Univerzita Karlova

Právnická fakulta

Metodika vyšetřování kybergroomingu

Studentská vědecká odborná činnost

Kategorie: doktorské studium

Rok odevzdání: 2023 Autor: Mgr. Daniel Oborák

Konzultant: Mgr. Marek Pačmag, MBA, LL.M.

XVI. ročník soutěže Studentské vědecké a odborné činnosti

Čestné prohlášení a souhlas s publikací práce

Prohlašuji, že jsem práci předkládanou do XVI. ročníku Studentské vědecké a odborné činnosti (SVOČ) vypracoval samostatně za použití literatury a zdrojů v ní uvedených. Dále prohlašuji, že práce nebyla ani jako celek, ani z podstatné části dříve publikována, obhájena jako součást bakalářské, diplomové, rigorózní nebo jiné studentské kvalifikační práce a nebyla přihlášena do předchozích ročníků SVOČ či jiné soutěže.

Souhlasím s užitím této práce rozšiřováním, rozmnožováním a sdělováním veřejnosti v neomezeném rozsahu pro účely publikace a prezentace PF UK, včetně užití třetími osobami.

V Praze dne 20. 4. 2023

Mgr. Daniel Oborák

Celkový rozsah vlastního textu práce (od úvodu po závěr), včetně mezer a poznámek pod čarou: 52 487 znaků.

Obsah

1. Úvod

Vyšetřování mravnostních trestných činů páchaných na dětech bylo odjakživa z hlediska kriminalistiky neobvykle obtížnou disciplínou vyžadující specifickou odbornost a zvláštní kriminalistické postupy. Její speciální povaha vyvěrá zejména z požadavku na citlivý přístup orgánů činných v trestním řízení k obětem těchto trestných činů. Požadavek na ohleduplnost k dětským obětem se projevuje zejména při stěžejním okamžiku trestního řízení, kterým je výslech oběti. Vzhledem ke skutečnosti, že zásadním požadavkem na vedení trestního řízení je co největší minimalizace sekundární viktimizace dětské oběti, každé opakování výslechu v jednotlivých fázích trestního řízení či pouhé doplnění předchozího výslechu z důvodu zjištění nových skutečností je nežádoucí. Je tak zcela zásadní a klíčové, aby výslech oběti a vytěžení jejího nejbližšího okolí byly prováděny na základě předepsaných postupů speciálně vyškolenými pracovníky, a to tak, aby negativní efekt trestního řízení na oběť trestného činu byl co možná nejvíce redukován.

Kybergrooming, jakožto způsob navazování kontaktů s dětmi prostřednictvím kyberprostoru za účelem jejich sexuálního zneužití, je z hlediska požadavků na erudovanost orgánů činných v trestním řízení a na preciznost jejich postupu v rámci trestního řízení oblastí ještě problematičtější, a to vzhledem ke skutečnosti, že u kybergroomingu se specifika mravnostních trestných činů páchaných na dětech kombinují se specifiky kriminality páchané v kyberprostoru.

Kriminalita páchaná v kyberprostoru představuje v současné době jednu ze zásadních výzev kriminalistiky a forenzních věd, a to především vzhledem ke specifické povaze digitálních stop, které bývají zpravidla centrem dokazování těchto trestných činů, a ke zvláštnostem způsobů jejich zajišťování. K řádnému zajištění digitální stopy a k jejímu následnému vyhodnocení je potřeba nejen speciálně vyškolených pracovníků a zvláštních metodických postupů, ale rovněž moderního softwaru a technického vybavení. Stejně tak je zapotřebí specialistů s vysokou úrovní odbornosti v roli znalců oboru Informační a komunikační technologie. I přes relativně dobrou technickou i personální vybavenost specializovaných útvarů Policie České republiky je však kybernetická kriminalita z hlediska objasněnosti na samém chvostu statistických přehledů kriminality.

Cílem této práce je vytvoření metodiky vyšetřování kybergroomingu zahrnující veškeré složky kriminalistické metodiky, včetně kriminalistické charakteristiky, typických stop, podnětu i předmětu vyšetřování a přehledu jednotlivých úkonů činěných v rámci vyšetřování

této trestné činnosti. Metodika si klade za cíl v dostatečné míře reflektovat duální povahu kybergroomingu, který si právě z důvodu tohoto svého specifika zaslouží vlastní přehled kriminalistických metod a policejní praxe. Cílem autora této práce tak není pouze akademicko-teoretický pohled na kriminalistickou praxi orgánů činných v trestním řízení, ale je jím rovněž snaha o vytvoření jakési praktické příručky pro správné pochopení a kriminalistické „uchopení" tohoto aktuálního a mimořádně společensky škodlivého fenoménu.

2. Kriminalistická charakteristika kybergroomingu

Pojmem **kybergrooming** rozumíme cílené navazování blízkého vztahu útočníka s obětí, kterou je zpravidla dítě, za účelem jejího pozdějšího sexuálního zneužití, přičemž k navazování a rozvíjení tohoto kontaktu dochází prostřednictvím kyberprostoru, převážně pak v prostředí sociálních sítí.

Útočník s dítětem navazuje přátelský až intimní vztah a v průběhu času posiluje v dítěti pocit důvěry. Chování útočníka má za cíl vyvolat v oběti falešnou důvěru a přimět ji k osobní schůzce.[1] Kontakt útočníka s dítětem může být udržován po dlouhou dobu, může trvat měsíce i roky, než útočník iniciuje osobní schůzku s dítětem. V některých případech komunikují útočníci s dítětem pod vlastní identitou, často však využívají identit fiktivních, a to k vlastní ochraně či k posílení důvěry dítěte. Mnohdy se vydává za osobu věkově blízkou své oběti, přičemž se při samotném osobním setkání může v takovém případech vydávat za rodiče svého mladšího alter-ega, který má setkání zprostředkovat a oběť k fiktivnímu „příteli z internetu" dopravit.[2] Útočníci s homosexuálními sklony se pak často vydávají za osoby opačného pohlaví.

Ve chvíli, kdy dítě odmítá vyhovět návrhům útočníka, které mohou zahrnovat on-line sexuální aktivity či osobní setkání, obvykle dochází k obratu ve způsobu komunikace.[3] Útočník poté dítě citově vydírá či mu dokonce vyhrožuje zneužitím informací, které mu dítě dříve poskytlo, zpravidla zveřejněním intimních fotografií a videí na veřejně přístupných sítích, jejich zasláním rodičům, kamarádům či škole. Vzhledem k blízkému vztahu útočníka a oběti však

[1] KOPECKÝ, Kamil. *Rizikové formy chování českých a slovenských dětí v prostředí internetu*. Olomouc: Univerzita Palackého v Olomouci. 2015.
[2] KOPECKÝ, Kamil. *Op. cit.*, s. 39
[3] KOPECKÝ, Kamil. *Op. cit.*, s. 39.

dostatečnou hrozbou pro dítě může být již pohrůžka ukončením vzájemné komunikace útočníkem.[4]

Samotné osobní setkání útočníka s obětí je obvykle nejkritičtějším momentem celého procesu kybergroomingu. Zatímco v kyberprostoru je manipulace útočníka limitována specifiky zprostředkované komunikace a samotnou povahou kyberprostoru (v kyberprostoru se například do jisté míry stírá společenský statusový rozdíl mezi dospělou osobou a dítětem[5]), při bezprostředním kontaktu útočníka s dítětem bývá útočníkovo psychologické působení na dítě mnohem efektivnější. Při osobním setkání pak může útočník dítě pohlavně zneužít či využít k výrobě dětské pornografie.[6]

V roce 2011 byla přijata Směrnice Evropského parlamentu a Rady 2011/93/EU ze dne 13. prosince 2011 o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii, kterou se nahrazuje rámcové rozhodnutí Rady 2004/68/SVV („směrnice 2011/93/EU"). Směrnice mimo jiné reagovala na rostoucí hrozbu kybergroomingu a v čl. 6 stanovila požadavek na zajištění trestnosti navazování kontaktu s dětmi k sexuálním účelům členskými státy.

Český zákonodárce reagoval na přijetí směrnice 2011/93/EU novelizací trestního zákoníku zákonem č. 141/2014 Sb. s účinností od 1. 8. 2014, kterou bylo do Hlavy III. zvláštní části trestního zákoníku vloženo nové ustanovení § 193b upravující skutkovou podstatu trestného činu navazování nedovolených kontaktů s dítětem.

Trestný čin navazování nedovolených kontaktů s dítětem je v českém právním řádu koncipován jako předčasně dokonaný trestný čin. Materiálně se jedná o přípravu k trestnému činu pohlavního zneužití, výroby a jiného nakládání s dětskou pornografií, zneužití dítěte k výrobě dětské pornografie, svádění k pohlavnímu styku a k jiným sexuálně motivovaným trestným činům. K jeho dokonání postačí již samotné pozvání dítěte na schůzku. Pro naplnění skutkové podstaty trestného činu navazování nedovolených kontaktů s dítětem tak není třeba dalších kroků ze strany útočníka, jak stanovuje evropská úprava. Úmysl pachatele však již v době pozvání musí směřovat ke spáchání sexuálně motivovaného trestného činu. Dítětem

---

[4] KUDRLOVÁ, Kateřina. *Kriminalita spojená s využíváním nových médií dětmi*. Praha, 2019. Disertační práce. Katedra trestního práva. Právnická fakulta Univerzity Karlovy. Vedoucí práce doc. JUDr. Bc. Tomáš Gřivna, Ph.D. s. 141.
[5] KOPECKÝ, Kamil. *Rizikové formy chování českých a slovenských dětí v prostředí internetu*. *Op. cit*.
[6] VLACH, Jiří, KUDRLOVÁ, Kateřina, PALOUŠOVÁ Viktorie. *Kyberkriminalita v kriminologické perspektivě*. Praha: Institut pro kriminologii a sociální prevenci, 2020.

zákon v tomto ustanovení rozumí osobu mladší patnácti let věku. Navrhovatelem setkání přitom musí být sám pachatel, nikoliv dítě.

Trestný čin navazování nedovolených kontaktů s dítětem podle ustanovení § 193b trestního zákoníku nelze zcela ztotožňovat s kybergroomingem. Ve shodě s Krupičkou lze uvést, že tato skutková podstata kriminalizuje až závěrečnou fázi kybergroomingu, tedy samotný návrh osobní schůzky ve skutečném světě učiněný útočníkem.[7] Kybergrooming však může být trestný rovněž jako trestný čin výroby a jiného nakládání s dětskou pornografií podle § 192 trestního zákoníku, zneužití dítěte k výrobě pornografie podle § 193 trestního zákoníku či jako trestný čin sexuálního nátlaku podle § 186 trestního zákoníku, a to v závislosti na konkrétních skutkových okolnostech případu.[8] Komunikace s dítětem za účelem jeho pozdějšího znásilnění může být rovněž v závislosti na konkrétních skutkových okolnostech kvalifikována jako příprava zvlášť závažného zločinu znásilnění dle § 185 odst. 1, odst. 2 písm. b) ve spojení s § 20 odst. 1 trestního zákoníku v případě mladistvého, či § 185 odst. 1, odst. 3 písm. a) ve spojení s § 20 odst. 1 trestního zákoníku v případě dítěte mladšího patnácti let, i když doposud nemuselo dojít k nabídce osobní schůzky.

Ačkoliv psychologické působení na osobu za účelem jejího zneužití může být zaměřeno i na dospělé osoby a stále bude takové jednání spadat do definice kybergroomingu, tato metodika se těmito případy záměrně nezabývá. Hlavním důvodem je skutečnost, že nejde o typický způsob páchání kybergroomingu, a vyšetřování tak bude probíhat zásadním způsobem rozdílně. Tato metodika zároveň nebude podrobněji rozebírat postupy orgánů činných v trestním řízení v případě dokonaného znásilnění či pohlavního zneužití oběti na osobní schůzce oběti a útočníka, jelikož vyšetřování těchto skutečností je předmětem metodiky vyšetřování znásilnění či mravnostní kriminality v obecném slova smyslu.

3. Typické stopy

Kriminalistickou stopou rozumíme každou změnu v materiálním prostředí či ve vědomí člověka, která je v příčinné nebo jiné souvislosti s kriminalisticky relevantní událostí, existuje

[7] KRUPIČKA, Jiří. *Kybergrooming – zrcadlo společnosti?* In: GŘIVNA, Tomáš, RICHTER, Martin, ŠIMÁNOVÁ, Hana (eds.). Vliv nových technologií na trestní právo. Praha: Auditorium, 2022, s. 356.
[8] KRUPIČKA, Jiří. *Op. cit.*, s. 357.

nejméně od svého vzniku do zajištění a je vyhodnotitelná současnými kriminalistickými metodami a prostředky.[9]

Kriminalistické stopy tradičně dělíme na **stopy materiální** a **stopy paměťové**.[10] Zvláštním druhem kriminalistických stop, které nabývají na významu zejména v posledních desetiletích, jsou pak **stopy digitální**. Digitální stopy lze definovat jako jakákoliv data či informace přenesená, vytvořená, uložená či modifikovaná za použití počítačového systému.[11] Ačkoliv jsou digitální stopy některými autory řazeny mezi stopy materiální[12], svou nestálostí a dynamickou povahou se blíží stopám paměťovým, přičemž jejich nositelem je namísto paměti člověka paměťové médium počítačového systému či jiné technické zařízení, které je k ukládání informací tohoto typu určeno. Digitální stopy jsou ze své podstaty stopami latentními, ke zviditelnění kriminalisticky významných informací je tak třeba použít dodatečných technických prostředků a činností.[13] Problematickým aspektem zajišťování digitálních stop je rovněž skutečnost, že nelze předem zcela bezpečně určit, zda se na konkrétním nosiči informací či v počítačovém systému kriminalistické stopy nacházejí, respektive jaký je jejich rozsah.[14] Před zajištěním počítačového systému či nosiče informací je tak třeba udělat alespoň základní předběžnou analýzu za účelem zjištění, zda daný nosič kriminalisticky významné informace vůbec obsahuje.[15]

Z hlediska vyšetřování kybergroomingu budou v centru zájmu orgánů činných v trestním řízení zejména právě stopy digitální, jejichž nositeli budou zejména konverzace na sociálních sítích, uživatelské účty oběti i pachatele, e-mailové zprávy, chaty, fotografie v digitální podobě či videa. Digitálními stopami však budou také data o těchto datech (tzv. metadata), přihlašovací logy, záznamy o poloze zařízení, logy IP adres a jiné záznamy o provozu telekomunikačních zařízení.

Druhým stěžejním typem kriminalistických stop budou stopy paměťové, kterými rozumíme vzpomínky v paměti zainteresovaných osob. Těmito osobami mohou být kromě

---

[9] MUSIL, Jan, KONRÁD, Zdeněk, SUCHÁNEK, Jaroslav. *Kriminalistika. 2., přepracované a doplněné vydání*. Praha: C. H. Beck, 2004. s. 78.
[10] PORADA, Viktor, STRAUS, Jiří. *Kriminalistické stopy: teorie, metodologie, praxe*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2012. s. 61.
[11] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. s. 403.
[12] KOLOUCH, Jan. *Op. cit*. s. 404.
[13] STRAUS, Jiří, PORADA, Viktor. *Teorie, metody a metodologie kriminalistiky*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2017. s. 358.
[14] STRAUS, Jiří, PORADA, Viktor. *Op. cit.*, s. 358.
[15] STRAUS, Jiří, PORADA, Viktor. *Op. cit.*, s. 358.

pachatele a oběti také jiné osoby, kterým se oběť svěřila, tedy například přátelé oběti, její rodiče či učitelé a vychovatelé.

Co se týče vzniku materiálních stop, tyto nabývají při vyšetřování kybergroomingu na významu v případě realizace osobního setkání pachatele a oběti. V případě dokonaného sexuálního zneužití či znásilnění oběti pak zajištění materiálních stop bude jedním z prvotních a nedokladných úkonů.

4. Zvláštnosti předmětu vyšetřování

Základní předmět vyšetřování je v obecné rovině dán ustanovením § 89 odst. 1 trestního řádu. Rozumíme jím odpovědi na otázky, zda se stal skutek, v němž je spatřován trestný čin a zda tento skutek spáchal obviněný, případně z jakých pohnutek. Dále jsou jím podstatné okolnosti mající vliv na posouzení povahy a závažnosti činu, podstatné okolnosti k posouzení osobních rodinných, majetkových a jiných poměrů obviněného a podstatné okolnosti umožňující stanovení následku, výše škody či bezdůvodného obohacení. V neposlední řadě jsou jím okolnosti, které vedly k trestné činnosti nebo které spáchání trestného činu umožnily.

Jednotlivé zvláštní aspekty předmětu vyšetřování kybergroomingu lze rozdělit do následujících kategorií:

1. informace o útoku;
2. informace o počítačovém systému;
3. informace o datech;
4. informace o pachateli;
5. případná mnohost útoků.[16]

Informacemi o útoku rozumíme informace o metodách a formě navazování kontaktů mezi pachatelem a dítětem, o samotné povaze útoku (tedy zda šlo pouze o komunikaci v rámci kyberprostoru, či zda došlo k osobnímu setkání, při kterém pachatel dítě přiměl k pohlavnímu styku či jej zneužil k výrobě pornografie), případně také o následku způsobeném jednáním pachatele. Vyšetřování se bude zaměřovat zejména na obsahovou stránku komunikace mezi pachatelem a obětí kybergroomingu. V případě vyšetřování kybergroomingu je třeba posuzovat povahu zvolených slovních formulací a sdělovaných skutečností, jelikož podle povahy

[16] Kategorizace zvláštních aspektů předmětu vyšetřování bude obdobná, jako je tomu v případě obecné kybernetické kriminality. Srov.: KOLOUCH, Jan. *Op. cit.,* s. 406 – 407.

a způsobu komunikace mezi pachatelem a obětí je posuzován úmysl pachatele přimět dítě k sexuálním praktikám a intenzita praktik, ke kterým útok směřoval.[17]

Pro naplnění znaků skutkové podstaty trestného činu navazování nedovolených kontaktů s dítětem je rovněž důležité posouzení, zda to byl právě pachatel, kdo případnou osobní schůzku mezi ním a dítětem inicioval.

Informacemi o počítačovém systému rozumíme především informaci o tom, z jakého koncového přípojného bodu telekomunikační sítě byl útok prováděn, tedy z jakého počítačového systému k útokům docházelo, prostřednictvím čehož je možné zjistit, kdo je uživatelem profilu na sociální síti, ze kterého byl útok prováděn. Předmětem vyšetřování tak bude zejména zjištění IP adresy, ze které se útočník ke svému profilu na sociální síti jako koncový uživatel připojoval.

Informacemi o datech rozumíme zejména informace o tom, zda nebylo s daty manipulováno, tedy zda nedošlo k pozměnění komunikace mezi pachatelem a obětí, či k úpravě případných fotografií či videí, které obsahují kriminalistické stopy. Orgány činné v trestním řízení musejí v rámci vyšetřování zkoumat, zda nebyla porušena integrita těch dat, která mohou sloužit jako důkaz v trestním řízení. U každé digitální stopy je nutné zkoumat její pravost. Jak zdůrazňuje Smejkal, u digitálních stop nelze bez dalšího presumovat, že jsou pravé, jen proto, že vzešly z počítače.[18] Pravost informací získaných z digitálních stop je tak třeba v průběhu řízení ověřovat.

Co se týče **osoby pachatele**, stěžejním dílčím předmětem vyšetřování bude prokázání skutečnosti, zda pachatel věděl, že jeho jednání směřuje vůči dítěti mladšímu věku patnácti let. Dovodit skutečnost, že pachatel věděl, že se jedná o osobu mladší patnácti let, lze prostřednictvím analýzy komunikace s obětí, kdy oběť běžně útočníkovi svůj věk sama sdělí. Skutečnost, že pachatel musel znát informaci o věku oběti lze však také prokázat již ze samotného profilu oběti, kde je věk uživatele zpravidla uveden.[19]

Předmětem vyšetřování bude rovněž tzv. druhý úmysl pachatele, tedy úmysl směřující ke spáchání jiného sexuálně motivovaného trestného činu. V tomto ohledu je klíčové posouzení povahy sexuálně motivovaných narážek, které jsou součástí komunikace mezi pachatelem a

---

[17] Usnesení Nejvyššího soudu ze dne 25.11.2020 sp. zn. 8 Tdo 1041/2020.
[18] SMEJKAL, Vladimír. *Op. cit.*, s. 714.
[19] Prokázat útočníkovu znalost věku oběti lze například také tehdy, když útočník na facebookovém profilu oběti dá *„to se mi líbí“* u narozeninové fotografie, u které je uveden věk oslavence.

obětí kybergroomingu.[20] Pro prokázání zavinění, které je v případě trestného činu navazování nedovolených kontaktů s dítětem vyžadováno ve formě úmyslu, je nutné analyzovat obsahovou stránku komunikace mezi pachatelem a obětí kybergroomingu, přičemž v tomto ohledu bude zásadní povaha sexuálně motivovaných narážek. Dále je třeba posoudit, jaká je role pachatele v rámci sexuálně laděné komunikace, zda je v této komunikaci dominantním prvkem, či zda je prvkem pasivním.

K osobě pachatele je v rámci vyšetřování třeba dále zkoumat, zda se jednalo o osobu se sexuální deviací, či zda se jednalo o sexuálně zdravou. Je nutné zdůraznit, že pro naplnění skutkové podstaty trestného činu navazování nedovolených kontaktů s dítětem není zapotřebí, aby pachatel byl osobou s pedofilní, hebefilní, efebofilní[21] či jinou sexuální deviací. Zkoumání duševního stavu útočníka, zejména za účelem zjištění jeho případných sexuálních odchylek a preferencí, má význam především co do určení druhu a výše trestu, případně pro účely posouzení, zda je v daném případě namístě uložení ochranného opatření. Posouzení sexuální deviace a jejího vlivu na jednání pachatele je rovněž zásadní pro určení, zda v daném případě nebyly vymizelé ovládací a rozpoznávací schopnosti pachatele, tedy zda byla osoba v době spáchání trestného činu příčetná, či zda nedošlo v důsledku sexuální deviace alespoň k jejich podstatnému snížení, tedy zda se v tomto případě nejednalo o zmenšenou příčetnost ve smyslu ustanovení § 27 trestního zákoníku. Zodpovězení těchto otázek bude předmětem vyšetření duševního stavu obviněného znalcem z oboru sexuologie ve smyslu ustanovení § 116 trestního řádu.[22]

Co se týče šetření k **mnohosti útoků** kybergroomera, jediný útočník bude obvykle komunikovat s větším počtem potenciálních obětí, aby zvýšil svou šanci na úspěšné vylákání pornografického obsahu či na zneužití dítěte. Nebývá výjimkou, že jeden útočník zakládá více profilů pod různými identitami, a to i v rámci jediné sociální sítě či seznamky. V rámci vyšetřování je tak zapotřebí provázat jednotlivé účty a *aliasy* založené a využívané jediným útočníkem s touto konkrétní osobou, resp. zpravidla také s jedním počítačovým systémem, ze kterého útoky činěné prostřednictvím většího počtu účtů směřovaly, a to prostřednictvím identifikace shodných markantů technického (IP adresy) i netechnického (jméno, přezdívka, modus operandi) charakteru.

---

[20] Usnesení Nejvyššího soudu ze dne 25.11.2020 sp. zn. 8 Tdo 1041/2020. Bod 51.
[21] Hebefilií rozumíme sexuální deviaci spočívající v sexuální náklonnosti vůči dospívajícím dívkám, efebofilií naopak rozumíme sexuální náklonnost vůči dospívajícím chlapcům.
[22] K tomuto více v kapitole 9. „Specifika následných úkonů“.

5. Zvláštnosti podnětů vyšetřování

Kybergrooming probíhá většinou skrytě a bez vědomí orgánů činných v trestním řízení, stejně tak bez vědomí rodičů, učitelů a dalších dospělých osob, které by bylo možné z hlediska kriminologie označit za tzv. schopné strážce[23]. Tam, kde by v případě groomingu ve skutečném světě pachateli hrozilo odhalení již samotnou přítomností jiných dospělých osob (např. na dětských hřištích, v okolí škol, ale rovněž také na dětských táborech či v zájmových kroužcích), se v případě kybergroomingu může útočník skrýt pod anonymním pláštěm kyberprostoru. Ze samotné anonymní povahy kyberprostoru a z jeho domnělé oddělenosti od skutečného světa vyplývá jeden ze zásadních kriminologických aspektů kybergroomingu, kterým je jeho relativně vysoká latence.

Oproti jiným typům kybernetické kriminality vysokou latentnost tohoto fenoménu podporuje rovněž skutečnost, že se dětské oběti kybergroomingu bojí rodičům či jiným dospělým osobám sdělit, že se stalo obětí internetového útočníka. Dětské oběti kybergroomingu, obzvláště ty mladší, se zpravidla domnívají, že ony samy se dopustily něčeho zakázaného a že budou potrestány, a to například rodičovským zákazem nebo omezením užívání internetu či sociálních sítí. Z těchto důvodů bývá samo dítě oznamovatelem jen v ojedinělých případech. Trestní oznámení zpravidla podává rodič dítěte, pedagog či jiná dospělá osoba. Pokud dochází k oznámení samotným dítětem, takové oznámení bývá učiněno na popud právě těchto osob. Z toho může vyplývat prvotní neochota či zdrženlivost oběti kybergroomingu spolupracovat s orgány činnými v trestním řízení na odhalení a dopadení pachatele. V tomto ohledu je nutné si uvědomit, že oběť kybergroomingu nemusí pociťovat zájem rodičů a okolí (potažmo zájem orgánů činných v trestním řízení) na vyšetření věci a na dopadení a potrestání pachatele jako zájem vlastní. Jak již bylo výše uvedeno, kybergrooming spočívá v navázání přátelského až intimního vztahu s dítětem, který nemusí být následným sexuálně motivovaným nátlakem na dítě zcela přetrhán. Motivací dítěte nespolupracovat s policií tak může kromě studu a strachu z potrestání jeho samotného pramenit rovněž ze snahy útočníkovi pomoci.

---

[23] Z anglického termínu *„capable guardians“*. Jedná se o osoby, které svou pouhou přítomností odrazují potenciální útočníky od spáchání trestného činu. Jde o součást teorie rutinní činnosti Cohena a Felsona, srov.: COHEN, Lawrence E., FELSON, Marcus. *Social Change and Crime Rate Trends: A Routine Activity Approach. American Sociological Review* [online]. 1979, 44 (4) [cit. 2023-04-15]. Dostupné z: doi:10.2307/2094589.

Při absenci osob, které by kybergrooming oznamovaly, se nabízí řešení v podobě vyhledávání trestné činnosti samotnými orgány činnými v trestním řízení, tedy zjišťování informací o trestných činech na základě vlastní operativně pátrací činnosti útvarů Policie České republiky. V kontextu nedávných projektů, které měly za cíl informovat veřejnost o hrozbách internetového predátorství za pomocí vytvoření falešných profilů dětí, jakými byly dokumentární film autorů Víta Klusáka a Barbory Chalupové s názvem *V Síti* či pořad *Černota* internetové televize *stream.cz*, by bylo možné uvažovat o vyhledávání a „chytání" kybergroomerů za pomoci falešných dětských profilů vytvářených a spravovaných přímo příslušníky Policie České republiky. Dle Krupičky však takové postupy mohou hraničit s řízenou policejní provokací a jsou nepřípustné bez podezření na konkrétní osobu.[24] Dle názoru autora této práce však může být případná institucionalizace vyhledávání profilů kybergroomerů „policejními agenty" při současném šetření ústavně zaručených práv a svobod dotčených osob v souladu s principy českého trestního práva procesního a mohlo by jít o vhodný návrh *de lege ferenda*.[25]

Orgány činné v trestním řízení se o existenci profilů útočníků na sociálních sítích a o dalším závadném obsahu spojeném se zneužíváním dětí včetně dětské pornografie dozvídají rovněž prostřednictvím tzv. **reportů** v rámci projektu *CyberTipline* americké neziskové organizace *National Center for Missing & Exploited Children* („NCMEC"). Provozovatelé sociálních sítí a dalších internetových služeb poskytují společnosti NCMEC informace o závadném obsahu, který na svých sítích detekují. Na základě těchto dat jsou vypracovávány reporty, které jsou prostřednictvím institucí mezinárodní justiční a policejní spolupráce přeposílány orgánům činným v trestním řízení států, na jejichž území se útočník dle zjištěné IP adresy nachází.[26] Tyto reporty jsou v případě České republiky zasílané prostřednictvím EUROPOLu Úřadu Služby kriminální policie a vyšetřování Policejního prezidia Policie České republiky. Obsahem těchto reportů jsou především soubory či záznamy komunikace, které byly vyhodnoceny jako závadné, společně s časovými značkami, údaji o profilu útočníka, IP

---

[24] KRUPIČKA, Jiří. *Op. cit.,* s. 352.

[25] Příkladem ze zahraničí může být operativně pátrací činnost britské policie v kyberprostoru, tzv. **covert sting operations** (volně přeloženo z angl. jako operace skrytého žihadla), kdy policie právě na výše uvedeném principu „loví" kybergroomery. Tato činnost má přísně stanovené mantinely, kdy nesmí ze strany policejního orgánu docházet k žádné formě iniciace komunikace s útočníkem, policejní orgán musí být v této komunikaci zdrženlivý a nesmí sám iniciovat osobní schůzku. Zdroj: Online grooming and UK law. Childnet International [online]. [cit. 2023-04-17]. Dostupné z: <https://www.childnet.com/wp-content/uploads/2014/08/online-grooming.pdf>.

[26] CyberTipline Reports [online]. NCMEC [cit. 2023-04-15]. Dostupné z: <https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata#reports>.

adresami jednotlivých přihlášení, časů podezřelých aktivit a dalších informací, na základě kterých lze provést jednoznačnou identifikaci zařízení, ze kterého byl útok proveden, potažmo i samotného pachatele.[27]

Vyloučeno není ani oznámení učiněné právnickou osobou, zpravidla bude takovou osobou provozovatel sociálních sítí či jiných služeb v rámci kyberprostoru, či ISP[28]. Oznamovatelem může být v případě kybergroomingu rovněž škola či jiná výchovně vzdělávací instituce, podobně jako je tomu rovněž u jiných druhů mravnostní kriminality páchané na dětech.[29]

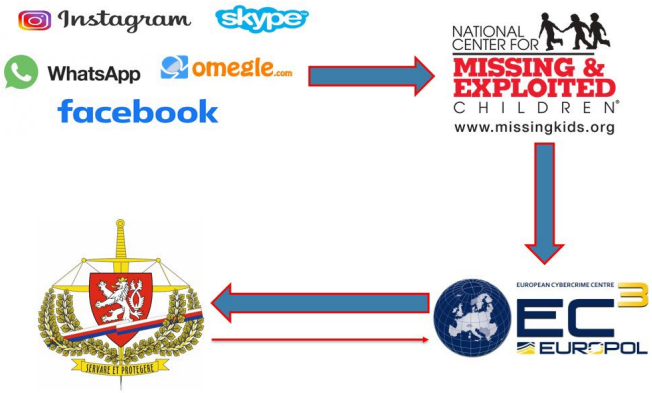


Diagram znázorňující cestu reportu NCMEC k národnímu policejnímu orgánu
Zdroj: Policie České republiky

6. Typické vyšetřovací situace

Vyšetřovací situací rozumíme stav, v němž se nalézá vyšetřování v určitém momentu, v němž se rozhoduje o dalším postupu ve vyšetřování.[30] Tento stav je determinován mnoha proměnnými, z nichž je z hlediska typizace vyšetřovacích situací nejpodstatnější **stupeň informační určitosti**, tedy kvalita a kvantita informací, které jsou obsahem souboru poznatků o trestném činu a o jeho pachateli, jež má v daný moment orgán činný v trestním řízení

[27] Některé případy dopadení pachatele na základě mezinárodní spolupráce s NCMEC byly v České republice medializovány. Příkladem je případ zneužívání sedmileté dívky otcem, který si styk nahrával na mobilní telefon. Zdroj: Muž měl zneužívat malou holčičku. Policie ČR [online]. [cit. 2023-04-15]. Dostupné z: <https://www.policie.cz/clanek/muz-mel-zneuzivat-malou-holcicku.aspx>.
[28] *Internet service provider* (zkr.), v překladu (z angl.) poskytovatel internetového připojení.
[29] CHMELÍK, Jan. *Rukověť kriminalistiky*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. s. 339.
[30] PORADA, Viktor.. *Op. cit.,* s. 838.

k dispozici.[31] Dalšími faktory mohou být podmínky materiální, organizační i personální, které se budou lišit například podle materiální vybavenosti vyšetřujícího útvaru, podle osobnosti vyšetřovatele, jakož i podle okolností, jenž ze strany orgánu činného v trestním řízení ovlivnit nelze, jako je počasí či politicko-společenská situace. Vyšetřovací situaci v případě kybergroomingu ovlivňuje také úroveň rizikového chování dětí na internetu či celková kybernetická gramotnost ve společnosti.[32] Aktuální vyšetřovací situace determinuje, jaké vyšetřovací verze budou vytyčeny, které úkony budou provedeny jako prvotní a jak bude probíhat následná etapa vyšetřování.

Typickou počáteční vyšetřovací situací v případě kybergroomingu bude situace, v níž orgány činné v trestním řízení zjistí skutečnosti nasvědčující tomu, že se stal skutek, v němž je spatřován trestný čin, v hrubých rysech pak mohou znát i skutečnosti objasňující způsob spáchání předmětného trestného činu, které mohou být obsahem již samotného trestního oznámení, přijatého reportu NCMEC či oznámení jiného subjektu.

Počáteční vyšetřovací situace kybergroomingu se pak budou lišit podle toho, zda již od počátku vyšetřování známe totožnost útočníka (jinými slovy zda vystupuje pod svým skutečným jménem – v ideálním případě se současným uvedením datumu narození), či zda vystupuje toliko pod přezdívkou či zda používá falešnou identitu.[33] Ztotožnění útočníka podle informací vyplývajících z profilu na sociálních sítích je možné na základě jednoduché prověrky učinit také v případech, kdy není uvedeno přímo jeho jméno a datum narození, ale je uvedena jeho e-mailová adresa či telefonní číslo.[34]

7. Typické vyšetřovací verze

Vyšetřovacími verzemi v kriminalistice rozumíme jeden z druhů tzv. kriminalistických verzí, mezi které dále řadíme operativně-pátrací verze a soudní verze.[35] Kriminalistickými verzemi rozumíme metodu kriminalistické praxe spočívající ve vyvození a prověrce všech

---

[31] PORADA, Viktor. *Op. cit.,* s. 838.
[32] HEJDUK, Marek. *Kriminalistické aspekty odhalování, prověřování a vyšetřování počítačové mravnostní kriminality. Bezpečnostní teorie a praxe.* Praha: Policejní akademie. 2021 (1). Dostupné z: <https://veda.polac.cz/wp-content/uploads/2021/04/Kriminalisticke-aspekty-odhalovani-proverovani-a-vysetrovani-pocitacove-mravnostni-kriminality.pdf. s.71>.
[33] Srov. typické počáteční situace v případě obecné kybernetické kriminality: PORADA, Viktor. *Op. cit.,* s. 967 – 969.
[34] A to prověrkou uvedených údajů v policejních informačních systémech jako jsou IS Telefony či Centrální databáze objektů, ve které můžeme rovněž zjistit případné provázání s jinými již dříve šetřenými incidenty.
[35] KONRÁD, Zdeněk, PORADA, Viktor, STRAUS, Jiří, SUCHÁNEK, Jaroslav. *Op. cit.,* s. 21.

dosud opodstatněných domněnek o příčinách a formách spojení všech jevů kriminalisticky významné události jako reálně možných objasnění doposud zjištěných skutečností. Cílem kriminalistických verzí je prověrka doposud zjištěných skutečností a získání znalosti o nových skutečnostech, přičemž kriminalistické verze jsou potřebné pro zaměření dalšího průběhu vyšetřování.[36]

V případě trestněprávního postihu kybergroomingu je středobodem vyšetřování objasnění skutečností prokazujících či vyvracejících naplnění znaku subjektivní stránky trestného činu ve formě úmyslu. Vytyčené vyšetřovací verze se tak budou alespoň zpočátku primárně zaobírat existencí či neexistencí úmyslu pachatele dítě prostřednictvím kybergroomingu zneužít. Typické vyšetřovací verze mohou být v případě, že je skutek kvalifikován jako navazování nedovolených kontaktů s dítětem podle ustanovení § 193b trestního zákoníku, s ohledem na výše uvedené vytyčeny takto:

1. osoba vylákala dítě k osobní schůzce s úmyslem jejího pozdějšího sexuálního zneužití či výroby pornografického materiálu, přičemž věděla, že se jedná o dítě ve věku mladším patnácti let;
2. osoba nabídla dítěti osobní schůzku bez úmyslu jejího pozdějšího sexuálního zneužití či výroby pornografického materiálu;
3. osoba nabídla dítěti osobní schůzku za účelem sexu či výroby pornografického materiálu, avšak zároveň se domnívala, že se jedná o osobu starší patnácti let.

8. Specifika počátečních úkonů

Bezprostředně poté, co se orgán činný v trestním řízení dozví o skutečnostech důvodně nasvědčujících tomu, že došlo ke spáchání trestného činu, je zapotřebí učinit neodkladné úkony, kterými se rozumí ty úkony, jejichž včasné neprovedení by mohlo zmařit účel trestního řízení.

V případě kybergroomingu se u vymezení počátečních úkonů projevuje zejména jeho kybernetická podstata, proto bude v plánu vyšetřování předním příčkám vévodit zajištění kriminalisticky relevantních dat, primárně tedy zajištění komunikace mezi pachatelem a obětí. Zásadní je rovněž zjištění IP adresy počítačového systému, ze kterého se útočník ke svému profilu přihlašoval, a to včetně data a času připojení prostřednictvím této adresy k dané sítí.

[36] KONRÁD, Zdeněk, PORADA, Viktor, STRAUS, Jiří, SUCHÁNEK, Jaroslav. *Op. cit.,* s. 20.

Klíčové je v tomto ohledu včasné zajištění **přihlašovacích logů** k účtu útočníka obsahujících IP adresy, které si lze vyžádat od provozovatele dané sociální sítě či jiné služby. Za součinnosti s poskytovateli internetového připojení (ISP), kteří po dobu šesti měsíců uchovávají informace o počítačových systémech včetně IP adres, času a délky používané služby, lze pak pomocí přihlašovacích logů k danému účtu určit koncový přípojný bod, tedy počítačový systém, ze kterého byl útok veden.[37]

Počátečním úkonem ve věci je rovněž **ohledání uživatelského účtu útočníka a uživatelského účtu oběti** na předmětné sociální síti či jiné službě. Ohledání uživatelského účtu orgány činíme za účelem prvotního zajištění kriminalistických stop nacházejících se přímo na profilu uživatele sociální sítě či jiné služby, než dojde ke zmrazení a poskytnutí těchto dat provozovatelem služby. Vyšetřovatel pořizuje prostřednictvím printscreenů obrazovky záznamy o veřejně dostupných informacích k předmětnému účtu, kterými mohou být jméno či *nick* účtu, přiložená fotografie, seznam přátel, zveřejněné statusy, webovou adresu účtu a další data. Součástí ohledání by mělo být zajištění tzv. **jednoznačného identifikátoru účtu**, tedy unikátního nezměnitelného kódu účtu, který každý jednotlivý účet v rámci předmětné sítě odlišuje od ostatních účtů, přičemž se takový kód nemění nehledě na případné změny jména, nicku, profilové fotografie či dalších údajů. Ohledání uživatelského účtu se řídí ustanovením § 113 trestního řádu a je třeba o něm vyhotovit protokol. Stejným způsobem lze učinit prvotní ohledání komunikace mezi útočníkem a dítětem při přijetí trestního oznámení.

Pro řádné zajištění komunikace mezi pachatelem a obětí je však třeba co nejrychleji zajistit data nacházející se na serverech třetích osob, zpravidla provozovatelů sociálních sítí a dalších internetových služeb, a to tak, aby nedošlo k jejich odstranění či pozměnění útočníkem v důsledku jeho obavy z trestního stíhání. Z důvodu požadavku na zachování dat v nezměněné podobě před jejich zajištěním je třeba využít institutu příkazu k uchování dat, tzv. **data freezing** či **data preservation**, ve smyslu ustanovení § 7b odst. 1 trestního řádu. V případě žádosti českých orgánů činných v trestním řízení o uchování dat nacházejících se v datových centrech umístěných na území jiných států, což se týká většiny „velkých“ provozovatelů internetových služeb, lze pak postupovat urychleně dle ustanovení § 65a odst. 1 zákona č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních, ve znění pozdějších předpisů, u něhož dochází k žádost o uchování dat českými orgány cestou přímé komunikace mezi Národní centrálou proti terorismu, extremismu a kybernetické kriminalitě Policie České republiky, která

[37] HEJDUK, Marek. *Op. cit.*, s. 73 – 74.

pro Českou republiku plní funkci kontaktního místa podle mezinárodní smlouvy, a příslušným zahraničním útvarem.

Takto uchovaná data si posléze orgán činný v trestním řízení vyžádá od provozovatelů služeb prostřednictvím příslušných zajišťovacích institutů trestního práva procesního, a to s ohledem na povahu zajišťovaných dat buď prostřednictvím ustanovení § 158d odst. 3 trestního řádu v případě, že se jedná o samotnou obsahovou stránku komunikace, nebo prostřednictvím postupu dle ustanovení § 88a trestního řádu pro případ, že se jedná o údaje o telekomunikačním provozu.

V případě, že je již od počátku známa osoba, která útoky prováděla, resp. je znám počítačový systém, z nějž byly útoky prováděny, je zapotřebí neodkladně provést **ohledání místa činu**, respektive **domovní prohlídku** případně **prohlídku prostor nesloužících k bydlení**[38] a zajistit veškeré nalezené hmotné nosiče dat a samotný počítačový systém, ze kterého byly útoky prováděny, a provést jejich ohledání. Při těchto úkonech by měla být zajištěna přítomnost experta z oboru výpočetní techniky, který navrhuje rozsah zajištění pro potřeby počítačové expertízy a zajišťuje podrobné zadokumentování situace, zejména stavu techniky v době zahájení úkonu, dále informace o tom, zda je či není technika v provozu a zda je připojena k síti elektronické komunikace.[39] V případě přítomnosti většího počtu počítačových systémů je třeba se soustředit rovněž na připojení jednotlivých počítačových systémů k internetové síti, a to co do zjištění způsobu připojení u jednotlivých systémů a co do identifikace jednotlivých ISP poskytujících připojení, případně je třeba určit a zaznamenat topologii lokální sítě a propojení počítačových systémů mezi sebou (např. v případě vedení útoků skrze firemní počítač).[40]

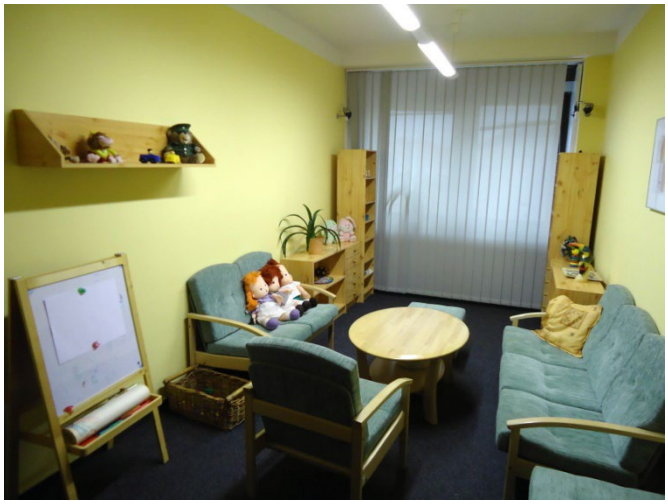
9. Specifika následných úkonů

Klíčovým momentem celého vyšetřování je **výslech oběti trestného činu – dítěte**. V tomto bodě vyšetřování se nejintenzivněji projeví povaha kybergroomingu jakožto trestného činu mravnostního, z čehož vyplývá požadavek na vysoce profesionální práci s obětí, a to z důvodu obzvláště vysokého rizika její sekundární viktimizace.

---

[38] Případně **osobní prohlídku** za účelem zajištění mobilního telefonu či jiného přenosného zařízení či nosiče, kterou má osoba u sebe.
[39] KONRÁD, Zdeněk, PORADA, Viktor, STRAUS, SUCHÁNEK, Jiří. *Op. cit.,* s. 348 – 349.
[40] KOLOUCH, Jan. *Op. cit.*, s. 427 – 428.

Výslech dítěte jakožto oběti trestného činu by měla vždy vykonávat osoba, která je v této oblasti vyškoleným specialistou. Výjimkou mohou být situace, kdy nelze takovou osobu zajistit a kdy by pozdější provedení úkonu mohlo zmařit účel trestního řízení. I v takovém případě je však vždy třeba dbát o to, aby nebylo dítě výslechem traumatizováno a aby bylo co nejvíce redukováno riziko vzniku jeho sekundární viktimizace. Je-li to pro dítě výhodné, měl by být výslech dítěte prováděn ve speciální výslechové místnosti.[41]



Speciální výslechová místnost pro děti – Krajské ředitelství policie Praha
Zdroj: Policie České republiky

Klást otázky dítěti jinými osobami je v souladu s ustanovením § 102 odst. 3 trestního řádu možné pouze prostřednictvím vyslýchajícího. Vzhledem k povaze kybergroomingu pak bude u výslechu dětí mladších patnácti let obvykle přítomen orgán sociálně-právní ochrany dětí nebo osoba mající zkušenosti s výchovou mládeže. Vhodná je rovněž přítomnost dětského psychologa. Rovněž lze zmínit, že výslech dětí mladších patnácti let by měl být prováděn v dopoledních hodinách.

Specifický přístup k dětské oběti mravnostního trestného činu by se měl projevovat ve všech stadiích výslechu. Již před začátkem samotného výslechu je důležité vhodným způsobem navázat kontakt s dítětem, při kterém je zásadní získat jeho důvěru.[42]

---

[41] Speciální výslechová místnost je přizpůsobena dětem tak, aby co možná nejvíce navozovala pocit bezpečí a pohody. Nezbytnou součástí vybavení jsou demonstrační pomůcky – panenky **Jája, Pája, maminka, tatínek, babička a děda**, na kterých dítě může popsat zneužití méně traumatizujícím způsobem. Zdroj: Standard vybavení speciální výslechové místnosti pro dětského účastníka trestního řízení [online]. Policie ČR [cit. 2023-04-17]. Dostupné z: <https://www.mvcr.cz/clanek/standard-vybaveni-specialni-vyslechove-mistnosti-pro-detskeho-ucastnika-trestniho-rizeni.aspx>.

[42] ČÍRTKOVÁ, Ludmila. *Forenzní psychologie. 3., upr. vyd.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2013. s. 179.

V úvodní fázi výslechu je třeba dítě poučit, a to přiměřeně jeho věku. Účelem poučení dítěte není pouze dodržení zákonných požadavků výslechu a šetření práv vyslýchané osoby, ale také seznámení dítěte s tím, co se konkrétně bude dít a jak bude rozhovor probíhat, čímž by měla vyslýchající osoba dítě do jisté míry uklidnit.

Je třeba zdůraznit, že traumatizující povaha kybergroomingu může mít významný vliv na kvalitu výpovědi dítěte, které se stalo obětí tohoto typu jednání. Dle Čírtkové mohou výpověď dítěte, které se stalo obětí mravnostní kriminality, negativně ovlivňovat některé obranné mechanismy jeho psychiky, jako je:

- *vytěsnění* – určité traumatizující komponenty děje mohou být vytěsněny, jelikož vzpomínky na tyto děje mohou psychiku dítěte silně destabilizovat;
- *popření* – dítě se brání akceptovat realitu tím, že ji zcela popře;
- *disociace* – vzpomínky na traumatizaci nejsou integrovány do celkového vnitřní života oběti, ač nejsou vytěsněny (v mysli dítěte dochází k odštěpení „dobré stránky“ a „zlé stránky“ pachatele, jako by šlo o dvě odlišné osoby);
- *idealizace – devalvace* – možná je také idealizace pachatele dítětem jdoucí ruku v ruce s devalvací sebe sama či svého okolí (například rodičů), a to za účelem iluzorního vyhnutí se konfliktu s blízkou osobou, kterou pro dítě kybergroomer představuje;
- *identifikace s agresorem* – je rovněž možná vnitřní akceptace pachatele dítětem a jeho identifikace s ním.[43]

Znalost uvedených obranných mechanismů ega dítěte, a to za současné schopnosti identifikovat vzpomínkové mezery v paměti vyslýchaného, je klíčová pro korektní vedení výslechu ze strany orgánu činného v trestním řízení i pro posuzování věrohodnosti výpovědi dítěte – oběti.[44] Vyslýchající musí počítat rovněž se zvýšenou sugestibilitou dítěte, tedy větší náchylností dítěte „vyhovět“ vyslýchajícímu kladnými odpověďmi na otázky.

Významným následným úkonem vyšetřování je analýza zajištěných digitálních stop, jež mohou být nositeli důkazů v trestním řízení, které se provádí za pomocí znaleckého zkoumání stop – **digitální forenzní analýzy**. Pro práci s digitálními stopami je klíčové, aby bylo v okamžiku jejich použití jako důkazu možné prokázat, že v průběhu řízení nedošlo k jejich

[43] ČÍRTKOVÁ, Ludmila. *Op. cit.,* s. 178 – 179.
[44] ČÍRTKOVÁ, Ludmila. *Op. cit.*, s. 179.

modifikaci. Základní zásadou zajišťování digitálních stop je proto **zásada zachování integrity digitální stopy**. Při práci s digitálními stopami, od jejich zajištění, přes jejich analýzu až do ukončení znaleckého zkoumání a následné předložení stopy jako důkazu před soudem, je třeba dodržovat určité principy, které k naplnění této zásady vedou.[45] Předně je třeba pracovat – pokud je to v dané situaci možné – s tzv. **duplikátem digitální stopy**, kterým se rozumí přesná bitová kopie datového nosiče, tedy přesná digitální reprodukce všech datových objektů obsažených na originálním fyzickém nosiči dat přenesená na nosič dat stejného typu. Oproti tomu běžná **kopie digitální stopy**, u které nedochází k přenosu dat na stejný typ média, nemusí obsahovat veškeré informace originálního nosiče, její průkazní a technická hodnota tak bude nižší.[46] S pouhou kopií dat se budeme muset spokojit v případě, že nemáme přístup k fyzickému nosiči. Pro zajištění integrity digitální stopy je třeba dále provést autentizaci duplikátu digitální stopy prostřednictvím kontrolního součtu, tzv. ***hashe***.[47] Ověřování *hashe* by mělo být prováděno průběžně, a to zejména, pokud nedochází k analýze dat bezprostředně po jejich zajištění.[48]

Smejkal k tomuto uvádí, že pořízení bitových kopií a jejich následné *hashování* přichází v úvahu v případě analýzy „neživých" zařízení, kterými se rozumí statické datové nosiče. V současné době se však stále častěji objevuje potřeba zajišťovat tzv. dynamická paměťová zařízení, u kterých by odpojení či vypnutí mohlo vést k nenávratné ztrátě relevantních dat, nebo takové odpojení není vzhledem k povaze systému vůbec možné. Při zajišťování dat z těchto systémů pak nutně dochází k určitému zásahu do samotného předmětu zkoumání, vzhledem ke skutečnosti, že pro uchování dat či pro analýzu běžícího systému je třeba spustit program, který do integrity datového nosiče či systému vždy do jisté míry zasáhne, jinými slovy provede změnu v takovém systému.[49] Zajišťování a vyhodnocování stop v dynamickém prostředí se označuje jako ***Live Forensics***, resp. ***Live Data Acquistition***.[50] Integrita digitálních stop tak v těchto případech nemůže být zajištěna zcela do důsledku.

---

[45] SMEJKAL, Vladimír. *Op. cit.,* s. 700.
[46] PORADA, Viktor. *Dokazování obsahu elektronických dokumentů.* Košická bezpečnostná revue. Košice, 2012, 2012 (2), 104 - 108. s. 105.
[47] Jedná se o proces, při kterém je soubor dat převeden na základě určité matematické funkce do relativně malého čísla, přičemž opětovným použitím stejného algoritmu lze porovnáním výsledných čísel zjistit, zda došlo ke změně v původním souboru dat.
[48] AMIRIDU, Radka. *Zajištění integrity elektronického důkazu*. Brno, 2021. Diplomová práce. Masarykova Univerzita. Vedoucí práce JUDr. Mgr. Jakub Harašta, Ph.D.
[49] SMEJKAL, Vladimír. *Op. cit.*, s. 699.
[50] K rozdílnosti zajišťování kopií „živých" a „neživých" zařízení viz KOLHE, Mahesh, AHIRAO, Purnima. *Live Vs Dead Computer Forensic Image Acquisition*. In: International Journal of Computer Science and Information Technologies. 2017, 8 (3), s. 455-457.

Obsahem samotné digitální forenzní analýzy jsou aktivity směřující k analýze všech procesů, které vznikly v průběhu kriminalisticky relevantní události, a to tak, aby mohlo být na základě výsledků analýzy zodpovězeno na základní kriminalistické otázky **Kdo? Co? Kde? Kdy? Jak? Proč?**. Výsledkem digitální forenzní analýzy je pak znalecký posudek. [51]

Významným následným úkonem vyšetřování kybergroomingu je, jak již bylo uvedeno ve čtvrté kapitole této práce, **znalecké zkoumání duševního stavu útočníka**, a to především co do potvrzení či vyvrácení hypotézy o sexuální deviaci pachatele a jejím případném vlivu na spáchání trestného činu. Ustanovení § 116 odst. 1 trestního řádu stanovuje požadavek, aby k vyšetření duševního stavu obviněného byl přibrán znalec z oboru psychiatrie. Přibrání jediného znalce v oboru sexuologie bude v takovém případě vzhledem k požadavku vyjádřeném ustanovením § 116 odst. 1 trestního řádu možné toliko v případě, že se bude zároveň jednat o znalce se specializací v oboru psychiatrie, v jiném případě bude ke znalci v oboru sexuologie nutné přibrat znalce v oboru psychiatrie.[52]

Samotné sexuologické vyšetření zahrnuje anamnestické vyšetření pachatele, zpracování informací ze spisu a *penilní pletysmografii* („PPG“).[53] Při PPG vyšetření se u vyšetřované osoby za pomoci falometru (jinak také pletysmografu) měří prokrvení penisu či pochvy či jiné fyziologické odezvy při promítání obrázků sexuálně deviantní i nedeviantní povahy. Dle Procházky pak zpravidla znalec dospěje k jednomu ze tří typů forenzně sexuologických závěrů:

1. v případě, že se pachatel dopustil předmětné trestné činnosti, potom – s ohledem na další zjištěné odborně relevantní informace – je postižen poruchou sexuální preference;
2. pachatel je nepochybně postižen poruchou sexuální preference, bez ohledu na to, zda mu bude či nebude předmětné sexuálně motivované jednání prokázáno;
3. pachatel nepochybně není postižen poruchou sexuální preference, bez ohledu na to, zda mu bude či nebude předmětné sexuálně motivované jednání prokázáno.[54]

---

[51] PORADA, Viktor. *Op. cit.*, s. 720.
[52] ŠÁMAL, Pavel. § 116 [Vyšetření obviněného]. In: ŠÁMAL, Pavel. *Trestní řád: komentář. 7., dopl. a přeprac. vyd.* V Praze: C.H. Beck, 2013. Velké komentáře. s. 1648–1649.
[53] PROCHÁZKA, Ladislav. Poznámky z oboru soudní sexuologie. Česká a slovenská psychiatrie [online]. [cit. 2023-04-18]. Dostupné z: <http://www.cspsychiatr.cz/detail.php?stat=35>.
[54] PROCHÁZKA, Ladislav. Poznámky z oboru soudní sexuologie. Česká a slovenská psychiatrie [online]. [cit. 2023-04-18]. Dostupné z: <http://www.cspsychiatr.cz/detail.php?stat=35>.

Při zkoumání přítomnosti ovládacích schopností pachatele v době činu, resp. jejich případného zmenšení, bude sexuologické zkoumání zaměřeno zejména na:

1. intenzitu pohlavní aktivity a pohlavního pudu pachatele;
2. rozsah a sílu jeho psychických zábran;
3. schopnost adaptace na společensky přijatelné formy sexuálního chování.[55]

10. Zapojení veřejnosti do vyšetřování a prevence

Vzhledem k vysoce latentní povaze kybergroomingu je pro účinnou ochranu společnosti před tímto společensky škodlivým jevem zásadní nejen to, aby rodiče, školy i orgány veřejné moci včasně a správně reagovaly na již proběhlý útok, ale klíčová je především jejich snaha o účinnou prevenci. Drtivá většina rizikových komunikací mezi potenciálními pachateli a potenciálními oběťmi kybergroomingu totiž zůstane při sebevětší snaze jejich zraku ukryta. Cestou, jejímž prostřednictvím lze s tímto stavem bojovat, není dítěti internet zakazovat či jej v jeho užívání nepřiměřené míře omezovat. Realitou současného světa je – chtě nechtě – přesun lidské komunikace a činnosti do kyberprostoru, přičemž ze samotné podstaty společnosti musí nutně docházet k přesunu společenských jevů pozitivních i negativních. Z tohoto hlediska je pak naopak žádoucí dětem při jejich interakci s kyberprostorem poskytovat tolik svobody, kolik je přiměřené jejich věku a psychologické zralosti. Je pak zásadní současně s poskytnutím dostatečného prostoru učit děti kybernetické gramotnosti a obecné ostražitosti při jednání s cizími lidmi, a to tak, aby si dítě dokázalo vytyčit vlastní hranice a aby se naučilo v síti bezpečně pohybovat. Jak již bylo ostatně uvedeno, jedním z významných faktorů ovlivňujících kriminalistickou situaci je právě úroveň ostražitosti dětí pohybujících se v kyberprostoru a míra kybernetické gramotnosti v populaci.

V České republice se tématem prevence nejen kybergroomingu zabývá Centrum prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci v čele s Kamilem Kopeckým a René Szotkowskim. Toto vědecké pracoviště mimo jiné realizuje projekt *E-Bezpečí*, který se při své činnosti zaměřuje na prevenci, vzdělávání, výzkum, intervenci a osvětu spojenou rizikovým chováním na internetu a se souvisejícími fenomény.[56]

---

[55] PORADA, Viktor. *Op. cit.*, s. 656.

[56] Informace o projektu. E-Bezpečí [online]. [cit. 2023-04-03]. Dostupné z: <https://www.e-bezpeci.cz/index.php/o-projektu/oprojektu>.

11. Závěr

Ačkoliv je kybergrooming fenoménem moderním, svou historií nepřesahujícím časovou hranici 21. století, jedná se stále jen a pouze o jinou formu pradávného společensky škodlivého jevu, kterým je vylákání dítěte dospělou osobou na odlehlé místo mimo dohled jeho přirozených ochránců, a to za účelem realizace určitého způsobu sexuální interakce. Každý z nás v dětství slýchával varování rodičů o „zlých lidech“ nabízejících sladkosti, které vzápětí dítě zatáhnou do tmavé dodávky nebo do křoví. Internet je prostorem bezrozměrným a zároveň nekonečným, kde se pomyslné „křoví“ může skrývat v každém dětském pokojíčku či ve školní lavici. Onen „zlý člověk“ může být v podstatě kýmkoliv, domnělým vrstevníkem ze stejného města, dospělým kamarádem, který jako jediný chápe problémy dvanáctiletého dítěte, nebo kreslenou postavičkou z videohry. A onou „sladkostí“ mohou být v době bezhotovostních plateb a PayPalu klidně i peníze.

Při potírání kybergroomingu a jemu podobných jevů si je potřeba uvědomovat hranice možností orgánů činných v trestním řízení a jejich represivního přístupu k této problematice. Bohužel, drtivá většina groomingových aktivit vůči dětem na internetu zůstane neodhalena a většina pachatelů zůstane za své jednání nepotrestána. Klíčem přitom není pouze zdokonalování kriminalistických postupů a technického a personálního vybavení Policie České republiky. Zásadní je posílení přímé prevence cílené na děti a zvýšení jejich kybernetické gramotnosti. Dle průzkumu projektu E-Bezpečí 26,77 % dětských respondentů (7274 dětí z 27177) v průzkumu v roce 2019 uvedlo, že dostali od jiného uživatele či uživatelky internetu nabídku na setkání v reálném světě, přičemž tohoto uživatele znali pouze z internetu. Z pozvaných pak na schůzku dorazilo téměř 70 % dětí (5081 z 7274).[57] Ačkoliv z uvedené statistiky nevyplývá, že se ve všech případech jednalo o uživatele dospělého, natožpak že se jedná o případy kybergroomingu, alarmujícím zjištěním je již samotný fakt, jak vysoké procento dětí je ochotné se s člověkem známým pouze z kyberprostoru v reálném světě setkat.

Výše uvedenou hrozivou statistiku lze brát jako apel na to, aby byl boj proti kybergroomingu – krom jeho potírání cestou trestněprávní odpovědnosti a trestního stíhání – veden také na druhé frontě, a to odspoda, cestou lepší informovanosti veřejnosti o tomto jevu a o způsobech, jak mu předcházet a jak se mu účinně bránit.

---

[57] KOPECKÝ, Kamil, SZOTKOWSKI, René. *České děti v kybersvětě: Jak se chovají online a co jim hrozí?* [online]. O2 Czech Republic a Univerzita Palackého v Olomouci, Centrum prevence rizikové virtuální komunikace, 2019. [cit. 2023-04-03] Dostupné z: <https://www.e-bezpeci.cz/index.php. s. 26>.

Seznam literatury

Monografie

ČÍRTKOVÁ, Ludmila. *Forenzní psychologie. 3., upr. vyd.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2013. ISBN 978-80-7380-461-9.

GŘIVNA, Tomáš, RICHTER, Martin, ŠIMÁNOVÁ, Hana (eds.). *Vliv nových technologií na trestní právo.* Praha: Auditorium, 2022, s. 345-359. ISBN 978-80-87284-95-7.

CHMELÍK, Jan. *Rukověť kriminalistiky.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-36-9.

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

KONRÁD, Zdeněk, PORADA, Viktor, STRAUS, Jiří, SUCHÁNEK, Jaroslav. *Kriminalistika: kriminalistická taktika a metodiky vyšetřování. 2. rozšířené vydání.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2021. ISBN 978-80-7380-859-4.

MUSIL, Jan, KONRÁD, Zdeněk, SUCHÁNEK, Jaroslav. *Kriminalistika. 2., přepracované a doplněné vydání.* Praha: C. H. Beck, 2004. ISBN 80-7179-878-9.

PORADA, Viktor, STRAUS, Jiří. *Kriminalistické stopy: teorie, metodologie, praxe.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2012. ISBN 978-80-7380-396-4.

PORADA, Viktor. *Kriminalistika: technické, forenzní a kybernetické aspekty. 2. aktualizované a rozšířené vydání.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-741-2.

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

STRAUS, Jiří, PORADA, Viktor. *Teorie, metody a metodologie kriminalistiky.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2017. ISBN 978-80-7380-666-8.

ŠÁMAL, Pavel. *Trestní řád: komentář. 7., dopl. a přeprac. vyd.* V Praze: C.H. Beck, 2013. Velké komentáře. ISBN 978-80-7400-465-0.

Odborné články

COHEN, Lawrence E., FELSON, Marcus. Social Change and Crime Rate Trends: A Routine Activity Approach. American Sociological Review [online]. 1979, 44(4) [cit. 2023-04-15]. ISSN 00031224. Dostupné z: doi:10.2307/2094589.

KOLHE, Mahesh, AHIRAO, Purnima. Live Vs Dead Computer Forensic Image Acquisition. In: *International Journal of Computer Science and Information Technologies*. 2017, 8(3), 455-457. ISSN 0975-9646.

KRUPIČKA, Jiří. Kybergrooming – zrcadlo společnosti? In: GŘIVNA, Tomáš, RICHTER, Martin, ŠIMÁNOVÁ, Hana (eds.). *Vliv nových technologií na trestní právo*. Praha: Auditorium, 2022, s. 345-359. ISBN 978-80-87284-95-7.

PORADA, Viktor. Dokazování obsahu elektronických dokumentů. Košická bezpečnostná revue. Košice, 2012, 2012 (2), s. 104 - 108. ISSN 1338-6956.

Studie

KOPECKÝ, Kamil. *Rizikové formy chování českých a slovenských dětí v prostředí internetu*. Olomouc: Univerzita Palackého v Olomouci. 2015. ISBN 978-80-244-4868-8, DOI 10.5507/pdf.15.24448619.

VLACH, Jiří, KUDRLOVÁ, Kateřina, PALOUŠOVÁ Viktorie. *Kyberkriminalita v kriminologické perspektivě*. Praha: Institut pro kriminologii a sociální prevenci, 2020. Studie (Institut pro kriminologii a sociální prevenci). ISBN 978-80-7338-189-9.

Kvalifikační práce

AMIRIDU, Radka. *Zajištění integrity elektronického důkazu*. Brno, 2021. Diplomová práce. Masarykova Univerzita. Vedoucí práce JUDr. Mgr. Jakub Harašta, Ph.D.

KUDRLOVÁ, Kateřina. *Kriminalita spojená s využíváním nových médií dětmi*. Praha, 2019. Disertační práce. Katedra trestního práva. Právnická fakulta Univerzity Karlovy. Vedoucí práce doc. JUDr. Bc. Tomáš Gřivna, Ph.D.

Judikatura

Usnesení Nejvyššího soudu ze dne 25.11.2020 sp. zn. 8 Tdo 1041/2020.

Právní předpisy

Směrnice Evropského parlamentu a Rady 2011/93/EU ze dne 13. prosince 2011 o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii, kterou se nahrazuje rámcové rozhodnutí Rady 2004/68/SVV.

Zákon č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních, ve znění pozdějších předpisů.

Zákon č. 141/1961 Sb., zákon o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů.

Zákon č. 141/2014 Sb., kterým se mění zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, a zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, ve znění zákona č. 105/2013 Sb.

Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

Internetové zdroje

CyberTipline Reports [online]. NCMEC [cit. 2023-04-15]. Dostupné z: <https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata#reports>.

KOPECKÝ, Kamil, SZOTKOWSKI, René. *České děti v kybersvětě: Jak se chovají online a co jim hrozí?* [online]. O2 Czech Republic a Univerzita Palackého v Olomouci, Centrum prevence rizikové virtuální komunikace, 2019. [cit. 2023-04-03] Dostupné z: <https://www.e-bezpeci.cz/index.php>.

Muž měl zneužívat malou holčičku. Policie ČR [online]. [cit. 2023-04-15]. Dostupné z: <https://www.policie.cz/clanek/muz-mel-zneuzivat-malou-holcicku.aspx>.

Online grooming and UK law. Childnet International [online]. [cit. 2023-04-17]. Dostupné z: <https://www.childnet.com/wp-content/uploads/2014/08/online-grooming.pdf>.

PROCHÁZKA, Ladislav. *Poznámky z oboru soudní sexuologie. Česká a slovenská psychiatrie* [online]. [cit. 2023-04-18]. Dostupné z: <http://www.cspsychiatr.cz/detail.php?stat=35>.

Standard vybavení speciální výslechové místnosti pro dětského účastníka trestního řízení [online]. Policie ČR [cit. 2023-04-17]. Dostupné z: <https://www.mvcr.cz/clanek/standard-vybaveni-specialni-vyslechove-mistnosti-pro-detskeho-ucastnika-trestniho-rizeni.aspx>.