Západočeská univerzita

Fakulta právnická

Diplomová práce

Kybernetická kriminalita páchaná na dětech

Daniela Podzimková

Plzeň 2024

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci zpracovala samostatně, a že jsem vyznačila prameny, z nichž jsem pro svou práci čerpala způsobem ve vědecké práci obvyklým.

V Praze dne 19.3.2024 ……

Daniela Podzimková

Poděkování

Ráda bych poděkovala panu JUDr. Michalovi Volfovi, za poskytnutí možnosti tuto diplomovou práci pod jeho odborným vedením zpracovat.

Dále bych ráda bych poděkovala panu por. Bc. Radovanovi Hladovi za spolupráci na celé diplomové práci a za poskytnutí rozhovoru. Za rozhovor děkuji i por. Mgr. Janovi Křemenovi. Poděkování také patří kpt. Mgr. Andree Světlíkové za poskytnutí kazuistik k diplomové práci.

Abstrakt

Název diplomové práce:

Kybernetická kriminalita páchaná na dětech

Cíl práce:

Cílem práce je analyzovat problematiku kybernetické kriminality páchané na dětech, zjistit její příčiny, určit jakých trestných činů se pachatelé dopouštějí, zmapovat aktuální situaci a průběh vyšetřování a dokazování.

Metoda:

V diplomové práci jsem zvolila metodu rozhovoru s vyšetřovateli kybernetické kriminality. Závěry z rozhovoru jsem poté shrnula a některé informace jsem použila do následujících kapitol.

Výsledky

Výsledky mé práce analyzovali, jakým způsobem je páchána kybernetická kriminalita na dětech, některé trestné činy, kterých se pachatelé dopouštějí a postup, jakým by měla být prováděna prevence kybernetické kriminality jako ochrany dětí před hrozbami internetu. V rámci rozhovoru byl vylíčen stav aktuální situace zneužívání dětí na internetu a způsob jakým se tato kriminalita vyšetřuje.

Klíčová slova:

Kybernetická kriminalita

Děti

Zneužívání dětí na internetu

Kybergrooming

Dětská pornografie

Kyberšikana

Prevence kybernetické kriminality

Abstract

Title of the theis:

Cybercrime committed against children

Aim of thesis:

The aim of the thesis is to analyze the issue of cybercrime committed against children, to find out its causes, to determine what crimes the perpetrators commit, to map the current situation and the course of investigation and proving.

Method:

In my diploma thesis, I chose the interview method with cybercrime investigators. I then summarized the conclusions from the interview and used some of the information in the following chapters.

Results:

The results of my work analyzed how cybercrime is committed against children, some crimes committed by perpetrators and the procedure by which cybercrime prevention should be carried out as a way to protect children from Internet threats. The current state of child abuse on the Internet and the way in which this crime is investigated were described in the interview.

Keywords:

Cybercrime

Children

Child abuse on the Internet

Cybergrooming

Child pornography

Cyberbullying

Prevention of cybercrime

Obsah

Úvod

Dnešní přetechnizovaná doba nás denně, ať už chceme nebo ne, přenáší do světa digitálního, do světa internetu a sociálních sítí. Naše každodenní fungování, denní aktivity a nejběžnější činnosti se přesouvají do kybernetického prostoru a my se tak stáváme neustálými uživateli virtuálních sítí. Internet a digitální technologie se staly nedílnou součástí života, jejíchž prostřednictvím se otevírají nové možnosti, ale také nová rizika, a to zejména pro nejzranitelnější členy naší společnosti – děti. Děti se totiž stávají uživateli internetu, sociálních sítí a mobilních aplikací stejně jako dospělí. Přístup k internetu je jim poskytnut prostřednictvím nejrůznějších zařízení, jako jsou chytré telefony, tablety, počítače a herní konzole. Prostřednictvím internetu mají děti příležitost ke vzdělávání, zábavě a komunikaci s ostatními. Spolu s novými možnostmi a rozšířenými obzory vznikl i nový druh kriminality – kyberkriminalita.

Kyberkriminalita, jako taková, může mít mnoho podob či forem. Aktuální hrozby v podobě kybernetických útoků jsou nejrůznější podvody, šíření malware, phishing, zneužití osobních údajů apod. Dle mého názoru je nejzávažnější kybernetická kriminalita ta, která je páchána na dětech, tedy na uživatelích, kteří ještě nemají dostatek zkušeností, rozumové vyspělosti či nejsou dostatečně edukovány o kybernetické bezpečnosti. Kybernetickou kriminalitou, která je na dětech páchána, je například kybergrooming, kyberšikana, sexting či online dětská pornografie. Kybernetická kriminalita páchaná na dětech představuje závažný problém, který má potenciál způsobit dlouhodobé emocionální, psychické a v některých případech i dokonce dlouhodobé fyzické následky, vyžaduje zvýšenou pozornost veřejnosti, a proto se stala tématem mé diplomové práce. Diplomová práce se v některých pasážích zaměřuje zejména na kybergrooming, tedy zneužívání dětí na internetu, jelikož tento typ kyberkriminality se v poslední době velmi rozšířil.

Cílem této práce je podrobněji prozkoumat fenomén kybernetické kriminality páchané na dětech, analyzovat jeho příčiny, zjistit jaké trestné činnosti se pachatelé v souvislosti s touto kyberkriminalitou dopouštějí, jak je tento typ kybernetické kriminality vyšetřován a v neposlední řadě bude věnována pozornost prevenci a ochraně dětí před těmito hrozbami.

Pojem kybernetické kriminality

Doba 21. století se nese ve znamení rozvoje digitalizace a digitálních technologií. Rychlé šíření dat a informací skrze internetové prostředky přenáší naše každodenní fungování, denní aktivity a běžné činnosti do kybernetického prostoru. S tím spojený vývoj komunikačních technologií přináší možnosti nepřetržitého spojení s virtuálním světem. Digitální zařízení se neustále zmenšují a zlehčují, což lidem umožňuje být nepřetržitě on-line.

Na způsob, jakým lidé komunikují, vzdělávají se, pracují a celkově žijí má digitalizace značný vliv. Žití našich životů jsme plynule přesunuli do kybernetického prostoru, kde mimo nás působí i jiní lidé, kteří se ve virtuálním prostředí často chovají tak, jak by se ve skutečnosti nezachovali, píší to, co by stěží vyslovili, konají takovou činnost a takové aktivity, jaké by mimo digitální prostor nikdy nekonaly. Svým působením v on-line prostředí se uživatelé také mohou dopouštět protiprávních jednání a mnohdy až trestných činů. Velmi často si totiž neuvědomují skutečnost, že právní řád platí v kybernetickém světě stejně tak, jako ve světě reálném. O trestných činech páchaných v kyber prostoru hovoříme jako o kybernetické (počítačové) kriminalitě.

Pojmu kybernetické kriminality se podrobně věnuje Vladimír Smejkal ve třetím vydání publikace *Kybernetická kriminalita*, kde uvádí hned několik zdrojů. Pod pojmem "počítačová kriminalita" je tedy třeba chápat páchání trestné činnosti, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení včetně dat, nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď: jako předmět této trestné činnosti, ovšem s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité, nebo jako nástroj trestné činnosti.[1]

Česká technická norma říká, že "počítačový zločin je zločin spáchaný pomocí systému zpracování dat nebo počítačové sítě nebo přímo s nimi spojený".[2]

Evropská unie uvádí, že „kyberkriminalitou" se obvykle rozumí široká škála různých druhu trestné činnosti, jejichž primárním nástrojem nebo cílem jsou počítače a informační systémy. Kyberkriminalita zahrnuje tradiční tr. činy (například podvod, padělání a krádež identity), tr. činy související s obsahem (například on-line šíření dětské pornografie nebo podněcování k rasové nenávisti)

[1] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 3. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. ISBN isbn978-80-7380-849-5.s.33.
[2] ČSN ISO/IEC 2382-8 (369001). Informační technologie - Slovníku. Část 8: Bezpečnost.

a tr. činy specifické pro počítače a informační systémy [například útoky proti informačním systémům, odepření služby a škodlivý software ("malware")].[3]

S působením společnosti na internetu narůstá počítačové kriminality a kriminality páchané ve skutečném světě ubývá. Policejní orgány při vyšetřování svoji práci přesouvají z terénu k psacímu stolu a počítači. Krádeže a jiné majetkové delikty nebo násilná trestná činnost dnes nejsou tak časté jako například před deseti lety. Vystřídala je trestná činnost páchaná v prostorách internetu.

Kybernetická kriminalita páchaná na dětech

Spolu s rozvojem digitálních technologií, vývojem on-line prostoru a rozšířením sociálních síti se kyberprostor zpřístupnil a otevřel pro širokou veřejnost včetně dětí. Současné děti se již od batolecího věku běžně setkávají s moderními technologiemi v podobě mobilních telefonů, tabletů, notebooků a dalších zařízení. Stále častěji se setkáváme s pojmem "internetová generace dětí", který označuje děti, jejichž vývoj je ovlivněn internetem a digitálními technologiemi, jelikož s těmito prostředky od mala vyrůstají.

Dítě je v dnešní době uživatelem internetu stejně jako dospělý, který je na rozdíl od dítěte rozumově vyspělý a měl by si tak uvědomovat rizika, která působení na internetu přináší. Děti pomocí internetových sítí přirozeně jako součást společnosti vstupují do on-line prostředí, kde se vzdělávají, hrají si a komunikují. O hrozbách a rizicích užívání internetu, ať už v podobě sociálních sítí, nákupních e-shopů, či například on-line plateb, velmi často nejsou poučeni dospělí lidé, natož pak děti. Dítě se tak může, stejně jako dospělý, stát obětí trestné činnosti na internetu.

Kybernetická kriminalita páchaná na dětech je poměrně čerstvým problémem, který se s rozvojem digitalizace a přístupu k digitálním technologiím stává stále závažnějším. Globální povaha internetu a snadnost vyrábění a distribuování nelegálních materiálů mezi různými servery a uživateli internetu vedla a vede ke vzniku velkého problému. Mezi nejrizikovější oblasti týkající se dětí patří: získávání osobních informací, fotografií a videí obětí; násilí různého druhu; pobízení k nebezpečnému a nevhodném chování, a také kyberšikana.

[3] Společné sdělení Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor. JOIN(2013)0001 ze dne 7. 2. 2013. CELEX 52013JC0001.

K problémům mezinárodních rozměrů dnes patří právě dětská online pornografie a kybergrooming.[4]

Druhy kybernetické kriminality páchané na dětech

Kybernetická kriminalita je pojem, který v sobě zahrnuje několik druhů kriminality, která je v kybernetickém prostředí páchána. Nejčastějším druhem kybernetické kriminality jsou podvodná jednání jejichž cílem je většinou majetkový prospěch. Mezi taková podvodná jednání zahrnujeme podvody s virtuálními měnami, podvodné e-shopy, podvodné inzeráty a další. Velmi známým druhem kybernetické kriminality je například phishing, pharming, nebo hacking. Setkat se v prostorách internetu můžeme ale i s vydíráním, stalkingem, s distribucí dětské pornografie, s porušováním autorských práv a s mnoha dalšími projevy protiprávního jednání. Mezi nejzávažnější formy počítačové kriminality patří organizovaná trestná činnost a kyberterorismus. Dítě může být předmětem těchto jednání stejně tak, jako dospělý, a to jak na straně oběti, tak v některých případech i na straně pachatele.

Zaměříme-li se na dítě jako na oběť trestné činnosti páchané v prostorách internetu, jako druhy kybernetické kriminality můžeme označit například kyberšikanu, kybergrooming, kyberstalking nebo on-line dětskou pornografii.

Kyberšikana

V reálném světě se šikana projevuje jako úmyslné jednání s cílem poškodit oběť a sociálně ji izolovat prostřednictvím opakovaného verbálního či fyzického napadání. S rozvojem digitálních technologií se tato jednání přesunula do virtuálního světa. Kyberšikana může být propojena se šikanou „klasickou“ (např. nahrávání fyzického napadení oběti a následné umístění tohoto útoku na web). Pro to, abychom mohli hovořit o kyberšikaně, je nutné, aby k šikanování byly použity informační a komunikační technologie či služby nabízené v kyberprostoru.[5]

Kombinace šikany “klasické” a kybernetické je časté zejména mezi školou povinnými dětmi, kteří jsou prostřednictvím školského zařízení v každodenním kontaktu a mají podobný režim a návyky. Věk dětí, kteří zažívají nebo se dopouštějí kyberšikany se bohužel stále snižuje. Příčinou je právě již zmiňovaná dostupnost

[4] HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha: Triton, 2012. ISBN 978-80-7387-545-9.s.35.
[5] KOLOUCH, Jan. *Cybercrime*. Praha: CZ.NIC, z. s. p. o., 2016. ISBN 978-80-88168-18-8. s. 309.

digitálních technologií a snadný vstup na sociální sítě, popřípadě na jiné internetové komunikační prostředky.

Kyberšikana probíhá na různých komunikačních platformách, zejména pak na sociálních sítích, jako jsou Instagram, Facebook, Tik Tok, Snapchat apod., na webových stránkách, v chatových místnostech, při on-line hrách a zkrátka všude tam, kde se lidé virtuálně setkávají a komunikují. Před rozmachem sociálních sítí byl hojně využívaným komunikačním prostředkem email, který jde v dnešní době v souvislosti s kyberšikanou spíše do pozadí, zůstává však prostředkem pro nejrůznější kybernetové podvody.

Hlavní iniciátor šikany je nadřazený oběti a často mívá silnou sociální pozici ve skupině. Tradičně za ním, ať už při on-line či off-line šikaně, stojí jeho stoupenci, kteří nečinně přihlížejí a tím posilují jeho postavení a přímo či nepřímo ho podporují v opakování činnosti.

Reakce těch ze skupiny, kdo o šikaně či kyberšikaně vědí, zásadně ovlivňuje to, jak se bude šikana dále rozvíjet. Pokud zbytek skupiny tento typ agrese jednoznačně odmítne a dá tuto skutečnost najevo, může to celý proces zastavit.[6]

Nejčastějšími projevy kyberšikany je pomlouvání, zastrašování, urážení, zesměšňování či jiné ztrapňování (sociální sítě, e-mail, SMS, chat, ICQ, Skype, hry aj.), dále pak pořizování zvukových záznamů, videí či fotografií, jejich grafické či jiné upravování a následné zveřejňování s cílem poškodit (zesměšnit) vybranou osobu nebo natáčení videí, při kterých je oběť napadána fyzicky či je jinak psychicky týrána a zesměšňována. Tato videa jsou následně zveřejněna online (jedná se o tzv. Happy Slapping). [7]

Dalším často zmiňovaným kritériem pro identifikaci kyberšikany je fakt, že oběť vnímá to, co se děje, jako nepříjemné a ubližující. Základní znaky kyberšikany tedy můžeme shrnout takto: (1) děje se prostřednictvím elektronických médií, (2) opakovanost, (3) záměrnost agresivního obsahu, (4) mocenská nerovnováha, (5) oběť vnímá toto jednání jako nepříjemné a zraňující. [8]

Jedním z faktorů, který podněcuje páchání kyberšikany je pocit anonymity. Útočník má pocit, že je v kyberprostoru nedohledatelný, a navíc ve své činnosti ničím

[6] HAWKINS, D. Lynn; PEPLER Debra J., *York University* and Wendy M.; CRAIG Wendy M., *Queen's University*. *Naturalistic Observations of Peer Interventions in Bullying.* Blackwell
[7] KOLOUCH, Jan. *Cybercrime*. Praha: CZ.NIC, z. s. p. o., 2016. ISBN 978-80-88168-18-8. s. 310.
[8] ŠEVČÍKOVÁ, Anna. *Děti a dospívající online: vybraná rizika používání internetu*. Praha: Grada, 2014. Psyché (Grada). ISBN 978-80-210-7527-6.s.121.

neomezený. Při klasické šikaně například ve školách hrozí přítomnost pedagoga, rodiče či jiné osoby, která by mohla případnému útoku zamezit. Díky internetovým technologiím však může útočník šikanovat kdykoli, z jakéhokoli místa a v podstatě jakoukoli osobu, kterou na sociálních sítích vyhledá či osloví.

Internet poskytuje útočníkovi de facto neomezený prostor a prostředky pro šikanování.[9] Útočení agresora může mít formu nenávistných či urážlivých komentářů, zveřejňování fotografií či videí, které oběť zobrazují nebo se oběti vysmívají. Jako daleko závažnější vnímám kyberšikanu oproti šikaně klasické v tom, že se útočný obsah, který je na sociálních sítích či webových stránkách zveřejněn, může stát virálním. Tím, že je daný obsah zveřejněn na internetu, tedy prostředku, který je přístupný široké veřejnosti, se velmi rychle šíří prostřednictvím sdílení mezi jeho uživatele. Jako obsah virální můžeme označit obsah zajímavý, který se nám může jevit vtipným či emocionálně silným. Zejména zveřejňování videí a fotografií, které se následně stanou virálními a dostanou se tak do povědomí dalších lidí mohou pro oběť znamenat silně traumatizující situaci. Jedním z prvních takových zaznamenaných případů se stal chlapec jménem Ghyslain Raza známý jako „Star Wars Kid".

Ghyslain Raza natočil sám sebe při předvádění bojové scény z Hvězdných válek. Snažil se napodobit postavu Dartha Maula. Spolužáci mu nahrávku ukradli a pro pobavení ostatních ji zveřejnili na internetu. Během několika týdnů nahrávka obletěla celý svět, byla mnohokrát upravována, vzniklo množství webů a blogů, na kterých byl chlapec zesměšňován.[10] Nahrávka se stala virální zejména pro to, že je na ni zaznamenán amatérský, aktérský počin chlapce s nadváhou a jeho pohyby mohou působit směšně. Nahrávka byla poprvé zveřejněna v roce 2003 a je stále možná ke zhlédnutí na platformě YouTube.

Svým způsobem se jedná o prvotní kauzu, která se dostala až k projednání u soudu. Rodina poškozeného zažalovala čtyři spolupachatele a požadovala odškodnění ve výši čtvrt milionu kanadských dolarů, vyhověno jí bylo v rámci mimosoudního vyrovnání.[11] Chlapec se musel dlouhodobě psychicky léčit a dodnes je v souvislosti s touto kauzou známou osobností.

[9] KOLOUCH, Jan. *Cybercrime*. Praha: CZ.NIC, z. s. p. o., 2016. ISBN 978-80-88168-18-8. s. 311
[10] tamtéž
[11] TAYLOR, Chris. Reconsidering 'Star Wars kid,' the early internet's meanest moment. Mashable, publikováno 28.10.2020., (cit. 7.3.2024). Dostupné z: https://mashable.com/article/star-wars-kid-cyberbullying/?europe=true#

Případů, kdy oběti kybernetické kriminality museli vyhledat psychologickou či psychiatrickou pomoc je nespočet. Bohužel zaznamenáváme i případy, které skončili sebevraždou oběti. Jedním z takových je případ Amandy Todd, dívky, která se od neznámé osoby na internetu nechala přesvědčit, aby ukázala ňadra na webkameru. Osoba však pořídila ze záznamu fotografii a o rok později zkontaktovala Amandu znovu. Pod výhružkami zveřejnění fotografie na sociálních sítích požadovala od Amandy další snímky. Fotografii pak útočník skutečně zveřejnil a Amanda se stala obětí šikany nejen ze strany svých spolužáků.

Ani po přestěhování do jiného města šikana neustala. I tam ji začala pronásledovat zmíněná fotografie. Nikdo jí nedokázal pomoci – škola, rodina ani přátelé. Několikrát se neúspěšně pokusila o sebevraždu – např. vypila bělidlo. A šikana dostala další rozměr – nesmírné množství nevhodných žertů dotýkajících se Amandina zoufalého činu, kde byla dále zesměšňována. Dne 7. září 2012 vyvěsila na youtube.com svůj poslední příspěvek, ve kterém popsala svá utrpení. O tři dny později, v jejích patnácti letech, spáchala sebevraždu.[12]

Video, kde Amanda pomocí psaného textu popisuje svůj příběh, je stále dostupné na YouTube. Pachatel, který fotografii zveřejnil byl ztotožněn a odsouzen k trestu odnětí svobody na 10 let a 8 měsíců.

I zdánlivě nezávažné činy či projevy kyberšikany mohou mít vážné a mnohdy až fatální následky. Drobné počáteční náznaky kyberšikany se pak mohou rozvinout v závažnější formy obtěžování a útoků a následkem je pak minimálně emoční a psychická nestabilita člověka, který se stal terčem obtěžování.

Kyberšikana (stejně jako klasická šikana) sama o sobě není trestným činem ani přestupkem. Vždy záleží na jednání, kterým útočník šikanoval. Pokud toto jednání mělo podobu například fyzického ublížení oběti, jejímu vydírání či zastrašování, pak by mohlo přicházet v úvahu uplatnění například § 146 (Ublížení na zdraví) či § 145 (Těžké ublížení na zdraví), § 175 (Vydírání) TZK. V případě obtěžování a pronásledování osoby by bylo možné využít ustanovení § 354 TZK (Nebezpečné pronásledování). Avšak u kyberšikany, která se může projevovat například neustálým zesměšňováním, ztrapňováním a psychickým ubližováním

[12] INTERNETEM BEZPEČNĚ 2018, Online vydírání [online] (cit. 7.3.2024), ISSN 2571-3736. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/online-vydirani/

prostřednictvím informačních a komunikačních technologií, bude aplikace některých výše uvedených ustanovení problematická, ne-li přímo nemožná.[13]

On-line dětská pornografie

V prostorách internetu je možné se dostat na různé webové stránky, včetně těch s pornografickým obsahem. Pornografie sama o sobě není trestným činem, nicméně pokud v ní figuruje dítě, právní úprava je jiná.

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. Český právní systém zakazuje zveřejňování, zprostředkování, nabízení, uvedení do oběhu a jiné zpřístupnění dětské pornografie. Zde je na místě podotknout, že i děti mohou být šiřiteli dětské pornografie. [14]

Nelze opomenout i jiné způsoby páchání trestného činu šíření dětské pornografie. Typickým příkladem je fotografování dětí – modelů za účelem uplatnění v reklamě či pro zahraniční časopisy. Organizátoři těchto akcí oslovují zpravidla rodiny ve složité sociální či finanční situaci s příslibem nafocení dítěte pro takového účely. Za touto záminkou se však může skrývat produkce dětské pornografie. Pachatelé často nutí své oběti, aby lákaly i další děti ke spoluúčasti. V některých případech jde tato trestná činnost ruku v ruce s užitím omamných a psychotropních látek.[15]

Kybergrooming

Virtuální svět je skvělé místo, kde se mohou setkávat lidé z celého světa. Skrze internetové komunikační prostředky dnes můžeme komunikovat v podstatě s kýmkoli, kdo má možnost internetového připojení. Kontakt s lidmi na sociálních sítích nám jistě může být přínosný a může nám usnadnit komunikaci nejen v pracovních, rodinných či jiných vztazích. Spolu s námi se však do virtuálního

[13] KOLOUCH, Jan. *Cybercrime*. Praha: CZ.NIC, z. s. p. o., 2016. ISBN 978-80-88168-18-8. s. 312
[14] POLICIE ČR (2023) [cit. 22.12. 2023], *Počítačová mravnostní kriminalita* [online], dostupné z <https://www.policie.cz/clanek/pocitacova-mravnostni-kriminalita.aspx>
[15] tamtéž

prostoru dostávají i lidé, kteří tyto prostředky zneužívají. Dítě je stejně jako dospělý uživatelem internetu, kde přes sociální sítě a jiné weby komunikuje nejen se svými rodiči a přáteli, ale často také s úplně cizími lidmi. Navázat s kýmkoli kontakt přes sociální síť je velmi jednoduché, stejně tak, jako vystupovat na sociální síti s falešnou identitou.

Děti, ostatně stejně tak jako mnozí dospělí, hledají na internetu v první řadě zábavu. Chtějí poznat nové přátele, chtějí, aby se někdo zajímal o to, co dělají a čemu se věnují. Dítě se na internet dostává ve věku, kdy ze všeho nejvíc potřebuje slova pochopení, slova útěchy, pochvaly a hlavně pozornost.

Kybergrooming je termín označující chování uživatelů internetu, které má v dítěti vyvolat falešnou důvěru a připravit ho na schůzku, jejímž cílem je oběť pohlavně zneužít.[16] V médiích je setkávání s neznámými z internetu obvykle vykresleno jako velmi nebezpečná aktivita, neboť na druhé straně klávesnice může sedět tzv. online predátor nebo kybergroomer. – tedy dospělý pedofil, který při online komunikaci předstírá, že je ve věku vyhlédnuté oběti a různými strategiemi včetně kupování dárků či vydírání láká oběť k osobnímu setkání, aby ji zneužil.[17] Zbraněmi kybergroomera jsou líbivá slova, sliby a předstíraný zájem, kterým snadno vzbudí v dítěti důvěru a emoční závislost.

Proces kybergroomingu

Proces manipulace dítěte prochází čtyřmi základními etapami (příprava kontaktu – kontakt s obětí – příprava na osobní schůzku – osobní schůzka), během nichž útočník využívá velké množství manipulačních technik a postupů.

1. **Etapa – příprava kontaktu**

V této etapě útočník připravuje podmínky pro realizaci manipulace oběti. Jedním z velmi často pozorovaných postupů útočníka – kybergroomera je vytvoření falešné identity. Útočník o sobě uvádí nepravdivé osobní údaje, jako jsou jméno, příjmení, věk či fotografie obličeje. Manipulátoři jsou obvykle podstatně starší než vyhlédnuté oběti, proto si svůj věk dle potřeby upraví a doplní o odpovídající fotografie.

[16] HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha: Triton, 2012. ISBN 978-80-7387-545-9.s.52.
[17] WOLAK, J., Finkelhor, D., Mitchell, K. J., Ybarra, M. L. (2010). Online „predators" and their victims: Myths, realities, and implicitations for pervention and treatment. *Psychology of Violence, 1(S), 13-16.*

2. **Etapa – kontakt s obětí**

Ve druhé etapě manipulace útočník navazuje kontakt s obětí a dále pracuje na budování a prohlubování virtuálního vztahu.

Charakteristickým rysem chování kybergroomera je tzv. efekt zrcadlení (mirroring). Predátor napodobuje oběť ve snaze prolomit zábrany, chová se jako její zrcadlový odraz. Pokud oběť útočníkovi sdělí, že se cítí například osamělá a má nějaké problémy a starosti, predátor odpoví, že má podobné problémy a plně ji chápe.

Kromě osobních údajů (jméno, věk, fotografie) se predátor snaží zjistit další informace - např. jméno školy, kterou žák/žákyně navštěvuje, oblíbené celebrity, zájmy a záliby apod. Tyto údaje pak slouží útočníkovi k sestavení obecného profilu oběti. K tomu, aby útočník navázal s obětí co nejužší vztah, často využívá různé formy úplatků a "dárečků".

V této etapě kybergroomingu se snaží útočník velmi často postupně snižovat zábrany dětí a mládeže v oblasti sexuality postupným zaváděním sexuálního obsahu do konverzace. Tím může být v prvé řadě diskuse o lidské sexualitě, sexuálním životě rodičů, může docházet také k tomu, že útočník dítěti nabídne různé erotické či pornografické materiály, například proto, aby vzbudil jeho zájem a snížil jeho stud. Útočník samozřejmě usiluje o získání fotografií či videozáznamů obnažené oběti (například se snaží přimět oběť k tomu, aby se mu ukázala na webkameru nebo aby mu zaslala své nahé fotografie).

3. **Etapa – příprava na osobní schůzku**

V této etapě již útočník disponuje diskriminujícími informacemi a osobními údaji oběti a plánuje osobní schůzku. I v této etapě využívá techniky cílené manipulace.

Ve chvíli, kdy predátor o oběti dostane dostatek informací a citlivých materiálů, může se pokusit pozvat ji na osobní schůzku. Pokud oběť odmítne na schůzku dorazit, útočník ji začne vydírat. Vyhrožuje, že o ní zveřejní kompromitující materiály – například zašle nahé fotografie jejím kamarádům, přátelům a rodičům, případně tyto materiály vytiskne a vyvěsí v okolí bydliště a školy oběti.

4. **Etapa – osobní schůzka**

Osobní schůzka je hlavním cílem kybergroomera. První schůzka útočníka s obětí může být úplně nevinná, nemusí ještě dojít k sexuálnímu či jinému zneužití

oběti. Útočník so může na schůzce pouze ověřit, zda je oběť skutečně nezletilá. Na schůzce rovněž může útočník prohloubit navázaný vztah s obětí dalším dárkem (úplatkem).

Útok (sexuální útok, fyzický útok apod.) má pro oběť nedozírné následky. Jak v oblasti fyzické, tak zejména v oblasti psychické. Pokud má kybergroomer dostatek účinných nástrojů pro manipulaci, může oběť donutit k opakovaným schůzkám, na kterých útoky pokračují. [18]

Sexting

V druhé etapě kybergroomingu se konverzace začíná stále více zaměřovat na téma sexuality. Sexting (česky sextování, slovo vzniklo složeninou slov sex a textování) je elektronické rozesílání textových zpráv, fotografií či videí se sexuálním obsahem. Tyto záznamy (fotografie, video) jsou pak často zveřejněny na internetu. Stává se to hlavně v případech, kdy dojde k ukončení vztahu mezi přáteli či partnery.[19] V případě kybergroomingu k ukončení kontaktu mezi obětí a predátorem. Pornografický či erotický materiál zobrazující dítě (oběť) se také často stává nástrojem k vydírání oběti.

Sexting podporuje šíření pornografie dětí, které je celosvětově zakázáno. V České republice již byla zaznamenána řada případů sextingu a mnoho z nich lze posuzovat právě jako šíření dětské pornografie.[20]

Mravnostní trestné činy

Mravnostní trestné činy nelze vysvětlovat výlučně mravní otupělostí nebo je chápat jako zvýšenou dráždivost na sexuální podněty při snížené ovládací schopnosti. Značný podíl na této kriminalitě totiž mají osoby zcela "zdravé", u kterých není psychiatrických ani psychologickým vyšetřením zjištěna anomálie v podobě sexuální úchylky. Nevyvratitelným faktem však je, že podstatná část této delikvence je páchána osobami, u kterých je zjišťování sexuálně patologická motivace, jejíž predikce zasahuje mimo vývojové vady i do špatné nebo nedostatečné mravní, sexuální, obecně pak společenské výchovy. [21]

---

[18] KOPECKÝ, Kamil, SZOTKOWSKI, René. *E-bezpečí: Kybergrooming a sextortion (průvodce studiem).* Dostupné z: [*E-bezpečí: Kybergrooming a sextortion*] Olomouc 2018. s.4-6.
[19] HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha: Triton, 2012. ISBN 978-80-7387-545-9.s.62.
[20] HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha: Triton, 2012. ISBN 978-80-7387-545-9.s.62.
[21] CHMELÍK, Jan. *Mravnost, pornografie a mravnostní kriminalita*. Praha: Portál, 2003. ISBN 80-7178-739-6.s.18.

Mravnostní trestné činy zasahují čtyři základní roviny: morální vztahy ve společnosti; život, zdraví občanů poškozených v důsledku protiprávního jednání ve sféře sexuálních vztahu; zdravý vývoj mládeže; dobré mravy v sexuálních vztazích mezi dospělými jedinci.[22]

Mezi mravnostní trestné činy v souvislosti s kybernetickou kriminalitou páchanou na dětech řadíme například sexuální nátlak (§ 186 zákona č. 40/2009 Sb., trestní zákoník dále jen *„TrZ"*), pohlavní zneužití (§187 TrZ), šíření pornografie (§191 TrZ), výroba a jiné nakládání s dětskou pornografií (§192 TrZ), zneužití dítěte k výrobě pornografie (§193 TrZ) nebo například navazování nedovolených kontaktů s dítětem (§193 TrZ). V mnohých případech si uživatelé internetu neuvědomují, že se svým chováním v kybernetickém prostoru stávají pachateli výše uvedených trestných činů.

Děti na internetu

Digitální technologie se přirozeně prostřednictvím dospělých dostaly i k dětem. Internet jim, stejně tak jako dospělým, otevírá dveře do světa informací, zábavy a možností komunikace. Stává se pro ně vzdělávacím nástrojem, ke kterému je však třeba přistupovat zodpovědně. Děti se v dnešní době k internetu dostávají velmi brzy a je především na rodičích a školních pedagozích, aby děti obeznámili s online prostředím a vedli je k bezpečnému užívání internetu. Děti se dnes k tabletům, chytrým hodinkám a ostatním mobilním zařízením dostávají ve velmi mladém věku, kdy je primárním účelem užívání zábava, vzdělání nebo zajištění bezpečnosti dítěte.

Mobilní zařízení se stále zmenšují, což lidem umožňuje být online a mít přístup k internetu kdykoli a kdekoli. S neustálým přístupem k internetu se může zvyšovat závislost na online světě. V současnosti stále více hovoříme o nadměrném užívání internetu dospělých, ale i dětí. Ranný kontakt dětí s moderními technologiemi sebou nese riziko nevědomosti v souvislosti s nedostatečnou rozumovou vyspělostí dítěte, což je téma, které vyžaduje pozornost. Nadměrné působení dětí na internetu, spolu s jejich nedostatečnou informovaností a nedostatečným poučením o užívaní sociálních sítí a jiných webových stránek, může dítě vystavit nebezpečí. Dítě se tak snadno může stát obětí internetového zločinu, ale stejně tak i jeho pachatelem.

[22] CHMELÍK, Jan. *Mravnost, pornografie a mravnostní kriminalita*. Praha: Portál, 2003. ISBN 80-7178-739-6.s.18.

Dítě jako pojem trestního práva

Dítě v rámci trestního práva požívá zvláštní právní ochrany, která je zavedena s ohledem na jeho rozumovou a volní vyspělost, emoční a fyzické potřeby a vysokou šanci nápravy v případě provinění. Zvláštní úpravu nalezneme primárně zakotvenou v mezinárodně právních dokumentech a na vnitrostátní úrovni v ústavním pořádku České republiky v Listině základních práv a svobod.

Mezinárodní právní úprava pojmu dítě

Mezinárodní právní úprava pojmu "dítě" je obsažena v několika mezinárodních dohodách a úmluvách. Klíčovým dokumentem v rámci mezinárodní úpravy pojmu „dítě“ je Úmluva o právech dítěte ze dne 20. 11. 1989. Pro účely této Úmluvy se dítětem rozumí každá lidská bytost mladší osmnácti let, pokud podle právního řádu, jenž se na dítě vztahuje, není zletilosti dosaženo dříve. [23]

Zájem dítěte musí být předním hlediskem při jakékoli činnosti týkající se dětí, ať už uskutečňované veřejnými nebo soukromými zařízeními sociální péče, soudy, správními nebo zákonodárnými orgány.[24]

Vnitrostátní právní úprava pojmu dítě

Zvláštní ochrana dětí je ve vnitrostátní právní úpravě garantována Listinou základních práv a svobod. Konkrétně v článku 32 odst. 1, který přímo uvádí, že zvláštní ochrana dětí a mladistvých je zaručena.[25]

Dalším pramenem vnitrostátního práva upravující pojem „dítě“ je bezpochyby trestní zákoník. Dle ustanovení § 126 TrZ se dítětem rozumí osoba mladší osmnácti let, pokud trestní zákon nestanoví odlišně. [26]

Definice pojmu dítě v § 126 TrZ je převzata z Úmluvy o právech dítěte. Vymezení osoby jako dítěte ve smyslu ustanovení § 126 je výrazem zvýšené trestněprávní ochrany osob mladších osmnácti let, které jsou předmětem útoku pachatele některých trestných činů.

Může jít např. o některé trestné činy proti rodině a dětem, u nichž je poškozeným právě dítě (např. ohrožování výchovy dítěte podle § 201, svádění

---

[23] *Úmluva o právech dítěte z roku 1989*, článek první.
[24] *Úmluva o právech dítěte z roku 1989*, článek třetí.
[25] *Listina základních práv a svobod jako součást právního řádu ČR* [online]. Plzeň, 2011 [cit. 2023-09-08]
[26] Zákon č. 40/2009 Sb., trestní zákoník. In [Systém ASPI]. Wolters Kluwer [cit. 2023-9-24]. Dostupné z: www.aspi.cz. ISSN 2336-517X. [https://www.aspi.cz/products/lawText/1/68040/1/2/zakon-c-40-2009-sb-trestni-zakonik]

k pohlavnímu styku podle § 202 odst. 1, podání alkoholu dítěti podle § 204, anebo o jiný druh trestné činnosti spáchané vůči dítěti (tj. vůči osobě mladší osmnácti let) je v takových případech obligatorním zákonným znakem objektivní stránky jejich základní skutkové podstaty. Dítě jakožto osoba mladší osmnácti let, může být předmětem útoku také v případě některých kvalifikovaných skutkových podstat, kdy spáchání trestného činu vůči němu je naplněním okolnosti zvláště přitěžující, která podmiňuje použití vyšší trestní sazby ve smyslu § 17 [jde např. o trestné činy znásilnění podle § 185 odst. 2 písm. b), sexuálního nátlaku podle § 186 odst. 3 písm. a), účasti na sebevraždě podle § 144 odst. 2].[27]

Zákon č. 218/2003 Sb. o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů (dále jen „ZSVM“) pro účely tohoto zákona zahrnuje pod pojem mládež děti a mladiství. Dítětem se dle § 2 odst. 1 písm. b) rozumí dítě mladší patnácti let, které v době spáchání činu jinak trestného nedovršil patnáctý rok věku. Mladistvým se dle ZSVM rozumí ten, kdo v době spáchání provinění dovršil patnáctý rok a nepřekročil osmnáctý rok svého věku. Mladistvým je i ten, kdo v době spáchání provinění dovršil patnáctý rok věku, ale u něhož není možné bez důvodné pochybnosti určit, že v době spáchání provinění překročil osmnáctý rok věku. [28]

Trestní odpovědnost dětí

Trestní zákoník v souvislosti s trestní odpovědností stanovuje, že kdo v době spáchání trestného činu nedovršil patnáctý rok věku, není za své jednání trestně odpovědný. Totožnou úpravu nalezneme i v § 89 zákona č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů; zákon o soudnictví ve věcech mládeže (dále jen „*ZSVM“*), které mimo jiné v následujících ustanoveních upravuje trestní řízení s dítětem mladším patnácti let.

---

[27] DRAŠTÍK, A., DURDÍK, T., FREMR, R., RŮŽIČKA, M., SOTOLÁŘ, A. *Trestní zákoník: Komentář*. [Systém ASPI]. Wolters Kluwer [cit. 2023-9-24]. ASPI_ID KO40_2009CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X. [https://www.aspi.cz/products/lawText/13/6500/126/komentar-wkcr-c-40-2009-sb-trestni-zakonik-komentar]

[28] Zákon č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů (zákon o soudnictví ve věcech mládeže). In [Systém ASPI]. Wolters Kluwer [cit. 2023-9-24]. Dostupné z: www.aspi.cz. ISSN 2336-517X. [https://www.aspi.cz/products/lawText/1/55745/1/2/zakon-c-218-2003-sb-o-odpovednosti-mladeze-za-protipravni-ciny-a-o-soudnictvi-ve-vecech-mladeze-a-o-zmene-nekterych-zakonu-zakon-o-soudnictvi-ve-vecech-mladeze?vtextu=Z%C3%A1kon%20o%20soudnictv%C3%AD]

Čin, který je spáchán dítětem do patnácti let věku nazýváme činem jinak trestným. Soud pro mládež může dle § 93 ZSVM v takovém případě uložit opatření jako například výchovné omezení [§ 93 odst. 1 písm. b)], zařazení do terapeutického, psychologického nebo jiného vhodného výchovného programu [§ 93 odst. 1 písm. c)], nebo v závažnějších případech například ochranné léčení [§ 93 odst. 1 písm. g)].

Trestní odpovědnost osoby počíná dnem, který následuje po dni dovršení patnáctých narozenin. Osoby, které dovršily patnácti let, ale nepřekročili osmnáctý rok života ZSVM označuje jako osoby mladistvé. Čin, kterého se mladistvý dopustil nenazýváme trestným činem nýbrž proviněním. Zákon o soudnictví ve věcech mládeže dále v ustanovení § 5 odst. 1 říká, že mladistvý, který v době spáchání trestného činu nedosáhl takové rozumové a mravní vyspělosti, aby mohl rozpoznat jeho protiprávnost nebo ovládat své jednání, není za tento čin trestně odpovědný.[29]

Trestní odpovědnost je tedy vázána nejen na věkovou hranici, ale vzhledem k nutnosti individualizace každého případu s ohledem na přítomnost jedince, který ještě není zcela psychicky a fyzicky vyvinut i na rozumovou a volní vyspělost.

Dopustí-li se však dítě mladší 15 let činu jinak trestného, učiní soud pro mládež, podle zákona o soudnictví ve věcech mládeže, opatření potřebná k jeho nápravě (výchovná povinnost, výchovné omezení, napomenutí s výstrahou, zařazení do terapeutického, psychologického nebo jiného vhodného výchovného programu ve středisku výchovné péče, dohled probačního úředníka, ochrannou výchovu a ochranné léčení). V řízení proti dětem mladším patnácti let, které se měly dopustit činu jinak trestného, postupuje soud pro mládež podle zvláštních právních předpisů upravujících občanské soudní řízení, neboť děti mladší patnácti let nejsou trestně odpovědné, a proto proti nim nelze vést trestní řízení.[30]

V rámci řízení vedeného proti dítěti mladšímu patnácti let, které se mělo dopustit činu jinak trestného musí být dítě zastoupeno opatrovníkem (advokátem), kterého věcně a místně příslušný soud ustanoví. Advokát vykonává svá oprávnění

[29] Zákon č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů (zákon o soudnictví ve věcech mládeže). In [Systém ASPI]. Wolters Kluwer [cit. 2023-9-24]. Dostupné z: www.aspi.cz. ISSN 2336-517X.
[30] Soustava státního zastupitelství, 2024 Nejvyšší státní zastupitelství [online] (cit. 2.3.2024), Ochrana dětí Dostupné z: https://verejnazaloba.cz/vice-o-sz/vse-podstatne-o-trestnim-rizeni/ochrana-poskozenych-a-ohrozenych-osob/ochrana-deti/

i po dosažení zletilosti dítěte až do skončení řízení ve věci dítěte mladšího patnácti let.

Účastníkem řízení je dále také orgán sociálně-právní ochrany dětí (OSPOD), zákonní zástupci dítěte, osoby, kterým bylo dítě svěřeno do výchovy nebo jiné obdobné péče, jakož i další osoby, o jejichž právech a povinnostech má být v řízení jednáno. Účastníkem řízení může být také státní zastupitelství.[31]

Mladistvému lze za spáchání provinění uložit opatření výchovná, opatření ochranná anebo opatření trestní. Výchovnými opatřeními se rozumí dohled probačního úředníka, probační program, výchovné povinnosti, výchovná omezení a napomenutí s výstrahou. Mezi ochranná opatření řadíme ochranné léčení, zabezpečovací detenci, zabrání věci či části majetku a ochrannou výchovu. Za provinění nejzávažnější lze mladistvému uložit trestní opatření. Trestními opatřeními v takovém případě jsou obecně prospěšné práce, peněžité opatření, peněžité opatření s podmíněným odkladem výkonu, propadnutí věci, zákaz činnosti, zákaz držení a chovu zvířat, vyhoštění, domácí vězení, zákaz vstupu na sportovní, kulturní a jiné společenské akce, odnětí svobody podmíněně odložené na zkušební dobu (podmíněné odsouzení), odnětí svobody podmíněně odložené na zkušební dobu s dohledem a odnětí svobody nepodmíněné. Uložená opatření podle zákona o soudnictví ve věcech mládeže musí přihlížet k osobnosti toho, komu je ukládáno, včetně jeho věku a rozumové a mravní vyspělosti, zdravotnímu stavu, jakož i jeho osobním, rodinným a sociálním poměrům, a musí být přiměřené povaze a závažnosti spáchaného činu.[32]

Postavení oběti

Oběťmi kybergroomingu jsou zpravidla děti a mládež, nejčastěji ve věku 11-17 let. Lze předpokládat, že oběti tvoří zejména ti uživatelé internetu, kteří tráví velké množství volného času v online komunikačních prostředcích, kde také navazují virtuální kontakty s ostatními (hledají zde kamaráda, přátele, životní partnery). V posledních letech se objevuje stále více případů kybergroomingu, ke kterým došlo na některé ze sociálních sítí (Facebook, Instagram, Twitter apod.). Ty

[31] Zákon č. 40/2009 Sb., trestní zákoník. In [Systém ASPI]. Wolters Kluwer [cit. 2023-9-24]. Dostupné z: www.aspi.cz. ISSN 2336-517X. [https://www.aspi.cz/products/lawText/1/68040/1/2/zakon-c-40-2009-sb-trestni-zakonik]

[32] Zákon č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů (zákon o soudnictví ve věcech mládeže). In [Systém ASPI]. Wolters Kluwer [cit. 2023-9-24]. Dostupné z: www.aspi.cz. ISSN 2336-517X.

díky propracovanému systému virtuálních sociálních vazeb poskytují ideální prostředí pro jeho realizaci. [33]

Chlapci mohou být do postavení oběti v rámci kybergroomingu vtaženi stejně jako dívky, nicméně procentuálně je jejich zastoupení daleko menší. Obecně lze říci, že do role oběti se může dostat jakékoliv dítě, které je schopné komunikovat přes internetové prostředky. Příkladem může být šestileté dítě, které sice ještě zcela nemá psací schopnosti a digitální gramotnost, nicméně v dnešní době je schopné s pachatelem komunikovat například prostřednictvím hlasových zpráv, fotografií či videí. Mezi nejčastější oběti patří děti s nízkou sebeúctou nebo nedostatkem sebedůvěry (lze je snadněji citově či fyzicky izolovat), děti s emocionálními problémy, oběti v nouzi (často hledají náhradu za své rodiče a potřebují pomocnou ruku), děti naivní a přehnaně důvěřivé (jsou ochotnější zapojit se do online konverzace s neznámými lidmi, obtížněji rozpoznávají rizikovou komunikaci) a adolescenti/ teenageři (zajímá je lidská sexualita, jsou ochotni o ni hovořit).

Dítě má přirozeně sníženou rozumovou vyspělost, a proto není zcela schopné rozpoznat potenciální nebezpečnou situaci. Jeho chování se jeví jako více důvěřivé a vzhledem k pubertálnímu vývoji se dítě přirozeně stává emocionálně náchylnější. Právě zmiňované důvěřivosti, nevinnosti či emocionální nestability internetoví pachatelé často využívají k manipulaci s dítětem, která má více méně stejný průběh u každého jednotlivého případu. Vylákat z dítěte osobní informace, a tedy získat si jeho důvěru, může pachateli zabrat pouhých několik dní nebo v některých případech dokonce několik hodin. Manipulačních technik, které pachatelé aplikují, je hned několik a často je můžeme rozdělit do několika fází, které jsou v souvislosti s kybergroomingem již zmíněny výše. Obecně lze konstatovat, že dítěti ve školním věku se od pachatele dostává to, co s ohledem na svůj vývoj a emocionální rozpoložení v inkriminovaném věku nejvíce potřebuje. Děti v prepubertální či pubertální fázi vývoje často mají pocit nedostatku pochopení a podpory od rodičů, často také postrádají zájem nejen ohledně jejich aktivit, ale ohledně celé jejich osoby. Pachatel tak snadno k manipulaci využije technik jako je lichocení, předstíraný zájem o dítě, pochopení a vyslechnutí jejich problémů a v neposlední řadě navodí dítěti pocit sobě rovného jedince, tedy dospělého člověka. Právě chování a přístup pachatelů k mladým dívkám, jako k dospělým ženám je to, čím si získají jejich přízeň. Dítě je ze své pozice zvyklé následovat

[33] KOPECKÝ, Kamil, SZOTKOWSKI, René. *E-bezpečí: Kybergrooming a sextortion (průvodce studiem).* Dostupné z: [*E-bezpečí: Kybergrooming a sextortion*] Olomouc 2018. s.3.

autority, podřizovat se, a tak logicky staršího internetového kamaráda poslouchá a neklade aktivní odpor. Z počátku proto, že nerozpozná škodlivé a nebezpečné chování a následně jedná ze strachu způsobeného potenciální nepříznivou reakcí okolí. Dítě na internetových platformách jako je Facebook, Instagram, Skype nebo Snapchat hledá primárně zábavu či přátele.

Právě již zmíněné neodhadnutí nebezpečné situace ze strany oběti, které zahrnuje počáteční lhostejnost oběti k obtěžování, počáteční vnímání situace jako bezproblémové, podlehnutí pachatelovu naléhání a v některých případech i odeslání choulostivých fotografií prudce vystřídá strach nejen o sebe sama, ale i o dopisující protějšek, strach svěřit se, strach o reakci okolí zejména rodičů a spolužáků, strach ze zneužití odeslaných údajů nebo například strach z postihu za odeslání intimních fotografií. Tyto dva jevy doprovází nepříjemné pocity smutku, psychické i fyzické vyčerpanosti, nejistoty, špatného svědomí, pocity studu, zamlklost, možné nevědomosti ohledně toho, komu se svěřit nebo například pocit odpovědnosti za vzniklou situaci.

Z počátku nevinná přátelská online konverzace se rázem může změnit v psychický teror. Přes lichocení, předstíraný zájem a ostatní manipulační techniky se pachatel velmi rychle dostává na konverzaci se sexuální tematikou, která obsahuje nepříjemné sexuální návrhy, otázky pachatele na intimní detaily týkající se oběti, zasílání erotických fotografií a videí, žádosti o erotické služby apod. Postupem času se obtěžování jen stupňuje nejen zesílenou frekvencí obtěžujících zpráv, ale i například neustálém naléhání na oběť, vyžadování osobní schůzky, obviňování oběti a v neposlední řadě samozřejmě vyhrožování oběti.[34]

Oběti ze zpráv krizové linky situaci velmi často podcenily a byly lhostejné k počátečnímu obtěžování a zkresleným informacím či požadavkům ze strany pachatele: “Zpočátku dívce SMS se sexuální tematikou nevadily, těšil ji něčí zájem.” “Nejdřív ji nevadilo, že vypadá jinak než na fotce, kterou ji poslal, a také, že je straší, než uváděl, protože na ni byl hodný.” “Dívka naléhání podlehla a s najatým fotografem erotické fotky nafotila” [35]

Psychická manipulace v rámci kybergroomingu probíhá obvykle delší dobu – od cca 3 měsíců po dobu několika let. Tato doba je přímo závislá na způsobu

[34] HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie -internetové oběti, pachatele a kriminality*. Praha: Triton, 2012. ISBN 978-80-7387-545-9.s.118-125.
[35] HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha: Triton, 2012. ISBN 978-80-7387-545-9.s.119.

manipulace a důvěřivosti oběti. Existují případy, kdy predátor manipuloval dítě po dobu 2 let, než došlo k osobnímu setkání a sexuálnímu zneužití. [36]

Role pachatele

Dle ustanovení § 22 odst. 1 TrZ je pachatelem trestného činu, kdo svým jednáním naplnil znaky skutkové podstaty trestného činu nebo jeho pokusu či přípravy, je-li trestná.[37]

Pachatelé mravnostní kybernetické kriminality jsou typicky lidé, kteří si neuvědomují následky svého chování a jednání v prostorách internetu. Většinou je ani nenapadne, že by jejich počínání mohlo být kvalifikováno jako trestný čin a pokud jejich jednání vyjde najevo, hájí se tím, že jiní to dělají také a oni sami nevěděli, že se jedná o trestnou činnost.

Kyberútočníci (predátoři) tvoří heterogenní skupinu, ve které nalezneme jak uživatele s nízkým, tak i vysokým sociálním statutem (právníky, učitele, policisty). V řadě případů oběť pachatele zná a je na něm závislá (v 85-95 % případů) (Choo 2009), často bývá útočníkem také známý rodiny oběti. Mezi útočníky dle výzkumů převažují osoby, které dosud nebyly trestány. Kybergroomery se ale někdy stávají i ti, kteří již byli za sexuální útoky proti dětem a mladistvým odsouzeni a došlo u nich k recidivě. U většiny útočníků byl diagnostikován patologický zájem o děti. Chování útočníků – kybergroomerů – vysvětluje například model sociálních dovedností (Olson et. all 2007), podle něhož útočníci navazují kontakty s dětmi, protože mají strach z navazování vztahů s dospělými. Vztahy s dětmi kybergroomeři vnímají jako méně ohrožující, cítí se bezpečněji než ve vztazích s dospělými. Z hlediska věku a vzhledu si děti a dospívající často představují útočníka jako nevzhledného postaršího pána, který o jejich „životě a světě“ neví zhola nic. Ve skutečnosti však může být predátorem i pohledný osmnáctiletý chlapec, do něhož by to nikdo „neřekl“. [38]

Pachatelem můžou být samozřejmě i ženy nebo vrstevníci či dokonce spolužáci oběti. Za klávesnici počítače a IP adresu se může schovat jak muž, tak

[36] KOPECKÝ, Kamil, SZOTKOWSKI, René. *E-bezpečí: Kybergrooming a sextortion (průvodce studiem).* Dostupné z: [*E-bezpečí: Kybergrooming a sextortion*] Olomouc 2018. s.3.
[37] Zákon č. 40/2009 Sb., trestní zákoník. In [Systém ASPI]. Wolters Kluwer [cit. 2023-9-24]. Dostupné z: www.aspi.cz. ISSN 2336-517X. [https://www.aspi.cz/products/lawText/1/68040/1/2/zakon-c-40-2009-sb-trestni-zakonik]
[38] KOPECKÝ, Kamil, SZOTKOWSKI, René. *E-bezpečí: Kybergrooming a sextortion (průvodce studiem).* Dostupné z: [*E-bezpečí: Kybergrooming a sextortion*] Olomouc 2018. s.3.

žena různých věkových kategorií. Ve spoustě případů se můžeme jen domnívat co je jejich motivem k páchání takové trestné činnosti.

Dokumentární kniha o zneužívání dětí na internetu s názvem „Kdo chytá v síti“, která vznikla jako reakce na český dokument režiséra Víta Klusáka a režisérky Barbory Chalupové (V síti, 2020) byla dle slov autorky Mariky Pecháčkové vytvořena jako přirozená reakce na film „V síti“. Původně měla obsahovat rozhovory s muži, kteří se „chytili do sítě“, tedy s pachateli trestné činnosti v souvislosti se sexuálním zneužíváním dětí na internetu, kteří byli zaznamenáni v rámci dokumentárního natáčení, aby mohli své jednání a pohnutky v rámci knižního rozhovoru vysvětlit. Ze všech mužů, které dívky v rámci dokumentárního filmu kontaktovali, s rozhovorem souhlasil jen jediný. Muž v rámci rozhovoru sdělil, že on sám má dvě děti, již pár let žije sám, internetové chatování je pro něj příležitost jako mluvit s lidmi, a právě ono kontaktování mladých dívek byl důvod jeho partnerského rozchodu. Sám pachatel si prý nebyl vědomý toho, že se dopouští trestné činnosti. Na závažnost a protiprávnost jeho jednání ho prý upozornila až jeho bývalá partnerka, která se o činech dozvěděla. On sám prý jen tušil, že při online komunikaci s mladými dívkami páchá trestnou činnost. Soudní znalec pro případy zneužívání a znásilnění a stejně tak sexuolog u tohoto muže neshledali projevy pedofilie. Dotazovaný muž sám v rámci rozhovoru vypověděl: „Líbí se mi to období, kdy se žena vyvíjí. V realitě bych si takhle mladé dívky oslovit nedovolil. Přes internet i to jde.“ [39]

Internet pro pachatele přináší především dostupnost oběti bez velkých finančních nákladů a pod rouškou internetové anonymity při získávání obětí z různých koutů jeho země či celého světa. Internet snižuje pachatelova rizika a sociální zábrany. Případné oběti ulehčují práci pachateli tím, že samy sebe natáčejí v různých, často intimních situacích, např. na mobilní telefony, používají webkameru při online komunikaci, navštěvují chatovací místnosti či užívají IM, vytvářejí blogy, uvádějí své osobní informace v profilech na sociálních sítích serverech apod.[40] Pro pachatele je tedy velmi snadné najít svou oběť na internetu.

Pachatel se nad obětí snaží získat co největší kontrolu, využívá jejích slabin, aby si získal její důvěru a nahnal ji strach. Na internetu může využívat nezkušenost

[39] PECHÁČKOVÁ, Marika. Kdo chytá v síti. Brno: BizBooks, 2020. ISBN 978-80-265-0919-6.s.44-48.
[40] HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie -internetové oběti, pachatele a kriminality*. Praha: Triton, 2012. ISBN 978-80-7387-545-9.s.141-142.

oběti, ať už jde o sexuální, či uživatelskou nezkušenost, může využít její osamělosti, zvědavosti či nedostatku peněz.

Pomocí vydírání a vyhrožování směřuje k oběti své požadavky. Oběť je zastrašována různými pohrůžkami a je na ni vyvíjen velký psychický nátlak. V některých případech se pachatel snaží v obětech vyvolat pocit, že to ony vzniklou situaci způsobily. Manipuluje jimi a pohrůžkami je zastrašuje a odrazuje od toho, aby se někomu svěřily se svým trápením.[41]

V povědomí veřejnosti figuruje mnoho stereotypních pohledů na profily pachatelů sexuálních trestných činů. Je těžké předcházet sexuálnímu zneužívání dětí ve chvíli, kdy si neuvědomujeme rozmanitost lidí, kteří se takového činu mohou dopouštět. Různí muži, ale také ženy sexuálně zneužívají děti a mladistvé různými způsoby, v různých kontextech a z mnoha různých důvodů. V médiích a široké veřejnosti existuje tendence spojovat sexuální zneužívání a komerční vykořisťování dětí výhradně s pedofilií. Weiss uvádí, že u pedofilie jde o erotické (erotosexuální) zaměření devianta na objekty v prepubertálním věku (tedy na chlapce a dívky bez znaku dospívání). Nejčastěji se zaměřují na děti ve věku 5-12 let. Pedofilové jsou lidé, kteří preferují fyzickou nezralost objektu, tedy nepřítomnost sekundárních pohlavních znaků (nepřítomnost pubického ochlupení a prsů u dívek, u homosexuálních pedofilů je to preference např. nepřítomnosti ejakulace o ochlupení u chlapců) (Weiss, 2002). Široká veřejnost často přehlíží fakt, že zcela „obyčejní“ lidé se mohou dopouštět sexuálního zneužívání a komerčního vykořisťování dětí. Protože mnoho lidí, kteří se dopouštějí sexuálního zneužívání dětí, nezapadá do stereotypů, které jsou hojně prezentovány v médiích, zůstává mnoho dětí společností zcela nechráněných. [42]

Právní kvalifikace vybraných kazuistických případů kybergroomingu

Pachatelé kybernetické kriminality se v souvislosti s nezletilými dětmi v rámci svého jednání mohou dopouštět trestných činů, jak proti důstojnosti v sexuální oblasti (Hlava III TrZ), tak trestných činů proti rodině a dětem (Hlava IV TrZ). V rámci diplomové práce představuji několik kazuistických příkladů se zaměřením na vybrané trestné činy v rámci páchání kybergroomingu. Jsou jimi

[41] HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie -internetové oběti, pachatele a kriminality*. Praha: Triton, 2012. ISBN 978-80-7387-545-9.s.142.
[42] HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie – internetové oběti, pachatele a kriminality*. Praha: Triton, 2012. ISBN 978-80-7387-545-9.s.57.

především ohrožování výchovy dítěte dle § 201 TrZ, svádění k pohlavnímu styku dle § 202 TrZ, navazování nedovolených kontaktů s dítětem dle § 193b TrZ, zneužití dítěte k výrobě pornografie dle § 193 a trestný čin vydírání dle § 175 TrZ, který řadíme mezi trestné činy proti svobodě a právům na ochranu osobnosti, soukromí a listovního tajemství (Hlava II TrZ).

Pachatelé se v rámci svého jednání mohou dopustit hned několika trestných činů najednou. Příkladem takového pachatele je mnohokrát medializovaný případ mladíka z Děčína. Své oběti mladý muž z Děčína trápil několik let, první dívky na internetu kontaktoval ještě jako nezletilý v roce 2009. Velmi důmyslným způsobem z nich vylákal jejich intimní fotografie. Když uspěl, začal své cíle vydírat. Hrozil jim zveřejněním fotek, pokud mu nebudou po vůli.[43] Oznámení bylo podáno na Policii v roce 2015 a během vyšetřování bylo zjištěno, že pachatel na internetu sexuálně zneužil více jak 160 dívek. Fyzicky žádné z dívek neublížil, vše se odehrávalo v kyberprostoru. Obžaloba byla podána pro zločin sexuálního nátlaku, šíření pornografie, výroby a jiné nakládání s dětskou pornografií, zneužití dítěte k výrobě pornografie, pohlavní zneužití, navazování nedovolených kontaktů s dítětem a ohrožování výchovy dítěte.[44] Nepravomocně byl v roce 2018 odsouzen soudem I. stupně k odnětí svobody na šest a půl roku. Kromě vězení by měl absolvovat také ochranou sexuologickou léčbu.[45] Tento případ je mimo jiné ukázkové chování zneužívání dětí na internetu.

Kazuistické případy

Obvodní ředitelství Praha II, Služba kriminální policie a vyšetřování, 5. oddělení se v rámci své činnosti zabývá případy, které se týkají kriminality mládeže, včetně kybergroomingu. Pro účely této práce mi se souhlasem byly poskytnuty anonymizované kazuistiky, na kterých bude následně rozebrána skutková podstata vybraných trestných činů.

Kazuistika č. 1

Pachatel přes sociální síť Instagram kontaktoval poškozenou nezletilou, která si ho na jeho žádost přidala mezi "sledující osoby". Následně ji pachatel bez

[43] https://www.lidovky.cz/domov/mladik-mel-zneuzit-163-divek.A171206_121339_ln_domov_jho [cit. 2024-3-14].
[44] https://www.lidovky.cz/domov/mladik-mel-zneuzit-163-divek.A171206_121339_ln_domov_jho [cit. 2024-3-14].
[45] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 3. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. ISBN isbn978-80-7380-849-5.s.358.

jejího předchozího vyžádání zaslal několik fotografií svého přirození a dále dívce opakovaně nabízel sexuální služby za peníze. Na dotaz poškozené dívky, zda pachatel ví, kolik je jí let odpověděl, že se domnívá, že je dívce 16 let. Nezletilé dívce však bylo pouhých 10 let. Potom, co se pachatel dozvěděl o věku nezletilé, přerušil komunikaci. Šetřením však bylo zjištěno, že pachatel kontaktoval i spolužáky poškozené a vybízel je k osobní schůzce a k pohlavnímu styku. K faktickému setkání nezletilých a pachatele již nedošlo. Jednání pachatele bylo kvalifikováno jako ohrožování výchovy dítěte dle § 201 odst. 1 písm. a) TrZ a svádění k pohlavnímu styku dle § 202 odst. 1 TrZ. Pachatel se ke skutku plně doznal a projevil účinnou lítost, a proto byla věc skončena dle § 307 odst. 1 TrŘ.

Kazuistika č. 2

Pachatel navázal komunikaci na sociální síti Instagram s poškozenou nezletilou, která dále pokračovala přes SMS zprávy, a která byla ze strany podezřelého záměrně směřována k intimním tématům. Pokud nezletilá pachateli odmítala odpovídat, vyhrožoval ji, že zveřejní na dětské seznamce a sociálních sítích smyšlený inzerát obsahující osobní údaje poškozené a nabídku jejích sexuálních služeb. Nezletilá dívka se svěřila svému otci, který věc ohlásil policii. Po ztotožnění pachatele bylo zjištěno, že se takového jednání dopouští opakovaně. Jednání pachatele bylo kvalifikováno jako trestný čin vydírání dle § 175 odst. 1 TrZ a trestný čin ohrožování výchovy dítěte dle § 201 odst. 1 písm. a) TrZ.

Kazuistika č. 3

Pachatel kontaktoval prostřednictvím mobilní aplikace Tik Tok poškozenou nezletilou dívku, se kterou následně komunikoval jak přes aplikaci Tik Tok, WhatsApp, tak i SMS zprávy. Explicitní konverzace se sexuální tematikou, sexuálními návrhy, postupy, co vše chce na nezletilé vykonat a zasílání videonahrávek z pachatelovy strany vyústilo až v osobní schůzku při které došlo k fyzickému kontaktu nezletilé a pachatele. K této kazuistice dodávám, že poškozené bylo 14 let a pachateli 40 let. Pachatel chtěl u dívky strávit noc, což se nesetkalo s přívětivou reakcí jejích rodičů a dívka následně utekla spolu s pachatelem do jiného města. Věc byla oznámena policii rodičemi nezletilé ihned po jejím útěku a kvalifikována jako trestný čin navazování nedovolených kontaktů s dítětem dle § 193b TrZ a ohrožování výchovy dítěte dle § 201 odst. 1 písm. a) TrZ.

Kazuistika č. 4

Mladistvá poškozená začala přes sociální síť Instagram komunikovat s neznámým pachatelem, který ji nabídnul peníze za to, že mu zašle svá intimní videa a fotografie. Poškozená tak s vidinou možného finančního obnosu učinila a poslala mu několik fotografií a videí, na kterých explicitně ukazuje svůj genitál. Pachatel poté začal nezletilé dívce vyhrožovat, že zaslaná videa a fotografie rozešle její rodině a spolužákům a následně požadovat finanční hotovost za to, že zaslaný intimní obsah smaže. Po dohodě o způsobu úhrady poškozená finanční obnos zaslala. Zaslání peněz však pachatele nijak nezastavilo a začal po poškozené požadovat ještě další finanční obnos. Věc oznámila sama poškozená, bohužel se osobu pachatele nepodařilo ztotožnit. Pachatelovo jednání bylo posouzeno jako trestný čin vydírání dle § 175 odst. 1 TrZ a trestný čin zneužití dítěte k výrobě pornografie dle § 193 odst. 1 TrZ.

Ohrožování výchovy dítěte

Trestný čin ohrožování výchovy dítěte je upraven v § 201 TrZ. Pachatelovu jednání se v souvislosti s obtěžováním dětí na internetu přičítá kvalifikovaná skutková podstata trestného činu ohrožování výchovy dítěte dle § 201 odst. 1 písm. a) TrZ, který zní: „kdo, byť i z nedbalosti, ohrozí rozumový, citový nebo mravní vývoj dítěte tím, že ho svádí k zahálčivému nebo nemravnému životu bude potrestán odnětím svobody až na dvě léta“. Takto kvalifikované škodlivé jednání spočívá v narušení ochrany zdravého rozumového, citového a mravního vývoje dítěte, což může výrazně ovlivnit budoucí mentální i sociální vývoj dítěte. Závažnost tohoto jednání se samozřejmě hodnotí na základě konkrétních okolností individuálních případů, nicméně jakákoli psychická či emocionální újma, která je dítěti způsobena zvyšuje závažnost případu. Oběť se může potýkat s vážnými psychickými i fyzickými následky, které mohou ovlivnit její celoživotní vývoj.

Z ustanovení § 201 odst. 1 TrZ vyplývá, že k narušení rozumového, citového nebo mravního vývoje osoby mladší, než osmnáct let nemusí fakticky dojít, neboť k trestnosti jednání pachatele stačí, jestliže tento škodlivý následek alespoň hrozí.[46]

[46] DRAŠTÍK, A., DURDÍK, T., FREMR, R., RŮŽIČKA, M., SOTOLÁŘ, A. *Trestní zákoník: Komentář*. [Systém ASPI]. Wolters Kluwer [cit. 2023-9-24]. ASPI_ID KO40_2009CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X

Pachatelem trestného činu ohrožování výchovy dítěte podle § 201 odst. 1 písm. a), b) nebo c) může být jakákoli fyzická osoba, tedy nejen osoba, která má zvláštní povinnost o ohrožené dítě pečovat. Jednání uvedené v odst. 1 písm. d) se může dopustit pouze fyzická osoba, která má zvláštní povinnost o dítě pečovat či vůči dítěti vykonává práva a povinnosti plynoucí z její rodičovské odpovědnosti. [47]

V kazuistice č. 1 se pachatel dopustil trestného činu ohrožování výchovy dítěte dle § 201 odst. 1 písm. a) TrZ, tedy svádění k zahálčivému či nemravnému životu tím, že kontaktoval nezletilou dívku, které zasílal fotografie s explicitním sexuálním obsahem, můžeme se domnívat, že vedl i konverzaci se sexuální tematikou, jako je tomu například v kazuistice č. 2 a 3.

Senát nejvyššího soudu se ve své praxi zabýval ohrožováním výchovy dítěte ve věci sp. zn. 7 Tdo 306/2023, kde mimo jiné judikoval, že právní posouzení skutku obviněného bylo nesprávně právně posouzeno soudem odvolacím. Odvolací soud ve svém rozhodnutí konstatoval, že krátkodobé jednání obviněného vůči nezletilé poškozené nedosáhlo takové intenzity, aby mohlo být posuzováno jako trestný čin, konkrétně jako přečin ohrožování výchovy dítěte dle § 201 odst. 1 písm. a) TrZ. Dále odvolací soud poukázal na skutečnost, že konverzace mezi obviněným a poškozenou díky včasnému a příkladnému postoji otce poškozené nebyla způsobilá ohrozit mravní vývoj tohoto dítěte, z jehož výpovědi mimo hlavní líčení lze mít za prokázané, že rodiče jí vštípili dobré mravní zásady.

Dle mého názoru dlouhodobost a intenzita jednání není podmínkou pro spáchání trestného činu ohrožování výchovy dítěte a to, jaké mravní zásady poškozená od svých rodičů obdržela a včasný zásah otce není nic, co by pachatele vymanilo z trestní odpovědnosti za spáchání tohoto trestného činu.

Senát nejvyššího soudu se k tomuto vyjádřil tak, že došlo k naplnění skutkové podstaty trestného činu podle § 201 odst. 1 písm. a) TrZ, a že se nejedná pouze o přípravu tohoto trestného činu. Nejvyšší soud argumentoval tím, že postoj otce nezletilé poškozené, který zakročil, je skutečností, která nemůže v žádném ohledu společenskou škodlivost jednání obviněného snižovat, neboť pouze zabránil vzniku škodlivého následku.

[https://www.aspi.cz/products/lawText/13/6500/126/komentar-wkcr-c-40-2009-sb-trestni-zakonik-komentar]

[47] tamtéž

Svádění k pohlavnímu styku

V souvislosti s pácháním kybergroomingu dochází v návaznosti na trestný čin ohrožování výchovy dítěte k naplnění skutkové podstaty dalšího trestného činu, a to svádění k pohlavnímu styku dle § 202 TrZ. Svádění k pohlavnímu styku spočívá v nabídnutí, slíbení nebo poskytnutí dítěti nebo jinému za pohlavní styk s dítětem, pohlavní sebeukájení dítěte, jeho obnažování nebo jiné srovnatelné chování za účelem pohlavního uspokojení úplatu, výhodu nebo prospěch. Pachateli takového trestného činu hrozí odnětí svobody až na dvě léta nebo peněžitý trest a pokud pachatel naplní znaky kvalifikované skutkové podstaty v § 202 odst. 2 TrZ jako je to, že čin spáchá na dítěti mladším 15 let, ze zavrženíhodné pohnutky, pokračuje v páchání činu po delší dobu či páchá trestnou činnost opětovně.

Hlavním smyslem dané právní úpravy je posílení ochrany zdravého duševního a mravního vývoje osob, které ještě nepřekročili osmnáctý rok svého věku a u kterých může právě s ohledem na jejich doposud neukončený vývoj dojít k vážnému a nežádoucímu narušení jejich hodnotového systému v důsledku nevhodného chování ze strany třetí osoby v sexuální oblasti. [48]

Trestného činu „svádění k pohlavnímu styku“ se dopustil pachatel v kazuistice č. 1, tím že nezletilou vybízel k pohlavnímu styku, za který nabízel finanční obnos, s vidinou dosažení svého vlastního sexuálního uspokojení.

Vydírání

Kybernetický útok (kyberšikana, kybergrooming apod.) může v některé fázi zahrnovat i vydírání. S vydíráním na internetu se často potýkají i dospělí lidé, kteří by však se svými zkušenostmi a schopnostmi řešit problémy měli být schopni vyhodnotit a vyřešit danou situaci. Nicméně nelze zlehčovat závažnost takového útoku, byť je směřován vůči dospělé osobě. Emocionální a psychický nátlak je velmi náročný pro každého jednice. Dovolím si ale tvrdit, že pro děti daleko více než pro dospělé. Vzhledem k nedostatku životních zkušeností a nedostatečného emocionálního, psychického, fyzického i morálního vývoje je dítě k nátlaku a vydírání daleko náchylnější. Důvěřivost dítěte, stejně tak jako nedostatek zkušeností je něco, co je u dítěte naprosto přirozené. Nedospělý jedinec je zvyklý následovat autority, podřizovat se starším, poslouchat a plnit příkazy, a proto není

[48] tamtéž

divu, že se děti nejen v kyberprostoru potýkají s nátlakem a vyhrožováním. Dalším důvodem, proč se děti dostávají do situací, kdy pod pohrůžkou či nátlakem plní to, co vyděrač žádá, je snaha ochránit svou reputaci, zdraví, život či mají strach z odhalení jednání, kterého se dopustili a bojí se trestu.

Trestný čin vydírání nalezneme v Hlavě II v ustanovení § 175 TrZ. Objektem trestného činu vydírání je svobodné rozhodování člověka. K dokonání trestného činu vydírání stačí samotné užití násilí, pohrůžky násilím, nebo pohrůžky jinou těžkou újmou, přičemž nemusí dojít k tomu, co pachatel svým jednáním sleduje.[49] V souvislosti s vylákáním citlivého obsahu z dětí pachatelé však spíše používají pohrůžky týkající se zveřejnění intimního obsahu zobrazující dítě, které vydírají.

Jestliže pachatel vyhrožoval poškozeným dívkám tím, že jejich erotické fotografie zveřejní v rozporu se smlouvou, na jejímž základě byly vytvořeny (že je nechá otisknout v časopisech vycházejících v České republice nebo, že je předá rodičům poškozených), není vyloučeno takovou formu nátlaku na poškozené, jímž je pachatel nutí, aby něco konaly, považovat za významný zásah do jejich osobního života, kterým je naplněn zákonný znak tr. činu vydírání spočívající v pohrůžce jinou těžkou ujmou. [50]

Pro naplnění uvedeného zákonného znaku se však nevyžaduje, aby pohrůžka jiné těžké újmy u poškozeného skutečně vyvolala obavy ze způsobení takové újmy. [51]

Pohrůžka zveřejnění intimních fotografií poškozeného skutečně může být pohrůžkou jiné těžké újmy ve smyslu § 175 odst. 1 trestního zákoníku a z hlediska naplnění subjektivní (ale i objektivní) stránky uvedeného trestního činu je irelevantní, že obviněný neměl k dispozici intimní fotografie poškozené a fakticky ji nemohl jinou těžkou ujmu způsobit. Fakt, že obviněný to možná pouze „zkoušel“, tedy využil nezpůsobilé prostředky, nemůže jeho trestní odpovědnost vyloučit, neboť v době svého jednání nemohl vědět, zda mu poškozená uvěří a jeho nátlaku se podvolí, či nikoli. [52]

---

[49] DRAŠTÍK, A., DURDÍK, T., FREMR, R., RŮŽIČKA, M., SOTOLÁŘ, A. *Trestní zákoník: Komentář*. [Systém ASPI]. Wolters Kluwer [cit. 2023-9-24]. ASPI_ID KO40_2009CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X. [https://www.aspi.cz/products/lawText/13/6500/126/komentar-wkcr-c-40-2009-sb-trestni-zakonik-komentar]

[50] Usnesení NS, sp. zn. 8 Tdo 612/2011 ze dne 15.6.2011.

[51] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 3. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. ISBN isbn978-80-7380-849-5.s.258.

[52] Usnesení NS, sp.zn. 7 Tdo 1579/2018 ze dne 23.1.2019. Právní věta autora.

Navazování nedovolených kontaktů s dítětem

Trestný čin navazování nedovolených kontaktů s dítětem je popsán v kazuistice č. 3, kdy pachatel navrhl a následně provedl setkání s nezletilou dívkou s úmyslem vykonání pohlavního styku, ke kterému nakonec nedošlo.

Ustanovení § 193b TrZ zní: „kdo navrhne setkání dítěti mladšímu patnácti let v úmyslu spáchat trestný čin podle § 187 odst. 1, § 192, 193, § 202 odst. 2 nebo jiný sexuálně motivovaný trestný čin, bude potrestán odnětím svobody až na dvě léta“. Objektem tohoto trestného činu je zájem na ochraně dětí mladších patnácti let před navozováním takových kontaktů se sexuálním účelem, které by mohly narušit jejich mravní a tělesný vývoj. Trestně postižitelný je i samotný návrh na setkání, který pachatel učinil dítěti mladšímu patnácti let za účelem dopustit se na něm některého ze sexuálně motivovaných trestných činů. [53]

Zneužití dítěte k výrobě pornografie

Trestný čin „zneužití dítěte k výrobě pornografie“ dle § 193 TrZ se také týká narušení mravního vývoje dítěte. V souvislosti s pácháním kyberkriminality v sexuální oblasti se pachatelé tohoto trestného činu velmi často dopouštějí. Základní skutková podstata ustanovení § 193 TrZ zní: „kdo přiměje, zjedná, najme, zláká, svede nebo zneužije dítě k výrobě pornografického díla nebo kořistí z účasti dítěte na takovém pornografickém díle, bude potrestán odnětím svobody na jeden rok až pět let“.

Co se týká popsaného jednání „přiměje, zjedná, najme, zláká, svede nebo zneužije dítě“, pak jde charakterizovat takto: „Přimět lze dítě využitím vlivu, který vyplývá ze vzájemného vztahu s pachatelem. Zjednáním se rozumí uzavření dohody (i konkludentní) mezi dítětem a pachatelem, že bude dítě participovat na výrobě pornografického díla. Dohoda předpokládá souhlasný projev vůle obou stran. Najmutí je speciálním případem zjednání, neboť se jedná tako o dohodu, jejímž znakem je ovšem úplata, nemusí mít však bezpodmínečně peněžní podobu. Zlákáním je získání dítěte k účasti zejména předstíráním určitých výhod, pozitiv apod. (nikoliv však úplatou), zejména když dítě váhá. Svedení spočívá v tom, že

[53] tamtéž

pachatel úmyslně vzbudí (jinak než zlákáním) v dítěti rozhodnutí účastnit se výroby pornografického díla. [54]

Oslovování nezletilých dětí na internetu má velmi často za cíl právě výrobu pornografického díla. Kromě toho, že pachatelé lákají oběti na peněžní obnos, jako je tomu v kazuistice č. 4, se setkáváme například s tím, že se pachatelé schovávají za falešné modelingové agentury a žádají obnažené fotografie či videa. Postup je více méně vždy podobný, ať už je oběť zlákána peněžním obnosem, kariérním růstem (např. výše zmiňované falešné modelingové agentury), nebo si k pachateli vytvořila citové pouto a následuje ho. Pokud pachatel vyláká z oběti intimní fotografie či videa v mnohých případech pak žádá pod pohrůžkou zveřejnění intimního obsahu zobrazující dítě další intimní obsah.

Otázkou mnoha soudních sporů zůstává, co vše je možné označit za pornografické dílo. V trestním zákoníku pojem „pornografické dílo“ vymezen není, nicméně vymezuje jej judikatura, která respektuje definici dle právní nauky a komentáře k trestnímu zákoníku, podle kterého je pornografickým dílem takové dílo, které zvláště intenzivním a vtíravým způsobem zasahuje a podněcuje sexuální pud, překračuje podle převládajících názorů ve společnosti uznávané hranice sexuální slušnosti, uráží neakceptovatelným způsobem cit pro sexuální slušnost, vyvolává pocit studu.[55]

Nutno však dodat, že vnímání toho, co je a není pornografické dílo, se historicky vyvíjí a závisí na subjektivním individuálním vnímání každého člověka. Proto někdy vyvstává otázka, co je a není pornografickým dílem a v návaznosti na to, zda byl či nebyl spáchán trestný čin zneužití dítěte k výrobě pornografie jako je tomu například v rozhodnutí sp. zn. 6 Tdo 832/2021 ve věci, která se týkala zneužití dítěte k výrobě pornografie. V této věci se mimo jiné řešila otázka, která díla lze označit jako díla pornografická. Odvolací soud a následně i soud dovolací argumentoval, že za dětskou pornografii nelze označit snímky oděných, dostatečně zahalených dětí, byť se jejich genitálie na fotkách mohou rýsovat a přispívat k sexuálnímu zájmu. Státní zástupce však oponoval tím, že děti byli na fotkách tzv.

[54] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 3. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. ISBN isbn978-80-7380-849-5.s.357.
[55] DRAŠTÍK, A., DURDÍK, T., FREMR, R., RŮŽIČKA, M., SOTOLÁŘ, A.*Trestní zákoník: Komentář*. [Systém ASPI]. Wolters Kluwer [cit. 2023-9-24]. ASPI_ID KO40_2009CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X. [https://www.aspi.cz/products/lawText/13/6500/126/komentar-wkcr-c-40-2009-sb-trestni-zakonik-komentar]

hypersexualizovány. Na snímcích byly zachyceny s velkými náušnicemi, podpatky, podvazky či krajkami, což dle státního zástupce vyvolávalo sexuální asociace. Samy zobrazené děti a jejich rodiče vnímaly snímky jako pornografické. Nejvyšší soud však dovolání odmítl a v souvislosti s otázkou týkající se pojmu pornografické dílo podpořil odvolací soud, který mimo jiné označil, které snímky jsou pornografické a pojem pornografického díla více dovysvětlil. Odvolací soud argumentuje tím, že z hlediska zaujímaných póz a použitých kostýmů se ne vždy zcela odlišuje od snímků, které bývají pořizovány např. v rámci tanečního sportu, aerobiku apod. Také dle odvolacího soudu lze snímky porovnat s fitness pózováním v plavkách. Nejvyšší soud neshledal důvody k odchýlení se od této argumentace a námitka tak byla odmítnuta.

Typické zneužití dítěte k výrobě pornografie pomocí slíbeného peněžního zisku a následné vydírání ze strany pachatele je zobrazeno v kazuistice č. 4. Oběť je, dle mého názoru, vystavena velkému strachu ze zveřejnění intimního materiálu, na kterém je zobrazena a je připravena udělat cokoli pro to, aby se její rodiče či spolužáci nedozvěděli o tom, čeho se dopustila. Nicméně ani zaslání peněžního obnosu pachateli či další intimní snímky jako úplata za nezveřejnění intimního obsahu, nezastaví pachatele od dalšího vydírání oběti.

Dětská pornografie je, dle mého názoru, velmi závažné téma, které se objevuje jak při kyberšikaně, tak při kybergroomingu a mělo by se mu od společnosti dostávat zvýšené pozornosti. Přestože je výroba a jiné nakládání s dětskou pornografií trestným činem dle § 192 TrZ stále existují webové stránky, které se zaměřují pouze na dětskou pornografii a evidentně se tak zveřejňování obdržených materiálů či výroba pornografického obsahu zobrazující nezletilé děti stává pro některé lidi byznysem. Společnost by měla věnovat zvýšenou pozornost všem trestným činům, které zahrnují děti, a to zejména ty sexuálně motivované včetně rozsáhlé problematiky dětské pornografie.

Brzká sexuální zkušenost může dle mého názoru ovlivnit psychické i fyzické zdraví dítěte a celkový mentální vývoj jedince. Neakceptovatelný, nemorální a protizákonný obsah zobrazující dětskou pornografii by neměl být přehlížen či nečinností tiše akceptován.

Rozhovor s vyšetřovateli kybernetické kriminality

Pro výzkumnou část diplomové práce jsem zvolila metodu rozhovoru, který mi poskytli pan por. Bc. Radovan Hlad, vedoucí stálé výjezdové skupiny kriminální služby obvodního ředitelství policie Praha II spolu s panem Mgr. Janem Křemenem vyšetřovatelem V. oddělení obecné kriminality obvodního ředitelství policie Praha, který se v rámci své práce specializuje na kriminalitu mládeže.

V rámci své činnosti se por. Bc. Radovan Hlad zabývá případy kybernetické kriminality, provádí vyšetřování, při kterém spolu s technickými odborníky zajišťuje důkazy, provádí výslech a shromažďuje důkazy pro další orgány činné v trestním řízení. Druhým respondentem je por. Mgr. Jan Křemen vyšetřovatel V. oddělení obecné kriminality obvodního ředitelství policie Praha, která se specializuje na kriminalitu mládeže věnuje se především případům, které se týkají dětské pornografie a kybergroomingu.

V rámci rozhovoru budou zodpovězeny otázky, které se týkají příčin zneužívání dětí na internetu, průběhu vyšetřování. Zajímá mě jeho pohled na problematiku zneužívání dětí na internetu obecně, jaký je současný stav, a zda bylo zaznamenáno zhoršení situace v souvislosti se stavem, který nastal v období pandemie COVID-19. Dále bych ráda pro účely diplomové práce zodpověděla otázky, které se týkají kvalifikace trestné činnosti páchané na dětech v internetovém prostředí, otázky, které se týkají osoby pachatele a osoby oběti a v neposlední řadě bych se ráda zaměřila na otázky, které se týkají prevence a osvěty kybernetické kriminality a zneužívaní děti na internetu.

Přepis rozhovoru

Tazatel: Daniela Podzimková

Respondenti: por. Bc. Radovan Hlad a por. Mgr. Jan Křemen

R1: por. Bc. Radovan Hlad

R2: por. Mgr. Jan Křemen

T: Jakým způsobem je páchána kybernetická kriminalita na dětech?

R1: Dochází k navázání kontaktu prostřednictvím seznamovacích sítí, které jsou určené vlastně pro tu věkovou skupinu, které se to nejvíce týká. Spočívá to v tom, že se někdo připojí buď pod nějakou fiktivní adresou, smyšlenu legendou na nějaké seznamce nebo sociální síti, která je pro děti svým způsobem atraktivní nebo

k nějaké komunikaci mezi mládeží a mnohdy se vydává za někoho, kým vůbec není. To znamená, že má smyšlenu legendu, pod kterou chce navázat se svou předpokládanou nebo budoucí obětí komunikaci a jde o to, že identita může být úplně smyšlená nebo může být nějakým způsobem poopravená…například si pachatel snižuje věk nebo používá falešné fotografie, ale může si nechat i svou identitu, takže může být třeba dospělý a snaží se s tím dítětem řešit nějaký problém, který dítě má, a není schopno řešit ho třeba v rodině, ve škole nebo v okolí svých blízkých kontaktů… A to dítě potom získává důvěru k tomu fiktivnímu protihráči a navážou nějaký kontakt a v okamžiku, kdy se dostane do určité formy závislosti a podobně, tak toho predátor nebo pachatel, může zneužít ve svůj prospěch. Asi tak bych to viděl já…Taky je důležitý uvědomit si, že hromadu těch internetových kontaktů a setkání na internetu a veřejných sítích, může směřovat k tomu, že pachatel usiluje o osobní kontakt, a ten pak může být daleko větší problém než jen dopisování přes sítě.

T: Proč se pachatelé dopouštějí kybernetické kriminality páchané na dětech? Jaká je jejich motivace v této trestné činnosti?

R1: No tak, zřejmě je motivace taková, že normálním kontaktem s těmi dětmi nejsou schopni navázat nějaký styk, protože běžně nepřichází do prostředí, kde se pohybují děti a jednoznačně je to nějaké sexuální uspokojení, jedná se o sexuálně motivovanou trestnou činnost. Těžko říct, že by to někdo dělal pro peníze. Chtějí uspokojit nějaké své sexuální potřeby, jelikož získání nějakého většího majetku na dítěti nepřichází v úvahu…

R2: Za mě je určitě důvodem i to, že jsou lidé obecně znudění například klasickou pornografií a hledají něco nového, nemají se na co koukat, co dělat a chtějí nový zážitek. A takhle se to reálně stupňuje…

T: Ale například v případech výroby a šíření dětské pornografie můžou být pachatelé motivovány finančním ziskem.

R1: Ano, tam samozřejmě může jít o finanční motivaci…Lidé, kteří získají nějaké fotky a videa to pak dál prodávají a je to samozřejmě obrovská obchodní síť. Ta dětská pornografie se šíří hlavně tímhle tím způsobem a proudí to hlavně z Asie. A samozřejmě třeba existují stránky s dětskou pornografií, které jsou zpoplatněné.

R2: Jako určitě je to jedna z forem, ale mnohem snazší je pro toho pachatele vydírat toho, kdo ty fotky pošle…

T: Na jakých internetových platformách probíhá kybernetická kriminalita páchaná na dětech?

R2: Všude tam, kde je to možné. Teď je hodně populární Instagram, Snapchat, Tik Tok…dřív se hodně používalo Omegle, což je nyní už zrušené. A Discord se ještě hodně používá.

T: Jaké trestné činnosti se pachatelé nejčastěji dopouštějí v rámci kybernetické kriminality na dětech?

R1: Tak určitě je to svádění k pohlavnímu styku, zneužití dítěte k výrobě pornografie, šíření pornografie, ohrožování výchovy dítěte, vydírání, navazování nedovolených kontaktů s dítětem, výroba a jiné nakládání s dětskou pornografií a pokud dojde k osobní schůzce, může dojít i například k naplnění skutkové podstaty znásilnění, sexuálního nátlaku nebo pohlavního zneužití, to už je pak samozřejmě daleko závažnější, když se to přesune z kyber prostoru do reality…

T: Myslíte si, že si pachatelé uvědomují, že se dopouštějí trestné činnosti?

R1: Určitě si to uvědomují…možná ti mladší pachatelé do 12 let si to neuvědomují, ale od 15 let už každý ví, co páchá. Je to navázané na věk pachatele…Spíš vnímám, že lidem chybí jakási zodpovědnost a neuvědomují si, jaké může mít jejich jednání dlouhodobé následky…napadá mě teď jeden příklad, kdy holčičku, která byla zneužívaná na internetu, pachatel trvale poškodil a trest, který dostal je bagatelní oproti tomu, co způsobil, protože ta holčička se z toho bude vzpamatovávat pět, možná deset let a možná se nevzpamatuje nikdy, to se klidně může stát.

T: Co za trest dostal?

R1: Dostala podmínečný trest.

T: Byla to žena?

R1: Byla to žena, vydávající se za mladíka…

T: Co bylo motivací v jejím případě?

R1: Zrovna u tohoto případu těžko říct co bylo její motivací…řekl bych, že jen zábava, zkoušela si, co může vymyslet…

T: Jsou i případy, kdy samo dítě vyvíjí aktivní účast na komunikaci s pachatelem?

R2: Ano i děti vyvíjí vlastní iniciativu, chovají se vyzývavě, a dokonce si i vymýšlejí to, že na nich byla spáchána trestná činnost.

T: Proč si to vymýšlejí?

R2: Velmi často se to děje v rozvedených rodinách, kde děti chtějí pozornost a dělají naschvály rodičům.

T: Jakého věku jsou děti, které se stávají oběťmi kybernetické kriminality?

R1: Začíná se od toho nejútlejšího věku. Já bych řekl, že se to týká už dětí od pěti let, ale u případů, které zaznamenáváme je dětem mezi jedenácti a čtrnácti lety.

T: To je velmi brzký věk…stávají se obecně oběťmi spíše dívky nebo chlapci?

R2: Týká se to chlapců stejně jako dívek …

T: Co se týče pachatelů kybernetické trestné činnosti, které se dopouštějí na dětech, jsou u nich shledávány nějaké deviace?

R1: Určitě. Jednotlivé deviace, ale nejsou úplně jednoduchá záležitost a myslím si, že i odborníci v tom nemají úplně jasno. Je to otázka, která chce více znalců a velikou profesní zkušenost. Jde o to, že u hodně pachatelů, kteří byli vyšetření vychází, že jsou úplně v pořádku…nikdo neshledá to, že by byli nemocní. Všechno to záleží na znaleckých posudcích, a to už pak není otázka pro policii, ale pro odbornou lékařskou vědu.

R2: Já, jak už jsem říkal, například u té dětské pornografie, těch pedofilů nebo lidí s nějakou deviací podle mě není zas tolik. Ale obecně toho pornografického materiálu je kvantum a ty lidi přestane bavit sledovat klasické porno, a tak hledají něco nového. V podstatě to má stupňující tendenci…

T: Skutečných pedofilů tedy moc není?

R2: Já to mám zkreslené tím, že v tom pracuju… mám pocit, že na dětské porno kouká snad každý. Jak říkám, ze zkušenosti, z velké části je to nuda těch lidí…

T: Kdo bývá oznamovatelem kybernetické kriminality týkající se dětí?

R2: Nejčastěji rodiče, učitelé ze školy, taky kamarádi té oběti a někdy se i stane, že oznamuje sama oběť.

T: Jakým způsobem je vyšetřována kybernetická kriminalita páchaná na dětech?

R2: Já tu kybernetovou kriminalitu řeším tak, že mi přijde většinou zpráva z policejního prezídia, že mám něco prověřit, takže v tom není zapojený výjezd, ani nikdo jiný a už nám to jde konkrétně na oddělení. Tam to funguje většinou tak, že organizace, která zaznamenala nějaký nevhodný obsah *(pozn. NCMEC, National Center for Missing & Exploited Children)* už má ta data zajištěná a já následně po tom, co mi to pošle policejní prezidium procházím ty materiály, jako například fotografie, videa nebo snímky nějaké komunikace a zjišťuji komu, kdo co posílal, zakládám nový spis a rozesílám na ostatní oddělení, kterých se to týká.

R1: Tady v souvislosti s tím vyšetřováním je důležité zmínit, že mladistvý nezletilý požívá v rámci trestního práva zvláštní ochrany, což znamená, že pří výslechu je nutná přítomnost zákonného zástupce dítěte, OSPODU *(pozn. orgánu sociálně- právní ochrany dětí)*, popřípadě nějakého znalce. A vzhledem k tomu, že se jedná o děti, je třeba vést výslech s rozvahou tak, aby se nemusel opakovat.

T: Existuje i nějaká mezinárodní spolupráce?

R2: Ta mezinárodní spolupráce funguje zrovna v tomhle případě dobře, což je u mezinárodních spoluprací celkem neobvyklé. Veškeré tyhle sítě, jako například Meta, jsou v programu NCMEC *(pozn. National Center for Missing & Exploited Children)*, což je organizace, která sbírá a analyzuje veškerá nahraná data, která se objeví a následně je prověřuje. Když zaznamenají incident, udělají kopii obrázků, pak to pošlou na Europol nebo Interpol, ty to pak pošlou do dané země a v té dané zemi se pak prověřují atributy, například na koho je vedené telefonní číslo a tak podobně.

T: A v návaznosti na tohle vyšetřování odebíráte zařízení, jako notebook nebo mobilní telefon, ze kterých pak sbíráte digitální stopy?

R2: Ano, z těch zařízení ty data pak taháme, ale většinou už je máme zajištěné, právě proto, že je sbírá ta organizace *(pozn. organizce NCMEC)*, takže i když v tom počítači ten důkaz není, tak my ho máme. Nicméně prověřujeme, jestli tam není něco dalšího. U těch mobilních telefonů se často obhajují tím, že ho ztratili a používal ho někdo jiný, ale ve většině případů se lidé přiznají.

T: Při vyšetřování identifikujete pachatele také podle IP adresy?

R2: Ano, používá se to, ale už to není, co to bývalo. Teď existují plovoucí IP adresy a tím je to celé složitější…A zároveň ve většině případů je již pachatel ztotožněný, protože k nám to přichází od té organizace *(pozn. organizace NCMEC)*.

T: Jaká je úspěšnost v dopadení pachatele?

R2: Já bych řekl, že téměř 100 %.

R1: Tam je důležité uvědomit si jednu věc, že u těchto věcí existuje obrovské množství latentní kriminality, která nejde objasnit, protože ty lidi se stydí, bojí se ostudy a tak dále…takže hromada věcích je skrytá, a to nikdy nevyjde na povrch, takže to my nezjistíme a neřešíme. Objasněnost nám tedy nedělá problém, ale bohužel si myslím, že ta latence je strašně velká.

R2: Když se o tom policie dozví, tak se na 99 % dozví pachatele. O to, o čem nevíme, nevíme...kolik toho je těžko říct…asi hodně, a hlavně ty věci vychází na povrch s nějakým časovým odstupem, takže nemusí být aktuální. Může jít o dva, tři roky staré kauzy…A co se týká těch mravnostních věcí, tak když je to oznámené, je většinou znám i pachatel.

T: Má policejní orgán dostatek prostředků pro vyšetřování kybernetické kriminality páchané na dětech?

R1: Já bych řekl, že tohle není tak o těch prostředcích, ale o lidech. Je to o kapacitě lidí.

R2: Já třeba řeším případ, kde je patnáct tisíc fotek, které musím projít, jsem na to sám a k tomu mám samozřejmě případy, na kterých taky musím pracovat. A jsem samozřejmě tlačený časem a musím to nějak vyhodnotit.

R1: Přesně tak… a je otázkou, jestli v reálné pracovní době je vůbec schopný se tomu případu věnovat a kvalitně ho vyhodnotit. Druhá věc je ta, že by to měl vyhodnotit nějaký znalec, protože součástí vyšetřování jsou i znalecké posudky.

T: Předpokládám, že znalecké posudky jsou ale velmi nákladné.

R2: Ano, znalecké posudky jsou extrémně problematická věc. Jedna věc je ta, že psychiatricko-psychologický posudek dítěte stojí 120.000 Kč z rozpočtu policie. Někdy má smysl, ale velice často smysl nemá vůbec…

R1: Další věcí je pak to, že znalců na dětskou psychiatrii je málo a na znalecké posudky jsou dlouhé čekací doby…ty případy se pak strašně komplikují…

T: Proč postrádá znalecký posudek smysl?

R2: My se toho ze znaleckého posudku tolik nedozvíme. U znaleckého posudku se člověk dozví, zda dítě vypráví příběh věrohodně, zda svému příběhu věří.

T: Z kazuistik, které jsem četla a z některých případů, které jsem měla možnost vyslechnout, jsem pochopila, že v průběhu vyšetřování celkem často dochází k odložení věci daného případu. Z jakých důvodů dochází k odložení oznámených případů?

R2: Když je nezletilý pachatel, tak se dost často odkládá. Pachatel pak dostane výchovné opatření nebo něco podobného. Tím, že se jedná o dítě tak se často uplatňuje subsidiarita trestní represe, tedy že se odkládá pro nízkou společenskou škodlivost. Také je tu spoustu možností odklonů…když se nejedná o něco závažného. U těch dětí je velká šance výchovné nápravy…

T: V souvislosti se sexuálními trestnými činy se vedou debaty o nízkých trestech za jejich páchání. Vnímáte tresty ukládané za páchání kybernetické kriminality na dětech jako přiměřené k povaze závažnosti tohoto druhu kriminality?

R1: Ty tresty vnímám obecně jako dostatečné, ale spíš by mělo být větší rozpětí…například v té základní skutkové podstatě bych nechal rok a v té kvalifikované třeba bych rozšířil rozpětí třeba až na 10 let. Samozřejmě, jak už jsem říkal, jsou i případy, kdy pachatel dostane podmínečný trest a není to v tom daném případě úměrné tomu, jakou újmu způsobil a ještě, když je v tom zapojené dítě…

R2: Třeba u té dětské pornografie…často jsou to lidé, kteří se chtějí podívat, protože to nikdy neviděli, dostanou pět, šest videí, po pár vteřinách to vypnou a většinou je to poučí, ničeho dalšího už se nedopustí… U těch větších sběratelů je to pak něco jiného.

T: Vnímáte v souvislosti s páchaním mravnostní kybernetické kriminality skutkové podstaty trestných činů tak, jak jsou v zákoně popsány, jako dostatečné nebo je například žádoucí trestní zákoník rozšířit o kybernetické trestné činy?

R1: Já si osobně myslím, že sexuálně motivované trestné činy by chtěly rozšířit. A jsem zastáncem toho, že legislativně by mohly být obecně kybernetické trestné činy lépe upravené zvláště pak ty mravnostní, páchané na dětech. Tam jde o to, že

by se nad tím musel někdo vážně zamyslet a musely by to dělat lidé, kteří tomu skutečně rozumějí.

R2: Souhlasím, pak by to mělo smysl.

R1: Měl by to být tým, který by měl být sestavený z nějakých odborných znalců v sexuální oblasti, dětské psychiatrie, také policista, IT specialista a taky třeba analytik.

R2: Já třeba teď, zaznamenávám pozitivní legislativní změnu, kdy dřív v České republice nebylo trestné animované dětské porno a teď už je to brané jako výroba dětské pornografie.

T: Musí být kriminalista, který se zabývá vyšetřováním kybernetické kriminality, IT odborníkem?

R2: Nemusí…to není nikdo.

R1: Měli by k tomu ale mít alespoň kladný vztah. Ale vystudované to tady nemá skutečně asi nikdo.

T: Zprostředkovává policie nějakým způsobem prevenci kyberkriminality?

R2: Ano, určitě, dělají se přednášky ve školách jak pro děti, tak pro rodiče.

R1: Já osobně jsem o kyberkriminalitě a o kyberšikaně přednášel pro děti i pro dospělé, zkrátka pro širokou veřejnost, a to v Praze i ve Středočeském kraji. Mimo přednášek, které se týkají kyberkriminality přednáším i například o drogové problematice.

T: Jakým způsobem by měla být aplikována prevence kybernetické kriminality tak, aby byla co nejúčinnější a zároveň atraktivní pro děti?

R1: Tak co se týče přednášek úplně nejlepší je, když přednáší ten, kdo se danými případy skutečně zabývá a může mluvit o skutečných případech, které řešil v rámci svojí práce. Autenticita je to, co hodně funguje nejenom na děti. Zároveň v souvislosti s tou prevencí vnímám bohužel to, že dnešní doba je velmi uspěchaná a hromada lidí je pod vlivem rodiny, která ten vliv velmi zanedbává. Rodina přesouvá hodně svých tradičních funkcí na učitele a osobní kontakt a komunikace mezi rodiči a dětmi chybí.

T: Jak by se měly chovat děti, pokud obdrží nějakou explicitní fotografii či jiný nevhodný obsah?

R2: Nejlépe zprávu ignorovat, uživatele zablokovat, nahlásit a pokud mají podezření na závažnější kriminalitu, tak ohlásit přímo na policii.

T: Zaznamenáváte v posledních letech nárůst kybernetické kriminality nebo se daří v souvislosti s prevencí a dalšími faktory kybernetické kriminalitě zamezovat?

R2: V rámci našeho oddělení se mi ta situace zdá pořád stejná…

R1: Já si myslím, že je určitá procentuální skupina lidí, která do tohoto nějakým způsobem vstupuje a ta skupina lidí se asi nemění. Dejme tomu, že existuje 1 % populace, které má takové sklony, a to procento zůstává stejný…ale pak je určitá skupina lidí, kteří vyhledávají dobrodružství, vzrušení, nové zážitky a ty do toho vstupují, aniž by měli jinou motivaci, než je touha poznat něco jiného, něco, co ještě neviděli nebo nezažili…a tihle lidé, když to toho vstoupí, tak získají zkušenost, která je buď záporná a upustí od toho, anebo je kladná a vstoupí do té skupiny 1 %, která je daná, a to se těžko dá zjistit nebo zmapovat…

R2: Z mého pohledu do toho většina lidí vstoupí na nějakou dobu – dva, tři měsíce a poté, co si to „vyzkouší“, už se toho znovu nedopustí…

T: Jsou aktuálně nějaké budoucí hrozby internetu?

R2: Teď zaznamenáváme aktuální trend, který je zatím v Americe, ale počítáme s tím, že brzo přijde i k nám, kdy si pachatelé píší s nějakou holkou, nechají si poslat fotky, třeba v plavkách, nemusí jít o nahé fotky a potom z toho udělají nějakou kompilaci, kdy její obličej dají do porna a následně jí vyhrožují, že buď jim pošle peníze, nebo materiál zveřejní. Ve výsledku o nic nejde, protože tam ve skutečnosti ty děti nejsou, ale už je to pro ně nějaký šok a je to nebezpečné jednání, spíš bych řekl, na hranici podvodu, kdy se využívá lidský stud.

R1: Tam jde o to, že je to nová forma vydírání a vydírání je vždycky příšerná věc, protože ty lidi to vždycky hodně rozhodí, stresuje je to, a ještě když je to mladý člověk…tak to na něm zanechá stopy…

T: Jak se proměnila kybernetická kriminalita páchaná na dětech v souvislosti s opatřeními týkajících se nemoci covid-19?

R2: Co se týká obecně trestné činnosti tak v covidu se míň oznamovalo…

R1: Celkově ubyla majetková trestná činnost, protože všichni seděli doma, přibyla násilná trestná činnost a co se týče té kybernetické kriminality, tak se domnívám, že k nárůstu došlo, protože lidi doma hodně koukali na internet, ale možná se to neprojevilo v tom konečném oznámení.

R2: Já bych řekl, že se to na těch dětech spíše projevuje teď, protože ta socializace jim nějakým způsobem chyběla a zároveň si nevybudovali takovou tu důležitou osobní odpovědnost.

T: Jaká by měla být osvěta v souvislosti s kybernetickou kriminalitou?

R1: Já si osobně myslím, že to osvěta souvisí se sexuální výchovou. Tím, že ta lidská sexualita je věc, o které lidi neradi mluví, neradi se svěřují, neradi nechávají něco vyplouvat na povrch, a každý v sobě to má nastavené trochu jinak. A tudíž vlastně objasňování sexuálně motivovaných trestných činů je složitý. Internet je samozřejmě úžasná věc, protože jsme schopni si tam zjistit hromadu zajímavých věcí, je to zdroj zábavy a tak dále, ale někdo by měl objasňovat lidem, že tam je spoustu negativních vlivů. Krásná osvěta kyberkriminality páchané na dětech byl film „V síti“. Tam je přesně ukázáno lidem, čeho se mohou vyvarovat. Obecně by měla být dobrá informovanost, mám ale na mysli obecně informace, třeba i ty, které se týkají lidské sexuality. Ta informovanost by měla být směřována k dětem, a to ze strany rodičů a učitelů ne ze strany toho, kdo si s dětmi píše přes internet, protože ten má přímo zájem na tom je poškodit.

T: Jak vy osobně vnímáte kybernetický prostor a to, co se v něm děje?

R1: Jako obrovský problém současné společnosti. My, jako obecně, jsme se přesunuli do toho kyberprostoru úplně všichni. Lidi si přestali povídat, přestali se scházet. Pořád se koná spoustu akcí jako jsou koncerty nebo besedy a na tyhle akce já, když přijdu, tak zjistím, že tam sedí lidi ve věkové kategorii padesát plus a těch mladých přijde strašně málo, protože ty se všichni pohybují v tom kyber prostoru a osobní kontakt jim nahrazuje internet. A když se nad tím zamyslím, tak obecně ubylo akcí, kde se lidi osobně potkávali. A to není v pořádku…vždycky je lepší vidět koncert na živo…a to stejné je i s mezilidskými vztahy. V dnešní době se spousta lidí upíná na virtuální vztahy a nežijou ty skutečné…

Závěry z rozhovoru

Rozhovor s panem por. Bc. Radovanem Hladem a panem por. Mgr. Janem Křemenem proběhl dne 22. 3. 2024 na Odbor obecné kriminality na Karlově náměstí 325/7 na Praze II.

V rámci rozhovoru bylo zjištěno, že kybernetická kriminalita se týká dětí již od velmi útlého věku. Již pětileté děti se mohou stát obětí kybernetické kriminality, pokud je jim umožněn přístup na internet. Kybernetická kriminalita je na dětech páchána formou kontaktování dítěte přes sociální sítě nebo chatovací místnosti s cílem sexuálně či finančně se na dítěti uspokojit. Kyberútočníci často vystupují pod falešnou identitou a využívají důvěřivosti dítěte. Aktuálně nejvíce využívané internetové sítě pro komunikaci, na kterých vyšetřovatelé zaznamenávají páchání kyberkriminality, jsou Instagram, Snapchat, Tik Tok a Discord. Stává se, že se internetová komunikace přesune z kybernetického prostředí do reality a dojde i na osobní schůzku, což může být velmi závažné s ohledem na sexuálně vedenou motivaci pachatele. Ověřila jsem si, že pachatelé nejsou motivováni jen sexuálně, ale i finančně, a to v případech dětské pornografie a vydírání, které následuje například po zaslání intimních fotografií.

Ohledně osoby pachatele jsem se dozvěděla, že ne každému je diagnostikována pedofilie. U většiny pachatelů je sexuální náklonnost k nezletilým způsobena tím, že je pro ně běžná pornografie stereotypní, nezajímavá, jsou jí přehlceni, a tak hledají něco nového, pro ně atraktivního. Osobně jsem měla za to, že pachatelé kybernetické kriminality si ne vždy uvědomují, že se v kybernetickém prostředí dopouštějí trestných činů. Por. Bc. Radovan Hlad je však toho názoru, že pachatelé moc dobře vědí, jakých trestných činů se dopouštějí, ale spíše si neuvědomují, jaké může mít jejich jednání škodlivé důsledky. Trestné činy, kterých se pachatelé nejčastěji dopouštějí jsou svádění k pohlavnímu styku, zneužití dítěte k výrobě pornografie, šíření pornografie, ohrožování výchovy dítěte, vydírání, navazování nedovolených kontaktů s dítětem a výroba a jiné nakládání s dětskou pornografií. Pokud je pachatel sexuálně motivován, nezůstane jen u dopisování a dojde k osobní schůzce může se jednat i o naplnění skutkové podstaty znásilnění, sexuálního nátlaku nebo pohlavního zneužití. Pachatelem takové kriminality může být samozřejmě jak dospělý, tak dítě.

Co se týká vyšetřování kybernetické kriminality, novou informací pro mne byla činnost organizace NCMEC (National Center for Missing & Exploited

Children), což je nezisková organizace, která působí v USA jako sběrné a komplexní nahlašovací centrum pro problémy týkající se zneužívání dětí. Organizace NCMEC tato hlášení předává bezpečnostním složkám po celém světě.[56] Její činnost spočívá v tom, že sbírá nevhodný obsah jako například dětskou pornografii nebo jiné nezákonné materiály od společností jako například Google nebo Meta a následně je rozesílá do zemí, odkud byl materiál zaslán, a které se budou zabývat vyšetřováním a stíhat osoby pro trestné činy.

Aktuální velmi rozšířenou kybernetickou kriminalitou je již zmiňovaný kybergrooming a online dětská pornografie. Kriminalisté již ale zaznamenávají i nové trendy, které jsou prozatím zaznamenány jen v zahraničí, ale brzy proniknou i do České republiky.

V souvislosti s vyšetřováním kybernetické kriminality jsem se dozvěděla, že problémem policejního orgánu je nedostatek personálu, který by se zabýval vyšetřováním, které z velké části probíhá prohlížením tisíců fotografií, videí či pročítáním komunikace mezi obětí a pachatelem, což je velmi časově náročná záležitost. Dále se dostalo i na problematiku znaleckých posudků, která spočívá v nedostatku znalců, finanční náročnosti a dlouhých čekacích lhůtách. Okrajově byl zmíněn i výslech, kdy bylo připomenuto, že celé trestní řízení probíhá tak, aby bylo co nejvíce šetřeno s osobou mladistvého.

Překvapením pro mě byla úspěšnost v dopadení pachatele, kterou oba kriminalisté hodnotili jako téměř 100 % s přihlédnutím k tomu, že existuje obrovské množství latentní kriminality, která pokud se neoznámí, neobjasní se.

Na mou otázku ohledně toho, zda je současná legislativa dostatečná, reagovali tak, že by trestní zákoník rozšířili o kybernetické trestné činy. Tresty ukládané za kybernetickou trestnou činnost páchanou na nezletilých vnímají obecně jako přiměřené, ale zaznamenávají i případy, kdy pachatel odejde s podmínkou a oni sami tento výsledek soudního procesu nevnímají s přihlédnutím k povaze závažného následku jako dostatečný.

V současné situaci dle kriminalistů kybernetická kriminalita stagnuje. Nezaznamenávají zhoršení ani zlepšení, což je dle mého názoru dobrá zpráva, jelikož kybernetickou kriminalitu považuji za nezastavitelnou a obsah, který se šíří přes internetové prostředky se může stát ze vteřiny na vteřinu virálním. Pokud se

[56] Boj společnosti Google proti materiálům zobrazujícím sexuální zneužívání dětí na internetu; Google Transparency report. Dostupné z: https://transparencyreport.google.com/child-sexual-abuse-material/reporting?hl=cs [cit. 23. 3. 2024]

daří situaci udržovat na stejném bodě, považuji to za dobrý výsledek. Co se týče vývoje v pandemii covid-19 celkově se proměnila situace s pácháním kriminality a té u té kybernetické zaznamenávají jisté zvýšení s ohledem na to, že nejen děti seděli doma a trávili čas na internetu.

Poslední kategorie otázek se zaměřovala na prevenci a osvětu kybernetické kriminality, kdy mi oba kriminalisté potvrdili, že policie je v provádění prevence týkající se kybernetické bezpečnosti aktivní. Sám por. Bc Radovan Hlad přednáší pro děti i širokou veřejnost o kybernetické bezpečnosti a jiné závažné trestné činnosti. Osvětu této problematiky vnímají především v komunikaci mezi rodiči a dětmi, povědomí široké veřejnosti a v sexuální výchově dětí.

Celkovou problematiku kybernetické kriminality, které jsou děti účastníci vnímají jako velký problém současné společnosti, který se bude jen prohlubovat a můžeme doufat, že přijetím příslušných opatření a zvýšením informovanosti a ochrany dětí můžeme omezit dopad této problematiky.

Příčiny kybernetické kriminality páchané na dětech

Kybernetická kriminalita, jak už byla výše představena, je vážným problémem, do kterého jsou již bohužel mimo dospělých, zapojeni i děti. Příčin kybernetické kriminality, která je na dětech páchána můžeme najít hned několik a je víc než žádoucí si důvody, proč se děti stávají oběťmi počítačové kriminality uvědomovat, neboť slouží jako vodítko při aplikaci prevence. Mezi příčiny řadíme motivy, které pachatele vedou k dopouštění se kriminality na dítěti pomocí internetových komunikačních prostředků, dále příčiny, které dítě mohou dostat do role oběti kybernetické kriminality a v neposlední řadě i příčiny, které vnímáme jako širší společenské či technologické faktory. V návaznosti na to, co již bylo v této práci uvedeno, shrnu několik příčin kybernetické kriminality, do které se děti dostávají.

Nedostatek dohledu rodičů

Kontrola aktivit dětí na internetu ze strany rodičů je, dle mého názoru, naprosto stěžejní. Děti, které od svých rodičů neobdrželi poučení o tom, jak se chovat na internetu a zejména pak na sociálních sítích, či rodiče nijak nekontrolují jejich aktivity, mohou být náchylnější k nebezpečím, které pohyb v kyberprostoru přináší. Mnohdy však absenci informovanosti vnímáme již u rodičů. Rodiče přirozeně na internetu konají jiné aktivity než děti, pohybují se na jiných webových

stránkách, s ohledem na generační rozdíl jsou aktivní na jiných sociálních sítích a celkově internet využívají docela jinak než jejich děti. V současné době, kdy se fenomén dětí na internetu dostává do povědomí široké veřejnosti, podnikají školy semináře pro rodiče, aby je s problematikou i s tím, jak děti internet a sociální sítě užívají obeznámili.

Z mého pohledu by poučení ze strany rodiče o tom, jak se chovat na internetu a na co si zejména dát pozor, mělo být minimální a základní preventivní opatření. Zejména v dnešní době, kdy mobilní telefony umožňují dálkový přístup může mít dohled rodičů zcela jiné rozměry. Díky moderním digitálním technologiím může být rodič informován o tom, jak dlouhou dobu dítě na internetových prostředcích tráví, mít přehled, s kým dítě komunikuje či například, kde se dítě nachází. Můžeme se setkat s názorem, že i dítě, stejně jako dospělý má právo na soukromí a tato kontrola ze strany rodiče je nadměrným zásahem do jeho soukromí. Újma, kterou by dítě v případě, že by se stalo obětí internetového trestného činu utrpělo, je však daleko závažnější než zásah do soukromí, který dítě pro své bezpečí musí strpět. Stejná kontrola může mít i formu zdravé komunikace mezi dítětem a rodičem. Rodič by měl mít přehled nejen o tom, s kým se dítě kamarádí, s kým komunikuje, na jakých sociálních sítích má registrovaný účet, jaké hry hraje a k jakým dalším aktivitám využívá internet, ale i o tom, jak se cítí, co ho aktuálně zajímá a zda například nemá nějaké problémy ve škole. Komunikace mezi dětmi a rodiči nejen, že může zamezit tomu, aby se dítě stalo obětí kybernetické kriminality, ale i pomoci dítěti, které se již obětí internetového trestného činu stalo. Za zmínku také stojí fakt, že mobilní telefon či jinou elektroniku s podobným využitím vlastní děti, které tyto prostředky k ničemu nepotřebují. K mobilním telefonům, tabletům a notebookům se dostávají již například osmi leté děti, pro které je hlavním a často jediným účelem takového zařízení hry a zábava. Rodiče by se v takovém případě kromě poučení a informování dítěte o bezpečnosti na internetu mohli primárně zamyslet nad tím, jak dítě zabavit jinak než mobilním telefonem či tabletem.

Nedostatečná edukace a informovanost dětí

Předchozí téma nedostatečného poučení o bezpečném chování na internetu od rodičů, je logicky provázáno s nedostatečnou informovaností dětí. Mobilní telefony, stejně tak jako jiná elektronická zařízení, se staly součástí našich životů a děti se tak již od batolecího věku setkávají s těmito technickými nástroji. Není

divu, že ve věku pozdějším chtějí být součástí moderní komunikace a digitálního prostředí po vzoru svých rodičů. A tak nejen rodiče, ale i škola by měla v rámci výuky do svých osnov zařadit výuku, která by představovala internet a poučila děti o jeho bezpečném užívání.

K tomu, aby škola i rodiče mohly dítě poučit a informovat, musí mít dostatečné znalosti o aktuálních kybernetických hrozbách. Nedostatek zdrojů a nedostatek času věnovat se kybernetické výuce doma nebo v rámci výuky ve škole je právě to, co může bránit dětem v získání potřebných znalostí o bezpečném užívání sociálních sítí a internetu celkově. Děti mají často snadný a neomezený přístup k online prostředí a nedostatek dozoru a poučení může vést k neuváženému chování a vystavení se různým rizikům. Je proto důležité, aby rodiče, učitelé a celá společnost společně pracovali na zlepšení vzdělávání dětí v oblasti kybernetické bezpečnosti a poskytovali jim nástroje a znalosti k bezpečnému a odpovědnému chování online. Zajištění digitální gramotnosti a vzdělávání o kybernetické bezpečnosti by mělo být zaměřeno na všechny věkové kategorie, abychom co nejvíce přispěli ke snížení rizik spojených s užíváním internetu.

Zranitelnost a důvěřivost dítěte

Zranitelnost a důvěřivost dítěte na internetu jsou pojmy, jež vyjadřují jeho náchylnost k rizikům a nebezpečím, které online prostředí přináší. Tato problematika však v souvislosti s užíváním internetu není záležitostí, která by se týkala výhradně dětí. Někteří dospělí jsou stejně tak jako děti, náchylní a důvěřiví a stávají se obětí kybernetických podvodů. Přestože se formy kybernetických podvodů neustále vyvíjí a zlepšují měli by mít dospělí lidé povědomí o aktuálních hrozbách a dostatek zkušeností na to se neuváženému chování vyvarovat.

Fakt, že dítě nemá dostatek rozumové vyspělosti a zkušeností rozpoznat hrozby či protiprávní chování na internetu navazuje na předchozí téma nedostatečné vzdělanosti v oblasti kybernetické bezpečnosti. Pokud se však zaměříme například na problematiku fenoménu zvaného kybergrooming, tedy sexuálního zneužívání dětí na internetu, můžeme zranitelnost a důvěřivost dítěte spatřovat například v tom, že dítě je zvyklé následovat a poslouchat autority, a tak není divu, že podlehne nátlaku starší osoby. Co se týče kybergroomingu svou roli zde jistě může hrát i naivita dítěte a čistý úmysl najít si například kamarády.

Anonymita online prostředí

Další příčinou páchání kybernetické kriminality ze strany pachatelů je jistě anonymita online prostředí, kdy uživatelé mohou interagovat na internetu bez odhalení své pravé identity a reálných osobních informací. Používání pseudonymů, přezdívek, falešných jmen a celkově falešných účtů v pachateli vyvolává pocit, že nejednají sami za sebe, a tak si dovolí psát, sdílet, komentovat a obecně se na internetu chovat tak, jak by se v reálném životě nikdy nechovali. Například si v souvislosti s páchaním kybergroomingu na sociálních sítích dovolí oslovit dítě, což by ve skutečnosti nikdy neudělali. Dalším příkladem může být kyberšikana, kdy si agresor (například spolužák dotyčného) ve škole oběti ani nevšimne, nicméně v online prostředí si dovolí psát nenávistné komentáře a vyvíjet tak tlak na jeho osobu. Obecně jsou lidé schovaní za klávesnici počítače pod přezdívkou či pseudonymem na sítích daleko aktivnější a odvážnější než ve skutečnosti.

Další nástraha anonymity spočívá v tom, že v online prostředí můžeme komunikovat s lidmi, jejichž totožnost není jasná nebo není ověřitelná. Účet se například může jevit jako profil dvanáctiletého dítěte, realita však může být taková, že za klávesnicí sedí čtyřicetiletý muž. Dítě tak může mít pocit, že si dopisuje se svým vrstevníkem, ve skutečnosti však osoba skrytá za falešným profilem může zneužít jeho důvěru a pokusit se například o manipulaci jeho osoby.

Pro ochranu před riziky spojenými s anonymitou online je důležité být obezřetný a opatrný při interakcemi s neznámými lidmi online a například si ověřovat totožnost a účinnou prevencí je také nekomunikovat s neznámými lidmi.

Finanční motivace pachatelů

Finanční motivace pachatelů je jednou z hlavních příčin páchání kybernetických podvodů obecně. Finančně motivováno je bohužel i páchání kybernetické kriminality v souvislosti s dětmi.

Pachatelé mohou cíleně vyhledávat děti jako oběti vydírání za účelem peněžního zisku. Například se pokoušejí získat citlivé informace, intimní materiály jako například fotografie či videa dětí a následně je využít k vydírání peněz od nich. V souvislosti s online dětskou pornografií již bylo zmíněno, že pachatelé vytvářejí a distribuují dětskou pornografii za účelem finančního zisku. Tato nelegální činnost může být pro pachatele velmi lukrativní, což je motivuje k pokračování v této trestné činnosti. Finanční obnos může také být nejprve použit jako motivace pro

dítě k vytvoření a zaslání intimních materiálů a následně vymožen od oběti zpět v rámci vyhrožování ohledně zveřejnění zaslaného obsahu.

Nedostatečná legislativa

V České republice je kybernetická kriminalita zaměřená na děti vážným problémem, stejně jako v mnoha dalších zemích. Zákonný rámec v České republice se snaží reagovat na tuto problematiku, ale je stále potřeba aktualizovat a posílit ochranu dětí v online prostředí. Trestní zákoník obsahuje ustanovení týkající se různých forem sexuální trestné činnosti a trestných činů, které se týkají rodiny a dětí, ale z mého pohledu by stálo za to, rozšířit trestní zákoník o trestné činy, které se týkají kybernetického prostoru, pro usnadnění aplikace zákona na skutkové podstaty trestných činů.

Úprava by mohla zahrnovat přesnější definice trestných činů v online prostředí, posílení trestů pro pachatele, posílení ochrany soukromí a osobních údajů dětí online a poskytování specifických prostředků pro ochranu a podporu obětí kybernetického zneužívání.

Je důležité, aby česká legislativa neustále reagovala na nové hrozby v digitálním prostředí, neboť kybernetické zločiny se velmi rychle modifikují. To může vyžadovat spolupráci mezi vládou, právníky, IT specialisty a například dětskými psychology.

Podceňování kybernetické kriminality

Podceňování kybernetické kriminality páchané na dětech ze strany policejních orgánů také může být faktorem, který podněcuje pachatele k trestné činnosti.

V případě, že policejní orgány nepřikládají dostatečnou vážnost kybernetické kriminalitě páchané na dětech, může pachatel zůstat nepotrestaný a pokračovat tak v další trestné činnosti. Jejich nečinnost může také vést k nedostatečnému vyšetřování a identifikaci pachatelů a tím pak například k odložení případu. Nečinnost policejního orgánu může vést pachatele k pokračování jejich nelegálních aktivit v oblasti kybernetického prostoru. Nízká prioritizace ze strany policejního orgánu může také vést k nedostatečné spolupráci mezi subjekty, jako jsou školy či rodiče zejména v oblasti prevence kybernetické bezpečnosti.

Další faktorem podceňování kybernetické kriminality jako takové může být nedostatek prostředků k odhalení trestné činnosti.

Podceňování kybernetické kriminality páchané na dětech můžeme vnímat i ze strany veřejnosti. Společnost by měla reagovat na fenomén obtěžování dětí na internetu a šířit celkové povědomí o problému kybernetických zločinů celkově a chránit tak děti ve veřejném společenském zájmu.

Odhalování a vyšetřování kybernetické kriminality

Kyberkriminalita může být namířena proti počítačům, jejich hardwaru, softwaru, datům, sítím, nebo v ní vystupuje počítač jen jako nástroj páchání trestného činu, případně je počítačová síť a k ní připojená zařízení prostředím, ve kterém se trestná činnost odehrává. Obtížnost sledování projevů kyberkriminality mimo jiné spočívá i v tom, že se uvedené jednání odehrává v prostředí, které je objektivně pouze obtížně vnímatelné. Dění v kyberprostoru je možné sledovat pouze za pomoci jiného počítače.[57]

Počítače, moderní technologie a internet nám do života kromě pozitivních aspektů vnesly i nové možnosti v oblasti páchání kriminality. Vyšetřování kybernetické kriminality je, jako každé jiné vyšetřování kriminality, proces, který zahrnuje identifikaci, sběr důkazů a analýzu informací souvisejících s trestnými činy. Tento proces má za cíl prokázat, zda se skutek stal, zda je trestným činem, a zda je konkrétní podezřelá osoba pachatelem dle § 22 odst. 1 TrZ tedy, že svým jednáním naplnila znaky skutkové podstaty tr. činu nebo jeho pokusu či přípravy, je-li trestná. [58]

Aby mohl být pachatel odsouzen, musí mu být prokázána vina v soudním řízení. V zásadě jde tedy o vypátrání podezřelé osoby, zákonné obvinění, podání obžaloby a její projednání soudem. Potřebujeme tedy mít k dispozici orgány, které budou nadány příslušnou pravomocí, přičemž budou příslušné k provádění trestního řízení (orgány činné v trestním řízení jsou Policie ČR, státní zastupitelství, soudy). [59]

---

[57] JIROVSKÝ, V. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007, s. 19

[58] Zákon č. 40/2009 Sb., trestní zákoník. In [Systém ASPI]. Wolters Kluwer [cit. 2023-9-24]. Dostupné z: www.aspi.cz. ISSN 2336-517X. [https://www.aspi.cz/products/lawText/1/68040/1/2/zakon-c-40-2009-sb-trestni-zakonik]

[59] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 3. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. ISBN isbn978-80-7380-849-5.s.830.

Klíčovou roli při vyšetřování kybernetické kriminality má policejní orgán, jehož úkolem je zajistit, aby vyšetřování bylo prováděno řádně, a to v souladu se zákonem. Vyšetřování internetové trestné činnosti vyžaduje zcela jinou metodiku, která se s příchodem nových technologií a neustále se rozšiřujícími způsoby páchání kyberkriminality vyvíjí.

Počítačová kriminalita je odhalována jednak vlastní pátrací činností policie, jednak na základě oznámení poškozených či jiných osob, někdy i na základě preventivní činnosti například v bankovní sféře. Podle proběhnuvšího procesu můžeme rozdělit průběh trestního řízení takto:

a) skutky, kdy vůbec není zjištěno, že se staly
b) skutky, kdy je zjištěno, že se staly, ale nejsou vyhodnoceny jako trestné
c) skutky, kdy je zjištěno, že se staly, jsou vyhodnoceny jako činy trestné, ale potenciální oznamovatel má důvody pro jejich utajení
d) skutky, které byly odhaleny a oznámeny, ale policie nenalezla pachatele (zde můžeme rozlišit dvě varianty - 1. neexistuje žádný podezřelý, 2. existuje, ale nepodařilo se šetření ukončit sdělením obvinění)
e) trestní stíhání obviněného pro určitý skutek bylo zastaveno státním zástupcem, takže obžaloba nebyla podána
f) obžalovaný byl obžaloby zproštěn
g) obžalovaný byl uznán vinným a rozsudek nabyl právní moci[60]

Zvláštní způsoby trestního řízení, jako jsou například upuštění od potrestání, podmíněné zastavení trestního stíhání, nebo v řízeních ve věcech mládeže odstoupení od trestního stíhání, jsou vzhledem k povaze trestné činnosti také možným alternativním řešením.

Přijetí oznámení a prověřování

Trestní řízení začíná sepsáním záznamu o zahájení úkonů trestního řízení nebo provedením neodkladných a neopakovatelných úkonů, které mu bezprostředně předcházejí. Oznamovatelem při oznámení počítačové kriminality spáchané na dítěti bývají rodiče oběti, pedagogové nebo například spolužáci či kamarádi dítěte, v některých případech i sama oběť.

[60] Tamtéž, s.832.

Přijetí oznámení od oznamovatele, jeho precizní zpracování a zajištění prvotních informací a důkazů je při řešení kyberkriminality životně důležité. V této fázi trestního řízení je třeba co nejpřesněji zajistit informace týkající se vlastního kybernetického útoku. Pokud je to možné, je třeba od oznamovatele (např. poškozeného) zajistit data v co nejméně změněné podobě [např. originály e - mailových zpráv, nosič informací (paměťové médium) či celý počítačový systém atp.], pokud to není možné, pak získat například kopie těchto dat, printscreeny aj.[61]

V případě kybergroomingu takovými důkazy mohou být například obrazové snímky komunikace oběti a pachatele včetně sdíleného mediálního obsahu jako jsou fotografie, videa apod. V případě dětské pornografie se jedná o nasbíraná videa či fotografie s pornografickým obsahem, které zobrazuje nezletilé.

Jelikož se jedná o mladistvého či nezletilého, je důležité zmínit, že v rámci trestního řízení je mu zajištěna zvýšená ochrana a je mimořádně šetřeno s jeho právy a vše samozřejmě probíhá dle právní úpravy obsažené v zákoně č. 218/2003 Sb. (ZSVM).

Výslech nezletilého probíhá za přítomnosti jeho zákonného zástupce a orgánu sociálně-právní ochrany dětí a mělo by být postupováno tak, aby již nebyl opakován, jelikož mimo jiné může být pro dítě účast na výslechu obzvlášť traumatizující. Vše je prováděno s ohledem na jeho věk, duševní vývoj a schopnost porozumění. V některých případech je u výslechu přítomen dětský psycholog či psychiatr.

Důkazní prostředky

Důkazy a jejich nalezení, zajištění, vytěžení a provedení v rámci trestního řízení hrají při vyšetřování trestné činnosti v kyberprostoru významnou roli, a to vzhledem ke svému specifickému charakteru. Na rozdíl od důkazů klasických – hmotných jsou důkazy spočívající v záznamu dat a procesů probíhajících v počítačových systémech a sítích obtížněji zjistitelné a hůře zaznamenatelné, snadno ovlivnitelné a obtížně interpretovatelné, pokud není dodržena správná metodika vyšetřování tohoto druhu trestné činnosti.[62]

[61] KOLOUCH, Jan. *Cybercrime*. Praha: CZ.NIC, z. s. p. o., 2016. ISBN 978-80-88168-18-8. s.411.
[62] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 3. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. ISBN isbn978-80-7380-849-5.s.824-825.

Digitální stopa

Používání digitálních stop, jako důkazních prostředků, je pro identifikaci pachatelů kybernetické kriminality klíčové.

Smejkal ve své publikaci shrnuje poznatky Porady a Raka týkajících se vymezení pojmu „digitální stopa“. Každé technologické zařízení, které získává, zpracovává, předává nebo uchovává data, zanechává záznamy (odrazy) o své činnosti. Tyto záznamy z kriminalistického hlediska jsou stopami. V oblasti IS/IT jsou tedy především digitální stopy, které lze definovat podle SWGDE (Scientific Working Group on Digital Evidence) jako jakékoliv informace s vypovídající hodnotou, uloženém nebo přenášené v digitální podobě.[63]

Z hlediska trestního či správního řízení je ale pro nás možná užitečnější užší definice International Organization of Computer Evidence (IOCE), která již není fungující organizací a která definovala původně digitální stopu jako jakoukoliv informaci, uloženou nebo přenášenou v binární formě, která může být předložena soudu jako věcný důkaz. V této definici je kladen důraz na předkládání důkazů soudu, a právě přeložitelnost důkazů soudu je hlavním úspěšnosti kriminalistické počítačové analýzy (na rozdíl od tzv. Znalecké analýzy prováděné za účelem soukromoprávním).[64] Lze také říci, že digitální stopa je fyzikální interpretací (záznamem) nehmotné informace, zakódované do digitálního formátu. [65]

Fyzické a datové objekty se stávají důkazy teprve tehdy, jsou-li akceptovatelné orgány činnými v trestním řízení. Klíčovou je právě otázka prokazatelnosti, že se stopa nacházela na určitém místě a že v procesu od jejího zjištění do ukončení znaleckého zkoumání nebyla žádným způsobem modifikována. Proto se pracuje s duplikátem digitální stopy, což je přesná digitální reprodukce všech datových objektů obsažených na originálním fyzickém objektu na fyzicky stejný typ datového média.[66]

Digitální stopa je technicky nějaký záznam nacházející se na nosiči informací ať už jím chápeme nosič trvalý [pevný disk, USB (flash), paměť,

[63] RAK, R; PORADA, V. Charakteristiky a specifika digitálních stop. *Bezpečnostní teorie a praxe*, 2005, č. 1, s 71-84, resp. PORADA, V.; RAK, R. Digitální stopy v kriminalistice a forenzních vědách. Soudní inženýrství, XVII. 2006, č. 1, s. 3-21.
[64] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 3. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. ISBN isbn978-80-7380-849-5.s.825.
[65] PORADA, V.; ŠEDIVÝ, P. Praktická využitelnost kriminalistických a forenzních aplikací v oblasti počítačové/kybernetické kriminality. *Karlovarská právní revue*, 2012, č. 3, s. 94-114.
[66] SMEJKAL, V. *Současné možnosti boje proti počítačové kriminalitě*. Data Security Management, XV., 2011, č. 4, s. 18-23.

CD/DVD/Blue-ray apod.] nebo dočasný (paměť počítače, datová zpráva při jejím přenosu apod.).[67]

Digitální stopy jsou tedy digitální informace, které uživatel nebo počítačový systém zanechává během své aktivity na internetu. Tyto stopy mohou zahrnovat IP adresy, protokoly, historii prohlížení, e-maily, chatovací zprávy, soubory a další digitální záznamy. Při vyšetřování kybernetické kriminality páchané na dětech tak, jak je v této práci popsána, jsou nejčastějšími digitálními stopami právě záznamy z internetové komunikace (e-maily, chatovací aplikace, online hry nebo sociální sítě), fotografie, videa či například historie prohlížení. Aby se policie v rámci vyšetřování k digitálním stopám dostala, musí samozřejmě účastník komunikace (pachatel či oběť) poskytnout kriminalistům komunikační zařízení (například mobilní telefon či počítač) pro zajištění těchto stop či poskytnout alespoň printscreen komunikace, výpis hovorů či inkriminované mediální soubory.

Digitální stopa, je tedy termín označující stopu, kterou každý člověk zanechává při aktivitách online. Jedná se o informace, které osoba uvolňuje při používání internetu, sociálních sítí, e-mailu, vyhledávání na internetu a dalších online činností. Digitální stopa může zahrnovat historii prohlížení, interakce na sociálních médiích, komunikaci e-mailem a mnoho dalšího. Tato stopa může být sledována, sbírána a analyzována různými subjekty, jako jsou společnosti shromažďující data, reklamní firmy, policie nebo kybernetičtí útočníci. Koncept digitální stopy je důležitý v kontextu ochrany soukromí a kybernetické bezpečnosti.

IP adresa

Dalším významným zdrojem informací je propojení počítačového systému do sítě a přidělení tzv. IP adresy. IP adresa (identity protokol) je adresa v IT prostředí číslo, které jednoznačně identifikuje síťové rozhraní v počítačové síti, která používá IP protokol. [68]

Pro identifikaci počítačového systému (a případně útočníka) je třeba znát kromě IP adresy i datum a přesný čas připojení počítačového systému do počítačové sítě. Díky své jedinečnosti a unikátnosti je právě IP adresa jedním z klíčových identifikátorů sloužících k identifikaci pachatele kyberkriminality. K vlastnímu

[67] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 3. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. ISBN isbn978-80-7380-849-5.s.834.
[68] HEJDUK, Marek. *Bezpečnostní teorie a praxe* 1/2021 vědecký článek. Policejní akademie České republiky v Praze student doktorského studia, s. 73.

zjištění koncového počítačového systému je však třeba znát principy připojování těchto systémů do počítačové sítě a principy využívané k přidělování IP adresy.[69]

IP adresa je tedy identifikátor, který je každému zařízení připojenému k počítačové síti přiřazený. IP adresa slouží k identifikaci a lokalizaci zařízení, které je připojené k síti, umožňuje vzdálenou komunikaci a výměnu dat. Každá IP adresa je unikátní, což znamená, že žádné dvě zařízení v téže síti nemají stejnou IP adresu. IP adresa je v kontextu vyšetřování používána pro identifikaci vlastníka a sledování jeho online aktivit.

Prevence kybernetické kriminality páchané na dětech

Jak již bylo řečeno, pokud budeme děti učit základním pravidlům bezpečného používání internetu, je velká pravděpodobnost, že se nestanou on-line obětí. [70] Prevence by měla být v první řádě ve formě poučení od rodičů, pedagogů či například i od Policie ČR o aktuálních hrozbách a bezpečném chování na internetu.

Následně by měla probíhat neustálá kontrola rodičů ohledně online aktivit dětí, s tím souvisí i komunikace nejen rodičů, ale i pedagogů s dětmi. Děti by měly vědět, že mají možnost poradit se s dospělými, pokud se cítí nejistě nebo nepříjemně v online interakcích a úkolem rodičů a pedagogů je vytvořit pro děti „bezpečné prostředí“ pro to, se svěřit.

Zásadní je pak i samotný přístup dítěte, kdy by jako uživatel internetu s nabytými informacemi od rodičů, pedagogů či z přednášek o kybernetické bezpečnosti, mělo dbát zvýšené opatrnosti a obezřetnosti při svých aktivitách v online prostředí. Děti by měly být naučeny chránit své osobní údaje a zabezpečit své účty na sociálních sítích a dalších online platformách.

Sdílení fotografií, videí a osobních informací

Je důležité děti učit a informovat o hrozbách kybernetického prostředí, zejména pak, že by neměli sdělovat své citlivé, osobní informace, fotografie, videa, adresu svého bydliště, telefonní číslo, adresu školy, jména, adresy, telefonní čísla rodičů, hesla a další osobní informace někomu, s kým se seznámili pouze prostřednictvím internetu a vědí o něm jen to, co jim sám sdělil. Měly by být opatrní

[69] KOLOUCH, Jan. *Cybercrime*. Praha: CZ.NIC, z. s. p. o., 2016. ISBN 978-80-88168-18-8. s.411.
[70] HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha: Triton, 2012. ISBN 978-80-7387-545-9.s.108.

ohledně toho, jaké informace a jaký obsah poskytnou v rámci internetové komunikace a celkově na sociálních sítích, neboť hrozí, že může být vše později zneužito.

Je důležité být opatrný zejména při sdílení fotografií dětí na internetu. Fotografie a videa na internetu mohou být snadno staženy a může s nimi být kýmkoli nakládáno. V případě zneužívání dětí na internetu mohou být použity jako manipulační prostředek nebo jako obsah pro nelegální stránky s dětskou pornografií. Sdílení fotografií na internetu také může zvýšit riziko kyberšikany, kdy se obsah může stát terčem nenávistných komentářů, zesměšňování a manipulace. Fotografie na internetu navíc mohou zanechat dlouhotrvající digitální stopu, která může ovlivnit děti v budoucnu. Může mít vliv nejen na jejich soukromí, ale například i na jejich budoucí profesní život.

Je proto důležité, aby rodiče věnovali pozornost tomu, co děti na internetu sdílí a spolu s dětmi komunikovali o tom, které fotografie zveřejní na internetu. Vždy by měli mít dohled nad dodržováním zásad ochrany soukromí a bezpečnosti, s využitím možnosti nastavení soukromí na sociálních sítích a jiných online platforem, aby minimalizovali riziko nejen nevhodného použití fotografií jejich dětí, ale i riziko kontaktu dítě s cizí osobou.

V souvislosti se sdílením fotografií dětí by se i samotní rodiče měli zamyslet nad tím, jaké fotografie svých dětí na sociálních sítích sdílí, neboť i tento obsah může být v budoucnu proti dětem použit, například jako prostředek kyberšikany.

V dnešní době mnoho slavných osobností či influencerů sdílí na sociálních sítích své osobní fotografie a videa, včetně těch zobrazujících jejich malé děti. Vše jimi sdílené považují za součást jejich obsahu, kterým si mnohdy na sociálních sítích i vydělávají. Veškerý mediální obsah, který je například na sociální síti Instagram sdílen, může být kýmkoli, pokud se jedná o veřejný profil, stažen a zveřejněn později či použit pro obrazové koláže apod. Například může být influencer osloven pro vytvoření reklamy na plenky, kterou následně vytvoří za účasti svého dítěte. V rámci své spolupráce s reklamní značkou si však neuvědomí, že reklamní fotografie a videa, které sám vytvoří a zveřejní, mohou zapříčinit budoucí kyberšikanu či jiné obtěžování dítěte. Zveřejňování obsahu, který zahrnuje děti, může mít dlouhodobé důsledky na jejich soukromí a bezpečnost.

Komunikace s neznámými lidmi a osobní schůzky

Součástí prevence by mělo být i poučení dětí o rizikách spojených s komunikací s lidmi, které osobně neznají. Jak již bylo řečeno, internet je místo, které slouží jako veřejný prostředek pro virtuální stýkání se s různými lidmi z celého světa, což může být přínosné a obohacující stejně tak, jako rizikové.

Děti na internetu mohou být kontaktovány různými lidmi, a to jak přátelskými, tak i nebezpečnými. Je důležité, aby děti byly obezřetné při komunikaci s lidmi na internetu a měly povědomí o bezpečnostních opatřeních, což by měli poskytnout rodiče a pedagogové v rámci výchovy a poučení o bezpečné komunikaci a užívání internetu a poučit je, jak rozpoznat a reagovat na nebezpečné situace online.

Děti by se měly vyvarovat přehnané důvěřivosti k lidem, které osobně neznají, jelikož lidé na internetu mohou lhát, slibovat a skrývat se za jinou identitu. Nikdy by neměli takovým lidem sdělovat osobní informace, odesílat fotografie a měly by jejich iniciativu a zájem spíše ignorovat. Osobní schůzky s lidmi, které neznají osobně by neměly probíhat za nevědomosti či neúčasti rodičů.

Pravidla a dohled rodičů

Rodiče by měli mít kontrolu nad tím, jakým způsobem dítě využívá online sítě a mimo to, i jak dlouhou dobu na moderních technologiích tráví. Jsou děti, kteří nemají nijak určenou dobu, kterou mohou na mobilním telefonu strávit a rodiče zároveň nijak nekontrolují jejich aktivity. Taková absence veškerých opatřeních je z mého pohledu skutečně riziková. V některých rodinách mají děti pravidla ohledně chování na internetu, ale rodiče již nijak nekontrolují jejich aktivity. Ideální stav vnímám takový, když má dítě pravidla pro používání elektroniky, je poučeno o možných hrozbách a rodiče zároveň mají přehled o jeho aktivitách.

V dnešní době existují technologické nástroje, jako jsou kontrolní programy a filtry obsahu, které mohou pomoci chránit děti před nevhodným obsahem a kontrolovat dobu strávenou online. Toto opatření se mi jeví jako rozumné, a zvláště u menších dětí vnímám tento prostředek ochrany jako nezbytný.

Co se týče doby strávené na internetu, což je faktor, který také může ovlivnit bezpečnost dítěte v kybernetickém prostoru, tvrdím, že by rodiče měli být vzorem pro své děti a netrávit na internetových komunikačních prostředcích příliš mnoho času a co se týče chování, respektovat ostatní uživatele, nesdílet osobní údaje, nepsat nenávistné komentáře a celkově dodržovat pravidla bezpečného chování na

internetu. Jako základ prevence kybernetické bezpečnosti vnímám kombinaci vzdělávání, komunikace a dohledu, což pomůže vytvořit bezpečné a zdravé prostředí pro to, aby mohly děti objevovat svět internetu.

Vzdělávání a osvěta

Jak již bylo řečeno, je zapotřebí dětem vysvětlit základy bezpečného chování online jakmile vstupují do kybernetického prostředí. Tato úloha náleží zejména rodičům a pedagogům. Rodiče a pedagogičtí pracovníci však nejsou jediným zdrojem vzdělání kybernetické bezpečnosti. V této kapitole se zaměříme na činnost preventivních opatření policejního orgánu a celkově společnosti, která také může přispět k šíření osvěty kybernetické bezpečnosti.

V rozhovoru bylo panem por. Bc. Radovanem Hladem zmíněno, že v souvislosti s osvětou kybernetické kriminality a zejména pak té, která je zaměřena na zneužívání dětí na internetu by se měla celkově společnost zaměřit na výchovu a vzdělání dětí v oblasti sexuální výchovy.

Tímto se opět dostáváme k tomu, že dle mého názoru, je klíčem osvěty, prevence a celkově poučení a výchovy, ať už sexuální anebo kybernetické, upřímná, otevřená a respektující, komunikace rodiče a dítěte. Škola má samozřejmě také svůj podíl na výchově dítěte a nerada bych, aby komunikace dítěte a pedagoga byla upozaděna, ale jak už jsme se v minulosti několikrát přesvědčili, fungující rodinné vazby jsou základem pro zdravé fungování jedince a já v souvislosti s prevencí vnímám jako zásadní stabilní rodiče, kteří s dítětem komunikují, pečují o jeho psychiku, podporují ho a zajímají se o něj. S tím souvisí i fakt, že podstatě ve většině případů delikventních jedinců zaznamenáváme příčinu v rodinném prostředí. Rodiče by měli dětem poskytovat péči a pozornost, nikoliv pouze materiální věci, které jim na chvíli možná dají pocit štěstí, ale nenahradí jim emoční zázemí a nedají jim pocit bezpečného místa. V dnešní uspěchané době, kdy nemá na nic nikdo čas by se nemělo zapomínat na základní atributy rodiny, jako je láska a péče.

Prevence Policie ČR

V rámci své činnosti a v návaznosti na rozšíření problematiky zneužívání dětí na internetu a kyberšikany provádí Policie ČR prevenci kybernetické bezpečnosti pro děti ve školách, pedagogické pracovníky a rodiče formou

přednášek za použití powerpointových prezentací, výkladu a samozřejmě současných názorných příkladů.

Obsahem prezentací je nejprve seznámení s danou problematikou, to znamená definování daného pojmu (např. kybešikana či kybergrooming apod.), následně navazují tím, jak se taková problematika projevuje a koho a kde postihuje. V rámci přednášky bývají zmíněny i reálné případy, které se skutečně staly a ně pak navazuje prevence toho, jak se chránit před daným nebezpečím.

Závěr

Diplomová práce přináší podrobný pohled na problematiku kybernetické kriminality páchané na dětech a její dopady na společnost. Během analýzy jsme identifikovali hlavní příčiny tohoto problému a v souvislosti s tím provedli rozbor trestných činů spojených s kybernetickou kriminalitou páchanou na dětech. Překvapivým zjištěním byla vysoká úspěšnost v dopadení pachatelů, ale zároveň také rozsáhlé množství latentní kriminality, což svědčí o závažnosti této problematiky.

Také mě překvapilo zjištění, že pachatelé jsou si vědomi, že páchají trestnou činnost, avšak často si neuvědomují škodlivé následky svého jednání, zejména v kontextu dětských obětí. Proto je klíčové zaměřit se na prevenci, která by měla být pečlivě zajištěna prostřednictvím efektivních preventivních programů a osvěty.

V rámci vyšetřování a dokazování těchto trestných činů bylo zjištěno, že mezinárodní spolupráce probíhá na dobré úrovni, což je zásadní pro úspěšné řešení těchto případů.

Celkově lze konstatovat, že kybernetická kriminalita páchaná na dětech je vážným problémem, který vyžaduje komplexní přístup z hlediska prevence, vyšetřování a trestního stíhání. Je nezbytné nejen zvýšit povědomí o této problematice, ale také aktivně spolupracovat na nalezení účinných opatření pro ochranu dětí v digitálním prostředí.

Seznam použité literatury

Knižní publikace:

SMEJKAL, Vladimír. *Kybernetická kriminalita*. 3. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. ISBN isbn978-80-7380-849-5

HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha: Triton, 2012. ISBN 978-80-7387-545-9.s.35

KOLOUCH, Jan. *Cybercrime*. Praha: CZ.NIC, z. s. p. o., 2016. ISBN 978-80-88168-18-8

HAWKINS, D. Lynn; PEPLER Debra J., *York University* and Wendy M.; CRAIG Wendy M., *Queen's University*. *Naturalistic Observations of Peer Interventions in Bullying.* Blackwell

ŠEVČÍKOVÁ, Anna. *Děti a dospívající online: vybraná rizika používání internetu*. Praha: Grada, 2014. Psyché (Grada). ISBN 978-80-210-7527-6

WOLAK, J., Finkelhor, D., Mitchell, K. J., Ybarra, M. L. (2010). Online „predators" and their victims: Myths, realities, and implicitations for pervention and treatment. *Psychology of Violence, 1(S)*

CHMELÍK, Jan. *Mravnost, pornografie a mravnostní kriminalita*. Praha: Portál, 2003. ISBN 80-7178-739-6

PECHÁČKOVÁ, Marika. Kdo chytá v síti. Brno: BizBooks, 2020. ISBN 978-80-265-0919-6

JIROVSKÝ, V. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007, s. 19

Právní předpisy:

Listina základních práv a svobod vyhlášená usnesením Předsednictva České národní rady č. 2/1993 Sb. jako součást ústavního pořádku České republiky

Zákon č. 40/2009 Sb., trestní zákoník

Zákon č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů (zákon o soudnictví ve věcech mládeže)

Úmluva o právech dítěte z roku 1989

Judikatura:

Usnesení NS, sp. zn. 8 Tdo 612/2011 ze dne 15.6.2011

Usnesení NS, sp.zn. 7 Tdo 1579/2018 ze dne 23.1.2019

Ostatní zdroje:

ČSN ISO/IEC 2382-8 (369001). Informační technologie – Slovníku. Část 8: Bezpečnost

Společné sdělení Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor. JOIN (2013)0001 ze dne 7. 2. 2013. CELEX 52013JC0001.

TAYLOR, Chris. Reconsidering 'Star Wars kid,' the early internet's meanest moment. Mashable, publikováno 28.10.2020., (cit. 7.3.2024). Dostupné z: https://mashable.com/article/star-wars-kid-cyberbullying/?europe=true#

INTERNETEM BEZPEČNĚ 2018, Online vydírání [online] (cit. 7.3.2024), ISSN 2571-3736. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/online-vydirani/

POLICIE ČR (2023) [cit. 22.12. 2023], *Počítačová mravnostní kriminalita* [online], dostupné z <https://www.policie.cz/clanek/pocitacova-mravnostni-kriminalita.aspx>

KOPECKÝ, Kamil, SZOTKOWSKI, René. *E-bezpečí: Kybergrooming a sextortion (průvodce studiem).* Dostupné z: [*E-bezpečí: Kybergrooming a sextortion*] Olomouc 2018.

DRAŠTÍK, A., DURDÍK, T., FREMR, R., RŮŽIČKA, M., SOTOLÁŘ, A.*Trestní zákoník: Komentář*. [Systém ASPI]. Wolters Kluwer [cit. 2023-9-24]. ASPI_ID KO40_2009CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X.

[https://www.aspi.cz/products/lawText/13/6500/126/komentar-wkcr-c-40-2009-sb-trestni-zakonik-komentar]

Soustava státního zastupitelství, 2024 Nejvyšší státní zastupitelství [online] (cit. 2.3.2024), Ochrana dětí Dostupné z: https://verejnazaloba.cz/vice-o-sz/vse-podstatne-o-trestnim-rizeni/ochrana-poskozenych-a-ohrozenych-osob/ochrana-deti/

https://www.lidovky.cz/domov/mladik-mel-zneuzit-163-divek.A171206_121339_ln_domov_jho [cit. 2024-3-14]

RAK, R; PORADA, V. Charakteristiky a specifika digitálních stop. *Bezpečnostní teorie a praxe*, 2005, č. 1, s 71-84, resp. PORADA, V.; RAK, R. Digitální stopy v kriminalistice a forenzních vědách. Soudní inženýrství, XVII. 2006, č. 1

PORADA, V.; ŠEDIVÝ, P. Praktická využitelnost kriminalistických a forenzních aplikací v oblasti počítačové/kybernetické kriminality. *Karlovarská právní revue*, 2012, č. 3

SMEJKAL, V. *Současné možnosti boje proti počítačové kriminalitě*. Data Security Management, XV., 2011, č. 4

HEJDUK, Marek. *Bezpečnostní teorie a praxe* 1/2021 vědecký článek. Policejní akademie České republiky v Praze student doktorského studia

Boj společnosti Google proti materiálům zobrazujícím sexuální zneužívání dětí na internetu; Google Transparency report. Dostupné z: https://transparencyreport.google.com/child-sexual-abuse-material/reporting?hl=cs [cit. 23. 3. 2024]

Přílohy

- Potvrzení o poskytnutí materiálů kriminální služby

POLICIE ČESKÉ REPUBLIKY
Obvodní ředitelství policie Praha II
Služba kriminální policie a vyšetřování
Stálá výjezdová skupina
Karlovo náměstí 325/7, 120 00 Praha 2

POTVRZENÍ

V magisterské práci studentky slečny Daniely Podzimkové nar.9.9.1999. Na zpracované téma kybernetová kriminalita páchaná na dětech byly použity materiály kriminální služby. Vše bylo použito tak aby nedošlo k narušení identity osob, které byly v případech zneužity. Rovněž identita osob pachatelů jednotlivých případů je pozměněna. Vše bylo použito se souhlasem kriminální služby Obvodního ředitelství policie Praha II a krajského ředitelství SKPV hl. města Prahy. Všechny zde uvedené případy jsou uzavřeny a v současné době již neprobíhá jejich vyšetřování.

Por. Radovan Hlad
Policie České republiky
Obvodní ředitelství policie Praha II
odbor obecné kriminality
stálá výjezdová skupina
120 00 Praha 2, Karlovo náměstí 325/7