UNIVERZITA JANA AMOSE KOMENSKÉHO PRAHA

BAKALÁŘSKÉ KOMBINOVANÉ STUDIUM

2015 – 2016

BAKALÁŘSKÁ PRÁCE

Tomáš Zemín

Mravnostní počítačová kriminalita páchaná na dětech

Praha 2016

Vedoucí bakalářské práce: Ing. Michaela Melicharová

JAN AMOS KOMENSKY UNIVERSITY PRAGUE

BACHELOR COMBINED STUDIES

2015 - 2016

BACHELOR THESIS

Tomáš Zemín

Vice cyber crime against children

Prague 2016

The Bachelor Thesis Work Supervisor: Ing. Michaela Melicharová

Prohlášení

Prohlašuji, že předložená bakalářská práce je mým původním autorským dílem, které jsem vypracoval samostatně. Veškerou literaturu a další zdroje, z nichž jsem při zpracování čerpal, v práci řádně cituji a jsou uvedeny v seznamu použitých zdrojů.

Souhlasím s prezenčním zpřístupněním své práce v univerzitní knihovně.

V Praze dne 22.2.2016 *Tomáš Zemín*

Anotace

Bakalářská práce pojednává o počítačové mravnostní kriminalitě páchané na dětech. Věnuje se obětem a přístupu k nim. Zabývá se typy pachatelů. Popisuje kybergrooming a sexting, způsoby jejich provedení a to, jejich hodnocení z pohledu trestního práva. Věnuje se prevenci a preventivním programům a boji s počítačovou mravnostní kriminalitou páchanou na dětech. Poukazuje na hlavní organizace, které tuto protiprávní činnost potírají.

Klíčové pojmy

Dítě, internet, kybergrooming, sexting, komerční sexuální zneužívání dětí, kyberkriminalita, online dětská pornografie, pedofilie.

Annotation

This thesis deals with cyber crimes against children. It is dedicated to the crime victims and approach to them. It deals with the types of offenders. It describes cybergrooming and sexting, the ways of their implementation and their evaluation in terms of criminal law. It also looks into prevention, prevention programs, and combating cyber crime against children. It refers to the main organizations that fight against these illegal activities.

Key words

Child, internet, cyber grooming, sexting, commercial sexual abuse of children, cybercime, online child pornography, paedophilia.

OBSAH

ÚVOD **7**

1. OBĚTI **9**

2. PACHATELÉ **11**

3. KYBERGROOMING **16**

3.1 Příprava kontaktu 17

3.2 Kontakt s obětí, navázání a prohlubování vztahu 18

3.3 Příprava na osobní schůzku 19

3.4 Osobní schůzka 20

3.5 Trestné činy 20

4. SEXTING **22**

4.1 Trestné činy 22

5. PREVENCE **24**

6. BOJ PROTI DĚTSKÉ PORNOGRAFII **28**

6.1 Interpol - ICSE DB 28

6.2 Europol - EC3 29

6.3 European Financial Coalition 30

6.4 Terre des Hommes – Sweetie 32

6.5 INHOPE a Insafe 36

6.6 Národní centrum bezpečnějšího internetu 37

7. KAZUISTIKA **38**

7.1 První oznámení a šetření, Praha, 2013 38

7.2 Druhé oznámení a šetření, Děčín, 2015 44

7.3 Společné šetření SKPV Děčín a Praha III 45

7.4 Vyhodnocení případu 49

Závěr **50**

Seznam použitých zdrojů **51**

ÚVOD

Děti berou v dnešní době počítače i internet jako samozřejmou součást svého života. Používají jej k učení, ke hrám, ke komunikaci. Pomocí internetu se seznamují s novými přáteli. Láká je anonymita, kterou jim internet poskytuje. Na internetu se mohou hodně naučit, ale také i hodně ztratit. Zranitelnost a důvěřivost dětí může být zneužita proti nim. Digitálním technologiím se přizpůsobil i svět zločinu, který využil právě anonymitu, kterou internet poskytuje. Trestná činnost sexuálního charakteru, která je páchaná na dětech, je doménou nejen jednotlivců, ale i mezinárodních organizovaných skupin. Jedná se o skupiny, které sexuálně zneužívají děti ke komerčním účelům nebo o skupiny osob, které vzájemně sdílejí dětskou pornografii, vyměňují si pornografické materiály, vytvářejí nové a vzájemně se ve své činnosti podporují. Dochází tak ke komerčnímu sexuálnímu zneužívání dětí, které vydělávají peníze on-line sexuálními aktivitami. K tomu při tom jen postačí připojení k internetu a webová kamera. Stejně tak i jednotlivec, který má v úmyslu sexuálně zneužít dítě, má jednodušší cestu, jak se s dítětem navázat kontakt. Není to dnes žádný podivín, který postává před školou a rozdává dětem bonbóny a při tom velmi riskoval, že bude u svého počínání přistižen. Daleko snadnější je pro takového útočníka lovit dítě ve virtuálním prostředí sociálních sítí a diskusních fór.

V souvislosti s mravnostní trestnou činností páchanou na dětech se hovoří o komerčním sexuálním zneužívání dětí, které bylo poprvé definováno v roce 1996 ve Stockholmu na kongresu proti komerčnímu sexuálnímu zneužívání. Jedná se o použití dítěte pro sexuální účely výměnou za peníze nebo za odměnu v naturáliích mezi dítětem a zákazníkem, dítětem a prostředníkem nebo dítětem a agentem, či jinými osobami, které vydělávají na obchodu s dětmi pro tyto účely[1]. Součástí této problematiky je pak obchodování s dětmi, které zahrnuje nelegální a utajované převážení osob přes státní hranice se záměrem přinutit je k sexuálně a ekonomicky vykořisťujícím činnostem. Dále se jedná o dětskou prostituci, která spočívá ve sjednání nebo nabízení služeb dítěte k provádění sexuálních aktů za peníze nebo jinou odměnu. Poslední je dětská pornografie, což je jakýkoli obrazový, textový nebo zvukový záznam, který používá

[1] BLATNÍKOVÁ, Šárka. *Sexuální vykořisťování jako forma závažné organizované kriminality.* 1. vyd. Praha: Institut pro kriminologii a sociální prevenci, 2010, s. 10-11, ISBN 978-807338-103-5

děti v sexuálním kontextu. V případě obrazové dětské pornografie se jedná o zobrazení dítěte při sexuální činnosti a to jak skutečné, tak i simulované, nebo vystavování pohlavních orgánů pro sexuální uspokojení uživatele, zahrnuje výrobu, rozšiřování nebo používání takového materiálu[2].

Cílem této práce je přiblížit problematiku mravnostní kriminality páchané na dětech prostřednictvím digitálních technologií. Zabývá se osobou pachatele a oběti, a hlavně fenomény kybergrooming a sexting, dvě věci, které mohou postihnout každé obyčejné dítě v každé rodině. Práce má seznámit a informovat o těchto negativních jevech, poukázat na tato jednání, jejich specifika a formy a ukázat, jak je na tato jednání pohlížení z hlediska trestního práva. Práce seznamuje se způsoby boje s počítačovou mravnostní kriminalitou páchanou na dětech a to hlavně představením institucí a programů, které se touto problematikou zabývají. Stejně tak je důležitá i prevence a osvěta, ke kterým má tato práce také přispět. Otázkou je, jak je tento boj efektivní, zda jsou zúčastněné subjekty schopny s touto ilegální činností bojovat. V závěrečné části práce byl pro ukázku vybrán případ z praxe, na kterém je konkrétně ukázáno, jak vypadá jednání pachatele, jak reagují oběti a jak postupují při odhalování trestné činnosti orgány činné v trestním řízení.

Práce by měla být přínosem pro lepší pochopení problematiky počítačové mravnostní kriminality páchané na dětech, měla by poskytnout jednoduchý přehled o tomto problému a lepší orientaci laické veřejnosti v této problematice.

Při tvorbě práce jsem vycházel z odborné literatury, veřejně dostupných informací a ze zkušeností, které jsem získal během své skoro osmnáctileté praxe u Policie České republiky. Nejvíce vlastních postřehů a zkušeností bylo v této práci zužitkováno díky působení ve funkci komisaře na Služby kriminální policie a vyšetřování na oddělení mravnostní kriminality a kriminality mládeže. Právě toto zařazení bylo hlavním důvodem k výběru tématu bakalářské práce.

[2] BLATNÍKOVÁ, Šárka. *Sexuální vykořisťování jako forma závažné organizované kriminality*. 1. vyd. Praha: Institut pro kriminologii a sociální prevenci, 2010, s. 11-12, ISBN 978-807338-103-5

1. OBĚTI

Dítě, které se stalo obětí trestného činu, požívá v českém právním řádu zvláštní ochrany. Dítě je zranitelná, bezbranná bytost, která zasluhuje ze strany společnosti zvláštní zacházení, pokud jí bylo ublíženo. Podle Úmluvy o právech dítěte, kterou vydalo OSN v New Yorku dne 20. listopadu 1989 je dítětem každá lidská bytost mladší osmnácti let, pokud podle právního řádu, jenž se na dítě vztahuje, není zletilost dosažena dříve[3].

Pro potřeby trestního práva je pojem dítě upraven v ustanovení § 126 trestního zákoníku, kde je uvedeno, že se dítětem rozumí osoba mladší osmnácti let, pokud zákon nestanoví jinak. Pokud zákon stanoví jinak, znamená to případ, kdy má trestní zákoník zájem na zvýšené ochraně věkově nejmladších dětí a rozlišuje proto u konkrétních trestných činů dvě základní věkové kategorie, dítě mladší patnácti let a dítě, čímž se myslí dítě mladší osmnácti let[4].

Dítě jako oběť trestného činu je dále chráněna zákonem č. 45/2013 sb. O obětech trestných činů. Ten zavádí pojem zvlášť zranitelnou oběť. Tou se stává oběť, která je mladší 18 let, osoba s fyzickým, mentálním nebo psychickým postižením, oběť trestného činu obchodování s lidmi, oběť trestného činu v sexuální oblasti nebo trestného činu zahrnujícímu násilí, pohrůžku násilí, jestliže je riziko vzniku sekundární újmy. Zvlášť zranitelná oběť může požádat o bezplatnou odbornou pomoc. Jedná se o psychologické a sociální poradenství, právní pomoc, právní informace nebo restorativní programy. Oběť má podle tohoto zákona nárok na informace o stavu řízení, na zajištění vlastního bezpečí, zejména utajení totožnosti, na přijetí opatření k zabránění kontaktu s pachatelem. Při výslechu dítěte trestní zákoník ukládá v § 102 povinnost přibrat pedagoga, nebo jinou osobu mající zkušenost s výchovou mládeže, která by se zřetelem na předmět výslechu a stupeň duševního vývoje vyslýchaného dítěte přispěla ke správnému vedení výslechu. Přibrání pedagoga nebo jiné osoby je povinností[5]. K výslechu se zpravidla přibírá sociální pracovník s příslušného oddělení sociálně

[3] Dokumenty. *United Nations: Information Centre Prague, Informační centrum OSN v Praze* [online]. Praha: UNIC Praha [cit. 2016-02-13]. Dostupné z: http://www.osn.cz/knihovna/dokumenty/osn/
[4] ŠÁMAL, Pavel. a kol. *Trestní zákoník I. § 1 až 139. Komentář*. 1. vyd. Praha: C.H.Beck, 2009, s. 1201, ISBN 978-80-7400-109-3
[5] JELÍNEK, J. a kol. *Trestní zákoník a trestní řád s poznámkami a judikaturou*. 2. vyd. Praha: Leges, 2011, s. 680, ISBN 978-80-87212-99-8

právní ochrany mládeže. Někteří rodiče se domnívají, že musí být přítomni u výslechu jejich dítěte, ale to není pravda. Zákon tuto povinnost orgánům činným v trestním řízení neukládá. Zpravidla se rodiče výslechu dětí, které jsou obětí sexuálních trestných činů, nezúčastňují. Z taktického hlediska je to výhodnější, jelikož děti se často stydí před svými rodiči hovořit. Nemusí to být ale pravdou a naopak se může jednat o dítě, které se doma rodičům svěřilo a bez své matky otce, se kterými se cítí v bezpečí, odmítá o činu hovořit. Přítomnost rodičů, ke kterým má dítě důvěru a cítí v nich oporu, mu může pomoci, aby se u výslechu cítilo lépe a nemělo problém sdělovat nepříjemné skutečnosti.

Výslechy dětských obětí se často provádějí jako neodkladný a neopakovatelný úkon ve speciálních výslechových místnostech. Výslechová místnost se skládá ze dvou částí. První z nich je určena přímo k výslechu oběti. Je zařízena tak, aby působila na oběť klidně, k čemuž slouží i vhodný výběr barev, nábytku a vybavení. Při výslechu je třeba v oběti navodit pocit pohody a bezpečí. Místnost je vybavena mikrofony a kamerami. Kamery jsou minimálně dvě, kdy jedna z nich snímá celkový pohled na místnost a druhá detail oběti, aby byly zachyceny projevy její neverbální komunikace a chování.

Druhá část je monitorovací místnost určená ke sledování výslechu a pořízení jeho záznamu. Obraz a zvuk je sem přenášen v reálném čase a je nahráván. V místnosti jsou monitory, které zobrazují záběry ze všech kamer a reproduktory přenášející zvuk. V této místnosti je při výslechu dítěte, který má povahu neodkladného nebo neopakovatelného úkonu přítomen soudce, pracovník orgánu sociálně právní ochrany dětí, dále zde může být státní zástupce, psycholog, nebo obhájce podezřelého. Obě místnosti jsou propojeny zařízením pro komunikaci s vyslýchajícím. Prostřednictvím tohoto zařízení mohou být z monitorovací místnosti kladeny doplňující otázky nebo usměrněn další postup ve výslechu. Výslechy dětí ve speciálních výslechových místnostech provádějí zvlášť vyškolení policisté, kteří prošli specializačním kurzem. Výslech jako neodkladný a neopakovatelný úkon je prováděn, aby se zamezilo sekundární viktimizaci dítěte. Za přítomnosti soudce je proveden pouze tento jeden výslech a dítě se již nemusí vyslýchat při jednání před soudem. Tím se zamezí tomu, že bude muset dětská oběť opět hovořit o tom, co se jí stalo, nebude si muset znovu muset vzpomínat na traumatický zážitek.

2. PACHATELÉ

Pachatelé sexuálních trestných činů páchaných na dětech mají různé vzdělání, pocházejí z úplných i neúplných rodin různého sociálního prostředí. Pachatele sexuálního zneužívání dětí lze rozdělit do dvou skupin[6]. Jednu tvoří preferenční, tzv. praví pedofilové. Jedná se o muže, kteří jsou sexuálně orientováni pouze na děti, tedy fyziologicky na osoby před pubertou. Často mají doma dětskou pornografii, kterou sami fotí nebo filmují.

Pedofilové se dál člení na pedofily svádivé a pedofily sadistické. Svádivý pedofil není primárně orientován na pohlavní styk s dítětem. Snaží se získat náklonnost a přátelství dítěte, je rád v jeho společnosti, s dospělými si nerozumí a to jak po sociální, tak i sexuální stránce. Takový člověk se většinou orientuje na práci s dětmi, může být učitelem, trenérem či dětským lékařem. Řada pedofilů tohoto typu, kteří dovedou svou deviaci potlačit či odfiltrovat, může být skvělými pedagogy, nikomu neubližují. Pokud se svádivý pedofil dopustí sexuálního trestného činu na dítěti, půjde nejčastěji o nepenetrativní aktivity, o mazlení a líbání, příležitostně orální styk. S vlastním dítětem se pedofil dopouští sexuálních aktivit velice vzácně. Tento fakt vysvětluje tzv. Westermarckův efekt. Jedná se o to, že pedofil nemá sexuální zájem o vlastní dítě, pokud s ním byl v intenzivním kontaktu od narození do přibližně třiceti měsíců věku a staral se o něj[7]. Se sadistickým typem pedofila má svádivý pedofil společnou jen preferenci dětského objektu.

Sadistický pedofil je agresivní, dítě pouze použije ke svému uspokojení a pak se jej zbaví. Jde o predátora, který si oběti vyhlíží na hřištích a v parcích, a vzrušuje ho, když jim působí bolest.

Do druhé skupiny pachatelů sexuální kriminality páchané na dětech patří tzv. situační pachatel. Jedná se o pachatele, který nemá primárně sexuální orientaci na děti, nejčastěji si vybírá za své oběti mladé dívky. Nejčastěji bývá takovým pachatelem muž., který prošel normálním vývojem, může být ženatý, může mít děti. V jeho životě ale došlo k některým změnám, které jej nasměrovaly k pedosexuálním aktivitám. Může se jednat o narození dítěte, rozvod, ztrátu zaměstnání, díky pocitu méněcennosti sáhne po

[6] ČÍRTKOVÁ, Ludmila. *Forenzní psychologie*. 2. vyd. Plzeň: Aleš Čeněk, 2009, s. 168-170. ISBN 978-80-7380-213-4.
[7] CHMELÍK, Jan a kol. *Mravnost, pornografie a mravnostní kriminalita*. 1. vyd. Praha: Portál, 2003, s. 175. ISBN 80-7178-739-6

nejdostupnějším objektu na vybití frustrace, kterým je dítě. Tento pachatel může zneužít i vlastní dítě. Rád druhé ovládá, chce nad nimi mít moc, ale k tomu ale většinou nepoužívá násilí.

Podtypem situačního pachatele je primitivní pachatel, který je mentálně i sociálně zaostalý, hrubý a nebezpečný. Nedokáže navázat vztah s dospělou osobou, proto si za sexuální partnery volí děti. Z typologie pachatelů sexuálního zneužívání dětí je důležité si uvědomit fakt, že lidé trpící pedofilií (sexuální devianti) nepřevažují nad sexuálními delikventy. Nejčastějšími pachateli jsou tedy osoby, které netrpí sexuální poruchou. Tyto osoby mají často nízké sebevědomí, komplex méněcennosti a může jim být také diagnostikována porucha osobnosti. Jsou nevypočitatelní, nejde je předem vytipovat a omezit jejich styk s dítětem. V tom tkví jejich nebezpečnost.

Pachatelé komerčního sexuálního zneužívání tvoří různorodý soubor lidí. Lze je rozdělit na tři skupiny. První jsou klienti. O těch platí to, co bylo zmíněno o pachateli sexuálního zneužívání dětí. Jde vlastně o zákazníka sexuálních služeb. Druhou skupinu tvoří kuplíři, tedy osoby, které mají ze zneužití dítěte prospěch. Jedná se o tzv. pasáky, výrobce a dodavatele dětské pornografie, majitele nevěstinců, provozovatele on-line pornografických chatů. Třetí skupinou jsou osoby, které jsou zapojeny do obchodu s dětmi a s dítětem nemusí ani přijít do styku. Jde o obchodníky s dětmi, překupníky.

Obchodování s dětmi není často dílem jednoho pachatele, ale zabývají se jím organizované skupin, často s mezinárodním přesahem. Pachatele v těchto skupinách lze rozdělit na čtyři úrovně[8]. Na nejvyšší úrovni jsou tzv. uzloví pachatelé. Jedná se o vůdce, kteří vydávají ostatním příkazy a určují dynamiku skupiny. Na druhé úrovni stojí koordinátoři, kteří mají za úkol řídit a koordinovat akce. Pachatelé na nižší úrovni již vykonávají konkrétní trestné činy a na rozdíl od pachatelů vyšších úrovní, jsou snadno nahraditelní. Může se jednat o pachatele, kteří například osobně zajišťují transport. Na nejnižším stupni žebříčku stojí ostatní pachatelé, jako jsou padělatelé nebo ostraha. Jedná se o řadové členy organizace, kteří mají na činnosti zpravidla nejmenší profit.

[8] BLATNÍKOVÁ, Šárka. *Sexuální vykořisťování jako forma závažné organizované kriminality*. 1. vyd. Praha: Institut pro kriminologii a sociální prevenci, 2010, s. 35. ISBN 978-807338-103-5

V případě odhalení pachatelů sexuálních trestných činů páchaných na dětech je časté odmítání odpovědnosti pachatelů. To lze kvalifikovat do šesti stupňů vědomého popírání[9].

- Popírání: událost, čin se nestal, pachatel plně popírá své jednání nebo tvrdí, že skutek spáchal někdo jiný, obviňuje tedy jinou osobu.
- Jiný výklad: událost, čin není možno hodnotit negativně, pachatel se částečně přiznává, ale pozitivně hodnotí událost, čin, neuznává svou vinu v chování.
- Odmítání nebo snižování vlastní zodpovědnosti: událost, čin nebyly osobně zapříčiněny, pachatel z části přiznává, vlastní odpovědnost popírá nebo snižuje, hledá obětního beránka.
- Odmítání viny: jiné jednání nebylo možné, pachatel převážně přiznává čin, vlastní odpovědnost částečně potvrzuje, spáchané činy minimalizuje.
- Minimalizace negativních následků: následky události, za kterou osobně zodpovídá, pachatel zlehčuje. Čin sice přiznává, potvrzuje vlastní zodpovědnost, ale následky činu minimalizuje.
- Znehodnocení zdroje kritiky: pachatel přiznává čin, potvrzuje vlastní zodpovědnost, ale zvyšuje hodnotu vlastní osobnosti v jiných oblastech života, snižuje hodnotu a význam jiných osob (včetně oběti) a institucí.

V souvislosti s pedofilií se lze setkat s dalšími pojmy a označeními. Nepiofilie je sexuální zájem o kojence a batolata. Dále se používá označení infantofilie, která se však někdy zaměřuje i na předškolní děti. Obecně se v nejužším slova smyslu považuje pedofilie jako zaměření na prepubertální děti kolem věku devíti let. Hebefilie je náklonnost k dospívajícím dívkám a efebofilie k dospívajícím chlapcům. Korofilie je lesbická náklonnost k dospívajícím dívkám[10].

Pachatelé k vzájemné komunikace a sdílení informací a materiálů s ilegální sexuální tématikou používají často neveřejnou část internetu, tzv. deep web nebo darknet. Tato část internetu není dostupná pro běžné prohlížeče. Právě zde fungují uzavřená fóra, kde probíhá výměna materiálů a je možno zde nalézt například i podrobně vypracovanou příručku pro pedofily. Odkaz, kde tuto příručku nalézt, zde

[9] MILFAIT, René. *Komerční sexualizované násilí na dětech*. Praha: Portál, 2008, s. 90-91, ISBN 978-80-7367-320-8

[10] Jsem pedofil: Mohu to vůbec říct nahlas? – 2. část. *Superrodina.cz* [online]. 2012 [cit. 2016-02-14]. Dostupné z: http://www.superrodina.cz/2012/05/23/jsem-pedofil-2/

nebudu z pochopitelných důvodů uvádět. Jedná se o elektronickou verzi v angličtině. Pokud by se vytiskla, tak by obsahovala 576 stran formátu A4 při použití písma vel. 12. Tato příručka je rozdělena na několik částí. První kapitoly pojednávají o pedofilii obecně, další pak o dětech, o jejich vývoji. Třetí kapitola již radí, jak se chovat bezpečně, aby nebyl útočník chycen. Jak má zničit důkazy, jak se má zachovat, když už je chycen třeba rodiči dítěte nebo policií. Příručka zachází až do takových detailů, že radí, jaké chemikálie použít pro zničení DNA, jaký používat software při online komunikace s dětmi. V případě, že dojde k odhalení, je zde návod, jak se chovat při útěku, jak si zařídit bezpečné nouzové obydlí, kde se dá schovat, než odezní prvotní pátrání. Dále je v kapitole o bezpečnosti popsáno i to, jak se má pedofil v případě odsouzení chovat ve věznici. Čtvrtá kapitola popisuje způsoby, jak tipovat a vyhledávat děti. Dává tipy, kde se snadno seznamovat s dětmi, jakým způsobem k tomu přistupovat, jaké jsou výhody a nevýhody jednotlivých technik, při čemž jsou zde použity poznatky z vývojové psychologie dítěte. Je zde třeba doporučeno pořídit si psa a jeho prostřednictvím navazovat kontakt s dětmi. Odbourává to prvotní nesmělost k navázání kontaktu a lidé si většinou myslí, že ti, co mají zvířata, tak je mají i rádi a tudíž jsou to hodní lidé. Další zde uváděnou možností je vytvoření tzv. magnetu na děti. Není třeba nikam chodit, útočník může zůstat doma, protože děti za ním přijdou sami. Jednou z rad je zde tzv. farma zvířat. Opět zde dochází k využití zvířat, o které mají děti zájem. Mohou si s nimi chodit hrát, krmit je a tak se dostávají do blízkosti pachatele a díky nedostatečné pozornosti rodičů s ním mohou být i sami. Další metodou je tzv. zábavní park. K tomu postačí mít na zahradě bazén, skákací hrad nebo velkou trampolínu, která přiláká děti. Příručka útočníkům radí, aby si vytvořili image pohodového a ochotného souseda, čímž získají důvěru rodičů dětí ze sousedství. Pátá kapitola je pojmenovaná Lovecká sezóna a podle názvu je zřejmé, co je její hlavní náplní. Zde jsou již konkrétní návody, jak sledovat děti, jak s nimi komunikovat, jak dítě ovládnout a mít jej pod kontrolou. Šestá kapitola již popisuje sex s dětmi. Je rozdělena na věkové kategorie dětí a to od dětí ve věku jednoho roku až do patnácti let. U každé kategorie jsou popsány sexuální praktiky, které lze s dětmi provádět a to i s uvedením možných rizik jak pro dítě, tak pro pachatele. V poslední kapitole příručka uvádí tipy, jak připravit dítě na sexuální styk jak po fyzické tak psychické stránce. Příručka je velmi obsáhlá, témata jsou podrobně zpracována. Z jejího obsahu je zřejmé,

že autor nebo autoři se v tomto prostředí pohybují a mají dost vlastních zkušeností. Znát informace z této příručky může policistům pomoci v jejich práci při odhalování sexuálních útočníků. Dají se pak během vyšetřování předpokládat další kroky pachatele, je možné odhadovat, jak se bude podezřelý chovat, jak bude reagovat, zda je jeho reakce spontánní nebo jedná podle naučených postupů a metod.

3. KYBERGROOMING

Grooming je označení pro manipulativní chování. Kybergrooming je typem tohoto chování, konkrétně se rozumí chování uživatele internetu, jehož cílem je získat důvěru dítěte a připravit ho na schůzku s cílem dítě pohlavně zneužít[11]. Termín kybergrooming, pro který se používají i anglická označení child grooming, cybergrooming, označuje chování uživatelů internetu tzv. predátorů, kybergroomerů, které má v oběti vyvolat falešnou důvěru a přimět ji k osobní schůzce. Výsledkem této schůzky může být sexuální zneužití oběti, fyzické násilí na oběti, zneužití oběti pro dětskou prostituci, k výrobě dětské pornografie apod. Kybergrooming je tedy druhem psychické manipulace realizované prostřednictvím internetu, mobilních telefonů a dalších souvisejících technologií[12]. Kybergrooming je velice často navázán na seznamky, veřejný chat, e-maily. S rozvojem sociálních sítí si kybergoomeři hledají své oběti i na těchto sítích. Ke kontaktování dětí jsou využívány i inzertní servery, kde jsou nabídky na výdělky například v oblasti modelingu. K navázání kontaktu s dítětem mohou být zneužity i webové stránky zaměřené na dětské uživatele internetu, stránky pro volnočasové aktivity, dětské herní portály. Pachatelé se vyznačují velkou trpělivostí, není pro ně problém si dlouho s dítětem jen tak psát a shromažďovat o něm informace.

Pachatele kybergroomingu lze dle Národního centra bezpečnějšího internetu rozdělit na několik typů. Prvním z nich je kvazivoyeur, kterému se stačí pouze dívat, oběť sleduje prostřednictvím web kamery, postupně ji manipuluje k co nejintimnějšímu chování a projevům, nejde mu o osobní setkání. Jde mu o aktuální uspokojení sexuálních potřeb. Další jsou experimentátoři, kteří se baví, než oběť zneužijí, naplňuje je radost „ze hry“, experimentátor je nevypočitatelný. Zkoumá nejrůznější portály, mění vlastní identitu a role podle vývoje situace. Postupně zvyšuje tlak na svou oběť. Třetím typem je kriminálník, který svou oběť nebo získaný pornografický materiál prodá, jeho cílem je získat oběť pro páchání trestné činnosti, ať dobrovolné či nedobrovolné.

[11] HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. 1. vyd. Praha: Triton, 2012, s. 52, ISBN 978-80-7387-545-9.
[12] BERSON, Illene. *Grooming Cybervictims: The Psychosocial Effects of Online Exploitation for Youth* [online]. University of South Florida. USA. Dostupné z: http://www.cs.auckland.ac.nz/~john/NetSafe/I.Berson.pdf, citováno dle KOPECKÝ, Kamil. *Kybergrooming: Nebezpečí kyberprostoru* [online]. Olomouc: NET UNIVERSITY s.r.o., 2010, ISBN 978-80-254-7573-7 [cit. 2015-11-28]. Dostupné z: http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=5:kybergrooming-studie

Většinou se jedná o výrobu a šíření pornografie nebo prostituci, někdy poskytuje za úplatu tipy pedofilním pachatelům. Vlastní sexuální stimulace je pro něj druhotným ziskem, prvotní je pro něho finanční zisk. Posledním typem je duševně nemocný kybergroomer, který nemá náhled. Chová se na základě akutních popudů a pohnutek. Jeho prožívání a chování záleží na typu onemocnění nebo stupni mentální retardace. Může být neschopen přiměřené orientace v situaci a ovládat své chování. Chápání sociálních nebo právních norem je u něj omezené či zcela vymizelé. Vyskytují se vzájemné kombinace uvedených typů pachatelů[13]. Jednání pachatele lze rozdělit na čtyři základní etapy[14], které budou popsány v následujících samostatných podkapitolách.

3.1 Příprava kontaktu

Pachatel si vytvoří svoji novou identitu, kterou používá pro navázání kontaktu s obětí. Pro své jednání může použít statickou identitu. To je identita, kterou si vytvoří na sociální síti nebo na komunikační platformě. Tuto identitu nemění. Druhým typem je dynamická identita, kterou si upravuje dle potřeby, může tedy vystupovat pod několika přezdívkami. Aby svoji oběť co nejefektivněji oslovil, dokáže pohotově a účelově měnit data na svém profilu. Udržet dynamickou identitu je pro útočníka podstatně náročnější než u identity statické. Pachatel si musí pamatovat více údajů, které často mění, musí si pamatovat právě ty aktuální, které používá. To se může projevit tím, že si útočník splete oběť, se kterou je právě v kontaktu nebo se dopustí chyby v komunikaci a uvede různé údaje při konverzaci. Právě tyto chyby v konverzaci, kdy si osoba třeba plete svůj věk, jsou signálem k opatrnosti, jelikož by se mohlo jednat právě o kybergoomera. Dalším typem identity je užití představitele nějaké autority, firmy, organizace. Pachatelé se představují jako jednatelé nebo zaměstnanci různých institucí, které pracují ve prospěch dětí. Může se jednat o spolek poskytující sociální služby nebo firmu organizující soutěže.

[13] MAŠKOVÁ, Anna, Kateřina LUKÁŠOVÁ, Rastislav PACÁK a Jana BRANDEJSOVÁ. *Kybergrooming a kyberstalking: Metodický materiál pro pedagogické pracovníky*. Národní centrum bezpečnějšího internetu, 2012. s. 6

[14] KOPECKÝ, Kamil a Veronika KREJČÍ. *Rizika virtuální komunikace: (příručka pro učitele a rodiče)*. Olomouc: NET UNIVERSITY s.r.o., 2010. s. 15-19, ISBN 978-80-254-7866-0.

3.2 Kontakt s obětí, navázání a prohlubování vztahu

Pachatel navazuje a prohlubuje kontakt s dítětem, pracuje na vybudování důvěry a na jejím prohlubování vytvářením přátelského vztahu. K tomuto je často využíván efekt zrcadlení (mirroring). Během tohoto jednání pachatel napodobuje oběť ve snaze prolomit její zábrany. Chová se jako její obraz, využívá k tomu právě svoji dynamickou identitu. Dítě se svěří, že má problémy s rodiči, pachatel hned odpoví, že má také takové problémy a že dítě chápe. Nemusí se jednat jen o stejné emotivní naladění, ale i pocit sounáležitosti a projev empatie. Dítě napíše, že se mu líbí nějaký film nebo třeba herec a pachatel reaguje stejně a konverzace se dostane na toto téma. Tím se více prohlubuje důvěra oběti, navozuje se pocit přátelství, protože mají mnoho společného. Oběti se pak lépe komunikuji a přestává si uvědomovat, že se baví s cizím člověkem. Ochota svěřit se neznámému člověku na internetu je díky anonymitě podstatně vyšší, než je tomu v reálném životě. Za tímto jednáním stojí hlavně potřeba získat o oběti co nejvíce informací. Pachatelé si velmi často vytvářejí profily obětí. Při sestavování profilů tak vychází jak z údajů, které mu sdělí sami oběti, tak i z veřejně dostupných informací na internetu. Pomocí internetových vyhledávačů mohou útočníci zjistit, kde oběť použila například svoje telefonní číslo nebo email a postupně z těchto dalších stránek doplňovat další osobní údaje do jejího profilu. Například telefonní číslo, které oběť uvedla v inzerci, adresu školy z profilu oběti na sociální síti atd. Stejným způsobem může útočník ověřovat věk, pohlaví dítěte, bydliště a další osobní údaje, které mu o sobě dítě samo v komunikaci sdělilo. K navázání co nejužšího vztahu s obětí pachatelé také využívají dárky a úplatky. Tyto úplatky mohou pomoci ověřit osobní údaj, který útočník od oběti získal. Dítěti třeba dobije kredit na mobilu nebo pošle něco poštou. Tím si ověří mobilní číslo nebo adresu. Zároveň si v očích oběti zvýší důvěru, protože pokud pošle dárek, tak mají dětské oběti tendenci přemýšlet tak, že to přeci musí myslet vážně. Pachatel tak může díky těmto falešným projevům přízně dítětem lehce manipulovat. Úplatek útočníkovi může sloužit také k získání nejcitlivějšího údaje, kterým je fotografie obličeje dítěte. Z úplatku se může stát mocná zbraň k ovládání dítěte. Z vlastní policejní praxe je mi znám případ, kdy pachatel obdarovával značkovým oblečením a penězi nezletilé chlapce. Ti k němu pravidelně docházeli a on jim prováděl orální sex. Při rozkrytí tohoto případu nastal problém, že chlapci nechtěli

spolupracovat s policií, protože návštěvy u pachatele pro ně byly dobrým zdrojem peněz.

Postupně dochází ze strany útočníka během komunikace k zavádění na sexuální obsah a ke snižování zábran dítěte. Cílem tohoto jednání je snaha postupně snižovat zábrany dětí a mládeže v oblasti sexuality postupným zaváděním sexuálního obsahu do konverzace. Tím může být v prvé řadě diskuze o lidské sexualitě, sexuálním životě rodičů, může docházet také k tomu, že útočník dítěti nabídne různé erotické či pornografické materiály, například proto, aby vzbudil jeho zájem a snížil jeho stud. Útočník se také snaží získat fotografie nebo videa obnažené oběti, snaží se ji přimět k zapnutí webkamery, jelikož se jedná o snadný způsob, jak získat video obnaženého dítěte. Takto získané materiály pak může útočník použít k vydírání dítěte. Pachatel se dále snaží dítě izolovat od okolního světa. Postupně se pro dítě stává nezastupitelným kamarádem, jediným, komu se dítě svěřuje se svými problémy a který mu doopravdy rozumí. Čím více důvěrných informací útočník zná, tím více je na něj oběť fixovaná a závislá. Zpočátku útočníka vyhledává dobrovolně, později ale již hlavně z donucení, protože nemůže vztah ukončit. Pachatel zná o své oběti důvěrné informace, zná její tajemství a toho také využívá k tomu, aby jí mohl ovládat.

3.3 Příprava na osobní schůzku

Pokud již má pachatel dostatek osobních a intimních údajů o oběti, začne s ní plánovat osobní schůzku. Zde začíná pachatel cíleně manipulovat se svojí obětí, jelikož musí překonat věkový rozdíl mezi sebou samým a svojí obětí. Běžné jsou případy, kdy útočník komunikoval po nějakou dobu s obětí pod svojí falešnou identitou. Při užití této krycí identity o sobě tvrdil, že je nezletilý. Po čase oběti oznámí, že mu rodiče zakázali přístup k internetu, ale že jeho starší třicetiletý bratr může v komunikaci pokračovat. Dítě pak přijme komunikaci s novou osobou, která je proti ní daleko starší. Útočník může dítěti například tvrdit, že jí na schůzce vyzvedne někdo dospělý, třeba otec nebo bratr. Touto osobou pak bývá pachatel, který dítě snadno odvede a pak jej může zneužít.

Pokud oběť odmítne dorazit na schůzku, kterou jí pachatel navrhne, útočník ji začne vydírat. Vyhrožuje, že o ní zveřejní kompromitující materiály, že rozešle její nahé

fotografie jejím přátelům, rodičům, že je vytiskne a rozvěsí v okolí školy nebo bydliště. Mnoho dětí těmto výhrůžkám nedokáže vzdorovat, dostane strach a raději se schůzkou souhlasí.

3.4 Osobní schůzka

Osobní schůzka je cílem všech snah pachatele kybergroominu. První schůzka útočníka s obětí může být zcela nevinná, nemusí dojít k sexuálnímu či jinému zneužití dítěte. Tato schůzka může sloužit pouze k ověření totožnosti oběti. Na schůzce rovněž může útočník prohloubit navázaný vztah s obětí dalším dárkem. Oběť tak získá pocit, že je útočník neškodný a že je skutečně tím opravdovým kamarádem z internetu. K útoku na oběť může dojít až po několika osobních schůzkách. Útok, a to jak sexuální tak i fyzický, má pro oběť nedozírné následky po psychické i fyzické stránce. Pokud má kybergroomer dostatek účinných nástrojů pro manipulaci, jako jsou třeba intimní fotografie, může oběť donutit k opakovaným schůzkám, na kterých útoky pokračují.

Více ohrožené mohou být dívky ve věku 11-17 let, které tráví mnoho volného času v on-line komunikačních prostředích, projevující znaky závislostního chování, mají sníženou sebeúctu a nedostatek sebedůvěry, strádají nedostatkem lásky a pozornosti, jsou osamělé a postrádají kritické myšlení. Jsou zvýšeně sugestibilní a otevřené manipulaci, neznalé a nepoučené[15].

3.5 Trestné činy

Jednání kybergroomera může naplnit hned několik skutkových podstat trestných činů. Trestní zákoník obsahuje od roku 2014 nově §193b, což je trestný čin navazování nedovolených kontaktů s dítětem. Tento paragraf popisuje jednání pachatele, které spočívá v tom, že navrhne setkání dítěti mladšímu patnácti let v úmyslu spáchat trestný čin pohlavní zneužití, výroba a jiné nakládání s dětskou pornografií, zneužití dítěte

[15] MAŠKOVÁ, Anna, Kateřina LUKÁŠOVÁ, Rastislav PACÁK a Jana BRANDEJSOVÁ. *Kybergrooming a kyberstalking: Metodický materiál pro pedagogické pracovníky*. Praha:Národní centrum bezpečnějšího internetu, 2012. s. 9

k výrobě dětské pornografie, svádění k pohlavnímu styku nebo jiný sexuálně motivovaný trestný čin. Za toto jednání může být pachatel potrestán odnětím svobody až na dvě léta[16]. Dále by také mohl pachatel naplnit znaky skutkové podstaty trestného činu obchodování s lidmi dle § 168. Zde zákon mimo jiné uvádí, že: „trestného činu se dopustí ten, kdo přiměje, zjedná, najme, zláká, svede, dopraví, ukryje, zadržuje nebo vydá dítě, aby ho bylo jiným užito k pohlavnímu styku nebo k jiným formám sexuálního zneužívání nebo obtěžování anebo k výrobě pornografického díla“[17]. Dalšími trestnými činy, kterých se může pachatel svým jednáním dopustit, jsou dle trestního zákoníku omezování osobní svobody dle § 171, vydírání dle § 175, poškozování cizích práv dle § 181. Nejzávažnější v případě kybergroomingu je spáchání trestného činu znásilnění dle § 185. V úvahu přichází i trestný čin sexuální nátlak podle § 186. Dalšími trestnými činy mohou být ještě i ohrožování výchovy dítěte dle § 201, nebezpečné vyhrožování § 353, nebezpečné pronásledování § 354.

[16] Zákon č. 40/2009 Sb, trestní zákoník. In: Sbírka zákonů. 2009, s. 354-463. ISSN 1211-1244. Dostupné ze www.mvcr.cz/soubor/sb011-09-pdf.aspx

[17] Zákon č. 40/2009 Sb, trestní zákoník. In: Sbírka zákonů. 2009, s. 354-463. ISSN 1211-1244. Dostupné ze www.mvcr.cz/soubor/sb011-09-pdf.aspx

4. SEXTING

Slovo sexting vzniklo složením dvou slov, kterými jsou sex a textování. Jedná se o elektronické rozesílání textových zpráv, fotografií či videí se sexuálním obsahem. Tyto záznamy pak často bývají zveřejňovány na internetu[18]. Riziko sextingu spočívá v tom, že útočník dostane k dispozici citlivý materiál, jako jsou intimní fotografie nebo videa, který může proti oběti snadno zneužít, takové materiály pak mohou po internetu kolovat několik let i přes snahu oběti tomu zabránit.

V roce 2013 byl proveden výzkum rizikového chování českých dětí v prostředí internetu. Ten provedly internetové portály Seznam.cz, Bezpečný internet.cz ve spolupráci s Univerzitou Palackého v Olomouci. Jednou ze zkoumaných věcí byl právě sexting. Výzkumný vzorek čítal 21372 dětí, z toho byla více než polovina děvčat, asi dvě třetiny dětí byly ve věku 11-14 let, třetina ve věku 15-17 let. Dle tohoto výzkumu 7,23% dětí umístilo na internet svojí „sexy" fotku nebo video, na kterých jsou částečně nebo úplně nazí. Z toho bylo asi 47% chlapců a 53% dívek. Asi tři čtvrtiny dotázaných toto jednání považuje za rizikové chování. Zajímavé byly důvody, proč to děti dělají. Odpovědi byly: „Protože jsem byl nadržený, zábava, on mi ji poslal taky, protože ho miluji a věřím mu na 100 %, byl to můj kluk, chtěl jsem fotku té druhé osoby." Skoro 12 % dětí odpovědělo, že nějaký jejich internetový kamarád umístil na internet svojí fotografii nebo video, kde byl svlečený[19].

4.1 Trestné činy

Sexting může v trestněprávní rovině představovat spáchání několika trestných činů. Jedná se o trestný čin dle § 191 trestního zákoníku, kde je ve druhém odstavci uvedeno: „*Kdo písemné, fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo*

a) nabízí, přenechává nebo zpřístupňuje dítěti, nebo

b) na místě, které je dětem přístupné, vystavuje nebo jinak zpřístupňuje,

[18] HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. 1. vyd. Praha: Triton, 2012, s. 62, ISBN 978-80-7387-545-9.

[19] Videa a dokumenty. *Bezpecnyinternet.cz* [online]. 2013 [cit. 2016-02-13]. Dostupné z: http://www.bezpecnyinternet.cz/ke-stazeni/bezpecny_internet_prezentace.pdf

bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty“[20]. Dále zde přichází v úvahu i trestný čin dle § 192, kterým je výroba a jiné nakládání s dětskou pornografií, § 193 zneužití dítěte k výrobě dětské pornografie, popř. § 201 ohrožování výchovy dítěte, které spočívá v tom, že pachatel svádí dítě k nemravnému životu a § 202 svádění k pohlavnímu styku, kde je popsáno trestné jednání pachatel spočívající v tom, že nabídne, slíbí nebo poskytne dítěti za úplatu, výhodu nebo prospěch a to i za pohlavní sebeukájení nebo obnažování. V trestním zákoníku je v § 203 dále upravena beztrestnost dítěte, které žádá nebo přijme úplatu nebo jinou výhodu či prospěch za výše uvedené jednání[21].

[20] Zákon č. 40/2009 Sb, trestní zákoník. In: Sbírka zákonů. 2009, s. 354-463. ISSN 1211-1244. Dostupné ze www.mvcr.cz/soubor/sb011-09-pdf.aspx

[21] Zákon č. 40/2009 Sb, trestní zákoník. In: Sbírka zákonů. 2009, s. 354-463. ISSN 1211-1244. Dostupné ze www.mvcr.cz/soubor/sb011-09-pdf.aspx

5. PREVENCE

Prevence by měla děti připravit na to, co je může na internetu potkat, jak mají na danou situaci reagovat. Žijeme v 21. Století a pro děti by měly být informace o jejich pohybu a bezpečnosti v kyberprostoru stejně důležité, jako to, že si nemají sedat do auta k cizímu člověku. Dítě by mělo umět rozpoznat ohrožení a v případě, že nastane, tak se z něho nevyděsit, zachovat klid, uvědomit si, že situace je řešitelná a nezlehčovat ji, neutěšovat se nadějemi, že nebezpečí pomine samo. Následně by mělo ukončit komunikaci, nereagovat, neodpovídat ani na nejlákavější sliby, nebo pohrůžky. Ihned potom vyhledat pomoc dospělého a s jeho pomocí zablokovat další komunikaci s útočníkem a s pomocí dospělého zajistit důkazy. K tomu stačí alespoň print screen komunikace s útočníkem nebo obrazovku monitoru s komunikací nebo fotografie nafotit fotoaparátem nebo mobilním telefon, který má dnes každý u sebe. Následuje nahlášení útoku na policii a případně i poskytovateli internetu. Je žádoucí, aby si děti tyto znalosti vhodnou formou osvojili již v mladším školním věku. Jsou základní součástí informační gramotnosti a předpokladem bezpečné práce s online technologiemi. Nejúčinnější metodou učení v předškolním a školním věku je vlastní zkušenost. Vhodné je tyto znalosti a dovednosti rozvíjet prakticky a interaktivně[22].

Pokud budou děti dobře informované, tak si budou ve virtuálním prostředí jisté a budou se zde umět pohybovat. Opatrnost a odpovědnost ze strany dětí, rodičů a učitelů pomohou k tomu, že se minimalizuje možnost útoku na dítě. Komunikace na internetu je stejná jako komunikace v reálném světě, jen si tuto skutečnost musí děti uvědomit. Pokud někoho neznají, tak mu na ulici při náhodném setkání také nesdělují své intimní informace a stejné to musí být i s virtuálním komunikačním partnerem. To by měl být základ bezpečné komunikace na internetu. Uvědomit si, s kým probíhá komunikace a jaké informace jsou mu poskytovány. Stejné je to i s tím, co o sobě každý na internetu dobrovolně sdílí, jaké osobní informace, kontakty na sebe i své blízké, osobní data, fotografie, místa svého výskytu a pobytu. Útočník někdy ani nepotřebuje tyto informace o oběti vyhledávat, jelikož mu je oběť už sama dávno sdělila třeba na sociální síti, stejně tak jako i mnoha dalším uživatelům.

[22] MAŠKOVÁ, Anna, Kateřina LUKÁŠOVÁ, Rastislav PACÁK a Jana BRANDEJSOVÁ. *Kybergrooming a kyberstalking: Metodický materiál pro pedagogické pracovníky*. Praha:Národní centrum bezpečnějšího internetu, 2012. s. 17

Než se děti začnou pohybovat v prostředí internetu, měli by jim jejich rodiče vysvětlit, jak se zde chovat. K tomu stačí několik základních zásad.

- Pokud s někým komunikuješ na internetu, tak mu nesděluj nic, podle čeho by tě mohl identifikovat a najít. Nepiš mu své příjmení, adresu, kam chodíš do školy, telefonní číslo, stejně buď i opatrný k informacím o své rodině a přátelích.
- Nikdy si nespoléhej na to, že znáš dobře člověka, se kterým jsi se seznámil na internetu.
- Nastav si správně zabezpečení svých profilů na sociálních sítích, informace, které zveřejňuješ, měj nastavené jako neveřejné, aby je viděli jen tvoji přátelé a ne cizí lidí.
- Udržuj v tajnosti svá hesla k emailům, profilům na sociálních sítích a komunikačních službám. Neříkej je ani nejlepším kamarádům.
- Na svých internetových stránkách a profilech nezveřejňuj intimní informace a fotografie, jedná se i o zdánlivě nevinné fotografie v plavkách nebo spodním prádle. Nevíš, kdo tyto obrázky vidí a k čemu je dále proti tobě použije.
- Buď opatrný při používání webové kamery, používej jí jen v kontaktu s člověkem, kterého znáš, nikdy se před kamerou nesvlékej. Pro člověka, se kterým komunikuješ, není problém si video nahrát.
- Neodpovídej na neslušné a vulgární zprávy a emaily.
- Nepřidávej si neznámé lidi mezi své přátele na sociálních sítích jen proto, že chceš mít více přátel než tvůj kamarád.
- Vždy se bezpečně odhlašuj ze svého profilu. Pokud se přihlašuješ třeba ve škole, mohl by tvůj profil, ze kterého se neodhlásíš, někdo cizí zneužít.

Jednou ze zajímavých aktivit v oblasti prevence je preventivní program pro děti, který společnost Google ve spolupráci s celorepublikový projektem zaměřeným na prevenci, vzdělávání, výzkum, intervenci a osvětu spojenou s rizikovým chováním na internetu E-Bezpečí a pod záštitou Ministerstva školství, mládeže a tělovýchovy ČR představila v roce 2013 a který se jmenuje Web Rangers[23]. Původní projekt Web Rangers realizoval Google poprvé v roce 2011 v Izraeli, kde zaznamenal velký úspěch

[23] V českém překladu Internetový strážce, rangers byli původně hraničáři, nyní se toto označení používá pro bezpečnostní složky v Texasu nebo pro speciální jednotky americké armády

mezi mládeží[24]. V rámci tohoto projektu žáci sdílí své znalosti o bezpečném používání internetu mezi sebou. Celý program je pro děti zcela zdarma, není časově náročný, děti si sami určí, kolik času chtějí do programu investovat.

Absolvování úvodního online kurzu zabere zhruba 1 hodinu, kreativní workshop pak okolo 5 hodin. Práce na samotném projektu může trvat kolem 10 hodin. Projekt je cílen na děti ve věku 13 až 16 let. Ve školním roce 2014/2015 se do programu zapojilo 79 škol ze 70 měst po celé České republice a na českých školách působilo 240 proškolených a certifikovaných Web Rangerů. Počet žáků, kteří se chtěli stát Web Rangerem, od prvního ročníku tak vzrostl téměř čtyřikrát. Ve školním roce 2015/2016 opět projekt pokračuje.

Základem je online kurz. Ten se skládá z devíti částí. Ty jsou dostupné na internetu na stránkách seduo.cz. Jedná se o osm videí a závěrečný test. Videa jsou v délce do deseti minut a jsou na následující témata:

- Jak tvořit bezpečná a snadno zapamatovatelná hesla
- Sexting: co patří na internet a co už ne
- Jak odhalit počítačové viry a podvodné zprávy
- Jak poradit s kyberšikanou
- Kybergrooming: kdo je kamarád a kdo je podvodník
- Jak chránit své soukromí na sociálních sítích
- Webcam trolling: jak rozeznat podvodné videochaty
- Závěr

Kurz na webu seduo.cz hodnotilo 230 uživatelů a dostal 4,5 bodu z pěti[25].

Děti vytvářejí vlastní projekty pro podporu kybernetické bezpečnosti, které dále slouží k osvětě mezi jejich vrstevníky. To je nejdůležitější myšlenka celého projektu. Aktivní účast dětí, které dále učí a pomáhají dalším dětem. V rámci projektu děti velmi často zpracovávají prezentace, letáky, plakáty, ale i vytvářejí videa, která upozorňují na problémové fenomény ve světě informačních technologií. Výsledkem jejich tvorby je mimo jiné i video Karkulka a bezpečnost na internetu. To je určeno pro děti z prvního

[24] *Web Rangers: Bojujeme za bezpečnější internet* [online]. Google, 2016 [cit. 2016-02-13]. Dostupné z: http://www.webrangers.cz/

[25] 7 lekcí, které z tebe udělají mistra internetové bezpečnosti. *Seduo.cz* [online]. Ptraha: LMC s.r.o., 2016 [cit. 2016-02-13]. Dostupné z: http://www.seduo.cz/7-lekci-ktere-z-tebe-udelaji-mistra-internetove-bezpecnosti

stupně základní školy. Vystupuje zde Karkulka, která si na internetu dopisuje s vlkem. Ten se chová jako klasický kybergroomer, snaží se od ní získat osobní informace a vylákat jí na schůzku. Karkulka dětem vysvětluje, jak by se měly na internetu chovat. Problematikou kybergroomingu se zabývá i několik dalších videí, která účastníci projektu natočili. Tato videa jsou dostupná na Youtube kanále, který se jmenuje Web Rangers ČR a SR. Další z věcí, které byly v rámci projektu vytvořeny, jsou komiksy. Jedním z nich je třeba komiks o kybergroomingu, kde mají děti při čtení volbu, jak by se zachovali v roli hlavního hrdiny komiksu[26].

Program vychází ze skutečnosti, že nejefektivněji si děti předávají znalosti vzájemně mezi sebou a to je právě jeho největší plus, protože informace, které dětem předají jejich vrstevníci, budou určitě lépe přijaty, než ty, které jim bude vykládat učitel nebo rodič. Tento preventivní program považuji za velmi efektivní a atraktivní pro děti.

[26] Projekt Web Rangers 2.0: Nejlepší projekty zaměřené na bezpečné chování teenagerů na internetu. *E-bezpečí.cz* [online]. Olomouc: Centrum PRVoK PdF, Univerzita Palackého v Olomouci, 2015 [cit. 2016-02-13]. Dostupné z: http://www.e-bezpeci.cz/index.php/tiskove-zpravy/971-webrangers2-nejlepsi-projekty

6. BOJ PROTI DĚTSKÉ PORNOGRAFII

Bojem proti dětské pornografii a se zabývají nejen orgány státní správy a orgány činné v trestním řízení, ale také mnoho neziskových a nevládních organizací a nadací. V dnešním globálním světě jsou pachatelé propojeni, mají k sobě blízko díky vyspělým komunikačním technologiím, což klade i velký důraz na technické a materiální vybavení a technické znalosti těch, kdo chtějí s touto kriminalitou úspěšně bojovat.

6.1 Interpol - ICSE DB

ICSE DB (International Child Sexual Explotation Image Database[27]) je zpravodajský a vyšetřovací prostředek, který umožňuje sdílet na mezinárodní úrovni informace k vyšetřování případů šíření dětské pornografie. Jedná se o databázi s obrázky a snímky ze scén z videí s tématikou dětské pornografie a zneužívání dětí. Databáze neobsahuje osobní údaje a je pod správou Interpolu, kde je součástí globální bezpečnostní policejní sítě I-24/7. Součástí této sítě jsou mimo jiné i databáze s forenzními daty jako jsou třeba otisky prstů nebo profily DNA, dále třeba databáze ztracených a odcizených cestovních dokladů, odcizených vozidel, střelných zbraní a nebezpečných materiálů. Daty do této sítě přispívají jednotlivé národní složky Interpolu, které mohou systém také vytěžovat. Přístup do ICSE DB je možný přímo na národní úrovni, není třeba žádat o informace centrálu Interpolu.

ICSE DB byla spuštěna v březnu roku 2008 a nahradila předchozí databázi ICAID (Interpol Child Abuse Image Database[28]), která se využívala od roku 2001. Databázi bylo možno spustit díky finančnímu přispění skupiny G8 a Evropské komise. Systém je určen k identifikaci zachycených obětí, identifikaci místa pořízení videa nebo fotografie a dále k identifikaci pachatele. K tomu jsou využívány markanty, které jsou na fotografiích. Tyto informace o každé fotografii jsou pak uloženy v databázi a při

[27] V českém překladu Mezinárodní databáze snímků sexuálního vykořisťování dětí
[28] V českém překladu Databáze Interpolu snímků zneužívání dětí

vzájemném porovnávání se pak daří nalézat například stejná místa, kde byly fotografie pořízeny nebo stejné osoby, které jsou na nich zachyceny[29].

V roce 2015 byla do ICSE DB aplikována technologie Microsoft Photo DNA[30]. Tato technologie počítá odlišné vlastnosti digitálního obrazu a vytváří jeho jedinečný popis, tzv. hash. Hash je matematický algoritmus, který převede vstupní data do relativně malého čísla. Hashe slouží k monitoringu šíření snímků na internetu na základě technologie Photo DNA. Policie ČR dostává upozornění o šíření závadového materiálu vždy mezi českými IP adresami, nebo mezi českými a zahraničními IP adresami. Tento report se generuje v systému automaticky a obsahuje veškeré údaje.

Za funkčnost ICSE DB pro potřeby Policie ČR je zodpovědný Odbor mezinárodní policejní spolupráce Policejního prezidia (OMPS). Samotné vytěžování systému a vkládání dat je na zodpovědnosti proškolených policistů, jedná se většinou o policisty zařazené u služby kriminální policie a vyšetřování na krajské úrovni. Metodickou záštitu nad systémem má Odbor informační kriminality, který byl původně podřízen Úřadu služby kriminální policie a vyšetřování na Policejním prezidiu, ale nyní je součástí Útvaru odhalování organizovaného zločinu. Pravidelně třikrát do roka jsou pořádány jak kurzy pro proškolení nových policistů, tak i obnovovací kurzy pro stávající policisty s oprávněním pro vstup do databáze.

6.2 **Europol - EC3**

V rámci Europolu byla v roce 2013 zřízena jednotka European Cybercrime Centre[31] (EC3) specializující se na mezinárodní počítačovou kriminalitu. V EC3 jsou tři skupiny zvané Focal Points (FP) zaměřené na analýzy v určitých oblastech kyberkriminality. První z nich je FP Terminal, která se zaměřuje na internetové podvody a zločinecké sítě, které k páchání trestné činnosti využívají platební karty a internetové platby. Druhou skupinou je FP Cyborg, která se zabývá high-tech

[29] Victim identification. *Interpol.int* [online]. Lyon: Interpol, 2016 [cit. 2016-02-13]. Dostupné z: http://www.interpol.int/Crime-areas/Crimes-against-children/Victim-identification
[30] Global efforts to identify child abuse victims via INTERPOL boosted with Microsoft technology. In: *Interpol.int* [online]. Singapore: Interpol, 2015 [cit. 2016-02-13]. Dostupné z: http://www.interpol.int/News-and-media/News/2015/N2015-041
[31] V českém překladu Evropské centrum kybernetického zločinu

kriminalitou. V jejím záběru jsou trestné činy, které škodí počítačům a počítačovým sítím Evropské unie. Jedná se například o hacking, phishing, krádeže identity. Třetí skupinou je FP Twins, která poskytuje pomoc a odborné znalosti v oblasti boje proti distribuci materiálů se zneužíváním dětí v on-line prostředí. Součástí EC3 je ještě Cyber Intelligence Team[32] (CIT), který se zaměřuje na sběr informací o počítačové kriminalitě z veřejně dostupných zdrojů s cílem rozšířit obraz zpravodajských služeb o počítačovou trestnou činnost v Evropské unii, čímž umožňuje rychle reagovat na nově vzniklé hrozby[33].

V rámci FP Twins je prováděna spolupráce již v prvotní fázi prověřování trestného činu. Nečeká se na výsledky domovních prohlídek či odborných posudků. Jakmile má policista k dispozici jakékoliv poznatky, třeba i neověřené a to i bez vazby na zahraničí, je vhodné je zaslat a během prověřování zasílat, Europolu do FP Twins. Zde dojde k dokonalé lustraci nejenom v interní databázi Europolu, ale i v otevřených zdrojích a vyšetřovatel může získat cenné poznatky ať už k historickému nebo i k aktuálnímu charakteru a to včetně poznatků ze sítě TOR. Odbor mezinárodní policejní spolupráce požaduje, aby se již od počáteční fáze prověřování spolupracovalo s FP Twins. Tímto se dá zjistit a případně potvrdit mezinárodní přesah, popřípadě při zjištění celorepublikového charakteru případu díky FP Twins může zůstat případ na jednom útvaru a nerozdrobí se na jednotlivé útvary územních odborů nebo krajských ředitelství. V případě, že se tak již stane, je třeba vyšetřování případu centrálně koordinovat.

6.3 **European Financial Coalition**

European Financial Coalition against Commercial Sexual Explotation of Children Online[34] (EFC) je koalice, která sdružuje klíčové subjekty z bezpečnostních složek i soukromého sektoru a neziskových organizací v boji proti sexuálnímu komerčnímu zneužívání dětí na internetu. Členy jsou mimo jiné EC3, Eurojust, což je orgán

[32] V českém překladu Kybernetický zpravodajský tým
[33] Combating Cybercrime in a Digital Age. *Europol.eu* [online]. The Hague: Europol, 2016 [cit. 2016-02-13]. Dostupné z: https://www.europol.europa.eu/ec3
[34] V českém překladu Evropská finanční koalice proti komerčnímu online sexuálnímu zneužívání dětí

Evropské unie, který byl zřízen pro podporu mezinárodní justiční spolupráce mezi zeměmi Evropské unie[35], Google, Microsoft, Mastercard, PayPal, VISA, International Centre for Missing & Exploiting Children, INHOPE, Missing Children Europe (MCE), European Police College CEPOL, italská, dánská, holandská a švédská policie. V rámci koalice je zřízeno pět pracovních skupin. Každá z nich zodpovídá za jeden ze strategických cílů koalice.

První skupina má na starosti operace vedené proti online komerčnímu zneužívání dětí a vede jí EC 3 a Eurojust. Skupina podporuje bezpečnostní složky, které vedou vyšetřování, dále také spolupracuje se soukromými subjekty. Skupina jim dodává mechanismy na podporu a analýzu testovacích nákupů, spolupracuje s poskytovateli platebního styku.

Druhá skupina má na starosti strategické analýzy a hlášení. Vůdčími organizacemi je zde opět EC3 a INHOPE. Cílem je posoudit a vyhodnotit poznatky k sexuálnímu komerčnímu zneužívání dětí v internetovém prostředí, jako jsou hostingové služby, diskusní skupiny. Skupina zajišťuje sběr a analýzu kvantitativních dat o problematice komerčního sexuálního zneužívání dětí a to na základě údajů, které jsou shromážděny od ostatních členů koalice.

Třetí skupina zajišťuje podporu a spolupráci se soukromým sektorem. Tuto skupinu vede Microsoft, PayPal a MCE. Cílem je ochrana oprávněných soukromých podnikatelských zájmů a proti zneužití zločinci s cílem spáchat trestné činy v souvislosti s komerčním sexuálním zneužíváním dětí. Skupina poskytuje podporu a pomoc poskytovatelům finančních a internetových služeb, pro které připravuje vzory a šablony pro smluvní zadání a odborné příručky a návody.

Čtvrtá skupina zajišťuje výcvik. Vede ji MasterCard, CEPOL a Microsoft. Jejím cílem je zdokonalovat bezpečnostní složky a soukromé subjekty v problematice boje proti kriminalitě komerčního sexuálního zneužívání dětí. Skupina zajišťuje školení, řeší právní, technické a provozní otázky, zajišťuje sdílení osvědčených a ověřených postupů.

Pátá skupina zajišťuje vnější vztahy. Vede jí VISA a MCE. Cílem je zvyšovat povědomí veřejnosti a osob s rozhodovací pravomocí o činnosti EFC. Skupina vydává informační letáky, vytváří veřejné internetové stránky, pořádá tiskové konference a

[35] Background: History of Eurojust. *EUROJUST: The European Union's Judicial Cooperation Unit* [online]. Den Haag: Eurojust, 2016 [cit. 2016-02-22]. Dostupné z: http://www.eurojust.europa.eu/about/background/Pages/History.aspx

vydává tiskové zprávy o své činnosti a pořádá odborné konference a setkání za účelem vzájemné informovanosti široké veřejnosti a subjektů, které se podílejí na boji proti kyberkriminalitě[36].

6.4 Terre des Hommes – Sweetie

„Jmenuji se Sweetie, je mi 10 let, žiji na Filipínách, každý den sedím před webovou kamerou a bavím se s muži. Stejně tak jako desítky tisíc dalších dětí. Ti muži po mě chtějí, abych si svlékala oblečení. I oni se svlékají, hrají si sami se sebou, chtějí, abych si i já hrála sama se sebou. Jakmile jsem online, tak ke mně přicházejí. Desítky, stovky. Každou hodinu. Je jich mnoho. Ale co nevědí je, že nejsem opravdová. Jsem počítačový model vytvořený kousek po kousku pro vystopování těchto mužů, kteří toto provádějí"[37]. Tímto začíná video organizace Terre des Hommes[38] prezentující projekt Sweetie.

Nezisková organizace Terre des Hommes byla založena v roce 1965 skupinou dobrovolníků, aby pomáhala zneužívaným dětem, dostala je z prostředí, kde jsou zneužívány a zajistila jim nové bezpečné prostředí, kde by se mohly dále rozvíjet. Terre des Hommes podporuje více než 200 projektů v 17 zemích světa, na kterých spolupracuje s lokálními partnery, kteří znají místní podmínky, znají místní kulturu a jsou schopni najít nejlepší způsoby řešení problémů. Terre des Hommes se zaměřuje na nejhorší formy kriminality páchané na dětech, kterými jsou dětské práce, obchodování s dětmi, týrání dětí a sexuální zneužívání dětí. Sexuální zneužívání zahrnuje dětskou prostituci, dětskou sexuální turistiku, dětskou pornografii a sex s dětmi prostřednictvím webové kamery.

Právě sex s dětmi prostřednictvím webové kamery, označovaný jako WCST (Webcam Child Sex Tourism[39]), je rychle se rozvíjející forma trestné činnosti páchané na dětech prostřednictvím internetu. Zisky z tohoto obchodu velmi rychle rostou,

[36] *European Financial Coalition against Commercial Sexual Exploitation of Children Online* [online]. Bruxelles, 2016 [cit. 2016-02-13]. Dostupné z: http://www.europeanfinancialcoalition.eu
[37] Sweetie: The face of webcam child sex tourism. In: *Youtube* [online]. 7.9.2015 [vid. 2015-29-11]. Kanál uživatele sweetie. Dostupné z: https://www.youtube.com/watch?v=yWLTEkryAQg
[38] V českém překladu Země lidí
[39] V českém překladu sexuální dětská turistika prostřednictvím webových kamer

důvodem je oproti klasické sexuální turistice relativní bezpečí pro ty, kteří tyto služby vyhledávají. Zákazníci jsou hlavně z bohatších zemí. Dříve museli tito pachatelé za účelem vyhledání svých obětí cestovat do zemí, jako je Thajsko, Kambodža nebo třeba Filipíny. To bylo časově i finančně náročné. Životní úroveň v těchto zemích je sice na nižší úrovni, jsou zde nižší ceny, ale nejdražší položkou je právě cena letenky. S příchodem vysokorychlostního internetu a jeho rozšířením i do odlehlých koutů světa se pro lidi vše zjednodušilo.

Za internetové sexuální služby se platí hlavně pomocí předplacených kreditních karet, které jsou anonymní, nejsou spojeny s žádným účtem, tudíž je skoro nemožné vystopovat jejich uživatele. Podle odhadů denně 750 000 uživatelů internetu hledá online sex s dítětem na více než 40 000 místnostech na veřejném chatu. Desítky tisíc dětí jsou zneužívány k online prostituci hlavně na Filipínách a dalších zemích, které trpí chudobou. V některých případech jsou děti zneužívány k této výdělečné činnosti organizovanými skupinami, jindy ji provozují sami třeba v internetových kavárnách, protože doma nemají připojení k internetu. V některých případech děti zneužívají jejich vlastní rodiče, kteří je nutí provádět sexuální představení a utěšují se iluzí, že pokud děti nemají fyzický kontakt s jinou osobou, tak se jim nic špatného nemůže stát. Terre des Hommes uvádí, že dítě na Filipínách si online sexem vydělá 500 až 1000 filipínských peso, kdežto ten, kdo provozuje webové kamery a děti k provozování online sexuálních služeb zneužívá, dostává 4000 až 5000 peso. Kurs peso k české koruně je asi 2:1. Zde je názorně vidět, jak velké peníze se v této kriminální činnosti vydělávají.

Příkladem může být dívka, která si říká Babe, bylo jí 14 let, když pracovala jako prostitutka před web kamerou. Babe je třetí ze šesti dětí, podle jejích rodičů a učitelů je to chytrá dívka. Její otec pracoval jako taxikář na tříkolce. V roce 2005 se po porodu nejmladšího dítěte matka Babe psychicky zhroutila. Rodiče Babe prodali část majetku, aby měli peníze na léčbu a živobytí. Babe se nakonec rozhodla, že začne pracovat v sexuálním průmyslu stejně jako mnoho jejích vrstevníků. Dostávala za jedno představení 6 až 20 dolarů. Při těchto představeních po ní muži chtěli, aby se svlékala a před kamerou prováděla různé druhy sexuálních aktů. V roce 2013 se Babe dozvěděla, že v oblasti, kde pracovala, policie provádí vyšetřování a hledá děti, které si vydělávají provozováním sexuálních aktivit přes webkameru. Kontaktovala lokálního partnera Terre des Hommes organizaci FORGE, která jí pomohla ukončit její činnost, poskytla

jí psychosociální pomoc, přístřeší a Babe se postupně učí, jak se vypořádat se svými zkušenostmi, spolupracuje s touto neziskovou organizací, komunikuje s dalšími dětmi[40].

Holandská pobočka Terre des Hommes vytvořila pro boj s dětskou online prostitucí projekt Sweetie, který byl zahájen koncem roku 2013. Podstatou celého projektu byl počítačem vytvořený virtuální model desetileté filipínské holčičky pojmenované Sweetie. Sweetie má realistické pohyby i mimiku obličeje. Pro tyto pohyby bylo využito digitálně snímaných pohybů opravdového člověka. Ve skladu na okraji Amsterdamu tým lidí z Terre de Hommes vytvořil svojí základnu, ze které komunikoval a díky vytvořené aplikaci ovládal každý pohyb avatara Sweetie. Činnost probíhala tak, že se lidé z týmu připojili na veřejný chat a stačilo pouze uvést, že je Sweetie desetiletou dívku z Filipín. Během několika vteřin Sweetie kontaktovali různí muži z celého světa, kteří požadovali, aby použila web kameru a svlékla si oblečení, za což byli ochotni zaplatit. Se Sweetie se dle zprávy, kterou vydala organizace Terre des Hommes, v době od 17.4.2013 do 12.6.201, tedy za dobu necelých dvou měsíců, 3 pokusilo v devatenácti veřejných chatovacích místnostech spojit 20 172 lidí. Více než 1000 mužů, kteří byli ochotni zaplatit 20 dolarů za online sex, se podařilo ztotožnit a údaje předat Interpolu. Zatímco tito muži komunikovali se Sweetie, probíhalo zjišťování jejich totožností z kousků informací, které o sobě dali. K tomu bylo používáno informací z Google, Facebook, Skype a dalších veřejných zdrojů. Bez jakéhokoliv narušování jejich počítačů a přístupům do nich, se podařilo zjistit jejich jména, adresy, telefonní čísla, obrázky a videozáznamy. Celkem se jednalo o muže ze 71 zemí, 254 mužů bylo z USA, 110 z Velké Británie, 103 z Indie a ostatní byli z dalších zemí po celém světě. Mnoho pachatelů pak bylo v Austrálii, Belgii, Dánsku, Polsku a Velké Británii obviněno. O projektu se díky médiím a dalším komunikačním kanálům dozvěděla více než miliarda lidí po celém světě, video Sweetie na Youtube v několika jazycích vidělo více než 7 miliónů lidí. Tato iniciativa se ale ne všude setkala s pochopením. Mluvčí Europolu Sotren Pedersen pro agenturu Reuters v roce 2013 vyjádřil k tomuto projektu výhrady, když uvedl, že kriminální vyšetřování, které

[40] Being a webcamsexgirl is terrifying. *Terre des hommes* [online]. Den Haag: Terre des Hommes Nederland, ©2015 [cit. 2015-12-02]. Dostupné z: https://www.terredeshommes.nl/en/being-webcamsexgirl-terrifying

používá takovéhoto podbízivého sledování, by mělo být ve výlučné pravomoci bezpečnostních orgánů[41].

V roce 2015 byl spuštěn projekt Sweetie 2.0. Na tento projekt darovala holandská Postcode Lottery, což je největší charitativní loterie v Nizozemsku, částku 3 860 750 eur. Do projektu se zapojili profesoři z university v Tilburgu klinický forenzní psycholog dr. Stefan Bogaerst u oddělení vývojové psychologie a dr. Bert-Jaap Koops, specialista na technologie a počítačovou kriminalitu z Institutu pro právo, technologie a společnost, aby pomohli s vylepšení Sweetie na verzi 2.0. Současně s tím bude zkoumána účinnost prevence a právní rámec pro boj s prostitucí prostřednictvím webových kamer. Sweetie 2.0 je nový pokročilý softwarový systém, který by měl bezpečnostním složkám po celém světě pomoci s odhalováním pachatelů trestné činnosti a zároveň by je měl i odradit potenciální pachatele od páchání jejich protiprávního jednání. Nová verze by měla pracovat automaticky a to tak, že bude sama prohledávat tisíce chatovací místnosti současně s pomocí chatovacích robotů a bude vyhledávat klíčová slova, jako třeba sex. Dále se bude vydávat za desetiletou filipínskou dívku. Jakmile bude nějaký zájemce požadovat sex show a bude ochoten za ní zaplatit, automaticky mu bude zasláno varování, které nebude možno smazat. To by mělo působit preventivně a mělo by to většinu mužů odradit. Pokud budou vědět, že mohou být sledováni, budou se bát, že bude jejich identita zjištěna. Celý systém, který má být koordinován s vyšetřujícím orgány jednotlivých zemí, bere v potaz odlišnosti právní úpravy dané problematiky v různých zemích. Nový projekt Sweetie 2.0 by měl v rámci prevence využívat systému catch-recatch a to s ohledem na to, že pachatelé pracují s různými emailovými účty. Tato metoda funguje tak, že osoba „X“ je spatřena v chatovací místnosti „Y“ a dostane varování s informací o tom, že její jednání je trestným činem dle platných právních norem dané země a je jí oznámeno, jaké to může mít důsledky podle trestního práva a zároveň obdrží tipy, kde vyhledat pomoc. Pokud tato osoba „X“ navštíví chatovací místnost „Y“ a použije k tomu jinou emailovou adresu, bude systémem stále rozpoznána jako výchozí osoba „X“. Bude jí vydáno druhé

[41] ESCRITT, Thomas a Kevin LIFFEY (ed.). Dutch activists track alleged child abusers with help of digital ”girl”. *Reuters.com* [online]. New York: Thomson Reuters, ©2013 [cit. 2015-12-02]. Dostupné z: http://www.reuters.com/article/2013/11/04/us-dutch-childabuse-idUSBRE9A30QQ20131104#SIErBYpaEmwuBRyb.97

a zároveň poslední varování. Pokud bude osoba X chycena potřetí, budou informace o ní předány policii[42].

Projekt Sweetie ukázal, že při odhalování dětské pornografie je potřeba aktivních opatření. Internet je veřejný prostor stejně tak jako park nebo ulice, kde jsme zvyklí vídat policii, která dohlíží na bezpečnost a pořádek. Proč tedy ne i na internetu? Problémem bývá nedokonalá legislativa, která policii neumožní, aby byla více aktivní, při svém aktivním jednání se mohou policejní orgány dostat do kolizního postavení provokatérů, které je v mnoha zemích v rozporu s právem a jeho výsledky nelze považovat za důkazy v případném trestním řízení.

6.5 INHOPE a Insafe

INHOPE je holandská nadace, která podporuje vznik internetových horkých linek po celém světě sloužících k boji proti dětské pornografii. Finančně podporuje vzniky těchto linek v zemích, kde je to hlavně z finančních důvodů obtížné. Horké linky umožňují veřejnosti anonymně oznamovat podezření na zjištěné materiály se zneužíváním dětí či další podobné protizákonné aktivity na internetu. Horké linky tato oznámení vyhodnotí a dále je potupují bezpečnostním složkám příslušné země. INHOPE provozuje nebo spolupracuje s 51 horkými linkami ve 45 zemích po celém světě. Díky iniciativě INHOPE byly zprovozněny horké linky v zemích Afriky nebo Jižní Ameriky. INHOPE spolupracuje s evropskou sítí center prosazující bezpečné a zodpovědné užívání internetu Insafe. Tato centra jsou zaměřena hlavně na osvětu mezi mladými lidmi, ale také nezapomíná na ostatní uživatele internetu, rodiče, pedagogy, politiky. Pomáhá se zvyšováním počítačové gramotnosti v populaci. V jednotlivých zemích EU jsou národní centra, která jsou zodpovědná za realizaci kampaní a osvěty. V České republice spolupracuje s INHOPE a Insafe Národní centrum bezpečnějšího internetu (NCBI). NCBI provozuje stránky internet-hotline.cz, které slouží k hlášení závadového obsahu internetu a pro osvětu užívá stránky saferinternet.cz.

[42] New software recognized potential pedophiles online. *Tilburg University: understanding society* [online]. Tilburg: Tilburg University, ©2015 [cit. 2015-12-02]. Dostupné z: https://www.tilburguniversity.edu/current/news/press-release-new-software-recognizes-potential-pedophiles/

6.6 Národní centrum bezpečnějšího internetu

Národní centrum bezpečnějšího internetu (NCBI) je neziskové nevládní sdružení, které bylo založeno v roce 2007 za účelem zvýšení bezpečnosti užívání internetu, informačních a komunikačních technologií. Činnost NCBI je zaměřena na děti, jejich rodiče i prarodiče, pedagogy, policisty, sociální pracovníky. NCBI pořádá konference, přednášky a semináře pro laickou i odbornou veřejnost. Partnery NCBI jsou významné subjekty komerční sféry i veřejné zprávy. Jedná se o Microsoft, Google, Intel, UPC, dále pak například Středočeský kraj a kraj Vysočina, magistrát hl. m. Prahy, Ministerstvo vnitra ČR[43].

NCBI má několik projektů. Jedním z nich je Safer Internet CZ. Jeho cílem je propagace bezpečnějšího používání internetu a komunikačních technologií. Hlavním nástrojem pro komunikaci je v tomto projektu webový portál saferinternet.cz a bezpecne-online.cz. tyto weby jsou zaměřeny na mladé lidi ve věku 12-18 let. V rámci tohoto projektu spolupracuje NCBI s Insafe.

Dalším významným projektem je ve spolupráci s INHOPE provoz horké linky sloužící k ohlášení ilegálního obsahu na internetu. K tomu jsou provozovány webové stránky horkalinka.cz a internet-hotline.cz. Zde mohou lidé učinit anonymní oznámení k závadovému obsahu internetu, který objeví. NCBI garantuje anonymitu osoby, která oznámení učiní. Pokud na sebe osoba uvede kontakt a chce být o výsledku informována, nebude tento kontakt bez souhlasu předán třetí straně. K oznámení je připraven jednoduchý formulář, který je variabilní podle druhu nezákonného obsahu. Po přijetí oznámení dojde k jeho analýze, a pokud je vyhodnoceno jako opodstatněné, je dále informována policie, poskytovatel internetových služeb nebo mobilní operátor a organizace INHOPE. NCBI nemůže garantovat, že bude škodlivý obsah z internetu odstraněn. To může učinit mobilní operátor nebo poskytovatel internetu na základě porušení interních pravidel nebo z rozhodnutí soudu. Pokud se nahlášený nezákonný obsah nachází mimo Českou republiku, je tento poznatek předán cestou INHOPE k prověření Interpolu[44].

[43] *Národní centrum bezpečnějšího internetu* [online]. Praha: Národní centrum bezpečnějšího internetu, 2012 [cit. 2016-02-13]. Dostupné z: http://www.ncbi.cz
[44] *Národní centrum bezpečnějšího internetu* [online]. Praha: Národní centrum bezpečnějšího internetu, 2012 [cit. 2016-02-13]. Dostupné z: http://www.ncbi.cz

7. KAZUISTIKA

Případ, který byl vybrán, byl řešen oddělením kriminality mládeže a mravnostní kriminality Služby kriminální policie a vyšetřování (SKPV) Obvodního ředitelství Policie Praha III. Případ byl nejprve v roce 2013 prověřován, ale nakonec byl odložen podle § 159a odst. 5 trestního řádu, jelikož se nepodařilo ztotožnit konkrétního pachatele. Následně se ale objevil podezřelý. Ve spolupráci s SKPV územního odboru Děčín se podařilo totožnost pachatele zjistit. Na šetření tomto případu jsem se aktivně podílel, byl jsem jeho hlavním zpracovatelem ve fázi prověřování ze strany SKPV Obvodního ředitelství Praha III. Jména osob, které v případu figurovaly, byla pro potřeby této práce změněna nebo byla vypuštěna příjmení zúčastněných osob.

7.1 První oznámení a šetření, Praha, 2013

Dne 25.11.2013 oznámila na místním oddělení v Praze 3 Pavla Radková, že její dcera Magda, roč. 2001, vede komunikaci sexuálního charakteru s neznámou osobou. Paní Radková půjčuje své dceři občas mobilní telefon, aby se Magda podívala na svůj profil na Facebooku. Dne 23.11.2013 se Magda zapomněla odhlásit ze svého profilu na telefonu matky a šla spát. Matka se podívala do telefonu a nalezla konverzaci s osobou Petra Horká. Ta kontaktovala Magdu prostřednictví služby Skype. Zde byla dohledána konverzace z 9.11.2015 z doby okolo 23.00 hod, kde si Magda s Horkou nejprve psaly, a pak došlo k videohovoru, kde Horká píše instrukce Magdě, jak si má stoupnout, že se má tvářit sexy, aby svlékla tričko a kalhoty. Magdě slibovala Horká mobilní telefon iPhone. U výslechu paní Radkové byla přítomna komisařka z oddělení analytiky kriminální policie, která se souhlasem matky zajistila komunikace ze Skype a zálohu profilu Magdy na Facebooku.

Pachatel měl na komunikační službě Skype založený účet. Od společnosti Skype byly v souladu s trestním řádem prostřednictvím Odboru informační kriminality Úřadu služby kriminální policie a vyšetřování Policejního prezidia ČR zjištěny informace k tomuto profilu. Byla zjištěna IP adresa, emailová schránka použitá při registraci a poskytovatel připojení se zjištěnou IP adresou, který, jak bylo zjištěno, sídlí v Královehradeckém kraji, kde také poskytuje připojení k internetu. Dále byla

prostřednictvím Policejního prezidia na základě podnětu oddělení analytiky zajištěna záloha profilu Petra Horká na Facebooku u provozovatele této služby v USA. Tento podnět byl později policisty oddělení analytiky zneplatněn, jelikož došlo ze strany Policejního prezídia ke změně postupu vyžadování této zálohy a pro vyžádání údajů od spol. Facebook by bylo třeba využít mezinárodní právní pomoci. Tímto postupem by z hlediska důležitého pro trestní řízení policejní orgán zjistil přístupové údaje, které se však podařilo získat jiným způsobem a tento krok by byl proto nadbytečný.

Na základě soudního příkazu dle § 88a odst. 1 trestního řádu, který vydal Obvodní soud Praha 3, byly vyžádány údaje od poskytovatele připojení v době, kdy se připojoval pachatel prostřednictvím zjištěné IP adresy, bohužel bylo ale zjištěno, že se v případě této adresy se jedná o NAT adresu (překlad IP adres), kdy v jednu dobu může prostřednictvím této IP adresy přistupovat více uživatelů. Dle poskytovatele připojení je zde připojeno asi 4000 klientů. Společnost užívá systém data retention, který slouží ke sledování síťového provozu pro plnění zákona č. 127/2005 Sb. o elektronických komunikacích. Systém byl zprovozněn od prosince 2013, tudíž nebyl poskytovatel schopen sdělit policii provoz IP adresy před tímto datem.

Ke zjištění konkrétní IP adresy uživatele bylo třeba zjistit i číslo portu, což by pak mělo poskytovateli připojení umožnit zjistit konkrétního uživatele. Oddělení analytiky vytvořilo webovou stránku, která v sobě měla php skript, který zaznamenával veškeré logovací přístupy, kde po kliknutí na odkaz na tuto stránku se uživateli objevila hláška, že stránka neexistuje, ale byl zaznamenán přístup tohoto uživatele a to jeho IP adresa včetně portu, který byl třeba k individuální identifikaci. Facebookový profil uživatele Petra Horká byl policisty neustále monitorován, jakmile se zde objevila nějaká osoba, která byla v seznamu přátel nebo komentovala nějaký obrázek, byl ihned učiněn pokus tuto osobu ztotožnit dle dat uvedených na profilu Facebooku a s využitím policejních evidencí. Jedna z těchto osob byla Kristýna, roč. 1992. Ta byla jedna z mála dospělých osob, které pachatel kontaktoval prostřednictvím Facebooku a nebo která vyvinula nějakou aktivitu na jeho profilu. Kristýna souhlasila se spoluprací s policií, dala k dispozici svůj účet na Facebooku i se svým heslem. S pachatelem si v minulosti psala, jelikož jí žádal, aby mu zaslala nějaké své fotografie, což odmítla. Z účtu Kristýny byla na profil Petra Horká zaslána zpráva, ať se podívá na odkaz, že mu tedy posílá fotky, o kterých se dříve bavily s informací, že jsou uloženy na webovém úložišti. Ve zprávě byl

přiložen odkaz na stránku vytvořenou analytiky kriminální policie. Pachatel po nějaké chvíli na odkaz dvakrát klikl a tím byla zaznamenána jeho IP adresa i s portem. Další komunikace již nebyla z tohoto profilu s pachatelem vedena. Následně Obvodní soud Praha 3 dle § 88a odst. 1 trestního řádu vydal příkaz ke sdělení informací k těmto IP adresám, které spravuje stejná společnost jako v předchozím případě. Ta ačkoliv uvedla, že má data retention zprovozněn od prosince 2013, tak nastaven pro užívání byl systém až od února 2015, tudíž opět nebyl zjištěn uživatel. Toto pochybení poskytovatele internetového připojení bylo ze strany oddělení analytiky kriminální policie oznámeno na Český telekomunikační úřad jako porušení zák. č. 127/2005 Sb o elektronických komunikacích.

Poslední pokus o zjištění totožnosti pachatele byl prostřednictvím společnosti Seznam, kde byla založena emailová schránka k účtu Skype. Obvodní soud Praha 3 vydal opět příkaz dle § 88a odst. 1 trestního řádu, k tomu, aby společnost Seznam poskytla dostupné informace k emailu podezřelého. K věci bylo zjištěno, že účet je v systému spol. Seznam registrován, ale nemá aktivní emailovou schránku. Dále ve své odpovědi spol. Seznam uvedla, že s ohledem na nález Ústavního soudu ČR sp.zn. Pl ÚS 24/10, jímž došlo ke zrušení ust. § 97 odst. 3 a 4 zák. č. 127/2005 o elektronických komunikacích, nedisponuje provozně lokačními údaji o účtu, a tudíž je nemohla poskytnout.

Vzhledem k tomu, profil Petra Horká byl na sociální síti Facebook policisty neustále monitorován, podařilo se ztotožnit několik dívek, které vešly v kontakt s Horkou. K jejich ztotožnění bylo použito převážně veřejně dostupných informací na jejich profilech na Facebooku, jakými byla místa výskytu, oblíbená místa, škola, kroužky, přátelé, rodina, znamení zvěrokruhu a z těchto informací se následně vycházelo při zjišťování informací z policejních informačních systémů. Zjištěné dívky byly na profilu Horké jako přátelé nebo komentovaly nějakou fotografii, nebo se jim tato fotografie nebo příspěvek líbily. Bylo tedy dáno podezření, že jsou s Petrou Horkou v kontaktu, a že i po nich může požadovat zaslání jejich intimních fotografií. Profil Petra Horká se několikrát změnil, měnilo se zde jméno na Petruška, Peťulinka, ale příjmení Horká se neměnilo, stejně tak i několik fotografií v profilu. Tyto profilové fotografie byly nalezeny prostřednictvím vyhledávače obrázků Google na internetu na

profilu osoby registrované na jiné sociální síti. Pachatel tyto fotografie táhl z internetu a použil pro svůj falešný profil.

Vyhodnocením zjištěných skutečností bylo zřejmé, že pachatel pravděpodobně náhodně vybere nějakou mladou dívku a další už pak tipuje a vybírá z okruhu jejích přátel na Facebooku. Dívky, které byly touto cestou zjištěny a byly z Prahy, byly vyslechnuty policisty SKPV Praha III. Další mimopražské byly vyslechnuty policisty příslušných územních odborů k tomu, jak se s Horkou zkontaktovaly, zda po nich chtěla poslat intimní fotografie, zda po nich chtěla intimní videohovor prostřednictvím služby Skype. Z výslechů a dalších poznatku v trestním řízení bylo zjištěno, že všechna děvčata byla kontaktována ze strany Petry Horké stejnou první zprávou, kde píše, že je bohatá, že hledá kamarádku, které by kupovala dárky a chodila s ní na nákupy. V prvotní komunikaci nebyla žádná narážka se sexuálním podtextem. Některé z dívek vůbec neodpověděly a Horkou si zablokovaly, některé si chvíli psaly, Horká se snažila, aby s ní komunikovaly přes službu Skype. To některé z nich omítly, že jej nemají nainstalovaný. K věci byly vyslechnuty dívky z mnoha měst v České republice:

Praha

Aneta (roč. 2002) nejprve s Horkou nechtěla komunikovat, potom si s ní chvíli psala.

Adéla (roč. 2001) byla kontaktována na Facebooku Horkou, ale ona si s ní dále již nepsala.

Mariana (roč. 2001), nebyl nezjištěn žádný negativní poznatek.

Klára (roč. 2002) byla kontaktována Horkou, o které už věděla od spolužaček Anety a Adély, že jim píše, spolu s Horkou psaly, Horká jí nabízela peníze a společné nákupy.

Daniela (roč. 2000) byla kontaktována Horkou, která jí nabízela peníze a společné nákupy, Daniela si jí odstranila z přátel.

Daniela (roč. 2000) byla kontaktována Horkou přes Skype s nabídkou kamarádství, Horká po ní chtěla, aby se svlékla, potom s ní Daniela komunikaci ukončila.

Denisa (roč. 2013) byla kontaktována na Facebooku Horkou, nabízela jí, že s ní půjde nakupovat a koupí jí nějaké věci, pak si jí Denisa zablokovala.

Náchod

Kristýna (roč. 1992) dostala na Facebooku od Horké nabídku na přátelství, chvíli si psali, Horvátová jí nabízela peníze a že jí bude kupokovat věci, chtěla po neposlat fotografie pak si jí Kristýna zablokovala, Kristýna na fotografiích vypadala daleko mladší, než ve skutečnosti je, její profil byl použit ke kontaktování pachatele.

Eva (roč. 1988) dostala žádost o přátelství a na Facebooku okomentovala její fotografii, žádný další kontakt mezi nimi nebyl.

Kolín

Zuzana (roč. 1999) se s Horkou seznámila na portálu Lidé.cz, kde si psaly na chatu v místnosti s názvem Absolutní pokec pro lidi věku 12-20 let. Zuzana jí napsala, že je jí 13 let. Horká jí psala, že má hodně peněz a že jestli má Zuzana webkameru, tak si může vydělat peníze tím, že se bude před kamerou svlékat. Dále jí Horká nabízela peníze, pokud sežene holky okolo patnácti let, které budou ochotny se svléknout před kamerou.

Jindřichův Hradec

Ivana (roč. 2004) byla kontaktována Horkou na Facebooku s nabídkou přátelství a společných nákupů, chtěla po ní, aby komunikovaly přes Skype, dále komunikace skončila.

Hradec Králové

Monika (roč. 2001) uvedla, že si spolu psaly na Facebooku a pak na Skype, Horká po ní nechtěla žádné intimní fotografie, Monika uvedla další své spolužačky, na které Horké také dala kontakty.

Michaela (roč. 2000) vypověděla, že jí o Horké pověděla kamarádka Monika, ona sama s ní v kontaktu nikdy nebyla.

Lucie (roč. 2000) byla kontaktována na Facebooku Horkou, ale její nabídku na přátelství nepřijala, neznala jí a do výslechu uvedla, že se jí to zdálo celé divné.

Kristýna (roč. 2000) o Horké jí pověděla kamarádka Monika, ona sama s ní v kontaktu nikdy nebyla.

Hodonín

Denisa (roč. 2002) byla kontaktována zprávou na Facebooku od Horké, že hledá kamarádku, Denisa jí psala, že je jí 15 let, Horká po ní chtěla komunikace na Skype, Denisa si nainstalovala a vytvořila účet na Skype, Horká se jí ptala, jestli má webovou kameru, to Denisa neměla, Horká po ní chtěla poslat fotografie, kde bude oblečená ale

bez obličeje, to, co se jí stalo, pověděla Denisa své sestře a ta jí další komunikace s Horkou zakázala.

Karlovy Vary

Lucie (roč. 2003) uvedla, že jí přišla na Facebooku nabídka na přátelství od Horké, to odmítla, dále jí přišla zpráva na Facebooku na chat, že se s ní chce Horká seznámit, chtěla po ní komunikace na Skype.

Jičín

Viktorie (roč. 2000) uvedla, že Horkou nezná a nikdy s ní nekomunikovala na Facebooku.

Jitka (roč. 1999) dostala od kamarádky kontakt na Petru Horkou, tak si jí přidala do přátel, aby měla více přátel na profilu na Facebooku, Horká jí psala, že je bohatá, psala jí stále každý den, až jí to obtěžovalo, komunikaci pak ukončily, žádné fotky po ní Horká nechtěla

Jitka (roč. 2002) uvedla, že její kamarádka Viktorie jí navrhla Horkou jako kamarádku na Facebooku, Jitka si jí přidala, Horká jí psala, proč si jí přidala, Jitka jí odpověděla, že jí chtěla mít v přátelích, dál si už nepsaly.

Pavlín, (roč. 1999) vypověděla, že jí na Facebooku oslovila Horká, že hledá přátele, nabídla jí společné nákupy, nabízela jí peníze.

Profil Petra Horká a jeho následné různé verze Petruška, Peťulinka, nevyvíjel aktivitu a nakonec z Facebooku zmizel. Věc byla následně dne 16.12.2014 dle § 159a odst. 5 trestního řádu odložena, jelikož se nepodařilo zjistit konkrétního pachatele.

7.2 Druhé oznámení a šetření, Děčín, 2015

Dne 11.8.2015 oznámila na policejním oddělení v Děčíně Lucie Hanková, že si její dcera Marie (roč. 2003) na Facebooku píše s nějakou osobou, která má profil Petlinka Horká. Ta jí napsala, že by jí chtěla dát nějaké peníze za to, že spolu budou kamarádit, že budou spolu chodit nakupovat a že je strašně bohatá. Z komunikace mezi Marií a Petlinkou Horkou bylo zjištěno, že Marii nabízela mobilní telefon, peníze (200.000,-Kč) a další dárky, kdy za to požadovala od Marie její intimní fotografie. V komunikaci se zmiňuje o tom, že to pro ni zatím každá oslovená dívka udělala. Dále chtěla Petlinka po Marii, aby si nainstalovala Skype a komunikovala prostřednictvím webkamery. Ve věci byly policisty SKPV územního odboru Děčín dne 12.8.2015 zahájeny úkony v tr. řízení pro podezření ze spáchání přečinu zneužití dítěte k výrobě pornografie dle § 193 odst. 1 ve stádiu pokusu dle § 21 odst. 1 trestního zákoníku. Policisté SKPV Děčín následně v policejních informačních systémech zjistili souvislost s případem, kde vystupoval facebookový profil Petra Horká, který byl šetřena na SKPV Praha III. Profilová fotografie i další zveřejněné fotografie na obou profilech jsou totožné. Se souhlasem Lucie Hankové bylo provedeno ohledání a záloha facebookového profilu její dcery, kde byla zajištěna komunikace s Petlinkou Horkou. Z veřejně dostupných informací profilu Petlinka Horká byly zjištěny další dívky, které s ní komunikovaly. Několik z nich se podařilo ztotožnit. Ty byly následně vyslechnuty ve spolupráci s místně příslušnými odděleními kriminální policie na územních obvodech v různých městech republiky. Jednalo se o následující města:

Náchod

Lucie (roč. 1994) byla kontaktována Horkou s nabídkou kamarádství a nákupů, zdálo se jí to podezřelé, konverzaci ukončila.

Rokycany

Petra (roč. 2002) uvedla, že jí na Facebooku kontaktovala osoba s profilem Petlinka Horká letos v srpnu, psala, jí, že je bohatá, že hledá kamarádku, se kterou by šla na nákupy, slibovala jí dárky. Spolu pak komunikovaly přes webovou kameru, tam po ní chtěla Horká, aby se svlékla do naha, za to jí slíbila peníze a poslala jí fotku, kde byly na váze narovnané pětitisícové bankovky. Petra se pak před kamerou svlékla do naha a dále dělala to, co po ní Horká chtěla. Hladila si prsa a hladila se v rozkroku. Pak se na žádost Horké ještě nějakou dobu předváděla nahá před kamerou. Za to měla od

Horké slíbeno 300.000,- Kč, které ale nedostala. Fotografie bankovek na váze byla nalezena na internetu jako fotografie ze zpráv k policejnímu zátahu na producenty drog.

Olomouc

Milena (roč. 1985) uvedla, že si jí do přátel přidala Petlinka Horká protože si s ní chtěla promluvit o Petrovi Švagrovi. S Petrem Švagrem se seznámila Milena na internetové seznamce, spolu si nějakou dobu psali, to pak ale přestalo. Pak jí od Švagra přišla SMS, aby si přidala do přátel osobu Petlinka Horkou. Když to udělala, tak si s ní pak psala, Horká psala, že je kamarádka Švagra, že on je nešťastný, že už si spolu nepíší a nabízela jí peníze, když si dále budou psát.

Uvedené telefonní číslo bylo policisty ztotožněno jako číslo evidované na osobu Barbora Krnová, byt. Náchod. Tato žena má syna, který se jmenuje Radek Šmola, (roč. 1989) který žije na stejné adrese jako jeho matka. Rodina Krnová využívá internetové připojení od stejné společnosti jako pachatel s facebookovým profile Petra Horká. Vzhledem ke stylu komunikace a ke skutečnostem, které vedly ke kontaktu mezi Milenou, Petrem Švagrem a Horkou, vzniklo podezření, že za identitou Petra Švagra a Petlinky Horké se skrývá stejná osoba a že by mohlo jít o zmíněného Radka Šmolu. K Radkovi bylo zjištěno, že pracuje jako dělník v jedné náchodské firmě, má invalidní důchod a toto zaměstnání mu sehnala jeho matka, která ve firmě také pracuje. Radek Šmola žije sám v garsoniéře, která je vedle bytu jeho matky v panelovém domě na sídlišti v Náchodě.

7.3 Společné šetření SKPV Děčín a Praha III

V prověřování případu nadále probíhala spolupráce mezi SKPV Děčín a SKPV Praha III. Ke ztotožnění pachatele byly podniknuty kroky stejné jako v předchozím šetření ze strany SKPV Praha III. Od paní Lucie Hankové byl získán souhlas s použitím facebookového profilu její dcery Marie. Z tohoto profilu byl kontaktován profil Petlinka Horvátová, která chtěla, aby si Marie nainstalovala službu Skype. Na oddělení analytiky SKPV Praha III byla vytvořena opět webová stránka s php skriptem, aby byla zaznamenána IP adresa pachatele včetně portu připojení. Při konverzaci s pachatelem předstírali policisté, že nedokážou nainstalovat Skype a poslali pachateli odkaz na

stránku, kde měl být návod. Jednalo se o stránku s php skriptem a v jejím názvu byla obsažena slova „Skype“ a „návod“. Pachatel na odkaz klikl a na základě toho se podařilo zjistit IP adresu a port. Lustrací samotné IP adresy byl zjištěn poskytovatel internetu, jednalo se opět o stejnou firmu z Královehradeckého kraje jako v předchozím pražském případu. Okresním soudem v Děčíně byl vydán příkaz ke sdělení údajů o uskutečněném telekomunikačním provozu dle § 88a odst. 1 trestního řádu. Na základě tohoto příkazu byla dle informací o portu a IP adrese zjištěna osoba Zdeněk Bikař (roč. 1943) bytem Hronov, který má syna Daniela (roč. 1972). Ten je svobodný a s rodiči žije v jedné domácnosti v Hronově. K těmto osobám nebyly zjištěny v policejních databázích žádné negativní poznatky.

Na základě zjištěných poznatků byli vytipováni dva možní pachatelé. Na základě IP adresy a portu Daniel Bikař. Na základě své předchozí komunikace Radek Šmola. V listopadu 2015 byla provedena společná akce policistů SKPV Děčín a SKPV Praha III. Účelem bylo současně předvést k výslechu oba podezřelé, provedení výslechu bylo připraveno na policejním oddělení v Hronově, kde byly pro tento účel nachystány dvě kanceláře a oba dva podezřelí měli být vyslýcháni v oddělených místnostech, ale současně. Policisté SKPV Děčín provedli ráno v půl sedmé šetření u Daniela Bikaře, kterého vyzvali, aby je následoval k podání vysvětlení, což on dobrovolně učinil. Současně s tím policisté SKPV Praha III navštívili ráno v šest hodin pracoviště Radka Šmoly, kde jej také vyzvali k podání vysvětlení a i on je dobrovolně následoval k provedení výslechu. Oba dva muži byli poté převezeni na policejní oddělení v Hronově, kde byli umístěni odděleně do dvou kanceláří, aniž by se vůbec potkali. Oba dva byli současně vyslechnuti k facebookovému profilu Horká. Bikař popřel, že by měl s tímto profilem něco společného a Šmola se pod tíhou důkazů a argumentů policistům nakonec přiznal, že profil Horvátová založil on. Během výslechu se neprokázalo se, že by se oba dva muži znali.

Vzhledem k tomu, že byla zjištěna IP adresa i příslušný port, na základě kterého byl ztotožněn jako uživatel p. Bitnar, byla tato skutečnost dále prověřena policisty oddělení analytiky SKPV Praha III. K věci bylo zjištěno, že se jednalo o technický problém v logování přístupu ze strany poskytovatele připojení.

Šmola během výslechu uvedl, že ve svém bytě bydlí sám, přítelkyni nemá, pracuje asi pět měsíců jako dělník. Je vystudovaný kuchař, před tím pracoval v chráněné

dílně. Má plný invalidní důchod třetího stupně. Neměl nikdy problémy psychického rázu, nikde se neléčil s psychickými problémy, občas pije alkohol, ale pouze příležitostně. Příležitostně také kouří marihuanu, asi tak jednou až dvakrát do měsíce. Kouří i cigarety. Užívá telefonní číslo, které je psané na jeho matku, používá jej on sám, ale občas z něho napíše nějakou zprávu někdo z kamarádů. Jedná se číslo, které již bylo policistům známo z předchozího šetření. Doma má Šmola notebook, na internet je připojen přes wi-fi od rodičů, kteří mají doma pevné připojení. Wi-fi není zabezpečená heslem. Na Facebooku má Šmola profil pod svým jménem, který je spojen i s výše uvedeným telefonním číslem. Na Skype aktivní profil pod svým jménem nemá.

Asi před půl rokem si založil profil na serveru Líbímseti.cz. Tam vystupoval jako Petr Švagr z Prahy, věk asi 28 nebo 29 let. V nějaké chatovací místnosti se seznámil s dívkou. Spolu si psali denně asi tři nebo čtyři měsíce. Vyměnili si na sebe i telefonní čísla. On si s ní již po nějaké době psát nechtěl, ale ona mu začala psát, že ho miluje. Napsal jí tedy, ať si přidá na Facebook do přátel Petlinku Horkou. To udělal proto, že si s ní chtěl psát jako někdo jiný, aby zjistil, jaký má na něho názor.

Asi před dvěma lety na Facebooku vytvořil falešný profil Petra Horká. Jednalo se o profil dívky, fotky našel na internetu. Na tento profil se připojoval pouze z domova ze svého notebooku. K tomuto profilu vytvořil nový email. Tím, že zapomínal heslo k přístupu na tento profil, tak jej musel často měnit. Proto docházelo i ke změnám jména profilu, Petra, Petruška, Peťulinka, Petlinka. Příjmení Horká ale stále zůstávalo stejné. Petlinka Horká byla poslední změna profilu. K facebookovému profilu vytvořil Šmola i profil na Skype. Tento profil používal jen k tomu, aby se seznamoval s dívkami. Uvedl, že vzhledem ke svému zdravotnímu stavu má problémy se seznámit s dívkou a tento způsob, kdy oslovoval mladá děvčata, mu připadal jako jednoduchý k seznámení. Dívky si vybíral náhodně, jak se dostal k jedné, tak pak z okruhu jejích přátel vybíral další. Kontaktoval je všechny stejným způsobem, napsal o sobě, že je bohatá dívka a že hledá kamarádku, které může koupit různé věci, jako jsou třeba telefony, popřípadě jí dát peníze. Když dívka zareagovala, tak si s ní chvíli psal. Pak se jí snažil nasměrovat na Skype, aby mu pak následně prostřednictvím webové kamery poslala své fotografie nebo video. Šmola měl kameru a mikrofon při komunikace vypnutý, nebylo poznat, že není dívka, za kterou se vydává. S dívkou komunikoval prostřednictvím psaných zpráv. Nejprve chtěl, aby se mu dívka ukázala ve spodním

prádle, pak chtěl, aby se postupně svlékala do naha. Když mu přišla fotografie, tak si jí uložil do stažených souborů, měl jí tam chvíli, a pak fotku smazal. Videa dívek si nenahrával, pouze se na ně díval. Dívky se s ním spíše spojovaly prostřednictvím web kamery přes službu Skype, než aby mu posílaly fotografie. Když byly dívky připojeny přes kameru, tak jim psal zprávy, ve kterých je navigoval a instruoval, co mají dělat. Psal jim, co si mají svléknout, jak si mají stoupnout, jak se mají ukázat. Nikdy žádné z těch dívek za to nic nedal. I přes to si s několika dívkami psal vícekrát a vícekrát se mu na kameře ukazovaly.

Šmola uvedl, že oslovoval dívky ve věku od 12 let výše. Tvrdil, ale zároveň, že to byly převážně dívky starší 18 let, což ze zjištěných profilů, které kontaktoval, nebyla pravda. Nezletilé si vybíral hlavně proto, že ty starší by mu nevěřily. Uvedl, že jej nezletilé dívky sexuálně nevzrušují, při sledování fotek nebo videa nemasturboval, ale připadalo mu to s těmito mladými dívkami všechno jednoduší. Uvedl, že se stydí za svůj vzhled i za své postižení a neumí navázat fyzický kontakt s dívkou. Proto na sociálních sítích a seznamkách vystupoval pod cizí identitou a hledal tak nějakou známost, se kterou by mohl prostřednictvím internetu komunikovat. Uvedl, že chtěl vidět dívky ve spodním prádle, nechtěl je ale vidět nahé. Na dotaz policistů, proč po nich tedy chtěl, aby se svlékaly a hladily se po nahém těle, nedokázal odpovědět. Několikrát během rozhovoru s policisty zdůrazňoval, že přeci není žádný pedofil.

Šmola byl vyzván k vydání notebooku, což dobrovolně učil a dále dobrovolně poskytl policii zálohu svého facebookového profilu, což bylo také zadokumentováno. Po celou dobu s policí spolupracoval. Pro případ, že by Šmola odmítl notebook vydat, byla již dopředu domluvena spolupráce se státním zástupcem, který by vydal příkaz k odnětí věci, popř. by byl jeho prostřednictvím podán návrh soudu k vydání příkazu provedení domovní prohlídky. Vzhledem k osobě podezřelého, který neměl žádnou trestní minulost, byl předpoklad, že bude ve věci spolupracovat a nebude dělat žádné problémy, což se také potvrdilo.

Spisový materiál vedený na kriminální policii v Děčíně byl postoupen na kriminální policii do Prahy, kde došlo ke kompletaci celého spisu, který byl následně postoupen na kriminální policii v Náchodě a to vzhledem k tomu, že zde došlo k jednání pachatele, zde se připojoval k internetu a z místa svého bydliště komunikoval s poškozenými.

7.4 Vyhodnocení případu

Na chování Radka Šmoly jsou patrné klasické prvky kybergroomingu. Vytvořil si pro seznamování jinou identitu, pod kterou na internetu vystupoval při kontaktování nezletilých dívek. Fotografie pro svůj falešný profil použil z jiné sociální sítě. K tomu, aby dívky přesvědčil a dosáhl svého cíle, jim sliboval peníze a dárky. Aby je ještě více motivoval, tak jim posílal fotografie telefonů nebo balíčků bankovek. Opět se jednalo o fotografie, které našel a stáhl z internetu. K ověření pravosti by bývalo obětem stačilo, kdyby na zaslanou fotografii použily vyhledávač obrázku a ihned by se jim zobrazily originální webové stránky, kde byly fotografie publikovány původně. Žádná z dívek to ale neudělala.

Oběť si pachatel vybral náhodně podle profilu na internetu. U tohoto profilu ale věděl, nebo dle fotografií a dostupných informací mohl poznat, že se jedná o nezletilou dívku. Z jejího okruhu si pak vybral další oběti. Pokud by dívky měly své profily lépe zabezpečené a neměly seznam svých přátel jako veřejnou informaci, pachatel by měl svojí činnost těžší. Takhle jedna dívka viděla, že její kamarádka má v přátelích stejnou osobu, tak si jí také přidala mezi své přátele. Ačkoliv to Šmola ve výslechu popřel, je zřejmé, že se zajímá o mladé dospívající dívky. Jeho sexuální preference bude ale muset posoudit sexuolog.

ZÁVĚR

Tak, jak se vyvíjí svět informačních technologií, vyvíjí se i zločin. Podsvětí dokáže využívat moderní technologie, protože mu to přináší jednodušší způsoby, jak dosáhnout svého cíle a zisků. Tomu se musí přizpůsobit i složky, které proti těmto negativním jevům bojují. Tato práce poukázala na to, že boj s tímto druhem kriminality nelze dělat jen na národní úrovni pouze v působnosti státního aparátu jedné země. Důležitá je v globálním světě mezinárodní spolupráce a spolupráce státních institucí s neziskovými organizacemi a nadacemi. Důležitá je činnost Interpolu a Europolu, díky které mohou různé země spolupracovat a sdílet informace, které usnadňují odhalování počítačové trestné činnosti páchané na dětech. Významné je i přispění firem, které části svých zisků investují právě do boje s touto kriminalitou a do preventivních programů. Projekt Web Rangers společnosti Google je dobrou ukázkou moderního přístupu k prevenci, kdy firma, která vydělává peníze díky internetu, část svých zisků zase vrací zpět, aby byl internet bezpečnější.

Problematické je rizikové chování samotných dětí, které je spojeno právě s jejich důvěřivostí a malou počítačovou gramotností. Riziková chování v sobě zahrnují hlavně poskytování osobních dat, jako jsou jména, adresy, telefonní čísla, emaily, dále pak odesílání nebo sdílení vlastních fotografií se sexuální tématikou, chatování s cizími lidmi na sexuální témata, dostavení se na schůzku s cizím člověkem, kterého dítě poznalo právě na internetu. Stejně rizikově se ale mohou chovat i rodiče, kteří si ani neuvědomí následky svého počínání a soukromá data nebo intimní fotografie svých dětí sami zveřejní. Takovým příkladem je stránka rajce.net. Jedná se o databázi fotografií. Je zde plno fotoalb z dovolených, kde jsou fotografie malých nahých nebo polonahých dětí na plážích nebo koupajících se ve vaně. Rodičům tyto fotografie připadají roztomilé, uloží je na server, aby se na ně mohli příbuzní podívat. Alba nejsou nijak chráněna heslem, jsou volně přístupná. Vyskytuje se zde plno uživatelů, kteří nemají žádná vlastní alba, ale hojně komentují fotografie nahých malých dětí. V tomto případě se nejedná o dětskou pornografii, ale dali by tito rodiče fotografii svého nahého dítěte cizímu člověku na ulici, kdyby je o to požádal? Domnívám se, že ne Chovejme se zodpovědně a nedělejme to útočníkům jednodušší. To je ta nejjednodušší prevence.

SEZNAM POUŽITÝCH ZDROJŮ

Seznam použitých českých zdrojů:

BLATNÍKOVÁ, Šárka. *Sexuální vykořisťování jako forma závažné organizované kriminality.* 1. vyd. Praha: Institut pro kriminologii a sociální prevenci, 2010, ISBN 978-807338-103-5

ČÍRTKOVÁ, Ludmila. *Forenzní psychologie*. 2. vyd. Plzeň: Aleš Čeněk, 2009, ISBN 978- 80-7380-213-4.

HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. 1. vyd. Praha: Triton, 2012, ISBN 978-80-7387-545-9.

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

JELÍNEK, Jiří. a kol. *Trestní zákoník a trestní řád s poznámkami a judikaturou*. 2. vyd. Praha: Leges, 2011, ISBN 978-80-87212-99-8.

KOPECKÝ, Kamil a Veronika KREJČÍ. *Rizika virtuální komunikace: (příručka pro učitele a rodiče)*. Olomouc: NET UNIVERSITY s.r.o., 2010. ISBN 978-80-254-7866-0.

MAŠKOVÁ, Anna, Kateřina LUKÁŠOVÁ, Rastislav PACÁK a Jana BRANDEJSOVÁ. *Kybergrooming a kyberstalking: Metodický materiál pro pedagogické pracovníky*. Národní centrum bezpečnějšího internetu, 2012.

MILFAIT, René. *Komerční sexualizované násilí na dětech*. Praha: Portál, 2008, ISBN 978-80-7367-320-8

ŠÁMAL, Pavel. a kol. *Trestní zákoník I. § 1 až 139. Komentář*. 1. vyd. Praha: C.H.Beck, 2009, ISBN 978-80-7400-109-3.

Seznam použitých internetových zdrojů:

7 lekcí, které z tebe udělají mistra internetové bezpečnosti. *Seduo.cz* [online]. Ptraha: LMC s.r.o., 2016 [cit. 2016-02-13]. Dostupné z: http://www.seduo.cz/7-lekci-ktere-z-tebe-udelaji-mistra-internetove-bezpecnosti

Background: History of Eurojust. *EUROJUST: The European Union's Judicial Cooperation Unit* [online]. Den Haag: Eurojust, 2016 [cit. 2016-02-22]. Dostupné z: http://www.eurojust.europa.eu/about/background/Pages/History.aspx

Being a webcamsexgirl is terrifying. *Terre des hommes* [online]. Den Haag: Terre des Hommes Nederland, ©2015 [cit. 2015-12-02]. Dostupné z: https://www.terredeshommes.nl/en/being-webcamsexgirl-terrifying

BERSON, Illene. *Grooming Cybervictims: The Psychosocial Effects of Online Exploitation for Youth* [online]. University of South Florida. USA. Dostupné z: http://www.cs.auckland.ac.nz/~john/NetSafe/I.Berson.pdf, citováno dle KOPECKÝ, Kamil. *Kybergrooming: Nebezpečí kyberprostoru* [online]. Olomouc: NET UNIVERSITY s.r.o., 2010, ISBN 978-80-254-7573-7 [cit. 2015-11-28]. Dostupné z: http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=5:kybergrooming-studie

Combating Cybercrime in a Digital Age. *Europol.eu* [online]. The Hague: Europol, 2016 [cit. 2016-02-13]. Dostupné z: https://www.europol.europa.eu/ec3

Dokumenty. *United Nations: Information Centre Prague, Informační centrum OSN v Praze* [online]. Praha: UNIC Praha [cit. 2016-02-13]. Dostupné z: http://www.osn.cz/knihovna/dokumenty/osn/

ESCRITT, Thomas a Kevin LIFFEY (ed.). Dutch activists track alleged child abusers with help of digital "girl". *Reuters.com* [online]. New York: Thomson Reuters, ©2013 [cit. 2015-12-02]. Dostupné z: http://www.reuters.com/article/2013/11/04/us-dutch-childabuse-idUSBRE9A30QQ20131104#SIErBYpaEmwuBRyb.97

European Financial Coalition against Commercial Sexual Exploitation of Children Online [online]. Bruxelles, 2016 [cit. 2016-02-13]. Dostupné z: http://www.europeanfinancialcoalition.eu

Global efforts to identify child abuse victims via INTERPOL boosted with Microsoft technology. In: *Interpol.int* [online]. Singapore: Interpol, 2015 [cit. 2016-02-13]. Dostupné z: http://www.interpol.int/News-and-media/News/2015/N2015-041

Jsem pedofil: Mohu to vůbec říct nahlas? – 2. část. *Superrodina.cz* [online]. 2012 [cit. 2016-02-14]. Dostupné z: http://www.superrodina.cz/2012/05/23/jsem-pedofil-2/

Národní centrum bezpečnějšího internetu [online]. Praha: Národní centrum bezpečnějšího internetu, 2012 [cit. 2016-02-13]. Dostupné z: http://www.ncbi.cz

New software recognized potential pedophiles online. *Tilburg University: understanding society* [online]. Tilburg: Tilburg University, ©2015 [cit. 2015-12-02]. Dostupné z: https://www.tilburguniversity.edu/current/news/press-release-new-software-recognizes-potential-pedophiles/

Projekt Web Rangers 2.0: Nejlepší projekty zaměřené na bezpečné chování teenagerů na internetu. *E-bezpečí.cz* [online]. Olomouc: Centrum PRVoK PdF, Univerzita Palackého v Olomouci, 2015 [cit. 2016-02-13]. Dostupné z: http://www.e-bezpeci.cz/index.php/tiskove-zpravy/971-webrangers2-nejlepsi-projekty

Sweetie: The face of webcam child sex tourism. In: *youtube*[online]. 7.9.2015 [vid. 2015-29-11]. Kanál uživatele sweetie. Dostupné z: https://www.youtube.com/watch?v=yWLTEkryAQg

Victim identification. *Interpol.int* [online]. Lyon: Interpol, 2016 [cit. 2016-02-13]. Dostupné z: http://www.interpol.int/Crime-areas/Crimes-against-children/Victim-identification

Videa a dokumenty. *Bezpecnyinternet.cz* [online]. 2013 [cit. 2016-02-13]. Dostupné z: http://www.bezpecnyinternet.cz/ke-stazeni/bezpecny_internet_prezentace.pdf
Web Rangers: Bojujeme za bezpečnější internet [online]. Google, 2016 [cit. 2016-02-13]. Dostupné z: http://www.webrangers.cz/

Seznam ostatních použitých pramenů:

Zákon č. 40/2009 Sb, trestní zákoník. In: Sbírka zákonů. 2009, s. 354-463. ISSN 1211-1244. Dostupné ze www.mvcr.cz/soubor/sb011-09-pdf.aspx

BIBLIOGRAFICKÉ ÚDAJE

Jméno autora: Tomáš Zemín

Obor: Bezpečnostní studia

Forma studia: kombinované studium

Název práce: Mravnostní počítačová kriminalita páchaná na dětech

Rok: 2016

Počet stran textu bez příloh: 54

Celkový počet stran příloh: 0

Počet titulů českých použitých zdrojů: 9

Počet titulů zahraničních použitých zdrojů: 0

Počet internetových zdrojů: 15

Počet ostatních zdrojů: 1

Vedoucí práce: Ing. Michaela Melicharová