PhDr. Marek Hejduk, MBA
Policejní akademie České republiky v Praze
student doktorského studia

Kriminalistické aspekty odhalování, prověřování a vyšetřování počítačové mravnostní kriminality

Úvod do problematiky metodiky vyšetřování

Vyšetřováním trestných činů se zejména zabývá věda, která se nazývá kriminalistika. Kriminalistika je v užším slova smyslu vědou o odhalování, prověřování, vyšetřování a prevenci trestné činnosti. Jejím cílem je poznat zákonitosti vzniku, nalezení a využití informací o spáchaných trestných činech.[1] Metodikou vyšetřování rozumíme proces poznání kriminalisticky relevantních událostí.[2] Předmětem zkoumání metodiky vyšetřování jsou následující okruhy zákonitostí objektivního světa:

- ✓ Zákonitosti vyhledávání, zajišťování, shromažďování, zkoumání a využívání kriminalistických stop, jiných soudních důkazů a kriminalisticky významných informací v zájmu rychlého, úplného a objektivního odhalování, vyšetřování a prevence trestných činů.[3]

Objektem zkoumání metodiky vyšetřování jsou prvky vzniku a průběhu kriminalisticky relevantních událostí, jejich projevy ve stopách a prvky procesu poznávání jednotlivých typů kriminalisticky relevantních událostí ve vyšetřovací a soudní praxi.[4] Cílem zkoumání je vytvořit uspořádaný systém o typových charakteristikách trestných činů a vytvořit doporučení pro efektivní postup policejních orgánů.

Metodika vyšetřování má dvě základní funkce:

- ✓ Poznávací funkci, která spočívá v shromáždění veškerých informací o trestných činech do homogenních skupin. Dále tato funkce spočívá v klasifikaci typických stop, které vznikají při páchání trestné činnosti a typických vyšetřovacích situacích, které se utvářejí při vyšetřování dané skupiny trestných činů.
- ✓ Formativní funkci, která vytváří typové modely činností policejních orgánů při procesu poznání určité skupiny trestných činů. Jde o systémy metod a operací, které představují tzv. typové modely.

Metodika vyšetřování jednotlivých druhů trestných činů se vyznačuje svojí pevně stanovenou strukturou. Struktura metodik vyšetřování jednotlivých druhů trestných činů se skládají z následujících částí:

---

[1] MUSIL, Jan; KONRÁD, Zdeněk a Jaroslav SUCHÁNEK. *Kriminalistika. 2., přepracované a doplněné vydání*. Praha: C. H. Beck, 2004. Beckovy mezioborové učebnice, s. 4.

[2] Kriminalisticky relevantní událost – trestný čin, přestupek, náhlá úmrtí, nešťastné náhody, působení přírodních sil – zkoumají se z hlediska kriminalistiky jen do té doby, než se prokáže, že se nejedná o trestný čin či přestupek.

[3] NĚMEC, Miroslav et al. *Teorie a metodologie kriminalistiky pro magisterské studium* – I. díl. Aktuální problémy kriminalistické praxe. Praha: Abook s. r. o. 2018, s. 52.

[4] Tamtéž.

- ✓ typová kriminalistická charakteristika dané skupiny trestných činů;
- ✓ stopy typické pro daný typ trestných činů;
- ✓ zvláštnosti předmětu vyšetřování;
- ✓ typické podněty k vyšetřování a jejich zvláštnosti;
- ✓ typické vyšetřovací situace vyskytující se při vyšetřování daného typu trestných činů;
- ✓ typické počáteční úkony a jejich zvláštnosti;
- ✓ typové vyšetřovací verze a zvláštnosti vytyčování vyšetřovacích verzí, plánování a organizace vyšetřování;
- ✓ zvláštnosti a následné etapy vyšetřování;
- ✓ zvláštnosti zapojení veřejnosti do vyšetřování a prevence.

Typová kriminalistická charakteristika

Pro současnou dobu 21. století je typický velký rozvoj informačních a komunikačních technologií. Dnes si již de facto nedokážeme představit celou řadu lidských činností bez využití internetových technologií a internetu. Tím, že se jednotlivé internetové technologie neustále rozvíjejí, dochází však i k zneužívání těchto prostředků k páchání trestné činnosti.

Doc. Požár uvádí: *„Počítače v podstatě neumožňují páchat novou neetickou a trestnou činnost, poskytují jen novou technologii a nové způsoby na páchání již známých trestných činů“.*[1]

S tímto konstatováním lze zajisté souhlasit, nicméně na druhou stranu současná doba přináší nová kriminální jednání, která donedávna nebyla trestně právně upravena jako trestný čin a často se taková jednání podřazovala pod obecnější skutky. Konkrétně jde o např. tzv. kybergrooming.

Doc. Němec definuje počítačovou (kybernetickou) kriminalitu jako „*taková kriminální jednání, při kterých jsou prostředky informačních a komunikačních technologií:*

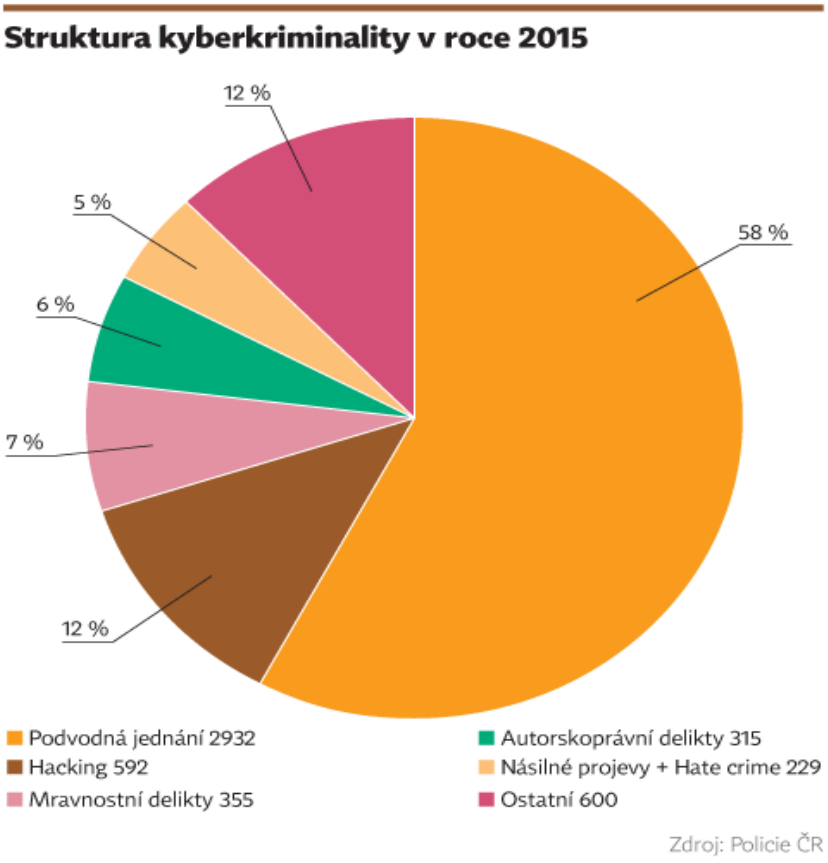
- ✓ *užity jako nástroj pro spáchání trestného činu,*
- ✓ *cílem útoku pachatele, přičemž tento útok je trestným činem, za podmínky, že jsou tyto prostředky užity či zneužity v informačním, systémovém, programovém či komunikačním prostředí (tedy v kyberprostoru)*“.[2]

Počítačová mravnostní kriminalita je jedním z druhů kyberkriminality.[3] Jde o kombinaci mravnostní kriminality s kyberkriminalitou. Jinými slovy jde o mravnostní kriminalitu, která je uskutečňována prostřednictvím IT prostředků. Předmětem útoku u počítačové mravnostní kriminality je právě mravnost s tím, že samotná trestná činnost je páchána za výrazného využití informačních a komunikačních technologií jakožto významného prostředku k jejímu páchání. Mravnostní trestné činy v kyber-prostoru zaujímají zhruba 7 % z celkového počtu kyberkriminality (viz struktura

[1] POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Aleš Čeněk, 2005, s. 249.
[2] NĚMEC, Miroslav et. al. *Teorie a metodologie kriminalistiky pro magisterské studium – II. díl*. Aktuální problémy kriminalistické praxe. Praha: Abook s. r. o. 2019, s. 305-306.
[3] Kyberkriminalita – trestná činnost, která je páchána v prostředí informačních a komunikačních technologií včetně počítačových sítí.

kyberkriminality za rok 2015).[1] Je však třeba podotknout, že mravnostní delikty v kyberprostoru jsou trestnou činností poměrně latentní, tudíž skutečná čísla mohou být v reálu značně jiná.

Počítačová mravnostní kriminalita představuje trestnou činnost, ve které jsou internetové technologie používány jako nástroj páchání trestného činu, případně kde se trestná činnost odehrává, tj. v IT prostředí, zpravidla ve virtuálním (online) prostředí – prostředí internetu. Tím, že jde o relativně nový fenomén v páchání trestné činnosti, je třeba, aby policie byla na samotné vyšetřování počítačové mravnostní kriminality dostatečně vybavena materiálně, ale rovněž i personálně, jelikož jde o oblast velmi odbornou a náročnou na odhalování. V rámci SKPV[2] by měly existovat specializované týmy, které se budou touto trestnou činností zabývat. Jedním z podkladů, které by měly tyto týmy využívat, by měla být též metodika vyšetřování této trestné činnosti.



Obrázek č. 1 – Struktura kyberkriminality za rok 2016 (zdroj: Jednotlivé druhy kyberkriminality. Policie ČR [online]. 2020 [cit. 2020-10-06]. Dostupné z: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx).

Klasifikace počítačové mravnostní kriminality

Počítačovou mravnostní kriminalitu můžeme klasifikovat dle trestně právního pojetí, tj. dle trestního zákona nebo dle kriminologického pojetí, které nabízí širší

[1] Jednotlivé druhy kyberkriminality. Policie ČR [online]. 2020 [cit. 2020-10-06]. Dostupné z: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx
[2] SKPV – Služba kriminální policie a vyšetřování.

souvislosti anebo v kombinaci. Pro účely této práce jsem zvolil klasifikaci dle kriminologického pojetí i trestně právního, tj. v kombinaci obou přístupů.

Kybergrooming

Kybergrooming je novým fenoménem páchání trestné činnosti v kyberprostoru. Termín grooming označuje specifické jednání, které spočívá v psychické manipulaci kybergroomerů,[1] která má za cíl v oběti vyvolat falešnou, zdánlivou důvěru a přimět ji k osobní schůzce, přičemž důsledkem takového chování může být zejména některý ze sexuálních trestných činů.[2]

Kybergrooming představuje psychickou manipulaci realizovanou prostřednictvím internetu, mobilního telefonu a sociálních sítí (internetové seznamky, Facebook, Twitter, atd.). Zahrnuje jednání manipulátora (kybergroomera), které má v oběti – dítěti vyvolat falešnou důvěru a přimět jej k určité aktivitě – osobní schůzce, focení, natáčení sebe sama. Cílem může být zneužití dítěte pro výrobu dětské pornografie. Typicky je vázán na chaty, messengery, internetové seznamky, sociální sítě, ale také třeba na různé internetové stránky s nabídkou modelingu, herní portály, apod.[3] Kybergroomer se snaží o osobní kontakt. Dítě „uplácí" dárky (např. dobití kreditu na mobilním telefonu), vydírá jej pořízenými snímky, pokračuje a zintenzivňuje manipulaci, která může vést i k osobnímu útoku na oběť. Jednou z forem kybergroomingu je i eroticky laděná komunikace a získání amatérských pornografických materiálů. Zásadním problémem u kybergroomingu je jeho zjišťování a dokazování a rovněž zejména anonymita, využití zabezpečených systémů a také skutečnost, že v počátečním stádiu ještě nejde zpravidla o trestný čin, zejména tam, kde není trestná forma přípravy.[4]

Trestně právní vymezení kybergroomingu

Kybergrooming je pojmem kriminologickým, nikoli trestně právním. Nicméně jednání představující kybergrooming můžeme podřadit pod skutkovou podstatu § 193b trestního zákona, která zní:

Navazování nedovolených kontaktů s dítětem.

„Kdo navrhne setkání dítěti mladšímu patnácti let v úmyslu spáchat trestný čin podle § 187 odst. 1, § 192, 193, § 202 odst. 2 nebo jiný sexuálně motivovaný trestný čin, bude potrestán odnětím svobody až na dvě léta."[5]

V tomto ohledu byla významná novela číslo 141/2014 Sb., která právě do trestního zákoníku zakomponovala tuto novou skutkovou podstatu trestného činu. Novela vstoupila v platnost 22. 7. 2014 a účinnou se stala 1. 8. 2014. Jde o odkazující skutkovou podstatu, která ve svém ustanovení odkazuje na trestné činy pohlavní zneužití, výroba a jiné nakládání s dětskou pornografií, zneužití dítěte k výrobě

[1] Kybergroomer je zpravidla sexuální útočník, který k prosazení svého cíle využívá IT prostředí.
[2] VÁLKOVÁ, Helena; KUCHTA, Josef a Jana HULMÁKOVÁ. *Základy kriminologie a trestní politiky.* 3. vydání. Praha: C. H. Beck, 2019, Beckovy mezioborové učebnice, s. 537.
[3] BERSON, I. H. Grooming Cybervictims: The Psychosocial Effects ofOnline Exploitation for Youth. University of South Florida. USA. (online) cit. 6. 10. 2020. dostupné zhttp://www.cs.auckland.ac.nz/~john/NetSafe/I.Berson.pdf
[4] VÁLKOVÁ, Helena; KUCHTA, Josef a Jana HULMÁKOVÁ. *Základy kriminologie a trestní politiky.* 3. vydání. Praha: C. H. Beck, 2019, Beckovy mezioborové učebnice, s. 537.
[5] § 193b zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

pornografie, svádění k pohlavnímu styku. V předchozí právní úpravě, tj. té před výše zmíněnou novelou, bylo možné postihnout kybergrooming pouze v souvislosti s výrobou dětské pornografie a zasíláním pornografie dítěti, popřípadě jako ohrožování výchovy dítěte v důsledku sexuální komunikace přes IT prostředky a svádění k pohlavnímu styku. Samotné jednání spočívající v usilování o setkání bylo trestně postižitelné pouze jako příprava znásilnění, což v praxi bylo velmi složité z hlediska dokazování – úmyslu pachatele). Nová úprava § 193b však míří rovnou na předstupeň onoho setkání, tedy už na jeho návrh, byť i zde musí být prokázán úmysl pachatele dítě nějakou formou sexuálně využít.

Rozbor skutkové podstaty trestného činu dle § 193b. Objektem trestného činu je ochrana dětí mladších 15 let před tzv. sexuálním vykořisťováním. Objektivní stránka spočívá v jednání pachatele, který navrhne setkání dítěti mladšímu 15 let v úmyslu spáchat některý z trestných činů, na který § 193b ve svém ustanovení odkazuje. Návrhem setkání rozumíme aktivní činnost směřující k dítěti mladšímu 15 let ve snaze vněm vzbudit rozhodnutí zúčastnit se osobní schůzky za účelem spáchání některého výše uvedeného trestného činu, uvedeným pod § 193b či jiného sexuálně motivovaného trestného činu. V praxi jde o navázání kontaktu prostřednictvím internetových technologií. Pachatelem může být kterákoli fyzická osoba, ale i právnická osoba. Z hlediska subjektivní stránky se vyžaduje zavinění ve formě úmyslu, přičemž je obligatorní sexuální motiv pro spáchání trestného činu.[1]

Statistika kriminality Policie České republiky je postavena na sledování druhů trestné činnosti podle „takticko-statistických klasifikací“ (dále jen „TSK“), nikoliv podle jednotlivých paragrafů. Trestný čin dle § 193b navazování nedovolených kontaktů s dítětem je zahrnut společně s dalšími skutkovými podstatami (§ 190, 192 -194) v TSK 290 – „ostatní mravnostní trestné činy“. Policejní statistika bohužel konkrétní statistikou, zabývající se § 193b, nedisponuje.

Dětská pornografie

Dětská pornografie může být definována několika způsoby, avšak legální definici postrádá. Např. Chmelík definoval dětskou pornografii následovně: *„zobrazení dětských pohlavních orgánů, pohlavního nebo jiného sexuálního styku s dítětem nebo mezi dětmi“*.[2] Jinými slovy jde vždy o jistou formu znázornění (např. foto či videozáznam) sexuálních motivů či aktivit, ve kterém je zobrazeno dítě jako aktér, tj. objekt. Dítětem se rozumí osoba mladší 18 let, pokud trestní zákon nestanoví jinak.[3] Veškeré takové aktivity směřují k vyvolání pohlavního vzrušení.

Širší definici dětské pornografie nabízí Blatníková: „*znázornění dítěte účastnícího se skutečné nebo předstírané explicitní sexuální aktivity, ať už je toto zobrazení provedeno jakýmkoliv způsobem, a rovněž tak jakékoliv vyobrazení sexuálních orgánů dítěte určené primárně k sexuálním účelům, je považováno za dětskou pornografii. Jde tedy o pornografický materiál (zvukový nebo obrazový), který zobrazuje dítě, které se aktivně nebo pasivně účastní jednoznačně sexuálního jednání, a to včetně dráždivého vystavování přirození, nebo skutečnou osobu se vzhledem dítěte, která se aktivně nebo pasivně účastní sexuálního kriminálního jednání, nebo realistické*

[1] ŠÁMAL, Pavel. *Trestní právo hmotné.* 7., přeprac. vyd. Praha: Wolters Kluwer, 2014, s. 627.
[2] CHMELÍK, Jan a kol. *Mravnost, pornografie a mravnostní kriminalita.* 1. vyd. Praha: Portál, s.r.o., 2003, s. 216.
[3] § 126 zákona č. 40/2009 Sb., trestní zákon, ve znění pozdějších předpisů.

znázornění neexistujícího dítěte, které se aktivně nebo pasivně účastní výše popsaného kriminálního jednání.“[1]

V českém právním řádu není nijak pojem dětská pornografie definován, na rozdíl od např. slovenského trestního zákona. V praxi se tedy může jednat například o snímky obnažených dětí zachycující polohy skutečného či předstíraného sexuálního styku nebo snímky obnažených dětí v polohách vyzývavě předvádějících pohlavní orgány. Trestní zákoník upravuje postih spojený s dětskou pornografií v paragrafech 191 – 193. V prvé řadě popisuje šíření pornografie, dále výrobu a jiné nakládání s dětskou pornografií, zneužití dítěte k výrobě pornografie a účast na pornografickém představení.

Dále v praxi však existují 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.[2]

Sexting

Sexting je rovněž relativně novým fenoménem, který můžeme definovat jako rizikové sdílení a šíření materiálů sexuální povahy s použitím internetu či mobilních telefonů. Samotné slovo sexting je odvozeno od spojení slov sex a textování a znamená posílání textového, fotografického, audio a video obsahu se sexuálním podtextem prostřednictvím internetových technologií.[3]

Pokud je následně obsah se sexuální tématikou zneužit, zpravidla při ukončení vztahu mezi dospělými lidmi, může být takový materiál zneužit k poškození druhé strany a to výhružkou zveřejněním. Pachatel v některých případech může pod pohrůžkou zveřejnění takovéhoto materiálu požadovat zaslání dalších fotografií či videa a psychickým nátlakem tak nutí poškozeného k výrobě a pořizování dalších materiálů, které pachatel vyžaduje buď pro vlastní potřebu, nebo se záměrem je sdílet na Internetu.[4] Takové jednání bychom pravděpodobně podřadili pod skutkovou podstatu vydírání dle trestního zákona.

Sexting však může zasahovat i do života dětí, kdy takové jednání bychom mohli podřadit pod § 192 a § 193, tj. pod problematiku dětské pornografie.[5] Právě mezi dětmi a mladistvými je sexting velmi oblíbenou činností. V praxi se setkáváme se situacemi,

[1] BLATNÍKOVÁ, Šárka. Pachatelé komerčního sexuálního zneužívání dětí v ČR – informace z výzkumu. *Trestněprávní revue*. 2010, roč. 9, č. 11, s. 355-362.
[2] Počítačová mravnostní kriminalita. *Policie* [online]. Praha, 2020 [cit. 2020-11-11]. Dostupné z: https://www.policie.cz/clanek/pocitacova-mravnostni-kriminalita.aspx
[3] KOHOUT, Roman a Radek KARCHŇÁK. *Bezpečnost v online prostředí*. Karlovy Vary: Biblio Karlovy Vary, 2016.
[4] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. s. 315.
[5] Zákon č. 40/2009 Sb., trestní zákon, ve znění pozdějších předpisů.

kdy děti posílají svojí nahou fotografii pomocí internetu zcela neznámým osobám, což následně může být sdíleno dále.[1]

Mezi hlavní rizika sextingu patří:

- ✓ potencionální útočník obdrží citlivý materiál, který může v budoucnu zneužít;
- ✓ v případě zveřejnění citlivého materiálu na internetu je prakticky nemožné tento materiál „smazat" – může být zneužit i po velice dlouhé době od zveřejnění;
- ✓ trestní odpovědnost za šíření sextingu;
- ✓ sexting se často stává prostředkem pro vydírání dětí v rámci tzv. kybergroomingu.[2]

Stopy typické pro daný typ trestných činů

Stopy typické pro počítačovou mravnostní kriminalitu můžeme rozdělit do dvou skupin a to na stopy digitální a stopy materiální (v případech, kdy dojde k fyzickému zneužití oběti). Pokud dojde k sexuálnímu zneužití, mnohdy jsou zanechány na těle oběti zřetelné stopy, které lze spolehlivě dokumentovat prohlídkou těla a vyšetřením lékařem, pokud je trestný čin oznámen bezprostředně po jeho spáchání.

Vedle materiálních stop jsou u počítačové mravnostní kriminality stěžejní stopy digitální. Digitální stopu můžeme vymezit následovně:

„Digitální stopa je jakákoliv informace s vypovídající hodnotou, uložená nebo přenášená v digitální podobě."[3]

Profesor Smejkal uvádí k digitálním stopám následující poznatek:

„*Stále častěji se součástí důkazního materiálu, a to nejen v oblasti počítačové kriminality nebo kriminality informační, ale v podstatě u většiny dalších trestných činů, zejména v oblasti hospodářské, trestných činů proti majetku a trestných činů proti pořádku ve věcech veřejných, stávají rovněž digitální stopy*."[4]

Profesor Straus definuje digitální (počítačovou) stopu v širším kontextu:

„*Počítačovou stopu lze charakterizovat jako změnu na nosiči informací, vzniklou v souvislosti s trestným činem, při jehož páchání byla použita výpočetní technika a která je zjistitelná za pomoci současných metod, prostředků a operací. Tyto stopy se nacházejí na pevném disku, vyměnitelných paměťových médiích, CD ROM, disketách atp*."[5]

Digitální (počítačová) stopa se vyznačuje oproti klasickým stopám specifickými rysy, neboť je zpravidla značně objemná (co se velikosti dat týče), dynamická a může být rozmístěna kdekoli v kyberprostoru. Životnost takovéto stopy může být velmi krátká

[1] Sexting.cz – vše, co chcete vědět o sextingu [online]. [cit. 11. 11. 2020]. Dostupné z: www.sexting.cz
[2] Sexting. *Internetem bezpečně* [online]. 2018 [cit. 2020-11-11]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/sexting/
[3] WHITCOMB, C. M. An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, Spring 2002 Volume 1, Issue 1.
[4] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015, s. 492.
[5] STRAUS, Jiří a kol. *Kriminalistická metodika*. Plzeň: Aleš Čeněk, 2006, s. 275.

a jakékoli průtahy jak v postupu před zahájením trestního stíhání, tak ve vyšetřování nutně vedou k její ztrátě.[1]

Mezi nejvýznamnější odlišnosti digitálních důkazů oproti stopám jiným (např. materiálním) patří zejména:

- ✓ nestálost;
- ✓ dostupnost (dosažitelnost);
- ✓ proces zajištění;
- ✓ reprodukovatelnost.[2]

Mezi další specifika digitálních stop řadíme:

- ✓ nehmotnost digitálních stop,
- ✓ latentnost digitálních stop,
- ✓ manipulovatelnost s časem v počítačových systémech,
- ✓ způsob uchování záznamů,
- ✓ dynamika činnosti počítačových systémů,
- ✓ komplexnost prostředí,
- ✓ vysoký stupeň interní a externí interakce probíhajících procesů,
- ✓ velký geografický rozsah prostoru s digitálními stopami.[3]

Z hlediska trestního práva procesního je digitální stopa subsumována pod věcný či listinný důkaz.

Typické vyšetřovací situace vyskytující se při vyšetřování daného typu trestných činů

Kriminální situace je tvořena podmínkami a okolnostmi, které umožňují páchání počítačové mravnostní kriminality. Tyto podmínky a okolnosti určují způsoby páchání této trestné činnosti a dále zákonitosti vzniku a zániku stop.

Jde o následující podmínky a okolnosti:

- ✓ úroveň právního systému – právní systém nám stanoví, jaké jednání je zákonné a jaké už nezákonné (trestné). V oblasti kyberkriminality obecně lze konstatovat, že leckdy nové metody pachatelů, které jsou používány prostřednictvím internetových technologií, pro páchání trestné činnosti, působí rychleji, než příslušná zákonná úprava daného protiprávního jednání. Jinými slovy trestná činnost v IT prostředí je zpravidla o krok napřed, než zákonná úprava. Proto je zcela zásadní, aby příslušné státní orgány (zákonodárce, nestátní organizace, atd.) včas reagovaly na proměnlivost páchání trestné činnosti v kyberprostoru a příslušné protiprávní jednání pojmenovaly a popsaly v daném právním předpise, aby mohlo dojít k postihu takového jednání a tím k ochraně společnosti. Jednotlivé nové druhy počítačové mravnostní kriminality jsou toho příkladem – např. kybergrooming, sexting, kybersex, atd.

[1] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. s. 403.
[2] Tamtéž.
[3] PORADA, Viktor a Eduard BRUNA. Digitální svět a dokazování obsahu elektronických dokumentů. Bezpečnostní technologie, systémy a management. [online]. [cit. 2. 12. 2020], s. 3. Dostupné z: http://trilobit.fai.utb.cz/Data/Articles/PDF/37bacb88-3602-4ea7-b9c8-7864970f89e7.pdf

- ✓ technická ochrana počítačových systémů – technická ochrana počítačových systémů a počítačů obecně (hardwaru) je rovněž velmi důležitou oblastí. U počítačové mravnostní kriminality je žádoucí, aby ze strany uživatelů (rodičů) byla nastavena technická ochrana na IT prostředcích, které např. neumožní vstup uživateli – dítěti, vstup na určité internetové stránky či blokaci nevhodného obsahu (např. obsahu se sexuální tématikou). Rovněž poskytovatelé či provozovatelé webových serverů či stránek mají v tomto ohledu klíčovou roli. Oni mohou totiž ovlivňovat obsah svých webových stránek, mohou nastavovat pravidla jednotlivých skupin, nastavovat oprávnění, podávat případně podněty na policii, pokud dochází k naplňování trestné činnosti, atd. Např. dlouholetý seznamovací portál lidé.cz skončil svoji činnost k 14. 12. 2020. Jedním z hlavních důvodů pro ukončení této stránky byla právě skutečnost, že zde působila celá řada sexuálních predátorů, kybergroomerů, atd.
- ✓ úroveň rizikového chování dětí na internetu – internet představuje nejen užitečný nástroj informací, ale též riziko. Převážně děti by měly být již od mala seznamovány s jednotlivými rizikovými faktory, které online svět přináší. Zásadní roli zde hraje výchova v rodině, vzdělání o IT gramotnosti na školách, pořádání osvětové činnosti v rámci škol, atd.
- ✓ úroveň rozvoje internetových technologií – rozvoj internetových technologií musí jít ruku v ruce s právními normami. V současné IT společnosti jsme svědky velmi rychlého rozvoje technologií, což vede k páchání nových forem trestné činnosti. Pachatelé využívají nové prostředky a metody k páchání. U počítačové mravnostní kriminality hovoříme o např. používání webkamer, instalaci sledovacích programů, používání online přenosů, atd.
- ✓ úroveň odborné připravenosti a technického vybavení OČTŘ[1] – abychom mohli s počítačovou mravnostní kriminalitou bojovat, musí být příslušné orgány na to patřičně vybaveny a to nejenom odborně z hlediska znalostí a zkušeností, ale též technicky. V roce 2016 vznikl útvar NCOZ[2], který problematiku počítačové mravnostní kriminality ve své gesci měl a odborně se tomu věnoval. Bohužel v současné době se již touto problematikou nezabývá a nyní je tato oblast v gesci ÚSKPV.[3]
- ✓ specifika prostředí, ve kterém je tato trestná činnost páchána – počítačová mravnostní kriminalita je typicky páchána ze své podstaty ve virtuálním, online prostředí, které nabízí vysokou formu anonymity. Jde o prostředí, ve kterém se složitěji získávají důkazy a další podklady pro trestní řízení.
- ✓ specifické postavení oběti – u počítačové mravnostní kriminality jde převážně o oběti z řad dětí. Děti tvoří skupinu zvlášť zranitelných obětí a proto je potřeba této skupině věnovat maximální pozornost a klást důraz na prevenci.
- ✓ specifické postavení pachatele, kyberútočníka – zpravidla jde o pachatele, kteří jsou výborní manipulátoři, znají a umějí uplatňovat techniky komunikace a následně techniky nátlaku na oběti.[4]

[1] OČTŘ – Orgány činné v trestním řízení.
[2] NCOZ – Národní centrála pro boj s organizovaným zločinem, která vznikla jako důsledek reorganizace ÚOOZ a ÚOKFK.
[3] ÚSKPV – Úřad služby kriminální policie a vyšetřování.
[4] NĚMEC, Miroslav et. al. *Teorie a metodologie kriminalistiky pro magisterské studium – II. díl. Aktuální problémy kriminalistické praxe.* Praha: Abook s. r. o. 2019, s. 305-306.

Zvláštnosti předmětu vyšetřování

Předmět dokazování je obecně vymezen v trestním řádu, nicméně pro každý druh kriminality je specifický.[1] Počítačová mravnostní kriminalita má dvě roviny, na rozdíl od kyberkriminality obecně. Je páchána nejenom v online prostředí, ale u některých forem též v prostředí reálném.

Níže je uveden příkladný výčet toho, co je u počítačové mravnostní kriminality potřeba zjišťovat:

- ✓ zda jde o jeden či více skutků, tj. problematika konkurence trestných činů,
- ✓ informace o metodách útoku – zaznamenání aktivit mezi kyberútočníkem a obětí; struktura a délka útoků – např. v navazování kontaktů; časové úseky mezi jednotlivými navozenými kontakty při komunikaci s obětí; přesun z online prostředí do reálného prostředí vylákáním na schůzku,
- ✓ informace o počítačovém systému – jaký počítač je koncovým přípojným bodem; prostřednictvím kterého počítačového systému došlo k protiprávnímu jednání; jakým způsobem byl počítačový systém připojen do sítě, atd.,
- ✓ informace o datech – jakou povahu mají napadená (vylákaná) data z oběti – např. se sexuálním motivem; dále co přesně je obsahem paměťových médií – uložená komunikace mezi pachatelem a obětí, fotografie, screeny obrazovek, atd.; originálnost uložených informací – zda došlo k pozměnění či manipulaci s daty a informacemi,
- ✓ informace o pachateli – jakým způsobem a jakými prostředky dochází ze strany pachatele k protiprávnímu jednání; jaký je rozsah znalostí pachatele o IT prostředcích, které používá při navozování kontaktů s obětí; motiv pachatele (např. vylákání oběti na schůzku a její sexuální zneužití),
- ✓ okolnosti, které umožnily spáchání trestného činu – otázka dostupných prostředků užitých ke spáchání trestného činu – IT prostředky, atd.[2]

Typické podněty k vyšetřování a jejich zvláštnosti

Specifickou zvláštností počítačové mravnostní kriminality je samotná skutečnost, že se její páchání odehrává v kyberprostoru a že oběti jsou zpravidla děti, které ještě nejsou natolik rozumově a mravně vyspělé, aby rozpoznaly nebezpečnost protiprávního jednání.

Tím, že typickými stopami jsou stopy digitální, může je pachatel ve velmi rychlé době ovlivňovat či ničit.

Podněty k vyšetřování u počítačové mravnostní kriminality můžeme zahrnout do tří následujících skupin:

- ✓ vlastní operativně pátrací činnost orgánů činných v trestním řízení s tím, že podněty od útvarů SKPV mívají největší informační hodnotu.[3] Mravnostním trestným činům v kyberprostoru se dříve věnoval též celostátní útvar Národní centrály pro boj s organizovaným zločinem (NCOZ), který však v současné době

[1] § 89 odst. 1 zákona č. 141/1961 Sb., trestní řád, ve znění pozdějších předpisů.
[2] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. s. 406-407.
[3] PORADA, Viktor a Jiří STRAUS. *Kriminalistika: (výzkum, pokroky, perspektivy).* 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2013, s. 528-529.

se touto problematikou již nezabývá. Tato problematika je v gesci Úřadu služby kriminální policie a vyšetřování Policejního prezidia ČR (ÚSKPV).[1]

- ✓ Oznámení fyzických či právnických osob. Jak již bylo výše uvedeno, obětí počítačové mravnostní kriminality bývá zpravidla dítě, je velmi složité zajistit či opatřit podnět k vyšetřování u samotné oběti. V praxi zpravidla jde o podněty podané blízkými osobami ve vztahu k dítěti. Může jít např. o rodiče, širší rodinu dítěte či učitele/pedagogy ve školách, atd.
- ✓ Oznámení organizací, které se počítačové mravnostní kriminalitě věnují. Zde má nezastupitelnou roli celá řada subjektů, které mohou být hlavním činitelem při podání podnětu k vyšetřování. V praxi jde např. o organizace, které se věnují obětem trestných činů (Bílý kruh bezpečí, Linka bezpečí, atd.). Dále jde o jednotlivé subjekty neziskových organizací, které se věnují preventivním aktivitám v oblasti kybergroomingu, sextingu, atd. Konkrétně jde např. o neziskovou organizaci you connected, z.s., která realizuje projekt Internetem bezpečně[2] či aktivity portálu E-Bezpečí, který provozuje Centrum prevence rizikové virtuální komunikace (Pedagogická fakulta Univerzity Palackého v Olomouci),[3] které disponuje svojí online poradnou.

Typické počáteční úkony a jejich zvláštnosti

Typickým počátečním úkonem v oblasti počítačové mravnostní kriminality je, tak jako v celé řadě jiných trestných činů, trestní oznámení. Každé trestní řízení začíná na základě sepsání záznamu o zahájení úkon trestního řízení či provedením neodkladných či neopakovatelných úkonů, které mu bezprostředně předcházejí.[4]

V počáteční fázi je velmi klíčové precizní zpracování přijatého oznámení a zajištění prvotních důkazů a informací. Jelikož jde o velmi citlivou problematiku (s mravnostním či sexuálním podtextem), je velmi důležité k tomu přistupovat profesionálním způsobem, aby nedošlo např. ke způsobení sekundární újmy u oběti, pokud je oznamovatelem - např. nevhodně zvoleným postupem OČTŘ.[5] Pokud to okolnosti dovolí, je vhodné od oznamovatele zajistit data v co nejméně změněné podobě, tj. aby šlo o originály (např. e-mailových zpráv, uložených datech na externích úložištích, komunikace na sítích v tzv. chatech, atd.). Pokud to technicky či z jiného důvodu není možné, je třeba zajistit alespoň kopie těchto dat prostřednictvím tzv. printscreenů, fotografiemi obrazovek PC, atd.[6]

Dalším významným zdrojem informací je propojení počítačového systému do sítě a přidělení tzv. IP adresy.[7] Abychom mohli identifikovat počítačový systém a následně i kyberútočníka, je nutné znát nejenom IP adresu, ale též datum a přesný čas připojení počítačového systému do počítačové sítě. IP je jedinečným, unikátním identifikátorem,

[1] Blíže: https://www.policie.cz/clanek/narodni-centrala-proti-organizovanemu-zlocinu-skpv.aspx
[2] Blíže: https://www.internetembezpecne.cz/
[3] Blíže: https://www.e-bezpeci.cz/index.php/71-trivium/1421-co-je-kybergrooming#
[4] § 158 odst. 3 zákona č. 141/1961 Sb., trestní řád, ve znění pozdějších předpisů.
[5] GŘIVNA, Tomáš; SCHEINOST, Miroslav a Ivana ZOUBKOVÁ. *Kriminologie.* 5. aktualizované vydání. Praha: Wolters Kluwer, 2019, s. 125-127.
[6] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. s. 411.
[7] IP (identity protokol) adresa je v IT prostředí číslo, které jednoznačně identifikuje síťové rozhraní v počítačové síti, která používá IP protokol.

který slouží následně k identifikaci pachatele. Jde tedy o velmi významný zdroj v rámci trestního řízení, s kterým následně OČTŘ pracují. Dílčí informace může OČTŘ získat od jednotlivých poskytovatelů internetového připojení (ISP – Internet Service Provider). Tito poskytovatelé uchovávají informace o počítačových systémech, včetně IP adresy, času a délce používání dané služby, atd.[1]

Od počátku přijatého oznámení je rovněž důležité, aby případy počítačové mravnostní kriminality byly řešeny dle místní příslušnosti, tj. zpravidla tam, kde vyšel najevo.[2] U počítačové mravnostní kriminality je v neposlední řadě velmi důležitá součinnost s dalšími státními orgány, právnickými a fyzickými osobami. Forma dožádání tak podstatně urychluje proces trestního řízení. Poskytovatelé internetových služeb zpravidla poskytují v rámci dožádání informace týkající se IP adresy, emailu, webové stránky, chatu.

Pro samotný průběh trestního řízení je klíčové zajištění nejenom počítačového systému, který byl k trestné činnosti použit, ale pochopitelně i určení uživatele – pachatele. Současně však musí být zachována zásada zákonných důvodů: *„Podmínkou trestního stíhání je, že prověřováním podle § 158 zjištěné a odůvodněné skutečnosti nasvědčují tomu, že byl spáchán trestný čin, a je-li dostatečně odůvodněn závěr, že jej spáchala určitá osoba, jestliže jsou splněny i další zákonné podmínky.“*[3]

Tzn. cílem je za pomocí zajišťovacích úkonů dojít k identifikaci osoby, která kyberútoky vede a k jeho zajištění. Pokud by v průběhu trestního řízení nedošlo ke zjištění konkrétní osoby, přicházelo by v úvahu odložení věci, pokud by následně nevyšly najevo nové skutečnosti, které by svědčily o tom, že daná osoba spáchala trestný čin, bylo by možné v řízení pokračovat.[4]

K zajišťovacím úkonům v rámci počítačové mravnostní kriminality řadíme:

Konrád uvádí, že počátečními úkony při vyšetřování počítačové kriminality jsou zejména:

1) ohledání místa činu,
2) domovní prohlídka a prohlídka jiných prostor,
3) zajišťovací úkony pro počítačovou expertizu a vyhledávání počítačových stop a důkazů.[5]

K těmto základním úkonům by pak bylo možné dále u počítačové mravnostní kriminality přiřadit následující:

4) vydání a odnětí věci,
5) odposlech a záznam telekomunikačního provozu,
6) operativně pátrací prostředky.

Ohledání místa činu, domovní prohlídky a prohlídky jiných prostor se odehrávají především v místě podezřelé osoby, přičemž se úkony zaměřují na veškerá dostupná

[1] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. s. 411.
[2] § 18 zákona č. 141/1961 Sb., trestní řád, ve znění pozdějších předpisů.
[3] FENYK, Jaroslav; CÍSAŘOVÁ, Dagmar; GŘIVNA, Tomáš a kol. *Trestní právo procesní.* 6. vyd. Praha: Wolters Kluwer, 2015, s. 89.
[4] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. s. 416.
[5] KONRÁD, Zdeněk; PORADA, Viktor a Jiří STRAUS. *Kriminalistika: kriminalistická taktika a metodiky vyšetřování*. Plzeň: 2015, s. 351-352.

počítačová zařízení, včetně jejich software.[1] V průběhu zajišťovacích úkonů je žádoucí, aby byl přizván znalec (expert). Rozhodujícím taktickým prvkem v případě ohledání místa činu i domovních prohlídek a prohlídek jiných prostor je moment překvapení a rychlost provedení samotného úkonu. Absolutní nutností je zabránění podezřelé osobě s jakoukoli manipulací s počítačovým systémem.[2]

Zásadní je též spolupráce s jednotlivými poskytovateli komunikační (internetových) služeb. Rovněž je důležitá součinnost s mezinárodními policejními institucemi Europol a Interpol a využití zahraničních specialistů. Důvodem bývá častý přeshraniční charakter počítačové mravnostní trestné činnosti.

Zajímavosti z praxe jsou metody vyšetřování, které jsou využívány ve Velké Británii, tj. v anglosaském právním systému. Tam se policejní taktika poměrně liší od českého přístupu. Britští policisté velmi využívají při potlačování počítačové mravnostní kriminality „agenty“, kteří online prostředí berou jako výhodu a vydávají se falešnými profily za děti. Prakticky využívají stejnou metodu, kterou využívají kyberútočníci, čehož by se hůře dosahovalo mimo online prostředí. Britští policisté takto využívají jednotlivé chaty na sociálních sítích a mají tím pádem možnost sledovat aktivity pedofilů či kybergroomerů. Zároveň online prostředí poskytuje dobrý prostor pro shromažďování důkazů a informací důležitých pro samotné trestní řízení a soudní proces. Britští policisté tento proces nazývají „operacemi skrytého bodnutí“.

Tyto skryté operace byly zavedeny v době, kdy se trestná činnost přemístila do prostředí internetu. Aby nedocházelo ze strany policie k tzv. provokacím, měla při své utajené činnosti reagovat pouze na nabídky, které jim poskytne samotný kyberútočník. Neměli by sami jakkoli vyvíjet prvotní aktivitu či iniciativu. Pachatel – kyberútočník je ten, kdo by měl učinit první krok vedoucí k trestnému činu. Největší výhodou těchto skrytých operací je skutečnost, že umožňují policii proaktivní boj proti pedofilům, kybergroomerům a dalším sexuálním predátorům na internetu. Jde o velmi silný nástroj, který je v praxi velmi účinný a zajišťuje anonymitu. Tento proces umožňuje sledovat de facto celý průběh trestné činnosti s možností opatřování jednotlivých důkazů pro trestní řízení. Existence těchto operací má poměrně silný odstrašující účinek na potencionální kyberútočníky.[3]

Typové vyšetřovací verze a zvláštnosti vytyčování vyšetřovacích verzí, plánování a organizace vyšetřování

Ve vztahu k počítačové mravnostní kriminalitě se vytvářejí verze zejména ke způsobu spáchání trestného činu. Konrád uvádí např. následující verze:

- ✓ verze o neoprávněném zásahu do vstupních dat,
- ✓ verze o provedení neoprávněných změn v uložených datech,
- ✓ verze o provedení neoprávněných pokynů k počítačovým operacím,
- ✓ verze o neoprávněném proniknutí do počítačových systémů a jeho databází,

[1] PORADA, Viktor a Jiří STRAUS. *Kriminalistika: (výzkum, pokroky, perspektivy).* 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2013, s. 532-533.
[2] Tamtéž.
[3] Online grooming and UK law: A submission by Childnet International1 to the Home Office [online]. UK [cit. 2020-11-30]. Dostupné z: https://www.childnet.com/ufiles/online-grooming.pdf

- ✓ verze o napadení cizího počítače, jeho programového vybavení a souborů dat v databázích.[1]

Ve výše uvedených případech jde spíše o obecnou problematiku kyber-kriminality. U počítačové mravnostní kriminality můžeme zaznamenat další možné verze:

- ✓ verze o zneužití počítače a jeho komunikačních prostředků (počítač a komunikační prostředky jsou použity jako nástroj vylákání oběti a jejího následného (sexuálního) zneužití),
- ✓ verze o neoprávněném přístupu pachatele k datům oběti (takto získaná data následně slouží jako prostředek pro vydírání).

S nárůstem a vývojem počítačové mravnostní kriminality, zejména pak s její rozmanitostí, dojde bezpochyby k vývoji a obměně uvedených vytýčených verzí.

Zvláštnosti a následné etapy vyšetřování

Následná etapa vyšetřování se skládá jednak ze znalecké činnosti v oblasti zkoumání výpočetní a komunikační techniky, technických prostředků a jiných nosičů informací. Rovněž je zcela zásadní zkušenost a odbornost vyšetřujících orgánů a to hlavně v oblasti práce s dětmi a mládeží, kteří tvoří citlivou skupinu obětí této trestné činnosti. U počítačové mravnostní kriminality jde hlavně o zkoumání informací uložených na nosičích dat v digitální podobě, které jsou zpravidla následně nosičem důkazů v trestním řízení.

S ohledem na autenticitu digitálních důkazních prostředků a jejich význam v pozdějším dokazování je nezbytností zabránit jakékoli změně či ztrátě v rámci zkoumaných digitálních informací. Z tohoto důvodu je více než vhodné přenést veškeré získané digitální důkazní prostředky na již zmiňovanou přesnou bitovou kopii, na níž je možné původní digitální informace mnohonásobně rekonstruovat.

Vedle znaleckého zkoumání je dále významný samotný výslech obviněného. Výslech obviněného proto bývá jedním z nejdůležitějších typických vyšetřovacích úkonů po sdělení obvinění konkrétní osobě. Výslech obviněného je zapotřebí velmi pečlivě připravit, neboť nároky kladené na OČTŘ jsou ve spojitosti s aspekty mravnostními, kybernetickými, ale i psychologickými poměrně značné. Obviněná osoba se obvykle snaží o vysvětlení jednání jako běžného jednání, zakrývá a zatajuje informace a bagatelizuje je a popírá jakýkoli stupeň zavinění.[2]

S ohledem na výše uvedené je zapotřebí opět klást na přibrání znalce nejen z oboru kriminalistické počítačové expertizy, ale i bezpečnosti a ochrany dat, oblasti soudní psychologie, lékařství apod. V podrobnostech na případné psychologické profilování pachatele a taktické postupy při výslechu obviněných, ale i svědků, lze odkázat na dostupnou literaturu.[3]

---

[1] STRAUS, Jiří a kol. *Kriminalistická metodika.* Plzeň: Aleš Čeněk, 2006, s. 284 a násl.
[2] PORADA, Viktor; STRAUS, Jiří. *Kriminalistika: (výzkum, pokroky, perspektivy)*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2013, s. 543.
[3] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC.

Zvláštnosti zapojení veřejnosti do vyšetřování a prevence

Počítačová mravnostní kriminalita je vysoce latentní kriminalitou. Dále se vyznačuje poměrně vysokou mírou tolerance ve společnosti, ve které jsou internetové technologie vnímány primárně pozitivně. Rovněž vysoká anonymita pachatele, jeho identifikace a následně oblast dokazování je u počítačové mravnostní kriminality velmi složitým procesem. Proto na jednu stranu existují represivní nástroje, nicméně nesmíme zapomínat na prevenci.[1]

Jelikož u počítačové mravnostní kriminality jsou převážnou částí obětí děti, je třeba této skupině věnovat velkou pozornost. Děti jsou velmi zranitelné, důvěřivé osoby, které se snadno mohou stát obětí trestného činu. Proto je velmi rozhodující v oblasti prevence, výchova a vzdělávání uživatelů v oblasti internetových technologií, které se chtě nechtě stávající součástí našeho každodenního života. Jde o budování tzv. informační gramotnosti. Důležitou roli zde má sehrát nejen výchova v rodině, ale především výchova a vzdělání ve školách a to nejen v rámci jednotlivých předmětů, ale též v rámci realizace jednotlivých školení a pořádání besed na téma rizik a hrozeb v IT prostoru.

Základní nástroj prevence v oblasti počítačové mravnostní kriminality představuje všeobecná primární prevence a výuka dětí v oblasti bezpečného používání internetových technologií, zejména sociálních sítí. Jedním z hlavních gestorů této problematiky je Ministerstvo školství, mládeže a tělovýchovy, které realizuje celou řadu preventivních programů, zaměřených na rizikové chování na internetu.[2] Neméně důležitou roli hrají rovněž rodiče, kteří v oblasti prevence představují nejdůležitější článek prevence a jsou schopni působit na děti již v útlém věku a již na začátku dokáží nastavit hranice tomu, jak se jejich děti (ne)budou v IT prostoru pohybovat (např. nastavením blokace některých stránek, kontrolou sociálních sítí, atd.).

Prevenci počítačové mravnostní kriminality můžeme rozdělit na ochranu technickou a ochranu spočívající v osvětové činnosti žáků (studentů), učitelů a rodičů.

Technická ochrana spočívá v instalaci ochranných prvků, programů či zařízení, která zamezují vstup či návštěvu určitých webových stránek.

Stěžejní preventivní aktivitou v oblasti počítačové mravnostní kriminality je však velmi dobře fungující komunikace mezi dítětem a rodičem.

Klíčové je též provádět osvětovou činnost na školách a zařazovat témata spojená s počítačovou mravnostní kriminalitou (rizikovým chováním na internetu) do systému vzdělávání v rámci vzdělávacích programů a školních osnov.

Nejúčinnější prevencí je kombinace výše uvedených metod/ochran.

Níže je uvedeno několik základních pravidel, jakým způsobem se před počítačovou mravnostní kriminalitou chránit.

---

[1] NĚMEC, Miroslav et. al. *Teorie a metodologie kriminalistiky pro magisterské studium – II. díl.* Aktuální problémy kriminalistické praxe. Praha: Abook s. r. o. 2019, s. 305-306.

[2] KOPECKÝ, Kamil. Strategie manipulace dětí v online prostředích se zaměřením na tzv. kybergrooming. Pediatrie pro praxi [online]. Solen, 2015, 2015(5) [cit. 2020-10-21]. ISSN 1803-5264. Dostupnéz:https://www.pediatriepropraxi.cz/artkey/ped-201505-0009_Strategie_manipulace_deti_v_online_prostredich_se_zamerenim_na_tzv_kybergrooming.php

Základní pravidla pro děti:

- ✓ V online prostředí nikomu nesvěřujte své osobní údaje – zejména své fotografie.
- ✓ Dbejte na to, s kým se v online světě bavíte – internetová komunikace je sice anonymní, nicméně dávejte pozor na to, co sdělujete.
- ✓ Všímejte si nesrovnalostí v komunikaci s cizími lidmi v online prostředí – pachatel (útočník) udává různý věk, mění informace, uvádí vám nepravdy.
- ✓ Uvědomte si, proč by zrovna chtěl někdo za každou cenu s vámi udržet vztah v online prostředí či tajit obsah komunikace.
- ✓ Nenechte se oklamat sliby a nikdy nepřistupujte na dary, které vám pachatel (útočník) nabízí.
- ✓ Vytyčte si své osobní hranice. Otázky mravnosti/sexuality neprobírejte s cizími lidmi v online prostředí. Za žádnou cenu nikomu neposílejte materiály se sexuální tématikou, stanou se totiž nástrojem vašeho vydírání.
- ✓ Nikdy nechoďte na osobní schůzky s cizími lidmi, aniž by o tom nevěděli rodiče. Uvědomte si veškerá rizika, která se vám mohou na osobní schůzce stát.

Základní pravidla pro rodiče:

- ✓ Komunikujte s dětmi o tom, co na internetu dělají. Nebojte se „sledovat“ aktivity, které vaše děti v online prostředí dělají. Neznamená, že pokud vaše dítě sedí u počítače, že je v bezpečí.
- ✓ Počítač nenechávejte umístěný v dětském pokoji a eliminujte čas na potřebné minimum, který tráví vaše dítě na počítači.
- ✓ Důkladně vysvětlete dítěti, jaká rizika na internetu mohou být.
- ✓ Nepoužívejte pouze zákazy. Tím, že dítěti zakážete internet, tak se dítě k internetu dostane jiným způsobem a problém se tím nevyřeší. Najde si jinou cestu a nástroje – např. wifi ve škole, používání internetu na mobilu, atd.[1]

Závěrečné shrnutí

Počítačová mravnostní kriminalita je novým fenoménem současné doby. Jde o vysoce společensky nebezpečný jev, který má závažné následky pro své oběti, především děti a mládež. Proto je zcela zásadní, aby všechny zainteresované subjekty prováděly účinná opatření proti páchání této kriminality. Jde o zapojení celé řady subjektů, nejenom policejních orgánů, ale jde též o zahrnutí širší komunity, např. pedagogických pracovníků, preventistů, psychologů, rodičů, neziskových organizací, atd. Nejde však jen o součinnost několika těchto subjektů. Též je důležité společně vytvářet a realizovat preventivní programy, které mohou napomoci v osvětě této problematiky a to hlavně na školách. Důležité je děti a mládež informovat o možných rizicích na internetu a metodách, jak se jim úspěšně bránit. Prevence je totiž v tomto ohledu zcela zásadní, jelikož újma spáchaná některou z forem počítačové mravnostní kriminality má na oběti zásadní negativní dopad ať už na zdraví fyzickém, ale hlavně též psychickém.

[1] E-nebezpečí pro učitele: Materiály pro studium. E-nebezpečí [online]. 2010 [cit. 2020-11-18]. Dostupné z: http://www.e-nebezpeci.cz/ke-stazeni/materialy-pro-studium-studie-atd

Literatura

Učebnice:

BLATNÍKOVÁ, Šárka. Pachatelé komerčního sexuálního zneužívání dětí v ČR – informace z výzkumu. *Trestněprávní revue*. 2010, roč. 9, č. 11.

FENYK, Jaroslav; CÍSAŘOVÁ, Dagmar; GŘIVNA, Tomáš a kol. *Trestní právo procesní.* 6 vyd. Praha: Wolters Kluwer, 2015.

GŘIVNA, Tomáš; SCHEINOST, Miroslav a Ivana ZOUBKOVÁ. *Kriminologie. 5. aktualizované vydání.* Praha: Wolters Kluwer, 2019. ISBN 9788075985545.

CHMELÍK, Jan a kol. *Mravnost, pornografie a mravnostní kriminalita.* 1. vyd. Praha: Portál, s.r.o., 2003. ISBN 80-7178-739-6.

KOHOUT, Roman a Radek KARCHŇÁK. *Bezpečnost v online prostředí*. Karlovy Vary: Biblio Karlovy Vary, 2016. ISBN 978-80-260-9543-9.

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

KONRÁD, Zdeněk; PORADA, Viktor a Jiří STRAUS. *Kriminalistika: kriminalistická taktika a metodiky vyšetřování*. Plzeň: 2015.

MUSIL, Jan; KONRÁD, Zdeněk a Jaroslav SUCHÁNEK. *Kriminalistika. 2. přeprac. a dopl. vyd.* Praha: C. H. Beck, 2004. Beckovy mezioborové učebnice. ISBN 80-7179-878-9.

NĚMEC, Miroslav et al. *Teorie a metodologie kriminalistiky pro magisterské studium – I. díl.* Aktuální problémy kriminalistické praxe. Praha: Abook s. r. o. 2018, 491 s. ISBN 978-80-906974-1-6.

NĚMEC, Miroslav et. al. *Teorie a metodologie kriminalistiky pro magisterské studium – II. díl. Aktuální problémy kriminalistické praxe.* Praha: Abook s. r. o. 2019. 407 s. ISBN 978-80-906974-2-3.

PORADA, Viktor; STRAUS, Jiří. *Kriminalistika: (výzkum, pokroky, perspektivy).* 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2013.

POŽÁR, Josef. *Informační bezpečnost.* Plzeň: Aleš Čeněk, 2005.

SMEJKAL, Vladimír. *Kybernetická kriminalita.* Plzeň: Aleš Čeněk, 2015.

STRAUS, Jiří a kol. *Kriminalistická metodika*. Plzeň: Aleš Čeněk, 2006.

ŠÁMAL, Pavel. *Trestní právo hmotné*. 7. přeprac. vyd. Praha: Wolters Kluwer, 2014. ISBN 9788074786167

VÁLKOVÁ, Helena; KUCHTA, Josef a Jana HULMÁKOVÁ. *Základy kriminologie a trestní politiky.* 3. vydání. Praha: C. H. Beck, 2019. Beckovy mezioborové učebnice. ISBN 9788074007323.

WHITCOMB, C., M. An Historical Perspective of Digital Evidence: A Forensic Scientist's View. International Journal of Digital Evidence, Spring 2002 Volume 1, Issue 1.

Právní předpisy a zdroje:

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

Zákon č. 141/1961 Sb., trestní řád, ve znění pozdějších předpisů.

Internetové zdroje:

BERSON, I. H. Grooming Cybervictims: The Psychosocial Effects ofOnline Exploitation for Youth. University of South Florida. USA. (online) cit. 6. 10. 2020. dostupné zhttp://www.cs.auckland.ac.nz/~john/NetSafe/I.Berson.pdf

Blíže: https://www.policie.cz/clanek/narodni-centrala-proti-organizovanemu-zlocinu-skpv.aspx

Blíže: https://www.internetembezpecne.cz/

Blíže: https://www.e-bezpeci.cz/index.php/71-trivium/1421-co-je-kybergrooming#

E-nebezpečí pro učitele: Materiály pro studium. E-nebezpečí [online]. 2010 [cit. 2020-11-18]. Dostupné z: http://www.e-nebezpeci.cz/ke-stazeni/materialy-pro-studium-studie-atd

Jednotlivé druhy kyberkriminality. Policie ČR [online]. 2020 [cit. 2020-10-06]. Dostupné z: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx

KOPECKÝ, Kamil. Strategie manipulace dětí v online prostředích se zaměřením na tzv. kybergrooming. Pediatrie pro praxi [online]. Solen, 2015, 2015(5) [cit. 2020-10-21]. ISSN 1803-5264. Dostupnéz:https://www.pediatriepropraxi.cz/artkey/ped-201505-0009_Strategie_manipulace_deti_v_online_prostredich_se_zamerenim_na_tzv_kybergrooming.php

Online grooming and UK law: A submission by Childnet International1 to the Home Office [online]. UK [cit. 2020-11-30]. Dostupné z: https://www.childnet.com/ufiles/online-grooming.pdf

Počítačová mravnostní kriminalita. Policie [online]. Praha, 2020 [cit. 2020-11-11]. Dostupné z: https://www.policie.cz/clanek/pocitacova-mravnostni-kriminalita.aspx

PORADA, Viktor a Eduard BRUNA. Digitální svět a dokazování obsahu elektronických dokumentů. Bezpečnostní technologie, systémy a management. [online]. [cit. 2. 12. 2020], s. 3. Dostupné z: http://trilobit.fai.utb.cz/Data/Articles/PDF/37bacb88-3602-4ea7-b9c8-7864970f89e7.pdf

Sexting.cz – vše, co chcete vědět o sextingu [online]. [cit. 11. 11. 2020]. Dostupné z: www.sexting.cz

Sexting. Internetem bezpečně [online]. 2018 [cit. 2020-11-11]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/sexting/

R E S U M É

Článek se zabývá problematikou kriminalistických aspektů odhalování, prověřování a vyšetřování počítačové mravnostní kriminality. V úvodu práce je vymezen úvod do problematiky metodiky vyšetřování. Dále se již práce zaměřuje na jednotlivé kroky (aspekty) metodiky vyšetřování počítačové mravnostní kriminality.

Klíčová slova: počítačová mravnostní kriminalita, metodika vyšetřování, kyberkriminalita, kybergrooming, dětská pornografie, sexting, digitální stopa, trestní zákon.

S U M M A R Y

HEJDUK, Marek: CRIMINALISTICS ASPECTS OF DETECTING, VERIFYING AND INVESTIGATING OF COMPUTER MORAL CRIME

The article deals with the issue of criminalistics aspects of the detection, control and investigation of computer moral crime. The introduction defines the introduction into the problems of investigation methodology. Furthermore, the work is focused on the individual steps (aspects) of the methodology of computer moral crime investigation.

Keywords: computer moral crime, investigation methodology, cybercrime, cyber grooming, child pornography, sexting, digital footprint, criminal law.