VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

PROBLEMATIKA DĚTSKÉ PORNOGRAFIE, JEJÍ DOSTUPNOST NA SOCIÁLNÍCH SÍTÍCH A MOŽNOSTI PREVENCE

Autor práce: Radek Buzek, DiS.

Studijní program: Bezpečnostně právní činnost

Forma studia: Kombinovaná

Vedoucí práce: Mgr. Zuzana Kocíková, MBA

Katedra: Katedra právních oborů a bezpečnostních studií

2024

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.
Žižkova tř. 1632/5b, 370 01 České Budějovice

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Radek Buzek, DiS.

Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Místo studia: Příbram

Název bakalářské práce: Problematika dětské pornografie, její dostupnost na sociálních sítích a možnosti prevence

Název bakalářské práce v anglickém jazyce: Child Pornography, its Availability on Social Networks and Possibilities of its Prevention

Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce: Mgr. Zuzana Kocíková, MBA

Datum zadání bakalářské práce: říjen 2023

Cíl bakalářské práce:
Hlavním cílem bakalářské práce je analýza rizik a dostupnosti dětské pornografie v online prostředí s explicitním zaměřením na sociální sítě a na konkrétní formy trestné činnosti páchané na dětech v kyberprostoru. Vedlejším cílem jsou návrhy řešení, prevence a vzdělávání zaměřené na informovanost dětí, rodičů a škol k problematice dětské pornografie.

Student: Radek Buzek, DiS.	24.11.2023 *datum*	*podpis*
Vedoucí práce: Mgr. Zuzana Kocíková, MBA	25.11.2023 *datum*	*podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	27.11.2023 *datum*	*podpis*
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	28.11.2023 *datum*	*podpis*
Rektor: doc. Ing. Jiří Dušek, Ph.D.	7.12.2023 *datum*	*podpis*

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z.ú. ČESKÉ BUDĚJOVICE

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce v elektronické podobě ve veřejně přístupné části infodisku VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucí(ho) a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Děkuji vedoucí bakalářské práce Mgr. Zuzaně Kocíkové, MBA za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

BUZEK, R. *Problematika dětské pornografie, její dostupnost na sociálních sítích a možnosti prevence*. České Budějovice: Vysoká škola evropských a regionálních studií, 2024. 76 s. Vedoucí bakalářské práce: Mgr. Zuzana Kocíková, MBA

Klíčová slova: dětská pornografie, kybernetická kriminalita, kyberprostor, prevence, sociální sítě

Tato bakalářská práce se zaměřuje na problematiku trestné činnosti šíření dětské pornografie, její dostupnosti na sociálních sítích a možnosti prevence. Dětská pornografie je závažným globálním problémem, který zasahuje do životů zranitelných dětí a mládeže. V posledních letech došlo k nárůstu případů, kdy je dětská pornografie dostupná na internetu a sociálních sítích, což zvyšuje riziko sexuálního vykořisťování dětí.

V teoretické části práce, která obsahuje vysvětlení základních pojmů, jsou identifikovány hlavní faktory, které přispívají k dostupnosti dětské pornografie na darknetech, sociálních sítích, s využitím anonymních účtů a šifrované komunikace, které mohou usnadňovat šíření nelegálního obsahu. Dále se bude zabývat možnostmi prevence a ochrany dětí před škodlivým obsahem na internetu. Nedílnou součástí této práce je zaměření na spolupráci mezi orgány činnými v trestním řízení, sociálními sítěmi, organizacemi pro ochranu dětí a dále postupy orgánů činných v trestním řízení při řešení a objasňování trestných činů mravnostního charakteru páchaných v kyberprostoru.

Druhá část bakalářské práce je zpracována formou kazuistiky a komparace třech případů z praxe, které ilustrují různé aspekty problematiky dětské pornografie dostupné a šířené na sociálních sítích. Cílem této práce je poskytnout ucelený pohled na problematiku dětské pornografie na sociálních sítích a zdůraznit důležitost prevence a ochrany dětí. Je nezbytné bránit se šíření tohoto nelegálního obsahu a aktivně přistupovat k ochraně dětí na internetu.

ABSTRACT

BUZEK, R. *Child Pornography, its availability on Social Networks and possibilities of its Prevention: Bachelor Thesis.* České Budějovice: The College of European and Regional Studies, 2024. 76 pgs. Supervisor: Mgr. Zuzana Kocíková, MBA

Key words: Child Pornography, Cybercrime, Cyberspace, Prevention, Social Networks

This bachelor's thesis focuses on the issue of the criminal activity related to the dissemination of child pornography, its availability on social networks and the possibilities of prevention. Child pornography is a serious global problem that affects the lives of vulnerable children and young people. In recent years, there has been an increase in the number of child pornography available on the Internet and social networks, increasing the risk of child sexual exploitation.

Theoretical part of the work, which contains an explanation of basic terms, identifies the main factors that contribute to the availability of child pornography on darknets, social networks, using anonymous accounts and encrypted communication, which can facilitate the spread of illegal content. It will also deal with the possibilities of prevention and protection of children from harmful content on the Internet. An integral part of this work is the focus on cooperation between law enforcement authorities, social networks, organizations for the protection of children, as well as the procedures of law enforcement authorities in solving and clarifying crimes of a moral nature committed in cyberspace.

The second part of the bechelor`s thesis is processed in the form of case studies and comparations of three cases from practice is processed. The cases illustrate various aspects of child pornography available and distributed on social networks. The aim of this work is to provide a comprehensive view of child pornography on social networks and to emphasize the importance of prevention and protection of children. It is essential to prevent the dissemination of this illegal content and take an active approach to protecting children on the Internet.

Obsah

Úvod

Dětská pornografie, její vytváření a šíření sexuálně explicitního materiálu zahrnujícího nezletilé osoby, představuje jednu z nejnebezpečnějších forem sexuálního zneužívání dětí a mládeže a bývá zahrnuta do oblasti kybernetické kriminality. Toto téma v současné společnosti získává stále větší pozornost, a to zejména v kontextu rostoucího vlivu anonymního digitálního prostředí a sociálních sítí. S nástupem umělé inteligence se tento problém prohlubuje, neboť dětská pornografie může být vytvářena uměle v digitálním prostředí.

Kybernetická kriminalita nastoupila s rozvojem informačních technologií, pro běžného uživatele mimo jiné s rozvojem osobních počítačů a telekomunikačních technologií. Informační technologie skýtají mnoho pozitiv, ale s jejich vývojem se mohou objevovat i určité negativní jevy, které se postupem času rozrůstají do vážných problémů, jako je dětská pornografie, kontaktování dětí pedofily prostřednictvím sociálních sítí, kyberšikana a další. Informační technologie se tímto stávají i určitou vážnou hrozbou, i přes veškeré své výhody.

S kybernetickou kriminalitou problematika dětské pornografie a její dostupnosti na sociálních sítích úzce souvisí. Digitální prostředí poskytuje pachatelům nástroje, které jim umožňují operovat na mezinárodní úrovni s relativní anonymitou a bez stanovených hranic. Toto bezprecedentní globální propojení má za následek, že dětská pornografie se stala mnohem obtížněji vystopovatelnou a vymahatelnou, než tomu bylo v minulosti. Orgány činné v trestním řízení mohou mít potíže na tento trend rychle a adekvátně reagovat, neboť současné trestné právní normy nejsou připraveny na tento druh kriminality a mezinárodní spolupráce mezi státy není optimální. Globálnost kyberprostoru proto vede často k problematickému postihu prostřednictvím současného trestního systému.

Děti a mladiství se dnes pohybují ve světě, kde jsou internet a sociální sítě běžnou součástí jejich každodenního života. Tento digitální svět však přináší nové výzvy a nebezpečí, včetně snadné dostupnosti dětské pornografie a jejího rychlého šíření. Tyto záležitosti se dotýkají nejen samotných obětí, které mohou být zneužity a vystaveny trvalým psychickým a fyzickým následkům. Dětská pornografie na sociálních sítích představuje dvojí hrozbu. Tento nelegální obsah může být na těchto platformách záměrně vytvářen a šířen, čímž se stává snadněji dostupným. A za druhé, sociální sítě mohou

sloužit jako prostředek pro hledání nových obětí a zprostředkování sexuálního zneužívání dětí, a to včetně online groomingu, tedy navazování důvěrného vztahu s dítětem za účelem jeho zneužití.

Svět se neustále mění, a s ním i způsoby, jakými se dětská pornografie šíří a jak na ni společnost reaguje. Je důležité se touto problematikou vážně zabývat a hledat cesty, jak ochránit naše nejzranitelnější členy společnosti, tedy děti a mládež. Tato bakalářská práce se pokusí přispět k lepšímu porozumění této problematiky, návrhu opatření, která by mohla přispět k ochraně nezletilých před touto závažnou formou zneužívání a k formulaci efektivních preventivních opatření.

1 Cíl a metodika bakalářské práce

Tato práce se ve své teoretické části zabývá problematikou dětské pornografie, její dostupnosti ve skryté části internetu tzv. darknetech a na sociálních sítích, jejím vytvářením pomocí umělé inteligence a návrhy preventivních opatření k ochraně dětí před touto formou zneužívání. Práce analyzuje rozsah a povahu dětské pornografie a identifikuje klíčové rizikové faktory a způsoby šíření dětské pornografie na internetu a sociálních sítích.

Tato problematika je jednou z forem kybernetické kriminality a je v současné době velmi aktuální a mimořádně citlivá, neboť dětská pornografie představuje závažné porušení lidských práv a způsobuje trvalé psychické a fyzické poškození dětí. Důsledky tohoto zneužívání jsou pro oběti devastující, a proto je nezbytné tuto problematiku pečlivě analyzovat a přijmout opatření k jejímu potlačení.

Cílem práce je tedy zhodnotit stávající preventivní opatření a právní rámce v oblasti dětské pornografie na sociálních sítích a navrhnout a ověřit účinné preventivní strategie a nástroje na ochranu dětí před touto závažnou trestnou činností.

V druhé části práce je, pro dosažení stanovených cílů, zvolena komparativní analýza třech reálných případů, které se týkají dětské pornografie na sociálních sítích. Tato metoda umožní získat hlubší pohled do problematiky a porovnat různé situace v praxi. Případy jsou vybrány tak, aby zahrnovaly různé aspekty této problematiky, jako je šíření obsahu, způsoby navázání kontaktů s oběťmi, průběh vyšetřování až k ustanovení pachatelů a seznámení se s postupy orgánů činných v trestním řízení (dále OČTŘ).

U vybraných případů je také proveden kvalitativní výzkum a rozhovor s vyšetřovateli. Tento výzkum zahrnuje sběr a analýzu důkazů a dalších relevantních informací. Rozhovory s vyšetřovateli jsou klíčovou součástí kvalitativní analýzy případů, neboť umožní získat detailnější a osobnější vhled do konkrétních situací týkajících se dané problematiky.

2 Vymezení základních pojmů

Tato kapitola se věnuje výkladu základních pojmů kriminalita, internet, kyberprostor, kybernetická kriminalita, dítě, dětská pornografie a sociální sítě, které jsou určeny pro lepší orientaci ve čtení této práce.

2.1 Kriminalita

Kriminalita se vyskytuje v každé společnosti a spolu s ní se také dochází k jejímu vývoji. Ačkoliv je kriminalita negativním jevem, který je pro společnost škodlivý, je reálně prakticky nemožné tento jev odstranit. Podle kriminologických publikací jsou dvě základní pojetí kriminality a to pojetí legální a sociologické. Legální pojetí definuje kriminalitu jako souhrn jednání, které trestní právo posuzuje jako trestné činy. A sociologické pojetí, které definuje kriminalitu jako odchylné chování od určité normy.[1]

Kriminalita je obecně chápána jako soubor činů nebo jednání, která jsou v rozporu s platnými právními normami v dané společnosti. Termín kriminalita může označovat širokou škálu činů, od menších společensky škodlivých jednání až po závažné trestné činy.[2] Mezi příklady kriminálních činů patří krádeže, loupeže, vraždy, podvody, únosy, vandalismus a mnoho dalších. Mezi nejzávažnější trestné činy lze zařadit trestné činy proti lidské důstojnosti v sexuální oblasti, které jsou uvedeny v hlavě III. zákona č. 40/2009 Sb. trestního zákona. Trestný čin zneužití dítěte k výrobě pornografie podle § 193 trestního zákona a další trestné činy úzce souvisí s kriminalitou kybernetickou, neboť dětská pornografie byla vyráběna i v minulosti, v době, kdy ještě nebyly počítačové sítě, internet a jiné komunikační systémy, ale až s nástupem těchto technologií začala být masivně šířena a uchovávána v kyberprostoru.

2.2 Internet

Internet je celosvětová síť počítačů a dalších zařízení, která je propojena prostřednictvím standardizovaných komunikačních protokolů.[3] Tato síť umožňuje počítačům a dalším IT zařízením komunikovat mezi sebou. Internet poskytuje přístup

[1] NOVOTNÝ, O., ZAPLETATL, J., a kol. *Kriminologie.* 3.vyd. Praha: ASPI-Wolters Kluwer, 2008, ISBN 9788073574093. s. 20.
[2] TOMÁŠEK, J. *Úvod do kriminologie: Jak studovat zločin.* Praha: Grada, 2010, ISBN 978-80-247-2982-4. s. 11.
[3] SMEJKAL, V. *Kybernetická kriminalita*. 3. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. ISBN 978-80-7380-849-5. s. 52.

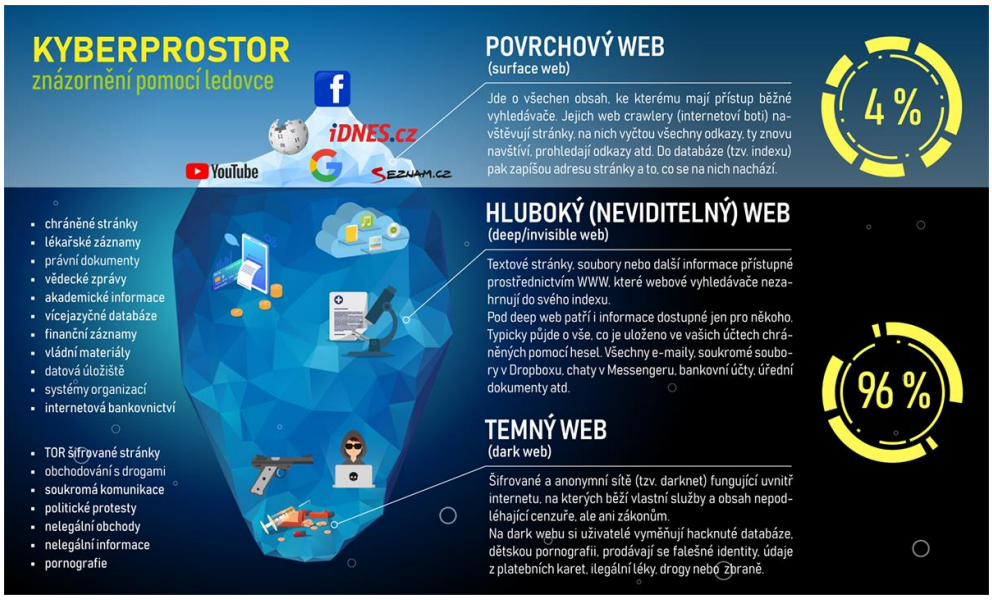
k obrovskému množství informací, služeb a zdrojů, a je neocenitelným nástrojem pro komunikaci, vzdělávání, zábavu, obchod a mnoho dalších činností.

Internet si lze představit jako je virtuální počítačový svět tzv. kyberprostor. K definici kyberprostoru je možné využít znění § 2 písm. a) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, kde je uvedeno, že „*kybernetickým prostorem je digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy a službami a sítěmi elektronických komunikací.*“ [4]

Kyberprostor si lze představit jako pomyslný ledovec, kde jeho viditelná část představuje tzv. “Surface Web“, který je dostupný veřejnosti za použití standardních webových prohlížečů. Tato část kyberprostoru obsahuje veřejně dostupné domény, včetně sociálních sítí.

Další částí kyberprostoru je tzv. darknet, také nazýván temný internet nebo temný web a je částí internetu, která není veřejně indexována standardními vyhledávači a není snadno přístupná běžným webovým prohlížečům. Tato část internetu je známá svou anonymitou a soukromím a velmi často slouží k různým legálním i nelegálním aktivitám, jako jsou například prodej ilegálních drog, zbraní, kybernetické útoky, hacking, krádeže dat, šíření dětské pornografie a další trestná činnost.

Obrázek 1: Znázornění kyberprostoru formou "ledovce"[5]



[4] Zákon č. 181/2014 Sb., o ., *o kybernetické bezpečnosti,* § 2 písm. a). In: Zákony pro lidi [online]. Praha: ©AION CS, 2010–2023 [cit. 2023-12-07]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-121.
[5]Kyberprostor. In: PortálDigi.cz [online]. 2019. [cit. 2023-12-07]. Dostupné z https://www.kurzy.portaldigi.cz.

Do této části webu se lze připojit například za využití TOR (The Onion Router) sítí, softwaru pro anonymní komunikaci a za využití tohoto nástroje lze procházet internetové stránky s příponou ".onion".

V temném webu dochází k závažné trestné činnosti včetně šíření dětské pornografie a ke komunikaci mezi sexuálními predátory, přes šifrované komunikační platformy, kteří si touto cestou své poznatky vyměňují a následně na sociálních sítích vyhledávají své oběti. S temným webem úzce souvisí i virtuální měna. Tedy forma měny digitální či kryptoměny, která existuje pouze v elektronické podobě. Díky své decentralizaci a schopnosti poskytovat relativní anonymitu, je používána k placení a obchodu s nelegálním obsahem a páchání kybernetické kriminality.

2.3 Kybernetická kriminalita

Kybernetická kriminalita, také nazývána „kyberkriminalita", je trestná činnost prováděná v digitálním prostředí prostřednictvím počítačů, sítí a internetu. Tato forma kriminality zahrnuje různé činnosti, které využívají technologie a digitální prostředí k nelegálním účelům.[6]

„Pojem kybernetická kriminalita je odvozován od pojmu kybernetický prostor, případně zkráceně kyberprostor. Kyberprostor můžeme označit jako „virtuální prostředí", které nemá začátek ani konec, nezná hranice národních států a nelze určit, jak rozsáhlý je. Kybernetická kriminalita, dříve také označována jako informační kriminalita, je definována u Policie ČR jako trestná činnost, která je páchána v prostředí informačních a komunikačních technologií, včetně počítačových sítí. Samotná oblast informačních a komunikačních technologií je buď předmětem útoku, nebo je páchána trestná činnost za výrazného využití informačních a komunikačních technologií, jakožto významného prostředku k jejímu páchání." [7]

„Kybernetickou kriminalitu lze považovat za činnosti zprostředkované počítačem, které jsou buď nezákonné, nebo jsou některými stranami považovány za nedovolené a které lze provádět prostřednictvím globálních elektronických sítí."[8]

[6] SMEJKAL, V. *Kybernetická kriminalita*. 3. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. s. 73.
[7]Policie ČR, *Kyberkriminalita* [online]. [cit. 2023-11-06]. Dostupné z: www.policie.cz/clanek/kyberkriminalita.aspx.
[8] DOUGLAS, T., BRIAN, D. L. *Cybercrime.* Taylor & Francis Ltd 2000. s. 13.

Podle Jirovského může být kyberkriminalita namířena proti datům, sítím, hardwaru, softwaru, ale může být využita i jako prostředek, nástroj pro páchání trestných činů a pachatel může snadno a rychle měnit svou identitu, realizovat různé hrozby a skrývat se v kyberprostoru.[9]

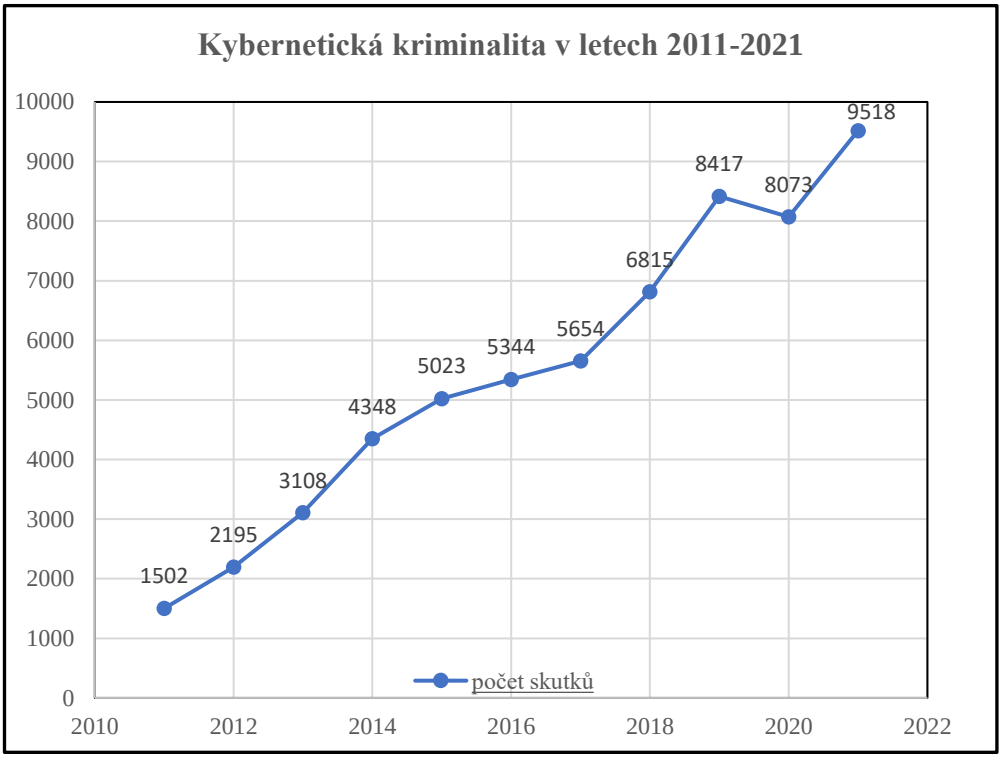
Kybernetické kriminalitě je věnována stále větší pozornost, neboť s dynamickým rozvojem informačních technologií dochází k novým společensky škodlivým jednáním. Pachatelé jsou velmi těžko dohledatelní, neboť páchající trestnou činnost v kyberprostoru s využitím různých anonymizačních nástrojů, například VPN služeb, které maskují jejich skutečnou IP adresu a umožňují jim provádět útoky z různých geografických umístění.[10] Pachatelé vytváří falešné online identity, účty na sociálních sítích nebo internetových fórech. Tím se tedy velmi snižuje pravděpodobnost určení místa, ze kterého je páchána trestná činnost a identifikace konkrétních osob.

Se vznikem kryptoměn v roce 2009 došlo k prohloubení tohoto problému, neboť pachatelé platí za nelegální obsah ve virtuálních měnách. Mnoho kryptoměn, jako například bitcoin, umožňuje anonymní transakce. Pachatelé mohou používat kryptoměny k provádění ilegálních transakcí a převodů, aniž by byli snadno identifikovatelní. Kyberkriminální aktivity, včetně šíření dětské pornografie, jsou často prováděny na již zmiňovaném dark webu a kryptoměny jsou běžně akceptovány jako prostředek platby za tyto služby.

Kybernetická kriminalita každým rokem narůstá po celém světě a jedná se tedy o globální problém. Zatímco například v roce 2011 bylo v České republice registrováno 1502 trestných činů v této oblasti, v roce 2021 to bylo již 9518 skutků. Za období let 2022-2023 nejsou v současné době statistky této trestné činnosti k dispozici. Každoroční nárůst této kriminality je patrný z níže uvedené tabulky, která čerpá z dat vnitřních systémů Policie ČR.[11]

[9] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. ISBN 978-802-4715-612. s. 19.
[10] SMEJKAL, V. *Kybernetická kriminalita*. 3. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. ISBN 978-80-7380-849-5. s. 72.
[11] Zdroj: vnitřní informační systémy a evidence Policie ČR.

Graf 1: Kybernetická kriminalita v letech 2011-2021[12]



Pod kybernetickou kriminalitu je možné zařadit mimo jiné i trestný čin šíření dětské pornografie dle § 191 trestního zákona, kterému je věnována samostatná část v kapitole legislativa.

2.4 Dětská pornografie

„Definovat dětskou pornografii lze mnoha způsoby. Vždy se ovšem jedná o určitou formu znázornění, například v podobě fotografie či videozáznamu, sexuálních motivů či aktivit, ve kterém je zobrazeno jako sexuální aktér nebo objekt dítě. Vše za účelem vyvolání pohlavního vzrušení. Může se jednat například o snímky obnažených dětí zachycující polohy skutečného či předstíraného sexuálního styku nebo snímky obnažených dětí v polohách vyzývavě předvádějících pohlavní orgány a v různých erotických polohách. Český právní systém zakazuje zveřejňování, zprostředkování, nabízení, uvedení do oběhu a jiné zpřístupnění dětské pornografie. Zde je na místě zmínit, že i děti mohou šířit dětskou pornografii. Nelze opomenout i jiné způsoby páchání trestného činu šíření dětské pornografie. Typickým příkladem je fotografování dětí – modelů za účelem uplatnění v reklamě či pro různé módní časopisy. Organizátoři těchto akcí oslovují zpravidla rodiny ve složité sociální či finanční situaci s příslibem nafocení dítěte pro takovéto účely.“[13]

[12] Zdroj: vnitřní informační systémy a evidence Policie ČR.
[13] Policie ČR, *Kyberkriminalita* [online]. [cit. 2023-11-08]. Dostupné z: www.policie.cz/clanek/kyberkriminalita.aspx.

Je důležité zdůraznit, že dětská pornografie je nezákonná a eticky nepřijatelná. Tento druh materiálu je závažným trestným činem v mnoha zemích a je striktně zakázán, neboť porušuje práva na ochranu dětí. Obecně je tato problematika považována za závažný zločin a mnoho zemí disponuje přísnými zákony a postihy pro ty, kteří jsou zapojeni do její výroby, distribuce nebo konzumace. V ČR lze trestné činy týkající se dětské pornografie zmínit například tyto:

a) výroba a šíření dětské pornografie
b) zneužití dítěte k výrobě pornografie
c) pohlavní zneužití[14]

Ochrana dětí před tímto druhem zneužívání a ochrana jejich práv je tedy prioritou pro mezinárodní a národní právní systémy. Silná ochrana dětí mladších 18 let před jejich zneužíváním je v Evropské unii zajištěna na základě rámcového rozhodnutí. Největší míru této kriminality zahrnuje šíření a distribuce v kyberprostoru, ve kterém je velmi obtížné pachatele identifikovat.[15]

2.4.1 Dítě

Pojem dítě se obvykle odkazuje na osobu, která dosud nedosáhla zákonného věku pro plnoletost nebo dospělost, což může být v různých jurisdikcích různé. Věková hranice, kdy je jednotlivec považován za dítě, se liší podle právním předpisů země. V České republice platí, že dítě je osoba mladší osmnácti let, pokud trestní zákon nestanoví jinak.[16]

2.5 Sociální sítě

Sociální sítě jsou online platformy, které umožňují uživatelům vytvářet uživatelské profily, sdílet fotografie, videa a další různý obsah. Komunikovat s ostatními uživateli, vytvářet skryté a uzavřené skupiny a využívat mnoho dalších služeb. Sociální sítě tedy slouží k propojení a komunikaci uživatelů ve virtuálním prostoru.

Vznik sociálních sítí můžeme datovat od konce 20. století, ale jejich masový rozvoj začal ve 21. století s rozšířením internetu a technologického pokroku. Milníkem

[14] BLATNÍKOVÁ, Š. *Pachatelé komerčního sexuálního zneužívání dětí.* Vyd. KUFR s.r.o. 2009. ISBN 978-80-7338-091-5. s. 41.
[15] Tamtéž.
[16] ČESKO. Zákon č. 40/2009 Sb., *trestní zákon, ve znění pozdějších předpisů,* § 126.

v historii moderních sociálních sítí byla sociální síť Friendster, která byla založena Jonathanem Abramsem v roce 2002 a spuštěna v březnu roku 2003. Jednalo se o sociální síť, za niž byla v roce 2003 společnost Google ochotna zaplatit 30 miliónů dolarů, ale tvůrci tuto nabídku odmítli.[17]

Nicméně, největší rozvoj sociálních sítí přišel s vytvořením facebooku v roce 2004 Markem Zuckerbergem, což bylo pro mnoho lidí významným okamžikem v historii sociálních médií. Facebook rychle získal oblibu a otevřel cestu pro mnoho dalších sociálních sítí, jako je twitter (dnešní síť X), instagram, LinkedIn a mnoho dalších.[18]

Sociální sítě jsou celosvětovým, stále se rozvíjejícím fenoménem. Patří v současnosti mezi nejnavštěvovanější webové služby s miliony aktivních uživatelů, kteří si navzájem vyměňují data různorodého charakteru. Jejich oblíbenost nestoupá jen u klasických uživatelů, ale také u velkých i malých firem nebo vzdělávacích institutů, kterým slouží pro marketing, reklamu a k propagaci svých výrobků, služeb nebo vzdělávání. Hrají klíčovou roli v komunikaci, sdílení informací a budování sociálních vztahů. Jejich počty se neustále mění a v současné době jich je dostupných nepřeberné množství. Tabulka níže zobrazuje ty nejpoužívanější, tedy ty s nejvyšším počtem aktivních uživatelů za měsíc.

Obrázek 2: Seznam dostupných sociálních sítí[19]

Pořadí	Sociální síť	Počet uživatelů měsíčně (v tisících)	Země původu
1	Facebook	2 603 000	USA
2	WhatsApp	2 000 000	USA
3	YouTube	2 000 000	USA
4	Messenger	1 300 000	USA
5	WeChat	1 203 000	Čína
6	Instagram	1 082 000	USA
7	TikTok	800 000	Čína
8	QQ	694 000	Čína
9	Weibo	550 000	Čína
10	Qzone	517 000	Čína
11	Reddit	430 000	USA
12	Telegram	400 000	Rusko
13	Snapchat	397 000	USA
14	Pinterest	367 000	USA
15	Twitter	326 000	USA
16	LinkedIn	310 000	USA
17	Viber	260 000	Japonsko
18	Line	187 000	Japonsko
19	YY	157 000	Čína
20	Twich	140 000	USA
21	Vkontakte	100 000	Rusko

[17] ŠVARCOVÁ A. *Než přišel Facebook.* In: kvalitni-internet.cz [online]. 2017. [cit. 2023-12-08]. Dostupné z https://www.kvalitni-internet.cz/nez-prisel-facebook-strucny-pruvodce-historii-socialnich-siti.
[18] Tamtéž.
[19] Sociální sítě. In: Sitevhrsti.cz [online]. [cit. 2023-11-25]. Dostupné z: https://sitevhrsti.cz/socialni-site/.

Sociální sítě přináší tedy mnoho pozitiv, ale současně i některá negativa. Mohou být zneužity k šíření různého nelegálního obsahu, a to včetně dětské pornografie. Tento nelegální obsah může být nahrán, sdílen a šířen bez vědomí nebo souhlasu oběti. Pachatelé mohou využívat dětskou pornografii k vydírání a manipulaci s oběťmi, což může vést k vážným psychickým a emocionálním důsledkům. K navazování kontaktů s obětmi využívají falešné nebo upravené identity a uživatelské profily.

Závažným problémem je navazování kontaktů s dětmi tzv. dětský grooming a mladistvými a následné možné zneužití dítěte k výrobě pornografie. Navazování kontaktů mívá několik fází, které jsou uvedeny v následujících podkapitolách.

2.6 Dětský grooming

Dětský grooming je termín používaný k popisu manipulativního chování dospělé osoby směrem k dítěti s cílem vytvořit důvěrný vztah, který může vést k sexuálnímu zneužívání. Tento termín se obvykle vztahuje na situace, kdy dospělá osoba systematicky buduje vztah s dítětem s úmyslem získat jeho důvěru, často za účelem následného sexuálního zneužívání. Podle Pavlovského *„Většinu sexuálních deliktů páchají lidé, kteří nejsou postiženi poruchou sexuální preference.“*[20] Tedy hlavně kyberprostor, nejčastěji sociální síť, poskytuje těmto lidem neomezený prostředek a prostor pro navazování kontaktů s dětmi a tuto aktivitu a případnou trestnou činnost páchá daleko více lidí, než by bylo možné bez internetu a současných technologií. V trestním zákoně je uveden § 193b navazování nedovolených kontaktů s dítětem. Toto ustanovení je reakcí na jednání pachatelů v kyberprostoru, včetně sociálních sítí.[21]

2.7 Kybergrooming

Termín "kybergrooming" označuje situace, kdy dospělá osoba využívá internet a digitální technologie k budování vztahu s dítětem s úmyslem sexuálního zneužívání. Je to moderní varianta tradičního dětského groomingu, který využívá online komunikaci a různé platformy.

Oběťmi kybergroomingu jsou tedy zpravidla děti a mladiství, přičemž častěji se jedná o dívky než o chlapce. Lze předpokládat, že oběti tvoří zejména ti uživatelé

[20] PAVLOVSKÝ, P. a kol. *Soudní psychiatrie a psychologie*, Praha: Grada, 2004. ISBN 978-80-247-4332-5. s. 188.
[21] SMEJKAL, V. *Kybernetická kriminalita.* 3. rozšířené a aktualizované vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. ISBN 978-80-7380-849-5. s. 219.

internetu, kteří tráví velké množství volného času v online komunikačních prostředích (chat, instant messengery), kde také navazují virtuální kontakty s ostatními (hledají zde kamarády, přátele, životní partnery). Sociální sítě díky propracovanému systému virtuálních sociálních vazeb poskytují ideální podmínky pro realizaci kybergroomingu, ale lze využít i různá diskuzní fóra, chatovací místnosti, online hry a další.[22]

Podobně jako v případě tradičního groomingu se kybergrooming může projevovat různými způsoby například lichotkami, budováním důvěry, sdílením osobních informací a postupným přesvědčováním dítěte, aby se účastnilo nevhodných online aktivit. Tyto aktivity můžou zahrnovat i vytváření fotografií nebo videí s pornografickou tématikou.[23]

Pachatelé kybergromingu cíleně vyhledávají kontakty s dětmi a pomalým plánovaným a strategickým postupem budují vztah důvěry, používají příkazy mlčení, tedy aby se oběť nikomu nesvěřovala, a po nějakém časem konverzace a výměně pornografického materiálu, oběť vydírají nebo se jí snaží namluvit, že je to pouze její vina.[24]

2.7.1 Prvotní navázání kontaktu

Je to první fáze, kdy útočník navazuje kontakt s dítětem, který obvykle zahájí například obyčejnou větou: *„Ahoj, jak se máš?“* nebo pod legendou, že zprávu odeslal omylem. Zpravidla vystupuje pod identitou stejného pohlaví a věku blízkému oběti, k čemuž má uzpůsobený profil na sociální síti. Má tedy například profilové a další fotografie dítěte, které lze volně stáhnout z internetu. Upravuje si svou identitu dle potřeby a může vystupovat pod několika přezdívkami a profily. Účelově si ve svých profilech přizpůsobuje věk, záliby, zájmy a další osobní údaje, aby mohl vybranou oběť co nejefektivněji oslovit. Jako jednoduchý příklad lze uvést, že si útočník zjistí z profilu oběti zálibu v jezdectví a že má velmi vřelý vztah ke zvířatům, ke koním (na profilu nalezne mnoho fotografií) a začne tedy cíleně s komunikací na toto téma.[25]

[22] KOPECKÝ, K. @ E-Bezpečí. *Kybergrooming.* In: kybergrooming.cz [online]. 2007-2021. [cit. 2023-11-30]. Dostupné z https://www.kybergrooming.cz.
[23] Tamtéž.
[24] MILFAIT, R. *Komerční sexualizované násilí na dětech*. Portál 2008. ISBN 978-80-763-7320-8. s 102.
[25] KOPECKÝ, K. @ E-Bezpečí. *Kybergrooming.* In: kybergrooming.cz [online]. 2007-2021. [cit. 2023-11-30]. Dostupné z https://www.kybergrooming.cz.

2.7.2 Ověření věku oběti

Při vzájemné komunikaci prostřednictvím sociálních sítí si nikdy nemůžeme býti jisti, s kým ve skutečnosti komunikujeme. Tedy i útočník si chce ověřit, že opravdu komunikuje s dítětem a jeho potencionální obětí. Po dítěti požaduje další a další aktuální fotografie, videa nebo případně online videohovory. Kromě osobních údajů, jako je jméno a věk, se útočník snaží zjistit další informace – například školu, kterou dítě navštěvuje, oblíbené herce, zpěváky, celebrity, zájmy, záliby a další údaje. Z těchto údajů si pak sestaví obecný profil oběti a snáze se mu prvotní kontakt navazuje.

2.7.3 Stupňování intimity

Intimita fotografií, které si navzájem oběť s útočníkem vyměňují, se zvyšuje a stupňuje. Fotografie zachycující obličej dítěte, přecházejí na fotografie celé postavy, přičemž pachatel postupně žádá fotografie s čím dál více odhaleným tělem nebo fotografie a videa v různých erotických polohách. V krajním případě může dítě zaslat pornografický materiál, kde je zcela odhalené nebo s detaily svých pohlavních orgánů. Obdobné fotografie zasílá útočník oběti, přičemž se většinou jedná o fotografie jeho přirození, případně je vyobrazen, jak masturbuje. Toto jednání je velmi nebezpečné, neboť dítě může napodobovat chování útočníka. V případě, že dítě odmítne dále posílat pornografický materiál, může ze strany pachatele docházet k následnému vydírání pod pohrůžkou, že již zaslané materiály zveřejní na internetu, poskytne je přátelům na sociálních sítích nebo rodičům dítěte.[26] Mnoho dětí těmto výhrůžkám nedokáže vzdorovat a raději se na případnou požadovanou osobní schůzku dostaví, než aby byly vystaveny ponížení a riziku kyberšikany ze strany svého okolí.

2.7.4 Vydírání oběti

V trestním zákoně takový trestný čin nalezneme v § 175. „*Kdo jiného násilím, pohrůžkou násilí nebo pohrůžkou jiné těžké újmy nutí, aby něco konal, opominul nebo trpěl.*“[27] Tedy pachatel může oběti vyhrožovat zveřejněním již zaslaných a získaných fotografií nebo videí a oběť tak vydírat. Pachatel na sociálních sítích využívá svou

[26] ECKERTOVÁ, L., DOČEKAL D. *Bezpečnost dětí na internetu.* Computer press 2013. ISBN 978-80-251-3804-5. s. 84-87.
[27] ČESKO. Zákon č. 40/2009 Sb., *trestní zákon, ve znění pozdějších předpisů*, § 175 odst. 1. In: Zákony pro lidi [online]. Praha: ©AION CS, 2010–2023 [cit. 2023-12-11]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40.

anonymitu a téměř neomezené možnosti z hlediska časového a v počtu útoků, což by u klasického vydírání nebylo možné.

Obecně lze k vydírání přiřadit i trestný čin sexuální nátlak dle § 186 trestního zákona, kde je v tomto ustanovení popsána svoboda rozhodování v pohlavních vztazích. Důsledek tohoto trestného činu může mít nepříznivý vliv na mravní vývoj dítěte. A pokud dojde k situaci, že se pachateli podaří svým konáním a nátlakem na dítě získat pornografický materiál, lze takové jednání dále kvalifikovat i jako trestný čin výroby a jiného nakládání s dětskou pornografií dle § 192 trestního zákona, případně zneužití dítěte k výrobě pornografie dle § 193 trestního zákona.

2.8 Sexting

Sexting je termín, který vznikl spojením slov "sex" a "texting“. Označuje tedy praktiku posílání sexuálně orientovaných zpráv, obrázků nebo videí prostřednictvím mobilních zařízení nebo internetu, nejčastěji přes sociální sítě.[28] Tato forma komunikace může být používána mezi partnery nebo jednotlivci k vyjádření intimních nebo sexuálních pocitů.

Je důležité mít na vědomí, že sexting může přinést různé právní a etické otázky, zejména pokud jsou účastníci nezletilí. Mnoho jurisdikcí má zákony, které regulují sexting mezi dospělými a nezletilými a v některých případech může být sexting považován za nelegální chování, zejména pokud zahrnuje nezletilé osoby nebo je šířen bez jejich souhlasu. Je tedy důležité býti obezřetní a respektovat soukromí a souhlas v jakémkoliv druhu sexuální komunikace.

Současná generace dětí prostřednictvím vzájemně zaslaných fotografií s pornografickou tématikou hledá, zkoumá a vyjadřuje svou sexualitu v kyberprostoru a považuje toto jednání za zcela běžné a normální. Většina si bohužel neuvědomuje rizika a nebezpečí následného zneužití zaslaných osobních a sexuálně explicitních materiálů.[29] Obětí poskytnuté materiály mohou být zneužity k různým formám kybernetických útoků, jako jsou například kyberšikana, manipulace s obětí, již zmiňované vydírání a další. Citlivý materiál může být v kyberprostoru dostupný neomezeně dlouhou dobu a jeho

[28] ECKERTOVÁ, L., DOČEKAL D. *Bezpečnost dětí na internetu.* Computer press 2013. ISBN 978-80-251-3804-5. s. 68.
[29] HOLLÁ, K. *Sexting a kyberšikana.* 1. vydání. IRIS 2016. ISBN 978-80-8153-061-6. s. 58.

odstranění je velmi problematické, ne-li nereálné.[30] Důsledky sextingu mohou být v některých případech až tragické, neboť nátlak na oběť může skončit psychickými problémy, sebepoškozováním nebo sebevraždou. A je tedy oprávněně považován za velmi rizikový.[31]

2.9 Kyberšikana

Slovo "šikana" je odvozeno od francouzského pojmu "chicané" a je chápáno jako psychické a fyzické týrání, pronásledování, zlomyslné obtěžování, útisk apod.[32]

Slovo kyberšikana, jak už název napovídá, je šikana probíhající v kyberprostoru prostřednictvím informačních a komunikačních technologií (například pomocí mobilních telefonů, počítačů nebo služeb v rámci internetu), jež mají za následek ublížení nebo jiné poškození oběti.[33] Definice kyberšikany vychází z definice tradiční šikany, která se odehrává v reálném světě, kdežto kyberšikana ve světě virtuálním, ale oba tyto jevy se vyznačují stejným základem:

- jedná se o úmyslně agresivní akt s cílem oběť zranit (ať už fyzicky, nebo psychicky)
- útoky na oběť jsou opakované a probíhají delší dobu
- oběť se nedokáže útokům účinně bránit (mezi agresorem a obětí existuje mocenská nerovnováha)[34]

Může se samozřejmě jednat i o nedorozumění mezi obětí a útočníkem, například nevhodný vtip, a tím nedomyšlené důsledky jednání ze strany útočníka.

V případě kyberšikany se definice rozšiřují o aspekt prostředí, ve kterém útoky probíhají a kterým je již zmíněný kyberprostor. Jak uvedené body napovídají, kyberšikana je skutečně závažným jevem, jenž je pro oběť velmi nepříjemný, neboť jí je dlouhodobě cíleně ubližováno a sama se s danou situací nedokáže vypořádat a útoky zastavit. Takové oběti se pak potýkají s mnoha negativními důsledky od sníženého

[30] KOPECKÝ, K. a kol. *Rizikové chování českých a slovenských dětí v prostředí internetu*. Olomouc, 2015. ISBN 978-80-244-4861-9. s. 44.
[31] KOŽÍŠEK, M., PÍSECKÝ V. *Bezpečně na internetu: průvodce chováním ve světě online.* Praha, 2016. ISBN 978-80-247-5595-3. s. 83.
[32] VANÍČKOVÁ, E. *Cesta za poznáním šikany, šikanování mezi dětmi.* Praha: Česká společnost na ochranu dětí - Růžová linka, 2002. ISBN 80-238-9448-X. s. 3.
[33] MULLER, M. *Jak chránit děti před pornografií na internetu*, 1. vyd. 2014. ISBN 978-80-262-0694-1. s 101.
[34] KOPECKÝ, K. a kol. *Rizikové chování českých a slovenských dětí v prostředí internetu*. 2015. ISBN 978-80-244-4861-9. s. 11.

sebevědomí, pocitů bezmocnosti, strachu, deprese, přes somatické potíže (například nechutenství), až po problémy v osobních vztazích a zhoršeným prospěchem ve škole. Zatímco u tradiční šikany lze odhadnout, kdy a kde k útoku dojde (nejčastěji ve škole), s kyberšikanou je možné se setkat v kybeprostoru kdekoliv a kdykoliv.[35]

V trestním zákoně ani v jiném zákoně není šikana sama o sobě definována jako trestný čin nebo přestupek, přesto šikana může svým charakterem naplňovat znaky některého z přestupků či trestných činů. Ve smyslu zákona č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže je trestně odpovědnou osobou osoba starší 15 let, která je dostatečně rozumově a mravně vyspělá. Protiprávní jednání s prvky šikany může být kvalifikováno jako přestupek dle zákona č. 251/2016 Sb., zákon o některých přestupcích. Nejčastěji se bude jednat o přestupky proti občanskému soužití, ublížení na cti, vyhrožování újmou na zdraví a další. Za přestupek je odpovědná osoba starší 15 let. V oblasti školské legislativy jsou základní informace obsaženy například v metodickém pokynu ministryně školství mládeže a tělovýchovy k prevenci a řešení šikany ve školách a školských zařízeních (č. j. MŠMT – 21149/2016.) Vzhledem k absenci statistik mezi jednotlivými evropskými státy je předpoklad, že výskyt kyberšikany v České republice bude s ostatními státy srovnatelný.[36]

2.10 Umělá inteligence

Umělá inteligence (dále AI) je v posledních letech velmi diskutovaným tématem a zažívá velký rozvoj. Systémy umělé inteligence dnes již zcela běžně nahrazují člověka v celé řadě úkolů a úloh.[37]

Jedná se o obor informatiky, který se zabývá vývojem počítačových systémů schopných provádět úkoly, které by obvykle vyžadovaly lidskou inteligenci. Tento obor zahrnuje různé techniky a metody, včetně strojového učení, hlubokého učení, přirozeného zpracování jazyka a dalších.[38]

Umělá inteligence přináší i svá rizika a může být využita i k vytváření pornografického obsahu. Jednou z technik v tomto směru je využívání generativních

[35] ECKERTOVÁ, L., DOČEKAL D. *Bezpečnost dětí na internetu.* Computer press 2013. 224 s. ISBN 978-80-251-3804-5. s. 64.
[36] CHROMÝ, J. *Kriminalita páchaná na mládeži*. Linde s.r.o. 2010. ISBN 978-80-7201-825-3. s. 46.
[37] CAHLÍK, V., JINDRA, V. *Co je vlastně umělá inteligence.* In: aidetem.cz [online]. 2022. [cit. 2023-12-10]. Dostupné z https://aidetem.cz/obecny-uvod-do-umele-inteligence/co-to-vlastne-je-ai/.
[38] Tamtéž.

modelů, jako jsou generativní konvoluční sítě (GAN). Tyto modely mohou generovat realistické obrázky a videa, včetně pornografického obsahu s vysokým stupněm detailu a přesvědčivosti a tento obsah může být poté snadno šířen přes sociální sítě.

Vytvoření pornografického obsahu zahrnující děti je možné generovat pomocí na internetu volně dostupných nástrojů umělé inteligence. Tvorba tohoto obsahu je tedy velmi snadná, nebezpečná a i pro experta je následně velmi obtížné rozpoznat, zda se jedná o autentickou fotografii nebo produkt softwaru využívajícího umělou inteligenci.[39]

2.10.1 Praktická ukázka

Pro názornou ukázku bylo v rámci této bakalářské práce provedeno vygenerování fotografie s dítětem pomocí umělé inteligence. K tomuto účelu byl použit nástroj gencraft veřejně dostupný na internetovém odkaze https://gencraft.com. Jako klíčové slovo pro vygenerování fotografie bylo zvoleno slovo “children“. Uvedený nástroj je zcela zdarma a vygenerování fotografie trvalo pouze několik vteřin. Na tomto příkladu je zřejmé, jak snadno lze vytvořit fotografie fiktivních osob a v případě kombinace s jinými nástroji, různými placenými verzemi a dále například softwaru dostupného na darknetu, je možné vytvářet i materiály s pornografickou tématikou. Tedy i dětskou pornografii.

Obrázek 3: Fotografie dítěte vytvořená umělou inteligencí[40]

[39] KOPECKÝ, K. *Umělou inteligencí generovaná pornografie způsobí řadu problémů, zneužívána bude k útokům na děti i dospělé.* E-Bezpečí, roč. 8, č. 2, s. 39-42. Olomouc: Univerzita Palackého, 2023. ISSN 2571-1679. Dostupné z: https://www.e-bezpeci.cz/index.php?view=article&id=3636.

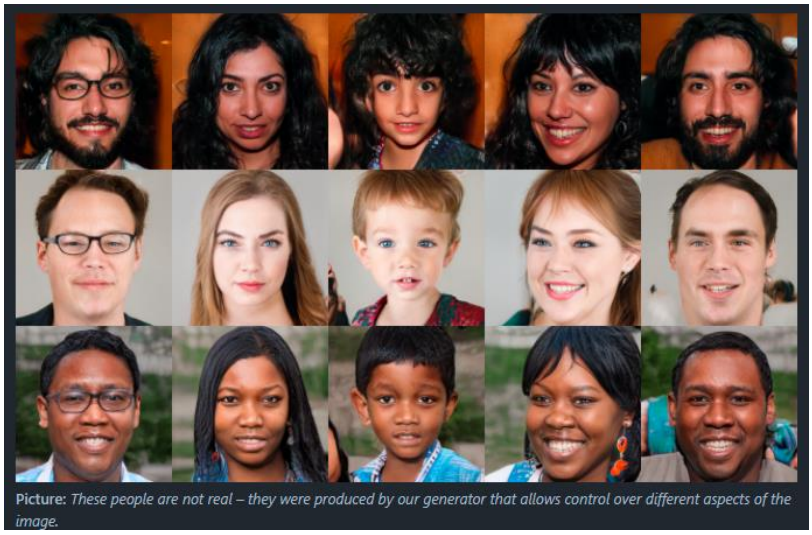
[40] Vlastní tvorba za pomocí umělé inteligence. Generováno nástrojem gencraft. Dostupný na odkaze: https://gencraft.com.

2.10.2 Deepfake

K tématu umělé inteligence je nutné zmínit i fenomén deepfake. Deepfake je termín, který označuje uměle vytvořená média, zejména videa, která jsou vytvořena nebo upravena pomocí pokročilých technik hlubokého učení tzv. neuronových sítí, zejména pomocí již zmiňovaných GAN. Tyto techniky umožňují vytvářet velmi realistické a přesvědčivé falzifikáty, za užití reálných materiálů, které poté mohou obsahovat například modifikované tváře nebo hlasy lidí.

Hlavními aplikacemi deepfake technologií je vytváření videí, kde jsou obličeje jedné osoby nahrazeny obličejem jiné, nebo modifikace pohybu rtů a obličejových výrazů takovým způsobem, aby odpovídaly novým obsahům. To může mít různé důsledky, od humoristických úprav a vytváření uměleckých děl, po potenciálně nebezpečné zneužití pro vytváření falešných zpráv, šíření dezinformací nebo napodobování politických či veřejných postav v manipulativních situacích nebo v pornografii.

Obrázek 4: Nereální lidé vytvoření umělou inteligencí systémem StyleGAN[41]



Deepfake videa se v oblasti pornografie objevují nejčastěji a s rozvojem neuronových sítí se jejich kvalita neustále zvyšuje. S dostupností různých aplikací se tato technologie rozšířila i mezi laiky a upravená videa jsou z tohoto důvodu v kyberprostoru snadněji dostupná.[42]

[41] WALIA, M. S. In: Analyticsvidhya.com [online]. 2021. @ Analytics Vidhya 2023. [cit. 2023-12-15]. Dostupné z https://editor.analyticsvidhya.com/uploads/89435Screenshot%20(70).png.
[42] KOPECKÝ, Kamil. *Deep fake – stručný úvod do problematiky*. E-Bezpečí, roč. 4, č. 1, s. 23-25. Olomouc: Univerzita Palackého, 2019. ISSN 2571-1679. Dostupné z: https://www.e-bezpeci.cz/index.php?view=article&id=1417.

Vážným problémem tedy může být narušení soukromí osob. Kdokoli může použít fotografie nebo videa, která jsou dostupná například na sociální síti a vytvoří z nich fotografie nebo videa kompromitující a dále je šířit kyberprostorem a tím poškodit pověst dané osoby.[43]

Celkově vzato, fenomén AI má obrovský dopad na naši společnost a každodenní život. Zatímco přináší řadu výhod, zároveň před námi klade i výzvy, které vyžadují odpovídající pozornost a regulaci. Je tedy nezbytné, aby se státy a mezinárodní organizace zaměřili na kontrolu technologií generativní umělé inteligence, které umožňují vytváření nelegálního obsahu. Tedy zavedení přísnějších zákonů týkajících se uměle generované pornografie, vytváření standardů pro softwarové nástroje, které generují takový obsah, a podporu výzkumu technologií pro rozpoznání a odhalení deepfake obsahu. Nesmíme také zapomenout na osvětu, prevenci a systematické vzdělávání všech, tedy dětí i dospělých.[44]

[43] KOPECKÝ, Kamil. *Umělou inteligencí generovaná pornografie způsobí řadu problémů, zneužívána bude k útokům na děti i dospělé.* E-Bezpečí, roč. 8, č. 2, s. 39-42. Olomouc: Univerzita Palackého, 2023. ISSN 2571-1679. Dostupné z: https://www.e-bezpeci.cz/index.php?view=article&id=3636.

[44] KOPECKÝ, Kamil. *Umělou inteligencí generovaná pornografie způsobí řadu problémů, zneužívána bude k útokům na děti i dospělé.* E-Bezpečí, roč. 8, č. 2, s. 39-42. Olomouc: Univerzita Palackého, 2023. ISSN 2571-1679. Dostupné z: https://www.e-bezpeci.cz/index.php?view=article&id=3636.

3 Dostupnost dětské pornografie v kyberprostoru

Dnešní technologická infrastruktura umožnuje rychlý a snadný přístup k různým informacím na internetu. Internet je tedy nejtypičtější představitel celého kyberprostoru a je v současné době nejběžněji využívanou informační technologií.[45] S tím jsou spojena i závažná rizika, jako je například snadná dostupnost dětské pornografie. Česká republika nijak zásadně neomezuje přístup k internetové síti a pornografie je tedy běžně dostupná na surface a deep webu, kde lze nalézt i pornografii dětskou, šířenou mezi uživateli sociálních sítí, emailových schránek a za pomocí dalších komunikačních služeb. Vyhledávání pornografického obsahu může být usnadněno také používáním tzv. hashtagů a klíčových slov, což umožňuje i jeho rychlé šíření.

Důležité je také zmínit, že sami děti mohou vytvářet pornografii, fotit se, natáčet a sdílet tento obsah v rámci svých vztahů a mezi přáteli prostřednictvím sociálních sítí a neuvědomovat si rizika následného dalšího šíření a to bez jejich vědomí a souhlasu.

3.1 Dostupnost pornografie na sociálních sítích

Jak již bylo v této práci zmíněno, součástí internetu jsou i sociální sítě. Jejich počet není možné přesně určit, neboť jejich dynamický vývoj je velmi rychlý, jsou vytvářeny nové, některé zanikají nebo jsou měněny jejich názvy. Sociálními sítěmi je možné nazvat cokoliv, kde dochází k výměně informací mezi uživateli ve virtuálním prostředí. Slouží k tomu různé aplikace a software nainstalovaný do mobilních telefonů, počítačů a dalších IT zařízení. V současné době, plné moderních technologií, bychom velmi těžko hledali někoho, kdo nevlastní mobilní telefon nebo jiné zařízení, který umožňuje přístup do internetové sítě. Společnosti, které sociální sítě provozují, ve většině případů neověřují identitu a věk uživatele, mají pouze doporučenou věkovou hranici pro registraci, kterou lze snadno uvést jako smyšlenou, fiktivní. Registrovat se tedy může prakticky kdokoliv a případná kontrola a regulace je velmi složitá. Uživatelé mohou snadno sdílet soukromé obsahy přes zprávy a různé uzavřené skupiny, což ztěžuje kontrolu obsahu ze strany daných společností, které konkrétní platformy provozují a spravují.[46]

[45] KUCHTA, J., VÁLKOVÁ, H. a kol. *Základy kriminologie a trestní politiky*. 1. vydání. Praha: C. H . Beck, 2005. ISBN 978-80-7400-429-2. s. 614.
[46] KOPECKÝ, K. a kol. *Rizikové chování českých a slovenských dětí v prostředí internetu*. 2015. ISBN 978-80-244-4861-9. s. 47-48.

Sociální sítě a online platformy samozřejmě používají různé filtry a mechanismy, které mají za cíl vyhledávat, blokovat nebo omezovat šíření pornografického obsahu. Tyto mechanismy mohou zahrnovat automatické rozpoznávání závadového pornografického materiálu ve formě obrázků, videí ale i textu nebo popisu médií. Nicméně, žádný systém není naprosto dokonalý a může dojít k úniku obsahu, který porušuje stanovená pravidla konkrétní sociální sítě.

Je velmi důležité, aby uživatelé sítí byli obezřetní, neporušovali daná pravidla a rodiče by měli využívat dostupné nástroje pro řízení, monitoring a filtrování obsahu na sociálních sítích, aby své děti ochránili.

3.2 Pornografie mezi dětmi a mladistvými a její rizika

Dostupnost pornografie na internetu je v současné době výrazným tématem diskuze v rámci společnosti a vědeckého výzkumu. Hlavními aspekty tohoto tématu jsou:

- vliv dostupnosti pornografie na děti a mladistvé
- dopady na individuální chování a psychiku
- regulace a etika
- prevence a výchova
- důsledky na mezilidské vztahy

Souhrnně tedy zkoumání vlivu snadné dostupnosti pornografie na společnost, konkrétně na děti a mladistvé, včetně sociálních a morálních aspektů. Analýza toho, jak pornografie ovlivňuje individuální chování jednotlivce, jeho sexuální preference a psychické zdraví. Zhodnocení stávajících opatření k regulaci pornografie na internetu a zkoumání etických otázek s omezením nebo cenzurou tohoto obsahu. Výzkum možných opatření a programů zaměřených na prevenci nežádoucích dopadů pornografie, zejména u mladých lidí. A v neposlední řadě analýza, jak dostupnost pornografie může ovlivnit mezilidské vztahy a sexuální výchovu.

Děti mohou v obrazech pornografie spatřit vzory mužské a ženské erotiky, které vzhledem k absenci vlastní zkušenosti mohou vnímat jako realitu. U mladistvých může pornografie sloužit k poznání intimity dospělých. Vznik závislosti na pornografii představuje významné riziko, kdy od raného věku dochází k vyhledávání online pornografie a postupnému zvyšování potřeby neobvyklých a drsnějších forem obsahu.

Pokud se dítě setká s pornografií, je vhodné, aby bylo informováno a poučeno o jejím obsahu a vyvarovalo se násilným formám.[47]

3.3 Viktimologie

Viktimologie je multidisciplinární obor zabývající se oběťmi trestných činů, jejich reakcemi na trestné činy a interakcemi mezi oběťmi a pachateli a s problematikou mravnostní trestné činnosti úzce souvisí. Tento obor zkoumá fyzické, psychické, sociální a ekonomické dopady trestných činů na oběti a jejich rodiny, stejně jako mechanismy, které mohou vést k těmto situacím. Zahrnuje dále studium různých aspektů jako je prevence kriminality, poskytování pomoci obětem, soudní jednání, rehabilitace obětí a vědecké výzkumy. Tento obor spolupracuje s různými disciplínami, včetně kriminologie, sociologie, psychologie a trestního práva. Cílem viktimologie je zlepšit porozumění obětem trestných činů a poskytnout jim adekvátní podporu a ochranu.[48]

Z pohledu viktimologie, v případech mravnostního charakteru zaměřených na děti a mladistvé v kyberprostoru, je nutné zmínit, že u následné viktimizace, tedy procesu poškozování a způsobování újmy konkrétnímu jedinci, který se stal obětí trestného činu,[49] jsou přítomny všechny její fáze.

- primární
- sekundární
- terciální

Primární fáze je samotný útok na oběť prostřednictvím internetu, sociálních sítí a dalších. Tato fáze může být dlouhodobá a snadno vyústí až k vydírání nebo fyzickému kontaktu a sexuálnímu zneužití oběti.

Sekundární fáze je proces vyšetřování OČTŘ, výslechy obětí a případně i hlavní líčení před soudem. Na děti může mít toto velmi negativní vliv a může prohlubovat újmu, která jim byla způsobena a narušit jejich sociální vztahy s blízkými.

Terciální fáze je dlouhodobý dopad na oběť, kde je nutné si uvědomit, že v rámci kyberprostoru mohou být závadové fotografie oběti nebo jiné explicitní materiály dále šířeny, nelze je již nikdy odstranit a situace se tedy může kdykoliv opakovat. Toto

[47] WEISS, P. a kol. *Sexuologie.* 1. vydání. Grada: 2010. ISBN 978-80-2472-492-8. s. 575.
[48] VELIKOVSKÁ, M. *Psychologie obětí trestných činů.* 1. vydání. Grada: 2016. s. 9-14.
[49] VELIKOVSKÁ, M. *Psychologie obětí trestných činů.* 1. vydání. Grada: 2016. s. 53.

uvědomění si, může v budoucnu oběť v jisté míře omezovat a může mít i neustálý strach z dalších útoků. Terciální fázi lze tedy v těchto případech označit jako nejrizikovější.

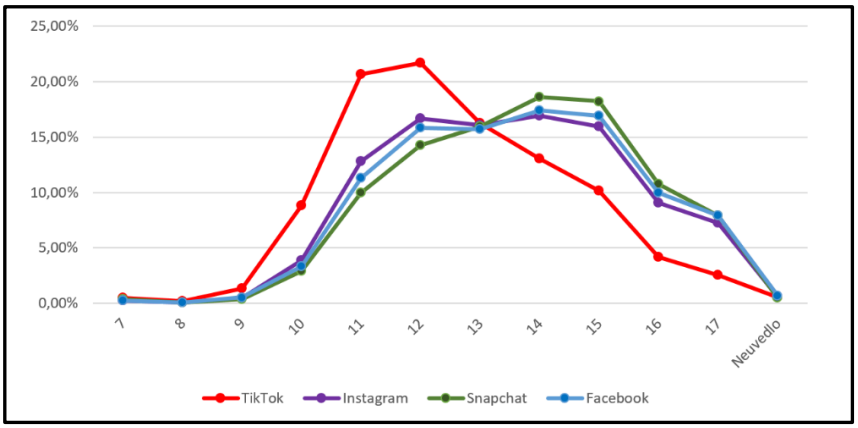
4 Ochrana dětí a mladistvých, prevence

České děti a mladiství masivně využívají sociální sítě. Následující kapitola je věnována ochraně dětí a mladistvých ze strany rodičů, školy a dalších zainteresovaných institucí.

4.1 Soukromí a bezpečnost dětí na sociálních sítích

Podle výzkumu „České děti v kybersvětě“ projektu E-Bezpečí v užívání sociálních sítí dominovala do roku 2015 sociální síť facebook, kterou používalo 80–90 procent dětí. I přes smluvní podmínky sociální sítě facebook, ve kterých je mimo jiné uvedeno, že tuto síť může používat pouze osoba starší 13 let, bylo výzkumem zjištěno, že až 59 procent dětí bylo ve věku 7–12 let. Tedy ochrana a kontrola ze strany rodičů zcela selhala. Bohužel ze strany tvůrců jednotlivých sociálních sítí není věk uživatelů nijak ověřován a účty lze registrovat pod smyšlenými údaji. V současné době je mezi dětmi a mladistvými nejvíce rozšířena sociální síť TikTok, přičemž nejvíce uživatelů tvoří věková skupina 10–12 let.[50]

Graf 2: Věkové rozložení dětských uživatelů u dominantních sociálních sítí[51]



4.1.1 Role rodičů

Prostředí internetové sítě a sociálních sítí může být pro děti a mladistvé velmi dobrým pomocníkem ke zjišťování různých informací, ale skrývá také mnoho nebezpečí a nástrah.[52]

[50] KOPECKÝ, K., SZOTKOWSKI, R. *České děti v kybersvětě (výzkumná zpráva)*. O2 Czech Republic & Univerzita Palackého v Olomouci, 2019. s 27.
[51] KOPECKÝ, K., SZOTKOWSKI, R. *České děti v kybersvětě (výzkumná zpráva)*. O2 Czech Republic & Univerzita Palackého v Olomouci, 2019. s 10.
[52] KOPECKÝ, K., SZOTKOWSKI, R. *České děti v kybersvětě (výzkumná zpráva)*. O2 Czech Republic & Univerzita Palackého v Olomouci, 2019. s 4.

„*Základními negativními rysy internetového prostředí je možnost nepřirozeného úniku do světa fantazie počítačových her, virtuálních lákadel a online efekt ztráty zábran, neboli princip disinhibice na internetu*.“[53] Proto je velmi důležité, aby si rodiče byli těchto hrozeb vědomi a u dětí již od útlého věku budovali určitou obezřetnost a zodpovědnost. Poučili je a vysvětlili jim případná rizika, týkající se hlavně sdílení různých materiálů na sociálních sítích, anonymity internetu, kontaktů s cizími osobami a nebezpečí šíření a výroby dětské pornografie. Z počátku by měli užívání internetu uskutečňovat pouze jako společnou rodinnou aktivitu a později, až se dítě osamostatní, nastavit určitá pravidla a limity. Tedy aby dítě trávilo na internetu pouze určitý daný čas.[54]

Diskuze o tom, zda dětem povolit užívání informačních technologií v kombinaci s internetem a sociálními sítěmi, není jednoduchá. Automaticky k této věci přistupovat negativně jako k něčemu špatnému nebo zakázanému by nebylo rozumné. Dítě by mohlo být “pozadu“ vůči ostatním vrstevníkům a snadněji se tak stát obětí šikany nebo kyberšikany.[55] Zvláště u starších dětí jsou zákazy kontraproduktivní a dítě spíše podnítí k užívání něčeho zakázaného “tajně“ a rodič tedy v danou chvíli ztrácí kontrolu nad tím, co vše dítě v online prostředí dělá.

Naopak Dočekal je názoru, že by rodiče měli podporovat své děti, které si chtějí splnit své “kybersny“. Jejich přání stát se youtuberem, influencerem apod., pro ně může být dobrá příležitost naučit se novým dovednostem jako je například natáčení, střihu videí, tančení, zpívání, komunikační dovednosti a další. A i kdyby se jim nepodařilo stát se slavnými, může to zvýšit jejich sebevědomí a je tedy žádoucí je v tomto podporovat.[56]

Ač zde hovoříme o poučení dětí ze strany rodičů, tak paradoxně mohou být problémem i samotní rodiče. Mnohdy činí jen ze zvyku, že sami zveřejňují fotky a videa svých dětí v příspěvcích na sociálních sítích, aniž by přemýšleli nad tím, zda by s tím dítě souhlasilo a zda to nevytváří určité riziko do budoucnosti. Je nutné si uvědomit, že zveřejňování různého obsahu na internetu je věc trvalá, tedy něco, co se již nedá odstranit. Ve velmi krátké době může být obsah sdílen, zkopírován a uložen na mnoha dalších

[53] KRČMÁŘOVÁ, B. *Děti a online rizika: sborník sudií.* 1. vyd. Praha. Sdružení linka bezpečí, 2012. ISBN 978-80-904920-2-8. s. 54.
[54] ECKERTOVÁ, L., DOČEKAL D. *Bezpečnost dětí na internetu.* Computer press 2013. ISBN 978-80-251-3804-5. s. 48.
[55] ŠEVČÍKOVÁ A., BLINKA L. a kol. *Děti a dospívající online.* 1. vyd. Grada 2014. ISBN 978-80-247-5010-1. s. 120-121.
[56] DOČEKAL, D. a kol. *Dítě v síti.* Mladá fronta 2019. ISBN 978-80-204-5145-3. s. 59.

místech internetové sítě. Změny jsou již nevratné a docílit úplného odstranění zveřejněného obsahu není technicky ani časově možné.[57]

Závažnou chybou je tedy zveřejňování fotografií a dalšího obsahu samotnými rodiči, kde jsou zachyceny nahé děti, i když se na první pohled nejedná o nic závažného, co by mohlo být považováno jako dětská pornografie. Může jít o zcela "nevinné" fotografie z dovolené u moře nebo obyčejné koupání v bazénu na vlastní zahradě.

4.1.2 Role škol a Policie ČR

Školní instituce se rovněž mohou podílet na snižování rizika užívání internetu a sociálních sítích, a to i v situacích, že k tomu ve většině případů nedochází ve škole samotné. Podobně jako u rodičů je i zde žádoucí, aby byly děti o tomto problému informovány a s přihlédnutím k jejich věku i náležitě poučeny. Ať již v rámci výuky předmětů zaměřených na informační technologie, tak i v rámci jiných předmětů, které s danou problematikou mohou souviset, jako je například občanská nauka.

Další možností ředitelů a pracovníků škol je kontaktovat například oddělení tisku a prevence Policie ČR a společně realizovat různé přednášky nebo preventivní programy na toto téma. Na těchto odděleních jsou vyškolení policisté a občanští zaměstnanci, kteří mohou dětem a mladistvým předat mnoho důležitých informací a poznatků z dané problematiky. Žáci by měli také vědět, že mají právo kdykoliv se na někoho důvěryhodného obrátit, neboť hledání podpory a případné pomoci u dospělých je jedním z účinných způsobů prevence.

4.1.3 OSPOD a další instituce

Orgán sociálně-první ochrany dětí (dále OSPOD) je v České republice každý ze státních orgánů, který má na základě zákona č. 359/1999 Sb., o sociálně-právní ochraně dětí, toto postavení přidělené. Tento orgán má mimo jiné za povinnost vyhledávat ohrožené děti a dále působit na rodiče, aby plnili povinnosti rodičovské péče a zodpovědnosti. OSPOD spolupracuje s orgány činnými v trestním řízení, ve kterém figuruje dítě nebo mladistvý.[58]

---

[57] ŠEVČÍKOVÁ A., BLINKA L. a kol. *Děti a dospívající online.* 1. vyd. Grada 2014. ISBN 978-80-247-5010-1. s. 161-163.

[58] Národní centrum bezpečnějšího internetu a Vysočina Education. *Dětská delikvence v prostředí internetu.* In: ncbi.cz [online]. [cit. 2024-01-06]. Dostupné z https://www.ncbi.cz/odborna-knihovna/category/6-metodiky-ucebni-materialy.html?download=89:metodika-detska-delikvence-v prostredi-internetu.pdf. s. 7.

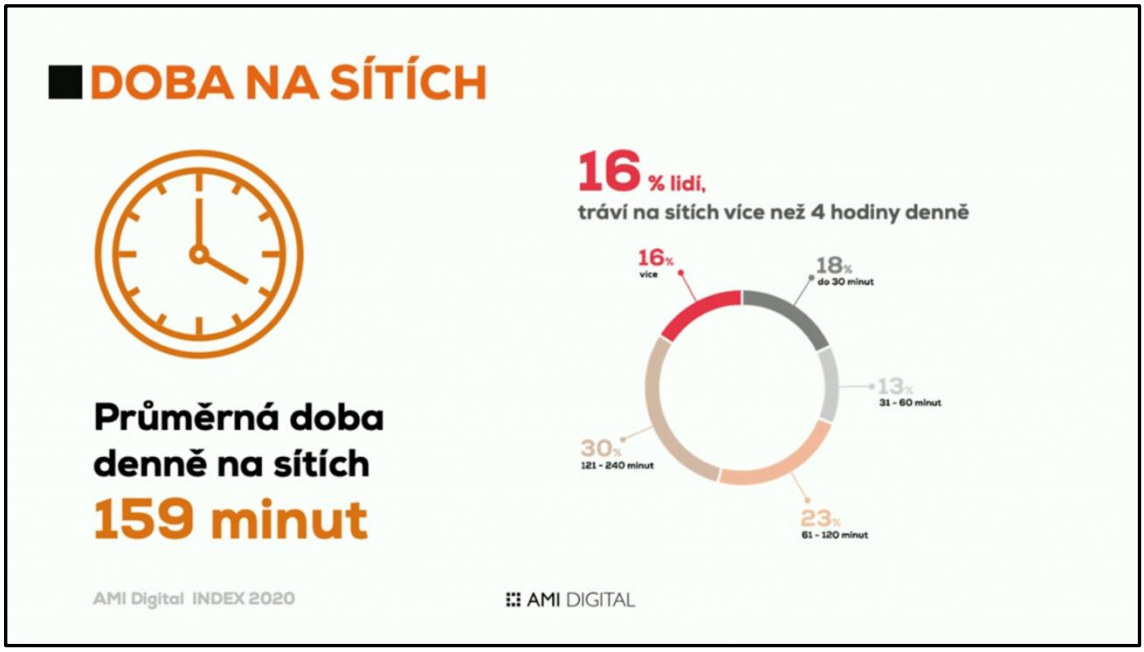
V neposlední řadě je možné se v České republice obrátit na různé instituce a neziskové organizace, které se mimo jiné zabývají i ochranou dětí a mladistvých. Například linku bezpečí pro děti – Bílý Kruh Bezpečí a další linky důvěry nebo krizové linky. Veškeré linky lze nalézt na internetu, kde jsou dostupné i veškeré informace, jak danou instituci kontaktovat. Ve většině případů mají linky bezpečí zajištěnou "nonstop" službu, která je poskytována bezplatně a je dostupná 365 dní v roce.

Na linkách bezpečí jsou odborně vyškolení konzultanti, kteří dokáží dětem poradit, povzbudit je a pomoci jim najít východisko z daného problému a případně zprostředkovat lokální pomoc ve všech místech České republiky.

„PŘÍBĚH (Z CHATU LINKY BEZPEČÍ): Na chat Linky bezpečí přišla dívka, která si již přes dva roky píše na chatu s jinou dívkou, se kterou si i vyměnily několik erotických až pornografických fotografií. Ukázalo se, že za dívku se vydával nějaký muž, který ji nyní vydírá a vyhrožuje jí, že pokud se s ním nesejde a nebude s ním mít pohlavní styk, tak její fotky zveřejní. Dívka má strach z reakce svého přítele, rodiny, přátel a ostatních lidí ve škole. Neví, co má dělat.„[59]

4.2 Čas strávený na sociálních sítích

Obrázek 5: Průměrná doba strávená na sociálních sítích uživatelů ČR[60]



[59] KRČMÁŘOVÁ, B. *Děti a online rizika: sborník sudií.* 1. vyd. Praha. Sdružení linka bezpečí, 2012. ISBN 978-80-904920-2-8. s. 90.
[60]AMI Digital Index 2021. In: amidigital.cz [online]. 2024. [cit. 2024-01-03]. Dostupné z https://amidigital.cz/ami-digital-index-2021.

Důležitou součástí prevence a ochrany dětí před negativními vlivy sociálních sítí je i důsledná regulace a kontrola času na těchto platformách stráveného. Sociální sítě využívá příležitostně až 92 procent českých uživatelů internetu a denně je přítomno na sociálních sítích až 79 procent těchto uživatelů. Průměrná doba, kterou lidé na sítích tráví, se pohybuje kolem 159 minut. Ukazuje to aktualizovaná studie AMI Digital Index 2020 realizovaná ve spolupráci s výzkumnou agenturou Stem/Mark. Průměrná doba se každým rokem zvyšuje a v posledních letech toto ovlivnila i pandemie COVID-19 a rostoucí využívání informačních technologií.[61]

Zvláště pak u dětí může být dlouhodobé a časté užívání sociálních sítí vážným problémem, neboť mohou zanedbávat své školní povinnosti a vzniká tím i riziko závislosti na internetu (tzv. netolismus) nebo riziko, že se stanou obětí sexuálních predátorů, kteří si vyhledávají své oběti v kyberprostoru.[62] Neustálá kontrola sociálních sítí, sledování příspěvků a publikování svých fotografií a videí, zvyšuje pravděpodobnost, že budou častěji sexuálními predátory kontaktováni a tyto materiály budou zneužity. Čas strávený na internetu a sociálních sítích ovlivňuje jejich reálný čas, který by mohly věnovat studiu nebo ho trávit se svými vrstevníky provozováním například sportovních nebo jiných společenských aktivit. [63]

Velice dobře tuto problematiku vystihuje dokument "V síti" Barbory Chalupové a Víta Klusáka, který byl natočen v roce 2020 a věnuje se online komunikaci dětí s dospělými, mezi nimiž ve velké míře figurují i již zmiňovaní sexuální predátoři. Dokument popisuje rizika online komunikace a především sexting a kybergrooming. V dokumentu je celá řada situací, které přímo naplňují skutkové podstaty různých trestních činů uvedených v hlavě III (trestné činy proti lidské důstojnosti v sexuální oblasti) a v hlavě IV (trestné činy proti rodině a dětem) trestního zákona. O těchto trestných činech je pojednáváno v další kapitole legislativa.

4.2.1 Netolismus

Termín netolismus (případně netholismus) lze vysvětlit pojmem závislost – v tomto případě závislost na "virtuálních drogách", mezi které můžeme zařadit sociální

[61]AMI Digital Index 2021. In: amidigital.cz [online]. 2024. [cit. 2024-01-03]. Dostupné z https://amidigital.cz/ami-digital-index-2021.
[62] ŠEVČÍKOVÁ A., BLINKA L. a kol. *Děti a dospívající online.* 1. vyd. Grada 2014. ISBN 978-80-247-5010-1. s. 43-44.
[63] BLINKA, L. *Online závislosti.* Grada 2016. ISBN 978-80-210-7975-5. s. 179-181.

sítě, počítačové hry, různé internetové služby, seznamky, diskuzní fóra, ale i užívání různých elektronických zařízení, jako je např. počítač, mobilní telefon, televize a dalších. Takto závislou osobu je možné označit slovem "netholik". Srovnáme-li netholismus s jinými závislostmi, je jeho podstata stejná – netholik je stíhán nekontrolovatelným nutkáním být neustále online, jinak řečeno musí mít svou virtuální drogu vždy po ruce. Pokud tomu tak není, dostaví se silné abstinenční příznaky. Pro neustálou potřebu sledovat a komentovat nové statusy, příspěvky a zprávy na sociálních sítích, může zanedbávat své potřeby a povinnosti. Tedy stejné potřeby a povinnosti, které lze pozorovat i u osob závislých na návykových látkách.[64]

4.3 Preventivní kroky

Kopřiva ve své knize uvádí, že dobrá, odpovědná výchova, je výchovou proaktivní. Proaktivní přístup k životu znamená, že se snažíme mít vliv na to, aby se staly ty "správné" věci. Lze konstatovat, že proaktivní výchova je tou nejlepší prevencí, jak se nedostat do situace, kdy už je pozdě a již neexistuje žádné dobré a vhodné řešení. Cílem je tedy vytvořit podněty a prostředí pro zdravý tělesný a psychický vývoj dítěte, vytváření správných návyků, budování dobrých vztahů a určování hranic a pravidel.[65]

Ministerstvo školství, mládeže a tělovýchovy České republiky zveřejnilo obecná pravidla bezpečného užívání internetu pro děti a rodiče. Tato pravidla publikovalo mnoho škol v ČR na svých webových stránkách, neboť podle ministerstva je žádoucí, aby byla všeobecně rozšířena a dodržována. Celý dokument je možné nalézt v původním znění na webových stránkách msmt.cz. Koncem roku 2023 vydalo ministerstvo vnitra, ve spolupráci s Národním pedagogickým institutem, příručku, jak se chovat na sociálních sítích a jak se vyvarovat rizikovému chování, která je určena pedagogům, preventistům, rodičům a dětem. V příručce je uvedeno desatero bezpečného chování v online světě.

Příručka rovněž obsahuje telefonické kontakty na linku bezpečí (116111), linku první psychické pomoci (116123), linku pro rodinu a školu (116000) a na nonstop linku důvěry (+420241484149, +4207777715215).[66]

[64] Internetem bezpečně. *Netolismus.* In: Internetem bezpecne.cz [online]. [cit. 2024-02-26]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/dobre-vedet/netolismus/.
[65] KOPŘIVA, P., a kol. *Respektovat a být respektován*. Kroměříž: Spirála, 2008. ISBN 978-80-904030-0-0. s. 217.
[66] Nová příručka radí, jak se chovat na sociálních sítích. In: msmt.cz [online]. MŠMT 2013-2024. [cit. 2024-01-08]. Dostupné z https://www.msmt.cz/nova-prirucka-radi-jak-se-chovat-na-socialnich-sitich.

Obrázek 6: Desatero pravidel bezpečného chování v online světě[67]

[67] Nová příručka radí, jak se chovat na sociálních sítích. In: msmt.cz [online]. MŠMT 2013-2024. [cit. 2024-01-08]. Dostupné z https://www.msmt.cz/nova-prirucka-radi-jak-se-chovat-na-socialnich-sitich.

5 Legislativa

Kybernetická kriminalita patří mezi společenské jevy, které jsou relativně nové, rozvíjející se, a proto je třeba, aby stát adekvátně reagoval na tento dynamický jev. Stát má k dispozici zákony a jiné předpisy, které mají napomoci regulovat chování společnosti. Kvalitní právní úprava a mezinárodní spolupráce zaručuje předpoklad v úspěšném boji proti kybernetické kriminalitě.

Je zde na místě, upozornit na rozmanitost úprav jednotlivých států a národů. Rozlišnosti můžeme pozorovat nejen v daném obsahu, jak je kyberkriminalita pojata a uchopena, nýbrž i v odlišnostech právních odvětví, jejichž obsahem je právě kybernetická kriminalita. Některé státy nemají v této oblasti zákony žádné nebo se existující zákony výrazně liší od zákonů v České republice. Skutek, který je v jedné zemi trestný, nemusí být v jiné zemi vůbec zahrnut do legislativy nebo může být legální.

5.1 Úmluva o počítačové kriminalitě

Úmluva o počítačové kriminalitě, plným názvem „Úmluva o kyberkriminalitě Rady Evropy“, známá také jako Budapešťská úmluva, je mezinárodní dohoda, která byla přijata v Budapešti dne 23. listopadu 2001. Cílem této dohody je poskytnout právní rámec pro boj proti kyberkriminalitě a zlepšit mezinárodní spolupráci v oblasti trestního řízení. Úmluva obsahuje ustanovení týkající se různých forem kybernetických trestných činů, včetně nelegálního přístupu k informacím, poškozování dat, počítačových podvodů, porušování autorských práv. V oddíle 3 a článku 9 obsahuje i ustanovení týkající se pornografie v kybeprostoru. Věnuje se zde i trestným činům související s dětskou pornografií. Úmluva si klade za cíl chránit jednotlivce, zejména děti, před různými formami kybernetické kriminitality, včetně nelegální výroby a šíření pornografického materiálu online. Státy se zavazují poskytovat vzájemnou pomoc při vyšetřování a trestním stíháním kybernetických deliktů.[68]

„Jménem České republiky byla Úmluva podepsána ve Štrasburku dne 9. února 2005. S Úmluvou vyslovil souhlas Parlament České republiky a prezident republiky ji ratifikoval. Ratifikační listina České republiky byla uložena u generálního tajemníka

[68] Úmluva o počítačové kriminalitě. In: eur-lex.europa.eu [online]. 2023. [cit. 2024-01-17]. Dostupné z https://eur-lex.europa.eu/CS/legal-content/summary/convention-on-cyberkrime.html.

Rady Evropy, depozitáře Úmluvy, dne 22. srpna 2013.“[69] Originální znění Úmluvy lze nalézt na webovém odkaze https://rm.coe.int/1680081561.

I přes existenci Úmluvy není mezinárodní spolupráce jednotlivých států ideální, neboť jsou velmi zdlouhavé a prodlužují tím průběh vyšetřování. Zahraniční subjekty na žádosti často vůbec nereagují a na požadované informace neodpoví. Vyžadování údajů ze zahraničí je možné pouze formou mezinárodní právní pomoci nebo na základě oprávnění podle § 88a odstavce 1 trestního řádu, tedy údajů o uskutečněném telekomunikačním provozu.

Výjimkou jsou tzv. „Emergency“ případy. Od 1. ledna 2017 drží národní centrála organizovaného zločinu Policie ČR (dále NCOZ) nepřetržitou službu pro níže uvedené závažné případy, pro rychlé vyžádání informací od zahraničních subjektů (Meta Platforms, Google, Microsoft a dalších). Vyžadování informací od českých poskytovatelů internetového připojení v těchto případech realizuje útvar zvláštních činností SKPV (dále ÚZČ). Tato služba je dostupná 24 hodin denně, 7 dní v týdnu.

Emergency případy:

- sebevraždy,
- dětská pornografie,
- spáchání závažného trestného činu, například vražda, terorismus (ohrožení života),
- dítě v ohrožení (například únos),
- podobné situace vyžadující zvláštního zřetele a okamžitou reakci

5.2 Právní úprava v ČR

Trestné formy jednání ve vztahu k dětské pornografii jsou obsaženy v zákoně č. 40/2009 Sb., trestní zákon, ve znění pozdějších předpisů. K trestnému činu šíření dětské pornografie podle § 191 zákon upravuje speciálním ustanovením užší okruh případů, a to konkrétně výrobu a jiné nakládání s dětskou pornografií v § 192. Zahrnuje přísnější regulaci případů, kdy někdo přechovává fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě.

[69] ČESKO. Sdělení č. 104/2013 Sb. m.s., *sdělení Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě,* oddíl 3, článek 9. In: Zákony pro lidi [online]. Praha: ©AION CS, 2010–2024 [cit. 2024-01-16]. Dostupné z: https://www.zakonyprolidi.cz/cs/2013-104.

Hrozbě vyšší trestní sankce se vystavuje ten, kdo vyrobí, doveze, vyveze, proveze, nabídne, činí veřejně přístupným, zprostředkuje, uvede do oběhu, prodá nebo jinak jinému opatří fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě, anebo kdo kořistí z takového pornografického díla. Dále trestní zákon obsahuje speciální úpravu trestné činnosti zneužití dítěte k výrobě pornografie podle § 193. Postihuje jednání pachatele, který přiměje, zjedná, najme, zláká, svede nebo zneužije dítě k výrobě pornografického díla nebo kořistí z účasti dítěte na takovém pornografickém díle.[70]

Další trestné činy, které je nutné zmínit, upravené zákonem č. 40/2009 Sb., páchané ve vztahu k lidské důstojnosti v sexuální oblasti jsou: vydírání (§175), znásilnění (§185), sexuální nátlak (§ 186), pohlavní zneužití (§ 187), kuplířství (§ 189), prostituce ohrožující mravní vývoj dětí (§ 190), šíření pornografie (§ 191), účast na pornografické představení (§ 193a), navazování nedovolených kontaktů s dítětem (§ 193b).[71]

5.3 Odhalování trestných činů a objasňování trestné činnosti

Jak již bylo zmíněno odhalování trestných činů v kyberprostoru a ustanovení osoby pachatele je velmi obtížné. Hlavní důvodem je anonymita internetu a neomezený virtuální prostor bez stanovených hranic. Částečné "skrytí" v internetu zvládne, za využití bezplatných a veřejně dostupných služeb, i naprostý laik s běžnými znalostmi o informačních technologiích. V případě páchání promyšlené sériové nebo organizované trestné činnosti, při které pachatelé využívají další podpůrné anonymizační služby, profesionální software a další prostředky, je poté velmi složité nebo i nereálné ustanovení konkrétních osob.

Vyžadování informací od zahraničních subjektů vede k časovým prodlevám ve vyšetřování, což může mít za následek ztrátu důležitých dat, které jsou pro objasnění případu stěžejní. Částečně tento problém řeší tzv. "freezing" dat, který je u určitých subjektů možný. Jedná se o "zmrazení" určených dat, které dané subjekty uloží do doby, než jsou vyžádány orgány činnými v trestním řízení. Bohužel i tato služba není řešena bezodkladně, neboť věc je nejprve nutné konzultovat s dozorujícím státním zástupcem, který musí udělit souhlas a až poté je žádost zaslána, cestou národní centrály proti organizovanému zločinu, konkrétnímu subjektu.

[70] Zákon č. 40/2009 Sb., *trestní zákon, ve znění pozdějších předpisů,* § 191-193.
[71] Tamtéž.

Objasnění trestných činů v kyberprostoru, i přes maximální snahu policejních orgánů, je velmi malé. Nutno podotknout, že policejní orgán se při vyšetřování musí řídit trestním řádem a trestním zákonem a při operativní pátrací činnosti nelze použít prostředky, které jsou sice dostupné a technicky proveditelné a dopomohly by k ustanovení pachatele, ale nejsou v souladu se zákonem a tedy legální.

6 Kazuistika

Praktická část této práce se věnuje třem případům mravnostního charakteru v kyberprostoru, navazování kontaktů s dítětem přes sociální sítě a zneužití dítěte k výrobě pornografie, které byly Policií ČR vyšetřovány. Rizikové chování obětí těchto trestných činů je spojeno s nedostatečnou znalostí nebezpečí internetového prostředí a nedostatkem uvědomění si důsledků svého jednání. Často mohou děti a mladiství svým rizikovým chováním na internetu, spojeným s nedostatkem opatrnosti, utrpět větší škody, než jim může způsobit samotné cílené jednání pachatelů. Pro ochranu a zajištění anonymity zúčastněných osob nejsou v praktické části práce uvedena žádná jména, názvy lokalit, či jiné osobní informace, které by vedly k identifikaci konkrétních osob.

6.1 Metodologie výzkumu a sběr dat

Praktická část bakalářské práce je zpracována formou případových studií, kazuistiky. Tyto studie se zaměřují na detailnější a hlubší analýzu sledovaných vzorků v porovnání s výzkumnými metodami, která jsou často zpracovány z obecnějších dat od většího množství respondentů. Je zde provedena analýza a komparace několika konkrétních případů, přičemž komparace případů může poskytnout hlubší vhled do různých aspektů trestných činů mravnostního charakteru a přispět k formulaci lepších strategií prevence a řešení. Data k zájmovým případům byla získána z interních systémů Policie ČR a na základě souhlasu s využitím spisových materiálů pro účely této práce, který udělil ředitel územního odboru Policie ČR plk. Mgr. Petr Petr.

V další části práce je zvolena výzkumná metoda dotazování, přičemž sběr dat zde byl realizován formou rozhovorů s vyšetřovateli konkrétních případů. Bylo jim položeno celkem 8 otázek k problematice mravnostní trestné činnosti. Cílem rozhovoru bylo získání relevantních informací pro další vyšetřování jiných případů, poskytnutí psychologické podpory obětem a nalezení cesty k nápravě či prevenci dalších obdobných trestných činů. Vyšetřovatelům byly dále položeny otázky k samotných pachatelům a obětem, se kterými v rámci vyšetřování hovořili. Z důvodu anonymity zainteresovaných osob, nejsou odpovědi v této práci zveřejněny, ale pouze zpracovány do obecných grafů. Získané informace mohou dopomoci k vytvoření si uceleného pohledu na páchání této trestné činnosti, zjištění jakým způsobem pachatelé vyhledávají a získávají pornografický materiál nejčastěji a jaký byl a dále může být celkový vliv na jejich oběti.

7 Případové studie

Pro lepší orientaci je ke každému případu přiřazeno křestní jméno pachatele. Z důvodu zachování anonymity jsou tato křesní jména zcela smyšlená.

7.1 Případ Ctirad

Tabulka 1: profil pachatele a oběti případ Ctirad[72]

profil pachatele		profil oběti	
pohlaví	**muž**	**pohlaví**	**žena**
věk	14	věk	9
rodinný stav	svobodný	rodinný stav	svobodná
povolání	student ZŠ	povolání	studentka ZŠ
použita sociální síť whatsapp			

Přijetí oznámení

Dne 15. 03. 2021 se dostavila na obvodní oddělení Policie ČR Pelhřimov paní H. T., která uvedla, že má 9letou dceru a v jejím mobilním telefonu nalezla video s pornografickou tematikou, na kterém je zachycena její nezletilá dcera. Doslovná citace z úředního záznamu o podaném vysvětlení dle § 158 odstavce 6 trestního řádu H. T.: „*Jedná se o video, kde je dcera oblečená, pak se svléká, rukou zajíždí mezi nohy. Je vidět, jak je nahá, jsou vidět její pohlavní orgány, přirození. Také jsou na videu vidět její prsa. Rozhodně je na videu moje dcera, je to natáčené v našem bytě v ložnici*“. Zájmové video oznamovatelka nalezla v historii komunikace sociální sítě aplikace whatsapp, ve které její dcera komunikovala s uživatelským profilem s názvem “Debil“, přičemž z komunikace vyplynulo, že uvedený uživatel požaduje po její dceři další fotografie a videa s pornografickou tematikou. Z důvodu, že v minulosti zhlédla dokument “V síti“, rozhodla se, že věc oznámí na Policii ČR.

Úryvek ze zájmové konverzace mezi pachatelem a obětí:

pachatel: „pošles mi prsa?“
oběť: „nevim“
pachatel: „muzes udelat video“
oběť: „ted ne, az nebude mamka doma“
pachatel: „dobře ale ukazes prsa“
oběť: „dobre“[73]

[72] Zdroj: Trestní spis Policie ČR.
[73] Doslovná citace z elektronické konverzace mezi pachatelem a obětí. Včetně pravopisných chyb a chybné gramatiky.

Zahájení úkonů trestního řízení a postup vyšetřování

Vzhledem k závažnosti oznámení si ihned případ, dle věcné příslušnosti, převzala služba kriminální policie a vyšetřování, oddělení obecné kriminality a oddělení analytiky a kybernetické kriminality Pelhřimov (dále OAKK). Úřední záznam o podaném vysvětlení dle § 158 odstavce 6 trestního řádu provedl vyšetřovatel, který téhož dne zahájil úkony trestního řízení pro podezření ze spáchání trestného činu zneužití dítěte k výrobě pornografie podle § 193 odstavce 1 trestního zákona, neboť na podkladě zjištěných skutečností byl dostatečně odůvodněn závěr, že „*neznámý pachatel, přinejmenším v době od 00:01 hodin dne 01 01. 2021 do 12:32 hodin dne 25. 06. 2020, kontaktoval pomocí sociální sítě whatsapp nezletilou Y. O., nacházející se v místě jejího bydliště a požadoval po ní pomocí zaslání fotografií a videosouborů jejího nahého těla, přičemž poškozená se takto dle jeho požadavků měla pomocí mobilního telefonu vyfotografovat, natočit krátká videa a zaslala mu požadované v elektronické podobě, přičemž k tomuto jednání přistoupil s vědomím, že jmenovaná je zjevně nezletilá*".[74]

Za přítomnosti pracovnice orgánu sociálně-právní ochrany dětí byl proveden výslech s poškozenou nezletilou osobou na protokol o výslechu svědka – osoby mladší 18 let. Výslech byl realizován ve speciální místnosti územního odboru Policie ČR Pelhřimov, uzpůsobené pro výslechy dětí a mladistvých. Celý výslech byl proveden formou rozhovoru s poškozenou, která byla před započetím výslechu, s přihlédnutím k jejímu věku, řádně poučena. Celý výslech byl zadokumentován na CD nosič a ze zajištěného záznamu byl následně proveden doslovný přepis.

Oznamovatelkou byl předložen, podle § 78 odstavce 1 trestního řádu, mobilní telefon její dcery, k provedení jeho ohledání a zajištění zájmové elektronické komunikace. V rámci sepsání protokolu o ohledání věci podle § 113 trestního řádu byla zajištěna elektronická komunikace z aplikace whatsapp mezi poškozenou a neznámým pachatelem. Telefon byl po provedeném úkonu zaslán na oddělení kybernetické kriminality Policie ČR Jihlava k provedení jeho kompletní zálohy dat přes zařízení UFED Cellebrite k vytvoření tzv. bitové kopie.

Z podání vysvětlení oznamovatelky a poškozené bylo známo pouze telefonní číslo, pod kterým pachatel komunikoval přes mobilní aplikaci whatsapp. Zjištěné telefonní číslo bylo ihned po oznámení prověřeno přes informační systém “Telefony“,

[74] Doslovná citace z policejního záznamu ZÚTŘ.

přes který bylo zjištěno, že se jedná o anonymní předplacenou SIM kartu společnosti O2 Czech Republic a. s. (SIM GO). Prostřednictvím útvaru zvláštních činností služby kriminální policie a vyšetřování České Budějovice (expozitura E1, dále ÚZČ) bylo zažádáno dle § 66 odstavce 2,3 zákona č. 273/2008 Sb. o Policii České republiky, o sdělení výrobního čísla zařízení IMEI, ve kterém byla SIM karta použita a dále o sdělení historie dobíjení SIM karty. Z následné odpovědi bylo zjištěno, že zájmová SIM karta byla užita ve dvou zařízeních s ustanovenými IMEI a byla dobíjena pouze jednou dne 12. 10. 2020 na částku 300 Kč, a to prostřednictvím platebního terminálu společnosti Sazka a. s.

Na základě čísla transakce dobití SIM karty byla zaslána žádost dle § 8 odstavce 1 trestního řádu na společnost Sazka a. s. s dotazem, kde a jakým způsobem byla SIM karta dobíjena. Z odpovědi společnosti Sazka a. s. bylo zjištěno, že SIM karta byla dobíjena dne 12. 10. 2020 v 14:05 hod. na terminálu Sazka a. s. v jedné z obcí ve středočeském kraji.

Vzhledem k velmi malému množství informací bylo přistoupeno k operativně pátrací činnosti ze strany příslušníků oddělení obecné kriminality SKPV Pelhřimov. Společně s vyšetřovatelem bylo provedeno šetření v místě zjištěného platebního terminálu společnosti Sazka a. s. Na místě bylo zjištěno, že terminál je umístěn v pobočce společnosti Česká pošta a. s., která se nachází v přízemí budovy obecního úřadu dané obce.

OAKK Pelhřimov provedlo operativní a cílené šetření v samotné aplikaci whatsapp. Po předchozí dohodě s dozorujícím státním zástupcem byla policistou dále vedena elektronická konverzace z mobilního telefonu poškozené. Po určité době byl pachateli zaslán speciální webový odkaz s legendou, že se jedná o erotickou fotografii. Po jeho otevření se pachateli objevila informace, že obrázek nelze otevřít. Tímto byl zaznamenán přístupový log (IP adresa), ze kterého bylo přistupováno do sítě internet. Konkrétně se jednalo o IPv6 adresu společnosti O2 Czech Republic a.s. Bližší informace ke zjištěné IPv6 byly následně vyžádány na základě sepsaného podnětu k podání návrhu na vydání příkazu ke zjištění údajů o uskutečněném telekomunikačním provozu podle § 88a odstavce 1 trestního řádu. Soudce okresního soudu Pelhřimov poté vyhotovil příkaz k zjištění údajů o telekomunikačním provozu. Z doručené odpovědi od společnosti O2 byl zjištěn koncový bod připojení a ustanovena konkrétní osoba, užívající dané internetové připojení.

Na základě zjištěných skutečností byl vyšetřovatelem případu vyhotoven podnět k podání návrhu na vydání příkazu k provedení domovní prohlídky podle § 83 odstavce 1 trestního řádu a příslušný soud příkaz k domovní prohlídce vydal. Domovní prohlídka byla realizována a bylo zajištěno několik kusů výpočetní techniky, mobilních telefonů a paměťových médií k další analýze a zjištění, zda neobsahují závadový obsah.

Při provádění domovní prohlídky a výsleších přítomných osob vyšlo najevo, že pachatelem a podezřelým by mohla být nezletilá osoba. Z tohoto důvodu byla na místo vyžádána pracovnice OSPOD Česká Lípa, která byla následně přítomna domovní prohlídce a veškerým dalším prováděným úkonům.

Vzhledem ke skutečnosti, že pachatelem byla osoba nezletilá, která není podle § 25 trestního zákona trestně odpovědná, byla celá věc, po řádném zadokumentování ze strany policejního orgánu Policie ČR Česká Lípa, odložena podle § 159a odstavce 2 trestního řádu a po skončení prověřování byl trestní spis předložen státnímu zástupci okresního státního zastupitelství Česká Lípa ve smyslu § 90 odstavce 1 zákona č. 218/2003 Sb., neboť přicházelo v úvahu podání návrhu na zahájení řízení proti dítěti mladšímu patnácti let, které se dopustilo činu jinak trestného.

I přes minimum informací, které byly na počátku prověřování známy, se podařilo danou věc objasnit. Nutno ale podotknout, že pachatelem byla osoba, která se v internetové síti žádným způsobem neskrývala a komunikovala s poškozenou z místa svého bydliště. V opačném případě by bylo její zjištění a ustanovení velmi obtížné.

Rozhovor s vyšetřovatelem

Tento rozhovor byl proveden se zkušeným policistou zařazeným na Oddělení obecké kriminality Policie ČR Pelhřimov, který prováděl vyšetřování uvedeného případu. U policie působí již 19 let a z toho 17 let jako vyšetřovatel.

Otázka č.1: Jak často se setkáváte s trestnými činy mravnostního charakteru, tedy například zneužití dítěte k výrobě pornografie dle § 193 trestního zákona?

Odpověď: Na našem oddělení je nás celkem šest vyšetřovatelů a každý se již s podobným případem setkal. Dané věci tedy nevyšetřuji pouze já. Mohu říci, že podobné skutky prověřuji v průměru 3x za rok.

Otázka č.2: Když porovnáte svou dlouholetou praxi v dané problematice, jaký je váš názor na tuto trestnou činnost? Je tato trestná činnost na ústupu, či vzestupu a z jakého důvodu?

Odpověď: S nástupem internetové sítě a rozvojem sociálních sítí je tato trestná činnost na vzestupu, neboť pachatelé mají mnohem větší možnosti, jak kontaktovat svou oběť. Dále je velkým problémem vyhodnocování samotné závadové komunikace a pornografických materiálů, což je časově velmi náročné.

Otázka č.3: Jsou si tyto trestné činy něčím podobné, nebo jsou jednání pachatelů zcela odlišná?

Odpověď: Většinou se jedná o stále stejná jednání pachatelů. V prvopočátku kontaktují oběť prostřednictvím sociálních sítí pod legendou nezávazného dopisování a ve většině případů pod smyšleným uživatelským profilem, přičemž se vydávají například za vrstevníka oběti. Po nějaké době společně elektronické komunikace vyžadují zasílání fotografií a videí s intimním obsahem.

Otázka č.4: Vedete si nějakou statistiku ohledně věku pachatelů, kteří páchají tuto trestnou činnost?

Odpověď: Já osobně nikoliv. Co vím, tak nejčastěji by se mělo jednat o pachatele ve věku kolem 35 let, který nemá partnerku a celkově hůře navazuje partnerské vztahy. Ale toto nemám nijak ověřeno. Dle mého názoru je věk pachatelů zcela různorodý. Vzhledem k tomu, že počítač nebo mobilní telefon má v dnešní době téměř každý a jejich ovládání, společně s připojením do internetové sítě, není nijak složité, a proto může být sexuálním útočníkem, ve virtuální prostředí, prakticky kdokoliv.

Otázka č.5: Jaký máte názor k páchání této trestné činnosti opakovaně, tzv. recidivu?

Odpověď: Pokud je pachatel nějakým způsobem nemocný, tedy má nějakou sexuální úchylku a toto není nijak řešeno, bude tuto trestnou činnost páchat i po případném odsouzení za předchozí delikt. Ale vzhledem k dnešním neomezeným možnostem, jak někoho kontaktovat, toto mohou dělat i zcela zdravé a vzdělané osoby.

Otázka č.6: Z Vašich zkušeností v rámci prověřování, konkrétně při prvním setkání s podezřelými při podání vysvětlení, doznávají se osoby samy k trestné činnosti a spolupracují?

Odpověď: Je to hlavně o přístupu vyšetřovatele. Je třeba tyto lidi řádně poučit a vše jim vysvětlit. Hodně záleží na tom, jaké nezpochybnitelné důkazy proti nim máme. Z tohoto důvodu úzce spolupracuji s oddělením analytiky a kybernetické kriminality.

Otázka č.7: Jaké bývají rozsudky za tyto trestné činy? Vybavujete si tresty, které byly pachatelům soudem uloženy?

Odpověď: Já osobně jsem se setkal pouze soudem uloženými podmíněnými tresty. Což si myslím, že je špatně, neboť tito pachatelé jsou velmi nebezpeční pro společnost.

Otázka č.8: Zhlédl jste dokument „V síti“, který se zabývá touto problematikou?

Odpověď: Vím, oč se jedná, ale zatím jsem tento dokument neviděl.

7.2 Případ Bořek

Tabulka 2: profil pachatele a oběti případ Bořek[75]

profil pachatele		profil oběti	
pohlaví	**muž**	**pohlaví**	**žena**
věk	16	věk	13
rodinný stav	svobodný	rodinný stav	svobodná
povolání	student ZŠ	povolání	studentka ZŠ
použita sociální síť instagram			

Přijetí oznámení

Dne 09. 08. 2019 bylo na obvodním oddělení Policie ČR Velké Meziříčí přijato oznámení od pana T. H., který uvedl, že v telefonu své nezletilé 13leté dcery, konkrétně v aplikaci instagram, nalezl konverzaci mezi ní a uživatelem “4blbec“, ve které si všiml i erotických videí a fotografií, které si mezi sebou přeposílali. Doslovná citace z úředního záznamu o podaném vysvětlení dle § 158 odstavce 6 trestního řádu T. H.: „*K věci mého oznámení bych chtěl říci, že již pár dní nazpět jsem si povšiml, že dcera bývá dlouho do noci vzhůru a něco dělá na svém mobilu, že si tam s někým píše. Já jsem se jí včera večer ptal, s kým si to pořád píše a na to mi neodpověděla a šla spát, tak jsem si řekl, že to nechám na ráno. Dnes ráno v době kolem 08:00 hodin, kdy dcera ještě spala, tak jsem jí vzal telefon a po zapnutí mně hned na telefonu vyskočila nějaká konverzace na instagramu, ze které jsem zjistil, že si zde dcera píše s nějakým hochem a jsou zde*

[75] Zdroj: Trestní spis Policie ČR.

posílané i fotografie a různá video erotického rázu. Jak odeslané ze strany dcery, tak přijaté ze strany nějakého toho mladíka.“

Úryvek ze zájmové konverzace mezi pachatelem a obětí:

pachatel: „kolik ti je“
oběť: „13“
pachatel: „a uz mas prsa?“
oběť: „jo“
pachatel: „mas nejake foto?“
oběť: „jo s kamoskou“[76]

Zahájení úkonů trestního řízení a postup vyšetřování

Případ byl, na základě místní a věcné příslušnosti dle PPP č.103/2013, postoupen na oddělení obecné kriminality SKPV Pelhřimov. Vzhledem ke skutečnosti, že prověřovaná osoba byla od samého počátku známa a to na základě podání vysvětlení oznamovatele a poškozené, byly zahájeny úkony trestního řízení pro podezření z provinění zneužití dítěte k výrobě pornografie podle § 193 odstavce 1 trestního zákona na tuto konkrétní osobu, neboť na podkladě zjištěných skutečností byl dostatečně odůvodněn závěr, že „*neznámý pachatel kontaktoval na sociální síti instagram, v době od 9. 5. 2019 do 8. 8. 2019, nezletilou K. H. a opakovaně ji přiměl k výrobě pornografických fotografií a videí, které mu poškozená zaslala "*.[77]

Za přítomnosti pracovnice orgánu sociálně-právní ochrany dětí byl proveden výslech s poškozenou nezletilou osobou na protokol o výslechu svědka – osoby mladší 18 let. Výslech byl realizován ve speciální místnosti územního odboru Policie ČR Žďár nad Sázavou, uzpůsobené pro výslechy dětí a mladistvých. Celý výslech byl proveden formou rozhovoru s poškozenou, která byla před započetím výslechu, s přihlédnutím k jejímu věku, řádně poučena. Celý výslech byl zadokumentován na CD nosič a ze zajištěného záznamu byl následně proveden doslovný přepis. Na základě § 78 odstavce 1 trestního řádu, byla dále provedena záloha elektronické komunikace ze zájmového instagram profilu mezi poškozenou a prověřovaným, která byla poté vyhodnocena.

[76] Doslovná citace z elektronické konverzace mezi pachatelem a obětí. Včetně pravopisných chyb a chybné gramatiky.
[77] Doslovná citace z policejního záznamu ZÚTŘ.

Za přítomnosti obhájce, na základě nutné obhajoby, bylo s prověřovaným mladistvým provedeno podání vysvětlení podle § 158 odstavce 6 trestního řádu, kdy využil svého práva a k věci odmítl vypovídat.

Operativním šetřením bylo zjištěno, že prověřovaný užíval ke komunikaci další uživatelské profily na sociální síti facebook. Vzhledem ke skutečnosti, že sociální síť instagram a facebook spravuje stejná společnost Meta Platforms Ltd., byl OAKK Pelhřimov sepsán podnět k podání návrhu na vydání příkazu ke zjištění údajů o telekomunikačním provozu dle § 88a odstavce 1 trestního řádu ke všem zjištěným uživatelským profilům. Z následné odpovědi od společnosti Meta Platforms Ltd., byly zjištěny registrační a logovací údaje k účtům. Tyto údaje poskytly policejnímu orgánu cenné informace, neboť při registraci účtů bylo použito telefonní číslo prověřovaného a veškeré přístupy do účtů byly realizovány přes poskytovatele internetu v místě jeho bydliště a ve škole, kterou navštěvoval.

Dále na základě § 78 odstavce 1 trestního řádu, prověřovaný vydal svůj mobilní telefon k provedení jeho analýzy a zálohy přes zařízení UFED Cellebrite a téhož dne mu bylo doručeno usnesení o zahájení trestního stíhání podle § 160 odstavce 1 trestního řádu.

Za přítomnosti obhájce byl s obviněným sepsán protokol o výslechu mladistvého obviněného, kdy k věci vypovídal, ale ke skutku se nedoznal.

Na základě zjištěných skutečností ve vyšetřování dané věci, navrhovaných důkazů, které zahrnovaly výslech poškozené a svědků, vyhodnocení zajištěných dat z mobilních telefonů a účtů na sociálních sítích a dalších, byl policejním orgánem sepsán návrh na podání obžaloby podle § 166 odstavce 3 trestního řádu proti obviněnému a tento návrh byl doručen okresnímu státnímu zastupitelství v Pelhřimově. Obžalovaný poté stanul před soudem, který v případu provinění zneužití dítěte k výrobě pornografie podle § 193 odstavce 1 trestního zákona rozhodl, že obžalovaný je vinen a vydal jménem republiky odsuzující rozsudek.

V tomto konkrétním případě byl od počátku pachatel ustanoven, neboť ho oběť znala a i přes to, že se k věci nedoznal a jeho spolupráce s OČTŘ byla minimální, byly navrhované důkazy dostačující a vedly k jeho usvědčení. Objasnění dopomohly skutečnosti, že pachatel se v internetové síti nijak neskrýval a používal uživatelské profily, kde uváděl celé své jméno. Registraci těchto profilů prováděl za použití

telefonního čísla, které měl registrované na svou osobu a do internetové sítě se připojoval v místě svého bydliště nebo ve škole.

Rozhovor s vyšetřovatelem

Tento rozhovor byl proveden se zkušenou policistkou zařazenou na Oddělení obecké kriminality Policie ČR Pelhřimov, který zpracovává trestní spisy stejného nebo podobného charakteru. U policie působí již 30 let a z toho 4 roky jako vyšetřovatelka.

Otázka č.1: Jak často se setkáváte s trestnými činy mravnostního charakteru, tedy například zneužití dítěte k výrobě pornografie dle § 193 trestního zákona?

Odpověď: Často, protože moje pracovní zaměření je právě na tuto problematiku.

Otázka č.2: Když porovnáte svou dlouholetou praxi v dané problematice, jaký je váš názor na tuto trestnou činnost? Je tato trestná činnost na ústupu, či vzestupu a z jakého důvodu?

Odpověď: Na oddělení obecné kriminality jsem pouze čtvrtým rokem, ale pokud mohu porovnávat z předchozími lety, tak jednoznačně na vzestupu. Když jsem na toto místo nastupovala z obvodního oddělení, tak jsme měli pár případů za rok, ale nyní jsou jich desítky, hlavně mezi mladistvými.

Otázka č.3: Jsou si tyto trestné činy něčím podobné, nebo jsou jednání pachatelů zcela odlišná?

Odpověď: Co já se setkala, tak to bylo vždy hodně podobné. Kontaktování na sociálních sítích, vzájemné dopisování a zasílání pornografického materiálu mezi mladistvými.

Otázka č.4: Vedete si nějakou statistiku ohledně věku pachatelů, kteří páchají tuto trestnou činnost?

Odpověď: Nevedu. Ale já měla případy, ve který figurovali všichni pachatelé a oběti do osmnácti let. Tedy v případech, které se podařilo objasnit.

Otázka č.5: Jaký máte názor k páchání této trestné činnosti opakovaně, tzv. recidivu?

Odpověď: Jedná se o závažnou trestnou činnost, ale je nutné rozlišovat, zda si dopisují dva vrstevníci a posílají si erotické fotografie nebo se jedná o tzv. sexuální predátory, kteří oběti vydírají nebo zneužívají. Tam bych určitě byla pro vysoké tresty a léčbu.

Otázka č.6: Z Vašich zkušeností v rámci prověřování, konkrétně při prvním setkání s podezřelými při podání vysvětlení, doznávají se osoby samy k trestné činnosti a spolupracují?

Odpověď: U mladistvých mám zkušenosti, že většinou ano a k věci se přiznají.

Otázka č.7: Jaké bývají rozsudky za tyto trestné činy? Vybavujete si tresty, které byly pachatelům soudem uloženy?

Odpověď: Detailně to nesleduji, ale u mladistvých jsou to většinou tresty podmíněné, případně ochranné opatření apod. Nevím o případu, ve kterém by dostal pachatel trest nepodmíněný.

Otázka č.8: Zhlédla jste dokument „V síti“, který se zabývá touto problematikou?

Odpověď: Neviděla. Ale zvažuji, že se na dokument podívám i se svými dcerami. Tedy na tu verzi pro děti a mladistvé.

7.3 Případ Mojmír

Tabulka 3: profil pachatele a oběti případ Mojmír[78]

profil pachatele		profil oběti	
pohlaví	**muž**	**pohlaví**	**žena**
věk	41	věk	13
rodinný stav	rozvedený	rodinný stav	svobodná
povolání	dělník	povolání	studentka ZŠ
použita sociální síť facebook			

Přijetí oznámení

Dne 26. 11. 2018 bylo na obvodním oddělení Policie ČR Humpolec přijato oznámení od paní P. J., která uvedla, že je vychovatelkou v dětském domově a v notebooku, který si děti půjčují, nalezla komunikaci na sociální síti facebook, kde si někdo psal s jejich 13letou žákyní P.K. a konverzace byla se sexuálním podtextem. Doslovná citace z úředního záznamu o podaném vysvětlení dle § 158 odstavce 6 trestního řádu P. J.: “*Na vychovatelně jsem notebook otevřela. Hned mi tam naskočil facebook a chat s osobou vydávající se za M. P. Přišlo mi to divné, proto jsem projela, tedy přečetla celou konverzaci. Divné mi to přišlo z toho důvodu, že poslední konverzace byla "umiš*

[78] Zdroj: Trestní spis Policie ČR.

lizat piča" a další bylo "umím a ty umíš kouřit čuráka". Proto jsem projela celou konverzaci. Při tom jsem zjistila, že ten chat byl chvilku sexuálně ražený a chvilku romanticky. Přitom zde byly fotky, kdy si P.K. na jedné z fotek vyfotila prsa, dále přirození, pak přirození a prsa, pak tam byla fotka přirození muže a dvě fotky obličeje muže. Fotky P.K. byly foceny přes web kameru na notebooku, kdy je patrné, že v pozadí je vybavení obýváku našeho dětského domova."

Úryvek ze zájmové konverzace mezi pachatelem a obětí:

pachatel: „jo a už si šukala někdy"
oběť: „ne vadi mi to"
pachatel: „jo lasko a prstiš"
oběť: „jo"
pachatel: „jo a kolik tam strkaš prstů"
oběť: „dva a nebo jeden"[79]

Zahájení úkonů trestního řízení a postup vyšetřování

Ihned po oznámení byly policejním orgánem obvodního oddělení Humpolec zahájeny úkony trestního řízení pro přečin zneužití dítěte k výrobě pornografie podle § 193 odstavce 1 trestního zákona a přečin ohrožování výchovy dítěte podle § 201 odstavce 1 písm. a) trestního zákona, neboť na podkladě zjištěných skutečností byl dostatečně odůvodněn závěr, že „*neznámý pachatel v přesně nezjištěné době, přinejmenším od 7. 8. 2018 do 24. 11. 2018, z dosud nezjištěného místa, vystupující na sociální síti facebook pod jménem M.P., facebookový profil "pexx.plxxx.50", se dne 7. 8. 2018 seznámil prostřednictvím sociální sítě facebook s nezletilá P.K., vystupující na sociální síti facebook pod profilem "bexx.thxxxx.3", a této zaslal dne 27. 8. 2018 přes aplikaci messenger v sociální síti facebook fotografii zobrazující pánské přirození, následně s ní vedl komunikaci s erotickým podtextem, kdy jí zejména sdělil, "Lasko tohle pero te bude šukat lasko"; poté ji požádal, přestože si byl vědom jejího věku 13ti let, aby mu zaslala erotické fotky, načež mu nezletilá P.K. zaslala prostřednictvím sociální sítě facebook dne 17. 11. 2018 a dne 24. 11. 2018 pomocí aplikace messenger přinejmenším čtyři své fotografie, na kterých je vyobrazena zejména s odhaleným přirozením a prsy; poslední komunikace proběhla dne 24. 11. 2018, kdy na její otázku "umis lizat piča", odpověděl "Jo umím a ty kouřit ptáka"*.[80] Dle věcné příslušnosti si případ převzala služba

[79] Doslovná citace z elektronické konverzace mezi pachatelem a obětí. Včetně pravopisných chyb a chybné gramatiky.
[80] Doslovná citace z policejního záznamu ZÚTŘ.

kriminální policie a vyšetřování, oddělení obecné kriminality a oddělení analytiky a kybernetické kriminality Pelhřimov.

Za přítomnosti pracovnice orgánu sociálně-právní ochrany dětí byl proveden výslech s poškozenou nezletilou osobou na protokol o výslechu svědka – osoby mladší 18 let. Výslech byl realizován ve speciální místnosti územního odboru Policie ČR Pelhřimov, uzpůsobené pro výslechy dětí a mladistvých. Celý výslech byl proveden formou rozhovoru s poškozenou, která byla před započetím výslechu, s přihlédnutím k jejímu věku, řádně poučena. Celý výslech byl zadokumentován na CD nosič a ze zajištěného záznamu byl následně proveden doslovný přepis.

Vzhledem ke skutečnosti, že byl znám facebookový profil pachatele a bylo ustanoveno jedinečné ID profilu, policista OAKK provedl ohledání zájmového profilu na protokol o ohledání věci dle § 113 trestního řádu a dále byl sepsán podnět k podání návrhu na vydání příkazu ke zjištění údajů o telekomunikačním provozu dle § 88a odstavce 1 trestního řádu a soudem vydaný příkaz byl přes ÚZČ zaslán na společnost Meta Platforms Ltd. Před tímto úkonem byl, prostřednictvím NCOZ, proveden tzv. „freezing“ dat, kdy se jedná o zmrazení obsahu zájmového uživatelského účtu na sociální síti za požadované období. Tento úkon je prováděn z důvodu uchování důležitých dat, neboť existovalo riziko jejich smazání ze strany uživatele účtu a tedy ztráty nebo zničení důležitých digitálních stop a důkazů proti pachateli.

Pomocí operativně pátracích prostředků, vyhodnocení dat ze zájmového uživatelského profilu na sociální síti facebook a přes interní evidence a systémy Policie ČR se podařilo ustanovit osobu pachatele. V rámci prověřování v přípravném řízení bylo nashromážděno dostatek potřebných informací a materiálů, aby bylo možné vyhotovit podnět k podání návrhu na vydání příkazu k provedení domovní prohlídky podle § 83 odstavce 1 trestního řádu a žádost o vydání souhlasu se zadržením podezřelého ve smyslu § 76 odstavce 1 trestního řádu. Soudce následně vydal příkaz k provedení domovní prohlídky a okresní státní zástupce vydal souhlas se zadržením na konkrétní osobu.

Policejním orgánem byla realizována domovní prohlídka a na místě došlo k zadržení podezřelého. Při domovní prohlídce byla zajištěna výpočetní a jiná IT technika, u které byla provedena analýza a záloha přes zařízení UFED Cellebrite. Po následném vyhodnocení všech získaných a zajištěných dat a provedeném výslechu osoby

zadržené ve smyslu § 76 odstavce 3 trestního řádu, bylo téhož dne zahájeno trestní stíhání podle § 160 odstavce 1 trestního řádu.

Za přítomnosti obhájce byl s obviněným sepsán protokol o výslechu obviněného, kdy k věci vypovídal a ke skutkům se doznal.

Na základě zjištěných skutečností ve vyšetřování dané věci, navrhovaných důkazů, které zahrnovaly výslech poškozené a svědků, vyhodnocení zajištěných dat z mobilních telefonů, tabletu a účtů na sociálních sítích a dalších, byl policejním orgánem sepsán návrh na podání obžaloby podle § 166 odstavce 3 trestního řádu proti obviněnému a tento návrh byl doručen okresnímu státnímu zastupitelství v Pelhřimově. Obžalovaný poté stanul před soudem, který v případu přečinu zneužití dítěte k výrobě pornografie podle § 193 odstavce 1 trestního zákona a přečinu ohrožování výchovy dítěte podle § 201 odstavce 1 trestního zákona rozhodl, že obžalovaný je vinen a vydal jménem republiky odsuzující rozsudek.

I tento případ, kde bylo podáno trestní oznámení na neznámého pachatele, se podařilo objasnit. Pachatel používal ke komunikaci s poškozenou uživatelský profil na sociální síti facebook se svým celým jménem. Při komunikaci nevyužíval žádné služby pro skrytí v síti internet a přístupy realizoval přes data mobilního operátora ve svém mobilním telefonu. Tyto skutečnosti ve velké míře dopomohly k jeho ustanovení.

Rozhovor s vyšetřovatelem

Tento rozhovor byl proveden se zkušeným policistou zařazeným na Oddělení obecké kriminality Policie ČR Pelhřimov, který vyšetřoval výše uvedený trestní spis a zpracovává trestní spisy stejného nebo podobného charakteru. U policie působí již 21 let a z toho 10 let jako vyšetřovatel.

Otázka č.1: Jak často se setkáváte s trestnými činy mravnostního charakteru, tedy například zneužití dítěte k výrobě pornografie dle § 193 trestního zákona?

Odpověď: Vyšetřuji většinou pouze případy mravnostního charakteru, takže se s tímto typem trestné činnosti setkávám velmi často.

Otázka č.2: Když porovnáte svou dlouholetou praxi v dané problematice, jaký je váš názor na tuto trestnou činnost? Je tato trestná činnost na ústupu, či vzestupu a z jakého důvodu?

Odpověď: Určitě na vzestupu. Když si zpětně vybavím počet případů z minulosti, tak jich mnoho nebylo. S nástupem internetu se toto výrazně změnilo a přibylo případů neobjasněných. Pachatelům nahrává anonymita internetu.

Otázka č.3: Jsou si tyto trestné činy něčím podobné, nebo jsou jednání pachatelů zcela odlišná?

Odpověď: Řekl bych, že je to hodně podobné. Pachatelé kontaktují oběti prostřednictvím sociálních sítí, nějakou dobu si s nimi píšou, získávají důvěru a následně vyžadují zasílání fotografií nebo videí s pornografickou tématikou. A to pouze v tom lepším případě. Máme i případy, kdy se pachatel chtěl s obětí setkat osobně nebo ji vydíral.

Otázka č.4: Vedete si nějakou statistiku ohledně věku pachatelů, kteří páchají tuto trestnou činnost?

Odpověď: Nevedu. Nemám na to čas a teď si nevybavím, která věková hranice převažuje.

Otázka č.5: Jaký máte názor k páchání této trestné činnosti opakovaně, tzv. recidivu?

Odpověď: Jedná se určitě o velmi závažnou trestnou činnost a konkrétní případy by měly být vždy řádně prošetřeny, aby se neopakovaly a pachatel byl potrestán.

Otázka č.6: Z Vašich zkušeností v rámci prověřování, konkrétně při prvním setkání s podezřelými při podání vysvětlení, doznávají se osoby samy k trestné činnosti a spolupracují?

Odpověď: Ve většině případů ano, protože máme většinou již dostatek důkazů získaných operativně pátrací činností, v rámci předchozího prověřování a z domovních prohlídek.

Otázka č.7: Jaké bývají rozsudky za tyto trestné činy? Vybavujete si tresty, které byly pachatelům soudem uloženy?

Odpověď: Nesleduji to. Vykonám svoji práci a více neřeším z důvodu, že by mě to nejspíše demotivovalo.

Otázka č.8: Zhlédl jste dokument „V síti“, který se zabývá touto problematikou?

Odpověď: Vím, o jaký dokument se jedná, ale neviděl jsem ho.

7.4 Analýza a komparace případů, statistiky

U všech případů byly oběti kontaktovány, pravděpodobně náhodně dle profilových fotografií, prostřednictvím sociálních sítí. Konkrétně se jednalo o sociální sítě whatsapp, facebook a instagram. I přesto, že se pokaždé jednalo o jinou sociální síť, možnosti pachatele, jak kontaktovat oběť, jsou ve všech případech totožné. Pouze s rozdílem, že u sociálních sítí facebook a instagram si může pachatel předem zobrazit, pokud jsou uživatelské profily veřejné a otevřené, fotografie uživatele, které na daných profilech sdílí. U sociální sítě whatsapp má pachatel k dispozici k nahlédnutí pouze jednu profilovou fotografii. I přes drobné rozdíly, lze u všech sítí odeslat oběti zprávu a dále jen čekat, zda zareaguje a odpoví. Všechny tyto sítě provozuje a spravuje společnost Meta Platforms Ltd. sídlící v USA. Tedy vyžadování údajů k účtům lze realizovat pouze na základě příkazu soudce podle § 88a odst. 1 trestního řádu a potřebné informace policejní orgán získá v průměru kolem 2 měsíců od sepsání žádosti.

Ve všech případech byly zahájeny úkony trestního řízení pro přečin podle § 193 odstavce 1 trestního zákona a u případu „Mojmír“ dále pro přečin ohrožování výchovy dítěte podle § 201 odstavce 1 písm. a) trestního zákona. Právní kvalifikace skutků se již v rámci celého trestního řízení nezměnila, neboť nebyly zjištěny skutečnosti, které by vedly k její změně nebo rozšíření.

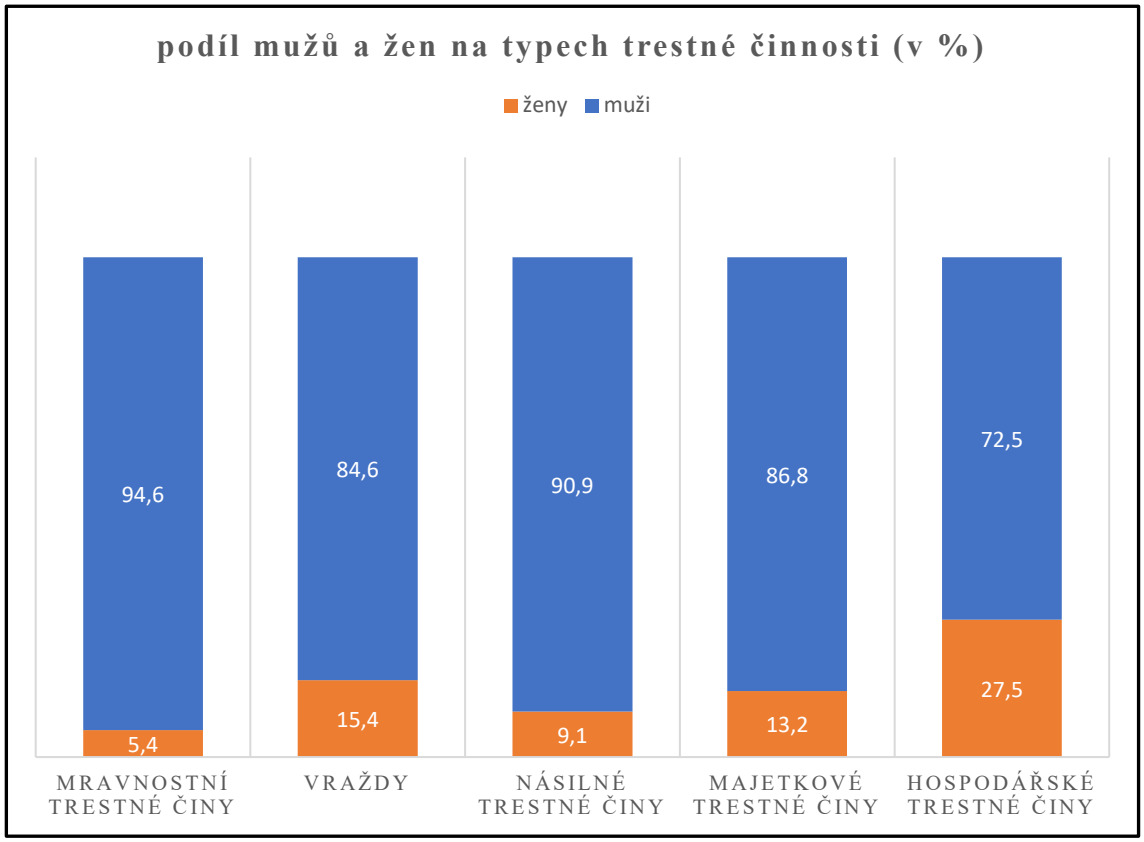
Samotný charakter trestné činnosti byl u prověřovaných případů obdobný. Pachatelé kontaktovali své oběti prostřednictvím sociálních sítích a po předchozí běžné komunikaci přešli do komunikace se sexuálním podtextem a vyžadovali zasílání intimních fotografií nebo videí, jak je z úryvků této komunikace patrné. U případu „Mojmír“ je nutné zmínit, že pachatel měl na svém účtu na facebooku profilovou fotografii, kde byl vyobrazen chlapec ve věku kolem 15-17 let a to z důvodu, aby lépe navázal kontakt s dívkami obdobného věku. Ve všech případech i samotní pachatelé zasílali obětem své intimní fotografie nebo videa. Během komunikace nedošlo k žádnému vydírání oběti nebo případnému osobnímu setkání, fyzickému kontaktu nebo pohlavnímu zneužití.

U všech skutků byly obětmi nezletilé osoby ženského pohlaví, přičemž oběti ve věku 8-15 let ve statistikách dominují, jak je zřejmé z níže uvedeného grafu číslo 7. Toto zjištění je velmi alarmující, neboť je zřejmé, že útoky sexuálních predátorů jsou ve většině případů cíleny na ty nejzranitelnější, tedy děti. A to i přesto, že sociální sítě jsou pro tuto věkovou hranici oficiálně zakázané a děti by neměly mít k těmto sítím přístup. Naopak

pachatelé byly vždy osoby mužského pohlaví v širší věkové kategorii od mladistvých až po dospělé osoby. Podíl mužů a žen na různých typech trestné činnosti je vyobrazen na grafu číslo 3, ze kterého je zřejmé, že u kriminality mravnostní je podíl u žen pouhých 5.4%.

Jak je dále patrné, největší podíl na všech typech trestných činů mají muži. Největší podíl žen oproti mužům je u hospodářských (27,5 %), majetkových trestných činů (13,2 %) a vražd (15,4 %). Naopak muži výrazněji převažují u násilných (90,9%) a mravnostních (94,6 %) trestných činů, kde je podíl žen minimální.

Graf 3: podíl mužů a žen na typech trestné činnosti[81]



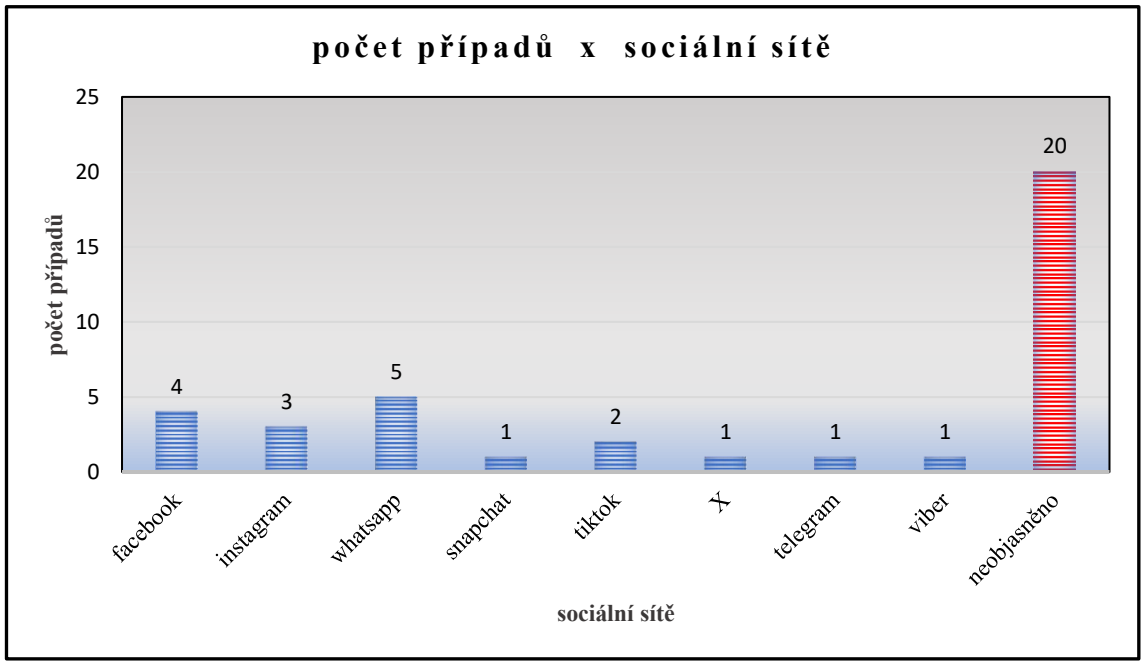
Analýzou všech tří případů nebylo zjištěno, že by pachatelé využili nějakých služeb nebo prostředků ke skrytí své identity v kyberprostoru. Mohlo to být z důvodu jejich neznalosti v oblasti informačních technologií nebo nízkého věku či intelektu. Všechny případy jen potvrzují současné statistky Policie ČR.

[81] Zdroj: vnitřní informační systémy a evidence Policie ČR.

Statistika počtu trestných činů, provinění a činů jinak trestných

Níže uvedený graf číslo 4 zobrazuje počet trestných činů, provinění nebo činů jinak trestných z hlav II, III a IV trestního zákona, které byly evidovány na Policii ČR kraje Vysočina, Územní odbor Pelhřimov za období od roku 2018 – 2023 a pachatelé k jejich páchání využili, zcela nebo z části, sociální sítě. V grafu číslo 4 a dalších jsou zahrnuty i všechny tři případy z praktické části této práce.

Graf 4: počet případů trestných činů a provinění za období od roku 2018–2023[82]



Z grafu vyplývá, že z celkového počtu oznámených případů, zůstala více jak polovina neobjasněna a musela být odložena podle § 159a odstavce 5 trestního řádu. Důvodem je anonymita kyberprostoru, tedy různých anonymních uživatelských účtů, anonymizačních služeb a složité spolupráci ze strany zahraničních subjektů s OČTŘ. Z praxe je známo, že provozovatelé sociálních sítí tiktok (Čína) a telegram (Rusko), neposkytují OČTŘ žádné informace.

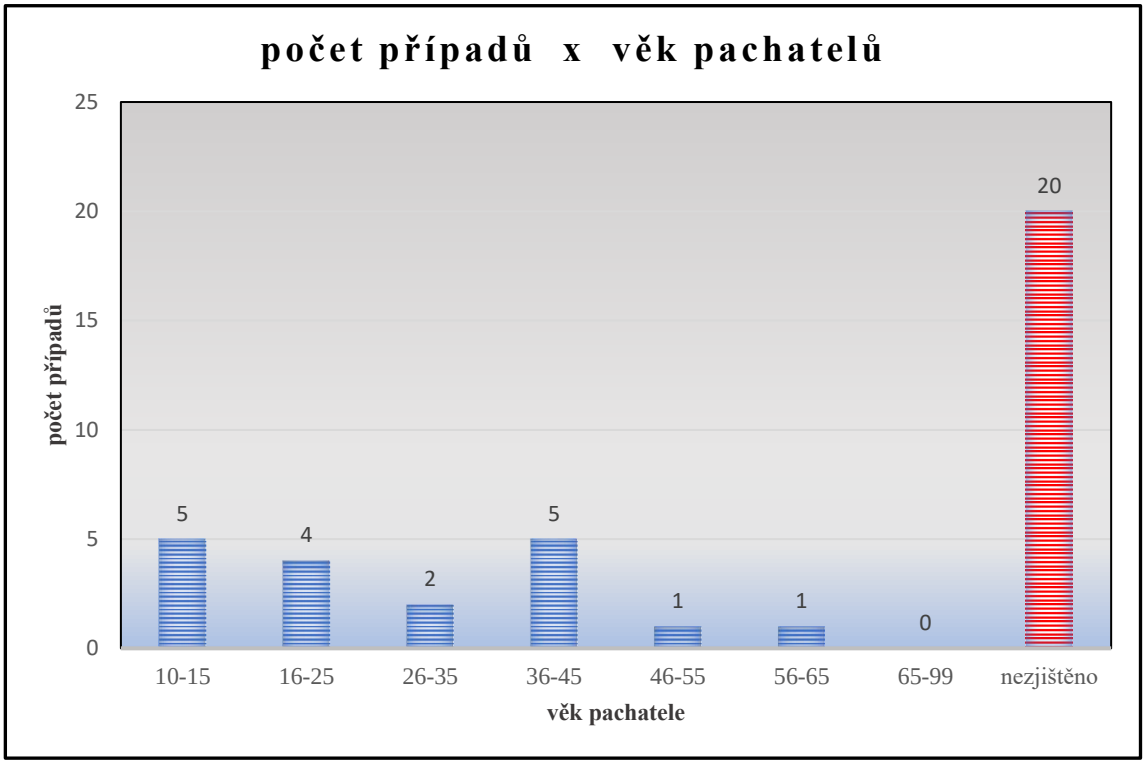
Statistika věku pachatelů

Graf číslo 5 vyobrazuje počet trestný činů nebo provinění ve vztahu k věku pachatelů. Z grafu je patrné, že k trestné činnosti mravnostního charakteru se uchylují hlavně osoby ve věku nezletilých a mladistvých, tedy mládež a osoby ve věku blízkých věku mladistvých. Další rizikovou skupinou jsou osoby ve věku mezi 36-45 let. Ze statistik Policie ČR vyplývá, že sexuálním predátorem, který své oběti hledá a oslovuje

[82] Zdroj: vnitřní informační systémy a evidence Policie ČR.

prostřednictvím internetu a sociálních sítí, je nejčastěji nezaměstnaný, rozvedený nebo svobodný muž ve věku kolem 40 let. Data v grafu obsahují pouze pachatele mužského pohlaví, neboť žádný z objasněných případů nebyl spáchán ženou. Sloupec nezjištěno vychází z dat neobjasněných skutků, u kterých nebyl zjištěn žádný poznatek k totožnosti pachatele.

Graf 5: věk pachatelů ve srovnání s počtem případů za období od roku 2018–2023[83]

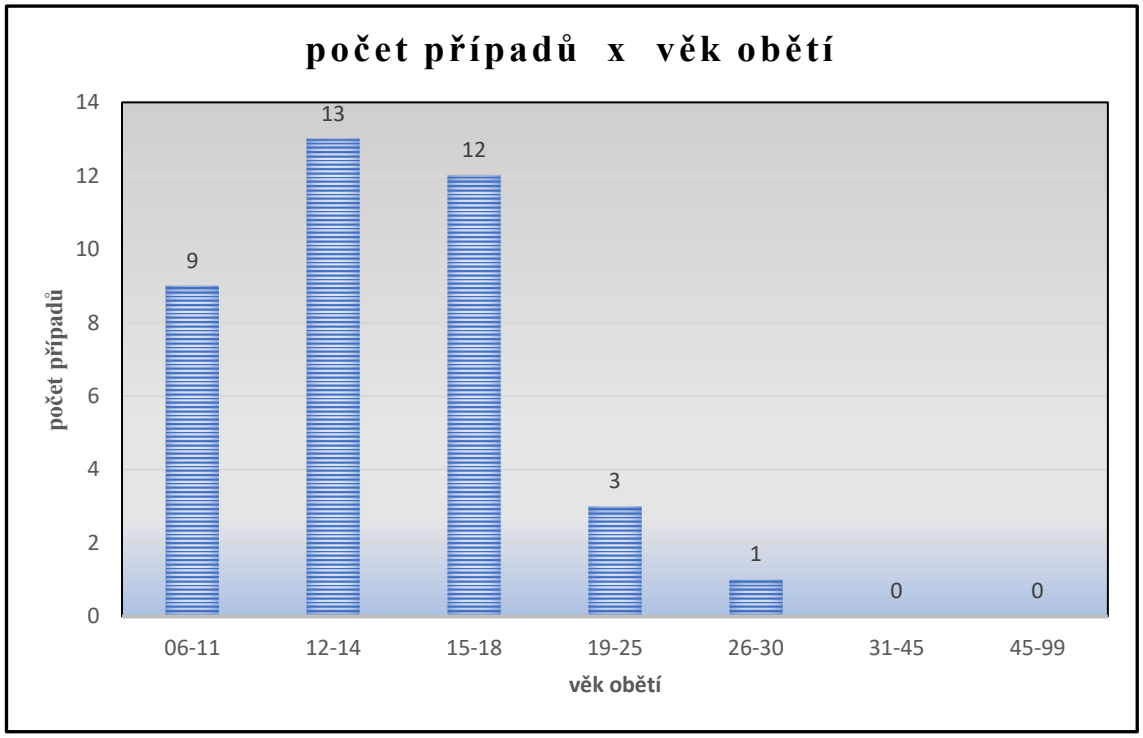


Statistika věku obětí

Graf číslo 6 zobrazuje statistiku věku obětí, na kterých byly spáchány trestné činy, provinění nebo činy jinak trestné mravnostního charakteru. Z grafu je zřejmé, že obětmi jsou nejčastěji nezletilé osoby ve věku mezi 6-14 let a osoby mladistvé ve věku mezi 15-18 let. Ve všech případech se jednalo o osoby ženského pohlaví. Tyto případy potvrzují statistiky Policie ČR, tedy že rizikovou skupinou jsou nejčastěji dívky ve věku kolem 12 let.

[83] Zdroj: vnitřní informační systémy a evidence Policie ČR.

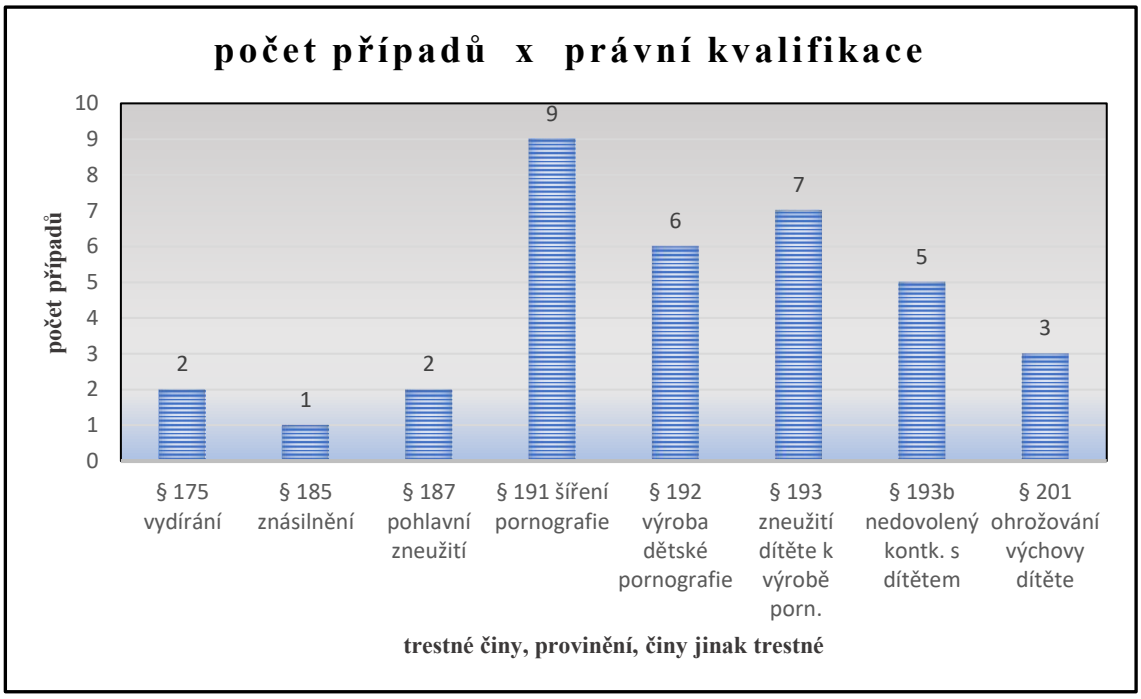
Graf 6: věk pachatelů ve srovnání s počtem případů za období od roku 2018–2023[84]



Statistika trestných činů, provinění, činů jinak trestných podle právní kvalifikace

Graf číslo 7 vyobrazuje právní kvalifikace trestných činů, provinění a činů jinak trestných, které byly za uvedené období prověřovány a souvisely s užitím sociálních sítí.

Graf 7: počet TČ a jejich právní kvalifikace za období od roku 2018-2023[85]



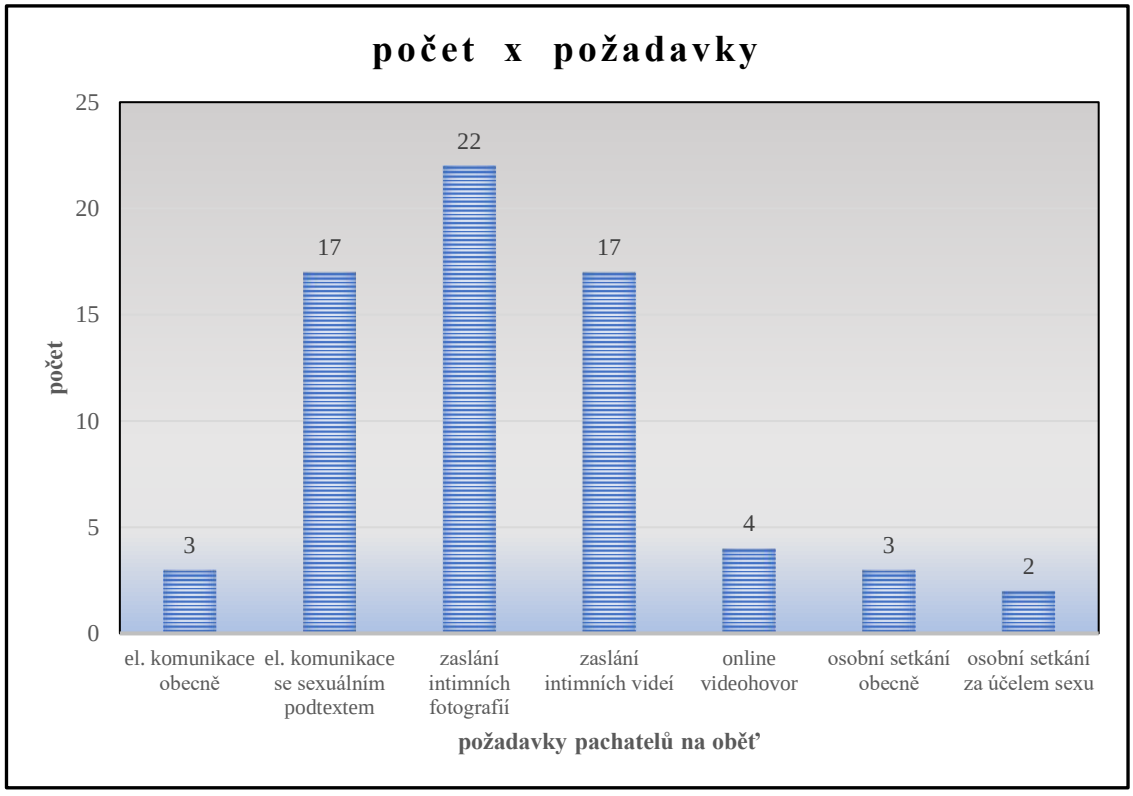
[84] Zdroj: vnitřní informační systémy a evidence Policie ČR.
[85] Tamtéž.

Z grafu je patrné, že nejčastějšími jsou šíření pornografie, výroba a jiné nakládání s dětskou pornografií a zneužití dítěte k výrobě pornografie.

Statistika požadavků pachatelů na oběť

Graf číslo 8 zobrazuje požadavky pachatelů po obětech, které vyplynuly ze vzájemné konverzace. Ve většině případů šlo o jejich kombinaci, tedy například žádosti o běžné dopisování, až po následný nátlak na oběť, aby zaslala intimní fotografie. Pachatelé se ve většině případů snažili z obecné konverzace a samotného navázání kontaktu, přejít do konverzace se sexuálním podtextem a získat od oběti intimní fotografie nebo videa. V několika případech pachatelé požadovali osobní setkání s obětí a ve dvou případech si domlouvali pohlavní styk. Ve čtyřech případech byly vyžadovány online video-hovory, ve kterých naváděli oběti k provádění různých sexuálních praktik, obnažování nebo masturbaci. Statistika byla zpracována na základě vyhodnocení a analýzy zajištěných elektronických dat a konverzací.

Graf 8: počet konkrétních požadavků pach. po obětech v příp. za období od 2018-2023[86]



[86] Zdroj: vnitřní informační systémy a evidence Policie ČR.

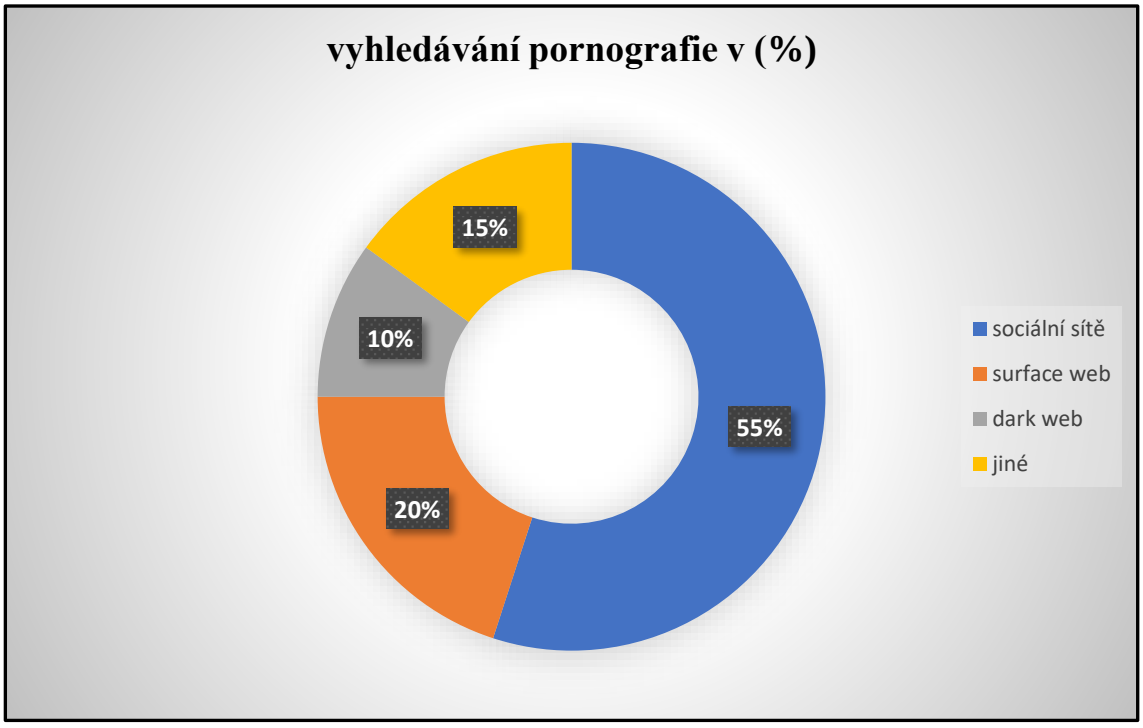
7.5 Rozhovory s vyšetřovateli

V rámci policejních výslechů jsou osobám prověřovaným nebo později v rámci trestního řízení osobám obviněným, pokládány různé otázky k objasnění dané věci. Pokud tyto osoby spolupracují a vzdají se práva nevypovídat, vyšetřovatel v protokolu uvede několik důležitých základních otázek, které slouží ke zjištění, kde a jakým způsobem pachatel získával dětskou pornografii nebo obecně jakoukoliv pornografii, jakým způsobem byla oběť kontaktována, jaké prostředky k tomu byly využity, zda tak činil opakovaně a zda došlo k případnému osobnímu setkání s obětí. Případně položí další otázky, které z výslechu vyplynou.

Níže uvedené statistiky zpracované do grafů a tabulky, vyobrazují odpovědi pachatelů na zmiňované otázky, kdy tyto odpovědi byly zjištěny z realizovaných rozhovorů s vyšetřovateli daných případů a policejních materiálů.

Statistika vyhledávání pornografie na internetu

Graf 9: vyhledávání pornografie na internetu dle výpovědí pachatelů[87]

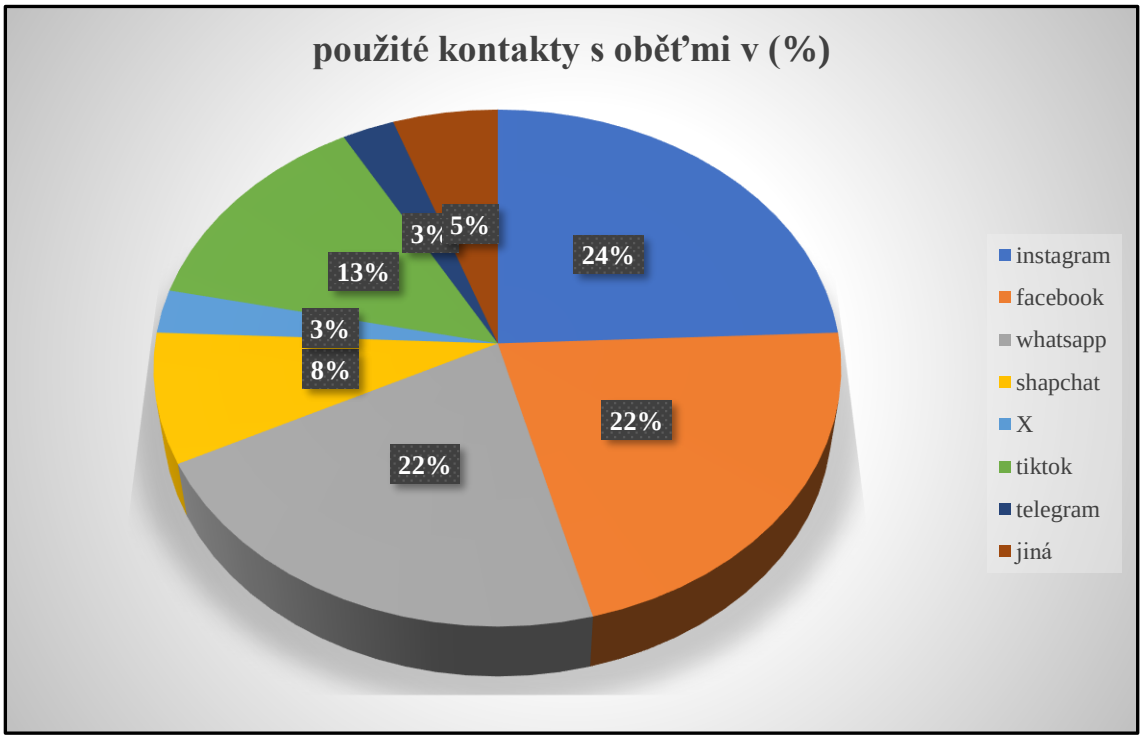


[87] Zdroj: rozhovory s vyšetřovateli a trestní spisy Policie ČR.

Z grafu číslo 9 je patrné, že nejčastěji jsou využívány sociální sítě s 55%. A to vzhledem k jejich dostupnosti a obrovskému počtu uživatelů a tedy potencionálních obětí. V 20% je využíván klasický „surface web“, tedy běžný indexovaný internetový prostor, kde lze pornografii vyhledávat za pomoci klasických internetových vyhledávačů. Dále v 10% „dark web“ a v 15% jsou použity jiné způsoby, jako například šíření a získávání pornografie přes emailové schránky, v diskuzních fórech, v rámci chatů počítačových her a dalších.

Statistika použitých sociálních sítí ke kontaktům s oběťmi

Graf 10: použité sociální sítě pro kontakt s oběťmi dle výpovědi pachatelů[88]



Z grafu číslo 10 je vidět, že v sociálních sítích dominují instagram, facebook a whatsapp s více jak 20% a s 13% síť tiktok. Ostatní sítě nejsou hojně využívány, neboť i mládež je používá minimálně a lze tím jen potvrdit oblíbenost sociálních sítí viz obrázek číslo 2 v teoretické části práce.

Statistika použitých služeb ke skrytí uživatele v internetu

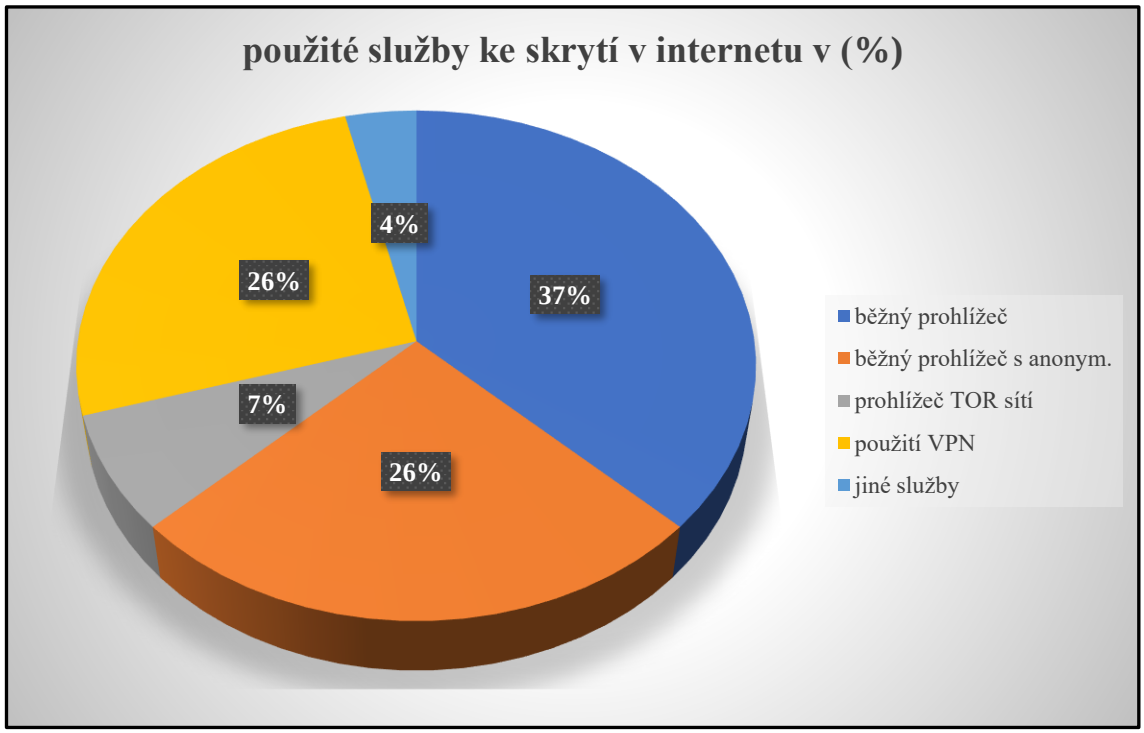
Níže uvedený graf číslo 11 vyobrazuje statistiku užití různých prostředků a služeb pro skrytí uživatele v internetu, které byly v rámci výpovědí prověřovaných osob zjištěny. Nejčastěji v 37% byl uváděn běžný webový prohlížeč, bez využití jakýchkoliv služeb pro

[88] Zdroj: rozhovory s vyšetřovateli a trestní spisy Policie ČR.

skrytí identity uživatele a v 26% se zapnutou volbou anonymního prohlížení webových stránek na internetu. I ve všech třech případech, které byly publikovány v praktické části této práce, pachatel použil pouze běžný webový prohlížeč a tato skutečnost tedy dopomohla k jeho brzkému ustanovení.

V 26% byla uváděna nebo v rámci zajišťování a vyhodnocení dat zjištěna, VPN služba, která v kombinaci s běžným webovým prohlížečem, zaručuje dostatečnou anonymitu. Pouze v 7% byl použit webovým prohlížeč k připojení do TOR sítí, webové stránky s příponou .onion a na "dark web", což plně koresponduje s hodnotami v grafu číslo 9.

Graf 11: použité služby pro skrytí uživatele v internetu[89]



Statistika doplňujících odpovědí

Pro ucelený náhled na chování osob páchající mravnostní trestnou činnost bylo, z informací z policejních výslechů a po konzultacích s vyšetřovateli, vybráno několik odpovědí na otázky, které byly pachatelům při výsleších položeny. Pro přehlednější zpracování byly odpovědi upraveny do variant obecného ano/ne.

Negativním zjištěním je, že až v 72% jsou oběti kontaktovány opakovaně a ve větším počtu a ze strany pachatelů nejsou tedy útoky zaměřeny pouze na jednu konkrétní

[89] Zdroj: rozhovory s vyšetřovateli a trestní spisy Policie ČR.

oběť, ale v reálném čase je obětí osloveno mnohem více. Neomezené možnosti internetu jsou zde jasně patrné. Za pozitivní zprávu je možné považovat pouze 8% osobních setkání s oběťmi, z čehož je zřejmé, že útoky jsou ve většině případů realizovány pouze v prostředí internetu.

Pro připojení do internetu jsou z informačních technologií nejčastěji používány mobilní telefony a to vzhledem k jejich současným funkcím, dostupnosti a kvalitě, přičemž plně nahrazují osobní počítače, fotoaparáty, videokamery a další elektronická zařízení.

Přístup do interentové sítě je ve většině případů realizován přes poskytovatele internetu mobilních operátorů (ISP) za využití mobilní dat. U přístupů přes různé wifi sítě jsou preferovány jakékoliv dostupné wifi sítě mimo bydliště, oproti wifi sítím domácím. Vzhledem k současné dostupnosti internetu, je toto logická volba, která navíc umožňuje skrytí identity uživatele, aniž by bylo nutné využít některou z anonymizačních služeb.

Tabulka 4: odpovědi pachatelů na doplňující otázky[90]

Otázky	**Odpověď**	
doplňující otázky	**ANO**	**NE**
opakované kontaktování obětí	72%	28%
osobní setkání	8%	92%
použitá zařízení k připojení do internetu		
mobilní telefon	90%	10%
osobní počítač	22%	78%
jiné	35%	65%
poskytovatelé připojení k internetu		
domácí internet/wifi	35%	65%
mobilní data	75%	25%
jiné připojení/wifi mimo bydliště	65%	35%

[90] Zdroj: rozhovory s vyšetřovateli a trestní spisy Policie ČR.

Závěr

Tato bakalářská práce zabývá problematikou dětské pornografie, její dostupnosti na sociálních sítích a možností prevence. Může odpovědět na otázku, jak snadné a dostupné je kontaktovat potencionální oběť, získat pornografický materiál z kyberprostoru a zda si děti a rodiče tato rizika uvědomují.

V teoretické části je vysvětleno čeho všeho se může kybernetická kriminalita týkat, jakým způsobem souvisí se sociálními sítěmi a dětskou pornografií a kde je nejčastěji vyhledávána a šířena. První skupinou mohou být sexuální predátoři, kteří přes sociální sítě své oběti cíleně kontaktují a v rámci následných elektronických konverzací pornografii získávají a druhou skupinou mohou být samotné děti, které pornografii vytváří, sdílí a zasílají si ji vzájemně mezi svými vrstevníky.

V kraji Vysočina bylo za období od roku 2018 do roku 2023 prověřováno celkem 38 případů trestné činnosti mravnostního charakteru páchané na mládeži. Jednalo se zejména o trestné činy šíření pornografie, výroba a jiné nakládání s dětskou pornografií a zneužití dítěte k výrobě pornografie. Dále také trestné činy ohrožování výchovy dítěte nebo vydírání. Uvedené trestné činy úzce souvisely s problematikou kybergroomingu, sextingu nebo kyberšikany, kdy tyto termíny byly rovněž v teoretické části práce vysvětleny a tím bylo dosaženo vedlejšího cíle práce. Nutno podotknout, že zjištěné a nahlášené případy jsou pouze vrcholem ledovce, neboť kybernetická kriminalita je latentní a OČTŘ se o většině skutků nedozví.

Praktická část práce pojednává o třech reálných případech z praxe. Provedenou analýzou a komparací těchto případů bylo zjištěno, že scénář, jak kontaktovat oběť, je ve své podstatě vždy obdobný a jeho provedení velmi jednoduché. Pachatel může ve velmi krátké době kontaktovat značné množství potencionálních obětí, na veřejně dostupném internetu, za použití veřejně dostupných a legálních služeb a procento jeho úspěšnosti je tedy velmi vysoké. Tyto informace mohou být přínosem pro rodiče a mohou dopomoci k následné prevenci a snížení viktimnosti jejich dětí.

Pokud by informační technologie v kombinaci s celosvětovou sítí internet sloužily pouze ke komunikaci mezi lidmi, ke zjišťování a předávání důležitých informací, legálnímu obchodování, sdílení dat apod., bylo by vše ideální. Informační technologie pomáhají člověku ve velkém množství jeho činností a ulehčují mu práci. Informační

technologie vykazují velmi rychlý rozvíjející se trend. Bohužel s tímto rychlým nástupem počítačů a dalších informačních technologií vzniká i globální problém ve formě kriminality páchané v kyberprostoru. Nejzávažnějším problémem je zneužívání dětí a šíření dětské pornografie ve spojitosti se sociálními sítěmi a dále postupné zdokonalování pachatelů páchajících kybernetickou kriminalitu. Podle trestního řádu má obviněný právo nahlédnout do kompletního spisového materiálu a činit si výpisky, záznamy a kopie. Pachatelé tedy snadno zjistí, jakým způsobem byli odhaleni, jaké mají OČTŘ postupy a technické možnosti a lze říci, že se tímto učí dané problematice. V případě následné recidivy mohou o to více ztížit OČTŘ jejich odhalení.

Je tedy zcela jisté, že v budoucnosti bude kybernetická kriminalita stále na vzestupu a způsoby páchaní trestné činnosti se budou neustále rozvíjet a zdokonalovat. Rizika pro děti a mladistvé budou v síti internet stále větší, a to i díky používání rozsáhlého počtu sociálních sítí. Vzhledem ke skutečnosti, že sociální sítě vyvíjí různé společnosti po celém světě, nemají jednotná pravidla a použitý software na koncových zařízeních je velmi různorodý, bude vážným problémem následné vyžadování informací od zahraničních subjektů a samotné zajišťování elektronického obsahu. Obsahu, který je nutné v určitých případech zajistit ihned, v rámci neodkladných a neopakovatelných úkonů. Některé aplikace, zpřístupňující danou sociální síť, jsou programovány s důrazem na anonymitu uživatele a neumožňují žádný export použitých dat, což může být pro OČTŘ velkým problémem ve vyšetřování.

Bezesporu mají sociální sítě i mnoho výhod a pozitiv, ale nevýhody a negativa převládají. Pro děti a mladistvé mohou být velkým rizikem v oblasti zneužívání, šíření pornografie, kyberšikany ve školních zařízeních i mimo ně a v neposlední řadě celkového narušení sociálních vztahů ve společnosti. Čím dál více a od stále nižšího věku používají děti sociální sítě a nechávají se “pohltit“ virtuálním světem. O to více strádá jejich svět reálný. Je tedy hlavně na rodičích, aby dětem vše vysvětlili, poučili je o případných rizicích a nastavili jasně daná pravidla. Otázkou ale zůstává, kdo poučí samotné rodiče, kteří sami nadmíru využívají sociální sítě, sdílejí fotografie svých dětí a tato závažná rizika si rovněž neuvědomují.

Seznam použitých zdrojů

Literární zdroje

1. BLATNÍKOVÁ, Š. *Pachatelé komerčního sexuálního zneužívání dětí*. Vyd. KUFR s.r.o. 2009. 133 s. ISBN 978-80-7338-091-5
2. BLINKA, L. *Online závislosti*. Grada 2016. 200 s. ISBN 978-80-210-7975-5
3. DOČEKAL, D. a kol. *Dítě v síti*. Mladá fronta 2019. 208 s. ISBN 978-80-204-5145-3
4. DOUGLAS, T., BRIAN, D. L. *Cybercrime*. Taylor & Francis Ltd 2000. 314 s. ISBN 978-04-152-1326-4
5. ECKERTOVÁ, L., DOČEKAL D. *Bezpečnost dětí na internetu.* Computer press 2013. 224 s. ISBN 978-80-251-3804-5
6. HOLLÁ, K. *Sexting a kyberšikana.* Vyd. IRIS 2016. 166 s. ISBN 978-80-8153-061-6
7. CHROMÝ, J. *Kriminalita páchaná na mládeži*. Linde s.r.o. 2010. 74 s. ISBN 978-80-7201-825-3
8. JIROVSKÝ, V. *Kybernetická kriminalita.* Praha: Grada, 2007. 288 s. ISBN 978-80-247-1561-2
9. KOPECKÝ, K. a kol. *Rizikové chování českých a slovenských dětí v prostředí internetu*, 1. vyd. 2015. 171 s. ISBN 978-80-244-4861-9
10. KOPECKÝ, K., SZOTKOWSKI, R. *České děti v kybersvětě (výzkumná zpráva)*. O2 Czech Republic & Univerzita Palackého v Olomouci, 2019. 32 s.
11. KOPŘIVA, P., a kol. *Respektovat a být respektován*. Kroměříž: Spirála, 2008. 286 s. ISBN 978-80-904030-0-0.
12. KOŽÍŠEK, M., PÍSECKÝ V. *Bezpečně na internetu: průvodce chováním ve světě online.* Praha, Grada 2016. 176 s. ISBN 978-80-247-5595-3
13. KRČMÁŘOVÁ, B. *Děti a online rizika: sborník sudií.* 1. vyd. Praha. Sdružení linka bezpečí, 2012. 178 s. ISBN 978-80-904920-2-8
14. KUCHTA, J., VÁLKOVÁ, H. a kol. *Základy kriminologie a trestní politiky*. 1. vydání. Praha: C. H . Beck, 2005. 636 s. ISBN 978-80-7400-429-2
15. MULLER, M. *Jak chránit děti před pornografií na internetu*, 1. vyd. 2014. 168 s. ISBN 978-80-262-0694-1
16. NOVOTNÝ, O., ZAPLETATL, J., a kol. *Kriminologie*. 3.vyd. Praha: ASPI-Wolters Kluwer 2008. 527 s. 978-80-735-7377-5

17. PAVLOVSKÝ, P. a kol. *Soudní psychiatrie a psychologie*, Praha: Grada, 4. aktualizované vyd. 2004. 240 s. ISBN 978-80-247-4332-5
18. SMEJKAL, V. *Kybernetická kriminalita.* 3. rozšířené a aktualizované vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. 1158 s. ISBN 978-80-7380-849-5
19. ŠEVČÍKOVÁ A., BLINKA L. a kol. *Děti a dospívající online.* 1. vyd. Grada 2014. 184 s. ISBN 978-80-247-5010-1
20. TOMÁŠEK, J. *Úvod do kriminologie: Jak studovat zločin.* Praha: Grada 2010. 216 s. ISBN 978-80-247-2982-4
21. VANÍČKOVÁ, E. *Cesta za poznáním šikany, šikanování mezi dětmi.* Praha: Česká společnost na ochranu dětí - Růžová linka, 2002, 11 s. ISBN 80-238-9448-X
22. VELIKOVSKÁ, M. *Psychologie obětí trestných činů.* 1. vydání. Grada: 2016. 168 s. ISBN: 978-80-247-4849-8
23. WEISS, P. a kol. *Sexuologie.* 1. vydání. Grada: 2010. 744 s. ISBN 978-80-2472-492-8

Elektronické zdroje

1. AMI Digital Index 2021. In: amidigital.cz [online]. 2024. [cit. 2024-01-03]. Dostupné z WWW: <https://amidigital.cz/ami-digital-index-2021>
2. CAHLÍK, V., JINDRA, V. *Co je vlastně umělá inteligence.* In: aidetem.cz [online]. 2022. [cit. 2023-12-10]. Dostupné z WWW: <https://aidetem.cz/obecny-uvod-do-umele-inteligence/co-to-vlastne-je-ai>
3. Kyberprostor. In: PortálDigi.cz [online]. 2019. [cit. 2023-12-07]. Dostupné z WWW: <https://www.kurzy.portaldigi.cz>
4. KOPECKÝ, K. @ E-Bezpečí. *Kybergrooming.* In: kybergrooming.cz [online]. 2007-2021. [cit. 2023-11-30]. Dostupné z WWW: <https://www.kybergrooming.cz>
5. KOPECKÝ, Kamil. *Umělou inteligencí generovaná pornografie způsobí řadu problémů, zneužívána bude k útokům na děti i dospělé.* E-Bezpečí, roč. Olomouc: Univerzita Palackého, 2023. ISSN 2571-1679. Dostupné z WWW: <https://www.e-bezpeci.cz/index.php?view=article&id=3636>

6. Nová příručka radí, jak se chovat na sociálních sítích. In: msmt.cz [online]. MŠMT 2013-2024. [cit. 2024-01-08]. Dostupné z WWW: <https://www.msmt.cz/nova-prirucka-radi-jak-se-chovat-na-socialnich-sitich>
7. Policie ČR, *Kyberkriminalita* [online]. [cit. 2023-11-06]. Dostupné z WWW: <https://www.policie.cz/clanek/kyberkriminalita.aspx>
8. Sociální sítě. In: Sitevhrsti.cz [online]. [cit. 2023-11-25]. Dostupné z WWW: <https://www.sitevhrsti.cz/socialni-site>
9. Úmluva o počítačové kriminalitě. In: eur-lex.europa.eu [online]. 2023. [cit. 2024-01-17]. Dostupné z WWW: <https://eur-lex.europa.eu/CS/legal-content/summary/convention-on-cyberkrime.html>

Legislativní dokumenty

1. ČESKO, Zákon č. 40/2009 Sb., trestní zákon, ve znění pozdějších předpisů. In: *Sbírka zákonů České republiky*. 2009. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2009-40>
2. ČESKO, Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Sbírka zákonů České republiky*. 2014. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2014-181>
3. ČESKO, Sdělení č. 104/2013 Sb. m.s.*, sdělení Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě,* oddíl 3, článek 9. In: Zákony pro lidi [online]. Praha: ©AION CS, 2010–2024. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2013-104>

Ostatní zdroje

Kromě výše uvedených zdrojů byly při zpracování bakalářské práce využity následující materiály:

- databáze, evidence a vnitřní informační systémy Policie ČR
- trestní spisy - na základě povolení ředitele ÚO PČR Pelhřimov
- vlastní zdroje
- V síti [dokument]. Režie CHALUPOVÁ, B., KLUSÁK, V. ČR: Česká televize, 2020

Seznam zkratek

AI – Umělá inteligence **(**(Artificial Intelligence)

GAN – Generativní konvoluční sítě (Generative Adversarial Networks)

IMEI – Identifikační číslo mobilního telefonu (International Mobile Equipment Identity)

IP – síťový protokol (Internet Protocol)

ISP – poskytovatel internetového připojení (Internet Service Provider)

NCOZ – Národní centrála proti organizovanému zločinu Policie ČR

OAKK – Oddělení analytiky a kybernetické kriminality Policie ČR

OČTŘ – Orgány činné v trestním řízení

OOK – Oddělení obecné kriminality Policie ČR

OSPOD – Orgán sociálně-právní ochrany dětí

PPP – Pokyn policejního prezidenta o plnění některých úkolů policejních orgánů Policie ČR v trestním řízení

SIM – Zařízení k identifikaci účastníka v telefonní síti (Subscriber Identity Module)

SKPV – Služba kriminální policie a vyšetřování

TOR – Softwarový systém (The Onion Router)

UFED – Sofwarový systém k extrakci a analýze dat (Universal Forensics Extraction Device)

ÚZČ – Útvar zvláštních činností Policie ČR

VPN – Virtuální privátní síť (Virtual Private Network)

ZÚTŘ – Zahájení úkonů trestního řízení

Seznam tabulek a grafů

Seznam příloh

Přílohy

Přílohy 1 - Souhlas s využitím spisových materiálů pro účely bakalářské práce

Příloha číslo 1 - Souhlas s využitím spisových materiálů pro účely bakalářské práce

por. Radek BUZEK, DiS.
komisař
Služebně zařazen u Policie ČR, KŘP kraje Vysočina, Územní odbor Pelhřimov, oddělení analytiky a kybernetické kriminality, Pražská 1738, Pelhřimov.

Žádost o udělení souhlasu s využitím spisových materiálů pro účely bakalářské práce

Tímto žádám o udělení souhlasu k využití spisových materiálů pro účely bakalářské práce, které jsou archivovány u Policie ČR, KŘP kraje Vysočina, Územní odbor Pelhřimov, oddělení obecné kriminality. Konkrétně budou k BP užity spisové materiály vedené pod č. j.:

KRPJ-121596/TČ-2018-161771
KRPJ-87372/TČ-2019-161771
KRPJ-25594/TČ-2021-161771

Materiály budou užity pro studijní účely, konkrétně pro uvedení třech skutečných případů, zejména popisy skutkových jednání, popisy dílčích úkonů v rámci šetření, prověřování a vyšetřování a skutkový popis rozhodnutí ve věci. Vše bude užito k tématu bakalářské práce: *„Problematika dětské pornografie, její dostupnost na sociálních sítích a možnosti prevence"*. Bakalářská práce je vypracovávána ke studiu na Vysoké škole evropských a regionálních studií, Žižkova tř. 1632, 370 01 České Budějovice. Pro ochranu a zajištění anonymity zúčastněných osob nejsou v praktické části práce uvedena žádná jména, názvy lokalit, či jiné osobní informace, které by vedly k identifikaci konkrétních osob a popisy skutků jsou uvedeny v souladu se zákonnými předpisy na ochranu osobních údajů.

por. Radek BUZEK, DiS.
OEČ 319 623

Souhlas uděluji x neuděluji

plk. Mgr. Petr PETR
ředitel územního odboru PČR Pelhřimov