohou dětem zabránit, aby se ve škole chovaly špatně, a informovat je o možných důsledcích špatného chování mimo školu (Matoušek & Kroftová, 1998).

Účinnou prevencí trestné činnosti mohou být také vzdělávací aktivity pro děti, které se přímo nepodílejí na trestné činnosti. Školy učí děti sociálním dovednostem, pravidlům slušného chování, tomu, jak nereagovat agresivně na agresi ostatních a jak odmítat určité nevhodné chování. Obecně školy rozvíjejí u dětí dovednosti řešit problémy. Školy podporují žáky v dobrém chování ve společnosti. Ke snížení kriminality mladistvých přispívá také vztah školy a dítěte a přístup školy k dětem. Například reakce školy při zjištění protispolečenského chování dítěte. Důležitým signálem může být způsob, jakým se provádí šetření, a zejména uplatňované sankce. Tyto signály jsou sdělovány všem dětem. Pokud škola netoleruje nepřijatelné chování, uplatňuje jasná pravidla žádoucího chování a kázně, neponižuje a netrestá žáky, dává jim šanci na nápravu a umožňuje učitelům

a ředitelům objektivní posuzování, budou mít děti vždy jasné hranice svého chování a budou vědět, že nebudou potrestány (Matoušek & Kroftová, 1998).

Škola by proto měla stanovit určité normy chování, na kterých se shodnou všichni učitelé a zaměstnanci, a učitelé by měli důsledně řešit problémy s chováním a používat stejné postupy k dosažení stanovených norem. Školy by neměly s řešením nevhodného chování pouze vyčkávat. Odměny jsou lepším výchovným nástrojem než tresty, proto se školy musí ujistit, že děti chápou, že budou odměněny, pokud se budou chovat v souladu s pravidly. Školy by měly mít zavedeny vhodné systémy odměn, které pozitivně odměňují děti, které dobře pracují, dobře se chovají a dosahují významných pokroků. Tyto odměny by měly být spravedlivé a měly by děti povzbuzovat k tomu, aby podnikaly potřebné kroky (Kyriacou, 2005).

Důležitou úlohou školy v prevenci kriminality mladistvých je udržet problémové žáky mimo třídu. Školy by měly přijmout opatření ke snížení pravděpodobnosti vyloučení problémových žáků, což je důležité i pro prevenci kriminality. Mnoho školních projektů zaměřených na snižování kriminality mládeže mělo velmi pozitivní dopad na počet vyloučených žáků a tvrdí se, že tímto způsobem je přerušena cesta od kriminality k delikvenci prostřednictvím vyloučení. Vyloučení ze školy je totiž velmi negativním ukazatelem a nálepkou dysfunkční osobnosti, která může vést člověka ke kriminalitě (Kyriacou, 2005).

Školský systém poskytuje také výchovné poradenství. Pedagogicko-psychologické poradny a linky důvěry nyní poskytují zásadní podporu. Na každé základní škole působí výchovný poradce, který pomáhá žákům s učením, profesním poradenstvím, volbou povolání a zvládáním krizí. Kromě toho má každá základní škola preventistu, jehož hlavním úkolem je chránit děti před sociopatickými jevy organizováním různých preventivních aktivit a spoluprací s rodiči a institucemi (Kyriacou, 2005).

Mladým lidem s duševními problémy a péči o ně jsou nyní věnovány značné prostředky a pozornost. Byly výrazně navýšeny rozpočty na vzdělávání, často na úkor „hlavního vzdělávacího proudu“. To je často předmětem kritiky veřejnosti, zejména když jsou místní základní školy a školská zařízení posuzovány z hlediska jejich infrastruktury a finanční životaschopnosti. V takových případech má veřejnost tendenci argumentovat, že jde o plýtvání prostředky a že není třeba investovat do problémových dětí, které stejně nelze převychovat. Vzhledem ke klesajícímu vlivu některých rodin na děti, rostoucímu socializačnímu vlivu médií v druhé polovině století a rostoucím obavám z neregulovaného

socializačního vlivu vrstevnických skupin je škola považována za jediné prostředí, kde lze děti optimálně ovlivňovat v souladu se zájmy společnosti. Je tomu tak proto, že výchovný proces nelze koordinovat bez pomoci rodiny (Kyriacou, 2005).

Preventivní a výchovná role pedagoga

Učitelé hrají v procesu prevence dětí nezastupitelnou roli. Spolu s rodiči jsou učitelé pro děti nejbližšími vzory. To platí zejména pro malé děti. Děti mají vysoce vyvinuté vnímací schopnosti a učitelé jim nevyhnutelně musí přizpůsobit své chování, řeč a jednání, aby mohli pozorovat a modelovat chování dětí (Kyriacou, 2005).

Učitelé a s nimi i třída hrají důležitou roli při žádoucím formování a rozvoji osobnosti dítěte. Děti vnímají učitele jako autoritu, ale s přibývajícím věkem se od něj postupně vzdalují a přimykají se ke skupině. Školní třídy si postupně vytvářejí vlastní subkultury, v nichž hrají hlavní roli společné zájmy, třídní zvyky, normy chování a požadavky. Skupiny vytvořené ve školních třídách se mohou stát jádrem kliky s negativní orientací. Ve všech typech škol, od základních tříd až po výchovné ústavy, se mohou v třídních kolektivech vyskytovat různé negativní jevy, jedním z nich je šikana. Čím intenzivnější jsou tyto jevy, tím vyšší je riziko delikvence. I zde je důležitým faktorem pedagogická intervence. V mnoha případech je prohlubování těchto negativních jevů umožněno nezájmem o proces učení ze strany učitelů a dalších odpovědných osob. Pokud například učitel věnuje malou pozornost jednotlivým dětem a jejich osudu, hodnotí děti pouze na základě špatných známek, pravidelně nekontroluje dodržování školního řádu a negativně popisuje určité skupiny dětí ve třídě, může to významně přispět k nárůstu delikventního chování. Naopak věnování plné pozornosti každému dítěti, podpora spolupráce a školní soudržnosti mezi dětmi, vnášení nadšení do třídy, vedení dětí, vytváření a udržování disciplinovaného prostředí, sbližování dětí ve vztazích mezi školou a domovem, podpora preventivních snah a výrazné snížení pravděpodobnosti budoucího delikventního chování. Učitelé výrazně snižují pravděpodobnost budoucího delikventního chování. Mohou také vytvářet prostředí příznivé pro studijní výsledky dětí (Kyriacou, 2005).

Je důležité, aby učitelé identifikovali děti s poruchami učení již na základní škole, včas je diagnostikovali, například v psychologických poradnách, a podporovali jejich rodiče. Tímto způsobem lze předcházet obtížím dětí s učením. Učitelé však musí být schopni komunikovat, spolupracovat a udržovat úzký kontakt s rodiči. Jinak se rodiče nebudou moci podílet na řešení problémů. V opačném případě nebudou schopni spolupracovat s rodiči na řešení problémů. Pokud učitelé s rodiči nekomunikují, nevysvětlují jim

problémy a budoucí rizika a nezapojují rodiče do řešení problémů jejich dětí, bude jejich snaha kontraproduktivní, rodiče zavádějící a v konečném důsledku dále oslabující vztah mezi učitelem a školou (Kyriacou, 2005).

Podle mnoha autorů je mravní výchova také důležitým způsobem prevence kriminálního chování žáků. V současné době mnoho školáků nechápe, že kriminální chování je nepřijatelné, a mnozí dospělí jim jdou příkladem. Školáci vědí, co je správné, legální a špatné. Mnoho žáků se však domnívá, že kriminální chování je pro ně a jejich kamarády přijatelné, a to je součástí obecného vnímání. Vědí, že takové chování je nezákonné, ale nesnaží se mu zabránit, protože nepotřebují potlačovat osobní cíle, jako je vzrušení, materiální odměna nebo prestiž mezi kamarády. Prostřednictvím mravní výchovy by učitelé měli dětem vysvětlit, že určité chování je špatné, že zapojení do takových nezákonných aktivit často znamená někomu ublížit nebo ho poškodit a že očekávané výhody takového chování jsou falešné a zavádějící (Kyriacou, 2005).

Volný čas je důležitou součástí prevence. Velmi důležitou roli zde hrají učitelé. Učitelé mají za úkol vytvářet prostor, kde se děti mohou věnovat vhodným volnočasovým aktivitám. Učitelé by měli děti vést a připravovat na aktivity, které pozitivně formují jejich osobnost, charakter, postoje, názory a schopnost sebepotvrzení. Je však třeba mít na paměti, že hlavní odpovědnost za mimoškolní výchovu nesou rodiče a že učitelé mají omezené možnosti ovlivňovat volnočasové aktivity dětí (Kyriacou, 2005).

Školy a učitele nelze považovat za jediné garanty vzdělávacího procesu. Není v jejich silách ani kompetencích eliminovat všechny negativní vlivy moderní společnosti na děti a mládež prostřednictvím preventivních a výchovných opatření (Kyriacou, 2005).

Sociální pedagogika a prevence trestné činnosti dětí a mladistvých

Sociální pedagogika se zabývá deviantním chováním a sociálním vývojem ohrožených skupin. Zabývá se výchovou a socializací, vlivem prostředí na výchovný proces, rozdíly mezi městským a venkovským vzděláváním, výchovnou situací problémových skupin, výchovou a vzděláváním menšin, interkulturní a multikulturní výchovou, výchovou a vzděláváním zdravotně postižených a zranitelných skupin. Důraz není kladen na vzdělávání společnosti jako celku, ale na vzdělávání na praktičtější mikroúrovni (rodina, škola atd.) a na spolupráci rodiny, školy a vzdělávacích institucí při řešení vzdělávacích problémů. Zaměřuje se na podporu zdravého životního stylu, žádoucích mezilidských vztahů a žádoucích způsobů komunikace. Zaměřením na zájmy a smysluplné

využití volného času pomáhá také předcházet nežádoucímu chování, sociopatickým jevům a v konečném důsledku i kriminalitě. Její zájmy sahají od mimoškolní a rodinné výchovy až po sociální práci s nepřizpůsobivými lidmi, zejména dětmi a dospělými (Mühlpachr, 2004).

Sociálně pedagogické ovlivňování volnočasových aktivit

Vzhledem ke zvýšenému riziku sociální morbidity u dětí a dospívajících má volný čas zvláštní význam pro primární prevenci. Kromě výchovné a relaxační funkce plní volný čas také funkci preventivní. Správné využívání volného času významně přispívá k prevenci sociopatického chování. V této oblasti jsou kompetentní jak sociální pedagogové, tak i rodiny a školy (Hájek, Hofbauer, Pávková, 2003).

Způsob, jakým děti a dospívající tráví volný čas, může být spontánní, nebo může být záměrný, plánovaný a cílevědomý. Pokud děti tráví svůj volný čas spontánně, děje se tak často prostřednictvím nápodoby. Nebezpečí však spočívá v tom, že děti nemusí nutně napodobovat pouze pozitivní, ale často i negativní vzory. Proto je důležité naučit je, jak svůj volný čas využívat. Zejména rodina může děti naučit, jak využívat volný čas. Rodiče a další příbuzní mohou být v rodině velmi silným vzorem. Rodiče mohou s dětmi trávit velkou část svého volného času a to, jak tráví svůj volný čas, má na ně přirozeně silný vliv. Školy a učitelé na všech úrovních mohou děti v tomto ohledu také vychovávat. Koneckonců jsou to právě učitelé, kteří by se měli zajímat o to, jak žáci tráví svůj volný čas. Důležitou roli však mohou sehrát i vychovatelé, pracovníci středisek volného času, organizací pro děti a mládež a tělovýchovných zařízení. Ti musí být schopni přizpůsobit svůj volný čas zájmům a zálibám dětí, které mají na starosti (Hájek, Hofbauer, Pávková, 2003).

Jak děti rostou, potřebují se stýkat s dětmi svého věku a často přebírají jejich vzorce chování. V období dospívání se zvyšuje touha patřit do skupin vrstevníků a klik. Pokud je však volný čas využíván moudře a s vhodným vedením, snižuje se riziko propadnutí do kliky s negativními tendencemi. Děti a dospívající, kteří pravidelně tráví volný čas v klubech, střediscích volného času a mládežnických organizacích, neprožívají nudu a nevyhledávají jiné potenciálně nevhodné kontakty (Hájek, Hofbauer, Pávková, 2003).

Výchovné působení na volný čas se ukazuje jako nezbytná a důležitá součást výchovného působení na děti a mládež. Vědomé a plánované působení vychovatelů však musí zohledňovat základní principy výchovy ve volném čase, zejména principy dobrovolnosti, pestrosti a atraktivity činností, aktivity, volného času, rekreace a zájmu. Činnosti volnočasové výchovy by měly být velmi citlivé a nenásilné a žáci by měli být motivováni k účinné účasti na těchto činnostech. Je třeba respektovat charakter prostředí, v němž se vzdělávání odehrává (Hájek, Hofbauer, Pávková, 2003).

3.4 Evropské kampaně pro kyberkriminalitu

Globalizace kyberkriminality je proces, který spočívá ve vzrůstající mezinárodní spolupráci a propojení kybernetických zločineckých skupin a jednotlivců po celém světě. To znamená, že kybernetická kriminalita není omezena žádnými hranicemi a může být prováděna kdekoli na světě. Tento trend globalizace umožňuje kyberzločincům provádět sofistikované útoky na různé cíle, včetně firem, vládních institucí nebo jednotlivců, a to pomocí internetových technologií a prostředků. Globalizace kyberkriminality může mít vážné důsledky pro společnost, ekonomiku a bezpečnost, neboť může docházet ke krádeži citlivých informací, šíření škodlivých virů, vydírání, sabotáži a dalším formám kybernetických útoků. Proto je důležité, aby mezinárodní společenství spolupracovalo a koordinovalo své úsilí v boji proti kyberkriminalitě a zajistilo účinné ochranné mechanismy a opatření (PČR, 2024).

DIGITAL Europe

Digitální Evropa pomůže EU dosáhnout vysoké společné úrovně kybernetické bezpečnosti. S tím, jak je stále více služeb připojeno k internetu, se kybernetická bezpečnost stala nedílnou součástí digitální společnosti. Silná společná úroveň kybernetické bezpečnosti nás chrání před škodlivými kybernetickými aktivitami, které ohrožují naše hospodářství a způsob života.

Kybernetická bezpečnost je také ekonomickou příležitostí. Celosvětový trh s produkty a službami roste tempem 15–20 % ročně. A to je předpokladem pro to, aby Evropa dosáhla digitální suverenity. Program „Digitální Evropa“ poskytuje příležitost k posílení kybernetické bezpečnosti na společné úrovni EU a podporuje strategii EU v oblasti kybernetické bezpečnosti. Digitální Evropa je investiční program, který má EU pomoci vytvořit technologický rámec založený na hodnotách. Zahrnuje nařízení GDPR, nový

návrh směrnice o bezpečnosti sítí a informačních systémů (NIS), umělou inteligenci a zákon o digitálních službách a trzích.

Bude rovněž investovat do budování evropské infrastruktury kybernetické bezpečnosti „kybernetický štít“, která podpoří šíření a zavádění nejmodernějších metod a zařízení kybernetické bezpečnosti. To je nezbytné pro budování digitální suverenity EU, která závisí na integritě a odolnosti její datové infrastruktury, sítí a komunikací. Část programu Digitální Evropa bude řídit Evropské kompetenční centrum pro průmysl, technologie a výzkum v oblasti kybernetické bezpečnosti, které bude zřízeno v Bukurešti. Toto kompetenční centrum bude propojeno se sítí národních koordinačních center. Bude rovněž koordinovat investice EU, členských států a průmyslu do kybernetické bezpečnosti. Jako operačních cílů Digitální Evropy pomůže EU dosáhnout celkově vysoké úrovně kybernetické bezpečnosti (European Council, 2024).

Závěr teoretické části

Kyberkriminalita je v dnešní době velkým a stále se rozvíjejícím problémem. Zatímco se technologie neustále zlepšují a nabízejí obrovské možnosti pro různé aktivity, zároveň se zvyšuje riziko kybernetických útoků a zneužití informačních systémů.

Myslím si, že je důležité, abychom se jako jednotlivci i jako společnost věnovali prevenci kyberkriminality. Několik doporučení a opatření, která by mohla pomoci snížit riziko kybernetických útoků, zahrnuje pravidelné zálohy dat. Důležité je pravidelně zálohovat veškerá důležitá data a chránit je tak před možnou ztrátou v případě útoku. Je vhodné své operační systémy, antivirový software a další programy udržovat vždy aktuální, aby byly chráněny před známými bezpečnostními hrozbami. Používejte silná hesla a nikdy je nezveřejňujte nebo nepůjčujte ostatním osobám. Doporučuje se také používat dvoufaktorovou autentizaci. Dbejte na své soukromí online a nezveřejňujte citlivé informace na veřejných webových stránkách nebo sociálních sítích. Mějte na svých zařízeních aktivní firewall a antivirový software, který vám pomůže ochránit se proti škodlivým útokům. Vzdělávání: Seznamte se s riziky kyberkriminality a naučte se, jak se chránit. Zapojte se do pravidelných školení a workshopů zaměřených na bezpečnostní opatření. Prevence kyberkriminality je nezbytná pro ochranu našich osobních informací, dat a finančních prostředků. Důležité je být ve střehu a nezanedbávat bezpečnostní opatření, která mohou pomoci minimalizovat riziko kybernetických útoků. Mějme na paměti, že prevence je vždy lepší než řešení případných škod.

Kyberkriminalita u mladistvých je velkým problémem, který je třeba řešit co nejefektivněji. Mladí lidé jsou často více náchylní k páchání těchto trestných činů, protože mají méně zkušeností a často nedoceňují důsledky svého jednání. Je důležité vzdělávat mladistvé o rizicích kyberkriminality a poskytovat jim prostředky a podporu k tomu, aby se vyhnuli pokušení kriminality online. Zároveň je také důležité, aby byla přijímána přísná opatření proti mladým pachatelům kyberkriminality, aby byli odrazeni od dalšího nelegálního jednání. Výchovné programy a nápravná opatření mohou hrát klíčovou roli v prevenci opakování těchto trestných činů a vytváření zdravějšího a bezpečnějšího online prostředí pro všechny uživatele. Sociální pedagog může hrát důležitou roli v prevenci kyberkriminality tím, že poskytuje vzdělávací a preventivní programy zaměřené na informační a digitální gramotnost. Pomáhá mladým lidem porozumět potenciálním rizikům online prostředí a naučit se, jak se chránit před kybernetickými hrozbami. Sociální pedagog může také pomoci mladým lidem rozvíjet dovednosti sociálního a emocionálního učení,

což může snížit jejich náchylnost k zapojení se do rizikového chování online, jako je šíření nenávisti, kyberšikana nebo kyberobtěžování. Dále může sociální pedagog spolupracovat se školami, rodiči a dalšími organizacemi na vytváření bezpečnějšího online prostředí pro mladé lidi a poskytovat podporu a poradenství těm, kteří se již stali obětí kyberkriminality. Celkově může zapojení sociálního pedagoga do prevence kyberkriminality přispět k zvýšení povědomí o této problematice a k posílení ochrany mladých lidí před kybernetickými hrozbami.

II. PRAKTICKÁ ČÁST

4 VÝZKUM

Přehled výzkumů pro tuto oblast

V praktické části jsou zahrnuty nejnovější výzkumy s názvy:

- Kyberprostor je pro adolescenty rizikový a ovlivňuje systém jejich hodnot, jak ukazuje výzkum psychologů – Univerzita Palackého v Olomouci; 2023.
- Threats Targeting Children on Online Social Networks - Karadimce, Aleksandar & Bukalevska, Marija; 2023.
- Cyberspace and Related Threats - Julia Nowicka, Marian Kopczewski, Zbigniew Ciekanowski, Agnieszka Król; 2023.
- Critical Analysis of the Risks in the Use of the Internet and Social Networks in Childhood and Adolescence - Patricia Núñez-Gómez1, Kepa Paul Larraaga Celia ,Felix Ortega-Mohedano; 2021

Úvod

V praktické části bakalářské práce se zaměřuji, tak jako v teoretické části, především na kyberprostor a mládež. Nejprve vymezím výzkumný problém, poté otázky a cíle, výzkumný soubor, výzkumnou metodu, způsob zpracování dat a v neposlední řadě analýzu a interpretaci dat.

Jako zdroje dat byly vybrány úřady Policie České republiky a Český Statistický Úřad. Statistiky kriminality vedené Policií České republiky neevidují data dle věkových kategorií či pohlaví oběti.

V praktické části budu pracovat se vzorkem dat reprezentujícím skupinu mladistvých ve věku 15 až 17 let včetně. Dospívající ve věku 15 až 17 let jsou z několika důvodů považováni za jednu z nejzranitelnějších skupin, pokud jde o kriminalitu a sociální problémy. Tato věková skupina čelí řadě rizik, do nichž patří

- vliv vrstevníků: dospívající jsou často ovlivňováni svými vrstevníky, což může vést k rizikovému chování, jako je zneužívání drog, kriminalita a další nežádoucí chování;

- psychosociální vývoj: v tomto věku hraje důležitou roli psychosociální vývoj a mladí lidé mohou mít potíže s vlastní identitou, sebeúctou a s tím, jak se orientovat ve složitém světě dospělých;
- nedostatek zkušeností: mladí lidé často nemají dostatek životních zkušeností potřebných k přijímání informovaných rozhodnutí, což je může ohrozit;
- zranitelnost: mladí lidé jsou zranitelní vůči různým formám násilí, včetně fyzického, psychického a sexuálního, a může pro ně být obtížné vyhledat pomoc;
- technologické hrozby: mladí lidé jsou dnes také vystaveni rizikům spojeným s používáním internetu a sociálních médií, jako je kyberšikana a kyberstalking.

Podle Policie ČR patří mladí lidé ve věku 15 až 17let (těsně před dosažením 18 let) do skupiny občanů považovaných za nezletilé. Tato věková skupina je považována za zvlášť náchylnou k porušování zákona nebo k páchání trestné činnosti. Policisté věnují zvláštní pozornost prevenci a výchově mladých lidí této věkové skupiny, aby minimalizovali pravděpodobnost, že se stanou oběťmi trestné činnosti nebo se sami trestné činnosti dopustí.

Pro vysvětlení zde uvedu takticko-statistickou klasifikaci Policie České republiky – případy, které se objeví v praktické části. Vysvětlení bude vycházet z trestního zákoníku České republiky. Z dané klasifikace bylo vybráno pět trestných činů jakožto případy nejčastěji se vyskytující během let 2019 až 2023, které zde budou vysvětleny podrobněji. Později se v tabulkách objeví obsáhlejší klasifikace, nicméně s ohledem na zadaný rozsah práce nelze podrobně pojednat i těchto dalších deliktech, které jsou však dále dohledatelné přímo v trestním zákoníku.

Nejčastěji páchanými trestnými činy v kyberprostoru jsou zejména majetkové, nicméně mládež je ohrožena zejména jinými těžšími delikty, a to:

173 **nebezpečné vyhrožování** (§ 353) – Nebezpečné vyhrožování je trestný čin, který spočívá v tom, že někdo někomu vyhrožuje násilím nebo jiným způsobem způsobí strach a pocit ohrožení. Podle trestního zákoníku se za nebezpečné vyhrožování považuje jednání, které má za následek vážné ohrožení fyzické bezpečnosti nebo zdraví osoby, na kterou je vyhrožováno, nebo na její rodinné příslušníky. Trest za nebezpečné vyhrožování může být

odnětí svobody až na dvě léta. V případě, že bylo vyhrožování prováděno veřejně nebo systematicky, může být trest zvýšen.

174 **nebezpečné pronásledování** (§ 354) – Nebezpečné pronásledování je trestný čin podle § 354 trestního zákoníku, který spočívá v tom, že pachatel stále znovu a záměrně sleduje nebo jiným způsobem obtěžuje určitou osobu a tím jí znemožňuje nebo podstatně ztěžuje soukromý život. Trestní zákoník stanoví, že za tento čin může být pachatel potrestán odnětím svobody až na dvě léta. Trest může být i vyšší, pokud pachatel využije pro své jednání přístupu k osobním údajům nebo pokud sledování či obtěžování způsobí oběti závažné tělesné nebo duševní utrpení. Nebezpečné pronásledování je vážný trestný čin, který narušuje osobní svobodu a bezpečí oběti. Je důležité tento druh chování nepodceňovat a případně se obrátit na právní zástupce či policii, aby byla oběti poskytnuta ochrana a pachatel potrestán.

181 **vydírání** (§ 175) – Vydírání je trestný čin podle § 175 trestního zákoníku, který spočívá v tom, že osoba za účelem zisku donutí jinou osobu k něčemu nebo k tomu, aby něco nečinila, hrozbou upuštění od plnění, snížení plnění, či poškození zdraví nebo majetku. Trestní sazba za vydírání může být až 8 let odnětí svobody.

202 **sexuální nátlak** (§ 186) – Sexuální nátlak je trestný čin podle § 186 trestního zákona, který spočívá v jednání, kdy pachatel donutí jinou osobu k provedení nebo snášení pohlavního styku, nebo k jinému sexuálnímu činu, použitím nátlaku či zastrašení. Trest za sexuální nátlak může být odnětí svobody až na dvě léta. Pokud je oběť nezletilá, trest může být až pět let odnětí svobody.

241 **šíření pornografie** (§ 191) – Šíření pornografie je trestný čin dle § 191 trestního zákoníku. Tento paragraf stanoví, že kdo zpřístupní, šíří, zobrazuje, uchovává nebo vytváří pornografický materiál osobám mladším osmnácti let, bude potrestán odnětím svobody až na dvě léta. Trest může být i delší v případě zvlášť závažného jednání nebo opakování. Tento trestný čin je považován za vážné porušení etiky a bezpečnosti občanů. Je důležité dbát na zákony a chránit děti a mladistvé před nevhodným obsahem.

Policie ČR eviduje případy dvou základních skupin: 1) děti (0–17 let včetně) 2) mladiství (15–17 let včetně). Práce je zaměřena zejména na skupinu adolescentů, a tedy pro účely výzkumu je vhodná právě druhá skupina. Mladiství jsou trestně odpovědní, ale mají zvláštní postavení v trestním řízení a mají nárok na zvláštní ochranu a péči v porovnání s dospělými. Mladiství ve věku 15–17 let jsou podrobeni zvláštním pravidlům a opatřením,

která mají za cíl podpořit jejich sociální a psychický rozvoj a jejich úspěšnou reintegraci do společnosti.

Pro zpracování praktické části bakalářské práce byly vybrány pouze některé kraje, a to: Hlavní město Praha, Středočeský kraj, Jihomoravský kraj a kraj Moravskoslezský. Tyto reprezentují nejobydlenější aglomerace obsahující největší podíl mladistvých ve věku 15–17let v ČR, kdy se počty pohybují přes 30 000 osob v daném věku. Z tohoto důvodu jsem se rozhodl pracovat právě s těmito vzorky obyvatelstva.

Kyberprostor bude zkoumán na základě vyšetřených kybernetických trestných činů.
Prevence byla zkoumána obsahovou analýzou ze zdrojů, jako jsou Policie České republiky a Ministerstvo vnitra České republiky. Čerpáno bylo z publikací těchto institutů. Práce zde obsahuje praktické pojednání a navazuje na teoretickou část o prevenci v kapitole 3.2.

4.1 Zkoumaný problém

Kyberkriminalita mezi mladistvými je stále častějším jevem v dnešní digitální společnosti. Není jen otázkou porušování zákonů a pravidel, ale také může mít vážné důsledky pro psychické a fyzické zdraví mladých lidí. Zkoumání daného problému je zaměřeno na analýzu získaných dat od Policie České republiky a Českého Statistického Úřadu.

4.2 Výzkumné cíle

Hlavním výzkumným cílem je zjistit, **zda a v jakých oblastech dochází k ohrožení mládeže v kyberprostoru a jaké jsou zkušenosti s efektivní prevencí těchto konkrétních ohrožení.**

Dílčí výzkumné cíle

1. Zjistit, zda a v jaké míře existují rozdíly mezi současnými druhy ohrožení u mládeže ve věku 15–17 let v nejlidnatějších krajích.

2. Zjistit, zda a v jaké míře existují rozdíly u zkoumaných druhů ohrožení u mládeže ve věku 15–17 let v letech 2019 až 2023 v rámci celé ČR.

3. Zjistit, zda a jaká preventivní opatření jsou prováděna.

4.3 Výzkumné otázky

Hlavní výzkumná otázka zní: **V jakých oblastech dochází k ohrožení mládeže v kyberprostoru a jaké jsou zkušenosti s efektivní prevencí těchto konkrétních ohrožení?**

Dílčí výzkumné otázky

1. V jaké míře existují rozdíly mezi současnými druhy ohrožení u mládeže ve věku 15–17 let v nejlidnatějších krajích?

2. V jaké míře existují rozdíly u zkoumaných druhů ohrožení u mládeže ve věku 15–17 let v letech 2019 až 2023 v rámci celé ČR?

3. Jsou prováděna nějaká preventivní opatření? Pokud ano, jaká?

4.4 Výzkumný soubor

Základní soubor představují všechny **případy šetřené Policií České republiky v rámci celé České republiky**. Jedná se o případy evidované od 1.1.2019 až do 31.12.2023. V roce 2019 bylo evidováno **115** skutků, roku 2020 bylo hlášeno **99** skutků, následný rok 2021 si připisuje celkem **111** skutků, rok 2022 přinesl rekordních **147** skutků a v roce 2023 bylo oznámeno **118** skutků.

4.5 Výzkumná metoda a technika

Při kvantitativní analýze dat se k získání přesných a objektivních informací hojně využívají různé výzkumné metody a techniky. V bakalářských pracích se používá popisná statistika.

Popisná statistika je odvětví statistiky, které se zabývá sběrem, analýzou a interpretací dat pro popis určité populace nebo jevu. Popisná statistika se zaměřuje na různé charakteristiky dat, jako je průměr a medián. Pomáhá pochopit strukturu dat a získat celkový obraz o zkoumaném jevu nebo skupině. Často se používá jako první krok při analýze dat a poskytuje podklady pro další statistické metody. Popisná statistika poskytuje ucelený pohled na data a základní informace o zkoumaném jevu nebo skupině. Grafy, tabulky a číselné specifikace lze použít k vizualizaci a porovnávání dat, k identifikaci vzorců a trendů a k odhalení odlehlých a extrémních hodnot. Obsahová analýza je výzkumná metoda zaměřená na identifikaci a interpretaci obsahu konkrétních materiálů, jako jsou texty, obrázky nebo zvukové nahrávky. Účelem obsahové analýzy je porozumět obsahu, tématům a vzorcům materiálu a hlouběji proniknout do jeho smyslu a významu. Tato metoda se často používá v oborech, jako je vědecký výzkum, marketing a psychologie, k analýze dat a získání informací, které lze využít k dalšímu rozhodování.

4.6 Zpracování dat

Data získaná od Policie České republiky a Českého Statistického Úřadu vyhodnocuji a popisuji stav, stanovuji průměry, vypočítávám poklesy a zvýšení v procentech, porovnávám předešlé roky.

U obsahové analýzy se zaměřuji na text z publikací Policie České republiky a Ministerstva vnitra České republiky.

4.7 Interpretace dat

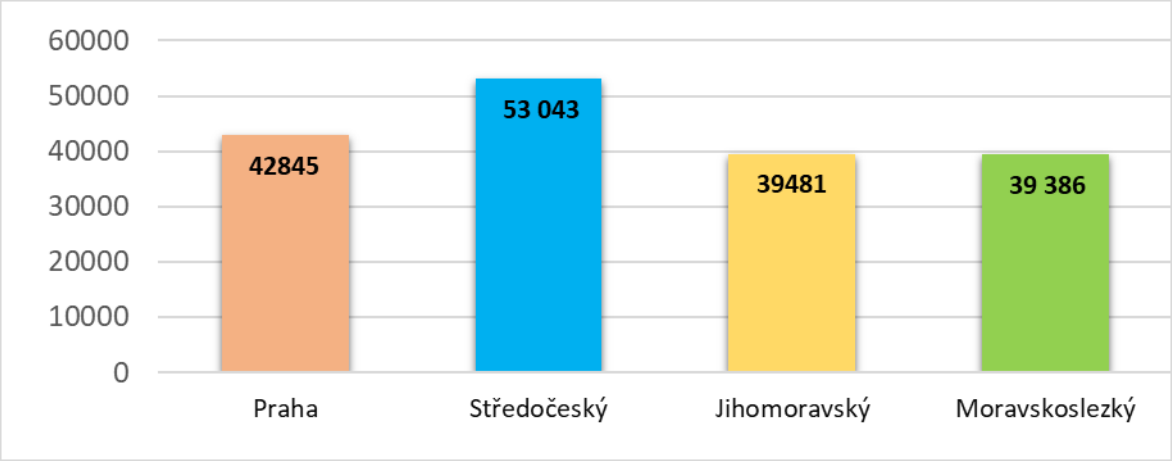
Rozdíly mezi současnými druhy ohrožení u mládeže ve věku 15–17 let v nejlidnatějších krajích.

Obyvatelstvo

V roce 2023 dosahovala populace České republiky 10 900 555 obyvatel. Z toho obyvatel ve věku 15–17 let bylo 366 319, což představuje 19,27 % obyvatelstva České Republiky.

V roce 2023 jako nejlidnatější kraje podle ČSÚ a zároveň nejlidnatější město v kategorii mladiství 15–17 let bylo hlavní město Praha, Středočeský Kraj, Jihomoravský, Moravskoslezský. Z výběru byly vybrány čtyři kraje, jelikož se zde nachází více než 30 000 obyvatel ve věku 15 až 17let.

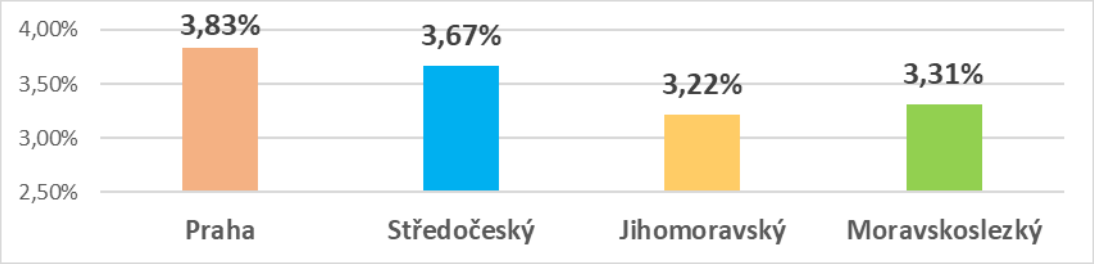
Obrázek 1 Mladiství ve věku 15–17 let napříč vybranými kraji



Zdroj: ČSÚ, 2024 (vlastní zpracování)

Nejlidnatějším krajem je kraj **Středočeský** s **53 043** obyvateli ve věku 15 až 17let (to představuje 3,67 % z celkového počtu 1 445 940 obyvatel ve Středočeském kraji). Následován je hlavním městem **Praha** s počtem obyvatel **42 845** ve věku 15 až 17 let (to představuje 3,83 % z celkového počtu 1 384 732 obyvatel v Praze). Na třetí příčce se umístil kraj **Jihomoravský** s počtem obyvatel **39 481** ve věku 15 až 17 let (to představuje 3,22 % z celkového počtu 1 226 749 obyvatel v Jihomoravském kraji). Poslední příčku obsadil kraj Moravskoslezský s počtem obyvatel **39 386** ve věku 15 až 17let (to představuje 3,31% z celkového počtu 1 189 204 obyvatel v Moravskoslezském kraji).

Obrázek 2 Procentuální zastoupení mladistvých (15–17 let) ve vybraných krajích



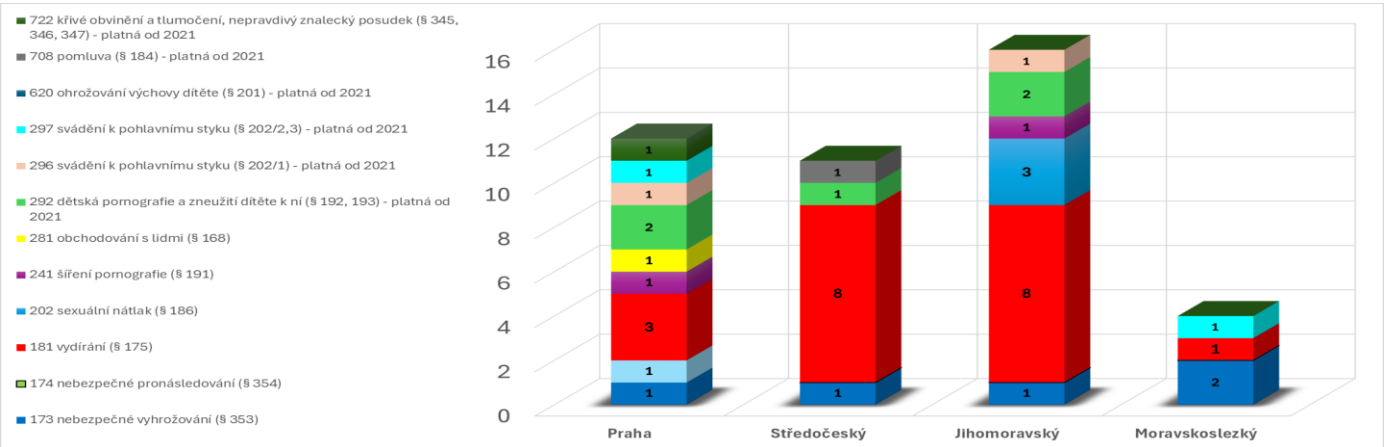
Zdroj: ČSÚ, 2024 (vlastní zpracování)

Největší procentuální zastoupení mládeže ve věku 15–17 let je v hlavním městě Praha. Následuje kraj Středočeský, Moravskoslezský a v poslední řadě kraj Jihomoravský.

Skutky páchané ve vybraných krajích

Společným trestným činem pro všechny kraje je **vydírání** s celkovým počtem 20 skutků z vybraných regionů. V rámci celé České republiky bylo zaznamenáno 51 skutků. Nejhůře dopadl kraj Jihomoravský. Následující trestný čin, který se objevuje napříč všemi kraji, je **nebezpečné vyhrožování** s celkovým počtem 5 skutků z vybraných krajů. V celkovém počtu 16 skutků v celé České republice se jedná o 31% podíl. Dalším společným trestným činem pro tři kraje je dětská pornografie a s ní související zneužití dítěte. Ve vybraných krajích se jedná o 5 skutků, což představuje 24% podíl z celkem 21 zaznamenaných případů. Následujícím je sexuální nátlak. Jen v Jihomoravském kraji se jedná o 3 případy z celkového počtu 11 v celé České republice, což představuje 27% případů. Ostatní zaznamenané případy jsou již po 1 skutku.

Obrázek 3 Počty skutků 2023 u mladistvých (15–17 let) ve vybraných krajích



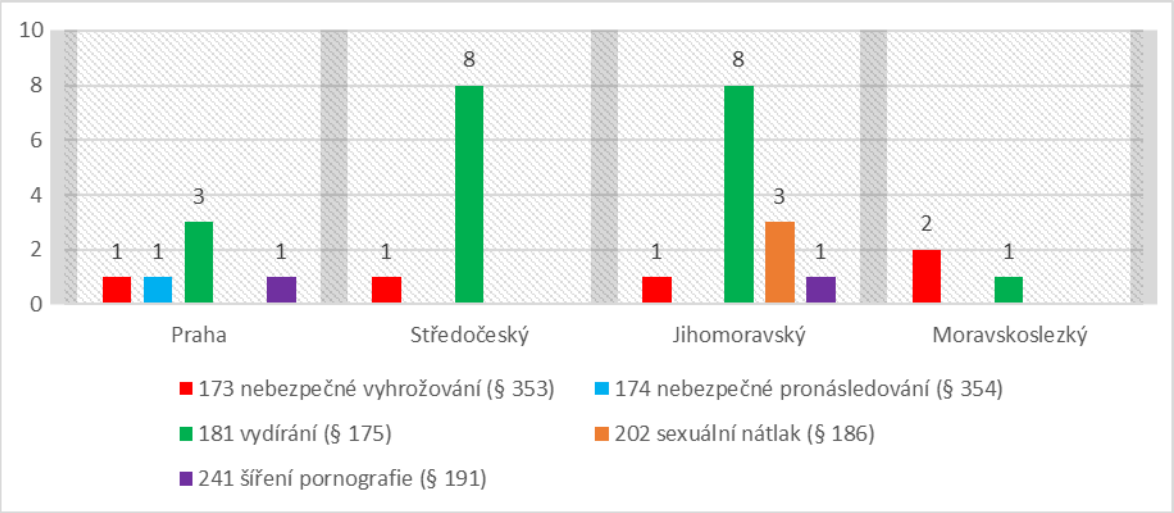
Zdroj: PČR, 2024 (vlastní zpracování)

Dále se blíže zaměřím na vybrané skutky v konkrétních krajích. Nebezpečné vyhrožování bylo zaznamenáno ve všech krajích. Pro Prahu, Středočeský a Jihomoravský kraj byl nahlášen pouze jeden případ a v Moravskoslezském to byly dva.

Detailní zobrazení vybraných skutků

U nebezpečného vyhrožování bylo nahlášeno po 1 případu v téměř každém kraji, pouze v Moravskoslezském kraji byly nahlášeny 2 případy. Nebezpečné pronásledování se objevuje pouze v hlavním městě Praha a zde se jedná o 1 případ. Šíření pornografie se objevuje v Praze a Jihomoravském kraji a zde se jedná taktéž o 1 případ v každém kraji. Sexuální nátlak byl zaznamenán pouze v Jihomoravském kraji, a to ve 3 nahlášených případech. Nejvíce hlášených případů bylo v Praze, a to celkem 3, ve Středočeském kraji již bylo hlášeno společně s Jihomoravským krajem celkem 8 případů. Nejlépe dopadl kraj Moravskoslezský s 1 případem.

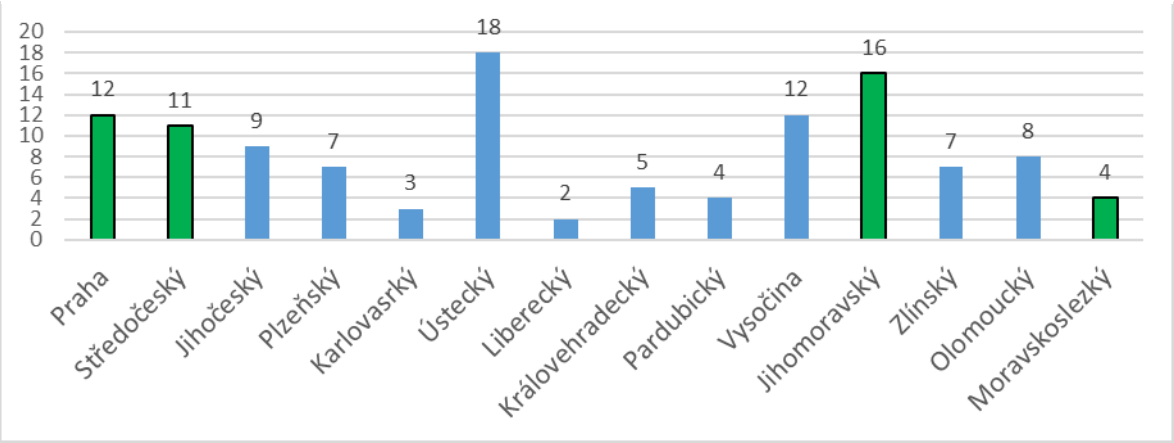
Obrázek 4 Počty vybraných skutků 2023 u mladistvých (15–17 let) ve vybraných krajích



Zdroj: PČR, 2024 (vlastní zpracování)

Všechny ohlášené případy za rok 2023, které se vztahují na Českou republiku. V průměru na Českou republiku připadá 8,43 případu. I přesto, že Moravskoslezský kraj je jedním z nejobydlenějších krajů, tak zde byly ohlášeny pouze 4 skutky. Z mého výběru se řadí na druhé místo z celé České republiky kraj Jihomoravský s 16 případy – v tomto kraji byla průměrná nezaměstnanost 2,5 %. Avšak Ústecký kraj si drží jasné prvenství s 18 případy a 4,0% nezaměstnaností (ta byla druhá nejvyšší hned po Karlovarském kraji s 4,3% nezaměstnaností).

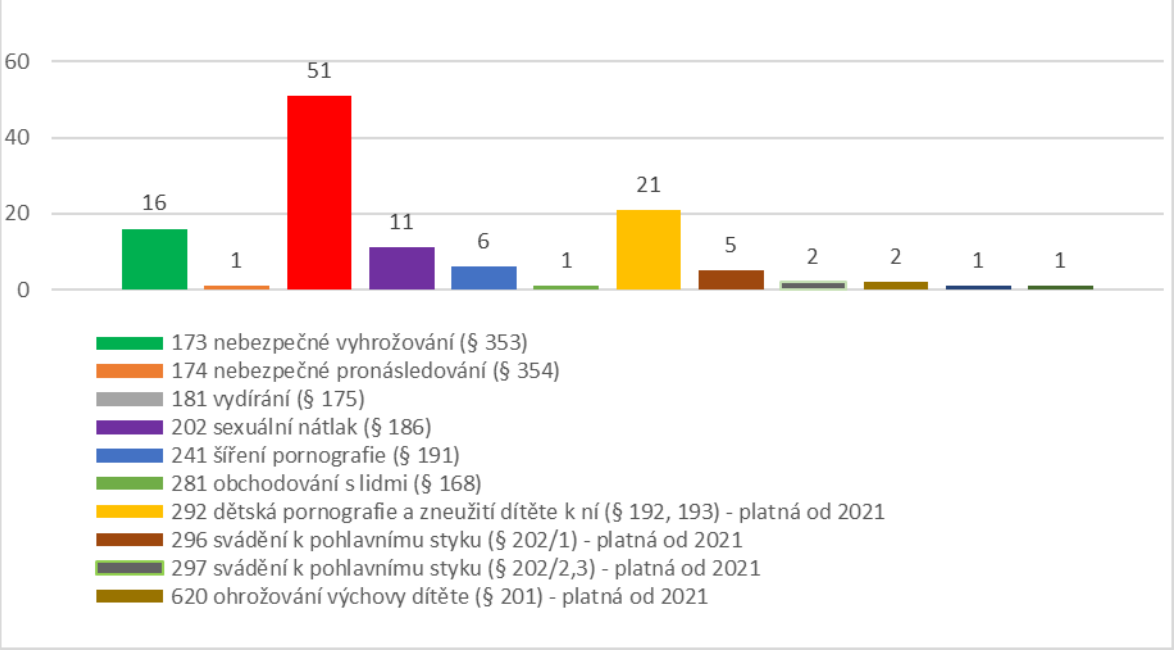
Obrázek 5 Počty skutků 2023 u mladistvých (15–17 let), Česká republika



Zdroj: PČR, 2024 (vlastní zpracování)

V České republice bylo za rok 2023 oznámeno nejvíce případů nebezpečného pronásledování s celkovým počtem 51. Na druhém místě byla dětská pornografie a zneužití dítěte v počtu 21 případů. Na třetím místě se 16 případy skončil delikt nebezpečné vyhrožování. Na čtvrtém místě byl pak sexuální nátlak s 11 případy, následovalo šíření pornografie se 6 případy. U ohrožování výchovy dítěte bylo hlášeno 5 případů. Ostatní případy byly spíše nahodilé či ojedinělé.

Obrázek 6 Druhy skutků 2023 u mladistvých (15–17 let), Česká republika



Zdroj: PČR, 2024 (vlastní zpracování)

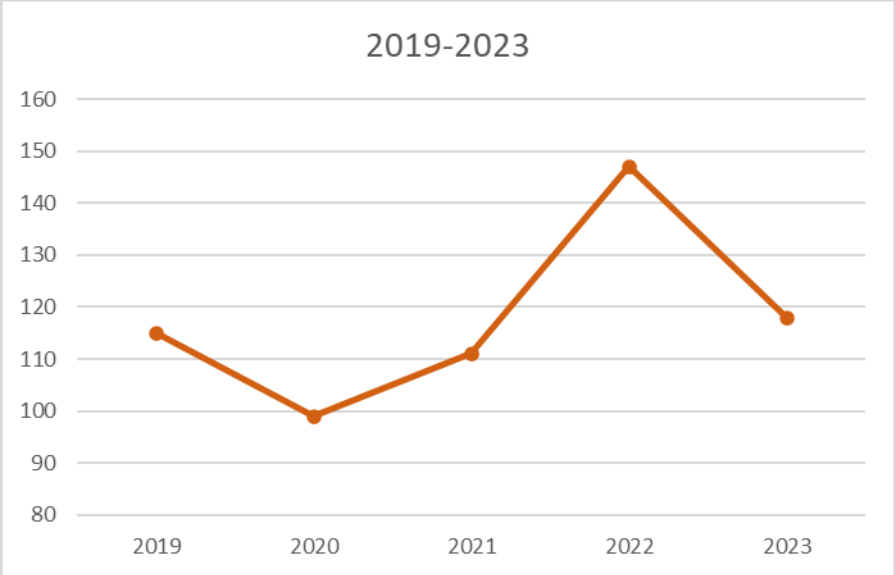
Rozdíly u zkoumaných druhů ohrožení u mládeže ve věku 15–17 let v letech 2019 až 2023 v rámci celé ČR.

V roce 2019 bylo nahlášeno celkem 115 případů kyberkriminality, a v roce 2020, kdy byla nařízena karanténa a vyučovalo se pouze od března, se snížil tento stav na 99 trestných činů. V roce 2021 se výskyt těchto činů mírně zvýšil na 111. Roku 2022 došlo k výraznému nárůstu na 147 skutků. V roce 2023 se ohlášené případy vrátily zpět k průměru 118 případů.

Tabulka 1 Vývoj počtu skutků v letech 2019–2023 u mladistvých (15–17 let)

Rok	2019	2020	2021	2022	2023
Počet skutků	115	99	111	147	118

Zdroj: PČR, 2024 (vlastní zpracování)



Obrázek 7 Vývoj počtu skutků v letech 2019–2023 u mladistvých (15–17 let)

Zdroj: PČR, 2024 (vlastní zpracování)

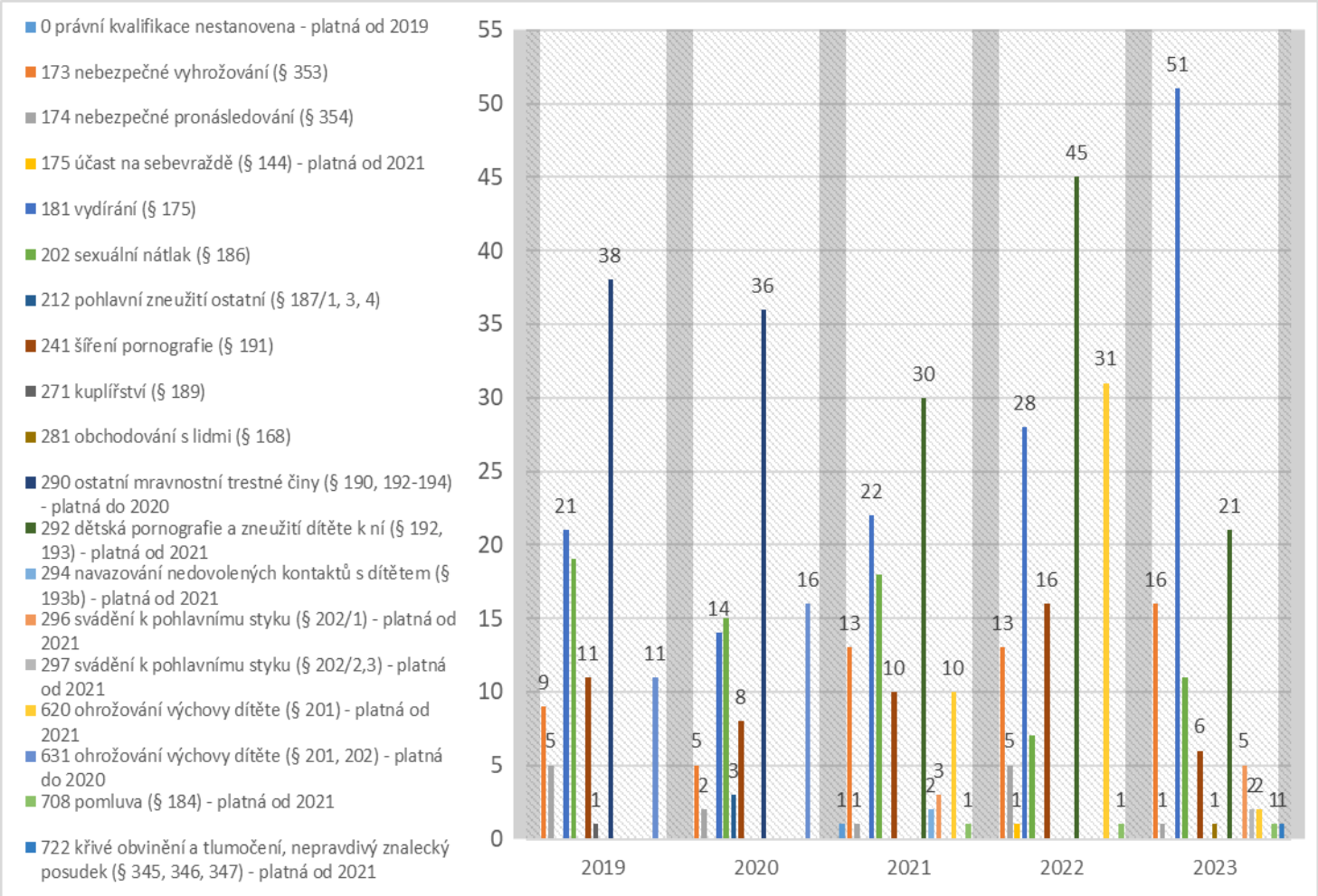
Během krize covid-19 došlo k poklesu, avšak s postupným uvolňováním začala kyberkriminalita opět postupně narůstat. V roce 2023 došlo k poklesu do spíše průměrných hodnot. Ať už je to pandemie, nebo jiné faktory, fyzické odloučení vedlo k nárůstu počtu činností, které se dříve prováděly bezprostředně, tváří v tvář. Lidé začali více komunikovat prostřednictvím videa, sociálních médií a různých online platforem.

S využitím lineární regrese můžeme dostat hodnoty predikce pro následující roky:

Rok 2024: -134, Rok 2025: -140, Rok 2026: -145, Rok 2027: -150, Rok 2028: -156

Obrázek 8 Vývoj páchaných skutků 2019–2023

Páchané skutky od roku 2019 do 2023 v České Republice



Zdroj: PČR, 2024 (vlastní zpracování)

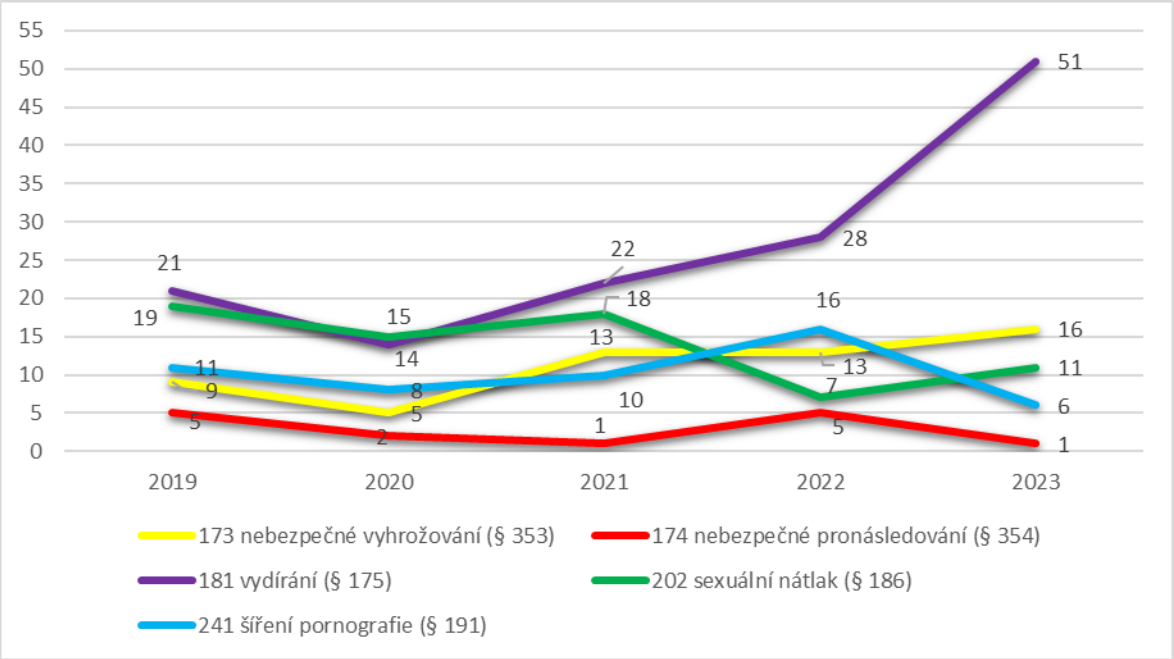
V roce 2021 se objevil jeden záznam o nenastavené právní klasifikaci. Nebezpečné vyhrožování bylo zaznamenáno nejvýše v 16 případech v roce 2023. Nebezpečné pronásledování bylo v roce 2019 a 2022 nejvyšší se zaznamenanými 5 případy. Účast na sebevraždě v roce 2022 vzrostla na jeden případ. Vydírání v roce 2023 vzrostlo na 51 případů oproti roku 2022, kdy se jednalo o 28 případů, což je nárůst o 82 %. Sexuální nátlak byl před covidem na hodnotě 19 případů a v roce 2022 klesl na pouhých 7 , ale v roce 2023 již bylo ohlášeno 11 případů, což značí znovu mírný nárůst. Pohlavní zneužití

bylo nahlášeno pouze ve 3 případech v roce 2020, tedy v roce, kdy byla karanténa. Šíření pornografie bylo nejvíce hlášeno v roce 2022, a to v celkovém počtu 16 případů, a v minulém roce tato hodnota klesla o 63 % na 6 případů. Od roku 2020 vstoupila v platnost nová klasifikace, která definuje dětskou pornografii a zneužití dítěte k ní. V roce 2021 bylo hlášeno 30 takových případů, následující rok to bylo 45 a minulý rok se tato čísla zmenšila na hodnotu 21. V dalším popisování záznamu bychom mohli pokračovat i nadále, ale to nelze s ohledem na požadovaný rozsah práce podrobně rozpracovat.

Popis vybraných činů

Nebezpečné vyhrožování od roku 2020 neustále narůstá. V roce 2020 bylo ohlášeno 5 případů, v roce 2023 se objevilo již 16 případů. Z toho můžeme usoudit, že se tento druh kybekriminality pohybuje směrem nahoru, a to od 2020 do roku 2023 v nárůstu o 220 %. Celkový nárůst od roku 2019 do roku 2023 činní 78 %. Nebezpečné pronásledování se začalo od roku 2019 do roku 2021 snižovat, a to z 5 případů na 1. Důvodem byla opět distanční výuka. Celkově se tedy od roku 2019 do roku 2023 jedná o 80% pokles. Sexuální nátlak se od roku 2019 z hodnot 19 případů snížil do konce roku 2023 na 11 případů, což činí 42% pokles. Zajímavou částí je šíření pornografie. V roce 2019 bylo hlášeno 11 případů, v roce 2020 již pouze 8, avšak v roce 2022 se počet zvýšil na 16 případů a v minulém roce spadl opět pod hodnoty covidové, a to na počet 6, což představuje 45% pokles. Velmi znepokojivá kategorie je vydírání, která v grafu připomíná spíše exponenciální růst od roku 2020. Od doby před covidem v roce 2019 s ohlášenými 21 skutky se do konce roku 2023 tento počet navýšil o 143 % na 51 skutků.

Obrázek 9 Vývoj vybraných skutků v letech 2019–2023



Zdroj: PČR, 2024 (vlastní zpracování)

Preventivní opatření

Sociální prevence kriminality

Sociální prevence kyberkriminality se zaměřuje na prevenci a snížení rizika trestné činnosti v digitálním prostředí prostřednictvím vzdělávání, osvěty a podpory jednotlivců i komunit. Zde je několik klíčových aspektů, jak lze sociální prevenci kyberkriminality provádět:

1. Vzdělávání a osvěta: Zvýšení povědomí o kybernetických hrozbách a způsobech, jak se chránit, je zásadní. To zahrnuje školení pro děti, mládež, rodiče a učitele o bezpečném chování na internetu, identifikaci potenciálních hrozeb (jako jsou phishingové útoky nebo podvodné weby) a ochraně osobních údajů.
2. Podpora digitální gramotnosti: Zlepšení digitálních dovedností jednotlivců pomáhá lidem lépe porozumět technologiím a digitálnímu světu, což může snížit riziko obětí kyberkriminality. To zahrnuje kurzy o používání různých aplikací, sociálních sítí, ale i základních bezpečnostních praktik.
3. Spolupráce s institucemi: Účinná prevence zahrnuje spolupráci s policií, školami, neziskovými organizacemi a dalšími subjekty, které se zabývají problematikou

kybernetické bezpečnosti. Tyto spolupráce mohou zahrnovat společné projekty, kampaně nebo workshopy.

4. Podpora obětí: Je důležité poskytovat podporu obětem kyberkriminality, a to nejen psychologickou, ale i právní pomoc. Oběti by měly mít přístup k informacím o tom, jak postupovat, pokud se stanou obětí kyberzločinu.
5. Zásady kyberbezpečnosti: Propagace a dodržování základních zásad kyberbezpečnosti, jako je používání silných hesel, dvoufaktorová autentifikace a pravidelná aktualizace softwaru, mohou výrazně snížit riziko kybernetických útoků.
6. Monitorování a analýza trendů: Sledování vývoje a trendů v oblasti kyberkriminality, aby bylo možné reagovat na nové hrozby a adaptovat prevenci na měnící se situaci v digitálním prostředí.

Celkově je sociální prevence kyberkriminality komplexní úkol, který vyžaduje zapojení různých aktérů a neustálou adaptaci na nové výzvy, které digitální svět přináší.

Policejní prevence

Policejní prevence zahrnuje soubor opatření a aktivit, jejichž cílem je předcházet kyberkriminalitě a zvyšovat bezpečnost občanů. Dělí se na několik typů:

1.1 **Primární prevence**: Primární prevence policejní kyberkriminality se zaměřuje na ochranu před trestnou činností v oblasti kyberprostoru, než k ní dojde. Cílem je snížit riziko vzniku kyberkriminality prostřednictvím různých opatření a aktivit. Zde jsou některé z nejdůležitějších aspektů primární prevence v této oblasti:

1.1.1 Vzdělávání a osvěta: Informování veřejnosti o rizicích spojených s používáním digitálních technologií a internetu. To zahrnuje školení o bezpečném chování online, rozpoznávání phishingových e-mailů, zabezpečení osobních údajů a používání silných hesel.

1.1.2 Zlepšení technologie zabezpečení: Doporučení a podpora používání sofistikovaných bezpečnostních opatření, jako jsou firewally, antivirové programy, šifrování dat a pravidelná aktualizace software.

1.1.3 Spolupráce s subjekty soukromého sektoru: Policie může spolupracovat s firmami a organizacemi na vývoji a implementaci bezpečnostních protokolů a technologií, které pomáhají chránit uživatele před kybernetickými hrozbami.

1.1.4 Monitoring online prostředí: Policie může provádět monitoring a analýzu online aktivit, které by mohly naznačovat potenciální kybernetické útoky. Tento přístup může identifikovat vzorce chování, které by mohly vést k zločineckým činům.

1.1.5 Zavádění legislativy a politik: Tvorba a implementace právních předpisů a politik, které se zaměřují na prevenci kyberkriminality a ochranu uživatelů. To zahrnuje také mezinárodní spolupráci při vyšetřování a stíhání kybernetické kriminality.

1.1.6 Podpůrné linie a služby: Zřízení hotline nebo online služeb, kde mohou lidé nahlásit podezřelé aktivity nebo získat rady týkající se kybernetické bezpečnosti.

1.1.7 Započtení mladistvých a komunitních programů: Programy zaměřené na mladé lidi, které je vzdělávají o bezpečnosti na internetu a potenciálních rizicích kyberkriminality.

Primární prevence je klíčová pro snížení incidence kyberkriminality a ochranu jednotlivců a organizací před možnými ztrátami a škodami způsobenými těmito trestnými činy.

1.2 **Sekundární prevence**: Sekundární prevence policejní kyberkriminality se zaměřuje na minimalizaci škod a prevenci opakování kybernetických trestných činů poté, co došlo k jejich spáchání. Tato fáze prevence zahrnuje různé strategie a postupy, které mají za cíl pomoci obětem a zlepšit reakční mechanismy policejních složek.

Mezi klíčové prvky sekundární prevence patří:

1.2.1 Informace a vzdělávání obětí: Poskytování informací o tom, jak se chránit před kyberkriminalitou a jak správně reagovat, pokud se stanou oběťmi.

1.2.2 Podpora obětí: Zajištění psychologické a právní pomoci obětem kybernetických trestných činů, aby se snížil dopad útoků na jejich životy.

1.2.3 Vyšetřování a odhalování trestných činů: Efektivní a rychlé vyšetřování kyberkriminality, které může vést k odhalení pachatelů a zajištění důkazů.

1.2.4 Spolupráce s dalšími institucemi: Koordinace s jinými bezpečnostními a právními orgány, jakož i s organizacemi zabývajícími se kybernetickou bezpečností.

1.2.5 Vypracování preventivních opatření: Na základě analyzovaných dat o kyberkriminalitě navrhování a implementace preventivních strategií, které by mohly minimalizovat riziko budoucích útoků.

1.2.6 Technologické nástroje a softwary: Využívání moderních technologií pro detekci a prevenci kybernetických útoků, například systémů pro detekci narušení (IDS).

1.2.7 Zvyšování povědomí v komunitě: Organizování kampaní a školení pro veřejnost, aby lidé byli lépe informováni o hrozbách v kyberprostoru a jak se jim vyhnout.

Sekundární prevence je tedy zaměřena na reakci na vzniklé problémy a na pomoc těm, kteří se stali oběťmi kyberkriminality, a zároveň posiluje celkovou odolnost společnosti proti těmto hrozbám.

1.3 **Terciární prevence**:

Terciární prevence policejní kyberkriminality se zaměřuje na opatření a strategie, které se uplatňují po výskytu kyberkriminality s cílem minimalizovat škody, podpořit rehabilitaci obětí a snížit pravděpodobnost recidivy viníků. Mezi hlavní cíle terciární prevence patří:

1.3.1 Podpora obětí: Poskytování psychologické a právní pomoci obětem kyberkriminality, jako jsou například poradenství, krizová intervence nebo asistence při podávání trestních oznámení.

1.3.2 Vyšetřování a stíhání: Efektivní a rychlé vyšetřování kyberzločinů včetně shromáždění důkazů a jejich předání k dalšímu stíhání viníků. To zahrnuje spolupráci mezi různými policejními složkami a mezinárodní organizace.

1.3.3 Programy pro pachatele: Implementace rehabilitačních programů pro pachatele kyberkriminality, které by měly vést k jejich reintegraci do společnosti a snížení rizika recidivy.

1.3.4 Vzdělávání a osvěta: Organizování vzdělávacích programů a osvěty zaměřené na prevenci recidivy, které se mohou zaměřovat jak na pachatele, tak na oběti a širokou veřejnost.

1.3.5 Technologická opatření: Zavádění technických prostředků a opatření na ochranu před kyberútoky, které mohou být součástí rehabilitačního procesu pro oběti.

1.3.6 Globální a komunitní přístup: Spolupráce s jinými státními orgány, soukromým sektorem a neziskovými organizacemi na vytváření komplexních přístupů k prevenci a řešení kyberkriminality.

Terciární prevence tak hraje klíčovou roli v reakci na kyberkriminalitu, snaží se o rychlé a účinné řešení následků a podporu všech zúčastněných stran.

Prevence na místní úrovni

Prevence kyberkriminality na místní úrovni je důležitou součástí ochrany jednotlivců, organizací a komunit před digitálními hrozbami. Zde je několik kroků a strategií, které mohou místní komunity využít k efektivní prevenci:

1. Vzdělávání a osvěta: Organizace místních seminářů a workshopů zaměřených na kybernetickou bezpečnost. Osvěta o běžných typech kyberkriminality (např. phishing, ransomware) a metodách, jak se bránit.
2. Spolupráce s místními školami: Začlenění témat kybernetické bezpečnosti do školních osnov. Vzdělávání dětí a mládeže o bezpečném používání internetu a sociálních médií.
3. Podpora obětem kyberkriminality: Vytvoření místních hotlines nebo poraden pro oběti kyberkriminality, kde mohou lidé získat informace a pomoc.
4. Zavedení programů pro sdílení informací: Vytvoření místních sítí nebo fór, kde se mohou lidé podělit o zkušenosti a upozornit na nové hrozby.
5. Spolupráce s místními podniky: Nabídnout podnikům školení v oblasti kybernetické bezpečnosti, aby se chránily před útoky a aby byly informovány o osvědčených postupech.
6. Podpora lokálních IT specialistů: Vytvoření skupiny odborníků na kybernetickou bezpečnost, kteří poskytují poradenství a pomoc místním obyvatelům a organizacím.
7. Ochrana osobních údajů: Osvěta ohledně důležitosti ochrany osobních údajů a využívání silných hesel, dvoufaktorové autentizace a šifrování.

8. Organizace akcí pro zvýšení povědomí: Například Dny bezpečného internetu, kde se lidé mohou dozvědět více o tom, jak se chránit online.
9. Monitorování a reakce na incidenty: Vytvoření systému pro sledování kyberbezpečnostních incidentů a rychlou reakci na vzniklé hrozby.
10. Podpora legislativy: Zapojení se do lokálních iniciativ, které se snaží prosazovat zákony a předpisy zaměřené na ochranu proti kyberkriminalitě.

    Tato opatření mohou výrazně přispět k prevenci kyberkriminality na místní úrovni a přispět k větší bezpečnosti celé komunity.

4.8 Limity výzkumu

Výzkum kyberkriminality mladistvých je velmi důležitý, ale má několik omezení. Hlavní omezení jsou následující:

- Nedostatek dostupných údajů: Kyberkriminalita páchaná na dětech je často podhodnocena, protože mnoho případů zůstává nerozpoznáno nebo neohlášeno. To znamená, že výzkumní pracovníci nemají přístup k dostatečným údajům, aby mohli tento jev důkladně studovat.
- Etické otázky: Výzkum kyberkriminality páchané na dětech může vyvolat řadu etických problémů, zejména s ohledem na soukromí a bezpečnost dětí. Výzkumní pracovníci by měli být při nakládání s citlivými informacemi o dětech velmi opatrní a dodržovat přísné etické normy.
- Nedostatek spolupráce: Vyšetřování kyberkriminality páchané na dětech často vyžaduje spolupráci s řadou agentur a organizací, včetně škol, sociálních služeb a právních institucí. Pokud tyto organizace nejsou ochotny spolupracovat, může být obtížné získat potřebné údaje a informace.
- Omezené zdroje: Výzkum kyberkriminality páchané na dětech vyžaduje čas, peníze a další zdroje. Pokud výzkumní pracovníci nemají zdroje na provedení komplexní studie, mohou být jejich zjištění omezená a nedostatečná.

Navzdory těmto omezením je důležité pokračovat ve výzkumu kyberkriminality mládeže, aby bylo možné tomuto jevu lépe porozumět a vyvinout účinné strategie prevence a reakce. Je třeba vyvinout úsilí k překonání těchto omezení a najít nové přístupy k výzkumu v této oblasti.

Jako největší limit výzkumu spatřuji problém v nahlášených případech. Jelikož ne každý jednotlivý případ je podán na policii a mnoho z obětí tuto skutečnost ani neoznámí.

4.9 Závěr praktické části

Obecný závěr praktické části

Při výzkumu daného tématu jsem pracoval s dostupnými statistickými údaji, kdy nelze vyloučit mírné odchylky, např. z důvodu latence trestné činnosti. Nelze tedy pracovat se stoprocentní jistotou. Za zvýšením kybekriminality může stát počet a složení obyvatel, anonymita, zahlcení policejních a justičních orgánů, sociální prostředí a ekonomické podmínky (chudoba, nezaměstnanost, sociální vyloučení), nedostatečné vzdělání a nedostatečný přístup ke vzdělávání, rozvojová nerovnost a nejednotnost v oblasti sociálního zabezpečení, nedostatečný dohled a řízení veřejné správy a spravedlnosti, nedostatečná právní pravidla a systémy provádění zákonů, špatně organizovaný systém vzdělávání a výchovy v rodině, počet a složení obyvatel, anonymita, zahlcení policejních a justičních orgánů, nezaměstnanost, a jiné. **Příčinu meziročního vzestupu** můžeme hledat například v množství výpočetní techniky a zařízení a jejich vývoji (UI), množství uživatelů výpočetní techniky a internetu, vývoji softwaru, počítačové gramotnosti a celkové dovednosti již od útlého věku, portálech, sociálních sítích, e-shopech, bazarech (Marketplace), anonymitě, rychlosti, rozsahu páchané trestné činnosti, vlivu médií a globalizace, a jiných.

Zodpovězení výzkumných otázek

V jaké míře existují rozdíly mezi současnými druhy ohrožení u mládeže ve věku 15–17 let v nejlidnatějších krajích?

V roce 2023 byl u mladistvých ve věku 15–17 let nejvyšší podíl ohlášené kyberkriminality v Ústeckém kraji, avšak tento kraj se k těm nejlidnatějším neřadí. Nejvyšší podíl ohlášené kyberkriminality v nejlidnatějších krajích byl u kraje Jihomoravského s 16 zaznamenanými skutky. Druhou příčku obsadila Praha s 12 skutky a na třetí příčce se umístil kraj Jihomoravský, též nejlidnatější kraj s 11 ohlášenými skutky. Poslední příčku zaujal kraj Moravskoslezský s pouhými 4 skutky. Největší rozmanitost ohlášených skutků připadá kraji Jihomoravskému a Praze. Společným skutkem pro všechny vybrané kraje bylo v roce 2023 nebezpečné vyhrožování.

V jaké míře existují rozdíly u zkoumaných druhů ohrožení u mládeže ve věku 15–17 let v letech 2019 až 2023 v rámci celé ČR?

Od roku 2019 do roku 2023 bylo ohlášeno 590 případů a průměr tedy činní 118 případů. Rok 2023 se přesně nalézá v aktuálním průměru, avšak od roku 2019 dochází k nárůstu kyberkriminality ve věkové skupině 15–17 let. Od roku 2020 velmi prudce stoupá vyhrožování. S tím souvisí nebezpečné vyhrožování, avšak tento čin nestoupá tak závratnou rychlostí. Ostatní vybrané činy spíše stagnují, či se mírně snižují. Z celkových výsledků však vyplývá, že se jedná o zvýšení oproti předchozím rokům, výjimkou zůstává rok 2022. Nejvíce ohlášených případů podle klasifikace připadá nebezpečnému pronásledování s 51 skutky a nebezpečnému vyhrožování se 16 skutky.

Jsou prováděna nějaká preventivní opatření? Pokud ano, jaká?

Ano, jsou, a existuje nespočet preventivních opatření, která jsou prováděna. Můžeme si uvést například: **Vzdělávací programy** – školy často pořádají programy zaměřené na bezpečnost na internetu, kybernetickou etiku a povědomí o rizicích. Tyto programy pomáhají dospívajícím pochopit, jak se chránit před kyberšikanou a dalšími hrozbami. **Rodičovské workshopy** – rodiče také absolvují školení o kybernetické bezpečnosti, aby mohli lépe sledovat aktivity svých dětí na internetu a rozpoznat potenciální rizika. **Spolupráce s policií a neziskovými organizacemi** – policie a různé neziskové organizace často spolupracují na projektech prevence kyberkriminality, v jejichž rámci mohou mladí lidé rozvíjet kritické myšlení a odpovědné používání technologií. **Technologické nástroje** – bezpečné online prostředí pro nezletilé pomáhá zajistit řada aplikací a softwarů pro ochranu soukromí a zabezpečení, jako jsou filtry obsahu a rodičovská kontrola. **Zpravodajské kampaně a online osvěta** – vedení kampaní na sociálních sítích a dalších platformách s cílem zvýšit povědomí o kyberšikaně, phishingu a další kyberkriminalitě. **Podpora komunikace** – povzbuzujte dospívající, aby o svých zkušenostech a problémech na internetu mluvili s dospělými a pomohli tak včas odhalit a řešit problémy.

V rámci činností Policie České republiky existuje několik preventivních opatření, jako jsou: **Vzdělávací programy** – policie pořádá pro školy workshopy a semináře zaměřené na kybernetickou bezpečnost, ochranu soukromí a rizika spojená s používáním internetu. **Prevence a osvěta** – policistům jsou pravidelně poskytovány informace o bezpečném chování na internetu a hrozbách, jako je kyberšikana, loupeže a phishing. K tomu využívají školení, brožury a online zdroje. **Podpora rodičům** – policie také poskytuje rodičům rady a pokyny, jak sledovat a regulovat aktivity svých dětí na internetu, jak rozpoznat příznaky

kyberšikany a jak s dětmi komunikovat o bezpečnosti na internetu. **Spolupráce se školami** – policie úzce spolupracuje se školami a vzdělávacími institucemi na vytváření bezpečného prostředí pro děti a mládež, a to jak ve škole, tak na internetu. **Prevence kyberšikany** – specifické programy a kampaně zaměřené na prevenci kyberšikany zahrnují jak zvyšování povědomí o kyberšikaně, tak zásahy v případě jejího výskytu. **Monitorování a reakce na incidenty** – policie rovněž reaguje na oznámení kyberkriminality, včetně případů, kdy jsou obětí nebo pachatelem trestného činu nezletilí. **Online platformy a zdroje** – policie provozuje webové stránky a další online platformy, kde mohou teenageři získat informace o kybernetické bezpečnosti a řešit problémy.

SEZNAM POUŽITÉ LITERATURY

ERIKSON, Erik H., 2002. Dětství a společnost. Praha: Argo. ISBN 80-7203-380-8.

KAISER, Günther, 1994. Kriminologie: úvod do základů. Beckovy právnické učebnice. Praha: C.H. Beck. ISBN 80-7179-002-8.

KNÝ, Milan a VÍTEK, Miloš, 2015. Předpoklady informačních systémů v systémovém inženýrství. Praha: Policejní akademie České republiky v Praze. ISBN 978-80-7251-447-2.

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

KOPECKÝ, Kamil, 2010. Kybergrooming - nebezpečí kyberprostoru. 1. Olomouc: Net University. ISBN 978-80-254-7573-7.

KRAUS, Blahoslav a POLÁČKOVÁ, Věra, 2001. Člověk - prostředí - výchova: k otázkám sociální pedagogiky. Brno: Paido. ISBN 80-7315-004-2.

KYRIACOU, Chris, 2005. Řešení výchovných problémů ve škole. Pedagogická praxe (Portál). Praha: Portál. ISBN 80-7178-945-3.

MACEK, Petr, 2003. Adolescence. Vyd. 2., upr. Praha: Portál. ISBN 80-7178-747-7.

MATOUŠEK, Oldřich a KROFTOVÁ, Andrea, 2003. Mládež a delikvence: [možné příčiny, struktura, programy prevence kriminality mládeže]. Vyd. 2., aktualiz. Praha: Portál. ISBN 80-7178-771-x.

NIKL, Jaroslav, 2000. Sociálně patologické jevy u dětí a mládeže se zaměřením na jejich prevenci. Praha: Policejní akademie České republiky. ISBN 80-7251-033-9.

NOVOTNÝ, Oto a ZAPLETAL, Josef, 2001. Kriminologie. Praha: Eurolex Bohemia. ISBN 80-86432-08-4.

NOVOTNÝ, Oto, 2004. Kriminologie. 2., přeprac. vyd. Praha: ASPI. ISBN 80-7357-026-2.

PÁVKOVÁ, Jiřina, 2002. Pedagogika volného času. Vyd. 3., aktualiz. Praha: Portál. ISBN

PROCHÁZKA, Miroslav, 2012. Sociální pedagogika. Pedagogika (Grada). Praha: Grada. ISBN 978-80-247-3470-5.

SMEJKAL, Vladimír, 2018. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 978-80-7380-720-7.

SMEJKAL, Vladimír, 2022. Kybernetická kriminalita. 3. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 978-80-7380-849-5.

SOBOTKOVÁ, Irena, 2012. Psychologie rodiny. 3. vyd. Praha: Portál. ISBN 978-80-262-0217-2.

ŠIMÍČKOVÁ-ČÍŽKOVÁ, Jitka, 2010. Přehled vývojové psychologie. 3., upr. vyd. Olomouc: Univerzita Palackého v Olomouci. ISBN 978-80-244-2433-0.

THOROVÁ, Kateřina, 2015. Vývojová psychologie: proměny lidské psychiky od početí po smrt. Praha: Portál. ISBN 978-80-262-0714-6.

VÁGNEROVÁ, Marie, 2012. Vývojová psychologie: dětství a dospívání. Vydání druhé, doplněné a přepracované. Praha: Karolinum. ISBN 978-80-246-2153-1.

VOJTÍŠEK, Petr, 2012. Výzkumné metody. Praha: Vyšší odborná škola sociálně právní. ISBN 978-80-905109-3-7.

ZAVRŠNIK, Aleš, 2017. Kyberkriminalita. Právní monografie (Wolters Kluwer ČR). Praha: Wolters Kluwer. ISBN 978-80-7552-758-5.

Internetové zdroje

A walk on the dark side, 2007. Online. ECONOMIST.COM. Europe.view. Dostupné z: https://web.archive.org/web/20071110134626/http://economist.com/displaystory.cfm?story_id=9723768. [cit. 2024-04-12].

BLESSING, Guembe; AZETA, Ambrose a MISRA, Sanjay, 2022. The Emerging Threat of Ai-driven Cyber Attacks: A Review. Online. Dostupné z: https://www.researchgate.net/publication/359038562_The_Emerging_Threat_of_Ai-driven_Cyber_Attacks_A_Review. [cit. 2024-04-12].

EUROPEAN COUNCIL, 2021. Cybersecurity: how the EU tackles cyber threats. Online. 2024. Dostupné z: https://www.consilium.europa.eu/en/policies/cybersecurity/. [cit. 2024-04-12].

EUROPEAN COUNCIL. Kybernetická bezpečnost v programu DIGITAL Europe. Online. 2024. Dostupné z: https://digital-strategy.ec.europa.eu/cs/activities/cybersecurity-digital-programme [cit. 2024-04-12].

HAMUDDIN, Budianto; RAHMAN, Fathu; PAMMU, Abidin a SANUSI BASO, Yusring. CYBERBULLYING AMONG EFL STUDENTS' BLOGGING ACTIVITIES: MOTIVES AND PROPOSED SOLUTIONS. Online. Dostupné z: https://www.researchgate.net/publication/344087428_Cyberbullying_Among_EFL_Students'_Blogging_Activities_Motives_and_Proposed_Solutions. [cit. 2024-04-12].

HOMELAD SECURITY, 2011. Secretary Napolitano and Attorney General Holder Announce Largest U.S. Prosecution of International Criminal Network Organized to Sexually Exploit Children. Online. Dostupné z: https://www.dhs.gov/news/2011/08/03/secretary-napolitano-and-attorney-general-holder-announce-largest-us-prosecution. [cit. 2024-04-12].

KUBRIN, Charis E. a WEITZE, Ronald, 2003. New directions in social disorganization theory. Journal of Research in Crime and Delinquency,. Online. Dostupné z: https://www.researchgate.net/publication/255699203_New_Directions_in_Social_Disorganization_Theory. [cit. 2024-04-12].

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY, 2024. Ministerstvo vnitra České republiky. Online. 2024. Dostupné z: https://www.mvcr.cz/. [cit. 2024-04-12].

OTEVRENASPOLECNOST. Online. 2024. Dostupné z: https://www.otevrenaspolecnost.cz/. [cit. 2024-04-12].

Policie České republiky: Jednotlivé druhy kyberkriminality, 2023. Online. Dostupné z: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx. [cit. 2024-04-12].

WILSON, Clay, 2008. CRS Report for Congress. Online. Dostupné z: //efaidnbmnnnibpcajpcglclefindmkaj/https://sgp.fas.org/crs/terror/RL32114.pdf. [cit. 2024-04-12].

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ZŠ	Základní škola
MŠ	Mateřská škola
USB	Universal Serial Bus (Univerzální sběrnice Serial Bus)
WiFi	Wireless Fidelity (Bezdrátové připojení)
DDos	Distributed Denial of Service (Distribuované odepření služby)
PČR	Policie České Republiky
P2P	Peer-to-peer (přímý přenos)
VPN	Virtual Private Network (bezpečné a šifrované spojení mezi zařízením)
UDSB	Union Dime Saving Bank
MOD	Masters of Deception
UCLA	University of California, Los Angeles
DoS	Denial-of-service
RBN	Russian Business Network
DVD	Digital Versatile Disc
MPack	Multipurpose Internet Mail Extensions
EU	Evropská unie
UI	Umělá inteligence
GDPR	General Data Protection Regulation
NIS	Národní informační středisko
p.	Případ
KK	Kyberkriminalita

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA 1: REGISTROVANÉ SKUTKY ZA OBDOBÍ 2019 AŽ 2023 PÁCHANÉ NA MLADISTVÝCH DO

registrované skutky
objekt napadení - **osoby celkem**
věk: **mladiství (15-17let)**
Česká republika po krajích
období **1. 1. - 31. 12. 2022**
TSK **0-999 - celková kriminalita**
místo spáchání: **spácháno internetem + ostatními sítěmi (kyberkriminalita celkem)**

TSK takticko-statistická klasifikace:	KRPA 0	KRPS -1	KRPC -2	KRPP -3	KRPK -19	KRPU -4	KRPL -18	KRPH -5	KRPE -17	KRPJ -16	KRPB -6	KRPZ -15	KRPM -14	KRPT -7	ČR celkem
173 nebezpečné vyhrožování (§ 353)	6	0	1	2	0	1	0	1	0	0	2	0	0	0	**13**
174 nebezpečné pronásledování (§ 354)	0	2	1	0	0	0	0	1	0	0	0	0	0	1	**5**
175 účast na sebevraždě (§ 144) - *platná od 2021*	0	0	0	0	1	0	0	0	0	0	0	0	0	0	**1**
181 vydírání (§ 175)	6	4	1	2	0	1	2	3	0	1	3	1	0	4	**28**
202 sexuální nátlak (§ 186)	2	0	0	0	0	2	0	1	0	0	1	0	0	1	**7**
241 šíření pornografie (§ 191)	0	0	0	0	0	1	0	1	7	1	4	0	0	2	**16**
292 dětská pornografie a zneužití dítěte k ní (§ 192, 193) - *platná od 2021*	8	0	0	0	0	9	1	3	0	2	13	2	0	7	**45**
620 ohrožování výchovy dítěte (§ 201) - *platná od 2021*	0	2	0	1	0	1	12	0	14	0	0	0	0	1	**31**
708 pomluva (§ 184) - *platná od 2021*	0	0	0	0	0	0	0	0	0	0	0	0	1	0	**1**
celkem	**22**	**8**	**3**	**5**	**1**	**15**	**15**	**10**	**21**	**4**	**23**	**3**	**1**	**16**	**147**

17 LET VČETNĚ (PČR, 2024)

registrované skutky
objekt napadení - **osoby celkem**
věk: **mladiství (15-17let)**
Česká republika po krajích
období **1. 1. - 31. 12. 2023**
TSK **0-999 - celková kriminalita**
místo spáchání: **spácháno internetem + ostatními sítěmi (kyberkriminalita celkem)**

TSK takticko-statistická klasifikace:	KRPA 0	KRPS -1	KRPC -2	KRPP -3	KRPK -19	KRPU -4	KRPL -18	KRPH -5	KRPE -17	KRPJ -16	KRPB -6	KRPZ -15	KRPM -14	KRPT -7	ČR celkem
173 nebezpečné vyhrožování (§ 353)	1	1	1	3	0	1	0	1	0	3	1	0	2	2	**16**
174 nebezpečné pronásledování (§ 354)	1	0	0	0	0	0	0	0	0	0	0	0	0	0	**1**
181 vydírání (§ 175)	3	8	7	4	2	5	2	1	3	3	8	2	2	1	**51**
202 sexuální nátlak (§ 186)	0	0	0	0	1	4	0	0	0	0	3	0	3	0	**11**
241 šíření pornografie (§ 191)	1	0	0	0	0	1	0	2	0	1	1	0	0	0	**6**
281 obchodování s lidmi (§ 168)	1	0	0	0	0	0	0	0	0	0	0	0	0	0	**1**
292 dětská pornografie a zneužití dítěte k ní (§ 192, 193) - *platná od 2021*	2	1	1	0	0	6	0	1	1	4	2	3	0	0	**21**
296 svádění k pohlavnímu styku (§ 202/1) - *platná od 2021*	1	0	0	0	0	0	0	0	0	0	1	2	1	0	**5**
297 svádění k pohlavnímu styku (§ 202/2,3) - *platná od 2021*	1	0	0	0	0	0	0	0	0	0	0	0	0	1	**2**
620 ohrožování výchovy dítěte (§ 201) - *platná od 2021*	0	0	0	0	0	1	0	0	0	1	0	0	0	0	**2**
708 pomluva (§ 184) - *platná od 2021*	0	1	0	0	0	0	0	0	0	0	0	0	0	0	**1**
722 křivé obvinění a tlumočení, nepravdivý znalecký posudek (§ 345, 346, 347) - *platná od 2021*	1	0	0	0	0	0	0	0	0	0	0	0	0	0	**1**
celkem	**12**	**11**	**9**	**7**	**3**	**18**	**2**	**5**	**4**	**12**	**16**	**7**	**8**	**4**	**118**

registrované skutky
objekt napadení - **osoby celkem**
věk: **mladiství (15-17let)**
Česká republika po krajích
období **1. 1. - 31. 12. 2020**
TSK **0-999 - celková kriminalita**
místo spáchání: **spácháno internetem + ostatními sítěmi (kyberkriminalita celkem)**

TSK takticko-statistická klasifikace:	KRPA	KRPS	KRPC	KRPP	KRPK	KRPU	KRPL	KRPH	KRPE	KRPJ	KRPB	KRPZ	KRPM	KRPT	ČR celkem
173 nebezpečné vyhrožování (§ 353)	0	1	1	0	0	1	1	1	0	0	0	0	0	0	**5**
174 nebezpečné pronásledování (§ 354)	1	0	0	0	0	0	0	0	0	0	0	0	0	1	**2**
181 vydírání (§ 175)	1	1	1	0	2	2	1	1	0	0	0	1	2	2	**14**
202 sexuální nátlak (§ 186)	0	0	0	1	0	3	0	1	0	0	9	0	1	0	**15**
212 pohlavní zneužití ostatní (§ 187/1, 3, 4)	0	0	0	0	0	0	0	0	0	0	3	0	0	0	**3**
241 šíření pornografie (§ 191)	0	0	0	0	0	2	0	2	0	2	1	0	0	1	**8**
290 ostatní mravnostní trestné činy (§ 190, 192-194) - *platná do 2020*	4	1	1	2	0	4	7	2	0	2	5	1	2	5	**36**
631 ohrožování výchovy dítěte (§ 201, 202) - *platná do 2020*	0	0	0	0	0	1	1	0	6	3	2	0	0	3	**16**
celkem	**6**	**3**	**3**	**3**	**2**	**13**	**10**	**7**	**6**	**7**	**20**	**2**	**5**	**12**	**99**

registrované skutky
objekt napadení - **osoby celkem**
věk: **mladiství (15-17let)**
Česká republika po krajích
období **1. 1. - 31. 12. 2021**
TSK **0-999 - celková kriminalita**
místo spáchání: **spácháno internetem + ostatními sítěmi (kyberkriminalita celkem)**

TSK takticko-statistická klasifikace:	KRPA 0	KRPS -1	KRPC -2	KRPP -3	KRPK -19	KRPU -4	KRPL -18	KRPH -5	KRPE -17	KRPJ -16	KRPB -6	KRPZ -15	KRPM -14	KRPT -7	ČR celkem
0 právní kvalifikace nestanovena - *platná od 2019*	0	0	0	0	0	0	0	0	1	0	0	0	0	0	**1**
173 nebezpečné vyhrožování (§ 353)	1	0	1	1	1	2	1	0	0	0	4	0	1	1	**13**
174 nebezpečné pronásledování (§ 354)	0	0	0	0	0	1	0	0	0	0	0	0	0	0	**1**
181 vydírání (§ 175)	1	8	1	0	0	2	2	1	0	1	1	0	3	2	**22**
202 sexuální nátlak (§ 186)	0	2	0	1	0	1	2	0	0	1	4	5	1	1	**18**
241 šíření pornografie (§ 191)	1	0	0	0	0	1	3	0	0	0	3	0	0	2	**10**
292 dětská pornografie a zneužití dítěte k ní (§ 192, 193) - *platná od 2021*	3	1	2	3	1	1	5	0	1	2	6	5	0	0	**30**
294 navazování nedovolených kontaktů s dítětem (§ 193b) - *platná od 2021*	0	1	0	0	0	0	0	0	0	0	1	0	0	0	**2**
296 svádění k pohlavnímu styku (§ 202/1) - *platná od 2021*	1	0	0	0	0	0	0	0	1	1	0	0	0	0	**3**
620 ohrožování výchovy dítěte (§ 201) - *platná od 2021*	0	2	0	0	0	0	0	0	0	2	0	0	6	0	**10**
708 pomluva (§ 184) - *platná od 2021*	0	0	0	0	0	0	0	0	0	0	1	0	0	0	**1**
celkem	**7**	**14**	**4**	**5**	**2**	**8**	**13**	**1**	**3**	**7**	**20**	**10**	**11**	**6**	**111**

registrované skutky
objekt napadení - **osoby celkem**
věk: **mladiství (15-17let)**
Česká republika po krajích
období **1. 1. - 31. 12. 2019**
TSK **0-999 - celková kriminalita**
místo spáchání: **spácháno internetem + ostatními sítěmi (kyberkriminalita celkem)**

TSK takticko-statistická klasifikace:	KRPA	KRPS	KRPC	KRPP	KRPK	KRPU	KRPL	KRPH	KRPE	KRPJ	KRPB	KRPZ	KRPM	KRPT	ČR celkem
173 nebezpečné vyhrožování (§ 353)	4	0	1	1	0	0	0	1	0	1	0	0	1	0	**9**
174 nebezpečné pronásledování (§ 354)	0	0	0	1	0	2	0	0	0	1	0	0	0	1	**5**
181 vydírání (§ 175)	1	2	1	1	1	1	1	0	0	5	5	1	0	2	**21**
202 sexuální nátlak (§ 186)	1	1	1	1	0	0	0	7	3	1	3	0	1	0	**19**
241 šíření pornografie (§ 191)	2	0	1	1	0	0	0	3	1	3	0	0	0	0	**11**
271 kuplířství (§ 189)	0	0	0	0	0	1	0	0	0	0	0	0	0	0	**1**
290 ostatní mravnostní trestné činy (§ 190, 192-194) - *platná do 2020*	2	1	2	0	0	2	1	7	2	12	2	5	1	1	**38**
631 ohrožování výchovy dítěte (§ 201, 202) - *platná do 2020*	0	3	0	0	0	0	0	0	4	0	4	0	0	0	**11**
celkem	**10**	**7**	**6**	**5**	**1**	**6**	**2**	**18**	**10**	**23**	**14**	**6**	**3**	**4**	**115**

		2023 běžný rok														
	Kraj - ředitelství PČr	KRPA	KRPS	KRPC	KRPP	KRPK	KRPU	KRPL	KRPH	KRPE	KRPJ	KRPB	KRPZ	KRPM	KRPT	Celkem
zdroj: PČr	děti do 18let	37	35	35	16	7	67	27	24	29	23	50	27	24	26	427
zdroj: PČr	mladiství 15-17let vč.	12	11	9	7	3	18	2	5	4	12	16	7	8	4	118
zdroj: Vlastní zprac.	mladší 15 let	25	24	26	9	4	49	25	19	25	11	34	20	16	22	309
	Kraj - obyvatelstvo	Praha	Středočeský	Jihočeský	Plzeňský	Karlovasrký	Ústecký	Liberecký	Královehradecký	Pardubický	Vysočina	Jihomoravský	Zlínský	Olomoucký	Moravskoslezký	
zdroj: Vlastní zprac./ ČSÚ	počet obyvatel děti do 18let	261492	309 306	124699	114 522	53 670	154680	87330	105 133	102609	98 251	237898	106697	119346	218 444	1 727 758
zdroj: Vlastní zprac./ ČSÚ	počet obyvatel. 15-17let včetně	42845	53 043	21934	20 496	10 277	29031	15770	19 186	18049	17 079	39481	18736	21006	39 386	266 319
zdroj: Vlastní zprac./ ČSÚ	počet obyvatel. mladší 15let	218647	256263	102765	94026	43393	125649	71560	85947	84560	81172	198417	87961	98340	179058	2 094 077
zdroj: ČSÚ	nezaměstnanost %	2,1	1,7	1,7	2,1	4,3	4,0	3,3	3,2	1,9	1,5	2,5	2,3	2,8	3,9	2,66

registrované skutky

objekt napadení - **osoby celkem** (mladistvý osoba mladší 18 let a starší 15 let.)
věk: **mladiství (15-17let)**
Česká republika po krajích
období **1. 1. - 31. 12. 2023**
místo spáchání: **spácháno internetem + ostatními sítěmi (kyberkriminalita celkem)**

	KRPA Praha	**KRPS** Středočeský	**KRPC** Jihočeský	**KRPP** Plzeňský	**KRPK** Karlovasrký	**KRPU** Ústecký	**KRPL** Liberecký	**KRPH** Královehradecký	**KRPE** Pardubický	**KRPJ** Vysočina	**KRPB** Jihomoravský	**KRPZ** Zlínský	**KRPM** Olomoucký	**KRPT** Moravskoslezký	**ČR celkem**
173 nebezpečné vyhrožování (§ 353)	1	1	1	3	0	1	0	1	0	3	1	0	2	2	**16**
174 nebezpečné pronásledování (§ 354)	1	0	0	0	0	0	0	0	0	0	0	0	0	0	**1**
181 vydírání (§ 175)	3	8	7	4	2	5	2	1	3	3	8	2	2	1	**51**
202 sexuální nátlak (§ 186)	0	0	0	0	1	4	0	0	0	0	3	0	3	0	**11**
241 šíření pornografie (§ 191)	1	0	0	0	0	1	0	2	0	1	1	0	0	0	**6**
281 obchodování s lidmi (§ 168)	1	0	0	0	0	0	0	0	0	0	0	0	0	0	**1**
292 dětská pornografie a zneužití dítěte k ní (§ 192, 193) - *platná od 2021*	2	1	1	0	0	6	0	1	1	4	2	3	0	0	**21**
296 svádění k pohlavnímu styku (§ 202/1) - *platná od 2021*	1	0	0	0	0	0	0	0	0	0	1	2	1	0	**5**
297 svádění k pohlavnímu styku (§ 202/2,3) - *platná od 2021*	1	0	0	0	0	0	0	0	0	0	0	0	0	1	**2**
620 ohrožování výchovy dítěte (§ 201) - *platná od 2021*	0	0	0	0	0	1	0	0	0	1	0	0	0	0	**2**
708 pomluva (§ 184) - *platná od 2021*	0	1	0	0	0	0	0	0	0	0	0	0	0	0	**1**
722 křivé obvinění a tlumočení, nepravdivý znalecký posudek (§ 345, 346, 347) - *platná od 2021*	1	0	0	0	0	0	0	0	0	0	0	0	0	0	**1**
celkem	**12**	**11**	**9**	**7**	**3**	**18**	**2**	**5**	**4**	**12**	**16**	**7**	**8**	**4**	**118**

objekt napadení - **osoby celkem**
věk: **mladiství (15-17let)**
Česká republika po krajích
období **1. 1. - 31. 12. 2021**
TSK **0-999 - celková kriminalita**
místo spáchání: **spácháno internetem + ostatními sítěmi (kyberkriminalita celkem)**

TSK takticko-statistická klasifikace:	KRPA	KRPS	KRPC	KRPP	KRPK	KRPU	KRPL	KRPH	KRPE	KRPJ	KRPB	KRPZ	KRPM	KRPT	ČR celkem
0 právní kvalifikace nestanovena - *platná od 2019*	0	0	0	0	0	0	0	0	1	0	0	0	0	0	**1**
173 nebezpečné vyhrožování (§ 353)	1	0	1	1	1	2	1	0	0	0	4	0	1	1	**13**
174 nebezpečné pronásledování (§ 354)	0	0	0	0	0	1	0	0	0	0	0	0	0	0	**1**
181 vydírání (§ 175)	1	8	1	0	0	2	2	1	0	1	1	0	3	2	**22**
202 sexuální nátlak (§ 186)	0	2	0	1	0	1	2	0	0	1	4	5	1	1	**18**
241 šíření pornografie (§ 191)	1	0	0	0	0	1	3	0	0	0	3	0	0	2	**10**
292 dětská pornografie a zneužití dítěte k ní (§ 192, 193) - *platná od 2021*	3	1	2	3	1	1	5	0	1	2	6	5	0	0	**30**
294 navazování nedovolených kontaktů s dítětem (§ 193b) - *platná od 2021*	0	1	0	0	0	0	0	0	0	0	1	0	0	0	**2**
296 svádění k pohlavnímu styku (§ 202/1) - *platná od 2021*	1	0	0	0	0	0	0	0	1	1	0	0	0	0	**3**
520 ohrožování výchovy dítěte (§ 201) - *platná od 2021*	0	2	0	0	0	0	0	0	0	2	0	0	6	0	**10**
708 pomluva (§ 184) - *platná od 2021*	0	0	0	0	0	0	0	0	0	0	1	0	0	0	**1**
celkem	**7**	**14**	**4**	**5**	**2**	**8**	**13**	**1**	**3**	**7**	**20**	**10**	**11**	**6**	**111**