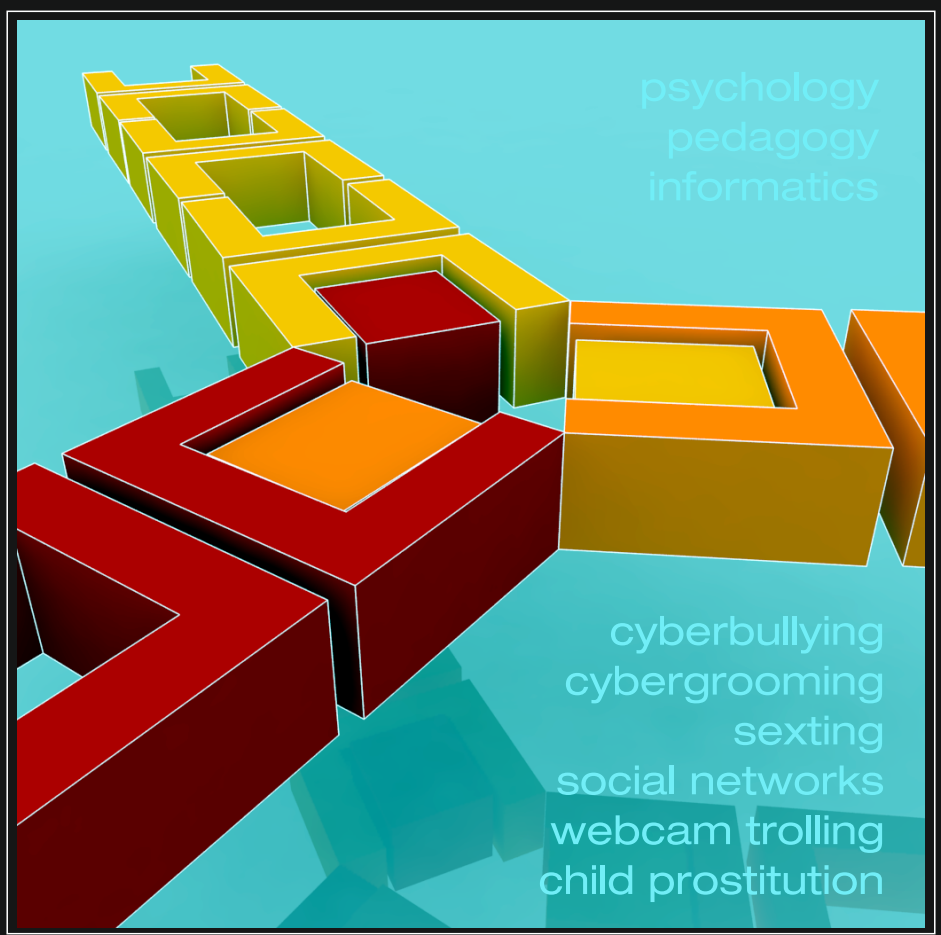


RIZIKOVÉ FORMY CHOVÁNÍ ČESKÝCH A SLOVENSKÝCH DĚTÍ V PROSTŘEDÍ INTERNETU

Kamil Kopecký a kol.

Univerzita Palackého v Olomouci
Pedagogická fakulta
Centrum prevence rizikové virtuální komunikace

RIZIKOVÉ FORMY CHOVÁNÍ ČESKÝCH A SLOVENSKÝCH DĚTÍ V PROSTŘEDÍ INTERNETU

Kamil Kopecký a kol.

Olomouc 2015

Oponenti:
doc. PaedDr. Ludvík Eger, CSc.
doc. PhDr. Hana Marešová, Ph.D.

Kolektiv autorů:
Mgr. Kamil Kopecký, Ph.D.
PhDr. René Szotkowski, Ph.D.
Mgr. Veronika Krejčí

Tato publikace vznikla za přispění výzkumného záměru Pedagogické fakulty Univerzity Palackého v Olomouci:
Od subjektivní implicitní teorie edukace k pedagogické znalosti. Proces konstituování kognitivního rámce věd o výchově v národním a mezinárodním kontextu.

1. vydání

ISBN 978-80-244-4868-8 (online : PDF)
ISBN 978-80-244-4861-9 (print)

DOI 10.5507/pdf.15.24448619

Obsah

1 Slovo úvodem

Internet je médium, jehož růst a proměny neustále pokračují. V současnosti internet představuje pravděpodobně nejdůležitější nástroj, prostřednictvím kterého spolu každodenně lidé komunikují. Stejně, jako se vyvíjí internet samotný, vyvíjejí se i způsoby komunikace, které využívají dospělí, ale také dětští uživatelé internetu.

V nedávném testování počítačové gramotnosti International Computer and Information Literacy Study (Fraillon, Ainley, Schulz, Friedman, & Gebhardt, 2014) obsadili čeští žáci přední příčky – v testu byli dokonce nejlepší na celém světě. Na dalších místech se umístila Kanada, Austrálie, Polsko, Norsko, Korejská republika a další země. Zajímavé je, že výsledky studie naznačují, že většinu potřebných dovedností se žáci naučili mimo školu (Brdička, 2014) – zejména doma.

Je tedy zřejmé, že děti využívají počítač velmi aktivně a aktivně také využívají internet a internetové služby. Ne vždy se však v kyberprostoru chovají bezpečně. Cílem naší publikace je představit čtenářům rizika, kterým jsou v prostředí internetu české a slovenské děti vystaveny, a navrhnout řešení, která umožní tato rizika účinným způsobem snížit.

Publikace *Rizikové formy chování českých a slovenských dětí v prostředí internetu* shrnuje výsledky tří výzkumů, realizovaných Centrem prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci v průběhu let 2014 a 2015. Konkrétně jde o výzkumy *Nebezpečí internetové komunikace 5* a *Rizikové chování slovenských dětí v prostředí internetu*, které se orientují na prevalenci rizikového chování spojeného s rizikovými formami komunikace v dětské populaci, a o studii *Analýza komunikace českých dětí a online predátorů*, která zkoumala, jaké komunikační strategie volí internetoví predátoři v rámci online útoků.

2 Úvod do problematiky

Internet a internetové služby jsou součástí každodenní komunikace dětí a dospělých uživatelů internetu – internet je pro ně zdrojem zábavy, poznání, zdrojem informací všeho druhu, prostředkem pro komunikaci s vrstevníky, ale také zcela neznámými uživateli internetu.

Internetová komunikace je velmi specifická – probíhá ve virtuálním prostředí, ve kterém nelze realizovat komunikaci se zachováním všech potřebných verbálních i neverbálních složek. S internetovou komunikací se pojí celá řada procesů, které zásadním způsobem ovlivňují jak obsah, tak i formu samotného internetového sdělení. Mezi nejvýznamnější procesy, které online komunikaci provázejí, patří tzv. *online disinhibiční efekt*.

Termíny disinhibice a disinhibiční efekt označují *odložení zábran a skrupulí, ztrátu nebo překonání nesmělosti, plachosti a ostychu, v krajních podobách může jít o obcházení tabu a zákazů, tedy o jistou odvázanost či nevázanost na normy, která může být až anomální* (Vybíral, 2005). Mezi další znaky patří např. *zvýšená zvědavost, pudové chování, impulsivní rozhodování, povolení uzdy exhibicionismu, odklon od reality a útěk do fantazií* apod. (Vybíral, 2002).

Následkem disinhibice pak lidé v internetovém prostoru sdělují velmi intimní a důvěrně informace o své osobě a tzv. odkládají zábrany. Odkládání zábran v online komunikaci může mít jak pozitivní, tak negativní vliv na komunikaci, v řadě případů pak vede k různým formám rizikové komunikace (trolling, flaming, kyberšikana, kybergrooming apod.).

Disinhibiční efekt vychází z šesti hlavních zdrojů (Suler, 2004):

1. *Anonymita („You Don`t Know Me" – Neznáš mě)* – Ti, kteří svou identitu skrývají pod přezdívkami a jsou do jisté míry chráněni před identifikací, mohou libovolně projevovat své názory, realizovat své sociální potřeby a ovlivňovat své komunikační partnery, bez dalších následků a jakéhokoliv postihu.

2. *Neviditelnost („You Can`t See Me" – Nevidíš mě)* – Komunikující navzájem nevidí, jak se druhý tváří, jakou má mimiku ve tváři nebo jak vypadá. Absence nonverbálních znaků komunikace je pak v komunikaci nahrazována grafickými symboly (emotikony) či různými akronymy (LOL, ROFL apod.).

3. *Asynchronicita („See You Later" – Tak příště)* – Nesoučasnost v komunikaci. Uživatel má možnost promyslet si svou odpověď, neboť nemusí reagovat pohotově jako při komunikaci v reálném světě.

4. *Solipsistická introjekce („It`s All in My Head" – Vše je v mé hlavě)* – Solipsimus je termín vyhrazený ve filozofii pro *přesvědčení člověka o tom, že vnější svět existuje jenom v jeho hlavě*. (Vybíral, 2005) Absence komunikace tváří v tvář může mít vliv na lidskou mysl, která podvědomě přiřazuje vizuální obraz, jak daný člověk vypadá a jak se chová, člověku, se kterým komunikujeme, na základě čtení psaného textu. Člověk si tak vytváří vlastní představu o jeho podobě, a to na základě svých potřeb, přání a očekávání. Ve skutečnosti pak komunikuje z části sám se sebou, realita se stává fantazií. Dominace našich vlastních představ při utváření představy o světě či člověku neboli solipsismus je v našich vztazích odjakživa a zcela přirozeně (Kovářová & Kopecký, 2012; Vybíral, 2005).

5. Disociativní představivost („It`s Just a Game" – Je to jen hra) – Nulová zodpovědnost. Někteří uživatelé internetu považují své internetové Já, postavu, kterou vytvořili v kybersvětě, za někoho jiného, tak proč za ni nést zodpovědnost v reálném světě. Vše považují za hru, která končí, jakmile vypnou počítač.

6. Minimalizace autority („We`re Equals – Jsme si rovni) – Na internetu se smazávají naše reálné společenské role, je nepodstatné, jaké má kdo postavení a sociální status.

Disinhibice je jedním z nejzjevnějších a nejspecifičtějších znaků elektronické komunikace jak u pubescentů a adolescentů, tak i u velkého množství dospělých. Je zjevné, že disinhibiční efekt je průvodním znakem celé řady jevů spadajících do oblasti rizikového chování na internetu, doprovází kyberšikanu, kyberstalking, sexting, kybergrooming, dětskou prostituci a další související fenomény.

2.1 Kyberšikana

2.1.1 Definujeme kyberšikanu

Definice termínu kyberšikana vychází z existujících definic tzv. tradiční šikany, v nichž je vnímána jako *agresivní, úmyslné, opakované jednání či chování prováděné vůči jednotlivci či skupině, který/á se nemůže snadno bránit* (Olweus, 1993; Whitney & Smith, 1993). Olweus však také upozorňuje, že je nutné rozlišovat mezi agresí a šikanou. Agresi vnímá jako jednorázovou záležitost, zatímco šikana je jev opakovaný, charakteristický právě nevyvážeností sil mezi agresorem a obětí.

Dalšími autory je pak šikana chápána jako *forma obtěžování založeného na nerovnováze sil a systematickém zneužívání moci* (Rigby, 1997; Smith & Sharp, 1994). V českém prostředí šikanu definuje zejména Kolář, který šikanování vymezuje jako *chování, při kterém jeden či více žáků úmyslně, většinou opakovaně týrá a zotročuje spolužáka či spolužáky a používá k tomu agresi a manipulaci* (Kolář, 2011).

Termín kyberšikana pak na tato vymezení logicky navazuje a rozšiřuje je o další specifika (zejména ve spojení s ICT). Konkrétnější vymezení kyberšikany uvádějí Hinduja a Patchin (Hinduja & Patchin, 2008) a Dehue, Bolman, Völlink, Pouwelse (Dehue, Bolman, Völlink, & Pouwelse, 2009). Hinduja a Patchin kyberšikanu definují jako *záměrnou, opakovanou a zraňující činnost využívající počítač, mobilní telefon a jiné elektronické přístroje*. Dehue, Bolman, Völlink, Pouwelse (Dehue et al., 2009) kyberšikanu popisují jako *týznění, hrozby, ponižování, ztrapňování nebo jiné útoky mezi mladistvými za pomocí internetu, interaktivních a digitálních technologií nebo mobilních telefonů*.

Pro potřeby našeho výzkumu jsme kyberšikanu vymezili s využitím zahraničních definic jako *formu agrese, která je realizována vůči jedinci či skupině s použitím informačních a komunikačních technologií a ke které dochází opakovaně* (Belsey, 2004; Smith et al., 2008), ať už ze strany původního agresora či tzv. sekundárních útočníků. A jak dodávají Kowalski, Limber a další (Kowalski, Limber, & Agatston, 2008), jde o *šikanování, k němuž dochází prostřednictvím e-mailů, ICQ, mobilních telefonů (SMS, MMS, telefonátů), chatu, webových stánek a jiných ICT*.

2.1.2 Kyberšikana vs. online obtěžování

Při zkoumání výsledků českých i zahraničních výzkumů (např. výzkumy EU Kids Online II, COST, NIK3-5 apod.) narazíme na velmi rozdílné výsledky incidence kyberšikany v dětské populaci, podle některých výzkumů

např. prevalence kyberšikany dosahuje 6 % (EU Kids Online II), podle jiných výzkumníků až 70 % (Juvonen & Gross, 2008). Tyto mnohdy až propastné rozdíly jsou způsobeny zejména různými definicemi kyberšikany a rozdílným vnímáním jednotlivých forem a projevů kyberšikany, které oběti či útočníci prožívají. Např. ve výzkumu EU Kids Online II (Černá, Dědková, Macháčková, Ševčíková, & Šmahel, 2013) se na kyberšikanu výzkumníci dotazují takto:

Děti nebo mladiství někdy někomu říkají nebo dělají sprosté nebo zraňující věci, což se může opakovat i několikrát v několika dnech. Může to zahrnovat:

a) škádlení někoho stylem, který nemá rád,
b) bití, kopání nebo strkání do někoho,
c) odvrhování někoho.

Když se někdo takto chová, může to být:
a) tváří v tvář (osobně),
b) přes mobilní telefon (texty, hovory, videoklipy),
c) přes internet (e-mail, komunikační aplikace, sociální sítě, chatovací místnosti).

Choval se k tobě někdo v POSLEDNÍCH DVANÁCTI MĚSÍCÍCH sprostě nebo zraňujícím způsobem? Stalo se ti něco takového na internetu za posledních dvanáct měsíců? (Černá et al., 2013)

Na základě výše uvedené definice se v ČR objevuje kyberšikana u 8 % dětí. Takto vymezená definice však pokrývá velmi malé množství jevů, které do oblasti kyberšikany spadají a které odpovídají základním kritériím pro odlišení kyberšikany a tzv. online obtěžování (např. online vydírání a vyhrožování, šíření ponižujících informací, videozáznamů a fotografií apod.). S těmito "projevy kyberšikany" již běžně pracuje řada zahraničních výzkumníků (USA, Belgie, Kanada, Německo), kteří např. měří incidenci případů *opakovaných nadávek a urážek, krádeže hesel s následným vniknutím na účet a poškozením oběti, vyhrožování, sdílení soukromé komunikace, šíření pomluv* apod. (Juvonen & Gross, 2008; Vandebosch & Van Cleemput, 2009). Vzhledem k tomu, že však do svých výstupů tito výzkumníci zahrnují projevy a formy kyberšikany, které byly v průběhu roku zaznamenány minimálně jednou, opět dochází ke zkreslení výsledků, neboť mezi základní znaky kyberšikany patří opakovanost jevu.

Nejednotné definice vedou k tomu, že je kyberšikana často zaměňována s tzv. online obtěžováním. Termínem online obtěžování označujeme

jednorázové útoky, které nezanechávají u obětí prakticky žádné nepříjemné pocity (Černá et al., 2013). „Opravdová“ kyberšikana musí splňovat zejména kritéria opakovanosti, musí být dlouhodobá a musí být vnímána jako ubližující.

Pro označení jednorázového útoku se také využívají termíny kyberútok či kyberobtěžování, které však nezanechávají vážné důsledky a lze je snadno zastavit, např. blokací závadného obsahu, nahlášením pachatele apod. V rámci těchto typů útoků jsou síly útočníka a oběti vyrovnané (Janis Wolak, Finkelhor, Mitchell, & Ybarra, 2008).

2.1.3 Výzkum kyberšikany v Evropě a USA

Výzkumy kyberšikany probíhají v posledních letech velmi intenzivně v řadě zemí z celého světa. Výzkumníci z USA (Brown, Demaray, & Secord, 2014) např. upozorňují, že u kyberšikany nezáleží na rozdílech u pohlaví (dívky nejsou častěji oběťmi kyberšikany než chlapci).

Další výzkumníci z Kanady (Beran & Li, 2007) upozorňují na propojení kyberšikany a tradiční šikany, přičemž jejich výzkum odhaluje, že 1/3 obětí kyberšikany byla současně oběťmi tradiční školní šikany. Další výzkumníci z USA upozorňují na fenomén přepínání rolí, kdy se oběti šikany či kyberšikany stávají agresory (Ybarra & Mitchell, 2004).

Zajímavá studie realizovaná na vzorku 10 008 osob ve věku 13–22 let z Velké Británie, USA a Austrálie (Ditch The Label, 2013) upozorňuje na to, že 7 z 10 dětí se stalo obětí kyberšikany, přičemž 20 % zažívá kyberšikanu denně. Podle této studie jsou pro kyberšikanu nejčastěji využívány sociální sítě Facebook, Ask.fm a Twitter.

Tab 1. Výskyt kyberšikany na vybraných sociálních sítích (Ditch The Label, 2013)

Sociální síť	***Oběti kyberšikany (%)***
BEBO	14,00
YOUTUBE	21,00
TUMBLR	22,00
INSTAGRAM	24,00
ASK.FM	26,00
TWITTER	28,00
FACEBOOK	54,00
MYSPACE	89,00

Riebel, Jäger a Fisher (Riebel, Jäger, & Fischer, 2009) z Německa potvrzují, že se také u německých dětí objevuje kyberšikana. Podle nich kyberšikanu prožilo 5,4 % dětí (a to opakovaně), občasné incidenty spojené s jednotlivými projevy kyberšikany potvrdilo 14,1 % respondentů.

V roce 2012 proběhl v Evropě výzkum závislostního chování dětí, který se věnoval také kyberšikaně (Tsitsika, Janikian, Mavromati, Tzavela, & Consortium, 2012). Zkušenosti s kyberšikanou potvrdilo 21,9 % vzorku více než 13 000 dětí ze 7 evropských zemí – Německa, Nizozemí, Polska, Rumunska, Španělska, Řecka a Islandu.

Další výzkumníci (Čechová & Hlistová, 2009; Kováčová, 2012) také upozorňují na nárůst počtu obětí kyberšikany na Slovensku (až 38,7 % dětí). Přehledné srovnání výzkumů kyberšikany v Evropě nabízí Hollá (Hollá, 2013), která srovnává výzkumy kyberšikany prováděné v Německu, Španělsku, Velké Británii, Irsku a Slovenské republice. Výzkum prováděný ve Španělsku (Ortega, Calmaestra, & Mechrán, 2008) na vzorku 1 661 respondentů ve věku 12–17 let například přinesl následující výsledky: 4,2 % respondentů se stalo oběťmi kyberšikany prostřednictvím mobilních telefonů, 7,5 % prostřednictvím internetu.

Nejnovější studie Hollé (Hollá, 2015) ze Slovenské republiky upozorňuje na to, že nejčastěji ke kyberšikanování chlapců dochází ve věku 17 let, statisticky jsou rovněž chlapci častěji kyberagresory. Nejčastějšími formami útoků, které používali chlapci, bylo odesílání hrubých urážlivých zpráv (28,9 %), rozesílání nepravdivých informací (24,3 %) a sdílení kompromitujících fotografií na internetu (19,6 %).

Kopecký, Szotkowski, Krejčí (Kamil Kopecký, Szotkowski, & Krejčí, 2014b) z České republiky upozorňují na nárůst vážných případů kyberšikany ve formě vydírání a vyhrožování dítěti, přičemž jsou k útoku zneužívány intimní materiály vylákané od dítěte. Poukazují také na propojení kyberšikany a sextingu, který napomáhá realizaci intenzivních útoků na děti.

2.1.4 Základní formy kyberšikany

Kyberšikana mnohdy začíná jako tradiční šikana (psychická nebo fyzická). Její projevy vychází z projevů psychické šikany (např. dehonestování, provokování, vyhrožování, vydírání atd.). Mezi nejznámější projevy (Kamil Kopecký, Szotkowski, & Krejčí, 2014a; Krejčí, 2010; Willard, 2007b) patří:

- **Publikování ponižujících záznamů nebo fotografií** (např. v rámci webových stránek, MMS zpráv)**.**

- **Ponižování a pomlouvání** *(denigration)* (v rámci sociálních sítí, blogů nebo jiných webových stránek)**.**
- **Krádež identity** *(impersonation)***, zneužití cizí identity ke kyberšikaně nebo dalšímu sociálně patologickému jednání** (např. zcizení elektronického účtu)**.**
- **Ztrapňování pomocí falešných profilů** (např. v rámci sociálních sítí, blogů nebo jiných webových stránek)**.**
- **Provokování a napadání uživatelů v online komunikaci** *(flaming/bashing)* (především prostřednictvím veřejných chatů a diskuzí)**.**
- **Zveřejňování cizích tajemství s cílem poškodit oběť** *(trickery/outing)* (např. v rámci sociálních sítí, blogů nebo jiných webových stránek, pomocí SMS zpráv apod.)**.**
- **Vyloučení z virtuální komunity** *(exclusion)* (např. ze skupiny přátel v rámci sociální sítě)**.**
- **Obtěžování** *(harassment)* (např. opakovaným prozváněním, voláním nebo psaním zpráv)**.**
- **Kyberšikana spojená s online hrami** (např. krádeže virtuálních postav či předmětů s následným vydíráním, vyhrožováním).
- **Tzv. happy slapping** (fyzický útok spojený s vytvořením záznamu, který je umístěn do prostředí internetu a dále sdílen).
- **Tzv. kyberstalking** (forma na pomezí stalkingu a kyberšikany, ve které dochází k dlouhodobému obtěžování oběti v kyberprostoru).

Mezi kyberšikanu řadíme i projevy tradiční psychické šikany posílené využitím ICT, například:
Dehonestování (ponižování, nadávání, urážení).
Vyhrožování a zastrašování.
Vydírání.
Očerňování (pomlouvání).
A další.

K těmto projevům jsou zneužívány především SMS zprávy, e-maily, chat, diskuze, IM (instant messenger) a VoIP (např. ICQ, Skype), blogy, sociální sítě nebo jiné webové stránky. Ojediněle se tyto formy objevují uvnitř ve virtuálních vzdělávacích prostředích (virtuálních světech) či online hrách (např. na bázi MMORPG). V rámci našich výzkumů je kyberšikana monitorována vzhledem k jejím jednotlivým projevům napříč vybranými komunikačními platformami (sociální sítě, IM, chat aj.) (Kamil Kopecký et al., 2014a).

Je zřejmé, že kyberšikana je komplex jevů a její projevy vznikají kombinací tří základních složek – *použité formy psychické šikany, formy šikanujícího obsahu* a *nástroje pro její šíření* (Kamil Kopecký et al., 2014a).

2.1.5 Kyberšikana jako třísložkový komplex

Použité formy psychické šikany	**Formy šikanujícího obsahu**	**Nástroje pro šíření kyberšikany**
Dehonestování (ponižování, nadávání, urážení) Pomlouvání Provokování Vyhrožování, zastrašování Vydírání Obtěžování Pronásledování	Text Videozáznam Audiozáznam Grafický záznam (fotografie, obrázek, karikatura) Volání, prozvánění Krádež identity[1] Atd.	Veřejné chaty (textové, videochaty), e-maily, instant messengery, ankety, sociální sítě, virtuální vzdělávací prostředí, online hry, VoIP, SMS, MMS, webové stránky, online datová úložiště (cloud) atd.

Kombinací jednotlivých složek pak vzniká konkrétní forma kyberšikany, např. vydírání pomocí fotografií v prostředí sociálních sítí. Vždy je však nutné mít na paměti, že kyberšikana musí být opakovaná, dlouhodobá a vnímaná jako ubližující. Jednorázové útoky, které z dlouhodobého pohledu nezanechávají v oběti prakticky žádné nepříjemné pocity, označujeme jako online obtěžování (nikoli jako kyberšikanu) (Černá et al., 2013).

[1] Vzhledem ke specifické povaze krádeže identity ji zařazujeme mezi formy šikanujícího obsahu, nejedná se totiž primárně o psychickou šikanu ani o technický prostředek či nástroj.

2.1.6 Mýty o kyberšikaně pohledem zahraničních výzkumníků

V posledních letech provází kyberšikanu celá řada mýtů, které vycházejí z nejednotného přístupu k samotnému vymezení termínu kyberšikana, rozdílné metodice výzkumu, velmi nevyrovnaným výsledkům prevalence kyberšikany v jednotlivých zemích a také častým zveličováním dopadů kyberšikany na oběť nejenom médii, ale také samotnými výzkumníky. Proto vzniká řada kritických studií, které se snaží upozornit na existující mýty a vyvrátit je.

Výzkumníci z USA (Sabella, Patchin, & Hinduja, 2013) definují 7 základních mýtů spojených s kyberšikanou:

Mýtus 1 – **Všichni vědí, co je kyberšikana**

Pohled na termín kyberšikana je velmi nejednotný, existuje velké množství definic a výkladů, které např. za kyberšikanu pokládají jakoukoli formu online agrese, někteří za kyberšikanu považují pouze formy útoků, které jsou zaměřeny na fyzické bezpečí uživatelů internetových služeb a za kyberšikanu nepovažují např. nadávky, urážky či sociální vyloučení z online komunity. Jiní autoři spojují kyberšikanu s konkrétními prostředími či technologiemi, skrze které je kyberšikana realizována (např. online-hry, sociální sítě apod.). Je velmi důležité pochopit, že vzájemný konflikt v sociální skupině (např. mezi dětmi či studenty) – např. ignorování, vytáčení, nadávání si či pošťuchování nemusí být automaticky známkami šikany, ať už k nim dochází online nebo v reálném prostředí (Willard, 2007b). Pro šikanu a kyberšikanu jsou typické *záměr/úmysl, opakování, poškození a nerovnováha sil* (Patchin & Hinduja, 2012) a ne každý konflikt tato kritéria naplňuje (Baas, de Jong, & Drossaert, 2013).

Mýtus 2 – **Kyberšikana dosahuje epidemiologických hranic**

Mýtus o epidemiologickém rozšíření kyberšikany v populaci pubescentů a adolescentů vychází na jedné straně z nejednotného vymezení kyberšikany (viz mýtus 1), ale také z nejednotné metodologie, jak vlastně kyberšikanu měřit. Některé studie např. uvádějí, že 72 % dětí má zkušenost s kyberšikanou (Juvonen & Gross, 2008), jiné naopak uvádějí prevalenci kyberšikany na úrovni menší než 7 % (Ybarra, 2004). Většina publikovaných studií hovoří o tom, že s některou z forem kyberšikany má zkušenost 6–30 % dětí, zatímco počet dětí, které se přiznaly k tomu, že šikanovaly jiné, se pohybuje v rozpětí od 4 do 20 % (Patchin & Hinduja, 2012). To znamená, že 70–80 % dětí nebylo „kyberšikanováno“ a neútočilo na ostatní.

Mýtus 3 – Kyberšikana způsobuje sebevraždu

V posledních letech došlo k několika případům, ve kterých dětské oběti kyberšikany spáchaly sebevraždu. Virální rozšíření těchto příběhů přispělo k tomu, že začala být kyberšikana zařazována mezi rizikové faktory vedoucí k sebevraždám (Beautrais, Collings, Ehrhardt, & Henare, 2005). Navzdory těmto tragédiím oběti kyberšikany ve většině případů sebevraždu nepáchají. Nicméně některé výzkumy potvrzují, že u osob zapojených v mládí do šikany/kyberšikany roste riziko výskytu faktorů spojených se sebevražednými myšlenkami, sebevražednými pokusy či dokonanou sebevraždou (Bauman, Toomey, & Walker, 2013) – jako jsou např. deprese a úzkost. Další studie (Hinduja & Patchin, 2010) realizované na vzorku více než 2 000 amerických studentů prokazují, že oběti tradiční šikany jsou 1,7 krát více a útočníci v tradiční šikaně dokonce 2,1 krát více náchylnější k pokusu o sebevraždu. U kyberšikany pak oběti 1,9 krát a útočníci 1,5 krát. Proč je však kyberšikana způsobující sebevraždu mýtus?

Odpověď je nutné hledat v definici termínu *způsobovat*. V našem kontextu by to znamenalo, že *kyberšikana přímo vede k sebevraždám*, nebo že *kyberšikana způsobuje sebevraždy*. To však nikdy nebylo výzkumem prokázáno. Bylo prokázáno, že mezi kyberšikanou a sebevraždami existuje *vztah* či *souvislost (korelace).* Většina obětí kyberšikany totiž sebevraždu nepáchá. Kyberšikana však mezi mladými lidmi může zhoršit již existující rizikové faktory spojené se sebevraždou, jako jsou deprese, sociální vyloučení, zdravotní postižení, pocity beznaděje apod. (Skapinakis et al., 2011). Bohužel média často případy zjednodušují a hledají příčiny ve zneužívání technologií, nikoli v psychickém zdraví obětí.

Mýtus 4 – Kyberšikana je rozšířena více, než tradiční šikana

O případech kyberšikany se v médiích hojně diskutuje, což by mohlo být signálem pro to, že je rozšířenější než tradiční formy šikany. Ve skutečnosti většina zahraničních výzkumů potvrzuje, že tomu tak není. Např. podle statistiky National Center for Educational Statistics (National Center for Education Statistics, 2012) zažilo šikanu 27,8 % studentů, zatímco kyberšikanu pouze 9 %. Další výzkumníci tato čísla potvrzují, např. podle výzkumníků z USA (Ybarra, Boyd, Korchmaros, & Oppenheim, 2012) tradiční šikanu potvrzuje 25 % studentů, zatímco kyberšikanu pouze 10 % respondentů. Kanadští výzkumníci (Beran & Li, 2007) provedli výzkum na vzorku 432 studentů 7. až 9. tříd kanadských škol a zjistili, že 1/3 obětí kyberšikany rovněž zažila běžnou tradiční šikanu. Tato data potvrzují další výzkumy (Ybarra & Mitchell, 2004),

které upozorňují na to, že velké množství pachatelů kyberšikany bylo rovněž jejími oběťmi, a také, že téměř polovina útočníků byla oběťmi tradičních forem šikany. Tento jev potvrzují i české výzkumy přepínání rolí mezi pachateli a oběťmi (Chráska, Kopecký, Krejčí, & Szotkowski, 2012; Kamil Kopecký et al., 2014a).
Z výše uvedeného vyplývá, že oba fenomény jsou v prostředí škol hojně rozšířeny a vzájemně propojeny.

Mýtus 5 – Stejně jako tradiční šikana, je i kyberšikana rituálem, prostřednictvím kterého teenageři získávají zkušenosti

Řada osob vnímá šikanu a kyberšikanu jako *něco, co oběť v principu posílí* (podle hesla: Co tě nezabije, to tě posílí.) a *co zvyšuje jeho psychickou odolnost.* Tím se snaží toto zraňující chování jaksi normalizovat – jako něco, čím si musel projít každý a co patří k lidskému životu. Tím vlastně tito lidé dětem sdělují, že sociální krutost je přirozená a že se předává z jedné generace na druhou jako nějaký rituál, kterým si všichni musí projít. A že je to vlastně něco, co je normálním projevem lidského vývoje (Sabella et al., 2013).

Tento přístup odsoudil mimo jiné prezident USA Barrack Obama ve svém projevu na konferenci zaměřené na šikanu 10. března 2011 (Obama, 2011), kdy mimo jiné řekl: *„Je třeba rozptýlit mýtus, že šikana je jen neškodným rituálem nebo nevyhnutelnou součástí dospívání. Není. Šikana může mít pro mladé lidi ničivé důsledky. Jako rodiče, studenti, učitelé a členové komunit musíme zabránit šikaně a vytvořit ve školách takové klima, ve kterém se všechny naše děti budou cítit v bezpečí.“*

Je zcela jedno, jak byla v minulosti šikana či kyberšikana rozšířena a všudypřítomná – nebyla přijatelná ani tehdy, není přijatelná ani dnes. Existují stovky studií, které prokazují negativní dopad šikany/kyberšikany na vývoj dětí (Bauman, 2011). Oběti šikany mají větší emoční problémy, objevují se u nich poruchy učení, poruchy chování, je u nich více pravděpodobné, že budou trpět depresí, úzkostí, nízkým sebevědomím a osamělostí.

Mýtus 6 – Původci kyberšikany jsou vyvrženci, nebo jednoduše „známé firmy“

Ve společnosti převládá názor, že většina dětských útočníků, kteří šikanují ostatní vrstevníky, to dělá proto, aby obětem ublížili (že jde o nějakou formu asociálního či sadistického chování inspirovaného jejich online aktivitami) (Finkelhor, 2011). Částečně mají pravdu, protože šikana je vedena potřebou

kontroly a nadvlády a může vést k většímu uznání mezi vrstevníky (Faris & Felmlee, 2011). Většina výzkumů se však shoduje v tom, že útočníci realizují kyberšikanu proto, aby se pomstili, nebo proto, že si s obětí „jen hrají" (König, Gollwitzer, & Steffgen, 2010; Sanders, Smith, & Cillessen, 2009). Jak uvádí psycholožka Elizabeth Englander z Massachusetts Aggression Reduction Centre (Englander, 2008): *„Hlavním motivem pachatelů kyberšikany je zejména vlastní hněv a touha po pomstě, druhým významným motivem je touha pobavit se – kyberšikana je pak vnímána jako žert."*

Podle výzkumu je mnoho původců kyberšikany frustrovaných nebo jinak citově rozrušených, jsou rozzlobeni a technologie je snadnou cestou, jak se frustrace zbavit. Z pohledu pachatelů je někdy kyberšikana vnímána jako prostředek spravedlivé odplaty za příkoří, které se jim stalo. Řada z pachatelů proto také odmítla závažnost svého chování v kyberprostoru, protože si neuvědomila, jaký dopad může mít jejich chování v reálném světě (offline). Tento typ útočníků je pak obvykle označován jako „neúmyslní pachatelé kyberšikany", protože – ačkoli byly jejich online příspěvky úmyslné, pachatelé nechtěli oběti způsobit bolest či problémy (Willard, 2007a). Neúmyslní pachatelé kyberšikany často věří, že bylo jejich chování neškodné, pouze se bavili nebo si s obětí pohrávali.

Velmi zajímavé výsledky o původcích kyberšikany poskytují Hinduja a Patchin (Sabella et al., 2013), kteří zjistili, že studenti, kteří byli ve škole hodnoceni známkami A („jedničkáři"), se častěji stávají původci a oběťmi kyberšikany, na rozdíl od studentů, kteří mají známky horší (C, D). Z toho, jak je žák či student ve škole úspěšný, nelze vyvozovat, že nebude týrat ostatní vrstevníky a nebude původcem kyberšikany. Z tohoto důvodu není snadné původce kyberšikany v komunitě dětí identifikovat a v řadě případů byli učitelé i rodiče šokováni, že někteří velmi dobří žáci či studenti mohou být do šikany či kyberšikany zapojeni. Je tedy mýtem, že by původci kyberšikany byli mezi učiteli a dětmi všeobecně známí („známé firmy").

Mýtus 7 – Kyberšikanu lze zastavit vypnutím počítače nebo mobilního telefonu

Zdá se být logické, že nejjednodušší cestou, jak kyberšikanu zastavit, je přestat používat počítače a mobilní telefony. Nicméně moderní informační a komunikační technologie jsou velmi důležité nástroje, které neslouží pouze k zábavě, ale také ke komunikaci, vzdělávání, udržování sociálních kontaktů, získávání informací apod. Proč by tedy měla být oběť, která se nedopustila ničeho špatného, trestána tím, že přestane moderní technologie používat? Je to

podobné, jako kdyby oběť tradiční školní šikany řešila svůj problém tak, že přestane chodit do školy (Sabella et al., 2013).

Navíc řadu forem kyberšikany vypnutí počítače nezastaví – např. kdokoli může vytvořit útočnou stránku o konkrétní osobě a nezaleží na tom, zda je oběť aktuálně online, pověsti o útočné stránce se mohou velmi rychle v online komunitě šířit a oběť o tom nemusí vědět. Propojení s technologiemi je pro děti velmi důležité – SMS, emaily a sociální sítě se staly primárními nástroji pro každodenní komunikaci. Odpojení od těchto komunikačních technologií není realistickým dlouhodobým řešením.

2.1.7 Diagnostika kyberšikany

Kyberšikanu je u dítěte poměrně obtížné rozpoznat, protože se její projevy kříží s projevy puberty – dítě mohou provázet různé změny nálad, může být uzavřené, může u něj dojít ke zhoršení prospěchu ve škole apod. V řadě případů odpovídají příznaky kyberšikany také příznakům klasických forem šikany, kyberšikana je obvykle s běžnou šikanou propojena. Mezi základní varovné příznaky, které kyberšikanu (či tradiční šikanu) provázejí, patří (Černá et al., 2013):

1. Dítě, které dříve informační technologie aktivně využívalo, se jim začne vyhýbat a odmítá je používat. Při čtení emailů či SMS zpráv může být dítě nervózní, nejisté a zarmoucené.

2. V celkovém chování je dítě sklíčené, ustrašené a apatické, časté jsou výkyvy nálad i chování (včetně hádek s vrstevníky a rodiči).

3. U dítěte se projevuje somatizace – bolesti břicha, hlavy, nechutenství, nevolnost, nespavost či noční můry.

4. Časté je rovněž vyhýbavé chování vůči lidem, předtím neobvyklé – chození za školu, trávení většiny času o samotě.

5. Zhoršení prospěchu ve škole.

Oběti kyberšikany jsou často uzavřené do sebe a nekomunikují o problémech s okolím (Krejčí, 2010). Důvodů pro takové chování může být více (strach, stud, rodiče neovládají práci na počítači, dítě nepozná, že jde o projevy psychického šikanování, bojí se, že mu rodiče zakáží používat internet atd.). Oběti kyberšikany na řešení svých problémů často zůstávají samy, což může vést k tomu, že situaci nezvládnou.

Mezi další varovné signály šikanovaní (ať již v rámci tradiční šikany či kyberšikany) patří následující (MŠMT, 2013):

a) za dítětem nepřicházejí domů spolužáci nebo jiní kamarádi;
b) dítě nemá kamaráda, s nímž by trávilo volný čas, s nímž by si telefonovalo apod.;
c) dítě není zváno na návštěvu k jiným dětem;
d) nechuť jít ráno do školy (zvláště když dříve mělo dítě školu rádo). Dítě odkládá odchod z domova, případně je na něm možno pozorovat i strach;
e) ztráta chuti k jídlu;
f) dítě nechodí do školy a ze školy nejkratší cestou, případně střídá různé cesty, prosí o dovoz či odvoz autem;
g) dítě chodí domů ze školy hladové (agresoři mu berou svačinu nebo peníze na svačinu);
h) usíná s pláčem, má neklidný spánek, křičí ze snu, např. „Nechte mě!";
i) dítě ztrácí zájem o učení a schopnost soustředit se na ně;
j) dítě bývá doma smutné či apatické nebo se objevují výkyvy nálad;
k) zmínky o možné sebevraždě;
l) odmítá svěřit se s tím, co ho trápí;
m) dítě žádá o peníze, přičemž udává nevěrohodné důvody (například opakovaně říká, že je ztratilo), případně doma krade peníze;
n) dítě nápadně často hlásí ztrátu osobních věcí;
o) dítě je neobvykle, nečekaně agresivní k sourozencům nebo jiným dětem, možná projevuje i zlobu vůči rodičům;
p) dítě si stěžuje na neurčité bolesti břicha nebo hlavy, možná ráno zvrací, snaží se zůstat doma;
q) své zdravotní obtíže může přehánět, případně i simulovat (manipulace s teploměrem apod.);
r) dítě se vyhýbá docházce do školy;
s) dítě se zdržuje doma více, než mělo ve zvyku.

2.1.8 Kyberšikana – Kdo jsou pachatelé?

Pachatelé kyberšikany tvoří heterogenní skupinu, ve které nalezneme dívky i chlapce, osoby s nízkým i vysokým sociálním statutem, děti s nižším i vyšším sebevědomím a různými kognitivními schopnostmi. Základní klasifikace pachatelů kyberšikany vychází z charakteristiky agresorů v rámci tradiční šikany. Agresory lze pro základní pochopení rozdělit na dvě základní skupiny.

Na jedné straně existují agresoři, kteří mají *nižší sebevědomí, snížené sociální dovednosti, trpí pocity nejistoty, nedostatečného uznání a osamělostí* (Shariff, 2008). V kolektivu bývají neoblíbeni a šikanování ostatních je reakcí na pocit vlastní nedostatečnosti a frustrace – šikanují, protože získaný pocit moci jim pomáhá kompenzovat jejich vlastní nedostatky (Černá et al., 2013). Často tak šikanují proto, aby si upevnili svoji pozici ve skupině a uspokojili svou touhu po převaze a moci (Olweus, 1993).

Na straně druhé však existují agresoři, kteří jsou naopak v kolektivu *uznávaní, mají velký okruh přátel, vyšší sociální dovednosti i sebevědomí a tyto vlastnosti využívají k obratnému manipulování ostatních* (Sutton, Smith, & Swettenham, 1999). Tento typ agresorů dokáže dobře odhadnout jednotlivé procesy ve skupině a využít je ve svůj prospěch – šikana je pak nástrojem pro získání dobrého postavení v kolektivu.

Mezi základní motivy, které se při šikanování uplatňují, patří (Kolář, 2011; Šmahaj, 2014):

a) *motiv upoutání pozornosti* – agresor se snaží být středem pozornosti, snaží si získat přízeň spolužáků,

b*) motiv zahnání nudy* – šikanování přináší agresorovi vzrušení a zábavu,

c) *motiv Mengeleho* – agresor zkoumá, co oběť vydrží, dochází ke stupňování těchto pokusů, a to jak na psychické, tak fyzické úrovni,

d) *motiv prevence* – častý pro oběti šikany, které přejdou do nového prostředí a ve snaze předejít šikanování začnou samy šikanovat, případně se přidají k nějakém agresorovi,

e) *motiv vykonat něco velkého* – tento motiv u neúspěšných žáků vyvolává pocit, že prostřednictvím šikanování jsou schopni výkonu a že se oni sami stávají příčinou významného děje.

U kyberšikany nalezneme také oba dva základní typy agresorů, nicméně velmi často se útočníky kyberšikany stávají právě samotné oběti tradiční šikany, které si v kyberprostoru především kompenzují to, co zažívají v reálném světě (Chráska et al., 2012; Kamil Kopecký et al., 2014a; Ybarra & Mitchell, 2004). Tyto oběti chtějí agresorům jejich chování oplatit, případně si vylepšit své vlastní postavení v rámci sociální skupiny oslabením pozic jiných vrstevníků. Někdy tyto pachatele označujeme jako *oběti/agresoři (bully-victim)* – právě ti si ze svých zkušeností odnášejí nejvíce negativních důsledků.

Specifický typ pachatelů představují tzv. *neúmyslní pachatelé kyberšikany*, které blíže charakterizujeme v kapitole o mýtech spojených s kyberšikanou.

Co se týče rozdílů mezi kyberšikanou u jednotlivých pohlaví – výsledky zahraničních výzkumů jsou rozporuplné, některé výzkumy dokladují, že se oběťmi a také útočníky stávají zejména dívky (Willard, 2007a) (chlapci jsou pak častěji oběťmi tradiční šikany), některé výzkumy rozdíly v pohlaví neprokazují (Slonje & Smith, 2008), někteří výzkumníci potvrzují převahu chlapců (ať již v pozici oběti či útočníka) (Aricak et al., 2008).

2.1.9 Kyberšikana – Kdo jsou oběti?

Při stanovení typů obětí kyberšikany se obvykle vychází ze základní typologie oběti tradiční šikany. Oběti tradiční šikany se obvykle dělí na *oběti pasivní* (Olweus, 1993) a na tzv. *oběti–provokatéry* (Kolář, 2011).

Mezi pasivní oběti patří děti, které jsou plaché, stydlivé, citlivé, nejisté, bývají i fyzicky méně zdatné a atraktivní, s nižším sebevědomím a horšími sociálními dovednostmi. Oběti–provokatéři jsou charakterističtí hyperaktivitou, impulsivností, agresivitou, často jsou vnímány jako „ti, co si šikanu zaslouží", zpravidla nemají téměř žádné přátele a v kolektivu vrstevníků nejsou oblíbeni (Perry, Kusel, & Perry, 1988). Ve většině případů se oběti a agresoři tradiční šikany znají z reálného světa, obvykle jsou to děti ze stejné třídy či školy.

Typologie obětí kyberšikany částečně koresponduje s typologií obětí tradiční šikany, patří mezi ně tedy jak oběti pasivní, tak i oběti–provokatéři. Vzhledem ke specifikům internetové komunikace a absenci přímého kontaktu mezi agresorem a obětí někteří autoři doplňují typologii o tzv. *agresory, kteří se stávají oběťmi,* a o *děti, které nevybočují, ale přesto jsou kyberšikanovány, protože jsou v online prostředí snadněji zranitelné* (Černá et al., 2013).

Přepínání rolí mezi agresory a oběťmi prokazuje stále více studií (Chráska et al., 2012; Kamil Kopecký et al., 2014a; Ybarra & Mitchell, 2004), je tedy zřejmé, že kyberprostor fyzické, psychické a sociální rozdíly stírá. Nemusí tak platit, že agresor běžné šikany je zároveň agresorem kyberšikany, jak bylo předpokládáno v dřívějších studiích.

Obecně pro oběti kyberšikany platí, že tráví větší množství času na internetu, více používají sociální sítě a instant messengery, zveřejňují o sobě mnoho osobních údajů. To však neznamená, že by se ti, kteří tráví hodně času na internetu, automaticky stávali oběťmi kyberšikany!

2.1.10 Kyberšikana a její dopad na oběť

Kyberšikana jako taková nezahrnuje osobní kontakt mezi agresorem a obětí, nicméně pro oběť je psychicky (emocionálně) škodlivá. Její dopad prokazují četné výzkumy realizované jak v Evropě, tak mimo ni. Někteří výzkumníci (Gradinger, Strohmeier, & Spiel, 2010) upozorňují na to, že se u obětí kyberšikany objevily sociální problémy, problémy v chování, nízké sebehodnocení, osamělost apod. Další výzkumníci upozorňují na to, že až 8 % obětí kyberšikany uvažovalo o sebevraždě (Hinduja & Patchin, 2010), oběti odmítaly chodit do školy nebo byly pravidelně nemocné.

Výzkumné studie realizované v zahraničí (USA, Austrálie, Evropa) dále upozorňují na následující dopad kyberšikany na psychický stav obětí (Šmahaj, 2014):

a) tenze, strach, stres,
b) změna self-konceptu oběti (sebevědomí, sebehodnocení, sebedůvěra, sebepojetí),
c) výskyt depresivních a neurotických obtíží,
d) časté poruchy spánku,
e) snížení frustrační tolerance,
f) pocit neřešitelnosti situace, ztráta životní pohody,
g) výskyt zkratkovitého jednání, suicidální myšlenky,
h) zvyšující se bezdůvodná agrese a impulsivnost,
i) celková psychická nestabilita,
j) trauma a posttraumatická stresová porucha.

2.2 Kybergrooming a sociální inženýrství

2.2.1 Definujeme kybergrooming

Termín kybergrooming (child grooming, online grooming) označuje *chování uživatelů internetu (predátorů, kybergroomerů), které má v oběti vyvolat falešnou důvěru a přimět ji k osobní schůzce* (Kamil Kopecký, 2010). Výsledkem této schůzky může být sexuální zneužití oběti, fyzické násilí na oběti, zneužití oběti pro dětskou prostituci, k výrobě dětské pornografie apod.

Další autoři definují kybergrooming jako *proces, ve kterém si pachatel (ve spolupráci se spolupachateli) připraví dítě ke zneužití a zajistí pro tento akt také vhodné podmínky. Mezi cíle útoku patří získání přístupu k dítěti, zajištění poddajnosti dítěte a zajištění mlčenlivosti dítěte, aby se zabránilo odhalení* (Craven, Brown, & Gilchrist, 2006).

Kybergrooming je tedy druhem psychické manipulace realizované prostřednictvím internetu, mobilních telefonů a dalších souvisejících technologií (Berson, 2003; Knoll, 2010; Kamil Kopecký, 2009; O'Connell, 2003; Penna, Clark, & Mohay, 2005).

Jedna z prvních studií věnovaných kybergroomingu (O'Connell, 2003) byla realizována ve Velké Británii a zaměřovala se na podrobný popis jednotlivých etap kybergroomingu a na strategie boje proti kybergroomingu. Autorka studie Rachel O´Connelová rozdělila kybergrooming do několika fází, kterými běžný útok prochází – a to na *fázi kontaktování/výběru oběti, fázi formování přátelství, fázi formování vztahu, fázi posouzení rizik, fázi exkluzivity, sexuální fázi* a *fázi samotného útoku*.

Další výzkumníci rozdělují jednotlivé etapy útoku (Kamil Kopecký et al., 2014b) na *fázi přípravnou* (příprava na kontakt s obětí), *fázi kontaktování oběti* (zahrnující formování přátelství a formování vztahu či sexuální fázi), *fázi přípravy na útok* (zlomové formy manipulace oběti) *a fázi samotného útoku*.

2.2.2 Specifické rysy kybergroomingu

Kybergrooming je podle některých autorů (Whittle, Hamilton-Giachritsis, Beech, & Collings, 2013) charakteristický:

1. Manipulací

Charakteristika kybergroomingu automaticky zahrnuje různé formy manipulativního jednání – od uplácení, přes lichocení, nabídky dárků či peněz, sexuální hrátky, k manipulaci silou a různé formy hrozeb (O'Connell, 2003; Ospina, Harstall, & Dennett, 2010). Způsoby, které volí útočníci v rámci manipulace, závisí na jejich osobnosti, okolnostech a osobnosti dítěte – na jedné straně mohou pachatelé u dítěte např. vzbudit pozitivní emoce, pocity zamilovanosti, či dokonce lásky, na straně druhé je mohou manipulovat zastrašováním, vyhrožováním či vydíráním (Kamil Kopecký, 2014b).

2. Dostupností obětí

Dostupnost obětí je pro kybergrooming rozhodujícím faktorem (J. Sullivan & Beech, 2002) a internet nabízí velké množství služeb, které umožňují kontaktovat velmi rychle velké množství dětí. Společně s možností kontaktovat dítě pachatelé získali velké množství výhod, které v minulosti neměli k dispozici, jako jsou například anonymita, přístupnost odkudkoli (pachatel nemusí opustit svůj domov a přesto je schopen s dětmi komunikovat) apod.

3. Budováním „vztahu“

V průběhu komunikace s dítětem je velmi důležité získat si jeho důvěru, naklonit si ho na svou stranu, sdílet s ním intimitu. V řadě případů proto útočníci synchronizují svoje vlastní chování a styl komunikace s dětskými uživateli a vytvářejí si s dítětem exkluzivní vztah. Někteří výzkumníci (Webster et al., 2012) identifikovali, že útočníci volí ve vztahu k dětem různé přístupy – např. zjistí, jaké mají děti koníčky, a poté dítě přesvědčují, že mají stejné zájmy a záliby. V některých případech se pachatel chová jako „mentor“ oběti, kterou „učí novým věcem“ (Webster et al., 2012). Útočníci se snaží být v komunikaci s dítětem co nejvíce pozitivní, přívětiví, důvěryhodní (Ospina et al., 2010), potřebují, aby jim dítě plně důvěřovalo. V některých případech dokonce oběti potvrdily, že se do pachatele zamilovaly (Janis Wolak et al., 2008).

4. Sexuálními tématy v komunikaci s dítětem

Dříve nebo později se v komunikaci pachatele a dítěte začnou objevovat sexuální témata, která útočník úmyslně do konverzace zavádí. European Grooming Project (Webster et al., 2012) definuje 3 typy online pachatelů: *hledače intimity* (intimacy seeking), *přizpůsobivé pachatele* (adaptable) a *hyper-sexualizované pachatele* (hyper-sexualized groomers). Právě hyper-sexualizovaní pachatelé zavádějí do komunikace sexuální témata velice rychle, často tak zahajují komunikaci s dítětem.

Komunikace pak může mít povahu např. flirtování, sexuální vulgarity, posílání odkazů na pornografické stránky či přímo posílání pornografických materiálů (někdy i vlastních) (O’Connell, 2003). Výměna intimních materiálů (tzv. sexting) je ve všech případech riziková, v některých případech vede k vydírání a vyhrožování (Kamil Kopecký, 2014b). Pachatelé si s dítětem vyměňují intimní materiály také proto, aby snížili zábrany dítěte ve vztahu k sexu (tzv. desenzibilizace dítěte) (Kamil Kopecký et al., 2014a; Olson, Daggs, Ellevold, & Rogers, 2007) a aby komunikaci určitým způsobem normalizovali.

5. Posuzováním rizik

Velmi důležitou část kybergroomingu tvoří etapa „posuzování rizik“, ve které se pachatel rozhoduje, jakým způsobem zajistit, aby nebyl odhalen a aby se mu podařilo dítě zmanipulovat a sexuálně zneužít.

Proto se někteří pachatelé snaží ochránit několika základními způsoby (Webster et al., 2012):

1. Technická ochrana – pachatelé používají více různých počítačů, mění si IP adresy, používají různé metody ukládání dat, mají celou řadu online falešných identit a účtů apod.

2. Přechod k soukromé komunikaci – pachatelé obvykle rychle opouštějí prostředí veřejných komunikačních služeb (veřejných chatů a otevřených sociálních sítí) a preferují komunikaci pomocí privátních emailů, instant messengerů či mobilních telefonů.

3. Zajištění osobní schůzky – pachatelé volí osobní schůzky daleko od domova dětí.

Velké množství pachatelů však žádná bezpečnostní opatření nedělá (Webster et al., 2012).

6. Podváděním

Pro oběť je velmi obtížné rozpoznat, že jí její virtuální kamarád lže – oběti totiž často ignorují varovné příznaky, které komunikaci provázejí. V některých případech pachatelé volí pro komunikaci s dítětem falešnou identitu jiného dítěte a k odhalení skutečné identity dojde teprve v rámci osobní schůzky. Řada z dětských obětí si je také vědoma, že komunikují s dospělou osobou, která jim lže, a přesto v komunikaci pokračují a dále riskují.

Charakteristiku kybergroomingu v českém prostředí doplňují také výzkumníci z Univerzity Palackého v Olomouci (Kamil Kopecký et al., 2014a), kteří upozorňují na to, že v českém prostředí existuje celá řada služeb, které svou povahou přímo vyzývají k tomu, aby byly využívány sexuálními predátory. Mezi ně patří např. sociální síť Líbímseti.cz, která umožňuje velmi podrobné vyhledávání uživatelů podle zadaných kritérií – jako je věk, pohlaví, ale třeba také sexuální preference, oblíbené sexuální praktiky apod. Tato síť umožňuje samozřejmě registraci i dětem, pro potenciálního pachatele je tedy snadné vyhledat potenciální nezletilé či zletilé oběti a např. je hromadně oslovit se zajímavou nabídkou. Kromě sociálních sítí predátoři rovněž zneužívají veřejné chatovací služby a internetové seznamky (pro dospělé i pro děti), které oběti využívají k vyhledávání kamarádů a partnerů.

Tytéž autoři rovněž upozorňují na to, že manipulace dítěte může probíhat řádově dny, týdny, měsíce, ale také několik let. Jedním z důvodů, proč útočník

oddaluje schůzku s dítětem, může být např. obava z tvrdých trestů, které by mu mohly hrozit, pokud by zneužil dítě mladší 15 let. Důvodem dlouhotrvající manipulace bývá též snaha útočníka navázat blízký vztah s obětí, a získat tak její plnou důvěru. Když je pak oběti nabídnuta možnost osobního setkání, většinou se na něj dostaví, poněvadž očekává schůzku s „nejlepším kamarádem“ či potenciálním „partnerem/partnerkou“. A pokud ne, bývá k setkání kybergroomerem, který si za dobu několikaměsíční komunikace nastřádal dostatek informací o její osobě (např. jméno a příjmení, bydliště, seznam přátel, obnažené fotografie atd.), přinucena skrze vydírání (Kamil Kopecký et al., 2014a). Dítě, které je vydíráno, zpravidla nekontaktuje dospělé osoby a samotné vydírání a zneužívání nenahlásí ani policii, ani rodičům, učitelům či kamarádům.

V samotném procesu kybergroomingu v rámci sociálních sítí lze rozlišit několik navazujících fází (Kožíšek, 2015):

1. Fáze tipování

Pachatelé systematicky prohlížejí profily, inzeráty a fotografie dětí, které se snaží oslovit pod různými záminkami. Také kontaktují přátele dětí, aby od nich získali další využitelné informace. Útočníci zpravidla pracují s více identitami.

2. Fáze kontaktování

Pachatelé si vytvoří účet, který odpovídá potřebám toho, kdo si o nich bude chtít zjistit informace. Útočníci naváží rozhovor s dítětem – snaží se mu lichotit, postupně přejdou k výměně fotografií. Dítěti nabídnou sexuálně explicitní fotografii, na kterou dítě reaguje tím, že pachateli zašle své vlastní intimní materiály. Pokud pachateli oběť vyhovuje, přejde ke komunikaci prostřednictvím privátního chatu, instant messengeru, případně přejde na zahraniční sociální síť (nejčastěji Facebook), kde komunikace dále pokračuje.

2.2.3 Výzkumy kybergroomingu

Výzkumy zaměřené na oběti a také pachatele kybergroomingu probíhají – vzhledem k vysoké nebezpečnosti tohoto fenoménu – jak v Evropě, tak v USA. Díky silné podpoře těchto výzkumných projektů ze strany Evropské komise a programu Safer Internet Plus vznikla celá řada studií, které poskytují výsledky o prevalenci kybergroomingu v jednotlivých zemích a také o strategiích útoků.

Jedna z prvních studií zaměřených na rizikovou komunikaci v online prostředí (Mitchell, 2001) upozornila na to, že průměrně jedno z pěti dětí bylo na internetu osloveno s žádostí o online sex. 3 % dětí rovněž obdržela zprávu s žádostí o osobní schůzku v reálném světě a 5 % dětí v rámci studie uvedlo, že byly obtěžovány, že se poté bály. Studie realizovaná stejným týmem o pět let později (Mitchell, Finkelhor, Jones, & Wolak, 2010) potvrdila nárůst počtu útočníků odsouzených k trestu odnětí svobody za online obtěžování o 21 %.

Nejčastějšími oběťmi kybergroomingu (online obtěžování) jsou dle výzkumníků děti ve věku 13–17 let (Katz, 2013; Janis Wolak, Finkelhor, & Mitchell, 2004). Přestože bylo jen malé procento dospívajících fyzicky sexuálně napadeno, důsledky pohlavního zneužití bývají velmi vážné, a to nejenom v oblasti fyzické, ale také psychické (např. negativní ovlivnění kognitivního, emočního či psychického vývoje dítěte) (Dombrowski, Ahia, & McQuillan, 2003).

Velmi zajímavé výsledky nabízí mezinárodní studie (Velká Británie, Norsko, Itálie a Belgie) European Online Grooming Project (Webster et al., 2012), která se zaměřuje na popis chování online útočníků a na strategie jejich útoků stejně jako na preventivní opatření, která lze integrovat do edukace dětí a dospělých.

Další výzkumníci se zaměřují zejména na rizikové faktory, které jsou s procesem kybergroomingu spojeny (Wachs, Wolf, & Pan, 2012), upozorňují např. na to, že v rámci jejich výzkumu kybergrooming v posledním roce reportovalo 21,4 % z výzkumného vzorku (111 z 518 dětí).

Zajímavé výsledky nalezneme také v pracích indických výzkumníků (Gupta, Kumaraguru, & Sureka, 2012), kteří se orientují na charakteristiku komunikace pedofilních uživatelů a dětí v rámci online groomingu. Na základě analýzy 75 záznamů komunikace identifikovali, že největší část pedofilní komunikace je zaměřena na formování vztahu s obětí. Obdobný přístup zvolili také výzkumníci z Kanady a USA (Black, Wollis, Woodworth, & Hancock, 2015), kteří provedli jazykovou analýzu komunikace pachatelů a obětí s využitím programu LIWC a sémantického slovníku.

2.2.4 Kybergrooming vs. sociální inženýrství

V českých podmínkách se často kybergrooming spojuje s termínem sociální inženýrství, pro potřeby této publikace však oba termíny odlišujeme (Kamil Kopecký, 2014a). Sociální inženýrství vnímáme jako *soubor strategií jak manipulovat uživatelem internetu, jak od něj získávat osobní údaje a další citlivé materiály* apod. Sociální inženýrství je tedy jakýmsi souborem technik

a strategií. Primárním cílem sociálního inženýrství však není sexuální zneužití dítěte či dospělého, sociální inženýrství může být zaměřeno např. na průnik na bankovní účet, na získání utajovaných informací atd. Sociální inženýrství se rovněž projevuje v běžných marketingových aktivitách a procesech, jako je např. telemarketing. Kybergroomer (útočník) pak využívá techniky sociálního inženýrství k tomu, aby zmanipuloval oběť a donutil ji k osobní schůzce, přičemž primárním cílem kybergroomingu je sexuální zneužití oběti.

2.2.5 Pachatelé online sexuálních útoků

Pachatelé online sexuálních útoků zaměřených na děti tvoří heterogenní skupinu, která se zaměřuje zejména na děti v pubertě či na adolescenty – především tedy na osoby nad 13 let věku (s drobnými individuálními odchylkami). Díky nesprávné interpretaci se termín sexuální útočník (abuzér, predátor) bohužel často zaměňuje za termín pedofil. Pedofilové se však zaměřují na děti prepubescentní (5/8–12 let věku), které zpravidla na internetu nejsou příliš aktivní, méně se zajímají o mezilidské vztahy či sexuální kontakty (DeLamater & Friedrich, 2002), méně často se také stávají oběťmi kybergroomingu (dále v textu).

Pachatele, kteří se zaměřují na online sexuální útoky, lze podle jejich motivace rozdělit do dvou základních skupin (Briggs, Simon, & Simonsen, 2011):

a) pachatele, kteří jsou vedeni především svou fantazií,
b) pachatele, kteří chtějí navázat sexuální kontakt ve skutečném světě.

První skupina pachatelů se orientuje zejména na kybersex, chtějí v online prostředí uspokojit své sexuální fantazie, ale netouží po setkání v reálném světě. Druhou skupinu již představují pachatelé, jejichž záměrem je dítě sexuálně zneužít v reálném světě – s dětmi navazují online kontakt, budují s nimi důvěrný vztah a připravují podmínky pro osobní schůzku.

Většina z pachatelů z těchto dvou skupin nebyla v minulosti trestně stíhána (až na výjimečné případy). Někteří z pachatelů jsou rovněž „posedlí dětskou pornografií“ (Briggs et al., 2011) – aktivně ji vyhledávají, shromažďují, vyměňují, vytvářejí sítě uživatelů, kteří pak tyto materiály vzájemně sdílejí.

Převážná část pachatelů je *hebofilně* či *efebofilně* zaměřena – orientuje se tedy především na pubescenty či adolescenty (Janis Wolak et al., 2008). Hebofily[2]

[2] V některých případech se termínem hebofil označují adolescenti obou pohlaví (Janis Wolak et al., 2008).

(zaměřují se na dospívající dívky) a efebofily (zaměřují se na dospívající chlapce) přitahují – na rozdíl od pedofilů – děti, u který se již objevují sekundární pohlavní znaky (tzv. *lolitky*), tedy děti v pubertě, pozdní pubertě či začátku adolescence. Věkově jde tedy o děti přibližně od 13 roku věku.

Pedofilně orientované jedince naopak přitahují převážně děti bez sekundárních pohlavních znaků – prepubescenti – či dospívající, kteří si zachovávají dětské rysy (vzhled, chování) (Weiss, 2002). Existuje velké množství různých definic, které se snaží více či méně zachytit podstatu tohoto termínu (Žák, 2009), řada z nich však není pravdivá – např. definice, že *při pedofilii jsou zneužívány děti, že pedofilie je společensky nebezpečná porucha chování* apod. Termín pedofil se díky mediálním zkratkám stal jakýmsi synonymem pro sexuálního násilníka zaměřeného na děti – což však není pravda. U pedofilů je třeba rozlišovat mezi kriminogenními (pachateli sexuálně motivovaných trestných činů) a nekriminogenními – nekriminogenní žijí v souladu se společenskými normami a nedopouštějí se žádných trestných forem jednání (Weiss, 2002; Žák, 2012). Pedofilové se obvykle orientují na děti ve věku 5–12 let (Weiss, 2002), tato věková hranice však není fixní. Případy, ve kterých by pedofil vylákal prepubescenta na osobní schůzku, jsou spíše raritní (Janis Wolak et al., 2008).

Jedna z nejznámějších typologií (Lanning, 2002) rozděluje online útočníky na útočníky situační, preferenční a smíšené. Jednotlivé kategorie si stručně charakterizujme.

1. Situační útočníci

Pokud situační útočníci poruší zákon, obvykle jsou trestně stíháni a vyšetřováni, jejich chování však není dlouhodobé a předvídatelné, jako např. u preferenčních útočníků.

A. „Normální" adolescent/dospělý pachatel – obvykle jde o typického adolescenta či dospělého hledajícího v online prostředí pornografii a sex (vyhledává různé erotické seznamky apod.).

B. Morálně bezohledný pachatel – obvykle jde o sexuálního útočníka, který je násilnické povahy a má za sebou násilnou trestnou činnost. Do této kategorie se řadí také rodiče – zejména matky – které nabízejí své děti k sexu jiným uživatelům internetu.

C. Profitující pachatel – tito pachatelé jsou motivováni ziskem a snaží se snadno zbohatnout na obchodování s dětskou pornografií.

2. Preferenční útočníci

A. Pedofilní (hebofilní) útočníci – jasně preferují děti. Jejích sbírky pornografie obsahují zejména dětskou pornografii (někdy i parafilně zaměřenou, ale to není primárním cílem).

B. Útočníci s rozmanitými sexuálními zájmy (diverse offenders) – tito útočníci mají velké množství deviantních/parafilních zájmů, nepreferují tedy pouze děti. Jejich sbírky pornografie se zaměřují na konkrétní druh parafilie, např. fetišismus, transvestitismus, exhibicionismus, voyerství, sadomasochismus atd.

C. Latentní útočníci – jejich původně latentní sexuální preference se projevily až poté, co došlo díky online komunikaci k oslabení jejich zábran, naplnění jejich tužeb. Poté se začali chovat nezákonně.

3. Smíšená skupina útočníků

Přestože tito pachatelé mohou porušit zákon, je málo pravděpodobné, že by byli trestně stíháni.

1. Reportéři masmédií – lidé, kteří mylně věří, že mohou ze zpravodajských důvodů (např. odhalení pachatele) obchodovat s dětskou pornografií a sjednávat si schůzky s podezřelými ze sexuálního zneužívání dětí, aby pak mohli např. zveřejnit nově získané informace. Zahrnuje tedy ty novináře, kteří kvůli příběhu porušují zákony.

2. Vtipálci (tvůrci tzv. pranků) - pachatelé, kteří rozšiřují nepravdivé nebo inkriminující informace, aby např. uvedli do rozpaků, ponížili či jinak ublížili vyhlédnutým obětem svých vtípků.

3. Starší kamarádi – pozdní adolescenti (ve věku kolem 20 let), kteří se snaží navázat sexuální kontakt s mladšími dívkami a chlapci.

4. Příliš horliví občané – lidé, kteří se snaží na vlastní pěst soukromě vyšetřovat sexuálně motivovanou trestnou činnost.

Online sexuální útočníci (kybergroomeři) jsou jen zřídka násilničtí (Janis Wolak et al., 2008), násilí je u sexuálně motivovaných trestných činů, které jsou iniciované internetovou komunikací, raritní. Většina kybergroomerů trpělivě rozvíjí v online prostředí vztah s dětskými oběťmi, aby pak tento vztah přenesli do reálného světa (Janis Wolak et al., 2004). To však neznamená, že by se v procesu kybergroomingu nevyskytovalo násilí vůbec – v roce 2004 bylo násilí,

hrozby či pokusy o znásilnění zaznamenáno u přibližně 5 % případů v USA (Janis Wolak et al., 2004).

Bohužel v posledních letech je zdokumentováno velké množství případů, ve kterých je násilí běžnou součástí kybergroomingu, zaznamenány jsou rovněž případy znásilnění a vraždy obětí (Kamil Kopecký, Szotkowski, & Krejčí, 2012; Kamil Kopecký et al., 2014a; Stokes, 2010; Webster et al., 2012).

2.2.6 Etapy kybergroomingu

Jak již bylo řečeno, existuje celá řada vymezení etap kybergroomingu, které vycházejí zejména z analýzy konkrétních případů, ve kterých došlo ke zneužití dítěte online predátorem (Kloess, Beech, & Harkins, 2014; Kamil Kopecký et al., 2014a; O'Connell, 2003).

Proces manipulace lze pro zjednodušení rozdělit do 5 hlavních etap:

A. Přípravná fáze

V přípravné etapě pachatel buduje svou virtuální identitu, pomocí které bude s dítětem komunikovat. Pachatel může pracovat s jednou, ale také s více různými falešnými identitami, velmi často volí např. identitu dítěte stejného či opačného pohlaví. Falešná identita umožňuje pachateli velmi rychle navázat s dítětem kontakt, který je pak založen např. na sdílení fotografií, videí, ale také zážitků a tajemství. V řadě případů pachatel dokázal právě prostřednictvím falešné identity vylákat z dítěte intimní materiály, kterými následně dítě vydíral (Kamil Kopecký, 2014b).

V některých případech rovněž pachatel využíval profil fiktivní dospělé osoby, přičemž svou virtuální identitu podpořil tzv. falešnou autoritou – doplnil do svého profilu informace o tom, že pracuje pro známou firmu (např. telekomunikační firmu, výrobce počítačů, mobilních telefonů, castingovou společnost apod.), profil doplnil firemními logy a odkazy na firemní stránky. Fiktivní autorita firmy dodala informacím, které pachatel sděloval dětem, na věrohodnosti. Poté pachatel kontaktoval děti např. s nabídkou speciálních akcí, ve kterých může dítě získat zdarma např. kredit, počítač, mobilní telefon apod. Důvěřivé děti pak pachateli zasílali své vlastní kontaktní údaje – telefonní čísla, adresy, skutečné osobní údaje apod.

V některých případech si pachatelé rovněž zjišťovali, ve které místnosti má dítě umístěný počítač. Je totiž podstatný rozdíl, zdali má dítě umístěno počítač v dětském pokoji, nebo zda je počítač např. v obývacím pokoji, kde hrozí vyšší

riziko náhodného odhalení např. rodiči dítěte. Jen velmi malé procento rodičů ověřuje pravidelně, co jejich dítě na počítači v dětském pokoji dělá.

B. Kontaktování oběti

V některých případech pachatelé kontaktují děti jakoby náhodně (např. pomocí formulace „*ahoj, omylem jsem si tě přidal do přátel, překlepl jsem se, ale jestli chceš, můžeme si psát. . já jsem Jitka"*), v jiných případech pachatelé kontaktují své oběti prostřednictvím diskusních fór orientovaných na děti, ale také např. na sexuální zkušenosti apod. V jiných případech využívají pachatelé možnosti sociálních sítí, které umožňují např. vybírat uživatele podle věku, pohlaví, regionu, ale také např. podle sexuální preference. Řada z dětských uživatelů nerespektuje minimální věkové hranice pro využívání sociálních sítí, falšuje svá data narození – pachatelé pak mohou kontaktovat bez problému např. děti mladší 13 let.

Součástí prvních kontaktů bývá *lichocení* (flattery) – pachatel chce získat náklonnost dítěte, proto jej často chválí, oceňuje, skládá mu komplimenty, oceňuje originalitu projevu dítěte, humor, snaží se být zábavný apod. To vše umožňuje navázat s dítětem pevný kontakt a postupně dítě manipulovat (Whittle, Hamilton-Giachritsis, & Beech, 2014).

C. Manipulace dítěte

Další etapu procesu kybergroomingu představuje soubor manipulativních technik, mezi které patří techniky *zrcadlení (tzv. mirroring), techniky získávání osobních informací o obětech (phishing), techniky profilování dětí, techniky vábení a uplácení (luring), strategie snižování zábran dětí a mládeže zaváděním sexuálního obsahu do konverzace, metody izolování dětí od okolí, strategie manipulace dětí prostřednictvím fotografií opačného pohlaví, techniky webcam trollingu* apod. Jednotlivé techniky si v krátkosti představíme.

Mirroring

Termínem mirroring označujeme napodobování komunikace dítěte pachatelem – a to jak po stránce obsahové, tak formální. Pachatel se stává pomyslným zrcadlem – komunikuje stejně, jako oběť, kterou si zvolil. Pokud oběť útočníkovi sdělí, že se cítí například osamělá a má problémy a starosti (rozvod rodičů, konflikty ve škole, problémy ve vztahu, …), útočník odpoví, že je na tom obdobně a plně ji chápe. A jako „spřízněná duše" jí nabídne, že se mu může s důvěrou svěřit (Kamil Kopecký et al., 2014a).

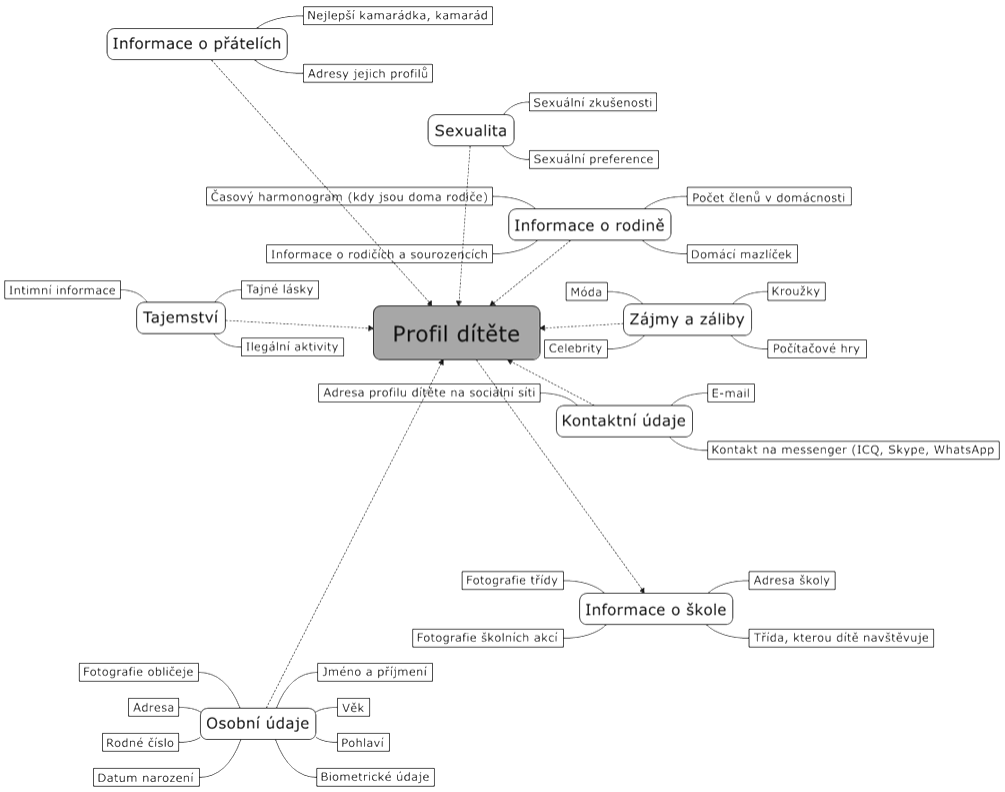
Mirroring se kromě kyberprostoru uplatňuje také v běžné mezilidské komunikaci a projevuje se zejména napodobováním nonverbálních projevů lidského chování (napodobováním gest, mimiky apod.) (Cahrtrand & Bargh, 1999). Mirroring umožňuje navázat užší mezilidský kontakt a prožívat pocit sounáležitosti.

Phishing a profilování obětí

Termínem phishing označujeme soubor technik zaměřených na získávání citlivých údajů oběti (osobní údaje, heslo, emailovou adresu, telefonní číslo, adresu profilů na sociálních sítích apod.). Čím více citlivých údajů útočník od oběti získá, tím snadněji jí může manipulovat a narůstá tak šance, že se mu podaří vylákat ji na osobní schůzku. Při získávání informací pachatel využívá falešných identit, internetových vyhledávačů, ale také informací od přátel oběti, které jsou napojeny na její veřejný profil (typicky např. Facebook). Pachatelé rovněž "vytěžují" z internetových zdrojů např. informace o zájmech a zálibách dítěte, které mu umožňují snadněji k dítěti proniknout a získat si jeho důvěru.

Internet obsahuje velké množství údajů, které však v řadě případů jeho uživatelé neukládají na jednom místě – např. na jednom profilu. Pachatelé proto mají na začátku procesu phishingu a profilování o dítěti k dispozici pouze omezené množství informací, např. pouze e-mail. Prostřednictvím internetových vyhledávačů však mohou díky znalosti e-mailové adresy odhalit např. telefonní číslo dítěte, z něj jsou schopni odvodit např. adresu dítěte, profily dítěte, postupně získávají fotografie či videa dítěte, informace o rodině dítěte a další citlivé informace.

Obr. 1. Profil dítěte – struktura informací



Vábení a uplácení dítěte

V některých případech pachatelé aplikují v procesu manipulace tzv. luring – uplácení dítěte dárky. Pachatelé mohou dítěti nabídnout hmotný či finanční dar (kredit do mobilního telefonu, mobilní telefon, mp3 přehrávač, tablet, počítačové hry, značkové oblečení apod.), který v řadě případů dítěti skutečně pošlou. Dárky pak slouží k upevnění vztahu s dítětem, ale také ověření informací, které pachatel od dítěte získal. V některých případech také slouží k získání vysoce citlivého osobního údaje dítěte – fotografie obličeje.

Snižování zábran dětí a mládeže zaváděním sexuálního obsahu do konverzace

Další techniky, které se uplatňují v procesu kybergroomingu, se zaměřují na postupné zvyšování tolerance dítěte ve vztahu k sexu. Útočník se u dítěte snaží potlačit přirozený stud a rozvinout jeho zájem o sexuální témata, proto dítěti začne nabízet erotické či pornografické materiály, diskutuje s dítětem o lidské

sexualitě, sexuálním životě rodičů, o menstruaci, masturbaci a dalších tabuizovaných tématech. Často se pak pro dítě stává mentorem v oblasti lidské sexuality - poučuje jej, nabádá k experimentování, zásobuje dítě fotografiemi a videi. Dítě postupně akceptuje, že je normální komunikovat s anonymním uživatelem internetu o intimních tématech a svěřovat se mu.

Webcam trolling

Webcam trolling (Kamil Kopecký & Kožíšek, 2013; Kamil Kopecký, 2013c, 2016) je velmi nebezpečnou technikou, jejíž podstatou je získat od dítěte intimní materiál pomocí podvrženého záznamu, který je dítěti přehráván prostřednictvím webkamery. Celý fenomén podrobně popisujeme v samostatné kapitole.

Strategie manipulace dětí prostřednictvím fotografií opačného pohlaví

Velmi nebezpečnou technikou, která byla zaznamenána v desítkách kauz sexuálního zneužití dítěte, je manipulace dítěte pomocí intimní fotografie osoby opačného pohlaví (Kožíšek, 2015). Technika je poměrně jednoduchá – nezletilému chlapci nabídneme prostřednictvím chatu či emailu fotografii dívky – fotografie však bude alespoň trochu intimní. Chlapec na tyto výzvy reaguje podobně, tj. dívce nabídne svou vlastní fotografii, která je částečně intimní. Útočník pak chlapci nabídne další – o trochu více intimní fotografii, chlapec opět zareaguje a manipulace tak probíhá až do fáze, kdy se chlapec vyfotí zcela obnažený a svou fotografii útočníkovi odešle.

Izolace dítěte

V průběhu procesu manipulace usiluje útočník o to, aby jeho vztah s dítětem zůstal co nejvíce důvěrný, aby se tedy dítě nesvěřilo např. rodiči či kamarádům. Jeho cílem je zaujmout roli skutečných rodičů dítěte, stát se pro dítě důvěrníkem, kamarádem, ale také autoritou. Čím více informací o sobě dítě pachateli prozradí, tím více se na něm stává fixované a závislé – pachatel zná tajemství dítěte, radí dítěti, jak se má chovat, rovněž však dítěti zakazuje, aby se o jejich komunikaci bavilo s jinou osobou. Pokud dítě nepřistoupí na tato pravidla hry, útočník začne dítě citově vydírat a vyhrožovat mu – např. tím, že pokud dítě prozradí, o čem spolu komunikují, rodič to nepochopí a dítě potrestá (Kamil Kopecký et al., 2014a).

Podle výsledků výzkumu Nebezpečí internetové komunikace 5 (dále v textu) potvrzuje přibližně 1/4 českých dětí, že po nich jejich internetový kamarád

chtěl, aby udržely komunikaci v tajnosti a aby se nikdo nedozvěděl, že se spolu baví a o čem spolu komunikují.

Technika překonávání věkového rozdílu mezi obětí a útočníkem

Základem této techniky je zajistit, aby dítě považovalo za normální, že komunikuje s dospělou osobou, nebo dokonce, že je ochotno s touto osobou jít na osobní schůzku v reálném světě. Pachatelé například napíší ze svého dětského profilu, že nebudou týden k dispozici na chatu, ale že bude doma „dospělý bratr/sestra", který bude online a se kterým si dítě může psát. Touto fiktivní osobou je samozřejmě pachatel.

Další metodu, jak překonat věkovou bariéru, využívají útočníci v situaci, kdy mají dorazit na osobní schůzku a dítě neví, že celou dobu komunikovalo s dospělým člověkem. Útočník na schůzce osloví dítě s tím, že „jeho syn/dcera" nemohou na schůzku z nějakého důvodu dorazit, ale že on = „tatínek" – oběť vyzvedne a doveze k nim domů. Pachatel navíc dítěti jako důkaz předloží záznam z komunikace, ve které s dítětem „jeho syn" komunikuje. Dítě má na reakci zpravidla několik sekund, pachatel na dítě na schůzce vyvíjí nátlak (např., že parkuje na zákazu parkování a musí rychle odjet).

Obě techniky byly identifikovány v řadě případů zneužití dětí, např. v kauze 17leté Ashleigh Hallové, která byla znásilněna a zavražděna v roce 2010 deviantem Peterem Chapmanem, který ke komunikaci používal 2 mobilní telefony - jeden pod identitou 17letého Petera, druhý pod identitou jeho otce. Oběti pak pod identitou Petera poslal SMS, že ji vyzvedne jeho otec. „Otec" se pak na schůzce prokázal SMSkami, které mu posílal jeho „fiktivní syn". Poslední SMS, kterou oběť odeslala, byla SMS: „*Mami, všechno je v pořádku, naložil mě tatínek od Petera."* (Armstrong, 2012; Kamil Kopecký et al., 2014a).

D. Bod zlomu

Bod zlomu představuje situace, ve které je dítě vyzváno agresorem, aby se s ním setkalo v reálném nevirtuálním světě. V této fázi agresor využívá veškeré dostupné strategie manipulace, které ovládá. Pokud dítě odmítne na schůzku jít, začne dítě systematicky vydírat zveřejněním citlivých informací dítěte – např. intimní fotografií, ponižujícím videem, odkrytím nebezpečného tajemství apod. Dítě pak zvažuje, zdali chce být vystaveno ponížení, ke kterému by zveřejněním intimních tajemství dítěte došlo, nebo zda na místo setkání dorazí. Tlak, který však vyvíjí agresor na dítě, je velmi intenzivní, dítěti např. napíše, že *pokud s ním nepůjde na osobní schůzku, tak např. v místě jeho bydliště a školy*

rozvěsí vytištěné plakáty s fotografií oběti, s jejím jménem a příjmením a nápisem – to je gay/lesba, případně zveřejní jiné tajemství dítěte.

E. Osobní schůzka

Osobní schůzka je nejrizikovější etapou kybergroomingu – na osobní schůzce totiž může dojít k sexuálnímu zneužití dítěte (tzv. syndrom CSA – Child Sexual Abuse). Sexuální zneužití dítěte je dle definice Rady Evropy *nepatřičné vystavení dítěte sexuálnímu kontaktu, činnosti či chování. Zahrnuje jakékoli sexuální dotýkání, styk či vykořisťování kýmkoliv, komu bylo dítě svěřeno do péče, anebo kýmkoliv, kdo se s dítětem dostane do nějakého styku*. *Takovou osobou může být rodič, příbuzný, přítel, odborný či dobrovolný pracovník či cizí osoba* (J Dunovský, Dytrych, & Matějček, 1995; Hanušová, 2006).

Sexuální zneužití dítěte může mít řadu forem (Ježková & Fraňková, 2012):

1. Bezkontaktní sexuální zneužívání:
- obnažování se před dítětem, masturbace před dítětem, setkání s exhibicionistou,
- pozorování nahého dítěte za účelem vlastního sexuálního vzrušení, uspokojení,
- vystavení dítěte sledování pornočasopisů, pornofilmů,
- přinucení dítěte sledovat soulož.

2. Kontaktní sexuální zneužívání:
- osahávání či líbání dítěte na intimních místech, laskání prsou, genitálií,
- nucení dítěte, aby manipulovalo pohlavními orgány svými či zneuživatele,
- vaginální, orální, análním styk (včetně znásilnění).

3. Komerční sexuální zneužívání:
- zneužití dítěte k dětské pornografii,
- zneužití dítěte k dětské prostituci.

Řada z dětských uživatelů internetových služeb podceňuje rizika, která jsou s možným sexuálním zneužitím spojena, velké množství dětí je však k osobní schůzce díky propracované a účinné manipulaci přinuceno. Snaží se pak co nejvíce zajistit bezpečnost, například tím, že:

a) na osobní schůzku jdou s kamarádem,
b) schůzku si domlouvají na veřejném místě.

Tyto strategie obrany jsou však neúčinné, děti zpravidla nejsou poučeny, jak v rizikové situaci zareagovat, navíc mohou být v šoku a nejsou schopny účinně reagovat. Pachatelé si v některých případech pořizují intimní fotografie a videa dítěte, které pak využívají k jeho opětovnému vydírání – pokud by se nepodvolilo požadavkům agresora, agresor zveřejní tyto záznamy a dítě se stane terčem veřejného posměchu.

2.2.7 K diagnostice dětských obětí

Jak již bylo řečeno, kybergrooming zahrnuje jak fázi bezkontaktní, ve které dítě není s útočníkem ve fyzickém kontaktu a komunikuje s ním prostřednictvím online služeb, tak fázi kontaktní, ve které jsou již v reálném skutečném kontaktu a pachatel může dítě sexuálně zneužít, znásilnit apod.

Pokud se dítě stalo obětí kybergroomingu a bylo sexuálně zneužito, je poměrně těžké toto odhalit. Zneužité děti se obávají vyhledat pomoc, pojmenovat svůj problém a svěřit se jiné osobě. Některé z nich mají také obavu z možné pomsty, existují však také oběti, které nechtějí pachateli ublížit, a proto zneužití neohlásí.

Proto mají také případy sexuálního zneužití dětí vysokou latenci – podle výsledků výzkumu *Kontinuální výzkum sexuálního chování české populace realizovaný v letech 1993, 1998, 2003 a 2008* (Weiss & Zvěřina, 2008) 69 % mužů a 79 % žen sexuálně zneužívaných v dětství nikomu zneužití neoznámilo.

U zneužitých dětí lze pozorovat následující varovné příznaky (Ježková & Fraňková, 2012):
a) náhlé, dlouhodobější, nápadné změny v chování a aktivitě dítěte (dítě do té doby družné se náhle izoluje, klidné dítě je náhle hyperaktivní a podobně),
b) změny v ladění – zvýšená úzkostnost nebo agresivita, depresivní symptomatika,
c) výkyvy či náhlý pokles ve školní výkonnosti či pokles koncentrace pozornosti, zhoršení prospěchu,
d) vyhýbání se kontaktům s vrstevníky a lidmi vůbec, vyhýbání se určitým lidem, apatie,
e) výrazné změny ve stravování, neopodstatněné nevolnosti, až zvracení, nebo naopak přejídání,
f) útěky z domova, sklony k sebepoškozování,
g) gynekologické obtíže, poranění (určitého typu).

2.2.8 Následky sexuálního zneužití

Následky sexuálního zneužití (či opakovaného zneužívání) jsou tím větší, čím mladší bylo dítě při zahájení zneužívání, čím déle zneužívání trvalo a čím těsnější je vazba mezi dítětem a pachatelem (Ježková & Fraňková, 2012). Mezi následky sexuálního zneužívání se řadí:

a) disharmonický vývoj osobnosti,
b) depresivní ladění, sebepoškozování, sebevražedné tendence,
c) pro okolí nesrozumitelné chování, „zlom" v chování, poruchy chování, rizikové chování,
d) narušení morálních hodnot, ztráta citu pro morální hodnoty, pro běžné hranice,
e) ztráta emočních vodítek pro správné posouzení situací a správné chování,
f) z hlediska následků se více „zabudovává" do osobnosti dítěte.

Následky zneužívání se mohou projevit i nízkým sebehodnocením, nenávistí k vlastnímu tělu, odporem k tělesné blízkosti s další osobou a odporem k sexuálnímu styku, také sebepoškozováním.

Zneužíváním se dítě může dostat do závažného vnitřního konfliktu, který s sebou nese také zvýšenou tenzi (napětí), úzkost až úzkostnost. Dítě je totiž ke zneuživateli vázáno citovou vazbou a věří, že ten tu je pro potřeby dítěte, na jeho ochranu (Ježková & Fraňková, 2012).

Mezi fyzické projevy, které mohou být se sexuálním zneužitím dítěte spojeny, patří (Hanušová, 2006; Vaníčková, Hadj-Moussová, & Provazníková, 1995):

A. *Traumata, fyzická poškození a další fyziologické projevy*
   - *kožní léze – hematomy, zvláště na obličeji, ve vlasech, na těle,*
   - *popáleniny – opařeniny, bodové popálenin od cigaret, popálené dlaně,*
   - *rány – těžko vysvětlitelné, zvláště v oblasti anální a kolem dutiny ústní,*
   - *alopecie – vytrhané vlasy,*
   - *zlomeniny – těžko rozpoznatelný mechanismus úrazu (hlavy, žeber),*
   - *subdurální hematom,*
   - *pohmoždění vnitřních orgánů,*
   - *bolesti při chůzi a sezení v oblasti konečníku či genitálií.*
B. *Poškození růstu a vývoje – podvýživa, opoždění psychomotorického vývoje*

2.3 Sexting

2.3.1 Definujeme sexting

Sexting představuje poměrně nový a rychle se rozmáhající fenomén, kterým pro potřeby našeho textu označujeme *elektronické rozesílání textových zpráv, vlastních fotografií či vlastního videa se sexuálním obsahem* (Jolicoeur & Zedlewski, 2010; Kamil Kopecký, 2012b), *ke kterému dochází v prostředí virtuálních elektronických médií – zejména internetu*. Často jsou k sextingu využívány mobilní telefony či tablety.

Jedna z prvních obecně užívaných definic sexting vymezuje jako *akt rozesílání fotografií zachycujících nahotu mezi mobilními telefony či dalšími elektronickými médii*, např. internetem (Streichman, 2011), a nově je dle některých autorů sexting spojován především s mladou generací, jež pořizuje své sexuálně laděné materiály (tzv. youth-produced sexual images) a dále je rozesílá a zveřejňuje (J. Wolak, Finkelhor, & Mitchell, 2012). Definice doplňuje Sullivan (K. Sullivan, Cleary, & Sullivan, 2004), který do sextingu řadí sugestivní textové zprávy a obrázky znázorňující nahé nebo částečně obnažené děti či dospělé, ty jsou pak dále šířeny mobilním telefonem či internetem. Množství platforem a nástrojů umožňujících šíření takovýchto materiálů doplňuje (Ringrose, Gill, Livingstone, & Harvey, 2012) o sociální sítě, hlavně Facebook a MySpace.

Sexting je dále definován jako *sdílení sexuálně laděných fotografií* (Lenhart, Purcell, Smith, & Zickuhr, 2010), přičemž jde o sdílení osobní, sdílení prostřednictvím textových zpráv, sdílení online či sdílení jinými cestami.

2.3.2 Prevalence sextingu

Výzkumy sextingu probíhají od roku 2009 v celé řadě zemí – v USA, Velké Británii, Austrálii, Kanadě, Číně (Jolicoeur & Zedlewski, 2010) a také v České a Slovenské republice (Kamil Kopecký, Szotkowski, & Krejčí, 2014c).

Zajímavé výsledky o prevalenci sextingu mezi mladými uživateli internetu a mobilních telefonů poskytuje např. výzkum realizovaný v rámci amerického projektu The National Campaign to Prevent Teen and Unplanned Pregnancy (*Sex and Tech: Results from a Survey of Teens and Young Adults*, 2008). V rámci tohoto výzkumu realizovaném na vzorku 653 teenagerů ve věku 13–19 let (a 627 dospělých ve věku 20–26 let) bylo prokázáno, že 38 % z nich odeslalo sexuálně laděné zprávy jiným lidem, 19 % nezletilých dále odeslalo své vlastní obnažené fotografie jiným osobám. U dospělých ve věku 20–26 již sexuálně sugestivní sextingové zprávy odeslalo 58 % respondentů, přičemž vlastní

obnaženou fotografii odeslalo 32 % z nich. Zajímavé je rovněž sledovat důvody, proč je sexting mladistvými uživateli realizován – 71 % dívek a 67 % chlapců odesílá sexuálně laděný obsah své partnerce či partnerovi, sexting se tak stává součástí jejich intimního vztahu. 21 % dívek a 39 % chlapců odeslalo intimní fotografie osobě, se kterou si naplánovali osobní schůzku (*Sex and Tech: Results from a Survey of Teens and Young Adults*, 2008).

Výzkum EU Kids Online probíhající rovněž na Slovensku (Tomková, 2010) stanovuje míru sextingu v populaci slovenských teenagerů v intervalu 4,6–9,6 % (4,6 % respondentů potvrzuje, že publikovali fotografie, na kterých jsou ve spodním prádle či zcela obnaženi). Výsledky tohoto zjištění porovnáme s výsledky našeho výzkumu.

Výzkumy prováděné v posledních letech v USA (Ybarra & Mitchell, 2014) rovněž prokazují, že přibližně 7 procent mladých Američanů ve věku 13 až 18 let odesílá své vlastní intimní materiály svým vrstevníkům. Autorky rovněž upozorňují, že je sexting znakem sexuálního vývoje a objevování, není to tedy problém primárně způsobený moderními technologiemi.

Aktuální výzkum rizikového chování českých a slovenských dětí (Kamil Kopecký et al., 2014c) prokazuje, že sexting v české a slovenské populaci provozuje 7–9 % populace ve věku 11–17 let. Více než 70 % dětí rovněž potvrzuje, že vědí, že je sexting rizikový.

Zajímavé výsledky poskytují také studie realizované mimo Evropu, např. výzkum sextingu u peruánských adolescentů (West et al., 2014). Ten dokazuje, že 20 % ze vzorku 949 středoškoláků realizovalo alespoň jednou sexting, přičemž chlapci provozují sexting více než dívky.

2.3.3 Rizika spojená se sextingem

Sexting je rizikový zejména proto, že oběť potenciálním útočníkům poskytuje citlivý materiál, který může být zneužit k různým formám kybernetických útoků (např. ke kyberšikaně, cílené manipulaci, vydírání apod.). Tento materiál může v prostředí internetu kolovat i několik let od svého pořízení a lze jej jen velmi obtížně z internetového prostředí odstranit. I po odstranění materiálů z konkrétních internetových stránek si již oběť nemůže být nikdy stoprocentně jistá, že k opakovanému útoku v budoucnu nedojde (Kamil Kopecký et al., 2014b).

Další riziko, které je spojeno se sextingem, představuje ztráta společenské pověsti a prestiže. V souvislosti s tím má oběť problémy např. se získáním nebo

udržením zaměstnání či sociálních vztahů, v komunitě pubescentů je pak označována za prostitutku, veřejně dehonestována, urážena a napadána. Sexting tak přechází v kyberšikanu se vzrůstající intenzitou útoků. V řadě případů (např. případy Jessica Renee Logan – 2008, Hope Witsell – 2009, Emma Jones – 2010) skončila kyberšikana spojená se sextingem sebevraždou oběti (Kamil Kopecký et al., 2014b).

Sexting může vést k vážným zdravotním problémům, mezi které patří. např. emoční a psychologická úzkost (Gordon-Messer, Bauermeister, Grodzinski, & Zimmerman, 2013; Sadhu, 2012), která může vyústit až v sebevražedné sklony (Curnutt, 2012). Některé studie (Benotsch, Snipes, Martin, & Bull, 2013) realizované v prostředí amerických škol dokazují, že se sexting pojí s rizikovým sexuálním chováním, zejména s počtem sexuálních partnerů a výskytem případů nechráněného sexu. Další studie (Dake, Price, Maziarz, & Ward, 2012) rovněž prokazují souvislost mezi sextingem a užíváním návykových látek, zejména užíváním marihuany, cigaret a nárazovou konzumací alkoholu.

2.3.4 Proč lidé realizují sexting?

Sexting je rizikový fenomén, který je úzce propojen s dospíváním současných pubescentů a adolescentů. Důvodů pro realizaci sextingu existuje celá řada:

1. Sexting je vnímán jako součást romantických vztahů

Jak potvrzuje celá řada autorů (Albury & Crawford, 2012; Döring, 2012; Lenhart et al., 2010; Ringrose et al., 2012), sexting je využíván v úvodních částech partnerských vztahů jako nástroj pro upoutání pozornosti partnera, flirtování, vzrušení apod. V rámci navázaného vztahu je pak sexting znakem lásky, intimity, vzájemné důvěry mezi partnery. Stejně tak sexting provozují partneři, kteří jsou na nějaký čas fyzicky odloučeni a komunikují spolu zejména prostřednictvím ICT.

2. Sexting funguje jako nástroj pro potlačení nudy

Řada z výzkumů dokazuje, že sexting je často provozován jako nástroj pro potlačení nudy (Lenhart et al., 2010). V řadě výzkumů (Kamil Kopecký et al., 2012; Kamil Kopecký, 2012b) se nuda stává velmi častým důvodem pro sdílení intimních materiálů s vrstevníky zejména v prostředí sociálních sítí.

3. Sexting vzniká jako produkt sociálního tlaku

V řadě zdokumentovaných případů sexting vznikl v rámci tlaku konkrétní sociální skupiny – například spolužáků/spolužaček či partnera/partnerky. Pokud sexting probíhá v rámci partnerského vztahu, dívky mohou být svými partnery přinuceny k sextingu (Lippman & Campbell, 2014), který se pak stává běžnou a normální součástí vztahu. Je pro partnery projevem vzájemné důvěry, lásky, fyzické přitažlivosti. Existuje množství případů sextingu, ve kterých se „mimo partnerský vztah" skupina spolužaček rozhodla, že společně nafotí intimní fotografie, které si vzájemně nasdílejí. Bohužel po úniku fotografií se tyto dívky staly terčem posměchu, kyberšikany, harrasmentu, byly označovány za „děvky", byly veřejně dehonestovány apod. (Kamil Kopecký et al., 2014b).

4. Sexting jako produkt konzumní společnosti, jako nástroj sebeprezentace

Řada z výzkumníků (Van Ouytsel, Walrave, & Van Gool, 2014) upozorňuje na souvislost mezi sextingem a požadavky současné konzumní společnosti. Lidská sexualita je v médiích a zejména v reklamě prezentována velmi výrazně, pubescentům a adolescentům jsou prostřednictvím mediální komunikace předkládány vzory fyzické krásy, ke které patří „být sexy". Sexting běžně provozují celebrity, zpěváci, herci, sportovci, sexting je součástí televize, filmu, hudebních klipů a dalších mediálních forem.

Dítě již od útlého věku potřebuje vzory chování, které může napodobovat. A právě média poskytují dětem informace o tom, že odhalovat se a sdílet intimitu je „normální". Děti pak nevnímají sexting jako něco nebezpečného a rizikového a jsou ochotné tento model chování napodobovat.

5. Sexting jako nástroj pomsty

Ve velkém množství zdokumentovaných případů sextingu u dětí i dospělých se stal zveřejněný intimní materiál nástrojem útoku. V některých případech sloužily intimní fotografie k vydírání dítěte (Kamil Kopecký, 2014b) – počáteční komunikace dětí přerostla ve výměnu fotografií, jejich intimita se stupňovala. Výsledkem pak bylo velmi intenzivní vydírání dítěte. V některých případech sexting slouží také jako nástroj pomsty ex-partnerům (Walker, Sanci, & Temple-Smith, 2013). Existují internetové stránky, na které chlapci nahrávají fotografie či videa svých bývalých přítelkyň a vulgárně je komentují (check this bitch out). V rámci stejného výzkumu respondenti uváděli, že „pokud sexting provozují chlapci, nic to neznamená, pokud jej však provozují dívky, jsou stigmatizovány".

2.4 Rizikové využívání sociálních sítí

Sociální sítě jsou specifické internetové služby, zaměřené primárně na získávání a udržování sociálních kontaktů s dalšími uživateli internetu. Mohou být zaměřeny univerzálně (Facebook, G+), nebo jsou zacíleny např. profesně (LinkedIn, Researchgate), na základě příslušnosti ke konkrétní třídě či studijní skupině (Spolužáci.cz) či podle dalších kritérií. Termín sociální sítě často splývá s termínem servery komunitních služeb.

Hranice mezi tím, co jsou a nejsou sociální sítě, jsou velmi neostré. Sociální sítě však mají řadu společných vlastností:

a) obsah sociálních sítí vytvářejí sami uživatelé,
b) sociální sítě umožňují vytvářet sociální vazby (např. spojovat se s přáteli, followery atd.),
c) sociální sítě obsahují velké množství osobních a citlivých informací, které o sobě zveřejňují a šíří sami uživatelé,
d) sociální sítě podporují jednoduché a efektivní sdílení informací.

Aby bylo možné sociální sítě hodnotit co nejvíce objektivně, je třeba uvědomit si, že mají vzhledem k jejich používání jak pozitiva, tak i negativa.

Pozitiva sociálních sítí
A. Sociální sítě umožňují navazovat mezilidské kontakty.
B. Sociální sítě jsou nástrojem pro překonání sociální izolace.
C. Sociální sítě umožňují realizovat reklamu s přesným cílením na cílovou skupinu.
D. Sociální sítě jsou zdrojem poučení.
E. Sociální sítě jsou zdrojem zábavy.

Negativa sociálních sítí
A. Sociální sítě obsahují velké množství zneužitelných osobních údajů.
B. Sociální sítě umožňují snadno, rychle a anonymně realizovat kyberšikanu, sexuální útoky na děti, kyberstalking apod.
C. Sociální sítě umožňují realizovat internetové podvody.
D. Sociální sítě mají úzkou vazbu na majetkovou kriminalitu.
E. Pro potřeby sociálních sítí často vznikají nebezpečné technologie, např. automatické označování obličejů na fotografiích (tzv. automatické tagování).
F. Sociální sítě se stávají terči internetových útoků vedoucích k úniku osobních údajů.

Většina veřejných sociálních sítí obsahuje kontrolní mechanismy, které např. zpřístupňují přístup na sociální síť od určitého věku (např. od 13 let na sociální síti Facebook), případně obsahují jiné mechanismy kontroly uživatelů (např. kontrola pomocí institucionálního emailu). Většinu těchto kontrolních mechanismů však lze snadno „obejít", např. zadat jiné datum narození. V praxi je pak běžné, že sociální sítě masově využívají i uživatelé, kteří kritéria pro přístup do dané sociální sítě nesplňují – tedy i děti.

Děti v prostředí internetu sdílejí velké množství osobních a citlivých údajů, které umožňují jejich velmi přesnou identifikaci. Často si neuvědomují, jak jsou osobní údaje důležité a jak snadno je lze zneužít ke kybernetickému útoku.

2.5 Jak se chránit před kyberšikanou a dalšími rizikovými jevy

Základem ochrany před kyberšikanou a dalšími rizikovými jevy je především prevence a dodržování základních bezpečnostních principů, ke kterým patří:
a) nesdílet citlivé informace s ostatními uživateli internetu (včetně partnerů), nezveřejňovat osobní fotografie, nesdílet jakékoli materiály sexuální povahy (fotografie, videa apod.),

b) nesvěřovat se se svými osobními problémy neznámým lidem,

c) dodržovat pravidla jednotlivých služeb (např. respektovat věkový limit pro používání sociálních sítí),

d) seznámit se s bezpečnostními riziky, která jsou s online službami spojena,

e) používat bezpečná hesla a silné kontrolní otázky, po ukončení práce na počítači se vždy odhlásit ze svých účtů,

f) přidávat si mezi své online přátele osoby, které známe z reálného světa – neznámé uživatele si prověřovat,

g) ověřovat si, že při komunikaci prostřednictvím webové kamery skutečně komunikujeme s konkrétní osobou (viz kapitola Webcam trolling).

Dodržování těchto základních bezpečnostních principů sice nemusí zajistit, abychom se nestali obětí kyberšikany, v každém případě však sníží dopady a důsledky kybernetického útoku. Usnadní také výsledné řešení.

Pokud se staneme obětí kybernetického útoku, je třeba opět dodržovat několik základních pravidel (pravidla jsou určena především dětským uživatelům internetu):

1. Zachovat klid

Prvním pravidlem, které je třeba dodržet v případě, že se staneme terčem kybernetického útoku, je zachovat klid – oběti v řadě případů řeší celou situaci verbálním napadáním útočníka a samy se pak stávají původci kybernetické agrese – navíc pachatele provokují k dalším aktivitám.

2. Ukončit komunikaci s útočníkem

Druhým pravidlem je ukončení komunikace s útočníkem. Ukončení komunikace vede k tomu, že útočníka může po čase přestat bavit investovat čas a energii do útoku, který nevyvolává u oběti příslušnou odezvu.

3. Nenechat se vydírat

Pokud zjistíme, že se nás virtuální útočník snaží vydírat, v žádném případě nepřistupujme na jeho pravidla hry. Útočník např. může vyhrožovat, že jestliže mu nepošleme své vlastní intimní materiály, pak zveřejní naši komunikaci a všechno, co od nás získal. V situaci, kdy bychom mu poslali další citlivé materiály, jeho útok nezastavíme – naopak, dáme mu k dispozici více zbraní, které může v rámci útoku využívat. V případě, že se staneme obětí vydírání či vyhrožování, okamžitě kontaktujme – v případě, že jsme dítě – rodiče, pokud jsme dospělí – Policii ČR či některou z internetových specializovaných poraden.

4. Uschovat si veškerý důkazní materiál

Pro úspěšné vyřešení případu je nutné mít k dispozici dostatek důkazních materiálů – záznamy komunikace (chat, e-mail), snapshoty internetových stránek, SMS zprávy apod. To vše přispěje k rychlejšímu odhalení a potrestání pachatele.

5. Blokovat útočníka a blokovat obsah, který rozšiřuje

V prvotních fázích útoku je velmi důležité co nejdříve zablokovat citlivé materiály, které o nás pachatel může rozšiřovat. Předtím je ale vhodné si vždy pořídit záznam o tom, že obsah skutečně na internetu byl – např. pořídit si snapshot z Facebooku, YouTube apod. Každá sociální síť je v současnosti vybavena blokačními mechanismy, které můžeme využít. Je velmi důležité, aby

se materiál, který do kyberprostoru unikne, nestal virálním (např. virální video). V tomto případě již není možné zastavit jeho šíření.

6. Odhalit útočníka

Pokud je to možné, odhalit útočníka – každý člověk o sobě v prostředí internetu zanechává množství digitálních stop, které je možné sledovat. Např. v prostředí Facebooku lze pachatele identifikovat pomocí okruhu jeho přátel, které můžeme postupně kontaktovat a zjistit, kdo je ukryt za konkrétní virtuální identitou. Nikdy však při odhalování identity útočníka neriskujme a raději přenechejme tuto činnost specialistům Policie ČR.

7. Oznámit útok dospělým

Kybernetické útoky mohou mít velkou intenzitu a dopad na oběť – zvláště na dětské oběti. V některých extrémních případech pak mohou vést až k sebevraždě. Proto je nutné vysvětlit dětem, že v rizikových situacích mohou vždy kontaktovat osoby, které jsou schopny pomoci jim situaci vyřešit – zejména svoje rodiče či učitele. Z našich výzkumů (Kamil Kopecký et al., 2014a) jednoznačně vychází, že děti kontaktují dospělé zejména ve velmi vážných situacích – např. jsou-li vydírány. Je však nutné, aby se děti nebály požádat o pomoc dospělé i tehdy, kdy je z jejich pohledu situace zvládnutelná i bez pomoci dospělého – např. v počátečních fázích útoku.

8. Nebát se vyhledat pomoc u specialistů

V případech online útoků na děti existuje velmi vysoká latence - velké množství dětských obětí neinformuje o kybernetickém útoku dospělé (rodiče, učitele), nekontaktuje policii ani jinou specializovanou instituci. Je to nejčastěji proto, že dítě poskytlo jinému uživateli svůj vlastní intimní materiál (intimní fotografie či video) a stydí se tuto informaci sdělit dospělým – má strach ze sekundární viktimizace, které by mohlo být vystaveno, stejně tak nechce, aby rodič věděl o tom, co udělalo - má strach z možných následků.

Proto děti v řadě případů kontaktují různé anonymní online poradny, které jsou schopny jim pomoci (např. *Linku bezpečí, Online poradnu projektu E-Bezpečí, Poradnu projektu Seznam se bezpečně!* apod.). Je nutné naučit děti, že mají tyto nástroje k dispozici a že mohou v online prostředí vyhledat velmi kvalitní pomoc.

Vše, co jsme si popsali výše, sníží dopad kyberšikany a dalších rizikových fenoménů na oběť – je však důležité uvědomit si, že např. kyberšikana je

onemocnění sociální skupiny – blokací obsahu tak řešíme pouze příznaky tohoto „onemocnění“, nikoli samotnou nemoc. Tu je možné „vyléčit“ pouze aktivní prací se sociální skupinou, ve které se dané rizikové chování objevuje.

Neexistují univerzální pravidla, která by mohla být aplikována ve všech případech, které mohou nastat – ke každému případu je nutné přistupovat individuálně a především citlivě.

3 Rizikové chování českých dětí v prostředí internetu (2014)

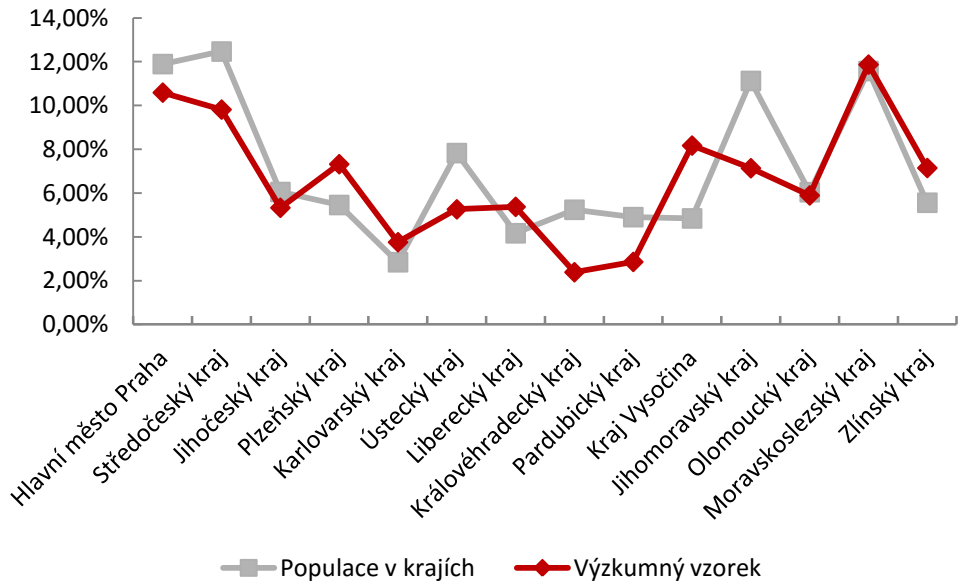
Výzkum *Rizikové chování českých dětí v prostředí internetu* monitoruje výskyt (a prevalenci) základních rizikových jevů spojených s využíváním ICT v populaci českých dětí. Byl realizován na reprezentativním vzorku ve všech krajích ČR v letech 2013–2014.

3.1 Metodologie

3.1.1 Charakteristika výzkumného vzorku

Výzkumu realizovaného na území České republiky se zúčastnilo 28 232 (n=28 231) respondentů ve věku 11–17 let. 55,54 % vzorku tvořily děti ve věku 11–14 let, 44,46 % ve věku 15–17 let. 46,76 % tvořili chlapci, 53,24 % dívky. Z genderového hlediska odpovídal výzkumný vzorek demografickému rozložení věkové struktury obyvatelstva v České republice. Výzkum probíhal ve všech krajích, nejvíce respondentů pocházelo z Moravskoslezského kraje (11,87 %) a Prahy (10,59 %). Svým rozsahem lze vzorek respondentů považovat za unikátní, a to jak v tuzemském, tak i celosvětovém měřítku.

Tab 2. Rozložení výzkumného vzorku ve srovnání s rozložením populace v krajích ČR



3.1.2 Charakteristika výzkumného nástroje

Vlastní výzkum byl s ohledem na zamýšlené množství respondentů orientován kvantitativně a jako výchozí výzkumná metoda byla zvolena metoda explorativní (explorační), v rámci které byl jako technika vybrán dotazník. Vlastní výzkumný nástroj, u kterého byly již v minulosti ověřeny jeho vlastnosti (validita, reliabilita), obsahoval celkem 71 položek (40 dichotomických, 2 polytomické, 22 s více možnými odpověďmi a 7 otevřených), jež vznikly na základě analýzy teoretických poznatků a byly sestaveny takovým způsobem, aby reflektovaly stanovené cíle a vzniklé problémy.

Dotazník byl respondentům distribuován elektronicky (on-line) prostřednictvím dotazníkového systému E-Bezpečí / Centra prevence rizikové virtuální komunikace, který disponuje e-mailovými adresami škol, školských zařízení, spolků zaměřených na děti a mládež a jiných institucí v České a Slovenské republice. Soupis adres pořídili členové výzkumného týmu v letech 2013–2014 z veřejně dostupných zdrojů.

Anonymní dotazník, jenž automaticky ověřoval, odkud byl odeslán (IP adresa, regionální příslušnost, monitoring chování respondentů za využití nástroje Google Analytics atd.), nabízel možnost uvedení e-mailové adresy školy, skrze niž mohli být její zástupci v kontaktu s výzkumným týmem.

Příprava výzkumu byla zahájena 1. 10. 2013, sběr dat probíhal od 1. 12. 2013 do 31. 3. 2014. Jejich vyhodnocení bylo realizováno v průběhu dubna 2014. Data byla naměřena převážně na nominální a ordinální úrovni, čemuž odpovídalo i jejich následné zpracování, použité numerické operace a statistika.

Výhodou elektronické verze výzkumného nástroje (dotazníku) byla automatizace sběru dat do příslušných tabulek. Následně bylo provedeno jejich třídění, zpracování a vyhodnocení.

3.2 Kyberšikana u českých dětí

3.2.1 Sledované formy kyberšikany

V rámci výzkumu byly sledovány tyto formy útoků spadající do oblasti kyberšikany:

a) Verbální útoky v kyberprostoru – ubližování formou ponižování, urážení, zesměšňování, ztrapňování dítěte.
b) Obtěžování prozváněním.
c) Vyhrožování a zastrašování dítěte.

d) Krádež identity.
e) Vydírání dítěte.
f) Ponižování, ztrapňování realizované šířením fotografie.
g) Ponižování, ztrapňování realizované šířením videa.
h) Ponižování, ztrapňování realizované šířením audia.

Aby byly tyto formy považovány za skutečnou kyberšikanu, výzkum sleduje jejich opakování v rámci jednoho roku (časová limita).

Výzkum sledoval fenomén kyberšikany z několika hledisek:

a) oběť kyberšikany (incidence, množství obětí v rámci časové jednotky, platformy, na kterých útok probíhá),

b) původce kyberšikany (incidence, množství útočníků v rámci časové jednotky, platformy, které jsou pro útok využity),

c) osoby zapojené do řešení kyberšikany (koho by oběť kontaktovala v situaci, kdy zažívá kyberšikanu),

d) další související jevy (specifické formy kyberšikany realizované např. prolomením účtu a následnou krádeží identity).

3.2.2 Výsledky výzkumu – oběti kyberšikany

Výsledky výzkumu jsme rozdělili na oddíl deskriptivní a relační. Na deskriptivní problémy jsme hledali odpovědi skrze základní veličiny deskriptivní statistiky (výpočet charakteristik polohy – míry ústřední tendence, výpočet směrodatných odchylek, výpočet procent apod.), přičemž nechybělo ani jejich grafické znázornění. Na relační výzkumné problémy a následnou verifikaci hypotéz jsme využili induktivní statistické postupy, konkrétně test nezávislosti chí-kvadrát pro čtyřpolní tabulku.

Deskriptivní oddíl

Deskriptivní oddíl sestává z tabulek absolutních četností a procentuálního podílů jednotlivých sledovaných nebezpečných komunikačních jevů. Pro grafické znázornění distribuce naměřených dat a zvýraznění genderových rozdílů byly použity histogramy.

Tab 3. Kyberšikana u českých dětí (dle jednotlivých forem) – oběti

	n	%	N (total)
Verbální útoky	9 455	**34,33**	27 538
Vyhrožování a zastrašování	3 380	17,84	18 951
Krádež identity	2 755	11,82	16 253
Vydírání	1 879	7,91	23 744
Ponižování, ztrapňování šířením fotografie	2 982	13,70	21 765
Ponižování, ztrapňování šířením videa	1 505	6,54	23 022
Ponižování, ztrapňování šířením audia	738	3,89	18 951
Průnik na účet	8 113	**34,80**	23 314

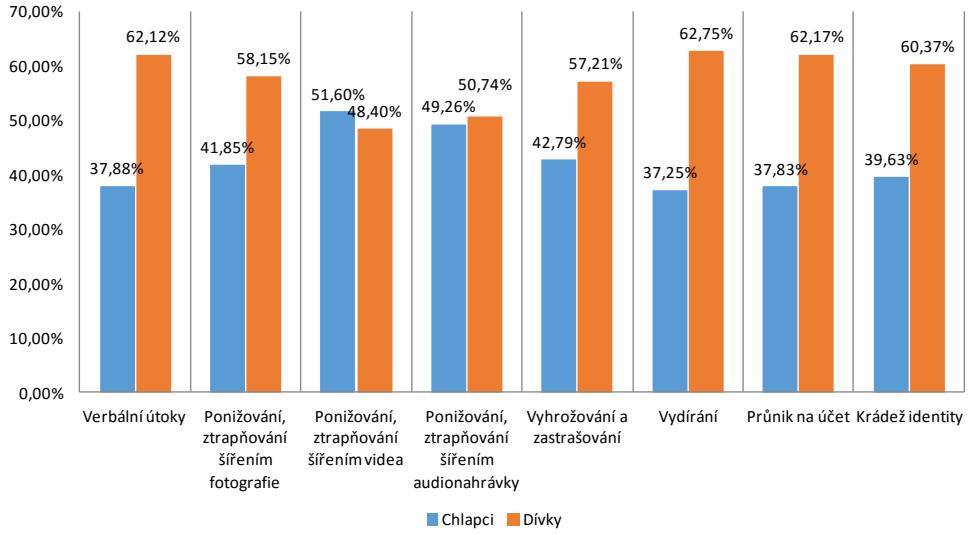
(n=16 253-27 538)

Poznámka: Počet respondentů byl u každé otázky jiný, jednotlivé formy respondentů se zkoumaly samostatně (oběť, agresor, platforma apod.). Dále aplikováno např. u agresorů. Ve všech případech jde o opakované formy útoku v rámci 1 kalendářního roku.

Nejčastěji jsou děti v České republice vystaveny průnikům na účet (prolomení hesla do online účtu), které potvrzuje více než 34 % (34,80 %) oslovených dětí. Na dalších pozicích pomyslného žebříčku nejčastějších forem kyberšikany se objevují verbální útoky (34,33 %) a poměrně rozšířené je také vyhrožování a zastrašování (17,84 %).

Podle výsledků našeho výzkumu se stávají oběťmi jednotlivých forem kyberšikany častěji dívky než chlapci, a to téměř ve všech sledovaných formách.

Graf 1. Kyberšikana u českých dětí – oběti (chlapci vs. dívky)



Tab 4. Rozdíly mezi oběťmi kyberšikany (chlapci vs. dívky)

Forma	***n*** ***(chlapci)***	***n*** ***(dívky)***	***%*** ***(chlapci)***	***%*** ***(dívky)***
Verbální útoky	3545	5813	37,88	62,12
Ponižování, ztrapňování šířením fotografie	1241	1724	41,85	58,15
Ponižování, ztrapňování šířením videa				
Ponižování, ztrapňování šířením audia	775	727	51,60	48,40
Vyhrožování a zastrašování	366	377	49,26	50,74
Vydírání	1445	1932	42,79	57,21
Průnik na účet	704	1186	37,25	62,75
Krádež identity	1463	2404	37,83	62,17
	1085	1653	39,63	60,37

Poznámka: Při srovnání celkových výsledků s výsledky pro jednotlivé skupiny dle pohlaví a věku došlo k odchylce 1,04 %, což představuje respondenty, kteří nevyplnili své pohlaví, ale vyplnili ostatní položky výzkumného nástroje.

3.2.3 Výsledky výzkumu – původci kyberšikany

V dalších částech výzkumu jsme se zaměřili na formy kyberšikany, které jsou využívány dětskými agresory. Následující tabulka shrnuje výsledky zjištění.

Deskriptivní oddíl

Tab 5. Kyberšikana u českých dětí (dle jednotlivých forem) – útočníci

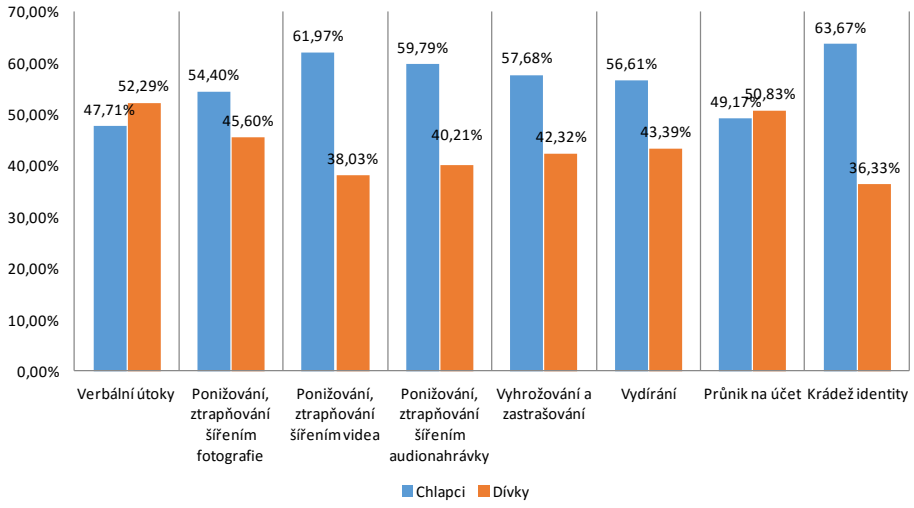
	n	%	n (total)
Verbální útoky	2 824	**12,22**	23 110
Vyhrožování a zastrašování	1 273	5,73	22 209
Krádež identity	509	8,97	5 675
Vydírání	564	2,56	22 061
Ponižování, ztrapňování šířením fotografie	1 251	6,75	18 541
Ponižování, ztrapňování šířením videa	705	3,23	21 841
Ponižování, ztrapňování šířením audia	575	2,61	22 021
Průnik na účet	5 492	**24,93**	22 032

(n=5 675-23 110)

Rozložení jednotlivých forem kyberšikany ze strany agresorů odpovídá rozložení forem kyberšikany, které zažívají oběti. Nejvíce frekventovanou formou útoku, kterou potvrzují dětští agresoři, jsou průniky na účet (24,93 %), následované verbálními útoky (12,22 %).

Pachateli – agresory – se dle našeho výzkumu stávají častěji chlapci než dívky – s výjimkou verbálních útoků, u těch jsou agresory častěji dívky.

Graf 2. Kyberšikana u českých dětí – útočníci (chlapci vs. dívky)



Tab 6. Rozdíly mezi pachateli kyberšikany (chlapci vs. dívky)

Forma	***n*** *(chlapci)*	***n*** *(dívky)*	***%*** *(chlapci)*	***%*** *(dívky)*
Verbální útoky	1341	1470	47,71	52,29
Ponižování, ztrapňování šířením fotografie	680	570	54,40	45,60
Ponižování, ztrapňování šířením videa	440	270	61,97	38,03
Ponižování, ztrapňování šířením audia	348	234	59,79	40,21
Vyhrožování a zastrašování	710	521	57,68	42,32
Vydírání	321	246	56,61	43,39
Průnik na účet	2687	2778	49,17	50,83
Krádež identity	326	186	63,67	36,33

Poznámka: Při srovnání globálních výsledků s výsledky pro jednotlivé skupiny dle pohlaví a věku došlo k odchylce 0,5 %, což představuje respondenty, kteří nevyplnili své pohlaví, ale vyplnili ostatní položky výzkumného nástroje.

Tab 7. Platformy a služby využívané k útokům na děti

	n	*%*
Sociální síť	4942	48,84
SMS	2668	26,37
Veřejný chat	2209	21,83
Neveřejný chat	2196	21,70
Jiná služba	910	8,99
E-mail	715	7,07
Blog	413	4,08

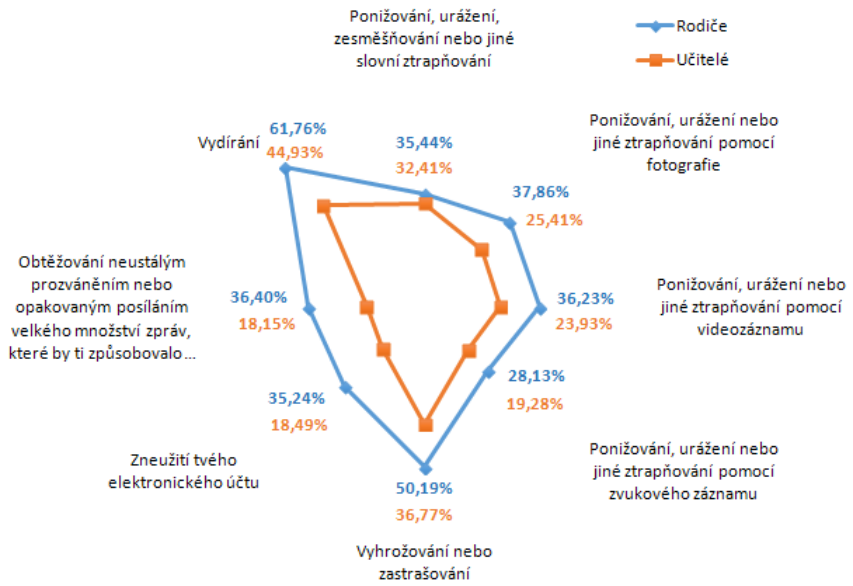
(n=10 118)

Nejčastější internetovou platformu, která je ke kyberšikaně zneužívána, představují sociální sítě (zejména sociální síť Facebook a Ask.fm). Opakované útoky v kyberprostoru potvrzuje přes 48 % českých respondentů. Kyberšikana také často probíhá prostřednictvím SMS zpráv (26,37 % útoků) a veřejného (21,83 %) a neveřejného (21,70 %) chatu.

V posledních letech se také k útokům stále více využívají webkamery, které umožňují získat od oběti audiovizuální materiály a využít je k následnému útoku. Zneužití webkamery ke kyberšikaně potvrzuje 2,67 % respondentů.

V dalších částech výzkumu jsme se zaměřili na otázku, zda by děti kontaktovaly rodiče či učitele v případě, že zažívají různé formy kyberšikany.

Graf 3. Koho by děti kontaktovaly?



V praxi platí, že čím je projev kyberšikany nebezpečnější, tím častěji se děti obracejí s prosbou o pomoc na dospělé. Rodiče by respondenti kontaktovali zejména v případech vydírání (61,76 % respondentů) a vyhrožování (50,19 %). Pro srovnání – při vydírání učitele kontaktuje 44,93 % českých dětí, při vyhrožování 36,77 %. Přibližně třetina dětí uvádí, že nekontaktují v případě kyberšikany ani učitele ani rodiče.

3.2.4 Přepínání rolí mezi obětí a útočníkem

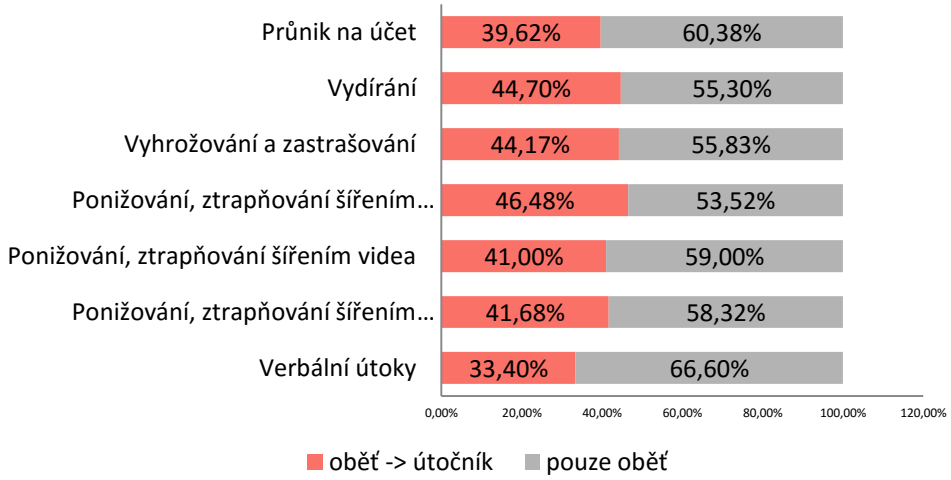
V dalších částech jsme se zaměřili na přepínání rolí mezi obětí a útočníkem. Nejprve jsme se zaměřili na to, zda se oběť kyberšikany stává útočníkem častěji, než respondenti, kteří kyberšikanou napadeni nebyli. Následně jsme analyzovali a popsali 2 základní formy přepínání OBĚŤ ←→ ÚTOČNÍK:

a) oběť se stává útočníkem, který využívá stejnou formu útoku, jakou zažíval jako oběť,
b) oběť se stává útočníkem, který využívá libovolnou formu kyberšikany.

Deskriptivní oddíl

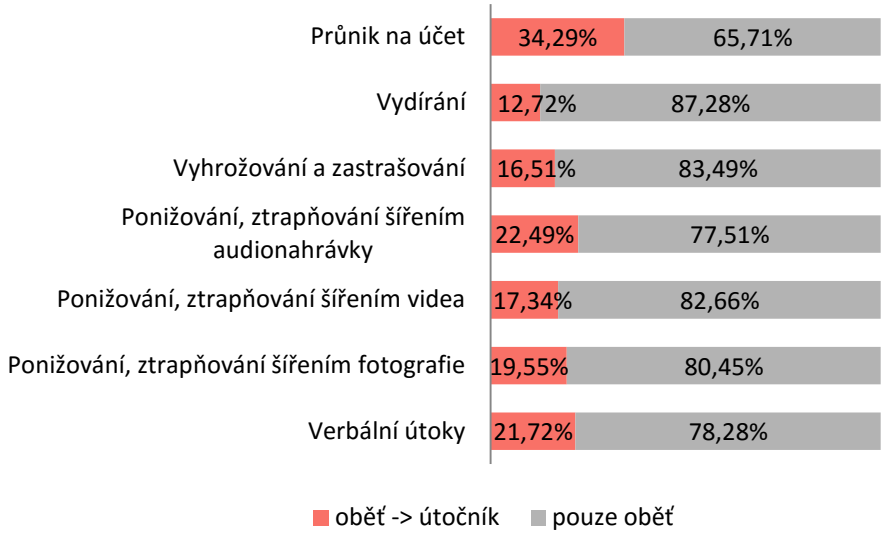
Následující grafy vyjadřují, jak moc se v daném vzorku přepínání rolí vyskytuje.

Graf 4. Přepínání rolí oběť – útočník (využívající libovolnou formu útoku)



Na základě výše uvedených výsledků výzkumu lze usuzovat, že se dětské oběti stávají agresory poměrně často – např. dítě, které bylo vydíráno, se v 44,70 % mění v útočníka, který vůči dětem využívá libovolné formy útoku. Méně často útočníci využívají stejnou formu útoku, jak zachycuje další graf. Pro potvrzení uvedeného předpokladu jsme využili induktivních statistických postupů, viz **Relační oddíl.**

Graf 5. Přepínání rolí oběť – útočník (využívající stejnou formu útoku)



Přepínání rolí je detailněji zachyceno v následující tabulce. Sloupec *Oběti (n)* zachycuje počty obětí jednotlivých forem kyberšikany. Následující sloupce vyjadřují „přepnutí role“ – oběť se mění v útočníka, který využívá stejnou formu útoku, jakou byla oběť šikanována (*Útočník A*), nebo se mění v útočníka, který využívá k útoku libovolnou formu útoku (*Útočník B*).

Tab 8. Přepínání rolí mezi obětí a útočníkem (data)

	Oběti (n)	***Útočník A (n_1)***	***Útočník B (n_2)***
Verbální útoky	9455	2054	3158
Vyhrožování a zastrašování	3380	558	1493
Vydírání	1879	239	840
Ponižování, ztrapňování šířením fotografie	2982	583	1243
Ponižování, ztrapňování šířením videa	1505	261	617
Ponižování, ztrapňování šířením audia	738	166	343
Průnik na účet	3864	1325	1531

Relační oddíl

Relační oddíl sestává z výsledků induktivních statistických postupů. V našem výzkumu jsme využili statistické metody pro analýzu nominálních dat, zejména pak test nezávislosti chí-kvadrát pro čtyřpolní tabulku. Níže uvádíme pouze vybrané výsledky provedených relačních analýz.

K ověření hypotetického tvrzení, zda se útočníky kyberšikany stávají častěji její oběti než jedinci, kteří kyberšikanu neprožili, jsme získaná data nejdříve zavedli do čtyřpolní tabulky a poté je podrobili statistickým analýzám. K vyhodnocení naměřených dat byl použit test nezávislosti chí-kvadrát a míry těsnosti vztahu (fí-koeficient, tetra-chorický koeficient korelace a koeficient kontingence C). Přepínání rolí bylo ověřováno u všech zaznamenaných projevů kyberšikany.

1. Verbální útoky:

Analýza uvedeného projevu kyberšikany u agresorů i obětí prokázala existenci statisticky významného vztahu (signifikace $p<0,0001$).

Na základě uvedeného výsledku bylo možno vyvodit následující závěr:

Respondenti, kteří byli napadeni verbálními útoky, uvádějí častěji než respondenti, kteří takto napadeni nebyli, že sami tento druh útoku také realizovali vůči jiným osobám (signifikace $p<0,0001$).

2. Vyhrožování a zastrašování:

Analýza uvedeného projevu kyberšikany u agresorů i obětí prokázala existenci statisticky významného vztahu (signifikace $p<0,0001$).

Na základě uvedeného výsledku bylo možno vyvodit následující závěr:

Respondenti, kterým bylo vyhrožováno, nebo byli zastrašováni, uvádějí častěji než respondenti, kteří takto napadeni nebyli, že sami tento druh útoku realizovali vůči jiným osobám (signifikace $p<0,0001$).

3. Vydírání:

Analýza uvedeného projevu kyberšikany u agresorů i obětí prokázala existenci statisticky významného vztahu (signifikace $p<0,0001$).

Na základě uvedeného výsledku bylo možno vyvodit následující závěr:

Respondenti, kteří byli vydíráni, uvádějí častěji než respondenti, kteří takto napadeni nebyli, že sami tento druh útoku realizovali vůči jiným osobám (signifikace p<0,0001).

4. Ponižování, ztrapňování šířením fotografie:

Analýza uvedeného projevu kyberšikany u agresorů i obětí prokázala existenci statisticky významného vztahu (signifikace p<0,0001).

Na základě uvedeného výsledku bylo možno vyvodit následující závěr:

Respondenti, kteří byli ponižováni, ztrapňováni pomocí fotografie, uvádějí častěji než respondenti, kteří takto napadeni nebyli, že sami tento druh útoku realizovali vůči jiným osobám (signifikace p<0,0001).

5. Ponižování, ztrapňování šířením videa:

Analýza uvedeného projevu kyberšikany u agresorů i obětí prokázala existenci statisticky významného vztahu (signifikace p<0,0001).

Na základě uvedeného výsledku bylo možno vyvodit následující závěr:

Respondenti, kteří byli ponižováni, ztrapňováni pomocí videonahrávky, uvádějí častěji než respondenti, kteří takto napadeni nebyli, že sami tento druh útoku realizovali také vůči jiným osobám (signifikace p<0,0001).

6. Ponižování, ztrapňování šířením audia:

Analýza uvedeného projevu kyberšikany u agresorů i obětí prokázala existenci statisticky významného vztahu (signifikace p<0,0001).

Na základě uvedeného výsledku bylo možno vyvodit následující závěr:

Respondenti, kteří byli ponižováni, ztrapňováni pomocí audionahrávky, uvádějí častěji než respondenti, kteří takto napadeni nebyli, že sami tento druh útoku realizovali také vůči jiným osobám (signifikace p<0,0001).

Průnik na účet:

Analýza uvedeného projevu kyberšikany u agresorů i obětí prokázala existenci statisticky významného vztahu (signifikace p<0,0001).

Na základě uvedeného výsledku bylo možno vyvodit následující závěr:

Respondenti, kterým se někdo dostal bez jejich svolení do elektronického účtu, uvádějí častěji než respondenti, kteří takto napadeni nebyli, že sami tento druh útoku realizovali vůči jiným osobám (signifikace p<0,0001).

3.3 Sexting u českých dětí

V rámci výzkumu jsme sledovali 2 základní formy šíření sextingu – umístění sexuálně laděného materiálu na internet (např. do profilu v rámci sociální sítě či do databáze digitálního úložiště fotografií) a přímé odeslání vlastního sexuálního materiálu jiným osobám (např. příteli, přítelkyni, kamarádovi, partnerovi atd.). Na základě těchto východisek vznikly 2 základní otázky (Q1, Q2), rozšířené o další subotázky monitorující motivaci respondentů k provozování sextingu. Zadání doplňuje otázka Q3, která se zaměřuje na nebezpečnost sextingu.

Deskriptivní oddíl

Q1. Otázka: **Umístil/-a jsi někdy na internet svou „sexy" fotografii nebo video, na kterých jsi částečně svlečený/-á nebo úplně nahý/-á?**

Sexting ve formě umístění vlastního intimního materiálu (fotografie či videa) na internet provozuje 7,41 % populace dětí ve věku 11–17 let (47 % tvořili muži, 53 % ženy).

Motivace pro Q1 (z odpovědí respondentů):

1. Byla to fotografie pro mojí holku / mého kluka. Moje holka/kluk chtěl/a vidět moje tělo.
2. Ze srandy.
3. Chtěl/a jsem se pochlubit, jak dobře vypadám.
4. Pubertální nerozvážnost.
5. Jen tak… pro zvýšení sebevědomí.
6. Chtěl/a jsem pozornost.
7. Poslala jsem fotku kamarádům na aplikaci Snapchat, u které fotka za 10 vteřin zmizí.

Q2. Otázka: **Poslal/-a jsi někdy někomu svou „sexy" fotografii nebo video, na kterých jsi částečně svlečený/-á nebo úplně nahý/-á?**

Vlastní sexuálně laděné materiály odeslalo jiným osobám 12,14 % respondentů ve věku 11–17 let.

Motivace pro Q2 (z odpovědí respondentů):

1. Byla to pro mého partnera (chtěl ji po mně, poslal mi na oplátku svou).
2. Ze srandy. Ta holka ji chtěla, později jsme se poznali osobně.
3. Můj kluk mě vydíral, že pokud mu fotku nepošlu, tak se se mnou rozejde.
4. Byl to kamarád - známe se naživo a věřím mu.
5. Obratem jsem dostal podobnou fotografii.
6. Byla to sázka a věděla jsem, že to dotyční nezneužijí.

Q3. Myslíš, že může být odesílání nebo zveřejňování fotografií nebo videí, na kterých jsi částečně svlečený/-á nebo nahý/-á, riskantní?

Více než tři čtvrtiny respondentů (77,50 %) považují sexting za rizikový a riskantní. Mezi nejčastější důvody, proč lze považovat sexting za rizikový, uvedli respondenti následující (seřazeno dle četnosti).

1. Intimní fotografie může být zneužita, například k vydírání a zesměšňování.
2. Když by se fotografie dostala na veřejnost, někdo mě potom může obtěžovat.
3. Fotky by mohl získat nějaký pedofil. A třeba by mě mohl znásilnit.
4. Fotografie může spustit kyberšikanu - lidé mě můžou zesměšňovat, psát urážlivé komentáře atd.
5. Příjemce by mohl fotku někde zveřejnit - a ta by se pak mohla nekontrolovaně šířit internetem.
6. Mohu se stát obětí pronásledování (stalkingu) a obtěžování.
7. Nahota je moje osobní věc.
8. Sexting mi může ohrozit budoucnost, třeba zaměstnání.
9. Co se dá na internet, to tam zůstane navždy. Fotky nikdy nejsou z internetu úplně smazané.
10. Moje fotky může někdo nahrát např. na pornografické stránky.

12,14 % respondentů rovněž uvedlo, že šířili materiál s obnaženými záběry mezi další uživatele internetu.

Relační oddíl

V rámci sextingu nás zajímalo, zda kromě respondentů samotných, kteří vyvěšují své intimně laděné (tj. částečně nebo zcela obnažené) fotografie na internet, následně umisťují jejich intimní fotky na internet i jejich kamarádi.

Prostřednictvím induktivní statistiky jsme prokázali existenci statisticky významného vztahu (signifikace p<0,0001).

Na základě uvedeného výsledku bylo možno vyvodit následující závěr:

Respondenti, jejichž intimně laděnou fotografii nebo video umístil jejich kamarád na internet, uvádějí častěji než ostatní respondenti, že svoji „sexy" fotografii umístili na internet sami (signifikace p<0,0001).

Z toho je patrné, že děti, které neuváženě zveřejňují své intimní fotografie na internetu, jsou daleko častěji posléze postiženy šířením daných materiálů prostřednictvím svých známých a kamarádů.

3.4 Děti a internetové seznamování

Děti a dospívající využívají internetové služby samozřejmě také ke komunikaci s ostatními a k navazování přátelství. Část výzkumu se proto zaměřovala právě na tyto oblasti.

Deskriptivní oddíl

Většina dětí (54,30 %) na internetu komunikuje s uživateli internetu, které neznají osobně a jejichž opravdovou identitu nemají jak ověřit. V zásadě tak mohou komunikovat jak s jinými dětmi, tak i dospělými. Přibližně 1/4 dětí (26,92 %) potvrdila, že po nich jejich internetový kamarád chtěl, aby udrželi komunikaci v tajnosti a aby se nikdo nedozvěděl, že se spolu baví a o čem spolu komunikují. Stejně tak 22,27 % dětí potvrdilo, že to samé požadovali po svých internetových kamarádech také oni.

V další části výzkumu jsme se zaměřili na to, zda jsou děti ochotné jít na osobní schůzku v reálném světě s lidmi, které znají pouze z internetu. 40,22 % dětí potvrdilo, že pokud by je internetový kamarád požádal o osobní schůzku v reálném světě, šly by na ní. Počet dětí, které jsou ochotné na schůzku jít, tak vzrostl ve srovnání s výzkumem Nebezpečí internetové komunikace IV (Kamil Kopecký et al., 2014a) o více než 4 %.

O schůzce by pak děti nejčastěji řekly kamarádům (55,56 %) či rodičům (42,03 %).

Tab 9. Osoby, kterým by se dítě svěřilo s tím, že bylo osloveno s žádostí o osobní schůzku

	2014 (%)	*2013 (%)*	*Změna (%)*
Kamarádi	55,56	58,70	-3,14
Rodiče	42,03	41,06	0,97
Jiné osoby	8,21	6,89	1,32
Učitelé	3,02	3,00	0,02
Nikdo	16,18	15,01	1,17

Dále jsme se zaměřili na skutečný počet dětí, které byly na osobní schůzku s neznámým uživatelem či uživatelkou internetových služeb pozvány. 43,56 % dětí potvrdilo, že bylo pozváno na osobní schůzku, více než polovina z pozvaných pak na schůzku šla (54,91 %). Téměř polovina dětí (49,96 %) však také potvrdila, že své internetové kamarády na osobní schůzky také pozvala.

Více než polovina dětí (58,25 %) považuje online komunikaci s lidmi, které nezná osobně, za riskantní a nebezpečnou. Pro ilustraci uvádíme několik odpovědí respondentů:

1. *Útočník by mohl mít falešný profil. Na schůzce by mě mohl sexuálně zneužít. (dívka, 13 let)*
2. *Útočník může být pedofil (nebo jiný úchylák) a mohl by mě sexuálně obtěžovat. (chlapec, 15 let)*
3. *Neznámý uživatel by mě mohl unést, třeba do zahraničí. (chlapec, 14 let)*
4. *Kdybych šel na schůzku, měl bych problém s rodiči. (chlapec, 12 let)*
5. *Ten „internetový kamarád" by mě mohl na schůzce napadnout, nebo mě i zabít. A prodat na orgány. (chlapec, 14 let)*
6. *Na schůzce by mi mohl vnutit drogy. (dívka, 13 let)*
7. *Protože podle jejich profilu nepoznáme a nikdy si nemůžeme být jisti, kdo to je. Je možné, že budeme čekat někoho úplně jiného a můžeme se setkat s pedofilem, nebo jiným zlým člověkem. (dívka, 15 let)*
8. *Může se jednat o podvodníka nebo úchyla, který se vydával za někoho úplně jiného. Schůzka na nějakém osamoceném místě je proto naprosto vyloučená, aby to člověka neohrozilo. Schůzka na veřejnosti, popřípadě s dalšími přáteli je v pořádku, to je bezpečné. (dívka, 16 let)*
9. *Je to velmi nebezpečné, může mi lhát, nejdříve říkat, že je mladý a pak se z něj může vyklubat pedofil či jiný nemocný člověk. Každý tohle z nás ví*

nebo alespoň já to vím dostatečně na to, abych věděla, co v danou situaci dělat, nepřidávám si dané lidi mezi svůj okruh přátel. Veřejnost nás na tohle hodně upozorňuje a já stále nechápu, jak někdo může být tak naivní a s někým takovým se setkat. Není dobré někomu takhle důvěřovat. (dívka, 16 let)

10. *Protože je možnost setkání se s úchylem, který tě zatáhne do kutlochu a tam ti ho narve do prdele. (chlapec, 15 let)*

To, že se dítě na internetu seznamuje, ještě automaticky neznamená, že bude vystaveno útoku – ve většině případů pravděpodobně děti skutečně komunikují s lidmi, kteří jim nechtějí ublížit (převážně vrstevníky). Riziko útoku však existuje. Děti často věří, že si dokáží na osobní schůzce poradit – sejdou se např. na veřejném místě, na osobní schůzku s sebou vezmou kamaráda, vezmou si s sebou mobilní telefon, aby bylo možné kontaktovat policii apod. Bohužel tato opatření nejsou v praxi účinná.

Relační oddíl

Ochotu dětí jít na osobní schůzku s kamarádem, kterého poznaly na internetu, lze považovat za velmi rizikový počin. V rámci preventivních aktivit projektu E-Bezpečí jsou proto děti upozorňovány na možná rizika takového jednání a je jim razeno, aby na schůzky s lidmi, jež poznaly na internetu, raději nechodily. A pokud by na ni i přesto chtěly dorazit, tak je jim doporučováno, aby o ní informovaly své rodiče.

V této souvislosti nás tak zajímalo, jestli lze nalézt nějaké rozdíly ve svěření se někomu o záměru jít na schůzku s kamarádem z internetu mezi pohlavími a věkem respondentů.

Prostřednictvím induktivní statistiky jsme prokázali existenci statisticky významných vztahů (signifikace $p<0,0001$).

Na základě uvedeného výsledku bylo možno vyvodit následující závěry:

Dívky uvádějí častěji než chlapci, že by o pozvání na schůzku řekly kamarádům nebo sourozencům (signifikace $p<0,0001$).

Chlapci uvádějí častěji než dívky, že by o pozvání na schůzku řekli rodičům (signifikace $p<0,0001$).

Starší děti (15–17 let) uvádějí častěji než děti mladší (11–14 let), že by o pozvání na schůzku řekli kamarádům (signifikace $p<0,0001$).

Starší děti (15–17 let) uvádějí častěji než děti mladší (11–14 let), že by o pozvání na schůzku řekly rodičům (signifikace p<0,0001).

Z těchto závěrů je patrné, že se dívky o pozvání na schůzku s kamarády, se kterými se seznámily na internetu, svěřují svým přátelům častěji než chlapci. Naproti tomu chlapci se zase o pozvání na danou schůzku svěřují svým rodičům častěji než dívky. Rozdíly ve svěřování se o záměru jít na osobní setkání byly zaznamenány i ve věkové struktuře respondentů. Starší děti (15–17 let) se o plánovaném setkání svěřují svým kamarádům a rodičům častěji než mladší děti (11–14 let).

3.5 Sdílení osobních údajů v prostředí internetu

Pro děti ale také dospělé uživatele internetu je v současnosti zcela normální sdílet v prostředí internetových služeb velké množství osobních údajů. Údaje mohou být centralizovány (např. v prostředí sociálních sítí), mohou však být na internetu také roztříštěné na více místech. V zásadě je však poměrně snadné osobní údaje na internetu vyhledat a spojit je do profilu potenciální oběti.

Deskriptivní oddíl

Následující tabulka obsahuje osobní údaje, které o sobě děti běžně na internetu zveřejňují.

Tab 10. Osobní údaje, které české děti běžně zveřejňují na internetu

Osobní či jiný citlivý údaj	*Četnost (n)*	*%*
Jméno a příjmení	17099	76,99
Fotografie obličeje	12529	56,41
E-mail	12375	55,72
Adresa školy	4960	22,33
Telefonní číslo	4695	21,14
Adresa bydliště	3285	14,79
Kontaktní údaje k messengeru (ICQ, Skype)	3107	13,99
Rodné číslo	672	3,03
Heslo k emailovému účtu	530	2,39
PIN kreditní karty	285	1,28
Žádný osobní údaj	2232	10,05

(Celková četnost n=22 209)

Mezi osobní údaje, které o sobě děti běžně na internetu sdělují, patří zejména jméno a příjmení (76,99 % dětí má tyto údaje na internetu uvedeny), fotografie

obličeje a e-mail. Sdílení fotografií obličejů se dnes již stalo běžnou praktikou, velké množství dětských (ale také dospělých uživatelů) sdílí svoje „selfie“ na internetu – převážně v prostředí sociálních sítí). Selfie je typ fotografického autoportrétu pořízeného z ruky za pomoci fotoaparátu či chytrého telefonu (často proti zrcadlu).

Selfie či jiný druh vlastního autoportrétu na internetu sdílí 56,41 % českých dětí – nejčastěji prostřednictvím sociální sítě Facebook. 29,98 % dětí potvrdilo, že po nich jejich internetový kamarád chtěl fotografii obličeje, čemuž více než polovina z oslovených dětí vyhověla (54,6 % z nich). Na druhou stranu 23,44 % dětí také požadovalo po svých internetových kamarádech fotografii obličeje.

Je nutno mít na paměti, že fotografie obličeje se velmi často využívají jako nástroje pro různé formy online útoků na dítě, např. v rámci kyberšikany či kybergroomingu. 65,52 % dětských respondentů si rovněž myslí, že zveřejňování či odesílání fotografií obličeje může být riskantní, přesto však fotografie sdílejí a odesílají ostatním.

Proč je rizikové sdílet fotografii obličeje? (výběr z odpovědí respondentů)

1. *Může být použita proti vám.*
2. *Fotku může někdo zneužít.*
3. *Protože to může ohrožovat váš život.*
4. *Mohl by tě nějak najít.*
5. *Nikdy nevíme, kdo se skrývá za počítačem, může to být pedofil a ten si mě pak podle fotky najde.*
6. *No nevím, může nás pak nějak vydírat?*
7. *Mám mladší sestru a nedovedu si představit, nebo spíš nechci si představit, že by někomu poslala fotku a něco se jí stalo. V mém případě, je to něco jiného. Jsem chlap, ale i tak, bych někomu koho neznám neposlal svou fotku.*
8. *Může na druhé straně být jiná osoba, než za kterou se vydává -> toto řeším tak, že s osobou nejdříve jdu na videohovor např. na Skype.*
9. *Když vypadáš blbě, budou se ti posmívat.*
10. *Dotyčný této fotky může zneužít, např. může jí sdílet bez mého svolení, může ním někoho vydírat (např. rodiče), dále se za mě může vydávat apod.*
11. *Protože toho může někdo využít např. posílat jí někomu nebo pronásledovat dotyčnou osobu.*
12. *Kdo má na internetu svoje fotografie nebo údaje o sobě, tak už je nikdy definitivně nesmaže. Pokud to mám k něčemu přirovnat, tak k tomu, že*

ten jedinec je jako nahý-vždy se může stát, že ty jeho fotky a jeho údaje někdo najde.

13. *Riziko zneužití do nějaké fotomontáže, riziko, že za mě někdo třeba podá inzerát s fotkou nebo naopak na nějaký takový odpoví.*
14. *Znásilnění, zneužití, vydírání, urážení, posmívání, okrádání, sledování, zabití.*
15. *Protože ten druhý to může zveřejňovat a upravovat a by to vypadalo strašně trapný a by to tomu druhému ublížilo, možná si sním rozumí ale nikdy nikdo neví kdo tam sedí na druhé straně.*
16. *Může ji nějakým způsobem zneužít – třeba založit falešný profil a moji fotografii tam použít.*
17. *Myslím si, že může zneužít mou fotografii k tomu aby si o mě mohl zjistit informace které bych mu jinak nechtěla dobrovolně dát např. :najít si mou rodinu a příbuzné, které bych tímto způsobem mohla ohrozit, moje bydliště, kam chodím do školy a jiné nebezpečné informace.*
18. *Protože by naší fotku zneužit k nepravostem.*
19. *Pokud pošleme někomu fotografii svého obličeje, může se mu podařit vytvořit fotomontáž s naším obličejem a těžko se pak vysvětluje spolužákům a lidem z okolí, že na té fotografii je tělo někoho jiného. Dalším rizikem je to, že nás dotyčný na ulici pozná a pak už je jednoduché nás vystopovat.*
20. *Lze dohledat podobné fotografie službami Google a vyhledat více informací o mně. Proto pro dané účely používám fotku určenou pouze pro zasílání jiným lidem. Ale celkově jde o neznámého člověka, takže je zde už nějaký podvědomý strach. Ale riskuji kvůli poznání nových lidí.*
21. *Může se na sociální síti podívat do tvých přátel fotografii jim poslat a ti mu můžou říct, kdo jsem a kde bydlím. Může jim třeba namluvit, že mě zná ze školky a rád by se se mnou po takové dlouhé době viděl nebo tak něco.*
22. *Může to být nějaký sexuální a nebezpečný deviant, který se vydává za někoho jiného.*
23. *Fotky, které mohou být poslané dotyčné osobě, která si o ně požádá, jak fotky obličeje, tak fotky intimní, by mohly být zneužity a rozposlány do různých internetových sití, nebo také různým lidem. Fotka by mohla kolovat, a když si pak na vás lidi ukazují, a říkají to je on/ona na té fotce, je to velmi nepříjemné.*

24. *Když člověk někomu pošle fotografii, tak druhá strana to může zneužít za účelem zkopírování identity a tak vás uvést do problému.*
25. *Protože si nás někdo podle fotografie obličeje může najít a znásilnit nebo jinak ublížit.*

(Výpovědi dětí neprošly jazykovou korekturou.)

Tab 11. Osobní údaje, které české děti sdělují svým internetovým kamarádům

Osobní či jiný citlivý údaj	***Četnost (n)***	***%***
Jméno a příjmení	13930	62,86
Fotografie obličeje	9691	43,73
E-mail	8660	39,08
Adresa školy	8424	38,01
Telefonní číslo	4938	22,28
Adresa bydliště	3485	15,73
Kontaktní údaje k messengeru (ICQ, Skype)	3304	14,91
Rodné číslo	740	3,34
Heslo k emailovému účtu	407	1,84
PIN kreditní karty	328	1,48
Žádný osobní údaj	4817	21,74

(Celková četnost n=22 162)

Relační oddíl

V deskriptivním oddíle jsme se zmínili o rizicích spojených s nejnebezpečnějším osobním údajem, který představuje fotografie obličeje. A dle námi naměřených dat je patrné, že se jedná o druhý nejčastěji zveřejňovaný osobní údaj.

V relačním oddíle nás proto zajímalo, zda nějak souvisí zveřejňování obrazového materiálu (fotografie, videa) s intenzitou následného zveřejňování těchto materiálů známými od respondentů z prostředí internetu.

Prostřednictvím induktivní statistiky jsme prokázali existenci statisticky významných vztahů (signifikace $p<0,0001$).

Na základě uvedeného výsledku bylo možno vyvodit následující závěr:

Respondenti, jejichž fotografii nebo video umístil jejich známý na internet, uvádějí častěji než ostatní respondenti, že svoji fotografii nebo video umístili na internet sami (signifikace $p<0,0001$).

3.6 České děti a sociální sítě

České děti patří k nejaktivnějším uživatelům sociálních sítí v Evropě. Další náš výzkum v rámci projektu E-Bezpečí tudíž směřoval to této oblasti.

Deskriptivní oddíl

Nejčastěji využívanou sociální sítí je u českých dětí Facebook s více než 80 % aktivních uživatelů. Více než polovina dětí, které Facebook používají, je ve věku 11–15 let (53,12 %). Lze předpokládat, že velké množství z nich nesplňuje minimální povolenou věkovou hranici pro vstup na tuto sociální sít, tj. 13 let věku. Na dalších místech se umístila sociální síť Google+, následovaná českou sociální sítí (dnes již spíše internetovou seznamkou) Lidé.cz. Děti dále využívají mikroblogovací systém Twitter, sociální síť Spolužáci.cz a síť Ask.fm.

Tab 12. Sociální sítě, které používají české děti

Sociální síť	*Četnost (n)*	*%*
Facebook	17344	80,95
Google+	9546	44,56
Lidé. cz	5931	27,68
Twitter	5678	26,50
Spolužáci. cz	4865	22,71
Ask. fm	4301	20,07
Libímseti. cz	1435	6,70
Gifyo	1179	5,50
Myspace	1152	5,38
LinkedIn	514	2,40

(Celková četnost n=21 425)

Pokud dítě osloví neznámý člověk s tím, aby si jej přidalo mezi své přátele na sociální síti (např. na Facebooku), 26,2 % z nich to učiní.

Zaměříme-li se na data o výskytu kyberšikany mezi dětskými uživateli sociální sítě Facebook, zjistíme, že více než třetina z nich zažila kyberšikanu prostřednictvím verbálního ponižování (38,08 % dětí). Kompletní přehled o výskytu kyberšikany na Facebooku pak uvádí následující tabulka.

Tab 13. Kyberšikana u dětských uživatelů Facebooku (oběti)

Forma kyberšikany	*Četnost (n)*	*%*
Verbální útoky	6604	38,08
Vyhrožování a zastrašování	2162	12,47
Vydírání	1007	5,81
Ponižování, ztrapňování šířením fotografie	2648	15,27
Ponižování, ztrapňování šířením videa	1349	7,78
Ponižování, ztrapňování šířením audia	2909	16,77
Průnik na účet	2124	12,25

(Celková četnost n=17 344)

4 Rizikové chování slovenských dětí v prostředí internetu (2014)

Výzkum rizikového chování slovenských dětí v prostředí internetu navazuje na výzkumy rizikového chování českých dětí, které byly realizovány Centrem prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci v letech 2010–2014. Aby bylo možné výsledná zjištění komparovat, zvolili jsme pro výzkum stejný výzkumný nástroj.

4.1 Metodologie

4.1.1 Charakteristika výzkumného vzorku

Výzkumu realizovaného na území Slovenské republiky se zúčastnilo 1 466 (n=1 466) respondentů ve věku 11–17 let. 71,10 % vzorku tvořily děti ve věku 11–14 let, 28,9 % ve věku 15–17 let. 44,96 % tvořili chlapci, 55,04 % dívky. Výzkum probíhal ve všech krajích, nejvíce respondentů pocházelo z Trenčianského kraje (44,42 %) a Bratislavského (18,82 %).

4.1.2 Charakteristika výzkumného nástroje

Vlastní výzkum byl s ohledem na zamýšlené množství respondentů orientován kvantitativně a jako výchozí výzkumná metoda byla zvolena metoda dotazníková. Výzkumný nástroj, u kterého byly již v minulosti ověřeny jeho vlastnosti (validita, reliabilita), obsahoval celkem 71 položek (40 dichotomických, 2 polytomické, 22 s více možnými odpověďmi a 7 otevřených), jež vznikly na základě teoretických poznatků a byly sestaveny takovým způsobem, aby reflektovaly stanovené cíle a vzniklé problémy.

Dotazník byl respondentům distribuován elektronicky (on-line) prostřednictvím dotazníkového systému E-Bezpečí / Centra prevence rizikové virtuální komunikace, který disponuje e-mailovými adresami škol, školských zařízení, spolků zaměřených na děti a mládež a jiných institucí v České a Slovenské republice. Soupis adres pořídili členové výzkumného týmu v letech 2013–2014 z veřejně dostupných zdrojů.

Anonymní dotazník, jenž automaticky ověřoval, odkud byl odeslán (IP adresa, regionální příslušnost, monitoring chování respondentů za využití nástroje Google Analytics atd.), nabízel možnost uvedení e-mailové adresy školy, skrze niž mohli být její zástupci v kontaktu s výzkumným týmem.

Příprava výzkumu byla zahájena 1. 10. 2013, sběr dat probíhal od 1. 12. 2013 do 31. 3. 2014. Jejich vyhodnocení bylo realizováno v průběhu dubna 2014. Data byla naměřena převážně na nominální a ordinální úrovni, čemuž odpovídalo i jejich následné zpracování, použité numerické operace a statistika.

Výhodou elektronické verze výzkumného nástroje (dotazníku) byla automatizace sběru dat do příslušných tabulek. Následně bylo provedeno jejich třídění, zpracování a vyhodnocení.

4.2 Kyberšikana u slovenských dětí

Výzkum kyberšikany neprobíhal pouze v rámci České republiky, ale byl rozšířen i na Slovensko. Zajímalo nás, zda ve společnosti, která byla po mnoho let součástí společného státu, nalezneme nějaké rozdíly.

4.2.1 Sledované formy kyberšikany

V rámci výzkumu byly opět sledovány níže uvedené formy útoků spadající do oblasti kyberšikany:

a) Verbální útoky v kyberprostoru – ubližování formou ponižování, urážení, zesměšňování, ztrapňování dítěte.
b) Obtěžování prozváněním.
c) Vyhrožování a zastrašování dítěte.
d) Krádež identity.
e) Vydírání dítěte.
f) Ponižování, ztrapňování realizované šířením fotografie.
g) Ponižování, ztrapňování realizované šířením videa.
h) Ponižování, ztrapňování realizované šířením audia.

Aby byly tyto formy považovány za skutečnou kyberšikanu, výzkum sleduje jejich opakování v rámci jednoho roku (časová limita).

Výzkum sledoval fenomén kyberšikany z několika hledisek:
a) oběť kyberšikany (incidence, množství obětí v rámci časové jednotky, platformy, na kterých útok probíhá),
b) původce kyberšikany (incidence, množství útočníků v rámci časové jednotky, platformy, které jsou pro útok využity),
c) osoby zapojené do řešení kyberšikany (koho by oběť kontaktovala v situaci, kdy zažívá kyberšikanu),
d) další související jevy (specifické formy kyberšikany realizované např. prolomením účtu a následnou krádeží identity).

4.2.2 Výsledky výzkumu – oběti kyberšikany

Výsledky výzkumu jsme stejně jako v případě výzkumu u českých dětí rozdělili na oddíl deskriptivní a relační. Na deskriptivní problémy jsme opět hledali odpovědi skrze základní veličiny deskriptivní statistiky (výpočet charakteristik polohy – míry ústřední tendence, výpočet směrodatných odchylek, výpočet procent apod.), přičemž nechybělo ani jejich grafické znázornění.

Na relační výzkumné problémy a následnou verifikaci hypotetických tvrzení jsme využili induktivní statistické postupy, konkrétně test nezávislosti chí-kvadrát pro čtyřpolní tabulku.

Deskriptivní oddíl

Deskriptivní oddíl sestává z tabulek absolutních četností a procentuálních podílů jednotlivých sledovaných nebezpečných komunikačních jevů. Pro grafické znázornění distribuce naměřených dat a zvýraznění rozdílů v použitých platformách užívaných pro realizaci kyberšikany (průměrná hodnota vs. vydírání) byly použity histogramy – ty byly i pro znázornění přepínání rolí oběť–útočník.

Tab 14. Kyberšikana u slovenských dětí (dle jednotlivých forem) – oběti

	n	%	N (total)
Verbální útoky	416	**28,38**	1466
Vyhrožování a zastrašování	230	16,81	1368
Krádež identity	129	9,52	1355
Vydírání	95	6,94	1368
Ponižování, ztrapňování šířením fotografie	182	12,75	1427
Ponižování, ztrapňování šířením videa	73	5,29	1380
Ponižování, ztrapňování šířením audia	47	3,42	1376
Průnik na účet	365	26,94	1355

(n=1355-1466)

Poznámka: Počet respondentů byl u každé otázky jiný, jednotlivé formy respondentů se zkoumaly samostatně (oběť, agresor, platforma apod.). Dále aplikováno např. u agresorů.

Nejčastěji jsou děti na Slovensku vystaveny verbálním útokům, které potvrzuje více než 28 % (28,38 %) oslovených dětí. Na dalších pozicích pomyslného žebříčku nejčastějších forem kyberšikany se objevuje průnik na účet či prolomení hesla do online účtu (26,94%), poměrně rozšířené je také vyhrožování a zastrašování (16,81 %).

V dalších částech výzkumu jsme se zaměřili na formy kyberšikany, které jsou využívány dětskými agresory. Následující tabulka shrnuje výsledky zjištění.

4.2.3 Výsledky výzkumu – původci kyberšikany

V dalších částech výzkumu jsme se zaměřili na formy kyberšikany, které jsou využívány dětskými agresory na Slovensku. Následující tabulka shrnuje výsledky zjištění.

Deskriptivní oddíl

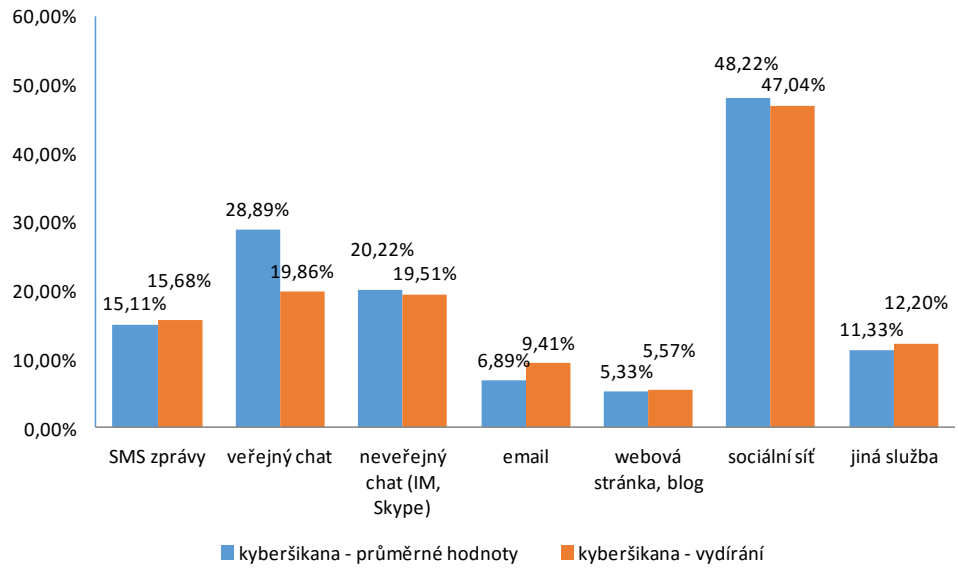
Tab 15. Kyberšikana u slovenských dětí (dle jednotlivých forem) – útočníci

	n	%	N (total)
Verbální útoky	161	**13,78**	1168
Vyhrožování a zastrašování	74	5,94	1245
Krádež identity	37	3,64	1016
Vydírání	47	3,72	1264
Ponižování, ztrapňování šířením fotografie	79	6,26	1262
Ponižování, ztrapňování šířením videa	46	3,62	1269
Ponižování, ztrapňování šířením audia	39	3,08	1266
Průnik na účet	291	28,64	1016

(n=1016-1269)

Rozložení jednotlivých forem kyberšikany ze strany agresorů odpovídá rozložení forem kyberšikany, které zažívají oběti. Nejvíce frekventovanou formou útoku, kterou potvrzují dětští agresoři, jsou útoky slovní (13,78 %), následované průnikem na účet (28,64).

Graf 6. Platformy užívané pro realizaci kyberšikany (průměrná hodnota vs. vydírání)



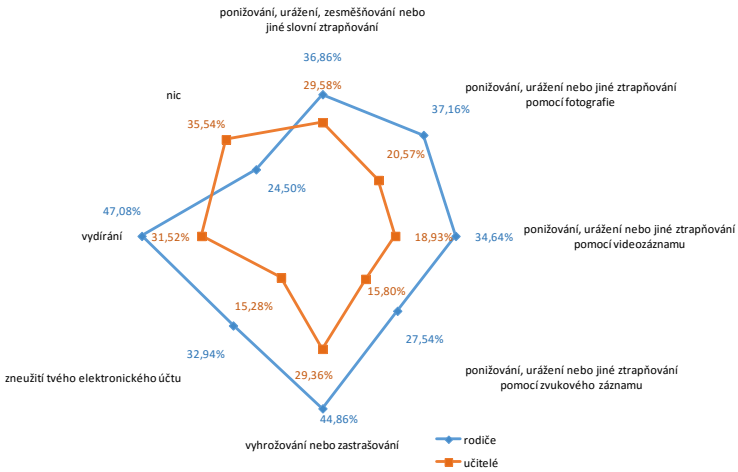
Nejčastější internetovou platformu, která je ke kyberšikaně zneužívána, představují sociální sítě (zejména sociální síť Facebook a Ask.fm). Opakované útoky v kyberprostoru potvrzuje přes 48 % slovenských respondentů.

Kyberšikana často probíhá také v prostředí veřejného (28,89 % útoků) a neveřejného (20,22 %) chatu.

V posledních letech se také k útokům stále více využívají webkamery, které umožňují získat od oběti audiovizuální materiály a využít je k následnému útoku. Zneužití webkamery ke kyberšikaně potvrzuje 2,53 % respondentů.

V dalších částech výzkumu jsme se zaměřili na otázku, zda by děti kontaktovaly rodiče či učitele v případě, že zažívají různé formy kyberšikany.

Graf 7. Koho by děti kontaktovaly?



V praxi platí, že čím je projev kyberšikany nebezpečnější, tím častěji se děti obracejí s prosbou o pomoc na dospělé. Rodiče by respondenti kontaktovali zejména v případech vydírání (47,08 % respondentů) a vyhrožování (44,86 %). Pro srovnání - při vydírání učitele kontaktuje 31,52 % slovenských dětí, při vyhrožování 29,36 %. Přibližně třetina dětí uvádí, že nekontaktují v případě kyberšikany ani učitele ani rodiče.

4.2.4 Přepínání rolí mezi obětí a útočníkem

V dalších částech jsme se zaměřili na přepínání rolí mezi obětí a útočníkem. V rámci výzkumu monitorujeme 2 základní formy přepínání:

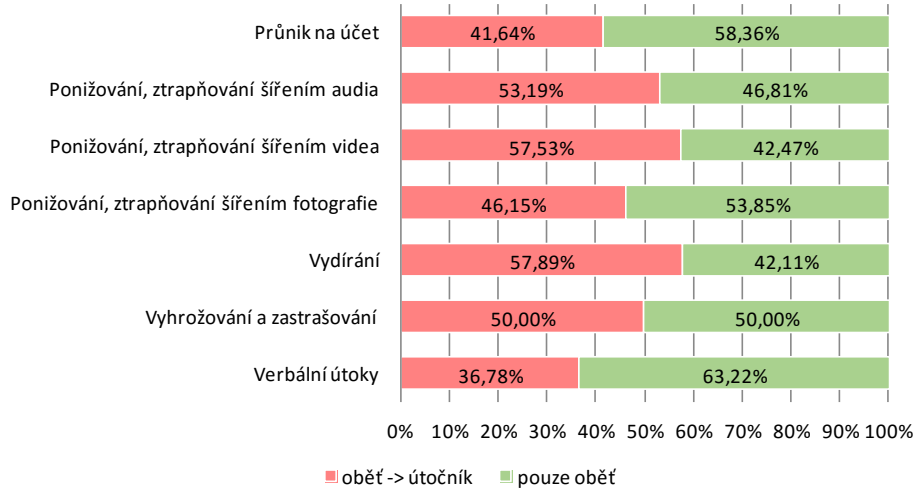
a) oběť se stává útočníkem, který využívá stejnou formu útoku, jakou zažíval jako oběť,

b) oběť se stává útočníkem, který využívá libovolnou formu kyberšikany.

Deskriptivní oddíl

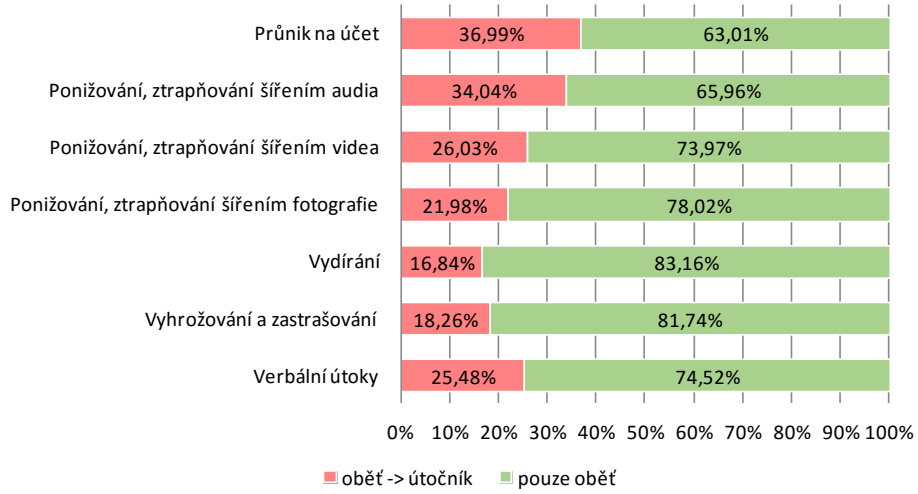
Následující grafy vyjadřují, jak moc se v daném vzorku přepínání rolí vyskytuje.

Graf 8. Přepínání rolí oběť – útočník (využívající libovolnou formu útoku)



Z výsledků výzkumu vyplývá, že se dětské oběti stávají agresory poměrně často – např. dítě, které bylo vydíráno, se v 57,89 % mění v útočníka, který vůči dětem využívá libovolné formy útoku. Méně často útočníci využívají stejnou formu útoku, jak zachycuje graf níže.

Graf 9. Přepínání rolí oběť – útočník (využívající stejnou formu útoku)



Přepínání rolí je detailněji zachyceno v následující tabulce. Sloupec *Oběti (n)* zachycuje počty obětí jednotlivých forem kyberšikany. Následující sloupce vyjadřují „přepnutí role“ – oběť se mění v útočníka, který využívá stejnou formu útoku, jakou byla oběť šikanována (*Útočník A*), nebo se mění v útočníka, který využívá k útoku libovolnou formu útoku (*Útočník B*).

Tab 16. Přepínání rolí mezi obětí a útočníkem (data)

	Oběti (n)	***Útočník A (n_1)***	***Útočník B (n_2)***
Verbální útoky	416	106	153
Vyhrožování a zastrašování	230	42	115
Vydírání	95	16	55
Ponižování, ztrapňování šířením fotografie	182	40	84
Ponižování, ztrapňování šířením videa	73	19	42
Ponižování, ztrapňování šířením audia	47	16	25
Průnik na účet	365	135	152

Závěry výzkumu dokazují, že se slovenské děti nejčastěji setkávají s verbálními formami kyberšikany a průniky na své internetové účty (emailové účty, účty v prostředí sociálních sítí atd), vážnějšími formami kyberšikany jsou ohroženy méně.

Velmi zajímavým zjištěním je přítomnost přepínání rolí mezi oběťmi a agresory. To je časté zejména u vážných forem kyberšikany (vydírání, vyhrožování), kde se více než 50 % obětí mění v agresory. Ti se zpravidla neomezují pouze na 1 formu útoku, ale provádějí útoky kombinované.

Slovenské děti se svěřují s kyberšikanou rodičům či učitelům teprve tehdy, když je útok vážný a děti jej nedokáží vyřešit. Hledají pak pomoc u dospělých osob.

Relační oddíl

Relační oddíl u výzkumu slovenských dětí sestává stejně jak u provedených analýz u českých dětí z výsledků induktivních statistických postupů. V našem výzkumu jsme opět využili statistické metody pro analýzu nominálních dat, zejména pak test nezávislosti chí-kvadrát pro čtyřpolní tabulku. Dále uvádíme pouze vybrané výsledky provedených relačních analýz.

K ověření hypotetického tvrzení, zda se útočníky kyberšikany u slovenských dětí stávají častěji její oběti než jedinci, kteří kyberšikanu neprožili, jsme získaná data nejdříve zavedli do čtyřpolní tabulky a poté je podrobili statistickým analýzám. K vyhodnocení naměřených dat byl použit test nezávislosti chí-kvadrát a míry těsnosti vztahu (fí-koeficient, tetra-chorický koeficient korelace a koeficient kontingence C). Přepínání rolí bylo stejně jako v případě českých dětí ověřováno u všech zaznamenaných projevů kyberšikany.

Výsledky provedených analýz jsou naprosto totožné s výsledky analýz realizovaných u českých dětí, tudíž zde neuvádíme jejich podrobný soupis. Souhrnně lze konstatovat, že útočníky kyberšikany u slovenských dětí se stávají častěji její oběti než jedinci, kteří kyberšikanu neprožili.

4.3 Sexting u slovenských dětí

Pro výzkum sextingu na Slovensku byl využit stejný výzkumný nástroj, pomocí kterého proběhlo měření v ČR. Obdobně, jako v ČR, jsme sledovali 2 základní formy šíření sextingu – umístění sexuálně laděného materiálu na internet (např. do profilu v rámci sociální sítě či do databáze digitálního úložiště fotografií) a přímé odeslání vlastního sexuálního materiálu jiným osobám (např. příteli, přítelkyni, kamarádovi, partnerovi atd.). Na základě těchto východisek vznikly 2 základní otázky (Q1, Q2), rozšířené o další subotázky monitorující motivaci respondentů k provozování sextingu. Zadání doplňuje otázka Q3, která se zaměřuje na nebezpečnost sextingu.

Deskriptivní oddíl

Q1. Otázka: **Umístil/-a jsi někdy na internet svou „sexy" fotografii nebo video, na kterých jsi částečně svlečený/-á nebo úplně nahý/-á?**

Sexting ve formě umístění vlastního intimního materiálu (fotografie či videa) na internet provozuje 7,6 % populace dětí ve věku 11–17 let (51 % tvořili muži, 49 % ženy; 55,81 % děti ve věku 15–17 let).

Motivace pro Q1:
1. Byla to fotografie pro mého partnera.
2. Chtěla jsem se pochlubit svým vzhledem (plavky, podprsenka, zhubla jsem).
3. Chtěla jsem zaujmout návštěvníky mého profilu na sociální síti.
4. Ze srandy. Z nudy.
5. Chtěla jsem ukázat, že jsem sexy.

Q2. Otázka: **Poslal/-a jsi někdy někomu svou „sexy" fotografii nebo video, na kterých jsi částečně svlečený/-á nebo úplně nahý/-á?**

Vlastní sexuálně laděné materiály odeslalo jiným osobám 9,31 % respondentů ve věku 11–17 let. Častěji odesílají jiným osobám materiály ženy (56 %), stejně tak častěji sexting provozují děti ve věku 15–17 let (60 %).

Motivace pro Q2:

1. Byla to fotografie pro mého partnera (chtěl ji po mně, poslal mi na oplátku svou).
2. Ze srandy. Z nudy.
3. Chtěl/a jsem se předvést (jak jsem krásný/á).
4. Byla jsem zamilovaná a chtěla jsem jej získat.
5. Kamarádka chtěla vidět mou intimní fotografii, věřil jsem jí.
6. Chtěla jsem s ním flirtovat.
7. Pro peníze.
8. Vyhrožoval mi.

Vyhrožování nelze za sexting považovat, protože je intimní materiál pod pohrůžkou od oběti vynucen.

Q3. Myslíš, že může být odesílání nebo zveřejňování fotografií nebo videí, na kterých jsi částečně svlečený/-á nebo nahý/-á, riskantní?

Téměř tři čtvrtiny respondentů (72,76 %) považují sexting za rizikový a riskantní. Mezi nejčastější důvody, proč lze považovat sexting za rizikový, uvedli respondenti následující (seřazeno dle četnosti).

1. Sexting lze zneužít k vydírání, šikaně/kyberšikaně, ponižování, obtěžování, zesměšňování zobrazené osoby.
2. Zobrazená osoba může být vystavena sexuálním útokům (od známých i neznámých osob), může dojít i ke zneužití či znásilnění.
3. Můžeme být obviněni z výroby a šíření dětské pornografie.
4. V dospělosti může někdo zneužít fotografii k poškození pověsti znázorněné osoby.
5. Fotografie se mohou dostat na pornografické stránky.
6. Fotografie a videa se mohou po internetu nekontrolovaně šířit.
7. Útočník si může vytvořit fake profil s těmito materiály.
8. Někdo může nad mými fotografiemi/videi masturbovat.

9. Co se dostane na internet, už nikdy nepůjde z internetu odstranit. Nejde to vrátit zpět.

Relační oddíl

V rámci sextingu u slovenských dětí nás rovněž zajímalo, zda kromě respondentů samotných, kteří vyvěšují své intimně laděné (tj. částečně nebo zcela obnažené) fotografie na internet, následně umisťují jejich intimní fotky na internet i jejich kamarádi.

Z provedených analýz bylo patrné, stejně jako u analýz realizovaných u českých dětí, že děti, které neuváženě zveřejňují své intimní fotografie na internetu, jsou následně daleko častěji postiženy šířením daných materiálů prostřednictvím svých známých a kamarádů.

5 Analýza komunikace mezi sexuálním abuzérem a obětí (2014)

V posledních letech se stále častěji objevují studie, které se snaží popsat komunikaci dětí a útočníků s využitím lingvistických nástrojů a analýzy obsahu komunikace (Black et al., 2015; McGhee et al., 2011). Vznikají tak velmi zajímavé výstupy, které dokumentují, jaká témata pachatelé útoků volí a jak na komunikaci reaguje oběť.

Řada autorů také upozorňuje na to, jak lze pomocí analýzy komunikátů rozpoznat, zda se jedná o pedofilního potenciálně nebezpečného abuzéra (Penna et al., 2005).

Další výzkumníci se zaměřují zejména na rizikové faktory, které jsou s procesem kybergroomingu spojeny (Wachs et al., 2012), upozorňují také na to, že v rámci jejich výzkumu kybergrooming v posledním roce reportovalo 21,4 % z výzkumného vzorku (111 z 518 dětí).

V českém prostředí byly také publikovány velmi zajímavé výsledky chování uživatelů sociálních sítí se zohledněním komunikace se sexuálními prvky (Kožíšek, 2015). Dílčí výsledky badatelů z firmy Seznam.cz, která provozuje v českém prostředí několik sociálních sítí, posloužily jako východiska pro realizaci naší analýzy.

5.1 Metodologie

Analýza psaných komunikátů dětí a útočníků v ČR vychází z konceptu výzkumu jazykové analýzy strategií groomingu výzkumníků z USA a Kanady (Black et al., 2015). Ti v rámci svého výzkumu provedli formální a obsahovou analýzu komunikátů pachatelů s využitím programu Linguistic Inquiry Word Count. V rámci analýzy autoři výzkumu pracovali s LIWC sémantickými kategoriemi, do kterých zařazovali slova pocházející z komunikace.

V naší analýze jsme se zaměřili na sledování konkrétních kombinací slov a vět, které jsou v procesu útoku na dítě využity. V rámci studie jsme analyzovali 267 záznamů mezi pachateli (sexuálními abuzéry) a oběťmi, které byly pořízeny při analýze případů hlášených oběťmi (či jejich rodiči) do online poradny Centra prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci v průběhu let 2012–2015. Záznamy komunikace byly zpracovány prostřednictvím programu pro kvalitativní analýzu textu Atlas.ti (Hwang, 2008).

V průběhu obsahové analýzy jsme se zaměřili na obraty, které se v komunikaci objevují často a jsou průvodním znakem jednotlivých fází útoku. Pro vymezení jednotlivých fází útoku jsme původně vycházeli z teoretického modelu průběhu fází kybergroomingu (O'Connell, 2003). Ten vymezuje v rámci procesu kybergroomingu *fáze formování přátelství, formování vztahu, fázi rizikového chování, fázi exkluzivity a sexuální fázi*. V řadě případů však v procesu reálného útoku neproběhnou všechny etapy tak, jak je vymezuje tento model. Proto jsme využili modelu alternativního (Kamil Kopecký et al., 2014b), který celý proces rozděluje na čtyři základní fáze: *příprava na kontakt s obětí; kontaktování oběti, navazování a prohlubování vztahu a manipulace oběti; příprava na útok; útok na oběť*. V některých případech jsou útoky velmi přímočaré – pachatel osloví několik desítek dětí např. s nabídkou brigády, která však v praxi znamená poskytnutí sexuálních služeb za příslušný finanční obnos – řada z útoků se tedy vymyká teoretickým konceptům kybergroomingu.

5.2 Výsledky analýzy

Výsledky kvalitativní analýzy textu realizované prostřednictvím programu Atlas.ti jsme rozdělili do jednotlivých fází kybergroomingu, čísla v závorkách udávají četnost dané syntaktické struktury v celém vzorku (267 záznamů chatové komunikace agresora s jinými uživateli). Ve všech případech útočníci ve věku 30–40 let komunikují s osobami mladšími 18 let (= dětmi), 41 % vzorku tvoří děti mladší 15 let. Jazykový materiál obsahoval 751 203 znaků.

V rámci jedné chatové komunikace se níže uvedené obraty mohou opakovat v závislosti na reakci osloveného dítěte. Pokud dítě např. neodpovídá, dospělý útočník svou žádost v různých časových intervalech několikrát zopakuje.

Tab 17. Komunikáty pachatele (fáze 1)

Fáze procesu	*n*
Kontaktování oběti	
Ahoj, chceš si psát?	163
Ahoj, chceš si se mnou povídat?	122
Skvělá nabídka brigády, chceš si rychle vydělat?	57
Jé, promiň, já si tě omylem přidala do přátel. Budeme si psát?	27
Ahoj, máš krásnou profilovku, chtěla by sis psát?	37
Jé, ty máš v profilu koně, já koně zbožňuju :) Máš ráda koně?	15
Ahoj kotě :) Dáme chat?	13
Ahoj, chceš si psát. . . třeba o sexíku?	79
Odkud jsi? Jsi kočka!	19
Ahoj, nemáš zájem si vydělat?	97
Ahoj, chceš něco reálného a krásně nezávazného?	17
Hledám kluka 12-15 let co se nudí, bez fotky nepište.	59
Hledám holku, co by šla třeba na webku, kolem 15 let.	29
Hledám holku, co by se chtěla rozmazlovat.	46
Hledám kluka, co by to chtěl zkusit s gayem, nebudeš litovat.	67

Komunikáty první fáze obsahují zejména běžné obraty sloužící k navázání prvotního kontaktu s virtuálním uživatelem, v řadě případů nelze rozeznat, zda se jedná o komunikaci rizikovou, nebo pouze běžnou.

V některých případech má komunikační obrat formu výzvy *Hledám kluka/holku*… V těchto případech již lze určit, že jde o komunikaci rizikovou. Např. podle statistik provozovatelů sociálních sítí děti nezjišťují věk ostatních diskutujících již v první fázi komunikace (např. *hledám holku 12–15 let, co se nudí*). Pokud je dítě osloveno, aby se ukázalo na webové kameře (např. *hledám holku, co by šla třeba na webku, kolem 15 let*), útočníkova webkamera zpravidla „nefunguje", útočník však vidí záznam z webkamery dítěte (Kožíšek, 2015).

Při analýze komunikátů jsme narazili také na projevy tzv. mirroringu, což je zrcadlové napodobování komunikace dítěte internetovým útočníkem. V praxi se mirroring projevuje např. ve větě *Jé, ty máš v profilu koně, já koně zbožňuju :) Máš ráda koně? Já mám farmu, kde mám stáje, 4 krásné hřebce a 2 klisny*… Pachatel nejdříve zjistil, že má dítě rádo koně, proto svou komunikaci připravil tak, aby byla pro dítě zajímavá a aby spolu mohli komunikovat o „společném zájmu".

Velmi oblíbený způsob navazování kontaktu představují online nabídky brigád (*Skvělá brigáda! Chceš si přivydělat?).* Řada z dětí, které na tyto nabídky reagují, se sexuálním kontaktem s tvůrcem nabídky počítají – z nich se v dalších etapách rekrutují tzv. online dětští prostituti.

Nyní se zaměříme na komunikáty, které spadají do druhé fáze a které již obsahují typické znaky online manipulace.

Tab 18. Komunikáty pachatele (fáze 2)

Fáze procesu	*n*
Navazování a prohlubování vztahu a manipulace dítěte	
a) komunikáty zaměřené na získání a upevnění důvěry dítěte	19
Ty jsi skvělá, s tebou si můžu říct všechno.	13
Spolu se můžeme bavit i o holčičích věcech, že jo?	29
Ty jsi pro mě jako moje ségra.	12
Ahoj, mám velký pozemek, kde mám i koně a stáje. Nechceš se někdy přijít podívat?	15
Mamka mi vůbec nerozumí, nechápe, co cítím.	37
Budeme si všechno říkat, ano? Ale nikomu to nesmíš říct, bude to naše tajemství, které nesmíš porušit.	
b) další komunikáty využívající technik manipulace	97
Dám ti 10000,- Kč, když budeš mít sex s mým bratrem.	65
Vyměníme fotky? Mám ale trošku intimní, nevadí?	

Některé obraty, které jsou v komunikaci využity, jsou primárně určeny na upevnění důvěry dítěte a na zvýšení exkluzivity online vztahu (*S tebou si můžu říct všechno. Můžeme se bavit o holčičích věcech. Ty jsi pro mě jako moje ségra.*). Pokud útočník získá důvěru dítěte, snadněji získá informace, které může využít k útoku na dítě v dalších fázích komunikace.

Jiné komunikáty jsou zaměřeny na izolování dítěte od rodiče (*Mamka ti nerozumí, já ano.*) – dítě se pak automaticky svěřuje internetovému uživateli, který supluje úlohu rodiče.

Pachatel na dítě zkouší různé postupy, např. předstírá, že je žena, a vybízí dítě k tomu, aby mělo „sex s jejím bratrem" (*Dám ti 10 000,- Kč, když budeš mít sex s mým bratrem.). V praxi* je však „bratrem" právě útočník maskující se za podvržený profil atraktivní ženy.

V komunikaci se také objevují výzvy, aby dítě udrželo komunikaci v tajnosti (*Budeme si všechno říkat, ano? Ale nikomu to nesmíš říct, bude to naše tajemství,*

které nesmíš porušit.). Požadavky na udržení komunikace v tajnosti potvrzují také další výzkumníci (Webster et al., 2012).

Vysokou četnost (n=65) vykazuje také komunikace zaměřená na vylákání intimní fotografie oběti. Útočník, maskovaný za falešný profil osoby opačného pohlaví, osloví v průběhu komunikace dítě s následující výzvou: *Vyměníme fotky? Mám ale trošku intimní, nevadí?* Následně pošle dítěti fotografii, na které je zachycena např. dívka ve vaně. Dítě – chlapec – pošle pachateli své vlastní foto, načež mu pachatel začne posílat stále odvážnější fotografie (Kamil Kopecký, 2014b; Kožíšek, 2015). Dítě reaguje a nakonec pachateli pošle svou vlastní intimní fotografii.

Pachatel tak získá prostředek pro vydírání prostřednictvím intimních materiálů – tzv. sextortion (Kamil Kopecký, 2014b; Strasburger, Jordan, & Donnerstein, 2012; Wilson, 2011). Sextortion patří k nejvíce nebezpečným formám internetových útoků na děti.

Tab 19. Komunikáty pachatele (fáze 3 a 4)

Fáze procesu	*n*
Příprava na útok a útok	
Jestli neuděláš, co ti říkám, všechno, co od tebe mám, půjde na internet.	79
Máš 3 minuty na to, abys mi vše poslala, jinak vše rozešlu tvým přátelům na Facebooku včetně tvých rodičů.	19
Nezahrávej si se mnou a udělej, co ti říkám! Vím o tobě všechno!	21
Vážně chceš, aby se tvoje matka/otec dozvěděla, jaká jsi děvka?	29 11
Vážně chceš, aby se tvůj kluk dozvěděl, cos mi poslala?	3
Vyzvednu tě v 11 na nádraží, jestli tam nebudeš, budeš mít problém.	9
Zajdeme na kafe a něco sladkého.	

Komunikáty, zachycující finální fáze útoku, již obsahují různé formy nátlaku na dítě s cílem přinutit jej k poskytnutí intimních materiálů, nebo přímo k osobní schůzce. Sextortion se projevuje např. v komunikátech: *Jestli neuděláš, co ti říkám, všechno, co od tebe mám, půjde na internet* (= intimní materiály). *Vážně chceš, aby se tvůj kluk dozvěděl, jaká jsi děvka?* V některých případech pachatel dítěti stanoví časový limit, do kterého musí odeslat intimní materiály (*Máš 3 minuty na to, abys mi vše poslala.).*

5.3 Shrnutí

Výše uvedené ukázky dokladují, že se komunikační obraty využívané útočníky často opakují a mohou tak sloužit k predikci potenciálního sexuálního útoku či obtěžování dítěte. Útočníci využívají v řadě případů poměrně sofistikovaných technik, pomocí kterých získají pozornost a náklonnost dětí, které jsou pak ochotné plnit jejich žádosti. Ve velkém množství však pachatelé volí pro útok na dítě cestu přímého nátlaku prostřednictvím vydírání a vyhrožování dítěti (Kamil Kopecký, 2014b).

Identifikaci pachatelů, kteří v prostředí sociálních sítí komunikují s dětmi, lze do jisté míry automatizovat. Většina provozovatelů sociálních sítí, které používají děti, využívá automatizace prostřednictvím „robotů“, kteří sledují klíčová slova v komunikaci uživatelů a podezřelé nálezy hlásí „lidským“ administrátorům služeb. Ti tak mohou případ např. oznámit policii, identifikovat pachatele, zablokovat účet apod.

Zásadní úlohu v oblasti ochrany dětí před útoky online abuzérů na internetu však hraje zejména primární prevence, v rámci které je možné dětské uživatele internetu a jejich rodiče seznamovat se strategiemi útoků – a to s využitím celé řady zdokumentovaných případů. Dítě je pak schopno v řadě případů rozpoznat strategie, které jsou online abuzéry pro útok využívány.

6 Další rizikové jevy

6.1 Trolling a webcam trolling

6.1.1 Trolling ve světě internetu

S rozvojem informačních komunikačních technologií a dostupností internetových služeb, které umožnily propojit velké množství uživatelů a zajistily jim vzájemně komunikovat a sdílet informace, se v prostředí internetu začaly objevovat také uživatelé, kteří chtěli komunikaci narušovat, provokovat, strhávat na sebe pozornost a poškozovat ostatní komunikující. Na scéně se objevili tzv. *internetoví trollové* a *trolling*.

Trolling byl v minulosti některými autory vnímán pouze jako odesílání provokativních zpráv jiným uživatelům internetových služeb, zatímco flaming byl definován jako distribuce zpráv obtěžujících (Porter, 1997; Wallace, 2001). V současnosti je však nutné tyto termíny redefinovat, protože současný trolling zahrnuje odesílání jakýchkoli zpráv či informací, které uživatele obtěžují, ale také provokují nebo na ně útočí (Bishop, 2014), stejně tak zahrnuje zcela nové

projevy, které nejsou spojené pouze s textovou formou komunikace (např. zakládání falešných internetových profilů).

Současný internetový trolling lze pro zjednodušení rozdělit na tzv. „*kudos trolling*“, jehož cílem je zejména pobavit internetové publikum, a na tzv. „*harm trolling*“, jehož cílem je internetovým uživatelům ublížit (Bishop, 2015). V praxi se však setkáváme obvykle s kombinací obou forem.

Trollové se projevují různými způsoby, mohou narušovat internetové diskuse, rozšiřovat špatné a nebezpečné rady, poškozovat důvěryhodnost zpráv či napadat jednotlivé diskutující uživatele (Donath, 1999). Trollové se podle Donath pokoušejí stát legitimními uživateli diskusních skupin a narušovat pak jejich činnost. Podle Donath je trolling jakousi hrou o podvodné identitě.

Jakmile trollové proniknou do skupiny, začnou rozvíjet svou falešnou identitu, stávají se akceptovanými členy skupiny a začínají narušovat aktivity skupiny, vyvolávají u diskutujících hněv, zároveň však brání svému odhalení (Dahlberg, 2001).

Někteří autoři (Shachaf & Hara, 2010) se ve svém výzkumu zaměřili na chování trollů působících na Wikipedii. Na základě zrealizovaných rozhovorů identifikovali řadu důvodů, pro které je trolling provozován – nuda, snaha upoutat pozornost, pomsta, zábava, touha poškodit komunitu apod. Další výzkumníci (Hardaker, 2010) provedli analýzu příspěvků trollů v rámci systému elektronických diskusních skupin Usenet. Na základě této analýzy identifikovali základní charakteristické rysy *trollingu: agrese, podvádění, narušování vztahů a snaha mít úspěch*. Pomocí těchto kritérií lze trolling odlišit od dalších forem antisociálního chování (např. kyberšikany). Další autoři, kteří se zabývali výskytem trollingu v rámci social media site YouTube (McCosker, 2013), potvrzují přítomnost provokativních a jedovatých postů komentujících různá sdílená videa (videa se záběry přírodních katastrof, tradičních kulturních událostí apod.).

Někteří autoři (Herring, Job-Sluder, Scheckler, & Barab, 2002) upozorňují na specifika mužského trollingu v rámci diskusních skupin zaměřených převážně na feminismus, ve kterých tvoří 90 % všech diskutujících ženy.

Mnozí autoři (Langos, 2010) vnímají trolling jako umisťování pobuřujících materiálů na webové stránky (sociální sítě apod.) s cílem napadat ostatní

uživatele a vyvolávat negativní emoční reakci. V některých případech trollové na internetové stránky umísťují nelegální materiály (např. dětskou pornografii).

Jiní trollové realizovali v prostředí internetu sociologické sondy do lidského chování – např. známý troll Jason Fortuny vyvěsil na internet podvodnou zprávu (hoax), ve které pod identitou ženy hledal „brutální svalnaté muže". Ozvalo se mu více než 100 zájemců, následně Fortuny vyvěsil jejich jména, fotografie, emailové kontakty a telefonní čísla na svůj blog (jeho aktivita vešla ve známost jako tzv. Craigslist Experiment) (Schwartz, 2008).

S masivním rozšířením Facebooku a dalších sociálních sítí začali trollové velmi často zakládat různé typy diskusních skupin a falešných profilů, které byly spojeny s nějakou společensky významnou událostí či osobností. Prostřednictvím těchto profilů poté „bavili" přítomné virtuální publikum, ale také poškozovali dobrou pověst konkrétních osob – např. herců, politiků či jiných celebrit. Některé formy trollingu jsou spojené také s případy úmrtí, vražd či sebevražd, ve kterých trollové zneužívají tragické situace k upoutání pozornosti na své vlastní aktivity (Phillips, 2011).

Tuto formu trollingu lze dokumentovat na následujícím případu z České republiky: Dvě dvacetileté Češky – Antonie Chrástecká a Hana Humpálová – byly 13. března 2013 uneseny v jihozápadním Pákistánu v provincii Balúčistán. O několik dní později se na sociální síti Facebook objevila diskusní skupina *Gratulujem Hanče a Tonče k novému životu v Pákistánu*. Stránka se poměrně nechutným způsobem vyjadřovala k případu unesených dívek a ironické textové komentáře doplňovala velmi názornou obrazovou dokumentací, ať již v podobě fotografií, nebo videí. Na nich byly znázorněny popravy zajatců, dekapitace, sadistické záběry mučení vězňů apod. Autor stránky rovněž doplnil texty o ironické rady, jak se chovat při cestování přes Pákistán: *Nebojte se Pákistán je bezpečná země, pro cestování. Nevěřte všem oficiálním zprávám od ministerstev zahraničí o nebezpečnosti cestování, přes tuto skvělou zem. Cestujte zásadně samy, maximálně po dvojicích. Jeďte autobusy nebo samostatně autem, nejlépe přes oblasti, které nejsou zcela pod kontrolou státní správy. V žádném případě si nenajímejte pohraniční stráž, nebo jakoukoli státní aparaturu pro bezpečí převozu. Nezapomeňte se obléct do vašeho tradičního oblečení a nesnažit se zapadnout do obecného outfitu Pákistánských žen. Nejlépe mluvte vaším rodným jazykem přímo při cestování. Řiďte se našimi radami a užijte si skvostné bezpečné cestování přes Pákistán* (Kamil Kopecký, 2013a).

Diskusní skupiny si postupně všimla veřejnoprávní média, která začala zveřejňovat záznamy ze skupiny v rámci běžného celostátního zpravodajství. Autor po několika dnech pod vlnou kritiky veškerý obsah ze skupiny stáhl a nahradil jej informacemi o tom, že byli uživatelé „trollováni".

Mezi další dokumentované případy trollingu probíhajícího prostřednictvím falešných profilů na sociálních sítích patří např. případ českého trollingu zaměřeného na známého českého herce, spisovatele, textaře a scénáristu Zdeňka Svěráka. Ten se počátkem listopadu 2013 stal obětí útoku neznámého uživatele Facebooku, který o herci vytvořil stránku *Znásilnil mě Zdeněk Svěrák*. Facebooková stránka „Znásilnil mě Zdeněk Svěrák" obsahovala v okamžiku zveřejnění několik obvinění z údajného znásilnění tímto hercem, zaslaných z fiktivních a anonymně vytvořených uživatelských účtů. Stránka například informovala o tom, že děti byly Zdeňkem Svěrákem zneužívány při natáčení dětských pořadů a sám autor jim za sexuální praktiky platil. Kauza byla medializována a Zdeněk Svěrák podal na autora skupiny trestní oznámení. Facebooková stránka „Znásilnil mě Zdeněk Svěrák" byla ze sociální sítě odstraněna druhý den po jejím zveřejnění v médiích (Kusá & Adámek, 2013).

S příchodem nových multimediálních technologií (zejména digitálních fotoaparátů a kamer, případně webkamer) se forma trollingu začala vyvíjet – původní ryze textové projevy trollů začaly být nahrazovány projevy vizuálními, audiovizuálními či přímo interaktivními. Se stále rychlejším rozšiřováním webkamer mezi uživatele internetu začal trolling pronikat do videochatu – pro pobavení ostatních (a zároveň pro zamaskování vlastní identity) začali internetoví trollové pouštět ostatním uživatelům internetu předtočené videosmyčky, kterými nahrazovali svůj skutečný obraz na webkameře (Kamil Kopecký, 2013c). Masivního rozšíření dosáhla tato forma trollingu zejména v prostředí videochatu Chatroulette, kde se s ní lze setkat doposud (Bartoněk, 2011). Tato forma trollingu začala být označována jako tzv. webcam trolling či chatroulette trolling.

6.1.2 Webcam trolling

Termínem „webcam trolling" tedy označujeme *rizikový komunikační fenomén spojený se zneužitím webové kamery, ve kterém je vyhlédnuté oběti místo skutečného obrazu z webkamery promítána předtočená videosmyčka* (Kamil Kopecký, 2013c). První zdokumentované případy webcam trollingu pocházejí z prostředí velmi rozšířeného videochatu Chatroulette (v prostředí Chatroulette hovoříme o tzv. chatroulette trollingu) a byly určeny zejména pro

pobavení jednotlivých diskutujících a pro ochranu vlastní identity maskované podvrženým videozáznamem.

Řada autorů však opakovaně upozorňovala na rizika, které s sebou využívání videochatů – zejména Chatroulette – nese, kromě vysoké koncentrace sexuálně explicitního obsahu bylo v těchto prostředích možné provádět útoky na bázi *de-anonymizace* (odhalení skutečné identity chatujících), realizovat *phishing* (získat od chatujících potenciálně citlivé informace, jako např. jejich jméno, informace o Skype účtu, facebookovém účtu) či provést tzv. *man-in-the middle attacks* (Xing, Dang, Han, Liu, & Mishra, 2010). V rámci phishingových aktivit byl webcam trolling využíván k manipulaci uživateli videochatu – těm bylo podsunuto podvržené video (např. video atraktivní mladé dívky či muže), prostřednictvím kterého útočník získával osobní informace (Xing et al., 2010). Ty mohl využít např. k vydírání, vyhrožování, dehonestování atd.

Většina videosmyček, které jsou v rámci webcam trollingu využívány, neobsahují zvukovou stopu. Útočník pak vyhlédnuté oběti tvrdí, že se ji na webkameře ukáže, ale že jeho webkamera nemá vestavěný mikrofon, že neovládá daný jazyk, případně, že preferuje textovou komunikaci před komunikací hlasovou (Kamil Kopecký, 2013c; Xing et al., 2010).

Webcam trolling lze provozovat v jakémkoli prostředí, které podporuje komunikaci prostřednictvím videochatu, tedy jak v rámci tzv. instant messengerů (Skype, ICQ), tak i v prostředí sociálních sítí (Facebook, G+ apod.). K provozování této služby lze využít celé řady volně dostupných počítačových programů, které po nainstalování do počítače simulují virtuální webkameru a do kterých lze nahrávat předtočené záznamy.

Webcam trolling může být provozován z různých důvodů, cílem může být:
a) pobavení sebe či ostatních uživatelů videochatu,
b) cílený útok na jiné uživatele internetových služeb (např. s cílem vylákat od nich jejich vlastní záznamy z webkamer, vydírat je, donutit k virtuálním sexuálním praktikám před webkamerou, sdílet vzniklé záznamy, získat jejich citlivé informace, získat peníze apod.),
c) snaha uspokojit své vlastní sexuální fantazie.

6.1.3 Zneužití webcam trollingu k útokům na dětské uživatele internetu

Útočníci, kteří webcam trolling využívají, se v řadě případů zaměřují na dětské uživatele internetu využívající online videochat. Strategie útoku je poměrně jednoduchá – pachatel nejdříve osloví dítě s žádostí o erotický videochat, představí se mu pod falešnou identitou doprovázenou podvrženou videosmyčkou (většinou osoby opačného pohlaví) a postupně dítě přesvědčí, aby se před webkamerou obnažilo. Pachatel si v průběhu videochatu obraz z videokamery dítěte zaznamenává a ukládá, aby jej mohl dále využívat např. k vydírání (Kamil Kopecký, 2013c).

Oběti jsou v rámci webcam trollingu zmanipulovány takovým způsobem, že v několikaminutové stopáži dokáží plnit příkazy útočníků a i heterosexuální jedinci jsou ochotni na videokameru vyzkoušet různé sexuální praktiky s kamarády stejného pohlaví. Takto vzniklé záznamy jsou obvykle sdíleny prostřednictvím specializovaných serverů, které obsahují zejména videosekvence chlapců ve věku 13–18 let (Kamil Kopecký & Kožíšek, 2013).

V řadě zdokumentovaných případů byl webcam trolling využit také k vydírání dítěte – útočník nejprve od dětské oběti vylákal intimní materiál, který následně použil k vydírání. Dítěti vyhrožoval, že pokud nebude před webkamerou plnit jeho příkazy, bude jeho intimní materiál zveřejněn (Kamil Kopecký, 2014b). Děti pak ze strachu plnily příkazy útočníka a poskytovaly mu další intimní materiály.

Motivace útočníků pro realizaci útoků na děti může být různá, někteří pachatelé se snaží vydíráním od obětí získat peníze (Get Safe Online, 2015), mezi další motivy patří např. touha užívat si pocit moci, který pachatel nad obětí má, realizovat prostřednictvím videochatu své sexuální fantazie (Briggs et al., 2011), případně donutit dítě k osobní schůzce – tzv. online grooming či kybergrooming (Child Exploitation and Online Protection Centre, 2013; Kamil Kopecký et al., 2014b; Tickle, 2012).

6.1.4 Strategie ochrany a obrany před webcam trollingem

Základní strategií ochrany a obrany před webcam trollingem je především dodržovat základní zásady bezpečného chování ve virtuálním prostředí, především:

a) *chránit si své osobní a citlivé údaje* (omezit jejich publikování v rámci online profilů, nesdělovat je neznámým osobám),
b) *dodržovat zásady pro zabezpečení profilů* (např. na sociálních sítích), ke kterým patří zejména tvorba bezpečného hesla a silné kontrolní otázky (K. Kopecký & Szotkowski, 2014) a nastavení základní či pokročilé ochrany soukromí (např. určit, kdo a jak může mé příspěvky vidět),
c) *nerealizovat sexting v jakékoli podobě* (nesdílet s ostatními uživateli žádné intimní materiály – ani fotografie, ani videa, neobnažovat se před webkamerou),
d) *provést technické zabezpečení počítače* (aktivní firewall a antivirový program).

Webcam trolling lze odhalit zejména díky absenci zvukové stopy ve videosmyčce, která je k útoku použita. Další možností, jak rozpoznat podvodné jednání a odhalit skutečnou identitu uživatelů, je oslovit je s žádostí, aby např. na papír napsali konkrétní vzkaz, který mu nadiktujete a který pak na webkameru ukáže. Pokud toto provedou v reálném čase, nejde pravděpodobně o podvodný videozáznam, ale o skutečné existující osoby.

6.2 Podvodné mobilní platby (m-platby)

Nový druh podvodu, který se v posledních dnech objevuje zejména v prostředí Facebooku, představují žádosti falešných přátel o pomoc při obnově fiktivní zablokované služby. Místo odblokování zablokovaného účtu však pachateli umožníte potvrdit finanční transakci u vašeho mobilního operátora (Kamil Kopecký, 2013b). Tento druh podvodu reportují jak dospělí, tak dětští uživatelé internetu.

Pachatel si založí falešný profil konkrétního uživatele a z něj poté požádá přátele ze seznamu přátel tohoto uživatele o „znovupřidání“. Ti to ve většině případů udělají. Pachatel pak tyto uživatele pod smyšlenou legendou (např. zapomenutí PINu k bankovnímu účtu, zablokovaná emailová schránka apod.) přesvědčí, aby mu poskytnuli telefonní číslo, na které může nechat zaslat PIN k obnovení přístupu na zablokovanou službu. Ve skutečnosti však nejde o validační PIN, ale o kód k provedení platby u mobilního operátora k uhrazení sázky u společnosti BWIN, ŠANCE, POKERSTARS apod.

Další variantou podvodu zaměřeného k vylákávání PINu je podvržená webová stránka k soutěžím o různá mobilní zaměření (tablet, mobilní telefon). Pro úspěšné přihlášení do soutěže však musí uživatel vyplnit přihlašovací údaje k účtu na Facebooku. Pachatel tak neoprávněně získá přístup ke konkrétnímu facebookovému profilu a opět žádá přátele o zaslání PIN kódu k platbám.

„*Uživatelé internetových služeb si často neuvědomují, s kým komunikují, a bez ověření zasílají PIN kódy „virtuálním přátelům", ačkoli jsou operátorem výslovně upozorňováni na to, že tento kód nemají předávat dál*", uvádí kriminalista Pavel Schweiner z oddělení informační kriminality Krajského ředitelství policie Olomouckého kraje.

Na Facebooku jako v reálném světě obvykle platí zásada „důvěřuj, ale prověřuj", proto je nutné jakoukoli snahu o validování účtu jiné osoby skrze váš mobilní telefon pečlivě prověřit, nejlépe tak, že dané osobě přímo zatelefonujete. Ideálním řešením pak zůstává nikomu tyto údaje nepředávat.

6.3 Útoky na účty elektronického bankovnictví (phishing)

V posledních letech se stále více objevují různé formy útoků na účty elektronického bankovnictví, které využívají podobná schémata útoku a před kterými je poměrně snadná obrana. Přesto se však stále najdou tací, kteří na některou z fází útoku reagují a zachovají se nebezpečně (Kamil Kopecký, 2015b).

Útok na účet elektronického bankovnictví (tzv. phishing) zpravidla prochází několika fázemi:

6.3.1 Fáze 1 – Spamový útok

Aby byl útok úspěšný, je nutné oslovit co největší počet uživatelů. Nejjednodušším a nejefektivnějším způsobem, jak se k uživatelům a jejich online účtům dostat, je rozesílání spamu se zprávou, která uživatele zaujme a donutí je reagovat. Mezi běžné typy zpráv, podle kterých phishingový útok rozeznáme, patří:

1. Informace o tom, že někomu dlužíme (detailní informace o dluhu jsou součástí samostatné přílohy, která obsahuje virus – zpravidla trojský kůň – který se do počítače nainstaluje a který shromažďuje informace o přihlašovacích údajích).

2. Informace o tom, že na náš účet přišla vysoká finanční částka, kterou musíme potvrdit přihlášením se ke službám elektronického bankovnictví (kliknutím na odkaz z emailu jsme přesměrování na podvrženou kopii naší bankovní

instituce, přihlášením ke „svému účtu“ pak útočníkovi sdělíme své přihlašovací údaje).

3. Informace o tom, že banka mění svou úroveň zabezpečení a že je nutné se co nejdříve k účtu přihlásit (kliknutím se opět dostaneme na podvrženou stránku, viz předchozí model).

4*. Informace o tom, že platnost internetového bankovnictví končí* a je nutné ji prodloužit (kliknutím se opět dostaneme na podvrženou stránku, viz předchozí modely).

5. Informace o tom, že jste obdrželi novou zprávu z bezpečnostního oddělení (kliknutím se opět dostaneme na podvrženou stránku, viz předchozí modely).

6.3.2 Fáze 2 – Získání uživatelského přístupu prostřednictvím falešné stránky

Jak již bylo řečeno, většina útoků na účty elektronického bankovnictví je spojena s vytvořením podvržené stránky, která klienty nutí přihlásit se ke svým účtům prostřednictvím uživatelských jmen, hesel, či dokonce certifikátů. Tyto stránky jsou zpravidla umístěny na anonymních serverech v zahraničí a existují pouze několik málo dnů. Pak jsou smazány a stopy zahlazeny (Kamil Kopecký, 2015b).

Podvodné stránky často využívají nepozornosti uživatelů při čtení internetových adres, např. se po kliknutí na odkaz v emailu otevře místo stránek www.mojebanka.cz stránka www.mojebanka.cn. Jen zlomek uživatelů zaznamená chybu v nepřesné koncovce domény či celé adrese.

6.3.3 Fáze 3 – Instalace podvodné aplikace a autorizace SMS platby

V posledních letech (zhruba od roku 2013) se tvůrci podvodných phishingových stránek chovají daleko nebezpečněji, než tomu bylo dříve – využívají totiž masivního rozšíření tzv. smartphonů a tabletů. Pomocí podvodných kódu integrovaných do www stránek se snaží přimět uživatele nainstalovat si do svých mobilních telefonů různé nebezpečné aplikace (tzv. malware), které v operačním systému telefonu běží tzv. „v pozadí“ a které ovládají příjem SMS zpráv – tedy i autorizačních zpráv internetových transakcí.

Metod, jak nahrát tyto nebezpečné aplikace do mobilních telefonů, je hned několik:

a) po přihlášení do fiktivního účtu vám podvodná stránka sama nabídne stažení aplikace do mobilního telefonu (např. aplikace TrustPort Mobile Security),

b) podvodná aplikace (či odkaz na ni) vám po přihlášení k účtu přijde ve formě SMS či MMS,

c) podvodná aplikace je součástí samotného spamu a instaluje se po otevření přílohy emailu.

Není výjimkou, že jsou podvodné aplikace distribuovány také pomocí známých obchodů s aplikacemi, např. Google Play.

6.3.4 Prevence jako základ obrany

Základem obrany před phishingovými útoky je samozřejmě prevence a dodržování jednoduchých zásad:

1. V počítači mít vždy nainstalován antivirový program, který umožňuje identifikovat nebezpečné viry v přílohách emailů či jiných zpráv.

2. Antivirovou ochranou vybavit také svůj smarthone či tablet.

3. Pro přihlašování do internetového bankovnictví vždy používat oficiální internetové stránky bankovní instituce (nikoli odkazy v emailech).

4. Pravidelně aktualizovat operační systém i jednotlivé programy.

5. Neotvírat přílohy emailů z neznámých zdrojů, neklikat na odkazy v těchto emailech.

6. Při zadávání hesel na internetu kontrolovat, zdali je přenos dat zabezpečen (adresa začíná https://).

7. Pokud možno nevypínat firewall ve vašem operačním systému.

8. Jakékoli otázky spojené s informacemi o podezřelých platbách vždy konzultovat přímo s bankovní institucí – ideálně osobně či telefonicky.

9. V případě potřeby navštívit stránky České bankovní asociace (www.czech-ba.cz), která informace o různých formách hackerských útoků zveřejňuje. Ověřovat si informace např. na webových stránkách www.hoax.cz.

10. V internetovém prohlížeči si aktivovat antiphishingový filtr.

6.4 Rizika online závislosti (netolismus)

S masivním využíváním internetových služeb a nových technologií je stále více diskutována otázka, zdali se tyto nové nástroje nepodílejí na vzniku netolismu, závislosti či závislostního chování jako takového. Online behaviorální závislosti tak představují další z rizik, kterým jsou děti i dospělí uživatelé internetu denně vystaveni.

Termínem *netolismus* označujeme *závislost (závislostní chování (behaviorální závislost) či závislost na procesu) na tzv. virtuálních drogách*. Mezi ně patří zejména počítačové hry, sociální sítě, internetové služby (různé formy chatu), virální videa, televize aj.

Je třeba říci, že ve vztahu k závislostem a závislostnímu chování v prostředí internetu neexistuje ustálená definice. Beard a Wolf definují závislost na internetu jako *používání internetu, které s sebou přináší do života jedince psychologické, sociální, pracovní nebo školní komplikace* (Beard & Wolf, 2001). Shapira pak popisuje závislost na internetu jako *neschopnost jedince mít kontrolu nad svým užíváním internetu*, jako *kompulzivní nadužívání internetu a podrážděné nebo náladové chování v důsledku nemožnosti jeho užívání* (Shapira, Goldsmith, Keck, Khosla, & McElroy, 2000).

Z výše uvedeného je zřejmé, že se jedná o psychickou/behaviorální závislost, nikoli o závislost fyzickou, ke které dochází při konzumaci návykových látek (alkohol, nikotin, opiáty atd.).

Obecně jsou podle WHO (WHO, 2015) definovány podmínky závislosti na návykových látkách takto:

a) silná touha nebo pocit puzení užívat látku,
b) potíže v kontrole užívání látky, a to pokud jde o začátek a ukončení nebo o množství látky,
c) užívání látky k odstranění abstinenčních příznaků,
d) průkazná tolerance (vyžadování vyšších dávek látky, aby se dosáhlo účinků původně vyvolaných nižšími dávkami),
e) postupné zanedbávání jiných potěšení a zájmů ve prospěch užívané psychoaktivní látky a zvýšené množství času potřebného k získání nebo užívání látky,
f) pokračování v užívání přes jasný důkaz zjevně škodlivých následků.

Nahradíme-li termín *návyková látka* termínem *návykový proces (behaviorální závislost)*, můžeme snadno znaky závislosti vypozorovat i v samotném

netolismu (Hlaváč, 2015) – např. silnou touhu zapnout počítač bez jasného cíle, zkontrolovat SMS, zkontrolovat statuty na sociální síti, neschopnost vymezit si začátek a konec aktivit na internetu, postupně zanedbávat další aktivity atd.

Závislostní chování ve vztahu k internetu lze rozdělit do pěti základních kategorií (K. S. Young, 2004):

1. Závislost na virtuální sexualitě (kompulzivní používání webových stránek pornografického zaměření).
2. Závislost na virtuálních vztazích (nadměrné věnování se virtuálním vztahům).
3. Internetové kompulze (např. hraní online počítačových her či internetové nakupování).
4. Přetížení informacemi (nadměrné surfování na internetu nebo hledání v databázích).
5. Závislost na počítači (nadměrné hraní počítačových her).

Co se týče diagnostiky závislostního chování ve vztahu k internetu, stále více odborníků se shoduje na skutečnosti, že závislostní chování patří do kategorie F 63. 8. – Jiné návykové a impulzivní poruchy Mezinárodní klasifikace chorob (MKCH-10) (Benkovič, 2007; Shaw & Black, 2008), dle dalších expertů (Griffiths, 1998) je závislostní chování zařazeno pod skupinu tzv. behaviorálních závislostí, které obsahují 6 základních komponent závislosti:

1. Význačnost (určitá aktivita se stane nejdůležitější v životě člověka a začíná ovládat jeho myšlení, cítění a chování).
2. Změny nálady (pocity vzrušení, flow stav, uklidňující pocity úniku a znecitlivění).
3. Tolerance (proces, při kterém je nutno stále více aktivity k dosažení předchozí míry uspokojení).
4. Odvykací symptomy (ukončení či omezení aktivity se projevuje abstinenčními symptomy).
5. Konflikt (konflikt s okolím, konflikt s ostatními aktivitami – prací, soukromým životem, koníčky apod.).
6. Relaps (tendence opakovat dřívější vzorce závislostního chování).

Stále více výzkumníků se rovněž snaží zjistit, jak moc je netolismus v jednotlivých zemích světa rozšířen. K diagnostice a měření prevalence pak využívají zejména testy IAT a CIAS-R. Zkratka IAT označuje test internetové závislosti – Internet Addiction Test, vytvořený americkou psycholožkou Kimberley Young (Kimberly S Young, 2008). Test je k dispozici na

http://netaddiction.com/internet-addiction-test/. CIAS-R je označení pro závislostní škálu, v originále Revised Chen Internet Addiction Scale (CIAR-R), která je využívaná k měření internetové závislosti zejména v Číně a Hong-Kongu (Mak, Lai, Ko, et al., 2014).

Netolismus je vnímán jako závažný problém zejména v asijských zemích – výzkum, realizovaný v Číně, Hong-Kongu, Japonsku, Jižní Korey, Malajsii a na Filipínách (Mak, Lai, Watanabe, et al., 2014) zjistil u více než 5 000 dětí ve věku 12–18 let vysokou prevalenci závislosti na online hrách – od 11 % v Číně po 39 % v Japonsku. Nejvíce asijských internetových závislých však bylo diagnostikováno na Filipínách–5 % (podle IAT) a 21 % (podle CIAS-R).

V letech 2011–2012 proběhl výzkum zaměřený na internetové závislostní chování (Research on Internet Addictive Behaviours among Eropean Adolescents) také ve vybraných zemích Evropy (Tsitsika et al., 2012). Výzkum proběhl ve Španělsku, Nizozemí, Německu, Polsku, Řecku, Rumunsku a Islandu a zapojilo se do něj více než 13 000 dětí ve věku 14–17 let. Podle jeho výsledků vykazuje znaky online závislosti 21,3 % španělských dětí, následovaných Rumunskem (16 %), Polskem (12 %), Nizozemím (11,4 %), Řeckem (11 %), Německem (9,7 %) a Islandem (7,2 %).

6.4.1 Závislostní chování ve vztahu k Facebooku (FAD)

FAD (Facebook Addiction Disorder), tedy závislostní chování na sociální síti Facebook, můžeme vnímat jako podskupinu závislosti na internetu zaměřenou na konkrétní internetovou službu, v našem případě sociální síť Facebook. Podle psycholožky Amy Summersové existuje 6 základních symptomů spojených s FAD (Summers, 2011):

1. Roste tolerance (k dosažení stejné míry uspokojení trávíme na Facebooku více času než dříve, pokud netrávíme dostatek času na FB, trpíme nespokojeností, frustrací).
2. Objevují se abstinenční příznaky (stres, podrážděnost, úzkost).
3. Dochází k redukci běžných sociálních/rekreačních aktivit (omezujeme aktivity probíhající mimo Facebook).
4. Preferujeme virtuální facebookové schůzky místo schůzek „v reálu“ (např. místo na schůzku zveme přítelkyni na chat na Facebooku).
5. Navazujeme na Facebooku velké množství virtuálních vztahů s neznámými, máme ve svém profilu více než 80 % neznámých uživatelů.
6. Projevy závislosti se objevují v běžném nevirtuálním světě (spojíme se na Facebooku). Zažíváme posedlost (pocity podobné jako u hazardu).

FAD dále diagnostikoval psycholog Michael Fenichel (Fenichel, 2009), který definoval tuto poruchu pomocí pěti průvodních jevů:

1. Noční užívání Facebooku vede k tomu, že se člověk dostatečně nevyspí a během druhého dne je unavený.

2. Uživatel tráví na Facebooku více než hodinu denně. Zde je třeba podotknout, že určit přesnou hranici, kdy je Facebooku příliš, není snadné. Údaj o hodině denně vychází z průměru v USA (cca v roce 2009), kdy běžný uživatel trávil na největší sociální síti zhruba 30 minut každý den. Samozřejmě pokud Facebook užíváte k práci, nemusíte dobu věnovanou mu profesionálně do limitu započítávat.

3. Obsese starými láskami a expartnery, které uživatel na Facebooku našel.

4. Užívání Facebooku na úkor práce a pracovních povinností.

5. Odloučení od největší sociální sítě v uživateli vzbuzuje pocity úzkosti a stresu. Představa delší doby bez připojení na Facebook vzbuzuje nezvladatelné nepříjemné pocity.

FAD je rovněž spojen s celou řadou *tělesných rizik*, ke kterým patří sedavý způsob života, obezita, cukrovka, srdeční nemoci, bolesti šíje, ramen, bederní páteře, kloubů, zápěstí, nemoci očí, silné zatěžování zraku, epilepsie, stres a s ním související problémy.

FAD je samozřejmě spojen také s *psychosociálními riziky*, ke kterým patří špatná organizace času, nepravidelnost v jídle, nedostatek spánku, zhoršení mezilidských vztahů, úzkost ve vztazích, neschopnost řešit problémy v komunikaci, u dětí dochází ke zhoršení školního prospěchu nebo soustředění se na práci, dochází k poruchám paměti atd.

6.4.2 Závislostní chování ve vztahu k hraní online her

Netolismus je velmi často spojen s prostředím online her na bázi MMORPG (massively multiplayer online role play game) – tedy her, ve kterých hrají online tisíce hráčů v jednom virtuálním prostředí. Tyto hry jsou celosvětově velmi rozšířené a oblíbené, hrají se nejen v zahraničí, ale také v České republice. Za typickou online hru nejčastěji vyvolávající či podporující závislostní chování je považován World of Warcraft (WoW), který má po celém světě předplaceno 10 milionů hráčů (Statista.com, 2015), další milióny hráčů tuto hru hrají na tzv. privátních serverech (kde hráči neplatí žádné poplatky).

Při pochopení podstaty netolismu je třeba uvědomit si, jaké potřeby dítěte či dospělého hraní online her vlastně uspokojuje. Vyjděme tedy z „pyramidy" hierarchie lidských potřeb amerického psychologa Abrahama Maslowa (Maslow, 1943).

Obr. 2. Pyramida lidských potřeb (Maslow)

Tyto potřeby lze uspokojit v běžném nevirtuálním světě a průměrný člověk o jejich uspokojení přirozeně usiluje. Zaměříme-li se na oblast online MMORPG her, můžeme říci, že MMORPG hry v kombinaci s dalšími internetovými službami jsou schopny uspokojit téměř beze zbytku veškeré lidské potřeby (Kamil Kopecký, 2011). A v případě, že z principu nemůže k uspokojení potřeby dojít (např. u fyziologických potřeb), jednoduše hráč potřebu potlačí. Uspokojení potřeb je v prostředí virtuálních online her ve srovnání s reálným nevirtuálním světem poměrně snadné – neúspěch můžete prostým opakováním změnit v úspěch.

Lákadlem, díky kterému MMORPG hry získávají stále nové hráče, je rovněž komunitní (chcete-li týmový) způsob hraní – bez spolupráce s ostatními hráči určité herní úkoly nemůžete splnit (např. zabít silného virtuálního protivníka). Proto také celá řada MMORPG (včetně WoW) umožňuje vytvářet sociální skupiny – tzv. gildy či týmy. S příslušností k týmu pak roste zodpovědnost, se kterou do hry hráči přistupují. Jejich přítomnost ve hře je pak nutná právě proto, že by bez nich celý tým nemohl zadané úkoly splnit. Online kooperace má i další pozitiva, např. silnější hráči pomáhají slabším. V praxi tedy mohou mít online hry pozitivní dopad – např. mohou děti učit *zodpovědnosti* (za svou roli ve skupině přátel), *spolupráci*, *rozvíjejí i další sociální dovednosti hráčů, logické myšlení, mimo jiné mají pozitivní vliv na zvyšování finanční gramotnosti hráčů*

(Kamil Kopecký, 2012a) apod. Obecně tedy neplatí, že jsou počítačové hry pouze zlem a žroutem času.

Velkým problémem, který podporuje rozvoj závislostního chování v prostředí MMORPG, je neexistence konce hry. MMORPG zpravidla nemají žádný konec, s rostoucím množstvím hráčů autoři do hry dodávají nové úkoly, rozšiřují herní možnosti, vydávají tzv. datadisky, které umožňují pokračovat ve hře do nekonečna. MMORPG tedy nelze vyhrát.

Online hraní v principu není nebezpečné, pokud jej jako hru vnímáte a dokážete mu vyhradit jasně dané meze a pravidla. K těm patří i stanovení začátku a konce. V principu není důležité, jak dlouho hru hrajete, pokud to nemá přímý vliv na váš reálný život. Existují hráči, kteří např. celý rok online hry nehrají – s výjimkou např. jednoho týdne v roce, kdy hrají intenzivně i 12 hodin denně. Řada hráčů rovněž online hru bere jako příjemnou relaxaci po namáhavém dni stráveném např. prací – i zde jde o projev běžné relaxace, potřeby odreagovat se. Bohužel v řadě případů netolismus vede ke ztrátě sociálních vztahů ve skutečném světě, destrukci rodiny, ztrátě zaměstnání atd.

Riziko vzniku netolismu roste zejména u těch, kteří již mají problémy v reálném světě a ty kompenzují ve světě virtuálním. Zde pak hledají útočiště a svůj neúspěch v realitě nahrazují úspěchem v kyberprostoru. Samozřejmě hra se může stát rovněž akcelerátorem neúspěchu v reálném světě.

Mezi zdravotní rizika, která jsou s hraním počítačových her spojena, patří dle Nešpora (Nešpor & Csémy, n.d.) *nezdravý životní styl s nedostatkem pohybu, onemocnění pohybového systému, obezita, virtuální nevolnost, zvýšené riziko úrazů a větší sklon riskovat, epilepsie, zhoršení interpersonálních vztahů a vyšší úzkost v sociálních vztazích, zvýšená agresivita a oslabení prosociálního chování*.

Podle profesora Michala Miovského z Kliniky adiktologie 1. lékařské fakulty Univerzity Karlovy a Všeobecné fakultní nemocnice v Praze vykazuje znaky závislosti na počítačových hrách 1–5 % českých dětí. Jako na závislé pohlíží odborníci na osoby, které tráví hraním počítačových her v průměru kolem 40 hodin týdně. U nich hrozí podobné znaky chování jako u lidí, kteří jsou závislí na látkových drogách – například přetrhání společenských vazeb, problémy v osobních vztazích, ale i zdravotní komplikace kvůli nedostatku pohybu (Skoupá, 2015).

6.4.3 Závislostní chování ve vztahu k mobilnímu telefonu

Mobilní telefony se staly běžnou součástí našich životů a jsou běžně přístupné jak dospělým, tak i dětem. Jsou cenově dostupné, uživatelsky přívětivé, dostatečně výkonné s komfortním uživatelským vybavením. Mobilní telefony jsou pro naše životy přínosné, jejich nadměrné používání však může mít na náš každodenní život významný a výrazný dopad.

Nadměrné používání mobilního telefonu je často považováno za behaviorální závislost, která je podobná dalším "nechemickým" závislostem, jako je patologické hráčství, kompulsivní nakupování, závislost na počítačových hrách apod. Studie realizované v zemích Asie a Austrálie identifikovaly symptomy závislosti na mobilních telefonech u pubescentů a adolescentů (Bianchi & Phillips, 2005; Toda, Monden, Kubo, & Morimoto, 2004). Ty dále upřesnili další autoři (Joel Billieux, 2012; Igarashi, Motoyoshi, Takai, & Yoshida, 2008; James & Drennan, 2005).

Mezi symptomy behaviorální závislosti na mobilním telefonu patří *touha používat neustále mobilní telefon, změny nálady, neschopnost regulovat používání mobilního telefonu a ztráta kontroly, emoční reakce, pokud telefon nefunguje, opakované kontrolování mobilu, neexistují situace, kdy byste mobilní telefon vypnuli, pociťujete nervozitu, pokud je mobilní telefon vybitý či mimo dosah* apod.

Mezi další negativa, která jsou s nadužíváním mobilních telefonů spojena, patří riziko dostat se do finančních potíží (vysoký účet za služby – stahování, nákupy aplikací apod.) (Joël Billieux, Van Der Linden, & Rochat, 2008), zdravotní rizika – např. poruchy spánku (Funston & MacNeill, 1999). Diskutovaná je rovněž otázka vlivu elektromagnetického záření na lidský mozek.

Fenomén nomofobie

Nomofobie (no mobile phone phobia) je jedním ze znaků behaviorální závislosti na mobilním telefonu a označuje *strach z toho, že mobilní telefon z nějakého důvodu nemůžeme používat* (King et al., 2013, 2014; Caglar Yildirim & Correia, 2015). Nomofobie vzniká jako produkt interakce mezi lidmi, informacemi a komunikačními technologiemi a postihuje velkou část populace mladých lidí.

Mezi typické příznaky nomofobie patří nervozita, kdykoli telefon nemáme u sebe, neustálá kontrola, jestli nám nepřišla nová zpráva, nutkání okamžitě reagovat, jakmile nás k tomu mobil vyzve, případně tzv. fantomové vibrace (pocit, že nám telefon v tichém režimu vibruje, i když to tak není).

Jedna z prvních studií, které se zaměřily na prevalenci nomofobie, proběhla ve Velké Británii (Daily Mail Online, 2008). Podle ní trpí nomofobií 53 % britských uživatelů mobilních telefonů. Podle autorů studie nomofobii vyvolává např. obava, že nemáme kredit, že máme vybitou baterii, že jsme v oblasti bez signálu apod.

Zajímavé výsledky poskytuje také studie, která proběhla v Indii (Murthy, 2012). 45 % sledovaných osob ve věku 18 až 30 let vykazovalo příznaky nomofobie, přičemž předcházející studie z roku 2009 naměřila úroveň pouze 20 % (Dixit et al., 2010).

Další studie proběhla na vzorku 537 tureckých vysokoškolských studentů a její výsledky dokazují, že 42,6 % z nich nomofobií skutečně trpí. Studie také potvrzuje, že se častěji oběťmi nomofobie stávají dívky než chlapci (C. Yildirim, Sumuer, Adnan, & Yildirim, 2015).

6.5 Dětská prostituce v online prostředí

Dětská prostituce realizovaná online představuje fenomén, který je v posledních letech často spojován zejména s prostředím sociálních sítí.

V této kapitole se pokusíme nastínit, kam sahají jeho počátky, v rámci které problematiky se s ním setkáváme, jaké jsou jeho příčiny, následky a kdo je oběť a útočník. Rovněž v této souvislosti uvedeme reálný příklad realizace dětské prostituce v online prostředí v podobě navazování prvotních kontaktů.

6.5.1 Počátky dětské prostituce

Z hlediska dějin lidstva není prostituce dětí nikterak novým jevem, obzvláště pokud vezmeme v úvahu definici dítěte dle Úmluvy o právech dítěte, jež nám říká, že se dítětem rozumí každá lidská bytost mladší 18 let (OSN, 1989).

Samotný výraz prostituce pochází z latinského *prostituere* a znamená vydávat se na obdiv, nabízet se k veřejnému smilstvu nebo vystavovat své pohlavní orgány (Vaníčková, 2007a), přičemž poslední uvedené je vzhledem k současné popularitě odvážných selfie fotek sdílených na internetu poměrně frekventovanou a mnohdy dobrovolnou záležitostí především dospívajících jedinců (viz kapitola o sextingu). Podle tvůrců dokumentu *Seznam se bezpečně!* jsou to právě dospívající, kteří přispívají k rozsáhlému šíření dětské pornografie na internetu, aniž by o tom měli vůbec tušení (Česká televize, 2013).

Abychom lépe pochopili problém dětské prostituce, tak je důležité nahlédnout alespoň ve stručnosti na prostituci stran jejího historického vývoje.

Počátky prostituce jako takové sahají již do doby prvobytně pospolné společnosti a záznamy o její existenci nacházíme v Eposu o Gilgamešovi starém přes čtyři tisíce let či ve Starém zákoně. V minulosti existovala prostituce posvátná nebo třeba pohostinná, která „*byla součástí pohostinnosti k bližnímu a byla známá u všech národů staré civilizace.*" (Vaníčková, 2007a) Kdokoliv (žebrák, host, …) překročil práh domu, tak měl právo na všechny projevy pohostinnosti jako pán domu. Muž tedy přenechal návštěvě svou postel, ženu, nebo nabídl panenství své dcery! První zmínky o legalizaci prostituce spadají asi do roku 530 př. n. l. ve starém Řecku, kde vznikaly i první školy, které umění prostituce vyučovaly. Ohromného rozvoje dosáhla prostituce dětí v 17. a 18. století, kdy bylo normou zaměstnávat v nevěstincích, jež běžně navštěvovali i 12–14letí chlapci, devítileté děti. Na přelomu 19. a 20. století se pak staly nezletilé prostitutky běžným standardem ve všech velkoměstech Evropy, což podporovalo i kuplířství jejich rodičů. Až 11. 6. 1922 byl schválen první aboliční zákon, který prostituci zakazoval. Světové války ale její rozmach opět podpořily. Valné shromáždění OSN však v roce 1949 přijalo *Konvenci o boji proti zneužívání lidských bytostí a vykořisťování bližního prostitucí*, kterou ratifikovala většina zemí (Vaníčková, 2007a).

Dle některých autorů (Ringdal, 2000; Vaníčková, 2007a) dnes mladé lidi v západní Evropě a v USA nevede k prostituci jen nouze a hlad, ale také touha po penězích a dobrodružství. A podle zprávy dětského fondu OSN je v současnosti předmětem sexuálního průmyslu (výroba dětské pornografie, poskytování sexuálních služeb) cca 1,8 až 2 miliony dětí, přičemž zkušenost s praktikami komerčního sexuálního zneužívání nebo jinými formami násilí sexuální povahy (prostituce je násilím často doprovázena) má 150 milionů dívek a 73 milionů chlapců, tj. celkem 223 milionů dětí (Milfait, 2015).

6.5.2 Komerční sexuální zneužívání a jeho formy

Pojem komerční sexuální zneužívání neboli *Commercial Child Sexual Abuse (CSEC)*, někdy také vykořisťování dětí, definoval Stockholmský kongres v roce 1996 jako každé užití dětí pro sexuální účely za finanční či jinou odměnu (Burčíková, Kutálková, & Hůle, 2008).

A dále u něj také rozlišil tři hlavní formy, kterými jsou (Jiří Dunovský, 2005):

- ***dětská prostituce*** (využití dítěte k sexuálním aktivitám za úplatu anebo za poskytnutí jiného plnění),

- ***dětská pornografie*** (jakékoliv zobrazení dítěte, které se skutečně nebo předstíraně zúčastní sexuálně explicitní aktivity, patří zde zpodobení dítěte, jeho sexuálních orgánů a rovněž samotná realizace sexuální aktivity), které se dnes v prostředí internetu a mobilních telefonů mnohdy nevědomky dopouštějí děti samotné,
- ***obchod s dětmi*** (jakákoliv transakce, při které je dítě jednou osobou či skupinou osob předáno jiné osobě či skupině osob za úplatu anebo za poskytnutí jiného plnění za účelem sexuálního průmyslu, dětské práce, prodeje orgánů atd.).

Všechny uvedené formy se spolu navzájem prolínají, to znamená, že například dětská pornografie uvádí dětskou prostituci nebo v ní přechází a obráceně.

Komerční sexuální zneužívání představuje miliardový byznys, a proto v roce 2000 druhý opční protokol k Úmluvě o právech dítěte vymezil kriminální jednání, které do oblasti komerčního sexuálního zneužívání spadá. V letech 2001 (kongres v Jokohamě), 2008 (sympozium v Rio de Janeiru) pak proběhla další setkání, jejichž účelem byla tvorba celosvětových směrnic, jež by umožnily proti komerčnímu sexuálnímu zneužívání bojovat (Blatníková, 2009).

Dalo by se říci, že výraznou měrou přispěl k rozvoji komerčního sexuálního zneužívání **Internet**, který z něj napomohl vytvořit globální problém. Různé služby v prostředí internetu a mobilních telefonů mají totiž nejen mnoho výhod, ale mohou být také příležitostí například k pořizování a sdílení dětské pornografie včetně lákání dětí k osobnímu setkání – jak již bylo popsáno v částech věnovaných kybergroomingu – kde dochází nejčastěji k sexuálnímu zneužití dítěte a k následnému nucení k dalším schůzkám za pomoci vydírání skrze foto/video záznam pořízený útočníkem, či dokonce obětí, které se její naivní nebo nerozvážné chování později vymstilo.

Internet je masmédium, neomezené a „anonymní" prostředí, jež snižuje citlivost dětí vůči sexuální tematice *„a za současného stavu naprosto nedostatečné sexuální výchovy v rodinách i ve školách přispívá k vytvoření domněnky, že ‚mít sex jako dítě' a ‚mít sex s nezletilým' je něco naprosto normálního a kdo se odlišuje, je divný.* " (Vaníčková, 2007a, 2007b)

Děti si dostatečně neuvědomují, že je na internetu obklopují stejní lidé jako v jejich okolí. Ztrácejí zábrany v domnění, že je tzv. virtuální svět jiný než svět reálný. A nedochází jim, že když se obnaží na síti, tak je to stejné jako kdyby tak učinily na ulici nebo ve škole, jelikož jsou oba světy spolu navzájem úzce propojeny (internet má však navíc takřka trvalou paměť!). Svým chováním tak

nahrávají útočníkovi, který od nich snadno získává materiály intimní povahy a skrze ně pak jednoduše s dítětem manipuluje, protože útok na sexualitu dítěte je považován za ten nejúčinnější.

6.5.3 Příčiny dětské prostituce online, typologie obětí

Jaké jsou tedy příčiny vzniku dětské prostituce nejen v online prostředí.

Dětská prostituce, potažmo komerční sexuální zneužívání, spadá do oblasti sociálně patologických fenoménů, jako je záškoláctví, šikana, delikvence, závislosti, extremismus, nadměrná agrese atp. Jde tak ruku v ruce s nízkou úrovní vzdělání, rozpadem nebo dysfunkcí rodiny a s chudobou (v našich podmínkách spíše s relativní chudobou ve srovnání například se zeměmi třetího světa), či dokonce s válečnými konflikty a rozvojem cestovního ruchu. Významným rizikovým faktorem vzniku dětské prostituce je rovněž osobní zkušenost se sexuálním zneužíváním v dětství.

Klasifikací dětské prostituce dle jejích příčin existuje vícero. Jiří Dunovský (Jiří Dunovský, 2005) například rozlišuje následující tři typy:

1. *Prostituci u dětí citově nevyzrálých*, které neumějí odhalit rizika manipulace a citového vykořisťování, takže snadno dokážou podlehnout útočníkovi či pasákovi.
2. *Ekonomickou prostituci*, jejíž obětí se může stát kterékoliv dítě s nedostatečně vytvořeným sebepojetím. Takovýto jedinec pak snadno podléhá diktátu vrstevnické skupiny a ze strachu z nepřijetí, například pro absenci značkového oblečení, mobilního telefonu atp. a z výsměchu podléhá možnosti snadného přivýdělku.
3. A *prostituci u zábavného typu oběti,* tj. u dítěte, které nemá rovněž potřebné sebepojetí, a snaží se jej proto dosáhnout směšným chováním až excesy a jednáním, o kterém si mylně myslí, že zaujme své okolí.

Vaníčková (Vaníčková, 2007b) pak popisuje u typů obětí komerčního sexuálního zneužívání výskyt dětské prostituce u dětí traumatizovaných, přinucených rodinou nebo nepříbuznou osobou, u dětí ulice a dětí se závislostí. A v neposlední řadě též hovoří o strategii zisku i o vrstevnickém vlivu na dítě.

Nás bude v souvislosti s online dětskou prostitucí zajímat zejména otázka vrstevnického vlivu, a to ve spojitosti s nedostatečným materiálním zabezpečením dítěte, tj. s chudobou, případně relativní chudobou rodiny. Podle závěrů Policie České republiky z roku 2009 se totiž mezi školáky rozšířil nový byznys – „*vydělávají si pár stovek v podobě kreditu do mobilu posíláním vlastních*

fotek neznámým lidem, kteří je kontaktují na internetu.“ (Wallerová & Vokáč, 2009) Přitom se jedná i o dvanáctileté děti, převážně však děti starší a dívky.

„*Pro dynamiku komerčního sexuálního zneužívání dětí je typické, že se stoupajícím věkem dítěte ubývá přinuceného chování dítěte vůči patologické podobě jeho „dobrovolné“ účasti*“ (Vaníčková, 2007b). Je ale zapotřebí upozornit na fakt, že se jedná o dobrovolnou účast pouze zdánlivou, jelikož je dítě vždy do sféry komerčního sexuálního zneužívání vehnáno pod různými okolnostmi. Děti – na rozdíl od dospělých – totiž nedokážou anticipovat následky svého chování a pokaždé u nich vyvstává otázka, jaká situace (např. ekonomické okolnosti) nebo událost (např. osobní, rodinná historie) z dětství vede k jejich patologickým myšlenkovým pochodům.

Každé dítě chce zapadnout do kolektivu a vyrovnat se svým spolužákům. Obzvláště teenageři vnímají kritiku za strany svých vrstevníků velice citlivě. A v případě odmítnutí a vyčlenění ze skupiny z důvodu absence nějaké věci typu moderního značkového oblečení, chytrého mobilního telefonu nebo třeba tabletu mohou usilovat o to vyrovnat se svým movitějším spolužákům a vyhnout se tak jejich posměchu. Tlak dnešní materialisticky založené společnosti je obrovský – a to nejen na děti, takže se pak nelze divit, když teenager usiluje o nalezení způsobu, jak svůj materiální nedostatek vykompenzovat. A v případě, že nepomohou, nebo nemohou pomoci jeho rodiče či blízcí lidé, může snadno podlehnout pokušení, manipulaci a slibům útočníka / pachatele komerčního sexuálního zneužívání, který mu nabízí snadnou a velmi rychlou cestu ven z momentální svízelné situace. Stačí se například v pohodlí domova vyfotit, i bez obličeje, a snímek pak útočníkovi za slušný obnos poslat... Jak rizikový tento „obchod“ ale bývá, popisuje kapitola věnovaná fenoménu zvanému kybergrooming.

Postupem času dochází k posouvání hranic a objevuje se první osobní zkušenost dítěte s pachatelem, kterou má zpočátku oběť tendenci utajit před svým okolím v přesvědčení, že se již nebude více opakovat, ale opak bývá bohužel pravdou. Patologické chování se opětovnými zkušenostmi dítěte začíná normalizovat a dítě si zvyká na určitý finanční standard, kterého prostitucí a mnohdy výrobou a šířením dětské pornografie docílilo. Snaží se všemožně obhájit své patologické jednání, což je ostatně ukázkově demonstrováno na výpovědích obětí komerčního sexuálního zneužívání ve filmu *Seznam se bezpečně 2*.

S věkem dítěte většinou ale klesá zájem útočníka/útočníků „o jeho služby“, a tak se vlivem svých patologických životních zkušeností stává takřka nezařaditelné do běžné, většinové společnosti. Po sociální, emocionální i duchovní stránce je

chudé a často není schopno pracovat „normálně“ za mnohem nižší příjem, než na jaký bylo zvyklé ze svého dřívějšího jednání.

Je nutno dodat, že velký podíl na rozvoji dětské prostituce a potažmo komerčního sexuálního zneužívání má společnost jako taková. Vyskytuje se v ní vysoká míra tolerance vůči prostituci a pornografii vůbec. Je v ní patrný odklon od morálních a duchovních hodnot. Víme také, že v dnešním moderním světě převládá konzumní způsob života, a v kurzu je tedy dostatečné finanční a materiální zázemí člověka. Média nám rovněž denně chrlí chybné vzory k nápodobě, jež jsou všeobecně tolerovány. Na internetu je dětská pornografie bytostně přítomna a navíc se potýkáme s vyšší mírou ochrany pachatele než oběti (Vaníčková, 2007a, 2007b).

6.5.4 Charakteristika pachatele dětské prostituce

Obecně lze pachatele sexuálního zneužívání dětí rozdělit na jedince, kteří využívají dítěte či mladistvého jakožto náhradního a snadno dostupného objektu, v případě momentální absence dospělého partnera/partnerky, a na jedince, kteří jsou deviantní – pedofilní, tedy trvale zaměření na dětské objekty.

85 % pachatelů tvoří muži a zbylých 15 % ženy, které však figurují většinou jako spolupachatelky nebo napomáhající (Milfait, 2015).

Při „*nekomplikovaném sexuálním zneužívání dětí hraje rozhodující roli více či méně narušená rodina a abúzora je nutno hledat především v ní, při komerčním sexuálním zneužívání jde většinou o přímé násilí či nátlak zprostředkovatelů i abúzorů k dosažení svých cílů zvenčí.* “ (Jiří Dunovský, 2005)

Rozdíl v sexuálním chování komerčního a nekomerčního typu pachatele není žádný. Pro komerční sexuální zneužívání je však příznačné, že *„je akt zneužití realizován buď prostřednictvím třetí osoby (tj. dalšího pachatele), nebo na základě dohody s dítětem, které své sexuální služby poskytuje za úplatu“* (Blatníková, 2009).

Potencionálním pachatelem komerčního sexuálního zneužívání dětí je člověk se sexuální deviací, dále jedinec obávající se dospělého – mohli bychom říci rovnocenného – sexuálního partnera a člověk vykonávající povolání, jež vyžaduje být stále na cestách. Dále také hrají roli snadná dostupnost a finanční nenáročnost dětí, moc a postavení dospělých a touha po vysokém bezpracném zisku (Vaníčková, 2007b).

Snaha o profilování konkrétního, typického pachatele by tedy byla sisyfovská. Vzhledem k faktu, že u pachatelů sexuálního zneužívání dětí nacházíme

rozličnou motivaci (sexuální motiv, touha po moci, hledání emocionální náklonnosti, levný a snadný přístup k objektu touhy atp.) k jejich chování a nelze přesně určit jejich společenské prostředí a postavení, útočníkem může být prakticky kdokoliv (lékař, vysokoškolský pedagog, prodavač, profesní řidič…).

6.5.5 Příklad dětské prostituce v online prostředí

Zde si uvedeme příklad dětské prostituce v online prostředí ve fázi navazování prvotního kontaktu. Jedná se o útržky komunikace zaznamenané Martinem Kožíškem, manažerem pro internetovou bezpečnost Seznam.cz a spolutvůrcem pořadů Seznam se bezpečně 1–3 (Kožíšek, 2014):

1. *Hledám kluka 12-14 let, co se nudí jak já, bez fotky nepište.*
2. *Kluk, co se nudí a šel by třeba na webku? Kolem 13ti?*
3. *Zajištěný podnikatel hledá…*
4. *Hledám holku, co by se nechala rozmazlovat.*
5. *Hledám kluka, co by to chtěl zkusit s gayem, nebudeš litovat*
6. *Byl jsem se ptát v mekáči, ale tam brigádníky nehledají : (*

Podle jeho průzkumu na 1 800 respondentech vycházejí nabídky na sex nejčastěji od dívek, a to v 77 % případů, chlapci se k nabídkám stavějí spíše pasivně. Ze všech oslovených dětí s nabídkou výdělku „pokud se nestydíš“ souhlasilo 21 % z nich… Kožíšek uvádí, že se průměrná cena sexu mezi dítětem a dospělým pohybuje kolem 750 korun, u gay styku jde až o 2 700 korun.

6.5.6 Následky dětské prostituce a její prevence

Následky dětské prostituce jsou celoživotní a devastující stran psychické, osobnostní, emocionální i sociální roviny dítěte, jež pozbývá své nevinnosti, dětství i zdraví, na které má nezadatelné právo. A co má negativní efekt na jednotlivce, to se v důsledku logicky odrazí na celé společnosti, ve které se pohybuje a působí. Vyvstává zde tak důležitost prevence tohoto sociálně patologického jevu.

Na školách by proto měla být věnována patřičná pozornost tomuto fenoménu, jelikož se komerční sexuální zneužívání, jehož je dětská prostituce součástí, dotýká zejména dětí školního věku. A přesto jej rodiče a široká veřejnost považují za jev spíše výjimečný. Patrně to odráží všeobecně nízkou informovanost o dané problematice, protože představa, že dítě sedící doma zavřené ve svém pokojíčku u počítače je v bezpečí – na rozdíl od situace, že pobíhá někde venku s kamarády, je mylná. Takže nejen děti, ale i rodiče by měli

vědět, jaká úskalí internet v souvislosti s komerčním sexuálním zneužíváním obnáší a jak rozpoznat závadové chování ve virtuálním prostředí a nepodlehnout nabídkám či slibům rozličných útočníků v kyberprostoru.

7 Primární prevence rizikového chování

V našem textu se zaměřujeme na témata, která jsou úzce spojena s primární prevencí rizikového chování, jejímž základem je dlouhodobá kontinuální práce s dětmi a mládeží, která je prováděna v menších skupinách a za aktivní účasti cílové skupiny. Primární prevenci můžeme rozčlenit na tzv. *specifickou* a *nespecifickou*. Specifickou primární prevenci lze rozdělit do tří úrovní (Ministerstvo školství, 2013):

1. Všeobecná primární prevence – zaměřuje se na běžnou populaci dětí a mládeže, zohledňuje pouze věková kritéria. Jedná se o programy pro větší počet účastníků (skupina do 30 účastníků).

2. Selektivní primární prevence – zaměřuje se na skupiny osob, u kterých jsou ve zvýšené míře přítomny rizikové faktory pro vznik a vývoj různých forem rizikového chování a jsou většinou více ohrožené než jiné skupiny populace. Pracuje se zde s menšími skupinami, případně i jednotlivci.

3. Indikovaná primární prevence – je zaměřena na jedince, u kterých se již vyskytly projevy rizikového chování. Jedná se o práci s populací s výrazně zvýšeným rizikem výskytu či počínajících projevů rizikového chování. Jedná se o individuální práci s klientem.

Prevence bývá ve společnosti často podceňovaná, protože se její výsledky nedostavují ihned, ale s časovým zpožděním, stejně tak je poměrně obtížné měřit, jak výskyt rizikového chování jednotlivé preventivní programy skutečně ovlivňují.

Mezi základní oblasti rizikového chování, na které se prevence zaměřuje, patří (Miovský, Skácelová, Zapletalová, & Novák, 2010):
a) záškoláctví,
b) šikana a extrémní projevy agrese,
c) extrémně rizikové sporty a rizikové chování v dopravě,
d) rasismus a xenofobie,
e) negativní působení sekt,
f) sexuální rizikové chování,
g) závislostní chování (adiktologie).

V širším pojetí pak k těmto oblastem řadíme další dva okruhy, které nelze jednoznačně zařadit do konceptu rizikového chování:

h) okruh poruch a problémů spojených se syndromem týraného a zanedbávaného dítěte,
i) spektrum poruch příjmu potravy.

Nová Národní strategie primární prevence rizikového chování dětí a mládeže 2013–2018 definuje následující rizikové formy chování dětí a mládeže (Ministerstvo školství, 2013):

1. Interpersonální agresivní chování – agrese, šikana, kyberšikana a další rizikové formy komunikace prostřednictvím multimedií, násilí, intolerance, antisemitismus, extremismus, rasismus a xenofobie, homofobie.

2. Delikventní chování ve vztahu k hmotným statkům – vandalismus, krádeže, sprejerství a další trestné činy a přečiny.

3. Záškoláctví a neplnění školních povinností.

4. Závislostní chování – užívání všech návykových látek, netolismus, gambling.

5. Rizikové sportovní aktivity, prevence úrazů.

6. Rizikové chování v dopravě, prevence úrazů.

7. Spektrum poruch příjmu potravy.

8. Negativní působení sekt.

9. Sexuální rizikové chování.

Do nespecifické primární prevence poté zařazujeme aktivity, které nemají přímou souvislost s rizikovým chováním a které napomáhají snižovat riziko vzniku a rozvoje rizikového chování prostřednictvím lepšího využívání volného času. Patří sem např. zájmové, sportovní a volnočasové aktivity a jiné programy, které vedou k dodržování určitých společenských pravidel, zdravého rozvoje osobnosti, k odpovědnosti za sebe a své jednání (Miovský et al., 2010; MŠMT, 2005).

7.1 Prevence rizikového chování na úrovni státu

Na úrovni státu je prevence rizikového chování koordinována paralelně více ministerstvy – např. Ministerstvo školství, mládeže a tělovýchovy se zaměřuje

na tzv. *školní prevenci*, Ministerstvo vnitra na tzv. *prevenci kriminality*, Ministerstvo zdravotnictví na tzv. *zdravotní prevenci* apod. Značná část rizikových fenoménů spadá do gesce více ministerstev, např. prevence extrémních a agresivních projevů, prevence drogové kriminality apod. Jednotlivé systémy prevence jsou realizovány paralelně, a ačkoli se zaměřují na podobná témata, v praxi často selhává vzájemná komunikace a koordinace jednotlivých aktivit (Miovský et al., 2010). Kromě toho se prevencí zabývají i nadrezortní orgány, jako např. Rada vlády pro koordinaci protidrogové politiky při Úřadu vlády a Republikový výbor prevence kriminality při Ministerstvu vnitra – v těchto orgánech jsou pak zastoupeny všechny věcně příslušné resorty.

Zaměříme-li se na úroveň školní prevence v gesci Ministerstva školství, mládeže a tělovýchovy, nalezneme zde *Pracovní skupinu zaměřenou na specifickou primární protidrogovou prevenci* a *Pracovní skupinu prevence kriminality a ostatních sociálně patologických jevů*, které jsou složené ze zástupců věcně příslušných rezortů, krajů, akademické obce, zástupců neziskového sektoru, školských poradenských zařízení atd. Cílem pracovních skupin je spolupráce, sjednocení přístupů a koordinací činností v dané oblasti napříč rezorty (Miovský et al., 2010).

Ministerstvo školství, mládeže a tělovýchovy dále metodicky vede a koordinuje síť školských koordinátorů, která je tvořena krajskými školskými koordinátory prevence (pracovníci odborů školství, mládeže a tělovýchovy krajských úřadů), metodiky prevence (pracovníci pedagogicko-psychologických poraden) a školními metodiky prevence (vybraní pedagogové ve školách a školských zařízeních).

V roce 2013 vznikla v gesci Ministerstva školství, mládeže a tělovýchovy Národní strategie primární prevence rizikového chování na období 2013–2018 (dále v textu jako Strategie). Strategie vychází ze zkušeností z minulých let a opírá se o současné trendy na poli primární prevence. Jejím hlavním cílem je prostřednictvím efektivního systému prevence fungujícího na základě komplexního působení všech na sebe vzájemně navazujících subjektů *minimalizovat vznik a snížit míru rizikového chování u dětí a mládeže* (Ministerstvo školství, 2013).

V obecné rovině je dílčím cílem Strategie *výchova k předcházení, minimalizaci či oddálení rizikových projevů chování, ke zdravému životnímu stylu, k rozvoji pozitivního sociálního chování a rozvoji psychosociálních dovedností a zvládání zátěžových situací osobnosti* jako standardní součást výchovně vzdělávacího

procesu v prostředí českých škol zabezpečovaná kvalifikovanými a kompetentními osobami a institucemi a dále pak motivace k opuštění rizikového chování, pokud již nastalo, a ochrana před dopady rizikového chování pokud již nastalo ve výrazné formě (Ministerstvo školství, 2013).

7.2 Prevence rizikového chování na úrovni školy

Stěžejním aktérem prevence rizikového chování na úrovni školy je zejména školní metodik prevence. Školní metodik prevence vykonává činnosti metodické, koordinační, informační a poradenské, jeho práce zahrnuje zejména (Miovský et al., 2010):

1. Koordinaci tvorby a kontroly realizace preventivního programu školy.

2. Koordinaci a participaci na realizaci aktivit školy zaměřených na prevenci záškoláctví, závislostí, násilí, vandalismu, sexuálního zneužívání sektami, prekriminálního a kriminálního chování, rizikových projevů sebepoškozování a dalších typů rizikového chování.

3. Metodické vedení činnosti učitelů školy v oblasti prevence rizikového chování (předcházení a časná pedagogická diagnostika rizikových projevů chování apod.).

4. Koordinaci spolupráce školy s orgány státní správy a samosprávy.

5. Kontaktování odpovídajícího odborného pracoviště a participaci na intervenci a následné péči v případě akutního výskytu rizikového chování ve škole.

6. Informační činnosti (zjišťování a předávání odborných informací o rizikovém chování, nabídkách programů a projektů, metodách a formách prevence, vedení databáze spolupracovníků školy apod.).

7. Další činnosti (vedení dokumentace apod.).

Jak již bylo řečeno, školní metodik prevence se výrazně podílí na přípravě a realizaci školních preventivních programů/strategií a také na realizaci minimálního preventivního programu.

Školní preventivní program je dlouhodobým preventivním programem pro školy a školská zařízení, který je součástí školního vzdělávacího programu (vycházejícího z příslušného rámcového vzdělávacího programu). Program má jasně definované a naplánované dlouhodobé a krátkodobé cíle a je naplánován tak, aby mohl být řádně proveden. Program musí podporovat zdravý životní

styl a být zdrojem podnětů pro zpracování a realizaci minimálního preventivního programu (Miovský et al., 2010).

Minimální preventivní program je konkrétním dokumentem školy zaměřeným na výchovu žáků ke zdravému životnímu stylu, na jejich osobnostní a sociální rozvoj a rozvoj jejich sociálně komunikativních dovedností. Je založen na podpoře vlastní aktivity žáků, pestrosti forem preventivní práce se žáky, zapojení pedagogů a spolupráci s rodiči. Minimální preventivní program je zpracován na období jednoho roku a zodpovídá za něj školní metodik prevence (Miovský et al., 2010).

Práce školního metodika prevence je velmi obtížná, musí disponovat velkým množstvím znalostí a dovedností z různých oborů, musí být schopen provádět základní či pokročilou diagnostiku školní skupiny, zároveň by měl sledovat nové trendy v oblasti rizikového chování dětí – kromě jiného právě také trendy spojené se zneužíváním ICT. V řadě případů je však toto nereálné – metodik vzhledem ke své vlastní pedagogické zátěži nemůže všechny tyto role plnit. Nabízí se tak možnost využít potenciálů různých preventivních projektů realizovaných státními a soukromými institucemi, které mohou účinným způsobem zajistit primární všeobecnou prevenci.

Do samotných aktivit v oblasti primární prevence jsou samozřejmě zapojeni i další učitelé, kteří pracují s jednotlivými skupinami dětí a jsou schopni diagnostikovat, zdali se ve skupině vyskytuje daný rizikový jev. V součinnosti se školním metodikem prevence a ředitelem navrhnou vhodné řešení problému, přičemž mohou využít širokou paletu nástrojů – kázeňských a jiných opatření (Chudý & Neumeister, 2014).

7.3 Digitální rodičovství jako součást prevence rizikového chování

Dalším aktérem, který se na primární prevenci výrazně podílí, je aktivní rodič – a to v rámci konceptu tzv. digitálního rodičovství. Digitální rodičovství je zjednodušeně koncept výchovy, ve které *rodič aktivně podporuje rozvoj informační a komunikační gramotnosti svého dítěte, ale také rozvíjí další složky jeho osobnosti (zejména sociální dovednosti, kritické myšlení, mediální gramotnost apod.)* (Kamil Kopecký, 2015a). V rámci digitálního rodičovství je důraz kladen mimo jiné na bezpečné používání ICT a podporu jeho pozitivního využívání.

7.3.1 Děti Generace Z

V rámci diskuse o konceptu digitálního rodičovství je třeba alespoň v krátkosti vysvětlit, jaké jsou vlastně současné děti a čím se liší od předcházejících generací. Děti 21. století (označované často také jako Generace Z, Generace I či Děti 3.0) (Bassiouni & Hackley, 2014; Horovitz, 2012) po celý svůj život vyrůstají pod vlivem informačních technologií, které vnímají jako běžnou a neviditelnou součást svého života. Internetové služby začínají aktivně využívat ve věku 2–3 let a mezi jejich první aktivity patří zejména hraní jednoduchých her a přehrávání videí (zejména pohádek). S příchodem mobilních dotykových zařízení se samozřejmě věková hranice kontaktu s technologiemi snížila, užívání tabletu je pro děti velmi uživatelsky přívětivé, audiovizuálně atraktivní a intuitivní. Od útlého věku tedy dítě zvyšuje své znalosti a dovednosti spojené s využíváním technologií, roste tak tedy jejich počítačová a informační gramotnost. Podle výsledků výzkumu počítačové gramotnosti ICILS 2013 (Brdička, 2014) jsou dokonce čeští žáci osmých tříd v počítačové a informační gramotnosti nejlepší na celém světě (předběhli takové země, jako Německo, Austrálii, Norsko apod.).

Je tedy zřejmé, že mají děti často vyšší IT znalosti a dovednosti než jejich rodiče, či dokonce učitelé. Tento stav je však bohužel *vykoupen nízkými sociálními dovednostmi, nízkou úrovní zkušeností (které logicky získávají v průběhu celého svého života), neschopností kriticky pracovat s informacemi a rozpoznat manipulaci, špatně nastavenými hranicemi chování, neschopností řešit konflikty, nadužíváním technologií na úkor dalších aktivit, závislostním chováním, destrukcí hodnotového systému* (Kamil Kopecký, 2015a) apod.

Tento rozpor často vede k rizikovým formám internetové komunikace, ve které se děti např. stávají oběťmi (ale také útočníky) různých forem kybernetické šikany, oběťmi internetové manipulace s cílem dítě sexuálně zneužít (tzv. kybergrooming), oběťmi různých forem internetových podvodů apod. Aby bylo možné tuto situaci změnit, je třeba aktivně s dětmi pracovat, věnovat jim svůj čas, umožnit jim načerpat zkušenosti a zvýšit úroveň jejich sociálních dovedností. Zásadní článek této změny představuje zejména samotný rodič.

7.3.2 Rodič jako základní nástroj změny

Dítě od nejútlejšího věku k rodiči vzhlíží, přijímá rodiče jako základní a zásadní autoritu, jako vzor, jako osobu, která dítěti umožňuje naplnit jeho potřeby (kromě biologických potřeb dítě potřebuje např. bezpečí, jistotu, sounáležitost, uznání, úctu apod.). Rodič se také stává základním prostředníkem, skrz kterého dítě poznává svět. V útlém věku lze dítě učit základní principy, které využije i v dalším životě – např. ***ověřovat si informace, dávat si pozor, jaké informace o sobě ostatním prozrazujeme, jak se chovat, abychom byli na internetu v bezpečí, s jakými riziky se na internetu můžeme setkat*** apod.

Stejně, jako rodič dítě učí, že nesmí např. na křižovatce přecházet na červenou, je třeba dítěti odmalička vštěpovat zásady bezpečného používání IT technologií, ale také dodržovat zásady určené samotným rodičům: např. *v počítači dítěte aktivovat rodičovský filtr a odfiltrovat nevhodný obsah (např. pornografické webové stránky), počítač zabezpečit antivirem, umístit PC na veřejně dostupném místě v bytě (a teprve později jej přesunout do dětského pokoje), společně s dítětem objevovat virtuální svět, nastavit dítěti pravidla používání počítače/notebooku či tabletu (např. délka, frekvence, účel používání)* apod.

Tato pravidla se mění s rostoucím věkem dítěte, např. od cca 9–10 let věku děti začínají aktivně využívat sociální sítě, začínají sdílet vlastní materiály – fotografie, videa, komunikují s dalšími uživateli, postupně se začínají zajímat o lidskou sexualitu apod. Pravidla je tedy nutné přizpůsobovat aktuální situaci – dítě postupně bude vyžadovat své soukromí, vyžadovat, aby mělo počítač ve svém pokoji apod.

Jak již bylo řečeno, děti často rozumí informačním a komunikačním technologiím lépe, než jejich rodiče. Aby tedy rodič pronikl do světa dítěte, může využít jednoduché strategie „začít spolu“ – tj. nechat se od svého dítěte poučit, nechat si vysvětlit, jak se používá třeba Facebook, jak se používají konkrétní programy, jak např. nasdílet informaci, jak ji z internetu smazat apod.

Dítě ocení, když je akceptováno jako autorita a zdroj informací, rodič na oplátku získá cenné informace o tom, co jeho dítě umí, s kým komunikuje a jaké služby využívá. Nejdůležitějším pravidlem tedy zůstává *zajímat se aktivně o své děti, komunikovat s nimi a mít přehled o tom, k čemu a jak děti počítač využívají*.

7.4 Vybrané projekty zaměřené na prevenci rizikového chování

V České republice existuje celá řada projektů orientovaných na prevenci rizikového chování v prostředí internetu. V následujícím textu se zaměříme na některé z nich.

7.4.1 Projekt E-Bezpečí (Univerzita Palackého v Olomouci)

Centrum prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého (dále Centrum PRVoK) realizuje národní certifikovaný projekt E-Bezpečí (www.e-bezpeci.cz). Projekt E-Bezpečí je zaměřený na nespecifickou primární prevenci v oblasti rizik spojených s elektronickou komunikací (patologické jednání navázané na online komunikaci). Kromě prevence uskutečňované především formou terénní edukace se zabývá také výzkumem, poradenstvím a intervencí v dané oblasti.

Projekt E-Bezpečí vznikl v roce 2008 díky grantové podpoře Grantové agentury ČR. Po ukončení tohoto grantu v roce 2009 byl projekt E-Bezpečí institucionálně zaštítěn Centrem prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci.

Témata projektu E-Bezpečí

Projekt E-Bezpečí se zaměřuje na tyto oblasti:

1. Kyberšikana (elektronická šikana).
2. Kybergrooming (manipulativní techniky sexuálních útočníků, kteří se jimi snaží donutit oběť k osobní schůzce s možností následného zneužití oběti).
3. Stalking a kyberstalking (nebezpečné pronásledování a nebezpečné vyhrožování v rámci reálného i virtuálního prostoru).
4. Spam a hoax (obtěžující, případně jinak poškozující nevyžádaná emailová pošta).
5. Phishing a sociální inženýrství (manipulativní metody útočníků vedoucí k vylákávání osobních údajů, zejména přístupových hesel k účtům).
6. Potenciálně riziková jednání uživatelů (např. sexting – rozesílání erotických materiálů mobilním telefonem).
7. Webcam trolling (zneužívání webkamer).
8. Potenciální rizika spojená s konkrétními virtuálními službami (sociální sítě – Facebook, Ask. fm, Líbímseti.cz aj, datová úložiště, úložiště uživatelských fotografií, videí atd.).
9. Ochrana bezpečí uživatelů služeb ICT (zabezpečení účtu, ochrana osobních

údajů ve virtuálním prostředí…).
10. Trestná činnost páchaná pomocí ICT.

Cíle projektu E-Bezpečí

Cílem projektu je především aktivní rozvíjení informovanosti o potenciálních rizicích spojených s ICT ve společnosti, a to zejména formou realizace vzdělávacích akcí i jinými osvětovými činnostmi, jejichž snahou je minimalizace těchto rizik, případně snížení škod, které mohou způsobit. Prevence hraje v dané problematice klíčovou roli – řešení vzniklých problémů je obvykle velmi komplikované a mnohdy také téměř nemožné (blokace závadného obsahu × rychlost jeho šíření v rámci virtuálního prostředí).

Mapování situace ve vývoji patologií spojených se zneužíváním ICT. Vzdělávání a výchova v dané oblasti – prevence v oblasti patologií spojených s užíváním ICT. Řešení situací spojených se zneužitím ICT – odhalování aktuálních problémů ve školách (v rámci výzkumného šetření i v rámci besed s žáky), nabízení možností řešení těchto problémů (poradenská činnost v rámci online poradny – psychologickýy, sociální a právní servis, intervence ze strany Policie ČR).

Cílové skupiny

Primární cílovou skupinu projektu E-Bezpečí představují děti, protože jsou to právě ony, které mohou být těmto jevům vystaveny nejvíce, také potenciální dopad na ně by mohl být největší. Děti tráví podstatnou část svého volného času virtuální komunikací na internetu, kde navazují různé sociální kontakty, komunikují s ostatními anonymními uživateli, zveřejňují citlivé informace atd. Nebezpečným komunikačním jevům tedy mohou být přímo vystaveny nebo se na nich podílet. Informovanost rodičů o problematice potenciálních rizik spojených s ICT je stále velmi nízká, v řadě rodin tak tato prevence prakticky není zastoupena. Také ve školách není z nejrůznějších důvodů této specifické prevenci věnován dostatečný časový prostor (především díky časové a odborné náročnosti), ačkoli se učitelé snaží ve většině případů prevenci zabezpečit.

Kromě dětí jsou tedy důležitou cílovou skupinou také rodiče, pedagogové a další osoby pracující s dětmi (pracovníci OSPOD, policisté, vychovatelé atd.). Mimo aktivity směřované na konkrétní cílovou skupinu se věnuje zvyšování informovanosti o dané problematice v rámci širší veřejnosti, a to např. veřejnými besedami, publikační činností, mediálními vstupy (rozhovory v médiích) atd.

Preventivní program E-Bezpečí

Preventivní program projektu E-Bezpečí zahrnuje několik navazujících částí:

1. Preventivní aktivity pro žáky 1. stupně ZŠ

První část preventivních aktivit pro žáky nižších stupňů ZŠ tvoří interaktivní workshopy realizované pro děti od 8 do 13 let. V rámci workshopů se děti učí rozpoznávat různé formy internetových rizik, vytvářet bezpečná hesla, konstruovat vlastní pravidla bezpečného chování na internetu – vše hravou a zábavnou formou s důrazem na emoční prožitek dítěte.

2. Preventivní aktivity pro žáky 2. stupně ZŠ a žáky SŠ

Aktivity pro žáky 2. stupně ZŠ a žáky SŠ mají formu interaktivních besed, ve kterých jsou žáci seznámeni se základními rizikovými formami chování, kazuistikou případů, metodami ochrany a obrany apod. Žáci vyvozují řešení konkrétních krizových situací, navrhují bezpečnostní pravidla a preventivní opatření, aktivně se zapojují do činnosti apod.

3. Preventivní aktivity pro učitele, rodiče a další cílové skupiny

Certifikovaná školení pro pedagogy poskytující průřez nejčastějšími patologiemi souvisejícími se zneužitím ICT, případně se zaměřují na konkrétní vybraná témata. Náplň školení často ovlivňují sami učitelé svými dotazy přímo na místě (např. si ověřují správnost svých postupů při řešení konkrétních situací).

Během školení se učitelé naučí jednotlivé situace identifikovat a v rámci možností také řešit. Jsou seznámeni s různými strategiemi prevence, řešení problémů i jejich právní kvalifikací.

Školení je doprovázeno prezentacemi a videoukázkami. Učitelé také získávají řadu materiálů, které mohou využít k dalšímu vzdělávání, případně k další práci s žáky.

4. Outdoorové preventivní aktivity.

Projekt E-Bezpečí rovněž participuje na řadě outdoorových aktivit, jako jsou *Veletrh vědy a výzkumu UP, Noc vědců, Rozhodni se sám,* festival *Utubering* apod. Smyslem těchto aktivit je zejména upozornit veřejnost na témata spojená

s rizikovým chováním v prostředí internetu, nabídnout jí strategie rozpoznávání potenciálně rizikového chování a poskytnout možná řešení.

Partnerství

Projekt E-Bezpečí v oblasti prevence spolupracuje s celou řadou subjektů jak na úrovni veřejného, tak i privátního sektoru. Aktivně spolupracuje např. s Policií ČR, pedagogicko-psychologickými poradnami, sdružením Linka bezpečí, s odbory sociálně-právní ochrany dětí, s pracovníky statutárních měst apod. Spolupracuje také s firmami Seznam.cz, Google, Vodafone, Allegro Group, IBM apod.

V roce 2015 získal projekt E-Bezpečí 1. místo v národním kole Evropské ceny prevence kriminality.

Další informace o projektu naleznete na internetových stránkách www.e-bezpeci.cz.

7.4.2 Seznam se bezpečně (Seznam.cz)

Projekt *Seznam se bezpečně!* původně vznikl jako doplňková aktivita sociální sítě Lidé.cz, na které bylo možné pozorovat jevy, ohrožující její uživatele. Za úkol měla informovat uživatele o rizicích seznamování nebo komunikaci s neznámými lidmi. V první fázi šlo o výrazné posílení administrátorského týmu, který dohlížel nad závadným obsahem a některé závažnější poznatky předával PČR. Šlo zejména o výměnu dětské pornografie na chatu, diskuzích nebo podvodné aktivity spojené s nákupem zboží.

Posun v projektu nastal v roce 2009, a to natočením filmu, který byl rozeslán na adresy všech uživatelů sociálních sítí provozovaných společností Seznam.cz (Lidé.cz, Spolužáci.cz, Hry.cz).

Během prvního týdne měl dokument milion přehrání a poradna, která vznikla souběžně s filmem, byla zahlcena příběhy lidí. Zároveň byl film distribuován na všechny základní školy a víceletá gymnázia jako doporučená učební pomůcka. Tuto snahu podpořilo Ministerstvo školství, mládeže a tělovýchovy ČR.

V roce 2012 se začaly v chování internetových uživatelů projevovat změny. Vzniklo proto pokračování dokumentu, které mělo premiéru na Zlínském filmovém festivalu pro děti a mládež. Film *Seznam se bezpečně 2* se věnuje tématům dětské prostituce, seznamování a sociálnímu inženýrství. Součástí pokračování projektu, byly i krátké hrané spoty „Křečci v síti“, které vznikly ve spolupráci s Divadlem v Dlouhé. Došlo také k výraznému propojení aktivit

s ostatními partnery – Policií ČR, Linkou bezpečí nebo projektem E-Bezpečí Univerzity Palackého v Olomouci a dalšími.

Na projekt Seznam se bezpečně! navazují odborné konference, vzdělávání učitelů a žáků a další aktivity, průměrně je zrealizováno přibližně 50 akcí ročně.

Hlavním úkolem celého projektu je popularizace vážných internetových témat. Proto vznikla společně se Studiem Ypsilon divadelní verze projektu s názvem#jsi_user. Prostřednictvím dramatizace je možné dětské i dospělé uživatele nejen pobavit, ale také jim zábavnou formou předat informace o rizicích internetových závislostí tak, aby jim porozuměli. Inscenace vznikala metodou kolektivní improvizace, debat a diskuzí, aby co nejvíce reagovala na aktuální události. Proto i text této hry je z 99 % autentický materiál z internetu.

V roce 2015 bylo natočeno pokračování filmu *Seznam se bezpečně! 3*, které je určené hlavně pro rodiče. Popisuje případ skautských vedoucích, kteří prostřednictvím internetu a sociálních sítí zneužili 39 dětí.

Sekundárním cílem aktivit spojených s prevencí rizikového chování je implementace získaných poznatků do internetových služeb. Získané poznatky motivují společnost Seznam.cz k tomu, aby při vytváření služeb přemýšlela nad jejich společenským dopadem a vytvářela je bezpečnější. Zavazující je i ocenění z rukou prezidenta ČR Miloše Zemana – Zlatý záchranářský kříž – za výjimečný nebo kreativní počin k osvětě a vzdělávání.

Bližší informace o projektu naleznete na www. seznamsebezpecne.cz.

7.4.3 Web Rangers (Google Inc.)

Projekt Web Rangers je jedním z mezinárodních projektů iniciovaných firmou Google, zaměřených na oblast rizikového chování v prostředí internetu. Projekt je úspěšně realizován v Izraeli, na Novém Zélandu, Nizozemí, Keni a dalších zemích včetně České republiky.

V České republice je projekt Web Rangers realizovaný ve spolupráci projektu E-Bezpečí Univerzity Palackého v Olomouci, firmy Google a Google Education Group (GEG). Je zaměřen na prevenci rizikového chování dětí v prostředí internetu. Projekt je tedy orientován především na oblast všeobecné primární prevence rizikového chování, která je v současnosti vzhledem k nárůstu kyberkriminality a souvisejících sociálně-patologických jevů velmi důležitá – umožňuje totiž na jedné straně rizikům předcházet, na straně druhé naučit se účinným způsobem bránit, případně pomáhat obětem v nouzi. Projektu se

ročně účastní přibližně 100 dětí z celé ČR, které jsou pečlivě vybrané organizačním týmem a u kterých je pravděpodobné, že mají o danou problematiku skutečně zájem.

Základním principem, ze kterého projekt Web Rangers vychází, je přenos znalostí a dovedností z lektorů na děti, které informace dále šíří různými kanály mezi své vlastní vrstevníky (např. spolužáky). Jedná se tedy o obdobu tzv. peer programů, které se v minulosti s úspěchem využívaly např. pro prevenci drogových závislostí.

Děti, zapojené do programu, procházejí přímým prezenčním výcvikem, který je zaměřen na pochopení základních principů fungování rizikových komunikačních jevů. Mezi základní témata, o kterých se účastníci programu dozví užitečné informace, patří zejména různé formy kyberšikany (vydírání, vyhrožování, provokování, obtěžování, zveřejňování cizích tajemství, fotografií a videozáznamů apod.), kybergrooming (riziková komunikace dítěte a dospělého uživatele internetu s cílem vylákat dítě na osobní schůzku a zneužít jej), sexting (dobrovolné sdílení vlastních intimních materiálů s jinými uživateli internetových služeb – zejména s partnerem/partnerkou) a rizika sociálních sítí (zneužití osobních údajů, blokace závadného obsahu apod.).

Edukace je realizována prostřednictvím souboru kazuistik, v rámci kterých dítě v roli oběti prožilo konkrétní rizikovou situaci, kterou bylo nuceno řešit. Děti si v kontextu jednotlivých případů uvědomují, v čem spočívá největší riziko jednotlivých forem kybernetických útoků a proč je nutné těmto kybernetickým hrozbám předcházet. Osvojí si také základní dovednosti spojené se strategií obrany a ochrany před těmito riziky, seznámí se se způsoby nahlašování a blokování závadného obsahu a získají celou řadu odkazů na zdroje pro realizaci svých projektových výstupů.

Součástí prezenčního výcviku je také seznámení se se zajímavými technologiemi, jako je např. Gooogle Glass, Oculus Rift, „chytré hodinky“ apod.

Každý „webranger“ má za úkol vymyslet a zrealizovat projekt, jehož cílem je rozšiřovat informace mezi další uživatele internetových služeb. Mezi typické výstupy mladých webrangerů patří např. krátká videa (klipy zaměřené na vybraná témata), komixy, webové stránky, addony do internetových prohlížečů, zrealizované přednášky a semináře pro děti a dospělé apod. Výstupy jsou poté šířeny prostřednictvím sociálních sítí (Google+, Facebook) a dalších komunikačních nástrojů.

Projekt Webrangers demonstruje, jak lze přenášet znalosti z akademického do komerčního prostoru a jak je možné pozitivním způsobem ovlivňovat společnost prostřednictvím mladé generace – dětí.

Bližší informace o projektu naleznete na www.webrangers.cz.

8 Zkušenosti s realizací programu školské primární prevence

8.1 Specifika edukace dětí mladšího školního věku

Projekt E-Bezpečí realizuje v rámci projektu Dětské univerzity Univerzity Palackého v Olomouci řadu interaktivních přednášek s workshopy pro děti ve věku 8–12 let (1. stupeň ZŠ). Jejich společným cílem je seznámit děti zábavným a aktivizujícím způsobem s problematikou bezpečného používání internetových služeb – a to prostřednictvím praktických činností a badatelsky orientované výuky.

Při edukaci dětí 1. stupně je nutné respektovat několik zásad:

1. Děti je nutné intenzivně motivovat a aktivizovat.

Základem efektivní práce s dětmi mladšího školního věku je především vhodná motivace a aktivizace. Motivaci lze realizovat např. prostřednictvím odměny, kterou děti získají, pokud se jim podaří splnit jednotlivé úkoly. Smysl odměn však řada propagátorů moderního přístupu ke vzdělávání odmítá s tím, že dítě se nebude chtít vzdělávat proto, aby získalo nové znalosti a dovednosti, ale proto, aby získalo odměnu. U dětí 1. stupně však může odměna sloužit jako „bonus“, který získá dítě po podání výkonu a neví o něm před ním.

2. Děti nesmí být v průběhu edukace traumatizovány.

Dítě, které prochází procesem prevence, by nemělo být vystaveno obsahu, který by jej mohl traumatizovat – jako jsou případy, kdy např. dítě pod vlivem kyberšikany spáchalo sebevraždu, dítě ublížilo jinému dítěti apod. V žádném případě nedoporučujeme využívat pro tuto formu edukace videa s dětskými oběťmi, jako je např. video Amandy Todd, která pod vlivem kyberšikany spáchala sebevraždu a natočila o svém příběhu velmi emotivní video. Toto video lze využít pro edukaci starších dětí, nikoli dětí 1. stupně ZŠ.

3. Děti musí dostat dostatek prostoru k sebevyjádření.

Děti jsou již od útlého věku nesmírně kreativní, vytvářejí si na různé situace a jevy názory a potřebují se o ně podělit s ostatními vrstevníky, ale také dospělými. Proto je vhodné jim dát dostatek prostoru pro sebevyjádření, pro rozvíjení jejich názoru apod. Dítě se může vyjádřit jak slovně (a diskutovat o svém názoru s ostatními), tak i písemně (např. zformováním vlastního pravidla bezpečného používání internetu, vytvořením bezpečného hesla, kresbou apod.).

4. Děti musí být motivovány k pozitivnímu a funkčnímu využívání technologií.

Cílem preventivních programů zaměřených na rizikové chování v prostředí internetu není dítě odradit od používání internetových služeb, ale naučit dítě tyto služby využívat co nejbezpečněji a naučit je rizikům předcházet. Pokud bude lektor dítě odrazovat od používání online technologií (např. způsobem, že *Facebook je zlo a nesmíte ho používat*…), děti postupně lektora přestanou respektovat jako autoritu a nebudou informace, které se jim bude snažit předat, akceptovat. V praxi pak bude takto realizovaná prevence neefektivní – s minimálním dopadem na dítě. Vhodné je představit dětem svět internetu realisticky – tj. např. formou, že *stejně jako v reálném světě, tak i v tom internetovém můžeme narazit na dobré a špatné, hodné a zlé uživatele, kteří se mohou snažit jim ublížit.*

Naším cílem je děti naučit předcházet rizikům a bránit se. Vhodné je také zbytečně nedémonizovat sociální sítě jako „nebezpečná prostředí“, ale spíše je představit jako nástroje, které mohou být využívány pozitivně, ale také negativně.

5. Děti se musí spolupodílet na vytváření vzdělávacího obsahu = výstupů z aktivit.

Osvědčeným způsobem, jak lze děti efektivně zapojit do preventivních aktivit, je nechat je spolupodílet se na vytváření výstupů z jednotlivých preventivních aktivit. V praxi to např. znamená nechat děti navrhnout specifické pravidlo používání internetové služby, algoritmus odhalení internetového útočníka, navrhnout nové způsoby zabezpečení emailového účtu, zpracovat videoklip propagující určité téma, navrhnout komix, plakát sociální reklamy apod.

8.2 Specifika edukace dětí staršího školního věku

Při realizaci programů primární prevence se zaměřením na děti staršího školního věku (od 12 let věku) je nutné uvědomit si, že takto staré děti již:

a) pravděpodobně mají účet na sociální síti (ačkoli porušují pravidla o minimální věkové hranici pro vstup do tohoto prostředí),
b) přicházejí do období puberty a aktivně se zajímají o informace, které jsou spojené např. s tématy lidské sexuality,
c) aktivně se na internetu seznamují, hledají kamarády, ale také možné partnery,
d) většina z nich má k dispozici mobilní telefon či tablet,
e) aktivně využívají komunikační služby typu WhatsApp, Viber, Skype,
f) jsou sebevědomé a v prostředí internetu si věří, mají celou řadu znalostí a dovedností o tom, jak ICT funguje a jaké služby se dají na internetu využívat.

Prevenci lze tedy vhodným způsobem orientovat na témata, která děti vstupující do puberty zajímají. Konkrétně například:
a) rizikové seznamování v prostředí internetu,
b) sexting a další formy rizikového sdílení informací,
c) rizikové používání sociálních sítí.

9 Slovo závěrem

Informační technologie se staly v posledních letech velmi důležitou součástí našich životů a řada z nás si již bez nich nedokáže svůj život představit. Současná generace dětí je s technologiemi v kontaktu již od útlého věku (první aktivní kontakt s počítačem či tabletem navazuje dítě ve věku 2–3 let), mobilní telefony se staly běžnou součástí dětského inventáře již od 2. třídy ZŠ, v dalších ročnících jsou děti velmi často vybaveny tablety, notebooky a další technikou. S technikou pak tráví také volný čas – s ICT vstávají a také usínají.

IC technologie mají na děti (ale i dospělé) zcela jistě pozitivní dopady – umožňují snadno a rychle komunikovat, rozvíjet kreativitu, vyhledávat informace, učit se, bavit se apod. Mají však také dopady negativní, které jsou reprezentovány nejrůznějšími rizikovými formami chování.

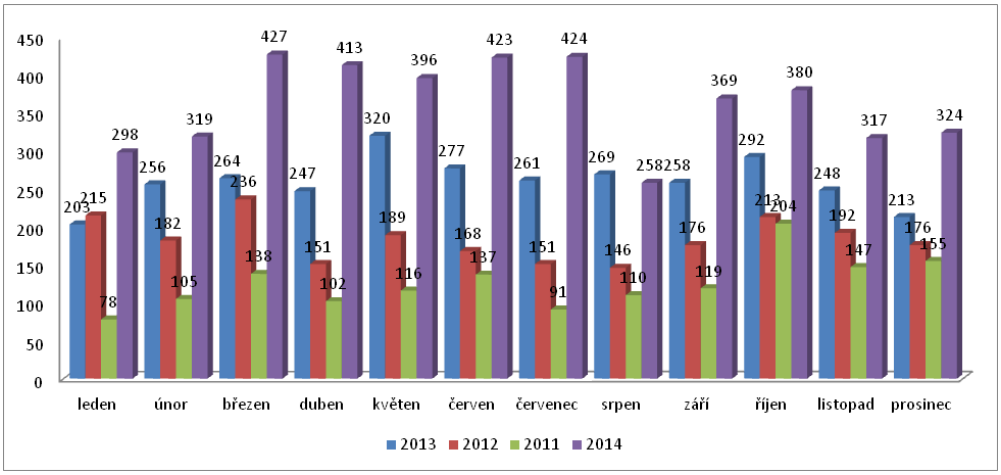
Cílem naší publikace bylo upozornit zejména na negativa, která jsou s využíváním informačních a komunikačních technologií v prostředí internetu úzce spojena, a nabídnout možná řešení existujících problémů.

Děkujeme, že jste naší publikaci věnovali svůj čas.

Kamil Kopecký
René Szotkowski
Veronika Krejčí

10 Příloha 1 – Statistika internetové kriminality v ČR (2011–2014)

Tab 20. Porovnání počtu spáchaných skutků v letech 2011–2014 (podle měsíců)



Zdroj: Statistické přehledy Policejního prezidia ČR

2014 .....4 348 spáchaných skutků
2013 .....3 108 spáchaných skutků
2012 .....2 195 spáchaných skutků
2011 .....1 502 spáchaných skutků

Tab 21. Trestné činy spáchané v prostředí internetu a ostatních počítačových sítí

Trestný čin (údaje od 1. 1. 2014 do 31. 12. 2014)	*Počet spáchaných skutků*
loupež (§ 173)	1
násilí proti úřední osobě mimo policie (§§ 323,4,5,6)	6
násilí a vyhrož. proti skup. obyvatel a jednotl. (§ 323,4,5,6)	1
nebezpečné vyhrožování (§ 353)	56
nebezpečné pronásledování (§ 354)	50
vydírání (§ 175)	53
porušování domovní svobody (§ 178)	1
útisk (§ 177)	1
sexuální nátlak (§ 186)	6
pohlavní zneužívání ostatní	1
ohrožování mravnosti (§ 191)	36
kuplířství (§ 189)	2
ostatní mravnostní trestné činy (§§ 190,192,193,194)	195
krádeže vloupáním do kiosků (§ 205)	1
krádeže vloupání do víkend. chat soukr. osob (§§ 178, 205)	1
krádeže prosté – motor. vozidel jednost. (§§ 205, 207)	1
krádeže prosté v jiných objektech (§ 205)	93
krádeže prosté ostatní (§ 205)	64
podvod (§ 209)	1745+369
zpronevěra (§ 206)	13
neoprávněné užívání cizí věci (§ 207)	1
zatajení věci (§ 219)	8
výtržnictví (§§ 358, 359)	2
ohrožování výchovy mládeže (§§ 201,202)	74
nedovolená výr. a držení psych. látek a jedů pro jednotl. (§ 283)	5
nedovolené ozbrojování (§ 279)	1
šíření toxikomanie (§ 287)	6
nedovolená výr. a držení psych. látek a jedů pro sebe (§ 284)	1
výroba a nakládání s lát. s hormon. účinkem (§ 288)	1
neoprávněné nakládání s osobními údaji	2
maření výkonu úředního rozhodnutí (§§ 337,410)	3
překup. a přechovávači – podílnictví (§§ 214,215)	5
šíření poplašné zprávy (§ 357)	11
hanob. národa, rasy, etnické a jiné skup. (§ 355)	5
podněcování k národní a rasové nenávisti (§ 356)	13
podpor. a propag. hnutí směř. svobody (§§ 403,4,5)	5
ostatní trestná činnost	133
tr. činy proti předpis. o nekalé soutěži (§ 248)	3
neoprávněné podnikání (§ 251)	10
krádež (§ 205)	10
padělání a pozměňování veřejné listiny (§ 348)	27
ohrož. zdraví závad. potravinami a jinými (§§ 156, 7)	18

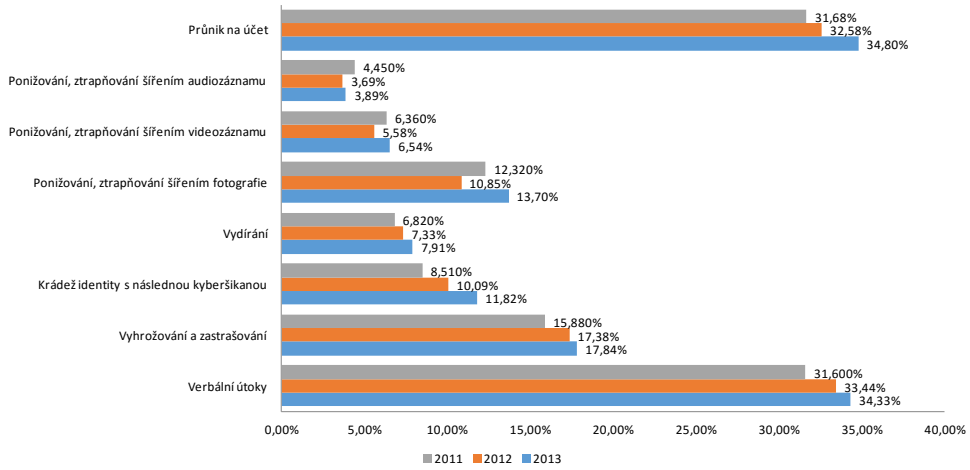
porušování tajemství dopravovaných zpráv (§ 182)	10
zpronevěra (§ 206)	7
neoprávněné nakládání s osobními údaji (§ 180)	1
neoprávněné držení platebního prostředku (§ 234)	103
poruš. práv k ochr. známce, obchod. jménu (§ 268)	17
poruš. autor. práv k databázi, padělání (§§ 270,1)	245
zastř. pův. věcí, tzv. praní špinavých peněz (§§ 216,7)	35
poškoz. a zneuž. záznamu na nosiči info. (§§ 231,2)	542
pojistný podvod (§ 210)	4
úvěrový podvod (§ 211)	340
ostatní hospodářské trestné činy (§§ 181,183,218)	4
Celkem	**4348**

Zdroj: Statistické přehledy Policejního prezidia ČR

11 Příloha 2 – Vývoj kyberšikany u českých dětí (2011–2013)

Následující graf a tabulka shrnují výsledky prevalence kyberšikany v populaci českých dětí, která byla naměřena s využitím výzkumného nástroje Centra prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci.

Graf 10. Vývoj kyberšikany v populaci českých dětí (2011–2013) – oběti



Tab 22. Vývoj kyberšikany v populaci českých dětí (2011–2013) – oběti

	2013	***2012***	***2011***
Verbální útoky	34,33 %	33,44 %	31,60 %
Obtěžování prozváněním	26,36 %	24,08 %	23,43 %
Vyhrožování a zastrašování	17,84 %	17,38 %	15,88 %
Krádež identity	11,82 %	10,09 %	8,51 %
Vydírání	7,91 %	7,33 %	6,82 %
Ponižování, ztrapňování šířením fotografie	13,70 %	10,85 %	12,32 %
Ponižování, ztrapňování šířením videa	6,54 %	5,58 %	6,36 %
Ponižování, ztrapňování šířením audia	3,89 %	3,69 %	4,45 %
Průnik na účet	34,80 %	32,58 %	31,68 %
	n>28000	*n>21000*	*n>12000*

12 Příloha 3 – Test úrovně nomofobie (NMP-Q dotazník)

Úroveň nomofobie se testuje pomocí tzv. NMP-Q dotazníku, který byl vytvořen výzkumníky z Iowa State Univerzity (Caglar Yildirim & Correia, 2015). Test obsahuje celkem 20 otázek – ke každé otázce přiřadíme hodnotu 1 (naprosto nesouhlasím) až 7 (silně souhlasím).

---

1. Cítil bych se nepříjemně bez neustálého přístupu k informacím prostřednictvím svého mobilního telefonu.

2. Naštval bych se, kdybych se nemohl podívat na informace na mém mobilním telefonu, kdybych to chtěl udělat.

3. Znervózňovalo by mě, kdybych nemohl na svůj mobilní telefon přijímat zprávy (události, počasí atd.).

4. Rozčílil bych se, kdybych nemohl používat mobilní telefon a jeho možnosti, kdybych chtěl.

5. Vyděsilo by mě, kdyby mi v telefonu došla baterie.

6. Zpanikařil bych, kdybych vyčerpal svůj měsíční datový limit nebo by mi došel kredit.

7. Kdybych neměl dostupný signál operátora nebo se nemohl připojit k Wi-Fi, pak bych neustále kontroloval, jestli už signál mám nebo jestli už je Wi-Fi dostupná.

8. Kdybych nemohl používat svůj mobilní telefon, bál bych se, že bych něco spletl.

9. Kdybych nemohl chvíli svůj mobilní telefon používat, cítil bych nutkání ho zkontrolovat.

Když s sebou nemám svůj mobilní telefon. . .

10. Cítil bych se nervózní, protože nemohu okamžitě komunikovat se svou rodinou a/nebo přáteli.

11. Bál bych se, protože by mě nemohla moje rodina nebo přátele kontaktovat.

12. Cítil bych se nervózní, protože bych nemohl přijímat SMS zprávy a hovory.

13. Byl bych nervózní, protože bych nebyl v kontaktu se svou rodinou a přáteli.

14. Byl bych nervózní, protože bych nevěděl, jestli mě někdo nechtěl zastihnout.

15. Byl bych nervózní, protože by byl přerušen můj trvalý kontakt s rodinou a přáteli.

16. Byl bych nervózní, protože bych byl odpojen od mé online identity.

17. Cítil bych se nepříjemně, protože bych nemohl aktualizovat informace ze svých sociálních sítí a online médií (v originále I could not stay up-to-date with social media).

18. Cítil bych se nepříjemně, protože bych nemohl přijímat upozornění na aktualizace od mých kontaktů v rámci sociálních sítí a online médií (v originále I could not check my notifications for updates from my connections and online networks).

19. Byl bych nervózní, protože bych nemohl kontrolovat emaily.

20. Měl bych divný pocit, protože bych nevěděl, co dělat.

Výsledky (Gregorine, 2015)

20 bodů: Nejsi nomofobik. Máš zdravý vztah ke svému mobilnímu zařízení a nemáš problém být od něj oddělen.

21–60 bodů: Mírná nomofobie. Jsi trochu nervózní, když zapomeneš svůj telefon na den doma nebo uvízneš někde bez Wi-Fi signálu, ale v zásadě netrpíš žádnou větší úzkostí.

61–100: Střední nomofobie. Jsi ke svému přístroji připoután. Často kontroluješ aktualizace, když jdeš po ulici nebo hovoříš s přáteli, občas cítíš úzkost, když jsi odpojen. Měl bys zahájit detox.

101–120: Těžká nomofobie. Bez svého mobilu nejsi schopen fungovat ani minutu, neustále jej kontroluješ. Je to první věc, kterou ráno kontroluješ, poslední věc, kterou kontroluješ v noci. Mobil dominuje většině tvých každodenních aktivit. Je třeba zasáhnout a zahájit detox.

13 Příloha 4 – Právní rámec rizikových komunikačních jevů

13.1 Trestní zákoník (Zákon č. 40/2009 Sb.)

Trestné činy proti svobodě
§ 175 Vydírání
§ 176 Omezování svobody vyznání

Trestné činy proti právům na ochranu osobnosti, soukromí a listovního tajemství
§ 182 Porušení tajemství dopravovaných zpráv
§ 183 Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí
§ 184 Pomluva Trestné činy proti lidské důstojnosti v sexuální oblasti (ad sexting)
§ 191 Šíření pornografie
§ 192 Výroba a jiné nakládání s dětskou pornografií
§ 193 Zneužití dítěte k výrobě pornografie

Trestné činy proti rodině a dětem
§ 202 Svádění k pohlavnímu styku

Trestné činy proti majetku
§ 230 Neoprávněný přístup k počítačovému systému a nosiči informací
§ 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat
§ 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti

Trestné činy obecně ohrožující
§ 287 Šíření toxikomanie

Trestné činy narušující soužití lidí
§ 352 Násilí proti skupině obyvatelů a proti jednotlivci
§ 353 Nebezpečné vyhrožování
§ 354 Nebezpečné pronásledování (tzv. kyberstalking)
§ 355 Hanobení národa, rasy, etnické nebo jiné skupiny osob
§ 356 Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod

Jiná rušení veřejného pořádku
§ 357 Šíření poplašné zprávy

Další formy trestné součinnosti
§ 364 Podněcování k trestnému činu
§ 365 Schvalování trestného činu

13.2 Občanský zákoník (Zákon č. 89/2012 Sb.)

Ochrana osobnosti

§ 81 (1) Chráněna je osobnost člověka včetně všech jeho přirozených práv. Každý je povinen ctít svobodné rozhodnutí člověka žít podle svého.

§ 81 (2) Ochrany požívají zejména život a důstojnost člověka, jeho zdraví a právo žít v příznivém životním prostředí, jeho vážnost, čest, soukromí a jeho projevy osobní povahy.

§ 84 Zachytit jakýmkoli způsobem podobu člověka tak, aby podle zobrazení bylo možné určit jeho totožnost, je možné jen s jeho svolením.

§ 85 (1) Rozšiřovat podobu člověka je možné jen s jeho svolením.

§ 85 (2) Svolí-li někdo k zobrazení své podoby za okolností, z nichž je zřejmé, že bude šířeno, platí, že svoluje i k jeho rozmnožování a rozšiřování obvyklým způsobem, jak je mohl vzhledem k okolnostem rozumně předpokládat.

§ 86 Nikdo nesmí zasáhnout do soukromí jiného, nemá-li k tomu zákonný důvod. Zejména nelze bez svolení člověka narušit jeho soukromé prostory, sledovat jeho soukromý život nebo pořizovat o tom zvukový nebo obrazový záznam, využívat takové či jiné záznamy pořízené o soukromém životě člověka třetí osobou, nebo takové záznamy o jeho soukromém životě šířit. Ve stejném rozsahu jsou chráněny i soukromé písemnosti osobní povahy.

§ 87 (1) Kdo svolil k použití písemnosti osobní povahy, podobizny nebo zvukového či obrazového záznamu týkajícího se člověka nebo jeho projevů osobní povahy, může svolení odvolat, třebaže je udělil na určitou dobu.

§ 87 (2) Bylo-li svolení udělené na určitou dobu odvoláno, aniž to odůvodňuje podstatná změna okolností nebo jiný rozumný důvod, nahradí odvolávající škodu z toho vzniklou osobě, které svolení udělil.

§ 88 (1) Svolení není třeba, pokud se podobizna nebo zvukový či obrazový záznam pořídí nebo použijí k výkonu nebo ochraně jiných práv nebo právem chráněných zájmů jiných osob.

§ 88 (2) Svolení není třeba ani v případě, když se podobizna, písemnost osobní povahy nebo zvukový či obrazový záznam pořídí nebo použijí na základě zákona k úřednímu účelu nebo
v případě, že někdo veřejně vystoupí v záležitosti veřejného zájmu.

§ 89 Podobizna nebo zvukový či obrazový záznam se mohou bez svolení člověka také pořídit nebo použít přiměřeným způsobem též k vědeckému nebo uměleckému účelu a pro tiskové, rozhlasové, televizní nebo obdobné zpravodajství.

§ 90 Zákonný důvod k zásahu do soukromí jiného nebo k použití jeho podobizny, písemnosti osobní povahy nebo zvukového či obrazového záznamu nesmí být využit nepřiměřeným způsobem
v rozporu s oprávněnými zájmy člověka.

13.3 Zákon o elektronických komunikacích (Zákon č. 127/2005 Sb.)

§ 67 Identifikace zlomyslných nebo obtěžujících volání
§ 93 Zneužití elektronické adresy odesílatele

13.4 Zákon o ochraně osobních údajů (Zákon č. 101/2000 Sb.)

§ 10 Při zpracování osobních údajů správce a zpracovatel dbá, aby subjekt údajů neutrpěl újmu na svých právech, zejména na právu na zachování lidské důstojnosti, a také dbá na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů.

§ 44 (2c) Fyzická osoba se jako správce nebo zpracovatel dopustí přestupku tím, že při zpracování osobních údajů shromažďuje nebo zpracovává osobní údaje v rozsahu nebo způsobem, který neodpovídá stanovenému účelu [§ 5 odst. 1 písm. d), f) až h)],

§44a (1) Fyzická osoba se dopustí přestupku tím, že poruší zákaz zveřejnění osobních údajů stanovený jiným právním předpisem.

§44a (2) Za přestupek podle odstavce 1 lze uložit pokutu do 1 000 000 Kč.

§44a (3) Za přestupek podle odstavce 1 spáchaný tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem lze uložit pokutu do 5 000 000 Kč.

14 Příloha 5 – Právní rámec dětské prostituce v ČR

Komerční sexuální zneužívání, tj. dětská prostituce, dětská pornografie a obchod s dětmi, představuje trestný čin, který není v českých zákonech definován jakožto celek, nýbrž je právně pokryt celou řadou dílčích trestných činů, kterými jsou ("Trestní zákoník. Předpis č. 40/2009," 2009):

14.1 Obchodování s lidmi, § 168 (Zákon č. 40/2009 Sb.)

(1) Kdo přiměje, zjedná, najme, zláká, svede, dopraví, ukryje, zadržuje nebo vydá dítě, aby ho bylo jiným užito

- *a) k pohlavnímu styku nebo k jiným formám sexuálního zneužívání nebo obtěžování anebo k výrobě pornografického díla,*
- *b) k odběru tkáně, buňky nebo orgánu z jeho těla,*
- *c) k službě v ozbrojených silách,*
- *d) k otroctví nebo nevolnictví, nebo*
- *e) k nuceným pracím nebo k jiným formám vykořisťování, anebo kdo kořistí z takového jednání, bude potrestán odnětím svobody na dvě léta až deset let.*

(2) Stejně bude potrestán, kdo jinou osobu než uvedenou v odstavci 1 za použití násilí, pohrůžky násilí nebo jiné těžké újmy nebo lsti anebo zneužívaje jejího omylu, tísně nebo závislosti, přiměje, zjedná, najme, zláká, svede, dopraví, ukryje, zadržuje nebo vydá, aby jí bylo jiným užito

- *a) k pohlavnímu styku nebo k jiným formám sexuálního zneužívání nebo obtěžování anebo k výrobě pornografického díla,*
- *b) k odběru tkáně, buňky nebo orgánu z jejího těla,*
- *c) k službě v ozbrojených silách,*
- *d) k otroctví nebo nevolnictví, nebo*
- *e) k nuceným pracím nebo k jiným formám vykořisťování, anebo kdo kořistí z takového jednání.*

(3) Odnětím svobody na pět až dvanáct let nebo propadnutím majetku bude pachatel potrestán,

- *a) spáchá-li čin uvedený v odstavci 1 nebo 2 jako člen organizované skupiny,*

b) vydá-li takovým činem jiného v nebezpečí těžké újmy na zdraví nebo smrti,

c) spáchá-li takový čin v úmyslu získat pro sebe nebo pro jiného značný prospěch, nebo

d) spáchá-li takový čin v úmyslu, aby jiného bylo užito k prostituci.

(4) Odnětím svobody na osm až patnáct let nebo propadnutím majetku bude pachatel potrestán,

a) způsobí-li činem uvedeným v odstavci 1 nebo 2 těžkou újmu na zdraví,

b) spáchá-li takový čin v úmyslu získat pro sebe nebo pro jiného prospěch velkého rozsahu, nebo

c) spáchá-li takový čin ve spojení s organizovanou skupinou působící ve více státech.

(5) Odnětím svobody na deset až osmnáct let nebo propadnutím majetku bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 nebo 2 smrt.

(6) Příprava je trestná.

14.2 Kuplířství, § 189 (Zákon č. 40/2009 Sb.)

(1) Kdo jiného přiměje, zjedná, najme, zláká nebo svede k provozování prostituce, nebo kdo kořistí z prostituce provozované jiným, bude potrestán odnětím svobody na šest měsíců až na čtyři léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Odnětím svobody na dvě léta až osm let bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1
a) v úmyslu získat pro sebe nebo pro jiného značný prospěch, nebo
b) jako člen organizované skupiny.

(3) Odnětím svobody na pět až dvanáct let nebo propadnutím majetku bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 těžkou újmu na zdraví.

(4) Odnětím svobody na osm až patnáct let nebo propadnutím majetku bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 smrt.

14.3 Svádění k pohlavnímu styku, § 202 (Zákon č. 40/2009 Sb.)

(1) Kdo nabídne, slíbí nebo poskytne dítěti nebo jinému za pohlavní styk s dítětem, pohlavní sebeukájení dítěte, jeho obnažování nebo jiné srovnatelné chování za účelem pohlavního uspokojení úplatu, výhodu nebo prospěch, bude potrestán odnětím svobody až na dvě léta nebo peněžitým trestem.

(2) Odnětím svobody na šest měsíců až pět let bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 na dítěti mladším patnácti let,

b) spáchá-li takový čin ze zavrženíhodné pohnutky,

c) pokračuje-li v páchání takového činu po delší dobu, nebo

d) spáchá-li takový čin opětovně.

14.4 Ohrožování výchovy dítěte, § 201 (Zákon č. 40/2009 Sb.)

(1) Kdo, byť i z nedbalosti, ohrozí rozumový, citový nebo mravní vývoj dítěte tím, že

a) svádí ho k zahálčivému nebo nemravnému životu,

b) umožní mu vést zahálčivý nebo nemravný život,

c) umožní mu opatřovat pro sebe nebo pro jiného prostředky trestnou činností nebo jiným zavrženíhodným způsobem, nebo

d) závažným způsobem poruší svou povinnost o ně pečovat nebo jinou svou důležitou povinnost vyplývající z rodičovské zodpovědnosti, bude potrestán odnětím svobody až na dvě léta.

(2) Kdo umožní, byť i z nedbalosti, dítěti hru na výherním hracím přístroji, který je vybaven technickým zařízením, které ovlivňuje výsledek hry a které poskytuje možnost peněžité výhry, bude potrestán odnětím svobody až na jeden rok, peněžitým trestem nebo zákazem činnosti.

(3) Odnětím svobody na šest měsíců až pět let bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 nebo 2 ze zavrženíhodné pohnutky,

b) pokračuje-li v páchání takového činu po delší dobu,

c) spáchá-li takový čin opětovně, nebo

d) získá-li takovým činem pro sebe nebo pro jiného značný prospěch.

14.5 Pohlavní zneužití, § 187 (Zákon č. 40/2009 Sb.)

(1) Kdo vykoná soulož s dítětem mladším patnácti let nebo kdo je jiným způsobem pohlavně zneužije, bude potrestán odnětím svobody na jeden rok až osm let.

(2) Odnětím svobody na dvě léta až deset let bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 na dítěti mladším patnácti let svěřeném jeho dozoru, zneužívaje jeho závislosti nebo svého postavení a z něho vyplývající důvěryhodnosti nebo vlivu.

(3) Odnětím svobody na pět až dvanáct let bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 těžkou újmu na zdraví.

(4) Odnětím svobody na deset až osmnáct let bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 smrt.

(5) Příprava je trestná.

14.6 Znásilnění, § 185 (Zákon č. 40/2009 Sb.)

(1) Kdo jiného násilím nebo pohrůžkou násilí nebo pohrůžkou jiné těžké újmy donutí k pohlavnímu styku, nebo kdo k takovému činu zneužije jeho bezbrannosti, bude potrestán odnětím svobody na šest měsíců až pět let.

(2) Odnětím svobody na dvě léta až deset let bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1

a) souloží nebo jiným pohlavním stykem provedeným způsobem srovnatelným se souloží,
b) na dítěti, nebo
c) se zbraní.

(3) Odnětím svobody na pět až dvanáct let bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 na dítěti mladším patnácti let,
b) spáchá-li takový čin na osobě ve výkonu vazby, trestu odnětí svobody, ochranného léčení, zabezpečovací detence, ochranné nebo ústavní výchovy anebo v jiném místě, kde je omezována osobní svoboda, nebo
c) způsobí-li takovým činem těžkou újmu na zdraví.

(4) Odnětím svobody na deset až osmnáct let bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 smrt.

(5) Příprava je trestná.

14.7 Navazování nedovolených kontaktů s dítětem, § 193b (Zákon č. 40/2009 Sb.)

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

14.8 Výroba a jiné nakládání s dětskou pornografií, § 192 (Zákon č. 40/2009 Sb.)

(1) Kdo přechovává fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě nebo osobu, jež se jeví být dítětem, bude potrestán odnětím svobody až na dva roky.

(2) Kdo vyrobí, doveze, vyveze, proveze, nabídne, činí veřejně přístupným, zprostředkuje, uvede do oběhu, prodá nebo jinak jinému opatří fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje

nebo jinak využívá dítě nebo osobu, jež se jeví být dítětem, anebo kdo kořistí z takového pornografického díla, bude potrestán odnětím svobody na šest měsíců až tři léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(3) Odnětím svobody na dvě léta až šest let nebo propadnutím majetku bude pachatel potrestán, spáchá-li čin uvedený v odstavci 2

a) jako člen organizované skupiny,

b) tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem, nebo

c) v úmyslu získat pro sebe nebo pro jiného značný prospěch.

(4) Odnětím svobody na tři léta až osm let nebo propadnutím majetku bude pachatel potrestán, spáchá-li čin uvedený v odstavci 2

a) jako člen organizované skupiny působící ve více státech, nebo

b) v úmyslu získat pro sebe nebo pro jiného prospěch velkého rozsahu.

15 Rejstřík

16 Seznam použité literatury

Albury, K., & Crawford, K. (2012). Sexting, consent and young people's ethics: Beyond Megan's Story. *Continuum: Journal of Media & Cultural Studies*, *26*(3), 463–473. Retrieved from http://www.tandfonline.com/doi/abs/10.1080/10304312.2012.665840?journalCode=ccon20

Aricak, T., Siyahhan, S., Uzunhasanoglu, A., Saribeyoglu, S., Ciplak, S., Yilmaz, N., & Memmedov, C. (2008). Cyberbullying among Turkish adolescents. *Cyberpsychology & Behavior : The Impact of the Internet, Multimedia and Virtual Reality on Behavior and Society*, *11*(3), 253–61. http://doi.org/10.1089/cpb.2007.0016

Armstrong, J. (2012). Peter Chapman posed as "Peter" on Facebook to lure Ashleigh Hall to her death. *Mirror Online*. Retrieved from http://www.mirror.co.uk/news/uk-news/peter-chapman-posed-as-peter-on-facebook-206399

Baas, N., de Jong, M. D. T., & Drossaert, C. H. C. (2013). Children's perspectives on cyberbullying: insights based on participatory research. *Cyberpsychology, Behavior and Social Networking*, *16*(4), 248–53. http://doi.org/10.1089/cyber.2012.0079

Bartoněk, J. (2011). Chatroulette vás vidí…. *Portál E-Bezpečí*. Retrieved from http://www.e-bezpeci.cz/index.php/temata/dali-rizika/313-chatroulette-vas-vidi

Bassiouni, D. H., & Hackley, C. (2014). "Generation Z" children's adaptation to digital consumer culture: A critical literature review. *Journal of Customer behaviour2*, *13*(2), 113–133.

Bauman, S. (2011). *Cyberbullying: What Counselors Need to Know*. Alexandria, VA: American Counseling Association.

Bauman, S., Toomey, R. B., & Walker, J. L. (2013). Associations among bullying, cyberbullying, and suicide in high school students. *Journal of Adolescence*, *36*(2), 341–50. http://doi.org/10.1016/j.adolescence.2012.12.001

Beard, K. W., & Wolf, E. M. (2001). Internet addiction. *Cyberpsychology & Behavior*, *4*(3), 377–382.

Beautrais, A., Collings, S., Ehrhardt, P., & Henare, K. (2005). *Suicide Prevention: a*

review of evidence of risk and protective factors, and points of effective intervention.

Belsey, B. (2004). *Cyberbullying: "Always on? Always Aware!"* Retrieved from http://www.cyberbullying.ca

Benkovič, J. (2007). Nelátkové závislosti v ambulanci praktického lekára. *Via Practica*, *4*(11), 530–533.

Benotsch, E. G., Snipes, D. J., Martin, A. M., & Bull, S. S. (2013). Sexting, substance use, and sexual risk behavior in young adults. *The Journal of Adolescent Health : Official Publication of the Society for Adolescent Medicine*, *52*(3), 307–13. http://doi.org/10.1016/j.jadohealth.2012.06.011

Beran, T., & Li, Q. (2007). The Relationship between Cyberbullying and School Bullying. *Journal of Student Wellbeing*, *1*(December), 15–33. Retrieved from http://www.ojs.unisa.edu.au/index.php/JSW/article/view/172

Berson, I. R. (2003). Grooming Cybervictims The Psychosocial Effects of Online Exploitation for Youth. *Journal of School Violence*, *2*(1), 5–18. http://doi.org/10.1300/J202v02n01_02

Bianchi, A., & Phillips, J. G. (2005). Psychological predictors of problem mobile phone use. *Cyberpsychology & Behavior : The Impact of the Internet, Multimedia and Virtual Reality on Behavior and Society*, *8*(1), 39–51. http://doi.org/10.1089/cpb.2005.8.39

Billieux, J. (2012). Problematic Use of the Mobile Phone: A Literature Review and a Pathways Model. *Current Psychiatry Reviews*, *8*(4), 299–307. http://doi.org/10.2174/157340012803520522

Billieux, J., Van Der Linden, M., & Rochat, L. (2008). The role of impulsivity in actual and problematic use of the mobile phone. *Applied Cognitive Psychology*, *22*(9), 1195–1210. http://doi.org/10.1002/acp.1429

Bishop, J. (2014). Digital Teens and the "Antisocial Network": *International Journal of E-Politics*, *5*(3), 1–15. http://doi.org/10.4018/ijep.2014070101

Bishop, J. (2015). *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance*. http://doi.org/10.4018/978-1-4666-6324-4

Black, P. J., Wollis, M., Woodworth, M., & Hancock, J. T. (2015). A linguistic analysis of grooming strategies of online child sex offenders: Implications for our understanding of predatory sexual behavior in an increasingly

computer-mediated world. *Child Abuse & Neglect*, 1–10. http://doi.org/10.1016/j.chiabu.2014.12.004

Blatníková, Š. (2009). *Pachatelé komerčního sexuálního zneužívání dětí*. Praha: Institut pro kriminologii a sociální prevenci.

Brdička, B. (2014). Výzkum počítačové a informační gramotnosti ICILS 2013. *Učitelský Spomocník*. Retrieved from http://spomocnik.rvp.cz/clanek/19347/VYZKUM-POCITACOVE-A-INFORMACNI-GRAMOTNOSTI-ICILS-2013.html

Briggs, P., Simon, W. T., & Simonsen, S. (2011). An exploratory study of Internet-initiated sexual offenses and the chat room sex offender: has the Internet enabled a new typology of sex offender? *Sexual Abuse : A Journal of Research and Treatment*, *23*(1), 72–91. http://doi.org/10.1177/1079063210384275

Brown, C. F., Demaray, M. K., & Secord, S. M. (2014). Cyber victimization in middle school and relations to social emotional outcomes. *Computers in Human Behavior*, *35*, 12–21. http://doi.org/10.1016/j.chb.2014.02.014

Burčíková, P., Kutálková, P., & Hůle, D. (2008). *Cool je-- vědět víc: ústavní výchova a rizika komerčního sexuálního zneužívání*. Praha: La Strada Česká republika. Retrieved from https://books.google.cz/books/about/Cool_je_v%C4%9Bd%C4%9Bt_v%C3%ADc.html?id=xT8iNQAACAAJ&pgis=1

Cahrtrand, T., & Bargh, J. (1999). The Chameleon Effect: The Perception-Behavior Link and Social Interaction. *Journal of Personality and Social Psychology*, *76*(6), 893–910.

Craven, S., Brown, S., & Gilchrist, E. (2006). Sexual grooming of children: Review of literature and theoretical considerations. *Journal of Sexual Aggression*, *12*(3), 287–299. http://doi.org/10.1080/13552600601069414

Curnutt, H. (2012). Flashing Your Phone: Sexting and the Remediation of Teen Sexuality. *Communication Quarterly*.

Čechová, D., & Hlistová, E. (2009). Šikanovanie cez internet. *Prevencia*, *58*(10).

Černá, A., Dědková, L., Macháčková, H., Ševčíková, A., & Šmahel, D. (2013). *Kyberšikana - průvodce novým fenoménem*. Grada Publishing, a.s.

Česká televize. (2013). Odborníci varují: Teenageři jsou největšími šiřiteli

dětské pornografie. Retrieved from http://www.ceskatelevize.cz/ct24/domaci/1116664-odbornici-varuji-teenageri-jsou-nejvetsimi-siriteli-detske-pornografie

Dahlberg, L. (2001). Computer-Mediated Communication and The Public Sphere : A Critical Analysis Introduction : Approaching the Question of the Internet and the Public Sphere, *7*(October), 1–30.

Daily Mail Online. (2008). Nomophobia is the fear of being out of mobile phone contact - and it's the plague of our 24/7 age | Daily Mail Online. Retrieved August 25, 2015, from http://www.dailymail.co.uk/news/article-550610/Nomophobia-fear-mobile-phone-contact--plague-24-7-age.html

Dake, J. A., Price, J. H., Maziarz, L., & Ward, B. (2012). Prevalence and Correlates of Sexting Behavior in Adolescents. *American Journal of Sexuality Education*.

Dehue, F., Bolman, C., Völlink, T., & Pouwelse, M. (2009). Pesten op het werk: De relatie met gezondheid en verzuim en de rol van coping. *Gedrag En Organisatie*, *22*(2), 97–117.

DeLamater, J., & Friedrich, W. N. (2002). Human sexual development. *Journal of Sex Research*, *39*(1), 10–4. http://doi.org/10.1080/00224490209552113

Ditch The Label. (2013). *The Annual Cyberbullying Survey*.

Dixit, S., Shukla, H., Bhagwat, A., Bindal, A., Goyal, A., Zaidi, A. K., & Shrivastava, A. (2010). A study to evaluate mobile phone dependence among students of a medical college and associated hospital of central India. *Indian Journal of Community Medicine : Official Publication of Indian Association of Preventive & Social Medicine*, *35*(2), 339–41. http://doi.org/10.4103/0970-0218.66878

Dombrowski, S. C., Ahia, C. E., & McQuillan, K. (2003). Protecting Children through Mandated Child-Abuse Reporting. *The Educational Forum*, *67*(2), 119–128. http://doi.org/10.1080/00131720308984549

Donath, J. (1999). Idenity and deception in the virtual community. *Communities in Cyberspace*, 29–59.

Döring, N. (2012). Erotischer Fotoaustausch unter Jugendlichen: Verbreitung, Funktionen und Folgen des Sexting. *Zeitschrift für Sexualforschung*, *25*(01), 4–25. http://doi.org/10.1055/s-0031-1283941

Dunovský, J. (2005). *Problematika dětských práv a komerčního sexuálního zneužívání dětí u nás a ve světě*. Praha: Grada Publishing, a.s.

Dunovský, J., Dytrych, Z., & Matějček, Z. (1995). *Týrané , zneužívané a zanedbávané dítě*. Grada Publishing, a.s.

Englander, E. (2008). Cyberbullying & Bullying in Massachusetts : Frequency & Motivations, (2008), 1–14. Retrieved from http://vc.bridgew.edu/marc_pubs/10/

Faris, R., & Felmlee, D. (2011). Status Struggles: Network Centrality and Gender Segregation in Same- and Cross-Gender Aggression. *American Sociological Review*, *76*(1), 48–73. http://doi.org/10.1177/0003122410396196

Fenichel, M. (2009). Facebook Addiction Disorder (FAD). Retrieved from http://www.fenichel.com/facebook/

Finkelhor, D. (2011). Crimes against Children Research Center • www.unh.edu/ccrc, (January).

Fraillon, J., Ainley, J., Schulz, W., Friedman, T., & Gebhardt, E. (2014). *Preparing for Life in a Digital Age: the IEA International Computer and Information Literacy Study International Report*. Retrieved from http://research.acer.edu.au/ict_literacy/8

Funston, A., & MacNeill, K. (1999). *Mobile Matters: Young People and Mobile Phones*. Retrieved from https://books.google.cz/books/about/Mobile_Matters.html?id=RTnqAAAACAAJ&pgis=1

Get Safe Online. (2015). Webcam Trolling | Get Safe Online. Retrieved April 10, 2015, from https://www.getsafeonline.org/social-networking/webcam-blackmail/

Gordon-Messer, D., Bauermeister, J. A., Grodzinski, A., & Zimmerman, M. (2013). Sexting among young adults. *Journal of Adolescent Health*, *52*(3), 301–306.

Gradinger, P., Strohmeier, D., & Spiel, C. (2010). Traditional Bullying and Cyberbullying. *Zeitschrift Für Psychologie / Journal of Psychology*, *217*(4), 205–213. http://doi.org/10.1027/0044-3409.217.4.205

Gregorine, C. (2015). This Scientific Test Will Tell You How Addicted You Are To Your Smartphone. *The Huffington Post*. Retrieved from http://www.huffingtonpost.com/2015/05/18/nomophobia-smartphone-

sep_n_7266468.html

Griffiths, M. (1998). Internet Addiction: Does It Really Exist? *Psychology and the Internet: Intrapersonal, Interpersonal, and Transpersonal Implications*.

Gupta, A., Kumaraguru, P., & Sureka, A. (2012). Characterizing Pedophile Conversations on the Internet using Online Grooming. *Eprint arXiv:1208.4324*. Retrieved from http://arxiv.org/abs/1208.4324

Hanušová, J. (2006). *Sexuální zneužívání*.

Hardaker, C. (2010). Trolling in asynchronous computer-mediated communication: From user discussions to academic definitions. *Journal of Politeness Research*, *6*(2), 215–242. http://doi.org/10.1515/JPLR.2010.011

Herring, S., Job-Sluder, K., Scheckler, R., & Barab, S. (2002). Searching for Safety Online: Managing "Trolling" in a Feminist Forum. *The Information Society*. http://doi.org/10.1080/01972240290108186

Hinduja, S., & Patchin, J. W. (2008). Cyberbullying: An Exploratory Analysis of Factors Related to Offending and Victimization. *Deviant Behavior*, *29*(2), 129–156. http://doi.org/10.1080/01639620701457816

Hinduja, S., & Patchin, J. W. (2010). Cyberbullying and Suicide. *Archives of Suicide Research*, *14*(3).

Hlaváč, J. (2015). Netolismus. Virtuální závislost, nebo závislost na virtuálnu? *Prevence*, (3), 6–8.

Hollá, K. (2013). Cyber bullying – inappropriate adolescent behaviour in the 21. *Journal of Interdisciplinary Research*, 40–44.

Hollá, K. (2015). Cyberbullying in Slovak Republic - The Analysis of Variance of Main Effects. *Slavonic Pedagogical Studies Journal*, *4*(2). http://doi.org/10.18355/PG.2015.4.2.136-146

Horovitz, B. (2012). After Gen X, Millennials, what should the next generation be called? Retrieved September 21, 2015, from http://usatoday30.usatoday.com/money/advertising/story/2012-05-03/naming-the-next-generation/54737518/1

Hwang, S. (2008). Utilizing Qualitative Data Analysis Software A Review of Atlas.ti. *Social Science Computer Review*, *11*(26 (4)), 519–527.

http://doi.org/10.1177/0894439307312485

Child Exploitation and Online Protection Centre. (2013). *Threat Assessment of Child Sexual Exploitation and Abuse*.

Chráska, M., Kopecký, K., Krejčí, V., & Szotkowski, R. (2012). Is a victim also and attacker? Research of cyberbullying at Czech pupils and students in the whole Czech Republic 1. *Journal of Technology and Information Education*, *4*(1), 75–79.

Chudý, Š., & Neumeister, P. (2014). *Začínajúci učiteľ a zvládanie disciplíny v kontexte 2. st. ZŠ*. Brno: Paido.

Igarashi, T., Motoyoshi, T., Takai, J., & Yoshida, T. (2008). No mobile, no life: Self-perception and text-message dependency among Japanese high school students. *Computers in Human Behavior*, *24*(5), 2311–2324. http://doi.org/10.1016/j.chb.2007.12.001

James, D., & Drennan, J. (2005). Exploring Addictive Consumption of Mobile Phone Technology. *Australian and New Zealand Marketing Academy Conference: Electronic Marketing*, (September), 87–96. Retrieved from http://anzmac.info/conference/2005/cd-site/pdfs/12-Electronic-Marketing/12-James.pdf

Ježková, Z., & Fraňková, A. (2012). Mýty a fakta o sexuálním zneužívání dětí - Šance Dětem. Retrieved September 17, 2015, from http://www.sancedetem.cz/srv/www/content/pub/cs/clanky/myty-a-fakta-o-sexualnim-zneuzivani-deti-63.html#co-je-sexualni-zneuzivani

Jolicoeur, M., & Zedlewski, E. (2010). *Much ado about sexting*. [S.l.]: National Institute of Justice.

Juvonen, J., & Gross, E. F. (2008). Extending the school grounds? - Bullying experiences in cyberspace. *Journal of School Health*, *78*(9), 496–505. http://doi.org/10.1111/j.1746-1561.2008.00335.x

Katz, C. (2013). Internet-related child sexual abuse: What children tell us in their testimonies. *Children and Youth Services Review*, *35*(9), 1536–1542. http://doi.org/10.1016/j.childyouth.2013.06.006

King, A. L. S., Valença, A. M., Silva, A. C. O., Baczynski, T., Carvalho, M. R., & Nardi, a. E. (2013). Nomophobia: Dependency on virtual environments or social phobia? *Computers in Human Behavior*, *29*(1), 140–144.

http://doi.org/10.1016/j.chb.2012.07.025

King, A. L. S., Valença, A. M., Silva, A. C., Sancassiani, F., Machado, S., & Nardi, A. E. (2014). "Nomophobia": impact of cell phone use interfering with symptoms and emotions of individuals with panic disorder compared with a control group. *Clinical Practice and Epidemiology in Mental Health : CP & EMH*, *10*(August 2015), 28–35. http://doi.org/10.2174/1745017901410010028

Kloess, J. A., Beech, A. R., & Harkins, L. (2014). Online child sexual exploitation: prevalence, process, and offender characteristics. *Trauma, Violence & Abuse*, *15*(2), 126–39. http://doi.org/10.1177/1524838013511543

Knoll, J. (2010). Teacher sexual misconduct: grooming patterns and female offenders. *Journal of Child Sexual Abuse*, *19*(4), 371–86. http://doi.org/10.1080/10538712.2010.495047

Kolář, M. (2011). *Nová cesta k léčbě šikany*. Portál.

König, A., Gollwitzer, M., & Steffgen, G. (2010). Cyberbullying as an Act of Revenge? *Australian Journal of Guidance and Counselling*, *20*(2), 210–244. http://doi.org/10.1375/ajgc.20.2.210

Kopecký, K. (2009, May). Kybergrooming aneb Kdo loví v chatu. *Česká škola*. Retrieved from http://www.ceskaskola.cz/2009/05/kamil-kopecky-kybergrooming-aneb-kdo.html

Kopecký, K. (2010). *Cyber Grooming, Danger of Cyberspace* (1st ed.). Olomouc: Net University Ltd.

Kopecký, K. (2011). Úvod do problematiky netolismu. Retrieved May 17, 2015, from http://www.e-bezpeci.cz/index.php/temata/dali-rizika/331-uvod-do-problematiky-netolismu

Kopecký, K. (2012a). K pozitivním vlivům hraní World of Warcraft. Retrieved May 17, 2015, from http://www.e-bezpeci.cz/index.php/temata/dali-rizika/517-pozitivawow

Kopecký, K. (2012b). Sexting among Czech preadolescents and adolescents. *New Educational Review*, *28*(2), 39–48. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84864819528&partnerID=tZOtx3y1

Kopecký, K. (2013a). Komentář - Lidské hyeny a Facebook. *Portál E-Bezpečí*.

Retrieved from http://www.e-bezpeci.cz/index.php/temata/socialni-sit/634-komenta-lidske-hyeny-a-facebook

Kopecký, K. (2013b). Podvodné mobilní platby na Facebooku. Retrieved from http://www.e-bezpeci.cz/index.php/temata/sociotechnika/774-podvodne-platby-na-facebooku

Kopecký, K. (2013c). Podvody s falešnými webkamerami řádí i v ČR. *Portál E-Bezpečí*. Retrieved from http://www.e-bezpeci.cz/index.php/temata/sociotechnika/637-podvody-s-falesnymi-webkamerami

Kopecký, K. (2014a). *Risky Behaviour of Students of Faculty of Education of Palacký University Olomouc within the Internet Environment* (1st ed.). Palacký University Olomouc.

Kopecký, K. (2014b). Stručný úvod do problematiky online vydírání českých dětí se zaměřením na tzv. sextortion. *Pediatrie pro Praxi*, *15*(6), 352–354. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84924623453&partnerID=tZOtx3y1

Kopecký, K. (2015a). Digitální rodičovství - starý koncept v novém kabátě. *Portál E-Bezpečí*. Retrieved from http://www.e-bezpeci.cz/index.php/rodice-ucitele-zaci/1012-digitalni-rodicovstvi

Kopecký, K. (2015b). Útoky na účty elektronického bankovnictvím neustávají ani v novém roce. Retrieved May 17, 2015, from http://www.e-bezpeci.cz/index.php/temata/sociotechnika/954-phishing-2014

Kopecký, K. (2016). Misuse of web cameras to manipulate children within the so-called webcam trolling. *Telematics and Informatics*, *33*(1), 1–7. http://doi.org/10.1016/j.tele.2015.06.005

Kopecký, K., & Kožíšek, M. (2013). *Podvody s webkamerami - webcam trolling*. Retrieved from http://www.slideshare.net/kopeckyk/podvody-s-webkamerami-webcam-trolling

Kopecký, K., & Szotkowski, R. (2014). Formal and Semantic Analysis of Computer Passwords of Czech Internet Users. In *EDULEARN14 Proceedings* (pp. 2794–2798). IATED. Retrieved from http://library.iated.org/view/KOPECKY2014FOR

Kopecký, K., Szotkowski, R., & Krejčí, V. (2012). *Nebezpečí internetové*

komunikace 3. Olomouc: Univerzita Palackého v Olomouci.

Kopecký, K., Szotkowski, R., & Krejčí, V. (2014a). *Nebezpečí internetové komunikace IV*. Olomouc: Univerzita Palackého v Olomouci.

Kopecký, K., Szotkowski, R., & Krejčí, V. (2014b). *Risks of Internet Communication IV* (1st ed.). Olomouc: Palacký University Olomouc. Retrieved from http://www.e-bezpeci.cz/index.php/ke-stazeni/doc_download/60-risks-of-internet-communication-iv

Kopecký, K., Szotkowski, R., & Krejčí, V. (2014c). *Výzkum rizikového chování slovenských a českých dětí v prostředí internetu 2014*. Olomouc. Retrieved from http://www.e-bezpeci.cz/index.php/tiskove-zpravy/914-sedm-z-deseti

Kováčová. (2012). *Kyberšikanovanie ako novodobý fenomén u žiakov stredných škôl – jeho výskyt a prevencia*. Banská Bystrica: Univerzita Matěje Béla.

Kovářová, V., & Kopecký, K. (2012). Fenomén - disinhibiční efekt. *Portál E-Bezpečí2*. Retrieved from http://www.e-bezpeci.cz/index.php/temata/dali-rizika/485-fenomen-disinhibini-efekt#_edn3

Kowalski, R. M., Limber, S. P., & Agatston, P. W. (2008). *Cyber Bullying: Bullying in the Digital Age*. Wiley-Blackwell. Retrieved from http://eu.wiley.com/WileyCDA/WileyTitle/productCd-0470693347.html

Kožíšek, M. (2014). Když se děti samy nabízejí. Praha: Seznam.cz. Retrieved from http://slideplayer.cz/slide/1984236/

Kožíšek, M. (2015). *Aktuální trendy v sociálním inženýrství*. Praha.

Krejčí, V. (2010). *Kyberšikana – kybernetická šikana* (1st ed.). Olomouc: Net University Ltd.

Kusá, J., & Adámek, L. (2013). Zdeněk Svěrák obětí trollingu. *Portál E-Bezpečí*. Retrieved from http://www.e-bezpeci.cz/index.php/temata/socialni-sit/782-zdenk-svrak-obti-trollingu

Langos, C. (2010). Internet trolling case sparks calls for an Online Ombudsman to handle social network user complaints relating to Internet content — what of the idea. *Internet Law Bulletin*, (September), 82–87.

Lanning, K. V. (2002). Sex offender continuum (Adapted from Chapter Four

Cyber “Pwdophiles”: A Behavioral Perspective). *Prosecuting Online Child Exploitation Cases*.

Lenhart, A., Purcell, K., Smith, A., & Zickuhr, K. (2010). Social media & mobile internet use among teens and young adults. *Pew Internet & American Life Project. Retrieved February*, *5*, 2010.

Lippman, J. R., & Campbell, S. W. (2014). Damned if you do, damned if you don’t…if you're a girl: Relational and normative contexts of adolescent sexting in the United States. *Journal of Children and Media*, 1–16. Retrieved from http://dx.doi.org/10.1080/17482798.2014.923009

Mak, K.-K., Lai, C.-M., Ko, C.-H., Chou, C., Kim, D.-I., Watanabe, H., & Ho, R. C. M. (2014). Psychometric properties of the Revised Chen Internet Addiction Scale (CIAS-R) in Chinese adolescents. *Journal of Abnormal Child Psychology*, *42*(7), 1237–45. http://doi.org/10.1007/s10802-014-9851-3

Mak, K.-K., Lai, C.-M., Watanabe, H., Kim, D.-I., Bahar, N., Ramos, M., … Cheng, C. (2014). Epidemiology of internet behaviors and addiction among adolescents in six Asian countries. *Cyberpsychology, Behavior and Social Networking*, *17*(11), 720–8. http://doi.org/10.1089/cyber.2014.0139

Maslow, A. H. (1943). A theory of human motivation. *Psychological Review*, *4*(50), 370–396. Retrieved from http://psychclassics.yorku.ca/Maslow/motivation.htm

McCosker, a. (2013). Trolling as provocation: YouTube’s agonistic publics. *Convergence: The International Journal of Research into New Media Technologies*, *20*(2), 1354856513501413–. http://doi.org/10.1177/1354856513501413

McGhee, I., Bayzick, J., Kontostathis, A., Edwards, L., McBride, A., & Jakubowski, E. (2011). Learning to Identify Internet Sexual Predation. *International Journal of Electronic Commerce*, *15*(3), 103–122. http://doi.org/10.2753/JEC1086-4415150305

Milfait, R. (2015). Komerční sexuální zneužívání dětí a dospívajících v číslech. Retrieved from http://www.sancedetem.cz/cs/hledam-pomoc/rodina-v-problemove-situaci/rizikove-chovani-dospeleho-k-diteti/komercni-sexualni-zneuzivani-deti-a-dospivajicich/komercni-sexualni-zneuzivani-deti-a-dospivajicich-v-cislech.shtml

Ministerstvo školství, mládeže a tělovýchovy. (2013). *Národní strategie*

primární prevence rizikového chování dětí a mládeže na období 2013-2018. Praha.

Miovský, M., Skácelová, L., Zapletalová, J., & Novák, P. (2010). *Primární prevence rizikového chování ve školství*. (M. Miovský, L. Skácelová, J. Zapletalová, & P. Novák, Eds.). Sdružení SCAN.

Mitchell, K. J. (2001). Risk Factors for and Impact of Online Sexual Solicitation of Youth. *JAMA*, *285*(23), 3011. http://doi.org/10.1001/jama.285.23.3011

Mitchell, K. J., Finkelhor, D., Jones, L. M., & Wolak, J. (2010). Growth and change in undercover online child exploitation investigations, 2000–2006. *Policing and Society*, *20*(4), 416–431. http://doi.org/10.1080/10439463.2010.523113

MŠMT. (2005). *Standardy odborné způsobilosti poskytovatelů programů primární prevence užívání návykových látek*. Praha.

MŠMT. (2013). Přímé a nepřímé varovné signály šikanování. *Věstník MŠMT*, *69*(8).

Murthy, R. (2012). Nomophobia strikes Indian phone addicts. *Asia Times*. Retrieved from http://www.atimes.com/atimes/South_Asia/NC27Df02.html

National Center for Education Statistics. (2012). *Indicators of School Crime and Safety: 2012*. Retrieved from http://nces.ed.gov/programs/crimeindicators/crimeindicators2012/

Nešpor, K., & Csémy, L. (n.d.). Zdravotní rizika počítačových her a videoher.

O'Connell, R. (2003). Typology of Cybersexploitation and on-Line Grooming Practices. *Director*, 1–22. Retrieved from http://www.jisc.ac.uk/uploaded_documents/lis_PaperJPrice.pdf

Obama, B. (2011). Obama Administration Holds Anti-Bullying Conference. Retrieved from http://www.civilrights.org/archives/2011/03/1170-bullying.html

Olson, L. N., Daggs, J. L., Ellevold, B. L., & Rogers, T. K. K. (2007). Entrapping the Innocent: Toward a Theory of Child Sexual Predators? Luring Communication. *Communication Theory*, *17*(3), 231–251. http://doi.org/10.1111/j.1468-2885.2007.00294.x

Olweus, D. (1993). *Bullying at school. Knowledge base and an effective intervention program*. Blackwell Publishing.

Ortega, R., Calmaestra, J., & Mechrán, M. y J. (2008). Cyberbullying. *International Journal of Psychology and Psychological Therapy*, *8*(2), 183–192. http://doi.org/10.1001/jamapediatrics.2013.3343

OSN. (1989). Úmluva o právech dítěte. Retrieved from http://www.osn.cz/wp-content/uploads/2015/03/umluva-o-pravech-ditete.pdf

Ospina, M., Harstall, C., & Dennett, L. (2010). *Sexual Exploitation of Children and Youth Over the Internet : A Rapid Review of the Scientific Literature*. Alberta, Canada.

Patchin, J. W., & Hinduja, S. (2012). *Preventing and responding to cyberbullying: Expert perspectives*. Thousand Oaks: Routledge.

Penna, L., Clark, A., & Mohay, G. (2005). Challenges of automating the detection of paedophile activity on the internet. *Proceedings - First International Workshop on Systematic Approaches to Digital Forensic Engineering*, *2005*, 206–220. http://doi.org/10.1109/SADFE.2005.4

Perry, D. G., Kusel, S. J., & Perry, L. C. (1988). Victims of peer aggression. *Developmental Psychology*, *24*(6), 807–814.

Phillips, W. (2011). LOLing at tragedy: Facebook trolls, memorial pages and resistance to grief online. *First Monday*, *16*(12). http://doi.org/10.5210/fm.v16i12.3168

Porter, D. (1997). *Internet Culture* (1st ed.). Routledge. Retrieved from http://books.google.cz/books/about/Internet_Culture.html?id=3RPHmoHlRXkC&pgis=1

Riebel, J., Jäger, R. S. R. S., & Fischer, U. C. U. (2009). Cyberbullying in Germany–an exploration of prevalence, overlapping with real life bullying and coping strategies. *Psychology Science Quarterly*, *51*(3), 298–314. http://doi.org/10.1089/109493104323024500

Rigby, K. (1997). *Bullying in schools - and what to do about it.* ACER.

Ringdal, N. J. (2000). *Nejtěžší povolání světa*. Brno: Doplněk.

Ringrose, J., Gill, R., Livingstone, S., & Harvey, L. (2012). A qualitative study of children, young people and "sexting": a report prepared for the NSPCC.

Methodology. Retrieved from http://eprints.lse.ac.uk/44216/

Sabella, R. a, Patchin, J. W., & Hinduja, S. (2013). Cyberbullying myths and realities. *Computers in Human Behavior*, *29*, 2703–2711. http://doi.org/10.1016/j.chb.2013.06.040

Sadhu, J. M. (2012). Sexting: The impact of a cultural phenomenon on psychiatric practice. *Academic Psychiatry*, *36*(1), 76–81.

Sanders, J., Smith, P. K., & Cillessen, A. (2009). Cyberbullies: Their motives, characteristics, and types of bullying. *XIVth European Conference of Developmental Psychology*. Vilnius, Lithuania.

Sex and Tech: Results from a Survey of Teens and Young Adults. (2008).

Shachaf, P., & Hara, N. (2010). Beyond vandalism: Wikipedia trolls. *Journal of Information Science*, *36*(3), 357–370. http://doi.org/10.1177/0165551510365390

Shapira, N. a., Goldsmith, T. D., Keck, P. E., Khosla, U. M., & McElroy, S. L. (2000). Psychiatric features of individuals with problematic internet use. *Journal of Affective Disorders*, *57*(1-3), 267–272. http://doi.org/10.1016/S0165-0327(99)00107-X

Shariff, S. (2008). *Cyber-Bullying: Issues and Solutions for the School, the Classroom and the Home*. Retrieved from https://books.google.com/books?hl=cs&lr=&id=qqwHcNLVDwUC&pgis=1

Shaw, M., & Black, D. W. (2008). Internet Addiction. *CNS Drugs*, *22*(5), 353–365.

Schwartz, M. (2008). The Trolls Among Us. *The Times Magazine*. Retrieved from http://www.nytimes.com/2008/08/03/magazine/03trolls-t.html?pagewanted=all&_r=0

Skapinakis, P., Bellos, S., Gkatsa, T., Magklara, K., Lewis, G., Araya, R., … Mavreas, V. (2011). The association between bullying and early stages of suicidal ideation in late adolescents in Greece. *BMC Psychiatry*, *11*(1), 22. http://doi.org/10.1186/1471-244X-11-22

Skoupá, A. (2015, October 6). České děti jsou čím dál závislejší na počítačových hrách. Vina je však na straně rodičů. *Hospodářské Noviny*. Praha. Retrieved from http://life.ihned.cz/zdravi/c1-64710810-ceske-deti-jsou-cim-dal-zavislejsi-na-pocitacovych-hrach-vina-je-vsak-na-strane-rodicu

Slonje, R., & Smith, P. K. (2008). Cyberbullying: another main type of bullying? *Scandinavian Journal of Psychology*, *49*(2), 147–54. http://doi.org/10.1111/j.1467-9450.2007.00611.x

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry, and Allied Disciplines*, *49*(4), 376–85. http://doi.org/10.1111/j.1469-7610.2007.01846.x

Smith, P. K., & Sharp, S. (1994). *School Bullying: Insights and Perspectives*. Routledge.

Statista.com. (2015). Number of World of Warcraft subscribers from 1st quarter 2005 to 1st quarter 2015 (in millions). Retrieved May 17, 2015, from http://www.statista.com/statistics/276601/number-of-world-of-warcraft-subscribers-by-quarter/

Stokes, P. (2010). Peter Chapman targeted thousands of young girls. Retrieved April 10, 2015, from http://www.telegraph.co.uk/news/uknews/crime/7397894/Peter-Chapman-targeted-thousands-of-young-girls.html

Strasburger, V. C., Jordan, A. B., & Donnerstein, E. (2012). Children, Adolescents, and the Media:. Health Effects. *Pediatric Clinics of North America*, *59*(3), 533–587. http://doi.org/10.1016/j.pcl.2012.03.025

Streichman, J. (2011). What is sexting? Retrieved from http://www.examiner.com

Suler, J. (2004). The online disinhibition effect. *Cyberpsychology & Behavior : The Impact of the Internet, Multimedia and Virtual Reality on Behavior and Society*, *7*(3), 321–326. http://doi.org/10.1089/1094931041291295

Sullivan, J., & Beech, A. (2002). Professional perpetrators: sex offenders who use their employment to target and sexually abuse the children with whom they work. *Child Abuse Review*, *11*(3), 153–167. http://doi.org/10.1002/car.737

Sullivan, K., Cleary, M., & Sullivan, G. (2004). *Bullying in Secondary Schools What It Looks Like and How To Manage It*. Paul Chapman Publishing. Retrieved from http://www.uk.sagepub.com/books/Book225571

Summers, A. (2011). Facebook Addiction Disorder — The 6 Symptoms of F.A.D.

Retrieved from http://www.adweek.com/socialtimes/facebook-addiction-disorder-the-6-symptoms-of-f-a-d/61408

Sutton, J., Smith, P., & Swettenham, J. (1999). Social cognition and bullying: Social inadequacy or skilled manipulation?, 435–450. http://doi.org/10.1348/026151099165384

Šmahaj, J. (2014). *Kyberšikana jako společenský problém*. Olomouc: Vydavatelství Univerzity Palackého.

Tickle, L. (2012). How police investigators are catching paedophiles online | Social Care Network | The Guardian. *The Guardian*. Retrieved from http://www.theguardian.com/social-care-network/2012/aug/22/police-investigators-catching-paedophiles-online

Toda, M., Monden, K., Kubo, K., & Morimoto, K. (2004). Cellular phone dependence tendency of female university students. *Nihon Eiseigaku Zasshi. Japanese Journal of Hygiene*, *59*(4), 383–6. Retrieved from http://www.ncbi.nlm.nih.gov/pubmed/15626025

Tomková, J. (2010). *Slovakia national perspectives report for EU Kids Online III. Network*. Retrieved from http://www.zodpovedne.sk/download/SLOVAKIA_NationalPerpectivesReport.pdf

Trestní zákoník. Předpis č. 40/2009. (2009). Retrieved from http://zakony.kurzy.cz/40-2009-trestni-zakonik/

Tsitsika, A. K., Janikian, M., Mavromati, F., Tzavela, E., & Consortium, the E. N. A. (2012). *Research on Internet Addictive Behaviours among European Adolescents*. Retrieved from http://www.eunetadb.eu/files/docs/FinalResearchInternet.pdf

Van Ouytsel, J., Walrave, M., & Van Gool, E. (2014). Sexting: Between Thrill and Fear—How Schools Can Respond. *Clearing House*, *87*(5), 204–212. http://doi.org/10.1080/00098655.2014.918532

Vandebosch, H., & Van Cleemput, K. (2009). Cyberbullying among youngsters: profiles of bullies and victims. *New Media & Society*, *11*(8), 1349–1371. http://doi.org/10.1177/1461444809341263

Vaníčková, E. (2007a). *Dětská prostituce*. Praha: Grada Publishing, a.s.

Vaníčková, E. (2007b). *Identifikace typů dětských obětí komerčního sexuálního*

zneužívání dětí. Praha: Univerzita Karlova v Praze.

Vaníčková, E., Hadj-Moussová, Z., & Provazníková, H. (1995). *Násilí v rodině : Syndrom zneužívaného a zanedbávaného dítěte*. Praha: Karolinum. Retrieved from http://katalog.kfbz.cz/documents/1842?locale=cs

Vybíral, Z. (2002). Výzkum disinhibice u mladých uživatelů chatu. In I. Plaňava & M. Pilát (Eds.), *Děti, mládež a rodiny* (pp. 275–288). Brno: Barrister&Principal.

Vybíral, Z. (2005). *Psychologie komunikace*. Portál.

Wachs, S., Wolf, K. D., & Pan, C.-C. (2012). Cybergrooming: risk factors, coping strategies and associations with cyberbullying. *Psicothema*, *24*(4), 628–33. Retrieved from http://www.ncbi.nlm.nih.gov/pubmed/23079362

Walker, S., Sanci, L., & Temple-Smith, M. (2013). Sexting: Young women's and men's views on its nature and origins. *Journal of Adolescent Health*, *52*(6), 697–701.

Wallace, P. (2001). *The Psychology of the Internet*. Cambridge University Press. Retrieved from http://www.cambridge.org/us/academic/subjects/psychology/applied-psychology/psychology-internet

Wallerová, R., & Vokáč, M. (2009). Děti na internetu riskují, své fotky posílají pedofilům za kredit do mobilu. *iDNES.cz*. Retrieved from http://zpravy.idnes.cz/deti-na-internetu-riskuji-sve-fotky-posilaji-pedofilum-za-kredit-do-mobilu-1ul-/domaci.aspx?c=A091122_195910_domaci_vel

Webster, S., Davidson, J., Bifulco, A., Caretti, V., Pham, T., Grove-hills, J., … Craparo, G. (2012). *Final Report –European Online Grooming Project*. Retrieved from https://www.researchgate.net/publication/257941820_European_Online_Grooming_Project_-_Final_Report

Weiss, P. (2002). *Sexuální deviace*. Praha.

Weiss, P., & Zvěřina, J. (2008). Sexuální zneužívání v České republice - Výsledky národního výzkumu.

West, J. H., Lister, C. E., Hall, P. C., Crookston, B. T., Snow, P. R., Zvietcovich, M. E., & West, R. P. (2014). Sexting among Peruvian adolescents. *BMC Public*

Health, *14*(1), 811. http://doi.org/10.1186/1471-2458-14-811

Whitney, I., & Smith, P. K. (1993). A survey of the nature and extent of bullying in junior/middle and secondary schools. *Educational Research*, *35*(1), 3–25. http://doi.org/10.1080/0013188930350101

Whittle, H., Hamilton-Giachritsis, C., & Beech, A. (2014). "Under His Spell": Victims' Perspectives of Being Groomed Online. *Social Sciences*, *3*(3), 404–426. http://doi.org/10.3390/socsci3030404

Whittle, H., Hamilton-Giachritsis, C., Beech, A., & Collings, G. (2013). A review of online grooming: Characteristics and concerns. *Aggression and Violent Behavior*, *18*(1), 62–70. http://doi.org/10.1016/j.avb.2012.09.003

WHO. (2015). WHO | Lexicon of alcohol and drug terms published by the World Health Organization. Retrieved May 17, 2015, from http://www.who.int/substance_abuse/terminology/who_lexicon/en/

Willard, N. (2007a). *Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress* (1st ed.). Champaign, IL: Research Press.

Willard, N. (2007b). *Educator ' s Guide to Cyberbullying and Cyberthreats* (1st ed.). Center for Safe and Responsible Use of the Internet.

Wilson, C. (2011). Online "Sextortion" Of Teens On The Rise: Feds. *Huffington Post*. Retrieved from http://www.huffingtonpost.com/2010/08/14/online-sextortion-of-teen_n_682246.html

Wolak, J., Finkelhor, D., & Mitchell, K. (2004). Internet-initiated sex crimes against minors: Implications for prevention based on findings from a national study. *Journal of Adolescent Health*, *35*(5), 424.e11–424.e20. http://doi.org/10.1016/j.jadohealth.2004.05.006

Wolak, J., Finkelhor, D., & Mitchell, K. J. (2012). How Often Are Teens Arrested for Sexting? Data From a National Sample of Police Cases. *PEDIATRICS*. http://doi.org/10.1542/peds.2011-2242

Wolak, J., Finkelhor, D., Mitchell, K. J., & Ybarra, M. L. (2008). Online "predators" and their victims: myths, realities, and implications for prevention and treatment. *The American Psychologist*, *63*(2), 111–128. http://doi.org/10.1037/2152-0828.1.S.13

Xing, X., Dang, J., Han, R., Liu, X., & Mishra, S. (2010). Intrusions into Privacy in Video Chat Environments: Attacks and Countermeasures, (July), 8. Retrieved from http://arxiv.org/abs/1007.1473

Ybarra, M. L. (2004). Linkages between depressive symptomatology and Internet harassment among young regular Internet users. *Cyberpsychology & Behavior : The Impact of the Internet, Multimedia and Virtual Reality on Behavior and Society*, *7*(2), 247–57. http://doi.org/10.1089/109493104323024500

Ybarra, M. L., Boyd, D., Korchmaros, J. D., & Oppenheim, J. K. (2012). Defining and measuring cyberbullying within the larger context of bullying victimization. *The Journal of Adolescent Health : Official Publication of the Society for Adolescent Medicine*, *51*(1), 53–8. http://doi.org/10.1016/j.jadohealth.2011.12.031

Ybarra, M. L., & Mitchell, K. J. (2004). Online aggressor/targets, aggressors, and targets: a comparison of associated youth characteristics. *Journal of Child Psychology and Psychiatry, and Allied Disciplines*, *45*(7), 1308–16. http://doi.org/10.1111/j.1469-7610.2004.00328.x

Ybarra, M. L., & Mitchell, K. J. (2014). "Sexting" and its relation to sexual activity and sexual risk behavior in a national survey of adolescents. *The Journal of Adolescent Health : Official Publication of the Society for Adolescent Medicine*, *55*(6), 757–64. http://doi.org/10.1016/j.jadohealth.2014.07.012

Yildirim, C., & Correia, A.-P. (2015). Exploring the dimensions of nomophobia: Development and validation of a self-reported questionnaire. *Computers in Human Behavior*, *49*, 130–137. http://doi.org/10.1016/j.chb.2015.02.059

Yildirim, C., Sumuer, E., Adnan, M., & Yildirim, S. (2015). A growing fear: Prevalence of nomophobia among Turkish college students. *Information Development*, (AUGUST), 0–10. http://doi.org/10.1177/0266666915599025

Young, K. S. (2004). Internet Addiction: A New Clinical Phenomenon and Its Consequences. *American Behavioral Scientist*, *48*(4), 402–415. http://doi.org/10.1177/0002764204270278

Young, K. S. (2008). *Assessment of Internet addiction*. *The Center for Internet Addiction Recovery.* Retrieved from http://www.icsao.org/fileadmin/Divers_papiers/KYoung-

internetaddiction5.pdf

Žák, K. (2009). *Pedofilie*. Masarykova Univerzita v Brně.

Žák, K. (2012). *Život a pocity nekriminálních pedofilů*. Masarykova Univerzita v Brně.

17 Anotace

Publikace *Rizikové formy chování českých a slovenských dětí v prostředí internetu* je moderní studií rizikových fenoménů spojených s interpersonálními útoky v kyberprostoru. V úvodních částech publikace shrnuje základní poznatky o vybraných rizikových jevech – kyberšikaně, kybergroomingu, sextingu a rizikovém chování v prostředí sociálních sítí. V dalších částech se již věnuje výsledkům vybraných výzkumných studií, které se na jednotlivé fenomény orientují.

Publikace *Rizikové formy chování českých a slovenských dětí v prostředí internetu* shrnuje výsledky tří výzkumů, realizovaných Centrem prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci v průběhu let 2014 a 2015. Konkrétně jde o výzkumy *Nebezpečí internetové komunikace 5* a *Rizikové chování slovenských dětí v prostředí internetu*, které se orientují na prevalenci rizikového chování spojeného s rizikovými formami komunikace v dětské populaci, a o studii *Analýza komunikace českých dětí a online predátorů*, která zkoumala, jaké komunikační strategie volí internetoví predátoři v rámci online útoků.

Další část se orientuje na netolismus a jeho různé druhy, zabývá se rovněž riziky spojenými s dětskou prostitucí a orientuje se také na další související fenomény.

Závěrečná část publikace je věnovaná zejména primární prevenci rizikového chování v prostředí internetu, popisuje základní preventivní strategie, zaměřuje se také na zkušenosti z realizace primární prevence v prostředí základních a středních škol.

Klíčová slova: *kyberšikana, kybergrooming, sexting, netolismus, rizika sociálních sítí, webcam trolling, dětská prostituce, primární prevence rizikového chování, výzkum.*

18 Annotation

Publications *Risky behaviour of Czech and Slovak children in the Internet environment* is an advanced study of risky phenomena associated with interpersonal attacks in cyberspace. In the introductory parts the book summarizes basic knowledge of selected hazardous phenomena - cyberbullying, cybergrooming, sexting and risky behaviour in a social networking environment. Other parts have been devoted to the results of selected research studies that focus on individual phenomena.

The publication Risky behaviour of Czech and Slovak children in the Internet environment summarizes the results of three surveys carried out by the Centre for the Prevention of Risky Virtual Communication, Palacky University in Olomouc, during 2014 and 2015. Specifically, the researches were *Dangers of internet communication 5* and *Risky behaviour of Slovak children in the Internet environment*, which focus on the prevalence of risky behaviour associated with dangerous forms of communication in the pediatric population, and the study *Analysis of communications of Czech children and online predators*, which examined what communication strategies cyber predators choose in online attacks.

Another part focuses on netolism and its various forms, it also deals with risks associated with child prostitution and other related phenomena.

The final part of the book is devoted mainly to primary prevention of risky behaviour in the Internet environment, describes basic preventive strategies and also focuses on the experience with primary prevention in elementary and secondary schools.

Keywords: *cyberbullying, cybergrooming, sexting, netolism, the risks of social networking, webcam trolling, child prostitution, primary prevention of risky behaviour, research.*

19 Annotation

Die Publikation *Die Risikoformen des Verhaltens der tschechischen und slowakischen Kinder in der Internet-Umgebung* ist eine moderne Studie von Risikophänomenen, die mit interpersonellen Angriffen in Cyberspace verbunden sind. In den einleitenden Teilen fasst die Publikation die Grundkenntnisse über die ausgewählten Risikophänomene zusammen – Cyber-Schikane, Cyber-Grooming, Sexting und über anderes Risikoverhalten im sozialen Netzwerk. In weiteren Teilen werden Ergebnisse der ausgewählten Forschungsstudien präsentiert, die sich auf einzelne Phänomene orientieren.

Die Publikation *Die Risikoformen des Verhaltens der tschechischen und slowakischen Kinder in der Internet-Umgebung* fasst Ergebnisse von drei Forschungen zusammen, die in den Jahren 2014 und 2015 von Fachleuten im Zentrum der Prävention der Risikokommunikation im Internet der Pädagogischen Fakultät der Palacký Universität in Olomouc realisiert wurden. Konkret geht es um folgende Forschungen: *Die Gefahr der Kommunikation im Internet 5* und *Risikoverhalten der slowakischen Kinder in der Internet-Umgebung*, die sich auf die Prävalenz des mit Risikoformen der Kommunikation in der Kinderpopulation verbundenen Risikoverhaltens orientieren, und um die Studie *Analyse der Kommunikation der tschechischen Kinder und den online-Prädatoren*, die erforscht hat, welche Kommunikationsstrategien die Internetprädatoren im Rahmen den online-Angriffen wählen.

Der weitere Teil orientiert sich auf verschiedene Formen der Internetabhängigkeit und der Abhängigkeit von Computerspielen, befasst sich sowohl mit Risiken, die mit der Kinderprostitution verbunden sind, als auch mit weiteren zusammenhängenden Phänomenen.

Der Schlussteil der Publikation ist vor allem der Primärprävention des Risikoverhaltens in der Internet-Umgebung gewidmet, beschreibt Präventionsgrundstrategien, orientiert sich auch auf Erfahrungen aus der Realisierung der Primärprävention in Primar- und Sekundarschulen.

Schlüsselwörter: *Cyber-Schikane, Cyber-Grooming, Sexting, Internetabhängigkeit und Abhängigkeit von Computerspielen, Risiken der sozialen Netzwerke, Webcam-Trolling, Kinderprostitution, Primärprävention des Risikoverhaltens.*

KATALOGIZACE V KNIZE - NÁRODNÍ KNIHOVNA ČR

Kopecký, Kamil
Rizikové formy chování českých a slovenských dětí v prostředí internetu / Kamil Kopecký, René Szotkowski, Veronika Krejčí. -- 1. vydání. -- Olomouc : Univerzita Palackého v Olomouci, 2015. -- 170 stran. -- (Monografie)
Anglické a německé resumé
Nad názvem: Univerzita Palackého v Olomouci, Pedagogická fakulta, Centrum prevence rizikové virtuální komunikace. -- Publikace je určena pro odbornou veřejnost
ISBN 978-80-244-4861-9

316.346.32-053.2 * 004.738.5 * 364.636:004 * 316.624 * 364.692 * 37.03:364-212 * (437.3) * (437.6)
- děti -- Česko
- děti -- Slovensko
- internet
- kyberšikana
- rizikové chování
- patologické závislosti
- prevence (sociální problémy)
- kolektivní monografie

316.4/.7 - Sociální interakce [18]

Mgr. Kamil Kopecký, Ph.D.
a kol.

Rizikové formy chování českých a slovenských dětí v prostředí internetu

Výkonná redaktorka prof. PaedDr. Libuše Ludíková, CSc.
Odpovědná redaktorka Mgr. Vendula Drozdová
Technická redakce Mgr. Kamil Kopecký, Ph.D.
Návrh a grafické zpracování obálky Mgr. Kamil Kopecký, Ph.D.

Publikace ve vydavatelství neprošla jazykovou ani technickou redakční úpravou.

Vydala a vytiskla Univerzita Palackého v Olomouci
Křížkovského 8, 771 47 Olomouc
www.vydavatelstvi.upol.cz
www.e-shop.upol.cz
vup@upol.cz

1. vydání

Olomouc 2015

Ediční řada – Monografie

ISBN 978-80-244-4868-8 (online : PDF)
ISBN 978-80-244-4861-9 (print)

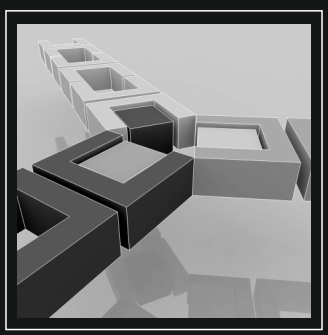
DOI 10.5507/pdf.15.24448619

Elektronickou verzi naleznete na internetových stránkách www.e-bezpeci.cz nebo na
www.flexibooks.cz.

Více informací o výzkumech realizovaných Centrem prevence rizikové virtuální komunikace naleznete na www.prvok.upol.cz a na www.e-bezpeci.cz.

Neprodejná publikace

vup 2015/0730



Odborná publikace **Rizikové formy chování českých a slovenských dětí v prostředí internetu** shrnuje výsledky tří výzkumů realizovaných Centrem prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci v průběhu let 2014 a 2015.

Jejím cílem je upozornit na nejvýznamnější rizika, kterým jsou v prostředí internetu české a slovenské děti vystaveny, a navrhnout řešení, která umožní tato rizika účinným způsobem snížit.

9 788024 448619