ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
FAKULTA BIOMEDICÍNSKÉHO INŽENÝRSTVÍ
Katedra zdravotnických oborů a ochrany obyvatelstva

Problematika zneužívání nezletilých osob v prostoru sociálních sítí

The Issue of Abuse of Minors on Social Networks

Diplomová práce

Studijní program: Civilní nouzové plánování

Autor diplomové práce: Bc. Dominika Kacetlová

Vedoucí diplomové práce: doc. PhDr. Barbora Vegrichtová, Ph.D., MBA

Kladno 2022

ZADÁNÍ DIPLOMOVÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení:	Kacetlová	Jméno:	Dominika	Osobní číslo:	456427
Fakulta:	Fakulta biomedicínského inženýrství				
Garantující katedra:	Katedra zdravotnických oborů a ochrany obyvatelstva				
Studijní program:	Civilní nouzové plánování				

II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

Problematika zneužívání nezletilých osob v prostoru sociálních sítí

Název diplomové práce anglicky:

The Issue of Abuse of Minors on Social Networks

Pokyny pro vypracování:

Předmětem této diplomové práce bude téma zneužívání nezletilých na sociálních sítích. Teoretická část bude věnována charakteristice základních pojmů z oblasti kybernetické kriminality, popisu vybraných sociálních sítí, způsobům a projevům zneužívání nezletilých osob v prostoru sociálních sítí a právním kontextům této problematiky. Dále bude teoretická část doplněna o aktuální oficiální statistiky z oblasti této problematiky, současné možnosti prevence a protiopatření. Empirická část práce bude zaměřena na oblast této problematiky z pohledu rodičů a vyučujících. Budou využity metody řízených rozhovorů s rodiči a pedagogy druhého stupně základních škol a víceletých gymnázií, které budou komparovány a analyzovány. Výstupem práce bude formulace doporučení možných způsobů prevence zneužívání nezletilých na sociálních sítích pro rodiče, základní školy a víceletá gymnázia.

Seznam doporučené literatury:

[1] PECHÁČKOVÁ, Marika, Kdo chytá v síti, Brno: BizBooks, 2020, ISBN 978-80-265-0919-6
[2] KRČMÁŘOVÁ, Barbora, Děti a online rizika: sborník studií, Praha: Sdružení Linka bezpečí, 2012, ISBN 978-80-904920-2-8
[3] HULANOVÁ, Lenka, Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality, Praha: Triton, 2012, ISBN 978-807-3875-459

Jméno a příjmení vedoucí(ho) diplomové práce:

doc. PhDr. Barbora Vegrichtová, Ph.D., MBA

Jméno a příjmení konzultanta(ky) diplomové práce:

Datum zadání diplomové práce: 21.09.2020
Platnost zadání diplomové práce: 18.09.2022

doc. Mgr. Zdeněk Hon, Ph.D.
vedoucí katedry

prof. MUDr. Jozef Rosina, Ph.D., MBA
děkan

PROHLÁŠENÍ

Prohlašuji, že jsem diplomovou práci s názvem Problematika zneužívání nezletilých osob v prostoru sociálních sítí vypracovala samostatně pouze s použitím pramenů, které uvádím v seznamu bibliografických odkazů.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

V Kladně dne 08.05.2022

…….

Bc. Dominika Kacetlová

PODĚKOVÁNÍ

Touto cestou bych chtěla poděkovat vedoucí práce paní doc. PhDr. Barboře Vegrichtové, Ph.D., MBA za odborné vedení práce, konstruktivní připomínky, cenné rady, čas a trpělivost.

Dále bych chtěla poděkovat všem respondentům z řad rodičů a vyučujících za podílení se na výzkumu diplomové práce.

ABSTRAKT

Hlavním tématem této diplomové práce je problematika zneužívání nezletilých osob v kyberprostoru, přesněji v prostoru sociálních sítí. Díky dostupnosti moderních technologií a téměř neomezenému připojení k internetu se téma zneužívání dětí na sociálních sítích stalo velmi palčivým a aktuálním tématem.

V teoretické části práce jsou vymezeny základní pojmy jako kyberprostor, sociální sítě, či kybernetická kriminalita. Jsou zde popsány typy kybernetické kriminality na sociálních sítích, prevence a protiopatření trestných činů, a právní kontext kybernetické kriminality páchané na dětech.

Praktická část je zpracována formou smíšeného výzkumu, provedeného prostřednictvím řízených rozhovorů s rodiči a vyučujícími základních škol a víceletých gymnázií. Na základě získaných dat je vytvořeno doporučení možných způsobů prevence zneužívání nezletilých osob v prostoru sociálních sítí pro rodiče a školy.

Klíčová slova

Zneužívání dětí; sociální sítě; kyberkriminalita; kyberprostor; prevence; řízený rozhovor; rodiče; škola.

ABSTRACT

The main topic of this diploma thesis is the abuse issue of minors in cyberspace - more specifically in the area of social networks. Thanks to the availability of moder technologies and almost unlimited internet connection, the topic of child abuse on social networks has become a very essential and relevant topic.

The theoretical part of the thesis defines basic concepts such as cyberspace, social networks and cybercrime. This part describes the types of cybercrime on social networks, criminal prevention and its countermeasures and also the legal context of cybercrime committed against children.

The practical part is processed as a mixed research created from the structured interviews with parents and teachers of primary schools and secondary schools. The recommendation for suitable methods of preventing the abuse of minors in the social network space for parents and schools is produced based on the gathered data.

Keywords

Child abuse; social networks; cybercrime; cyberspace; prevention; structured interview; parents; school.

Obsah

1 ÚVOD

Historie internetu se začala psát v 50. letech 20. století, v roce 1991 byl internet distribuován široké veřejnosti. Od této doby se postupně internet rozrostl do gigantických rozměrů, jak jej známe dnes. Stala se z něj každodenní součást života většiny lidí na světe.

Internet je největším úložištěm cenných dat, místem mnoha příležitostí. Umožňuje snadnou komunikaci lidí na velkou vzdálenost. Za účelem snadného propojení osob z různých koutů světa či vzdálených míst vznikly sociální sítě. Ty jsou využívány ke komunikaci uživatelů, sdílení různých zážitků, sdružování osob, které vyznávají stejné hodnoty, ale i k činnostem jako jsou obchody. Díky velké dostupnosti moderních technologií a připojení k internetu jsou sociální sítě místem pro všechny. Pro dospělé, děti, obchodníky, ale i pro podvodníky.

S postupem času se kriminalita z ulic rozšířila i na internet a sociální sítě, proto i v kyberprostoru musí člověk být stejně obezřetný jako v reálném světě. Na internetu lze narazit na podvodníky, kteří se orientují na různé skupiny osob. Bohužel se i zde najdou podvodníci a útočníci, kteří svoji trestnou činnost orientují na děti a dospívající osoby, které ve většině případů podvod neodhalí a ocitají se tak v nebezpečí. Na toto téma v minulosti v Česku nejvíce upozornil dokumentární snímek V Síti, který byl i mým impulzem pro vznik této diplomové práce.

Tématem této diplomové práce je problematika zneužívání nezletilých osob na sociálních sítích. Teoretická část práce se věnuje odborné terminologii z oblasti kyberprostoru, kybernetické kriminality a prevence trestných činů páchaných na dětech v kyberprostoru. Empirická část práce je zaměřena na probíhající prevenci ve školách a v rodinách.

Cílem této diplomové práce je na základě výzkumu identifikovat slabá místa v preventivní činnosti, formulovat doporučení možných způsobů prevence zneužívání nezletilých osob v prostoru sociálních sítí pro rodiče, základní školy a víceletá gymnázia.

2 CÍLE PRÁCE A HYPOTÉZY

Hlavním cílem této diplomové práce je formulace doporučení možných způsobů prevence zneužívání nezletilých osob na sociálních sítích pro rodiče, základní školy a víceletá gymnázia.

Dílčí cíle práce:

- Seznámit čtenáře s problematikou zneužívání nezletilých osob na sociálních sítích
- Zjistit, zda na školách probíhá prevence zneužívání nezletilých osob na sociálních sítích
- Zjistit, zda v rodinách probíhá prevence zneužívání nezletilých osob na sociálních sítích
- Zjistit, zda probíhá komunikace mezi rodiči a školami na téma bezpečnosti dětí na internetu
- Potvrdit či vyvrátit stanovené hypotézy

2.1 Stanovené hypotézy

Pro diplomovou práci byly stanoveny následující výzkumné otázky, které jsou z důvodu lepší srozumitelnosti pro širokou veřejnost sepsány pod pojmem hypotézy:

HYPOTÉZA 1: Prevence zneužívání nezletilých osob na sociálních sítích by měla vycházet od rodičů i škol.

HYPOTÉZA 2: Aplikace rodičovské kontroly zná více než polovina rodičů.

HYPOTÉZA 3: Většina rodičů shledává internet nebezpečným místem pro děti.

HYPOTÉZA 4: Bezpečnost dětí na internetu je probíraným tématem v interakci mezi školou a rodiči.

3 PŘEHLED SOUČASNÉHO STAVU

3.1 Internet

Internet je celosvětově distribuovaný dynamický počítačový systém skládající se z jednotlivých, pomocí IP protokolů propojených, menších počítačových sítí. Tento neustále vyvíjející se systém propojení umožňuje vzájemný přenos dat a informací, komunikaci, a poskytování služeb mezi subjekty. Systém je vázaný na hardware, ovšem vytváří neomezený a těžko definovatelný kyberprostor. [1]

3.1.1 Historie internetu

Počátky vzniku internetu se datují do druhé poloviny padesátých let 20. století. Lze říct, že vznik internetu byl reakcí USA na vypuštění první umělé sovětské družice Sputnik 1 v říjnu roku 1957, kdy si Spojené státy uvědomily, že jejich zaostávání v kosmických a vojenských technologiích, by pro ně mohlo mít během studené války vážné následky. Proto v roce 1958 byla ministerstvem obrany USA založena agentura Advanced Research Project Agency (ARPA), která se zaměřovala na podporu výzkumných projektů. Na základě podpory od ARPA vzniklo několik neformálních skupin programátorů, které působily na řadě univerzit, např. na bostonské MIT, či kalifornské Barkeley. [1, 2]

Mezi jednotlivými programátorskými skupinami ovšem chyběla efektivní komunikace, takže působily takřka izolovaně. Proto počátkem 60. let Joseph C. R. Licklider založil skupinu Intergalactic Network, která sdružovala dílčí programátorské skupiny, a začala pracovat na konceptu paketových sítí. V roce 1968 vznikl projekt Arpanet a byl agenturou ARPA vypsán tendr na vývoj paketové sítě, který vyhrála firma Bolt, Beranek and Newman (BBN). BBN, která pracovala na jádru sítě a zařízeních IMP, předchůdcích routerů, zapojila do projektu univerzitní pracoviště z Utahu, Santa Barbary, Stanfordu a Los Angeles, která vyvíjeli software, jehož prostřednictvím by jejich počítače

mohly komunikovat. Historicky první odeslaná zpráva prostřednictvím Arpanetu byla odeslána 29. října 1969. [2]

Do paketové sítě se postupně připojily další americké univerzity či instituce. V roce 1973 získala síť připojením University College London a norského seismologického ústavu NORSAR mezikontinentální charakter. Na principu paketového systému začaly fungovat i další různé sítě, které ovšem nemohly mezi sebou komunikovat. Proto se v tentýž roce začali Bob Kahn a Vint Cerf věnovat sjednocení protokolů paketových sítí, které bylo možné díky technologii protokolů TCP/IP. Propojením geograficky vzdálených a technologicky rozmanitých sítí vznikla „síť sítí“, tedy internet. [2, 3]

Československo se oficiálně k internetové síti připojilo 13. února 1992 na Českém vysokém učení technickém v Praze, které bylo napojenu pouze na jedinou mezinárodní linku Praha – Linz. [2, 3]

Internet byl ale stále legislativně určen pouze pro akademickou komunitu. K jeho distribuci pro širokou veřejnost došlo po změně legislativy v USA v roce 1991, a postupně v dalších státech. Pro laika ovšem byl ovšem systém nepoužitelný, jelikož programy byly psané pro použití programátorů. Milník, kterým se internet stal použitelným pro laika, byl vznik služby World Wide Web, tedy WWW. [2, 3]

3.2 Kyberprostor

Slovo kyberprostor je do češtiny přejaté z anglického Cyberspace. Jedná se o virtuální svět, fiktivní prostor, který vznikl vytvořením internetu. Tento prostor je paralelou k reálnému světu, nemá hranice, je dynamický. Nelze říct, že kyberprostor je jednoduše internet nebo web, jelikož nezahrnuje jen webové stránky, ale i data, uživatele, služby a počítačové systémy.

Ačkoli se jedná o virtuální realitu, je kyberprostor závislý na jeho materiálním základu, tzn. že v případě absolutního kolapsu všech materiálních medií by došlo k nenávratnému poškození kyberprostoru, či k jeho úplnému zániku. [1, 4, 5]

Legislativně se dá kyberprostor definovat dle zákona č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů, § 2 písmena a), kterým se kybernetickým prostorem rozumí *„digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.“* [6 § 2 p. a)]

Do kyberprostoru se připojila značná část společnosti, odhadem 3,6 miliard osob, což svědčí o jeho otevřenosti a globálnosti. Lze se zde jednoduše dostat k různým datům a informacím, bohužel i k nesmyslným či lživým informacím, které mohou mít za následek ovlivnění mínění uživatele. Tento virtuální svět má tedy i jistý dopad na svět reálný. [1]

Co se rozdělení kyberprostoru týče, lze jej rozdělit na tři části. První část, Surface Web, je zjednodušeně prostor, kde se pohybuje běžný uživatel, a tvoří přibližně pouze 4 % kyberprostoru. Další dvě části, zbylých 96 %, jsou Deep Web a Dark Web, označované jako Darknets. Nejedná se o samostatné sítě, ale o aplikační vrstvu existujících sítí. [1]

3.2.1 Surface Web

Surface Web, v češtině povrchový web, představuje část kyberprostoru, která je přístupná všem uživatelům internetu. K pohybu na Surface Webu není zapotřebí žádného speciálního software, ale pouze standartního prohlížeče. Obsahuje veřejně přístupné stránky, které lze najít vyhledávačem po zadání

klíčových slov, bez zadávání jakéhokoliv hesla. Surface Web je také označován jako Clearnet, Visible Web nebo Indexed Web. [1, 7, 8]

3.2.2 Deep Web

Jak už bylo výše zmíněno Deep Web se společně s Dark Webem řadí mezi Darknets, které nemají díky mediím u běžných uživatelů dobrou pověst. Ovšem většina uživatelů se na Deep Webu pohybuje, aniž by o tom tušila. Do této části kyberprostoru spadají internetové soukromé stránky s omezeným přístupem, ale i státem cenzurované stránky nebo stránky nelegální. Klasické vyhledávače tyto stránky vyhledat neumí. Přihlášením se do e-mailu, na sociální sítě nebo do e-shopu, vstupuje uživatel do Deep Webu. Lze sem řadit i firemní intranety. Zjednodušeně řečeno, tato část kyberprostoru se uživateli otevírá zadáním přihlašovacích údajů a hesla, nebo konkrétního odkazu. [8, 9]

3.2.3 Dark Web

Poslední částí kyberprostoru je Dark Web, který má mezi běžnými uživateli internetu tu nejvíce negativní pověst. Většina lidí si jej představí jako místo, kde se ilegálně obchoduje s drogami, zbraněmi, bílým masem, dětskou pornografií, citlivými údaji, falešnými doklady, či jako místo, kde lze objednat vraždu. Dle studie z roku 2016 se přibližně 50 % stránek na Dark Webu opravdu zabývalo ilegální činností. Ovšem i tato mince má dvě strany. Dark Web využívají za účelem ochrany vlastní identity různé skupiny odhalující konspirace, disidenti či žurnalisté. Anebo také lidé žijící v totalitních režimech, kteří touto cestou organizují protesty, komunikují na Facebooku či sledují videa na YouTube. [1, 8, 10]

Na Dark Web se lze dostat pomocí speciálních softwaru. Jedním z příkladů takového softwaru je prohlížeč Tor, vytvořený programátory z Americké národní výzkumné laboratoře spravované vládou, s cílem vytvořit prostředí,

kde by mohli bezpečně sdílet informace různé instituce či jedinci, např. agenti. V roce 2002 byl Tor zpřístupněn veřejnosti z důvodu bezpečnosti komunikace. Vládní složky se díky tomuto kroku mohly schovat mezi anonymní uživatele. [1, 8, 10]

Dark Web není z klasických prohlížečů typu Chrome, Opera nebo Mozilla přístupný z důvodu, že tyto prohlížeče neumí vyhledat stránky s koncovkou .onion, kterou stránky na Dark Webu využívají. [10]

3.3 Sociální sítě

Sociální sítě jsou internetové služby, které umožňují svým uživatelům mezi sebou komunikovat, sdílet spolu informace, fotografie, videa či své pocity prostřednictvím vytvořených účtů. Zjednodušeně je hlavním cílem sociálních sítí sdílení obsahu. Pro pohyb na sociálních sítích se musí uživatel zaregistrovat a vytvořit si vlastní profil. Téměř veškerý obsah sociálních sítí je tvořen samotnými uživateli, např. přidáváním různých příspěvků, statusů apod. Mezi uživateli jsou oblíbená různá diskusní fóra, chaty, stránky, či skupiny, které se věnují určitým tématům. [13, 14]

Na sociálních sítích jsou vytvářeny různé komunity lidí, které něco spojuje, může se jednat o spolužáky, fanoušky konkrétního sportovního týmu, výtvarné skupiny, nebo čistě jen přátelství osob. [13]

Jak už bylo výše zmíněno, každý uživatel se musí zaregistrovat a vytvořit si vlastní profil, který je virtuální vizitkou uživatele. Uživatel si zde nastaví svoje osobní údaje, dle kterých může být pro ostatní uživatele na sociální síti dohledatelný. Mimo jména a příjmení, např. i místo bydliště, profilovou fotografii, dosažené vzdělání, rodinný stav, záliby, nebo stručný životopis. Ovšem uživatel by si měl raději rozmyslet uvedení přesné adresy bydliště,

číslo telefonu, čísla účtů apod. Jednoduchým pomocníkem při rozhodování, co sdílet na sociálních sítích, pro uživatele může být pravidlo, sdílet pouze údaje a informace, které by byl ochotný veřejně vyvěsit na místě s velkou koncentrací lidí, např. autobusové zastávce. Stejné pravidlo lze aplikovat i na přidávání příspěvků. Téměř na všech sociálních sítích lze na příspěvky uživatelů reagovat. Příspěvky lze komentovat, sdílet či označit, že se uživateli líbí. [12, 13]

Sociální sítě můžeme rozdělit na české a mezinárodní sociální sítě. České sociální sítě se dříve těšily velkému zájmu uživatelů, ovšem v současné době jsou mezi uživateli více populární mezinárodní sítě, jimž dominují zejména Facebook, Twitter a Instagram, proto české sítě postupně z internetu mizí. [12, 13]

3.3.1 Facebook

Facebook je největší mezinárodní sociální sítí, kterou využívá přes 2,7 miliardy uživatelů z různých koutů světa. Dostupný je ve více než 80 jazycích. Facebook byl založen v roce 2004 Markem Zuckerbergem, jenž je prezidentem společnosti Meta Platforms, která zaměstnává přes 50 tisíc lidí. Síť byla původně studentským projektem Harvardovy univerzity, který se rozšířil i na ostatní univerzity, a později se otevřel veřejné společnosti. [13, 15, 16, 17]

Jako na každé sociální síti je i na Facebooku potřebný účet uživatele a vytvořený profil, dle kterého může být uživatel ostatními uživateli dohledán. Uživatel si může v současné době přidávat ostatní uživatele do přátel, komunikovat s nimi přes zprávy a komentáře pod příspěvky na tzv. zdi. Může vstupovat do různých tematických skupin, prohlížet si různé události či stránky, které by ho mohli zajímat. Facebook má ve své nabídce i prodejní místo, Marketplace, kde mohou uživatele prodávat různé věci. [13, 15, 16, 17]

Dle pravidel Facebooku si každý uživatel může založit pouze jediný účet, a to pod svým reálným jménem. Uživatel musí být starší 13 let, nesmí být odsouzený sexuální delikvent, nebo uživatel, kterému byl účet dříve smazán pro porušení smluvních podmínek. [17]

3.3.2 Twitter

Twitter je po Facebooku druhou největší mezinárodní sociální sítí, kterou využívají stovky miliónů uživatelů. Síť je přístupná v 10 různých jazycích, ovšem v Česku je její popularita nižší, a to zřejmě z důvodu absence češtiny. Síť je oblíbená především u žurnalistů. [13, 18]

Twitter funguje na principu přidávání příspěvků, tzv. tweetů, které mohou být maximálně 140 znaků dlouhé a zobrazují se na profilu autora. K tweetům se mohou v komentářích vyjadřovat další uživatelé, kteří autora sledují. Důležitým prvkem při psaní tweettů je i používání tzv. hashtagů, které mohou označovat hlavní témata příspěvků, a díky kterým ostatní uživatele mohou tweety vyhledat dle tématu. [13, 18]

3.3.3 Instagram

Instagram je sociální síť určená především pro mobilní telefony. Využívat ji mohou jednotlivci, ale i různé firmy. Slouží ke zveřejňování fotografií či videí, které může uživatel upravit dle jeho libosti různými filtry, nálepkami či popisky. Zveřejňovány mohou být také různá videa. Instagram nabízí také doplnění fotek či videí o zvukovou stopu, na výběr jsou různí interpreti. Příspěvky je zde také možné označovat hashtagy. [13, 19]

Stejně jako na dalších sociálních sítích, i zde je spojení mezi uživateli. Každý uživatel může sledovat další uživatele, se kterými lze komunikovat

pomocí komentářů u příspěvků nebo prostřednictvím zpráv, které se zde nazývají Direct. [13, 19]

3.3.4 TikTok

Stejně jako Instagram, je i TikTok určen spíše pro mobilní telefony, jelikož se jedná o aplikaci. Tato sociální síť je dostupná pro více jak 150 zemí, v 75 různých jazycích, včetně češtiny. Je populární především u teenagerů, nejvíce uživatelů spadá do věkové kategorie od 13 do 24 let, ale lze zde narazit i na uživatele v důchodovém věku. TikTok ovšem není používám jen jedinci, ale i různými společnostmi, které využívají tuto sociální síť ke svému marketingu. [20, 21]

TikTok funguje na principu nahrávání a sledování krátkých videoklipů, které lze vytvářet přímo přes aplikaci. Jedná se o videa o délce 3 až 60 vteřin, která mohou být doplněny hudbou, filtry či různými popisky. Videoklipy jsou tvořen na různé témata, lze zde narazit opravdu na cokoliv. Převládají ovšem videa s různými tanečními kreacemi, výzvami, karaoke, parodiemi, či videa s domácími mazlíčky. [20, 21]

Uživatelé mají možnost si u videoklipů nastavit, kdo jej může vidět. I zde funguje přidávání hashtagů, které zařadí videa do různých kategorií. Komunikace mezi uživateli zde probíhá pomocí komentářů pod videi. Pokud chce uživatel vyjádřit druhému uživateli podporu, může jej začít sledovat, či označit jeho video srdíčkem, které vyjadřuje, že se uživateli líbí. [20, 21]

3.3.5 YouTube

Ačkoli by se mohlo zdát, že YouTube není sociální síť, opak je pravdou. Youtube není typickou sociální sítí, ale nabízí uživatelům částečně stejné

možnosti komunikace jako ostatní sociální sítě, a to prostřednictvím přímých zpráv nebo komentáři pod videi, proto jej lze k nim řadit. [13, 22]

YouTube je největší světová video služba, která je denně využívány více než 2 miliardami uživatelů, a je druhou nejpoužívanější stránkou hned po vyhledávači Google. Umožňuje uživateli nahrát vlastní video, či přehrávat videa ostatních uživatelů. Videa lze sdílet na dalších sociálních sítích. [13, 22]

3.3.6 Snapchat

Další z populárních sociálních sítí pro mladé a děti je i Snapchat, který byl původním projektem studentů Stanfordských studentů. Jedná se o aplikaci, s jejíž pomocí lze sdílet fotografie či krátká videa s přáteli, které bude moci příjemce zobrazit jen po omezenou dobu, od 1 do 10 sekund. Pokud si příjemce udělá snímek obrazovky obsahu, odesílatel je aplikací informován. Videa či fotky mohou být doplněny o různé filtry, popisky atd. Uživatelé mezi sebou mohou komunikovat prostřednictvím zpráv, hovorem či video hovorem. [23, 24]

3.3.7 Badoo

Badoo je sociální síť určená pro seznamování lidí. Funguje od roku 2006 a má přibližně 200 milionů uživatelů. Seznamování uživatelů je založeno na principu společných vlastností. Uživatelé si prohlíží profily ostatních uživatelů, případně je označují, že se jim líbí. Pokud je mezi uživateli shoda, jsou propojeni, a mohou si začít psát prostřednictvím zpráv. Síť bývá využívaná nejen jako seznamovací síť, ale i jako prostředek k nalezení nových přátel. Badoo má jak webovou verzi, tak i mobilní aplikaci, a jeho užívání v základní verzi je zdarma. [25, 26]

3.3.8 Tinder

Tinder je sociální síť fungující na principu seznamovací sítě. Vznikl v roce 2012, je dostupný ve 190 státech, ve více než 40 jazycích. Lze jej spustit jako aplikaci, ale i jako webovou stránku. Uživatel si zde prohlíží profily dalších uživatelů či uživatelek v jeho preferenční kategorii, ve které zde nastavit věkové rozmezí uživatelů, či rozmezí vzdálenosti, kde konkrétní uživatel nachází. Uživatel každý profil označí, zda se mu líbí či nelíbí. Pokud dojde ke vzájemné shodě, mohou se uživatelé kontaktovat. [27, 28]

3.3.9 Lidé.cz

Lidé.cz byla největším českým zástupcem ve světě sociálních sítí. Fungovala od roku 1997 do prosince 2020. Do nástupu Facebooku se jednalo o nejpopulárnější českou sociální síť. Jejím provozovatelem byla firma Seznam.cz, která v roce 2014 z důvodu nezájmu uživatelů, pozměnila koncept na seznamovací síť. Bohužel síť nepřinášela Seznam.cz dostatek financí, které byly potřebné pro její údržbu, čím dál častěji se na síti objevovaly fotografie či texty se sexuální tématikou, proto se firma rozhodla činnost sítě celkově ukončit. [13, 29]

3.4 Kybernetická bezpečnost

Kybernetická bezpečnost je podmnožina bezpečnosti, která se zakládá na uvědomění si každého uživatele, že může být v kyberprostoru ohrožen. Nelze ji přesně definovat, zjednodušeně ale lze říct, že se jedná o soubor opatření aplikovaných v kyberprostoru, zabezpečující ochranu počítačových systémů, dat, uživatelů a kyberprostoru. [1]

Mezi tři prvky kybernetické bezpečnosti řadíme technologie, procesy a lidi. Lidé jsou zásadním, ale nejslabším prvkem kybernetické bezpečnosti, a zároveň

nejčastějším cílem kybernetických útoků. Proto je důležité, aby i běžní uživatelé internetu znali základní pravidla fungování kyberprostoru a bezpečnosti, pochopili základní funkce systémů zařízení, které používají. Dále analyzovali aplikace, které využívají, četli smluvní podmínky aplikací a případně aplikace s nevyhovujícími podmínkami nevyužívali. A především aby se v problematice kybernetické bezpečnosti vzdělávali. [1]

V České republice je gestorem kybernetické bezpečnosti Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), jehož výkonným prvkem je Národní centrum kybernetické bezpečnosti (NCKB). [11]

3.5 Kybernetická kriminalita

Stejně jako kybernetickou bezpečnost není možné kybernetickou kriminalitu přesně definovat, a to z důvodu dynamičnosti této problematiky. Kybernetická kriminalita, nebo také kyberkriminalita či počítačová kriminalita, je trestná činnost zahrnující škodlivé jednání vůči počítačovému systému, počítačové síti či jinému objektu za použití počítačového systému. Aby bylo možné mluvit o kybernetické kriminalitě, musí se jednat o kriminalitu při které jsou informační a komunikační technologie využity jako nástroj pro spáchání trestného činu, nebo jsou cílem útoku v kyberprostoru. Které trestné činy lze zahrnout do kybernetické kriminality je možné zjistit z různých klasifikací kybernetické kriminality. [1, 12]

Klasifikací kybernetické kriminality je hned několik. Některé se řídí dle právních norem, jiné jsou dle vnímání různých autorů či organizací řešící kybernetickou kriminalitu. Pro příklad jsou níže uvedeny dvě klasifikace. [1]

3.5.1 Klasifikace dle eEurope+

Dle klasifikace eEurope+ se kybernetické trestné činy dělí na:

1) Zločiny porušující soukromí (Nelegální nakládání s osobními daty)
2) Zločiny se vztahem k obsahu počítače (Rasismus, výzvy k násilí, dětská pornografie aj.)
3) Zločiny se vztahem k duševnímu vlastnictví
4) Ekonomické zločiny (Padělání a podvody, neoprávněný přístup, sabotáž, špionáž, šíření virů, hackerství)

3.5.2 Klasifikace dle Úmluvy o kyberkriminalitě a dle dodatkového protokolu

,,Úmluva o kyberkriminalitě dělí kybernetické trestné činy do čtyř kategorií:

1) *trestné činy proti utajování, integritě a dostupnosti počítačových dat a systémů (Offences against the confidentiality, integrity and availability of computer data and systems),*
2) *trestné činy související s počítači (Computers-related offences),*
3) *trestné činy související s obsahem (Content-related offences),*
4) *trestné činy související s porušováním autorských práv a práv souvisejících (Offences related to infringements of copyright and related rights),*

Dodatkový protokol pak definuje další kybernetické trestné činy:

1) *šíření rasistických a xenofobních materiálů pomocí počítačových systémů (Dissemination of racist and xenophobic meterial throught computer systems),*
2) *rasisticky a xenofobně motivované vyhrožování (Racist and xenophobic motivated threat),*

3) *rasisticky a xenofobně motivované útoky (Racist and xenophobic motivated insult),*
4) *popírání, snižování, schvalování nebo ospravedlňování genocidy nebo zložinů proti lidskosti (Denial, gross minimisation, approval or justification of genocide or crimes agains humanity).“* [1, s. 112]

3.6 Kybernetická kriminalita na sociálních sítích

3.6.1 Sociální inženýrství

Sociální inženýrství neboli sociotechnika, je způsob manipulace, ovlivňování či přesvědčování osob, za účelem získání různých informací či provedení určité akce, které by osoba za normálních okolností neposkytla či akci neprovedla. Takový útok může být mířen na náhodné i konkrétní osoby. Za své cíle si sociotechnici mohou vybrat náhodnou skupinu obětí, oběti vytipované dle věku či pohlaví, nebo konkrétní právnické či fyzické osoby. Útočníci si před svým útokem snaží s obětí vybudovat důvěru, využívají její nepozornosti, ochoty, lenosti, hlouposti či strachu. Tato příprava oběti může být na dlouhodobé bázi. [1, 13]

V případě sociálních sítí a mladistvých oslovují útočníci jejich oběti většinou pod nějakou záminkou. Mohou to být různé koníčky, místo bydliště, oblíbené kapely či seriály nebo filmy, společní přátelé apod. Zjednodušeně lze říct, že se útočník snaží svůj útok koncipovat tak, aby svou oběť zaujal. Informace o své oběti většinou získává z veřejně dostupných informací na sociální síti, které oběť sama sdílí. V některých případech lze narazit na útočníky, jež používají jako záminku třetí osobu. Záminka může být postavena na prohrané sázce s kamarádem, na kamarádovi, kterému se oběť údajně líbí, na kamarádovi, ze kterého si chce osoba udělat srandu. Výjimkou není ani záminka rady na intimní témata typu: Ahoj, je mi 15 a ještě jsem neměl holku,

myslíš si, že je to divné? V tomto případě je oběť rovnou donucena ke konverzaci na intimní témata. [13]

Někteří útočníci ovšem tuto fázi útoku přeskakují a oslovují oběť s konkrétním požadavkem, který může mít sexuální podtext, či být vulgární. Ti svůj útok realizují na větším počtu obětí, aby měli větší šanci úspěchu. V případě neúspěchu mohou potenciální oběť znovu zkusit oslovit prvním popsaným způsobem, pod jinou identitou. Často se jedná o nabídku finanční částky, či jiné benefity za protislužbu, většinou za nahé fotografie nebo sex. Oběti ve většině případů slibovanou odměnu ovšem neobdrží, útočník se vymluví nebo použije získaný materiál k vydírání oběti. [13]

Útočníci k dosažení svých cílů využívají falešné profily s fotografiemi lidí či vrstevníků, které někde odcizili, nebo fotografie své předchozí oběti. Nepoužívají fotky slavných osobností, jelikož by to bylo snadno odhalitelné. Jejich slabinou ovšem mohou být jejich falešná jména, či přezdívky, které mohou již z počátku vyvolat podezření. Falešná jména se leckdy skládají z různých křestních jmen a podivných příjmení např. Hanka Bohatá, Lenka Zkušená apod., přezdívky mohou být často vulgární, se sexuálním kontextem. Stejně tak mohou být odhalitelní díky jejich vyjadřování. Používají buď složité skladby vět, které by dítě nebylo schopné dát dohromady, nebo naopak ve své snaze napodobit mluvu vrstevníků dětské oběti dělají příliš mnoho pravopisných chyb, používají archaismy, či výrazy, které pro momentální generaci dětí již nejsou aktuální. Bohužel tyto chyby však dítě ve většině případů nedokáže odhalit. Nápadným indikátorem ještě před prvním kontaktem může být věkové vymezení preferencí útočníka. V různých chatovacích místnostech lze často takového vymezení vidět: Holka na skype max 16? [13]

Po prvním kontaktu s obětí se většinou útočník s konverzací snaží přestoupit na jinou platformu, která mu poskytuje nástroje k zaznamenávání videohovoru. Využíván bývá například Skype, či Facebook, pomocí kterého si útočník může ověřit, že opravdu komunikuje s dítětem či mladistvým, a zároveň se díky tomuto kroku dostane ke kontaktům oběti. Tyto kontakty může útočník v případě potřeby využít k získávání informací o oběti, či k jejímu vydírání ve smyslu, že jejich konverzaci, či vyměněné fotografie pošle jejím kontaktům. [13]

3.6.2 Webcam trolling

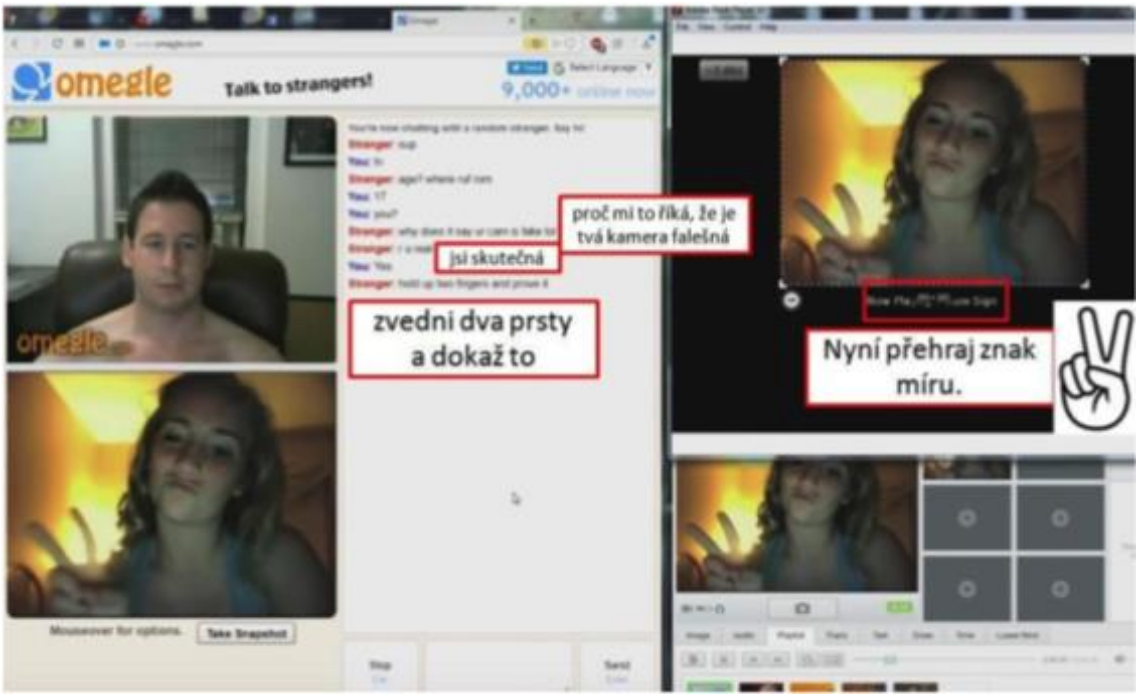
Dalším fenoménem kybernetické kriminality je webcam trolling, který je jednou z metod sociotechniky. Jedná se o používání podvodného software na komunikačních sociálních sítích např. na Facebooku, či Skype za účelem nalákání dětí a mládeže na erotické hovory nebo k získání intimních záběrů, k manipulování oběti či k jejímu vydírání. [13, 30]

Webcam trolling je postaven na promítání falešných videozáznamů namísto skutečného záznamů z webkamery. Vše, co k jeho uskutečnění pachatel musí udělat je zakoupení nikterak drahého software, který umožňuje vytvoření virtuální webkamery. Tato virtuální webkamera je následně propojena s různými messengery, či videochaty a namísto reálného kamerového záznamu je oběti promítána předpřipravená videosmyčka. Na takové videosmyčce se mohou nacházet záběry různých atraktivních dívek či mladých chlapců. Komunikace mezi pachatelem a obětí poté může probíhat ve smyslu sexuálních témat, čímž se útočník snaží ze své oběti vylákat intimní záběry. Oběť netuší, že tento videohovor je nahráván a může být následně zneužit. [13, 30]

Různé videosmyčky jsou volně ke stažení na internetu, ovšem ve většině z nich je absence zvuku. Sociální inženýři, schovávající se za tváří mladého

chlapce či dívky, v tomto případě využívají různé výmluvy, proč tomu tak je. Často se objevují výmluvy na rozbitý mikrofon, nebo že nemohou mluvit, protože rodiče jsou vedle v pokoji. Ačkoli je tohle jedna ze slabin webcam trollingu, oběti leckdy stačí, že svůj protějšek pouze vidí, a dopisují si přes chat. Absence zvuku videa může být prvním ukazatelem na to, že se jedná o podvrh. Další indicie mohou být přímo v obrazu videa, např. kulaté kliky na dveřích, které se v Česku nepoužívají, či knihy z různých cizích jazycích. V podvržených videích jsou často dělané střihy, obraz není plynulý. [13, 30]

Nejjistějším způsobem, jak webcam trolling odhalit, je požádat osobu na druhé straně videohovoru, aby na kameře provedla úkon, který nelze v daný moment zfalšovat. Osvědčená je žádost o napsání vzkazu na papír v reálném čase, kde se bude nacházet jméno osoby, současné datum a čas, a nějaké další domluvené slovo. [13, 30]



Obrázek 1 - Webcamtrolling [31]

3.6.3 Kybergrooming

Kybergrooming je jednání realizované za použití online komunikačních prostředků, či jiných moderních technologií, které má za cíl vzbudit v oběti pocit důvěry, přimět jej k osobní schůzce, či jej zneužít k jiným účelům, např. terorismu. Jedná se o psychickou manipulaci, při které jsou využívány různé metody sociotechniky, a její nejčastější obětí jsou mladistvé osoby ve věku 11 až 17 let, bez ohledu na pohlaví. Samotný kybergrooming má několik etap, probíhá obvykle na dlouhodobé bázi v závislosti na důvěřivosti oběti a způsobu manipulace. Výsledkem celého tohoto procesu může být sexuální zneužití na osobní schůzce. [1, 13]

Ze všeho nejdříve si útočník svoji oběť vytipuje, prohlíží různé profily lidí ve svém preferenčním rozmezí, navštěvuje různá diskusní fóra orientovaná na mládež. Rizikovou skupinou jsou adolescenti, děti a dospívající s nízkou sebedůvěrou a sebeúctou, děti s emociálními problémy, a naivní, či přehnaně důvěřivé děti. Útočník si vybírá více obětí pro zvýšení šance úspěchu. Stejně tak má útočník více profilů s falešnými identitami, které mohou být vzájemně propojené (spřátelené) pro vytvoření větší důvěryhodnosti. Tyto profily mohou být odhalitelné díky chybám, které jsou již popsány výše. Vodítkem například také může být datum založení profilu, počet a složení přátel (přátele jednoho pohlaví a věku), upravené až umělé fotografie, či fotografie pouze z jedné série. [1, 13, 31]

Druhou fází je oslovení oběti, které probíhá pod nějakou záminkou. Tou mohou být společné zájmy, společní přátelé, škola apod., nebo dvojsmysly typu: „Pěkné fotky, sluší ti to. Škoda že na nich není vidět víc.“ [13]

Třetí etapou kybergroomingu je již zmiňované vyvolání důvěry. Pachatel se staví do pozice kamaráda dítěte či mladistvého, většinou je jeho falešná

identita založena na roli vrstevníka oběti. Využíván je efekt zrcadlení. Útočník řeší s obětí její problémy, dává ji rady a pocit, že ji rozumí, případně řeší údajné stejné problémy nebo má stejné zájmy, což dává oběti pocit sounáležitosti. Informace, které pachatel využívá jsou ve většině případů informace, které oběť sama sdílí. [1, 13, 31]

K vybudování vztahu s obětí mohou kybergroomeři využít ve čtvrté fázi procesu i jisté motivační prostředky. Jednat se může např. o finanční odměnu (dobití kreditu, hotovost, koupě nového telefonu, lístků na koncert atd.), nabídku setkání se slavnými osobnostmi, či nabídku pomoci s něčím, co sama oběť nezvládne. Často pachatel za odměny požaduje od oběti protislužbu v podobě intimních fotografií nebo nahotu na webkameře, osobní schůzku, ovšem někdy mají různé nabídky úplatků v oběti pouze vyvolat pocit, že protistraně na ni záleží. Opírá se o smyšlené tvrzení, že má bohaté rodiče, nebo velmi dobře placenou práci. [1, 13]

Další etapou je příprava na osobní setkání. Kybergroomer si dává záležet na izolování oběti od jejího okolí, ujišťuje se, že oběť o jejich konverzaci bude zachovávat mlčenlivost. Nabádá ji k udržování „jejich tajemství". Zároveň se pachatel snaží v oběti vyvolat emoční závislost na jeho osobě, oběti často lichotí, dává ji pocit vlastní důležitosti. Navázaný ať už kamarádský či milostný vztah se stává pro oběť velmi důležitým. Především děti a dospívající se mohou do manipulátora zamilovat dokonce pouze na základě základních informací, a jsou ochotni udržovat vztahy na dálku. Častým jevem je i snižování zábran oběti zaváděním intimních a sexuálních témat do konverzace. U mladistvých mezi 13 a 18 rokem života vystupuje do popředí zájem o sexuální témata, různé materiály s erotickou tématikou či první sexuální kontakty, nebo i touha po lásce a porozumění opačného pohlaví. Přistoupí-li oběť k výměně

sextingových snímků, získává pachatel materiál k vydírání oběti, která v tomto případě zpravidla nepožádá o pomoc žádnou dospělou osobu. [1, 13, 31]

Předposlední etapou kybergroomingu je nabídka samotného osobního setkání, o které útočník celou dobu usiloval. Útočník může svoji oběť pozvat do kina nebo na procházku, často i do vlastního bytu. Nejčastěji se ale jedná o místa volena tak, aby oběť neměla velkou možnost úniku či dovolání se pomoci. Může se jednat o různé opuštěné objekty, uzamčené budovy, sklepy, auto či místa v přírodě s malou frekventovaností. V případě že oběť stále osobní setkání odmítá, může jej kybergroomer začít vydírat již získaným materiálem, a ke schůzce oběť nátlakem donutit. [13, 31]

Poslední fází je samotná osobní schůzka oběti a útočníka, která může mít několik scénářů. Od těch úplně nevinných až po ty se sexuálním napadnutím dítěte, nucením k výrobě pornografie či prostituci, opakovaném zneužití či zabitím oběti. V případě výrazného věkového rozdílu oběti a pachatele je útočníkem využita technika překonávání věkového rozdílu. Pachatel se může vydávat za rodiče virtuálního kamaráda oběti, staršího sourozence, či známého. [13, 31]

Následky takového osobního setkání mají na oběť obrovský, lze říct celoživotní dopad. Oběť může mít řadu psychických následků, mezi které patří depresivní až sebevražedné tendence, disharmonický vývoj osobnosti, ztráta citu pro morální hodnoty, sklony k rizikovému chování, problémy v budoucím sexuálním životě, aj. Bohužel většina obětí si svoji zkušenost nechává pro sebe, nehlásí ji, a nevyhledá potřebnou odbornou pomoc. [13, 31]

Nejčastějšími oběťmi kybergroomerů jsou děti ve věku od 11 do 17 let, dle statistiky již zaniklé stránky Lidé.cz z roku 2013 se v 56 % jedná o dívky, a v 44 % o chlapce. [13]

3.6.4 Kyberstalking

Pojmem kyberstalking označujeme opakované a stupňující se obtěžování, pronásledování, při které útočník využívá informační a komunikační technologie. Jedná se o dlouhodobé, opakované kontaktování oběti, jehož cílem je vyvolání strachu oběti o vlastní osobu nebo o osoby blízké. Stalking v kyberprostoru je pro pachatele snazší než v reálném životě, jelikož sama oběť o sobě sdílí dobrovolně spoustu informací, a zároveň lze na sociálních sítích jednoduše navázat kontakt. [13, 32, 33]

Může se jednat o různé pachatelem zasílané nevyžádané SMS zprávy, e-mail, telefonáty, zprávy na messengerech, komentáře pod příspěvky na sociální síti oběti, aj. Kyberstalkeři jsou vytrvalí a postupují systematicky, mají vytvořených několik falešných identit, pod kterými kontaktují oběť. Mají různé motivy pro svoje počínání, mezi které patří: obtěžování, vyhrožování a vydírání oběti; poškození oběti před společností; demonstrace vlastní síly; opětovné navázání vztahu (ex-partneři). [1, 13, 32, 33]

Obsah zpráv zasílaných kyberstalkerem oběti je leckdy příjemný a veselý, ovšem může se jednat o zprávy zastrašující, urážející a nepříjemné. Časté jsou i případy, kdy se zprávy ze začátku jeví příjemné, ale postupně přechází do nepříjemné formy, kdy se útočník snaží svoji oběť donutit ke kontaktu vydíráním, nadávkami či vyvoláváním pocitu viny. [34]

Časté je propojení kyberstalkingu s klasickým slakingem, kdy pachatel fyzicky pronásleduje oběť, zároveň kontaktuje oběť, dává ji najevo, že ví, co dělá, kde se v současné době nachází, co má na sobě apod. Pachatel často oběti vyhrožuje fyzickým násilím, či zabitím, nebo ublížením blízké osobě oběti. V těchto případech je vysoké riziko napadení, či vraždy vyšší než u pouhého kyberstalkingu. [34]

Typickým projevem kyberstalkingu je již zmiňované poškození reputace oběti. Pachatel se pomocí šíření nepravdivých informací snaží oběť očernit před jejím okolí. Konat tak může pomocí komentářů, přidáváním příspěvků na profil oběti, rozesíláním zpráv, ale i vytvořením falešné stránky, kde sdílí nepravdivé informace o oběti. [34]

Od roku 2010 lze legislativně kyberstalking a stalking po splnění jistých podmínek brát jako trestný čin, který je ukotven v trestním zákoníku, § 354 Nebezpečné pronásledování. [1, 13]

3.6.5 Sexting

Jednou z podob populárního nebezpečného chování na sociálních sítích je tzv. sexting. Jedná se pojem složený ze slov sex a texting, který označuje elektronické rozesílání zpráv, fotografií, či videí se sexuální tématikou. Výměna takových materiálů se může uskutečňovat mezi partnery, ale i mezi naprosto neznámými osobami. V obou případech se jedná o rizikovou činnost, kdy odesílatel ztrácí kontrolu nad tímto obsahem. Sexting je v mnoha případech propojen s kybergroomingem, kdy útočník získává kompromitující materiál, kterým lze oběť vydírat, jedná se o tzv. eskalovaný sexting. Eskalace sextingu probíhajícího mezi dospělými partnery může dojít do fáze, kterou lze označit jako revenge porn, porno pomstu, jež může nastat po ukončení vztahu partnerů. V případě osob do 18 let se ovšem jedná o šíření dětské pornografie. [1, 13, 31]

Ačkoliv může být odesílatel protějškem ubezpečen, že se sextingový materiál nedostane dále k třetí straně, není zde nikdy jistota. Především obrazový materiál může být šířen dále, díky čemuž dochází k dehonestaci oběti. Ve veřejném kyberprostoru mají takové materiály dlouhodobou životnost a téměř není možné je smazat. [13]

Nejzávažnější forma sextingu je sexting s nezletilými osobami, který lze klasifikovat, jak už bylo výše zmíněno, jako šíření dětské pornografie, či jako ohrožování mravní výchovy. Přesto, že je v České republice pohlavní styk zákonem povolen od 15 let, nesmí být do 18 let věku pořizovány žádné intimní materiály. V tomto případě se i nezletilá osoba, která pořizuje a rozesílá vlastní intimní materiál, stává výrobcem a šiřitelem dětské pornografie. Výroba a šíření dětské pornografie je zakořeněna v zákoně č. 40/2009 Sb., trestního zákoníku, § 192 Výroba a jiné nakládání s dětskou pornografií. [13, 31]

Z výzkumu v roce 2014 bylo zjištěno, že zhruba 70 % dětí považuje sexting za rizikový, přesto přibližně 18 % dětí ve věku 17 let a 5,5 % dětí ve věku 12 let již své sextingové materiály rozesílá. V českém prostředí dle zdrojů z roku 2018 publikovalo svoje intimní materiály 10 % dětí, a 35 % dotazovaných dětí uvedlo, že byly příjemcem textových zpráv se sexuální tématikou. [31]

3.6.6 Kyberšikana

Kyberšikana, anglicky Cyberbullyin, lze označit chování osoby vůči jiné osobě, které má za cíl ublížit, zastrašit, vyvézt z rovnováhy či jej jinak ohrozit, za použití informačních technologií. Kyberšikana stejně jako tradiční šikana je na dlouhodobé bázi a zahrnuje opakované jednání. Dalším společným znakem s tradiční šikanou je nepoměr mezi sílí oběti a útočníka, a vnímání dění obětí jako nepříjemné a ubližující. [1, 13, 35]

Virtuální svět poskytuje k využití útočníkovi nástroje a prostředky, díky nimž je možné napadat oběť opakovaně i přes geografické vzdálení se oběti. Tento fakt může mít na oběť větší dopad než v případě tradiční šikany. Mezi nejčastější projevy kyberšikany patří: pomlouvání, urážení, ztrapňování a zastrašovaní přes sociální sítě; pořizování fotografií, videozáznamu či zvukových záznamů a jejich následné sdílení na sociálních sítích se záměrem veřejně zesměšnit

či poškodit oběť; pořizování různých záznamů, kde dochází k fyzickému napadání obětí, a jejich následné sdílení na internetu; vytváření internetových stránek či účtů využívaných k poškozování oběti; vyhrožování a vydírání pomocí internetu; aj. Kombinace kyberšikany a tradiční šikany není ničím výjimečným. [1, 13, 35]

Samotná kyberšikana není dle zákona trestným činem ani přestupkem, ovšem trestat ji lze dle charakteru útoku, např. jako ublížení na zdraví (§ 146 trestního zákoníku), vydírání (§ 175 trestního zákoníku), či jako již jednou zmiňované nebezpečné pronásledování (§ 354 trestního zákoníku). [1]

Dle české části projektu EU Kids Online II, který probíhal v letech 2011–2014, zažilo 8 % českých dětí ve věku od 9 do 16 let alespoň jednu z forem kyberšikany, což je o 2 % více než je Evropský průměr. [35]

3.7 Děti a dospívající na internetu

Používání chytrých telefonů, notebooků, tabletů, či jiných zařízení, ze kterých je možné se připojit k internetu, je v dnešní době u dětí nepsaných standardem. Důvodem toho může být fakt, že se v současné době rodí děti do světa, kde si již život bez chytrých zařízení leckdo neumí představit. Děti a dospívající používají chytrá zařízení nejen k přístupu k internetu, ale i k zábavě, hraní her, či k vzájemnému kontaktu se svými vrstevníky. V podstatě chtějí být „vždy online“. [35]

Dle statistiky Českého statistického úřadu z roku 2012 využívá internet přibližně 69 % české populace, kdy ve věku 16-24 let jej využívá 96 % dospívajících. Statistika z roku 2008 zase uvádí, že ve věkové skupině 12-18 let využívalo internet přibližně 93 % dětí. Ovšem dnes mohou být tato čísla ještě vyšší. Česká část výzkumu projektu EU Kids Online IV z roku 2018 uvádí, že 84 %

českých dětí ve věku 9-16 let se připojuje denně k internetu z mobilu, z toho 29 % je stále online. [35, 36]

Co se týče času stráveného dětmi a dospívajícími na internetu, 35 % respondentů české části výzkumu EU Kids Online IV odpovědělo, že tráví během všedního dne na internetu více jak 4 hodiny denně, 9 % více jak 7 hodin. O víkendu se trendy pohybují výše, více než 4 hodiny denně tráví na internetu 51 % respondentů, 7 a více hodin pak 22 % dotazovaných mladistvých. Sociální sítě alespoň jednou týdně navštěvuje 81 % dětí a dospívajících, 70 % je navštěvuje denně. [36]

Negativní zkušenost s používáním internetu uvedlo celkově 36 % dotazovaných dětí a dospívajících, ve věkové kategorii 15-17 let se jednalo o 50 % respondentů. 29 % dětí a dospívajících uvedlo, že se alespoň jednou měsíčně na internetu setkalo se sexuálně explicitními materiály. Zprávu se sexuálním obsahem obdrželo 35 % dotazovaných, 10 % zveřejnilo nebo odeslalo zprávu se sexuálním obsahem. Od 25 % dotazovaných se někdo snažil získat intimní informace. [36]

Mezi dětmi a dospívajícími je časté seznamování přes internet. V České republice má zkušenost s komunikací přes internet s neznámým člověkem 49 % dotazovaných osob ve věku 9-17 let. Na osobní schůzku s neznámým člověkem z internetu šlo 23 % nezletilých, z toho 2 % uvedla, že ze schůzky byla hodně rozhozena. V 7 % případů se jednalo o schůzku s dospělou osobou. [36]

3.8 Disinhibiční efekt „online“

Nástrahy a rizika číhající na děti a dospívající na internetu byly popsány v předchozích kapitolách. Disinhibiční efekt je ovšem riziko, které si každý uživatel nevědomky podvědomě vytváří sám. Jedná se o *„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.“ [39, s. 272] Tento efekt má za následek sdílení více důvěrných a intimních informací než v reálném světě, je k vidění téměř u všech uživatelů sociálních sítí či různých diskusních fór, a pramení ze šesti hlavních zdrojů. [39, 40]

Obrázek 2 - Zdroje disinhibičního efektu [40]

Jedním ze zdrojů disinhibičního efektu je anonymita, která dává uživateli pocit ochrany při projevování se na internetu. Uživatel skrytý za svojí přezdívkou nabývá přesvědčení, že jeho chování v rámci kyberprostoru bude bez jakýchkoliv následků či postihu. Tento pocit podporuje i další zdroj, neviditelnost. Uživatel na druhé straně internetu nemá možnost vidět momentální nonverbální reakci a mimiku uživatele. Díky asynchronicitě

si uživatel může promyslet svoji odpověď a odpovědět později. U některých uživatelů často dochází i potlačení, či minimalizaci autority, kdy kohokoliv na internetu vnímají jako sobě rovného, bez ohledu na reálný společenský status či postavení osoby. [40]

Solipsistická introjekce je pojmenování pro jev, při kterém lidská mysl, díky absenci komunikace tváří v tvář, vytváří vlastní obraz, představu člověka, se kterým jedinec komunikuje. Tato představa je utvářena na základě vlastních potřeb a očekávání, což vede k tomu, že jedinec z části komunikuje sám se sebou. Někteří uživatelé mohou své Já pohybující se na internetu chápat jako další osobnost kterou stvořili, jako jinou osobu, za kterou nenesou odpovědnost v reálném světě. Jejich odpovědnost za tuto osobu končí v momentě, kdy vypnou počítač. [40]

3.9 Dospívání dětí

Dospívání, neboli adolescence, je období druhé dekády života a vývoje jedince. Jedná se o přechod mezi dětstvím a dospělostí, kdy dochází ke komplexní proměně osobnosti, a to k psychické, tělesné a sociální. Probíhá ve věku od 10 do 20 let. Jedinec nacházející se v tomto zajímavém období hledá vlastní identitu, přehodnocuje svoje názory a postavení vůči společnosti, uvědomuje si prožívání, jak komunikuje s ostatními, či jak smýšlí. Velký vliv v dospívání jedince hrají společenské a kulturní podmínky, požadavky a očekávání společnosti. Adolescence je pro jedince náročným obdobím, kdy se musí vyrovnat s fyzickou proměnou vlastního těla, psychickou proměnou, proměnou ve vztahu sám k sobě, ale i ve vztahu k ostatním lidem, a zároveň si vydobýt přijatelné společenské postavení. Charakteristickými znaky období adolescence jsou nejistota, pochybnosti o vlastních dovednostech, kompetencích a postavení ve společnosti, ale i ochota v některých oblastech života experimentovat. [37, 38]

Díky pokládání si otázek a zároveň odpovídání na ně si jedinec vymezuje svoje názory, a tím celkově utváří svoji osobnost. Vstřebává do sebe získané informace a zkušenosti, prožité důležité události a pocity, které si s sebou nese celý život. V tomto období jedinec současně prochází fází pubescence, která je z pohledu dospělých složitá k pochopení chování dospívajícího. Ačkoliv dospělý člověk má již zkušenosti s vlastní adolescencí, může mít problém porozumět dospívání dalšího jedince především z důvodu proměny společnosti. Adolescence dnešních jedinců se díky vlivu změn společenských hodnot, životního stylu, či sociální a morální normy značně liší od dospívání předešlých generací. [38]

Celé období od 10. do 20. roku života lze nazývat dospíváním, ovšem při porovnání 12letého a 18letého adolescenta uvidíme zásadní rozdíly, proto lze adolescenci členit do tří fází: časná adolescence, střední adolescence a pozdní adolescence. Každá fáze adolescence má vlastní charakteristické znaky. [37, 38]

3.9.1 Časná adolescence

Časnou adolescencí je nazváno období dospívání jedince ve věku 10-13 let. Projevují se první pubertální znaky tělesného dospívání, tedy začíná fáze pohlavního dozrávání jedince, která později pokračuje i ve fázi střední adolescence. Výskyt sekundárních pohlavních znaků zapříčiňuje u jedince zvýšený zájem o vrstevníky opačného pohlaví. Objevují se první problémy ve vztahu dítě-rodič. [37, 38]

3.9.2 Střední adolescence

Období od 13 do 15 let věku je zásadním při hledání a utváření si vlastní identity. Jedinec se pokouší jistými způsoby odlišovat od společnosti. Příkladem může být styl oblékání, či preference poslechu specifického stylu hudby.

Na rozdíl od časné adolescence v období střední adolescence není jedinec zcela schopen regulace svého chování, proto prochází změnami, které si do jisté míry způsobil sám. Dospívající má potřebu větší svobody rozhodování, která má za následek vyšší míru odpovědnosti, ale i ztrátu pocitu jistoty. Rozvojem kompetencí dospívající ujišťuje sebe i ostatní o své nezávislosti, čímž se kompenzuje jeho pocit nejistoty. [37, 38]

3.9.3 Pozdní adolescence

Poslední fáze adolescence probíhá ve věku od 15 do 20 let, a je obdobím komplexnější psychosociální proměny. Na jejím počátku dochází k pohlavnímu dozrání jedince a často i k prvnímu pohlavnímu styku. Mění se osobnost i společenská pozice dospívajícího především v následku ukončení profesní přípravy a nástupem do zaměstnání či k dalšímu studiu. Vztahy s rodiči se opět stávají stabilními, rozvíjí se vztahy s vrstevníky, vznikají partnerství. Na základě sdílení stejných hodnot vzniká příslušnost k sociálním skupinám, což uspokojuje potřebu někam patřit. [37, 38]

Důležitým znakem je uvědomění si možnosti ovládat vlastní život, ale i ochota experimentace s různými způsoby chování a sebevymezení. Dospívající také často přemýšlí nad svými plány a cíli do budoucna, které jsou důležité pro to, jak se dospívající ujme své role dospělého jedince. Rozhodujícími mohou být faktory, mezi které patří např. následné studium na vysoké škole, ekonomická samostatnost, nastávající rodičovství, nebo přetrvávající bydlení u rodičů. [37, 38]

3.10 Sexuální zneužívání dětí

Sexuální zneužívání dětí, které se také označuje jako CSA syndrom (Child Sexual Abuse), je fenoménem, kterému se začíná věnovat více pozornosti než dříve, ačkoliv dle statistik nepřibývá nahlášených případů. Bohužel

je nahlášen, či odhalen jen zlomek skutečných případů zneužívání dítěte. Sexuální zneužívání je také zároveň součástí syndromu zneužívaného a týraného dítěte, který je označován jako CAN syndrom (Child Abuse and Neglect), zahrnující také psychické a fyzické týrání, šikanování, systémové týrání, šikanování, zanedbávání, sekundární viktimizaci a Münchhausenův syndrom by proxy. [41]

Dle usnesení Rady Evropy z roku 1992 sexuální zneužívání dětí lze definovat jako *„nepatřičné vystavení dítěte pohlavnímu kontaktu, činnosti či chování. Zahrnuje jakékoli pohlavní dotýkání, styk nebo vykořisťování kýmkoliv, komu bylo dítě svěřeno do péče anebo kýmkoli, kdo dítě zneužívá. Takovou osobou může být rodič, příbuzný, přítel, odborný či dobrovolný pracovník či cizí osoba. Sexuální zneužívání se dělí na bezdotykové a dotykové. Bezdotykové zneužívání zahrnuje např. setkání s exhibicionisty a účast na sexuálních aktivitách, kde nedochází k žádnému tělesnému kontaktu, např. vystavování dítěte pornografickým videozáznamům. Kontaktní zneužívání je takové, kde dochází k pohlavnímu kontaktu, včetně laskání prsou a pohlavních orgánů, pohlavnímu styku, pohlavnímu styku orálnímu nebo análnímu.“* [42, s.72]

Za bezdotykové sexuální zneužívání dítěte lze považovat setkání s exhibicionistou, který před dítětem či dospívajícím obnažuje své genitálie či masturbuje. Dále do této kategorie lze zařadit také další sexuální aktivity, při kterých nedochází k tělesnému kontaktu, např. voyerismus, harassment, nucení dítěte k pořizování pornografických snímků, či k prohlížení pornografických časopisů. Do této kategorie lze začlenit tedy případy sexuálního zneužívání na sociálních sítích, které nepřerostly do fyzické formy. [43, 44]

Dotykové sexuální zneužívání zahrnuje obtěžování, kdy je dítě osahováno na erotogenních zónách, nepenetrační sexuální zneužívání, při kterém dochází

k dotýkání se genitálů, či prsou různými předměty, genitálem nebo rukou, ale i k líbání či k žádosti o masturbaci. Dále jakákoliv penetrace do vagíny, úst a konečníku. V neposlední řadě rozhodně i znásilnění, či incest. [43, 44]

Další zvláštní formou je komerční sexuální zneužívání, kdy je dítě použito pro sexuální účely výměnou za finance či jinou formu odměny. K takovému „obchodu" může docházet mezi dítětem a pachatelem, ale i mezi dítětem zákazníkem a prostředníkem, který tímto způsobem na dítěti vydělává. [43]

3.11 Příznaky sexuálního zneužívání

Projevy příznaků sexuálního zneužívání dítěte se liší dle věku dítěte, ale obecně lze říct, že vždy se jedná o změnu jeho chování. Společným znakem u všech dětí a mladistvých je fakt, že se bojí svoji velice bolestivou a psychicky náročnou zkušenost pojmenovat, svěřit se s ní další osobě a vyhledat pomoc. [41, 45]

U zneužitého dítěte lze pozorovat psychické příznaky, kterými jsou: strach, úzkost, deprese, agrese, afektivní chování, nebo přehnané udržování čistoty. Příznakem mohou být i výkyvy koncentrace, výkonnosti, zhoršení prospěchu, ale i stranění se vlastních vrstevníků a celkově ostatních osob, nebo vyhýbání se konkrétním lidem. Fyzickým příznakem mimo jistých známek poranění mohou být nevolnosti až zvracení, poruchy příjmu potravy, ale i přejídání. [41, 45]

Děti středního školního věku mohou mimo výše popsaných příznaků vykazovat i další příznaky, ke kterým patří např. sebepoškozování, suicidální tendence nebo naopak sexuálně laděné hry. U mladistvých se může jednat o zvýšené sexuální chování, prostituci, abúzus drog a alkoholu, suicidální pokusy, či útěky z domova. [45]

3.12 Následky sexuálního zneužívání

Následky zneužívání jsou promítány do celého života oběti. Jejich míra závisí na tom, v jakém věku začalo zneužívání dítěte, jak dlouho trvalo, a jaká byla vazba mezi dítětem a pachatelem. Pokud zneužívání začalo již v raném věku dítěte, dopady na jeho pozdější život jsou ve většině případů větší, ovšem u každé oběti je to individuální. U obětí se v průběhu života projevuje depresivní ladění, narušení morálních hodnot, disharmonický vývoj osobnosti, poruchy chování, rizikové chování, nízké sebehodnocení, nenávist k vlastnímu tělu, odpor k sexuálnímu styku, či odpor k tělesné blízkosti s další osobou, což vede k problému navázat zdravý partnerský vztah. Oběť se také stává zranitelnější, což v dospělosti může vést k opakované zkušenosti se sexuálním zneužíváním. [41, 44]

3.13 Prevence a protiopatření zneužívání nezletilých osob na sociálních sítích

Nejdůležitějším a základním článkem prevence zneužívání nezletilých osob na sociálních sítích je zajisté rodina, na kterou v prevenci navazuje škola, či další organizace. Každý by měl alespoň částečně připravit dítě na rizikové situace, se kterými se může v kyberprostoru potkat. Pro prevenci vycházející od rodiče je zcela jistě zásadní komunikace a vzájemná důvěra ve vztahu rodiče a dítěte. Prevence ze strany rodiče by měla být pozitivní, tzn. že pokud rodič upozorní dítě na konkrétní rizikovou situaci, měl by dítěti nabídnou různá možná řešení. [55]

Hlavním tématem prevence rodičů je seznamování se v online prostředí a komunikace dítěte s neznámými lidmi. Zde je nutné dětem a dospívajícím vysvětlit, že ne každý neznámý člověk je na internetu hrozbou, ale i tak by dítě

mělo ke seznamování přistupovat obezřetně. Rodič by měl dítě naučit jaké informace lze sdílet, a které nikoliv, aby bylo dítě v bezpečí, a stejně tak upozornit na kterých stránkách je zvýšené riziko, že dítě narazí na predátora. [55]

Nastavení jednotlivých bezpečnostních zásad by se mělo odvíjet od věku a mentální úrovně dítěte. Pravidla vhodná pro děti mladšího školního věku již nejsou vhodná pro starší děti, tzn. že je vhodné v přibývajícím věkem dítěte opatření ubírat, a dát mu pocit, že mu důvěřujeme. [55]

Různé rady, jak s dětmi o této problematice hovořit, jak je připravit, či jaké lze využít bezpečnostní opatření, nabízí spousta informačních webů zabývající se tématikou bezpečného internetu pro děti, či přímo tématikou prevence zneužívání nezletilých osob v prostoru sociálních sítí. Jednou z nabízejících se možností jsou tzv. rodičovské zámky či aplikace rodičovské kontroly, kterých je v dnešní době nepřeberné množství, a mají různé funkce, od nastavení povoleného času stráveného na internetu, až po filtrování obsahu. Např. Google Family Link, Microsofr Family Safety, nebo Norton Family. [55, 56, 57, 58]

Obrázek 3 - Logo Google Family Link [59]

Obrázek 4 - Logo Norton Family [60]

3.14 Osvěta

3.14.1 V síti

Jednou z nejvýraznějších osvětových kampaní probíhající v České republice byl zajisté film V síti, jehož tvůrci jsou Vít Klusák a Barbora Chalupová. Jedná se o experimentální dokumentární film, který se zaobírá tématem zneužívání dětí na sociálních sítích. Tři mladě vypadající dospělé herečky se na sociálních sítích vydávaly za dvanáctileté dívky, dopisovali s muži všech věkových kategorií, kteří je aktivně oslovovali. V drtivé většině se jednalo o tzv. predátory. Film divákovi zprostředkovává zkušenost mladých dívek s predátory, kteří po svých obětech požadovali sex přes webkameru, či nahé snímky, nebo naopak zasílali své nahé snímky, či odkazy na pornografii. V nejednom případě byly dívky vydírány. V rámci experimentu se tyto tři dívky pod dohledem ochranky s některými predátory setkaly tváří v tvář na osobních schůzkách. [46, 47]

V rámci natáčení dokumentu si tří dívky, z prostředí kulisami vytvořených tří dětských pokojíčků, dopisovaly s 2458 potencionálními predátory.

Natáčení probíhalo pod dohledem ředitelky Linky důvěry, právníka, sexuoložky a psycholožky. Na základě dokumentu bylo zahájeno několik trestních stíhání predátorů. Vznikly dvě verze filmu, V síti a V síti: Za školou. V síti je standardní distribuční verze přístupná od 15 let. V síti: Za školou je verze pro diváky od 12 let, a zároveň verze pro školní projekce, které fungují jako osvěta přímo pro děti ve školách. [46, 47]

V rámci projektu fungují webové stránky V síti (www.vsitifilm.cz), na kterých lze najít rady pro děti, jak být na internetu v bezpečí, rady pro rodiče, pedagogy, ale i pro osoby, které by mohly být potencionálními predátory. Dále si zde lze najít film online ke shlédnutí, objednat školní projekci, či kontaktovat odbornou pomoc. [46]

Obrázek 5 - Plakát filmu V síti [48]

3.14.2 Buď safe online

Buď safe online je osvětový projekt pod záštitou MŠMT, který vznikl v roce 2018. Jedná se o spolupráci společnosti Avast a influencera Jiřího Krále. V rámci programu společnost a Jiří Král pořádali na školách sérii přednášek

na téma bezpečného internetu. V roce 2020 byl na webu projektu spuštěn online kurz, který edukuje děti, jak správně zvládnout konkrétní situace na internetu. Na webu projektu, mimo online kurzu pro děti, lze také nalézt rady pro rodiče či pedagogy. [49]

3.14.3 #SayNo!

Kampaň #SayNo!, česky #ŘekniNe!, je projektem evropského policejního úřadu Europol z roku 2017, jehož úkolem je varovat před nárůstem případů sexuálního zneužívání a vydírání dětí na internetu. V rámci kampaně vzniklo video, které je k dispozici ve 29 evropských státech, znázorňující dívku a chlapce, kteří jsou vykořisťováni zločineckou organizací za účelem finančního zisku, a sexuálním delikventem hledajícím další pornografický materiál. Dále video obsahuje rady, jak se nestát obětí, či jak vyhledat pomoc. [50, 51]

3.14.4 Den bezpečnějšího internetu

Den bezpečnějšího internetu, anglicky Safer Internet Day, je celosvětová kampaň, na které se v České republice podílí Ministerstvo vnitra společně s Policií ČR, zaměřená na prevenci kriminality v kyberprostoru. Projekt začal v roce 2004 jako inciativa projektu EU SafeBorders, později byl převzat sítí Insafe. Insafe je evropská sít center pro bezpečnější internet, realizující osvětové a vzdělávací kampaně, a provozující linku pomoci. V dnešní době projekt probíhá přibližně ve 200 zemích světa. [52, 53]

V roce 2022 tento den vycházel na 8. února, a jednalo se již o 19. ročník projektu. V rámci projektu Policie ČR vydala několik krátkých instruktážních videí na téma internetové bezpečnosti, která se týkají nejen prevence kriminality na sociálních sítích páchané na dětech, ale i zabezpečení účtů a rad pro rodiče. [53, 54]

3.15 Informační weby

Jak již bylo výše zmíněno, na internetu lze nalézt poměrně mnoho webových stránek zabývající tématikou bezpečného internetu pro děti a dospívající, problematikou kybernetické kriminality, a především prevencí kyberkriminality páchané na dětech. Na těchto stránkách se lze dočíst o možnostech prevence, či případně jak řešit již vzniklé problémy. Jsou zde umístěny i kontakty na odbornou pomoc, na různé organizace řešící tuto problematiku. V některých případech se jedná přímo o informační weby konkrétních nadací. Mezi tyto informační weby patří např.: E-bezpečí (www.e-bezpeci.cz), Safer Internet (www.saferinternet.cz), Internetem bezpečně (www.internetembezpecne.cz), Jak na internet (www.jaknainternet.cz), Bílý kruh bezpečí (www.bkb.cz), či Nadace Naše dítě (www.nasedite.cz).

3.16 Právní kontext kybernetické kriminality páchané na dětech

České právní normy ve vztahu k internetové trestné činností páchané na dětech:

- Zákon č. 218/2003 Sb., zákon o soudnictví ve věcech mládeže
- Zákon č. 110/2019 Sb., o zpracování osobních údajů
- Zákon č. 205/2017 Sb., o kybernetické bezpečnosti
- Zákon č. 40/2009 Sb., trestní zákoník
    - § 144 Účast na sebevraždě
    - § 150 Neposkytnutí pomoci
    - § 175 Vydírání
    - § 180 Neoprávněné nakládání s osobními údaji
    - § 181 Poškození cizích práv
    - § 184 Pomluva

- § 186 Sexuální nátlak
- § 187 Pohlavní zneužití
- § 191 Šíření pornografie
- § 192 Výroba a jiné nakládání s dětskou pornografií
- § 193 Zneužití dítěte k výrobě pornografie
- § 193a Účast na pornografickém představení
- § 193b Navazování nedovolených kontaktů s dítětem
- § 202 Svádění k pohlavnímu styku
- § 203 Beztrestnost dítěte
- § 209 Podvod
- § 353 Nebezpečné vyhrožování
- § 354 Nebezpečné pronásledování
- § 364 Podněcování k trestnému činu
- § 365 Schvalování trestného činu
- § 367 Nepřekažení trestného činu
- § 368 Neoznámení trestného činu [61]

4 METODIKA

Pro zpracování praktické části diplomové práce byla využita metoda smíšeného výzkumu, tedy kombinace kvalitativního a kvantitativního výzkumu. Data byla získávána pomocí polostrukturovaného rozhovoru vedeného s vyučujícími druhého stupně základních škol, vyučujícími odpovídajících tříd víceletého gymnázia a rodiči. Zjištěná data byla následně analyzována pomocí popisné statistiky.

4.1 Polostrukturovaný rozhovor

Jak již bylo výše řečeno, v diplomové práci byl použit polostrukturovaný rozhovor s vyučujícími a rodiči. Otázky rozhovoru byly sestaveny způsobem, který umožnil získání i kvantitativních dat, která mají vypovídající hodnotu pouze pro tuto práci a nelze jim připisovat globální význam. Jednotlivé zkoumané otázky, jež byly řešeny v rozhovorech jsou uvedené v přílohách této práce.

Výzkumné šetření probíhalo od 13. dubna 2022 do 2. května 2022. Rozhovory s rodiči nezletilých osob probíhaly v domácím prostředí respondentů. S vyučujícími v prostorech základních škol, či gymnázií, a prostřednictvím video rozhovorů pomocí šifrované aplikace. V případech, kdy rozhovory s respondenty z řad vyučujících probíhali prostřednictvím video hovoru z jejich domovského prostředí, byli respondenti více klidní a ochotnější zodpovídat doplňující otázky. Naopak při některých rozhovorech v prostředí škol byli respondenti lehce nervózní a více „vážili svá slova“. Někteří z oslovených vyučujících rozhovory odmítli z důvodu nedůvěry k rozhovorům, nahrávání rozhovoru a pozdějšímu přepisu.

Každý respondent byl nejdříve obeznámen s tématem a způsobem výzkumu. Dále proběhlo seznámení s budoucím průběhem rozhovoru a jeho možnostmi, mezi které patřilo například rozhovor bez udání důvodu předčasně ukončit. Následně byly představeny jednotlivé položky informovaného souhlasu a vysvětlen proces nakládání s daty a jejich uchovávání. Respondent byl ujištěn o zachování jeho anonymity ve výzkumu. Informovaný souhlas je součástí příloh práce.

Doba trvání rozhovoru byla u každého respondenta odlišná, průměrně ovšem rozhovor trval od 10 do 30 minut. Rozhovory byly nahrávány na diktafon, později byly pro přehlednější práci s daty přepsány do počítače. Získaná data byla statisticky zpracována a podrobena obsahové analýze.

Výzkumné rozhovory byly provedeny s 15 respondenty z řad vyučujících, a 15 respondenty z řad rodičů.

4.2 Kritéria výběru respondentů

Výzkum v rámci praktické části diplomové práce se řídil kritériem, které bylo ukotveno v samotném zadání práce. V případě výběrů respondentů z řad vyučujících se jednalo o omezení výběru na vyučující druhého stupně základních škol, a vyučující odpovídajících tříd víceletých gymnázií. Rozhovory proto tedy byly vedeny s vyučujícími žáků ve věku od 12 do 15 let včetně.

Při výběru respondentů z řad rodičů bylo nastaveno kritérium věku dítěte, jehož hranice byly stejné jako v případě vyučujících, a to 12-15 let.

5 VÝSLEDKY

5.1 Vyhodnocení rozhovorů s rodiči

5.1.1 Otázka č. 1: Věk dítěte?

Tabulka 1 - Rodiče – Věk dítěte respondentů

Věk dítěte	Počet	Podíl
12 let	5	33 %
13 let	3	20 %
14 let	3	20 %
15 let	4	27 %

Otázka č. 1 zjišťovala věk dětí respondentů, který byl kritériem rozhovoru. Z celkového počtu respondentů uvedlo 33 % respondentů, že jsou rodičem dítěte ve věku 12 let, 20 % ve věku 13 let, 20 % ve věku 14 let, a 27 % ve věku 15 let.

5.1.2 Otázka č. 2: Navštěvuje Vaše dítě základní školu nebo víceleté gymnázium?

Tabulka 2 - Rodiče – Škola dítěte respondentů

Škola	Počet	Podíl
Základní škola	8	53 %
Víceleté gymnázium	7	47 %

Otázka č. 2 se dotazovala na typ školy, kterou dítě respondenta navštěvuje. Respondenti v 53 % uvedli základní školu, ve 47 % víceleté gymnázium. Procentuální podíl typů škol by v tomto případě téměř vyrovnaný.

5.1.3 Otázka č. 3: Pohlaví Vašeho dítěte?

Tabulka 3 - Rodiče – Pohlaví dítěte respondentů

Pohlaví dítěte	Počet	Podíl
Dívka	8	53 %
Chlapec	7	47 %

Tabulka 3 znázorňuje rozložení pohlaví dětí respondentů. V 8 případech, tedy 53 % se jednalo o dívky, v 7 případech, tedy 47 % o chlapce. V případě otázky č. 3 lze říci, že rozložení pohlaví dětí respondentů je také téměř vyrovnané.

5.1.4 Otázka č. 4: Má Vaše dítě přístup k internetu? Z jakých zařízení?

Otázka č. 4 zjišťovala, zda dítě respondenta má přístup k internetu. Kladná odpověď Ano zazněla od všech respondentů, tedy ve **100 %** případů.

Tabulka 4 - Rodiče – Zařízení dětí s přístupem k internetu

Zařízení	Počet	Podíl
Mobilní telefon	13	87 %
Notebook	7	47 %
Stolní PC	5	33 %
Tablet	5	33 %
Herní konzole	2	13 %

Pomocí doplňující otázky k otázce č. 4 bylo zjištěno, jak je znázorněno v tabulce 4, že mobilní telefon vlastní děti respondentů v 87 % případů. Druhé nejčastěji uváděné zařízení s přístupem k internetu, které děti vlastní byl notebook, který uvedlo 47 % dotazovaných. Dále 33 % respondentů uvedlo,

že jejich dítě má k dispozici stolní počítač, stejně tak tablet. Herní konzoli s přístupem k internetu vlastní 13 % dětí.

5.1.5 Otázka č. 5: Jak Vaše dítě získalo konkrétní zařízení?

Tabulka 5 - Rodiče – Způsob získání zařízení

Způsob získání zařízení	Počet	Podíl
Od rodičů	13	87 %
Vlastní koupě	3	20 %
Součást domácnosti	3	20 %

Otázka č. 5 zjišťovala, jak děti respondentů získali zařízení s připojením k internetu, která vlastní. 87 % dotazovaných uvedlo, že alespoň jedno zařízení dítě dostalo od rodiče. Rodiče své dítě v některých případech obdarovali zařízením z důvodu nutnosti, např. kvůli kontaktu s dítětem, které dojíždí do školy v jiné obci, nebo kvůli distanční výuce během pandemie COVID. Často se ovšem jednalo o dary k narozeninám, k Vánocům, jmeninám, či o odměnu za vysvědčení ke konci školního roku.

Případů, kdy si dítě alespoň jedno ze zařízení, které vlastní, zakoupilo samo, bylo 20 %. Jedno z dětí si zakoupilo svůj první mobilní telefon za peníze, které si postupně ušetřilo z darů k narozeninám od prarodičů, druhé dítě si stejným způsobem našetřilo na novější a modernější telefon, než který získalo darem od rodičů. V třetím případě se jednalo o domluvu s rodiči, kdy si dítě našetřilo polovinu částky a druhou doplatili rodiče.

Jako součást vybavení domácnosti označilo alespoň jedno zařízení 20 % dotazovaných rodičů. Zde se jednalo především o stolní počítače, ze kterých

má přístup k internetu celá rodina, ale i o notebooky, či mobilní telefony po starším sourozenci.

5.1.6 Otázka č. 6: Limitujete nějakým způsobem čas dítěte na internetu? Jak?

Tabulka 6 - Rodiče – Omezení času dítěte na internetu

Omezení času dítěte na internetu	Počet	Podíl
Ano	12	87 %
Ne	3	13 %

Na otázku č. 6 odpovědělo 13 % respondentů, že čas svého dítě na internetu žádným způsobem nelimitují. Kladně odpovědělo 87 % dotazovaných, kteří byli následně dotázáni, jakým způsobem své dítě limitují.

Tabulka 7 - Rodiče – Způsob omezení času dítěte na internetu

Způsob omezení	Počet	Podíl
Verbálně	8	67 %
Aplikačně	4	33 %

Většina dotazovaných rodičů, kteří odpověděli, že čas strávený dítětem na internetu nějakým způsobem omezují, 87 %, na doplňující otázku k otázce č. 6 odpověděla, že čas svého dítětem omezují verbálně (67 %). Ve dvou případech se jednalo o domluvu mezi rodičem a dítětem, kdy byla nastavena hranice stráveného času na maximálně 3 hodiny denně, v dalším případě mělo dítě přístup k internetu pouze v případě, kdy mělo splněné všechny povinnosti a domácí úkoly. V ostatních případech bývá dítě upozorněno, aby zařízení odložilo, či přímo vypnulo. Ovšem přibližně polovina rodičů, kteří své dítě

omezují verbálně, se shoduje na tom, že vždy není úplně lehké se s dítětem domluvit, a jeho čas na internetu 100 % ohlídat.

Respondentů, kteří uvedli, že používají různé aplikace k omezení času dítěte na internetu bylo celkem 33 %. Jeden z respondentů uvedl, že přístup k internetu ze zařízení dítěte povoluje jedině v případě, kdy má dítě hotové domácí úkoly. Další respondent zase uvedl, že je správcem Wi-Fi routeru, a v případě potřeby, kdy si dítě neplní své povinnosti, či se chová nevhodně, odpojí pomocí správcovské aplikace zařízení dítěte od Wi-Fi.

5.1.7 Otázka č. 7: Věříte svému dítěti při pohybu na internetu?

Tabulka 8 - Rodiče – Důvěra respondentů k pohybu dětí na internetu

Důvěra	Počet	Podíl
Ano	11	73 %
Ne	3	20 %
Nejsem si jistý	1	7 %

Důvěru k pohybu vlastního dítěte na internetu v otázce č. 7 potvrdilo 73 % respondentů. Jeden z dotazovaných rodičů uvedl, že dítěti věří, protože je i v jiných oblastech rozumný a spolehlivý.

Nedůvěru vyjádřilo 20 % dotazovaných. Jeden z těchto 3 respondentů by rád věřil svému dítěti, ale „člověk nikdy neví“. Další svému dítěti v této oblasti nedůvěřuje, protože by mohlo na internetu vyhledávat různé stránky, kam by dítě vůbec chodit nemělo, nebo kam by si rodiče nepřáli, aby chodilo. Poslední respondent uvedl, že se v dnešní době na internetu nachází spousta „toxických“ lidí, které by dítě nemělo poznat. Doplnil, že spíše nedůvěřuje ostatním uživatelům, ale i svému dítěti, protože by nemuselo poznat, kteří uživatelé jsou zlí.

Nejistotu u této otázky vyjádřil pouze jeden respondent (7 %), který se obává možnosti dítěte navštěvovat různé stránky, které by respondent jako rodič neschvaloval.

5.1.8 Otázka č. 8: Má Vaše dítě účet na nějaké sociální síti? Víte na jaké?

Tabulka 9 - Rodiče – Účet dítěte na sociálních sítích

Účet dítěte na soc. síti	Počet	Podíl
Ano	14	93 %
Nevím	1	7 %

Dle odpovědí respondentů na otázku č. 8, má 93 % dětí dotazovaných založený účet na některé ze sociálních sítí. Jeden respondent odpověděl, že neví o tom, že by jeho dítě mělo někde založený účet, ale nemůže s jistotou tvrdit, že tomu tak není.

Tabulka 10 - Rodiče – Sociální sítě dětí respondentů

Sociální sít	Počet	Podíl
Facebook	14	100 %
Instagram	9	64 %
Tik Tok	5	36 %
YouTube	2	14 %
Snapchat	1	7 %
Twitter	1	7 %

Tabulka 10 zobrazuje data získaná doplňující otázkou k otázce č. 8, která zjišťovala, na kterých sociálních sítích, o kterých rodiče vědí, mají děti založené účty. Nejčetnější odpovědí byl Facebook, na kterém má účet 100 % dětí respondentů, kteří odpověděli kladně na otázku č. 8. Druhým v pořadí byl

Instagram s 64 %. Méně, než polovina respondentů také označila Tik Tok (36 %), YouTube (14 %), Snapchat (7 %) a Twitter (7 %).

Více než polovina dětí respondentů má tedy založený účet minimálně na dvou sociálních sítích, o kterých má jeho rodič povědomí. Část respondentů uvedla, že si ovšem nejsou úplně jistí, zda dítě nemá založený účet i na dalších sociálních sítích, o kterých respondent nemá tušení, jelikož není úplně možné uhlídat veškerou aktivitu dítěte na internetu.

5.1.9 Otázka č. 9: Kontrolujete nějakým způsobem činnost dítěte na internetu? Pokud ano, jak?

Tabulka 11 - Rodiče – Kontrola činnosti dítěte na internetu

Kontrola	Počet	Podíl
Ano	8	53 %
Ne	7	47 %

Z tabulky 11 lze vyčíst, že 53 % respondentů nějakým způsobem kontroluje činnost svého dítěte na internetu, 47 % nikoliv.

Tabulka 12 - Rodiče – Způsob kontroly činnosti dítěte na internetu

Způsob kontroly	Počet	Podíl
Prohlížení historie	3	37,5 %
Visuální kontrola	2	25 %
Aplikační kontrola	2	25 %
Kontrola aktivity	1	12,5 %

Tabulka 12 zobrazuje četnost způsobů kontrol činností dětí na internetu, tedy data získaná doplňující otázkou k otázce č. 9.

Z respondentů, kteří odpověděli kladně na otázku č. 9, celkem 37,5 % uvedlo, že jako způsob kontroly činnosti dítěte na internetu, využívají nahlížení do historie internetového prohlížeče. Jeden respondent tento krok odůvodnil tím, že se jedná o nejrychlejší způsob, jak zjistit, zda dítě na internetu nevyhledává nevhodný obsah, jako pornografické stránky apod.

Visuální kontrolu, tedy způsob nahlížení dítěti „přes rameno", využívají dva respondenti (25 %). Dle jednoho respondenta, který takto činí, se jedná o rychlou kontrolu, která je možná díky umístění stolního počítače v obývacím pokoji, a zároveň se nejedná o úplné narušení soukromí dítěte, jako je podle něj prohlížení historie prohlížeče.

Stejně tak 25 % respondentů využívá aplikační kontrolu činnosti. Oba respondenti uvedli, že využívají aplikaci, která rodiči zašle upozornění v případě, kdy dítě vyhledává přednastavený nevhodný obsah.

Kontrolu aktivity na sociální síti využívá pouze jeden respondent (12,5 %), který tímto způsobem hlídá, aby jeho dcera nepřidávala na soc. sítě nevhodné fotografie, které by např. mohly zobrazovat vybavení domácnosti, či prozradit, že se v době přidání fotografie, nikdo z rodiny nenachází doma. Ovšem respondent dále uvádí, že tímto způsobem kontroluje i příspěvky, které dcera na sociální síti komentuje, odpovědi na komentáře, dle kterých by mohl zjistit, zda není dcera obětí kyberšikany, či zda není kontaktována zcela cizím člověkem.

5.1.10 Otázka č. 10: Znáte aplikace rodičovské kontroly? Používáte je? Proč?

Tabulka 13 - Rodiče – Znalost aplikací rodičovské kontroly

Znalost	Počet	Podíl
Ano	11	73 %
Ne	4	27 %

Na otázku, zda respondenti znají aplikace rodičovské kontroly odpovědělo 11 respondentů (73 %) kladně. Zbylí 4 respondenti (27 %) tyto aplikace neznají. Jeden z těchto respondentů má povědomí o tom, že takové aplikace existují, ale nikdy se nezajímal ani nevyhledával informace o tom, jak fungují a co vše je možné s nimi dělat. Další dva o možnosti aplikační rodičovské kontroly prý slyšeli během rozhovoru poprvé. Poslední odpověděl, že o takových aplikacích neslyšel, ale půjde si po rozhovoru vyhledat informace a popřemýšlí, zda by nebylo dobré začít jeden z aplikačních rodičovských zámků využívat.

Tabulka 14 - Rodiče – Využívání aplikací rodičovské kontroly

Využívání aplikací	Počet	Podíl
Ano	6	55 %
Ne	5	45 %

Doplňující otázka se tázala respondentů, kteří znají aplikace, zda je používají. Ze 73 % respondentů, kteří na otázku č. 10 odpověděli ano, aplikační rodičovskou kontrolu používá pouze 6 respondentů (55 %), jak je možné vidět v tabulce 14. Dle respondentů se jedná o způsob, jak zajistit alespoň částečně zajistit bezpečnější pohyb dítěte na internetu. Někteří uvádějí, že aplikace používají především k blokaci nevhodného obsahu, či k omezení času dítěte na internetu. Jeden z dotazovaných rodičů využívá aplikaci také ke kontrole stahování

aplikací či programů do zařízení dítěte. Aplikace zašle rodiči upozornění v momentě, kdy chce jeho dítě něco stáhnout do svého zařízení. Rodič stahování buď potvrdí, nebo zamítne. Respondent tak činí z důvodu častého stahování různých nových her dítětem, z nichž jsou některé zpoplatněné. Tímto krokem se ovšem snaží omezit také čas, kdy dítě hraje hry off-line, nebo možnému stažení viru do zařízení.

Ze 45 % respondentů, kteří aplikace rodičovského zámku znají, ale nepoužívají je, jeden uvedl, že dříve jednu z aplikací využíval, ovšem jeho syn momentálně rozumí počítačům a různým zařízením více než respondent, a zdá se být rozumný, proto od používání aplikační kontroly upustil. Jiný z respondentů zase odpověděl, že aplikaci nevyužívá, protože si není jistý, zda by ji zvládl naistalovat či následně ovládat. Složitou instalaci jako důvod uvedl i další respondent, ovšem ve smyslu, že se mu do takového kroku „nechce ani pouštět".

5.1.11 Otázka č. 11: Omezujete nějakým způsobem obsah, ke kterému má Vaše dítě na internetu přístup?

Tabulka 15 - Rodiče – Omezení obsahu na internetu

Omezení obsahu	Počet	Podíl
Ano	8	53 %
Ne	7	47 %

Více než polovina dotazovaných rodičů na otázku č. 11 odpověděla, že nějakým způsobem omezují obsah, který si může jejich dítě na internetu zobrazovat, tedy i vyhledávat. Z těchto 8 respondentů (53 %), dále 6 uvedlo, že omezení probíhá na aplikační bázi, dva omezují dítě verbálně.

Respondenti nejčastěji hovořili o blokaci stránek s erotickým obsahem, stránek s násilným obsahem, zobrazující brutalitu či např. fotografie mrtvých těl, autonehody apod. Někteří uváděli také omezení přístupu k seznamovacím portálům, a blokaci plateb.

5.1.12 Otázka č. 12: Myslíte si, že Vašemu dítěti hrozí na internetu nějaké nebezpečí? Jaké?

Tabulka 16 - Rodiče – Nebezpečí hrozící na internetu

Nebezpečí na internetu	Počet	Podíl
Ano	11	73 %
Ne	3	20 %
Nevím	1	7 %

Tabulka 16 znázorňuje počet a podíl odpovědí na otázku č. 12. Lze z ní vyčíst, že 73 % rodičů shledává internet potencionálně nebezpečným místem pro pohyb dítěte. Nejčastější odpovědí na doplňující otázku, jaké nebezpečí číhá na nezletilé na internetu, byla odpověď „pedofilové“. Ti se k dětem mohou dle jednoho z rodičů dostat cestou seznamovacích portálů, ale i her, a následně se je mohou snažit vylákat na osobní schůzku. Druhou nejčastější odpovědí, kterou uvedli tři dotazovaní, byl pojem „predátoři“. Jedna z respondentek odkazovala na dokumentární film V Síti. Predátoři byli v rozhovoru spojování s vydíráním dětí, s pedofilií, a v jednom případě s groomingem. Dále respondenti uváděli jako příklad nebezpečí různé podvodníky, kteří se budou snažit z dětí vymámit peníze, stažení viru, který poškodí zařízení. Od jednoho z dotázaných zaznělo, že jsou nebezpečné i různé momentálně populární challenge, tedy výzvy, které vycházejí od kdejakých youtuberů či influencerů. Takové výzvy mohou být příčinou fyzického úrazu dítěte, ale dle respondenta mohou na dítěti

zanechat i psychické následky poté, co se dítě stane kvůli výzvě obětí kyberšikany, kterou mimo jiné vzpomenuli další dva respondenti.

5.1.13 Otázka č. 13: Řešil jste nějakým způsobem s Vaším dítětem jeho bezpečí na internetu? Jak?

Na otázku č. 13 odpovědělo 100 % respondentů kladně. Dle odpovědí všichni respondenti dali svému dítěti jakousi průpravu o tom, jak být na internetu v bezpečí. Průprava ve všech případech prý proběhla verbálně. Přibližně polovina respondentů varovala své dítě před cizími lidmi na internetu, kteří mohou být zlí, a mohou se vydávat za někoho známého. Od jedné respondentky proběhlo varování, které se týkalo přidávání kontaktů, přátel, na sociálních sítích. Dceři vysvětlila, že někteří uživatelé mohou ukrást fotky jejím kamarádům a na Facebooku či jiné sociální síti, se mohou vydávat za její přátelé. Další respondent upozorňoval dítě na nebezpečné stránky, kde mohou být viry. Zaznělo i upozornění na dezinformace, či nebezpečné challenge. Dítěti bylo doporučeno se vždy zamyslet, jestli to, co se píše na internetu nebude hloupost.

5.1.14 Otázka č. 14: Myslíte si, že by měl zásady bezpečného internetu s dítětem řešit rodič, anebo škola? Proč?

Tabulka 17 - Rodiče – Zásady bezpečného internetu – rodič anebo škola

Kdo	Počet	Podíl
Rodič	1	7 %
Škola	0	0 %
Rodič i škola	14	93 %

U otázky č. 14 se téměř všichni respondenti (93 %), vyjímaje jednoho (7 %), shodli na tom, že prevence trestných činů páchaných na nezletilých osobách v prostoru internetu by měla vycházet jak od rodiče, tak od školy. Velká část respondentů pro tento názor uvádí jako důvod to, že rodič zná své dítě nejlépe, ví, které internetové stránky navštěvuje, jaké je povahově, a jak k němu v této problematice přistupovat. Škola by měla ovšem tuto problematiku řešit s dětmi také, alespoň obecně. Dle jedné respondentky bohužel škola nemá prostor přistupovat v problematice prevence ke každému dítěti individuálně, proto by se dítě mělo o problematice ve škole dozvědět obecné informace, které by s ním následně rodič probral individuálně. Další z rodičů je názoru, že by prevence měla vycházet především z rodiny, ale ve škole by se problematika měla probírat také, jelikož někteří rodiče nemusí dané problematice rozumět, takže by ji mělo dítě znát alespoň ze školy. Jiný z rodičů zase předpokládá, že škola dítěti tuto problematiku vysvětlí z odborného hlediska, a rodič z osobního. Během rozhovorů s rodiči zazněl i názor, že pokud dítě uslyší zásady bezpečného internetu od více zdrojů, tím větší jim bude dávat váhu.

Pouze v jednom případě zazněl názor respondenta, který říkal, že otázka prevence by měla být věcí rodiče, nikoliv školy, protože ve škole se mají děti učit odborným předmětům, a tato problematika je spíše osobního rázu.

5.1.15 Otázka č. 15: Řešila s Vámi někdy škola Vašeho dítěte v rámci prevence problematiku bezpečnosti dětí na internetu?

Tabulka 18 - Rodiče – Komunikace školy s rodiči na dané téma

Komunikace o tématu	Počet	Podíl
Ano	6	40 %
Ne	9	60 %

Přesně 60 % oslovených respondentů na otázku č. 15 odpovědělo, že mezi nimi a školou dítěte neproběhla žádná komunikace zaměřená na tuto problematiku. V tomto případě jeden z respondentů uvedl, že prozatím asi nebylo nutné nebo potřeba tuto problematiku řešit.

Naopak 6 dotazovaných rodičů odpovědělo, že komunikace ze strany školy na toto téma proběhla. Čtyři ze šesti rodičů se shoduje, že v rámci rodičovských schůzek byli upozorněni na to, aby problematiku bezpečného internetu doma s dítětem probrali. Zbylí 2 respondenti byli školou informování o nadbytečném používáním mobilních telefonů dětmi během přestávek. Jedna respondentka uvedla, že prý „o přestávce stojí šest dětí v hloučku a jen koukají do telefonu". Rodiče byli požádáni, aby dětem v tomto směru domluvili, a následně podepsali souhlas se zákazem používání mobilních telefonů během vyučování i přestávek.

5.1.16 Otázka č. 16: Svěřilo by se Vám vaše dítě s problémem týkající se sociálních sítí?

Tabulka 19 - Rodiče – Důvěra dítěte k rodiči

Důvěra dítěte k rodiči	Počet	Podíl
Ano	5	33 %
Asi ano	7	47 %
Ne	2	13 %
Nevím	1	7 %

Na otázku č. 16, která zjišťovala, zda si rodiče myslí, jestli by se jim svěřilo jejich dítě s problémem týkajícím se sociálních sítí, odpovědělo kladně celých 33 % respondentů. Někteří zdůraznili, že vztah mají se svým dítětem celkově dobrý vztah, dítě se jim svěřuje i s jinými problémy, takže by se jim s daným problémem jistě svěřilo také.

Celkem 47 % respondentů si nebylo úplně jisto, zda by se jim dítě svěřilo, ale předpokládají, že ano. Dva z respondentů si byli 100% jistý, že by se jim jejich dítě nesvěřilo, protože oni by se ve věku svého dítěte svým rodičům s takovým problémem také nesvěřili. Jeden respondent odpověděl, že by to bylo asi „padesát na padesát".

5.1.17 Otázka č. 17: Řešil jste již nějaký problém týkající se Vašeho dítěte a internetu?

Tabulka 20 - Rodiče – Řešení nastalého problému

Řešení nastalého problému	Počet	Podíl
Ano	5	33 %
Ne	10	67 %

Nastalé problémy týkající se dítěte a sociálních sítí již řešilo 33 % dotázaných rodičů. V jednom případě se jednalo o stažený vir do počítače, díky kterému se na ploše počítače zobrazovala stránka, která tvrdila, že počítač je zablokován Policií ČR, a pokud uživatel nezaplatí pokutu převodem z účtu, bude Policií vyšetřován. Respondentka uvedla, že to jejího syna velmi vyděsilo, takže to šel ihned nahlásit rodičům. Problém byl vyřešen „tvrdým restartem" počítače a následným posílením antiviru. V dalším případě se jednalo o kontaktování dítěte cizí osobou z falešného profilu na Facebooku, které bylo ukončeno blokací uživatele. Facebooku se týkala zkušenost i dalších dvou respondentů. Jednalo se o odcizení účtu dítěte, a nabízení erotických služeb dítěti prostřednictvím falešného ženského profilu. Pátý respondent, který odpověděl na otázku č. 17 kladně, řeší problém závislosti dítěte na sociální síti.

5.1.18 Otázka č. 18: Jaké ponaučení jste dal/a dítěti, když začalo používat internet?

U otázky č. 18 zaznělo mnoho různých odpovědí. Rodiče se ovšem velice často shodovali v doporučení nedávat nikomu vlastní adresu. Tímto krokem prý chrání dítě před případným pedofilem, nebo jejich domácnost před krádeží. Děti by také dle několika respondentů neměli sdílet s nikým fotky jejich domova, nikdy nikam či nikomu nepsat, že jsou doma sami, či že vůbec nikdo není doma. Co se sdílení fotek týče, několikrát zaznělo doporučení nesdílet s nikým žádné fotky, a rozhodně ne ty, na kterých by bylo dítě nahé.

Nejvíce respondentů svým dětem radilo nenavazovat kontakt s lidmi, které nezají, protože by jim tito lidé mohli ublížit, zneužít informace, které by jim dítě poskytlo. Ve dvou případech rodiče svému dítěti poradili, jak si řádně zabezpečit účet na sociální síti a nastavit si jeho soukromí. Stejně tak ve dvou případech bylo doporučeno netrávit na sociálních sítích moc času. Jeden respondent s dítětem řešil jeho fyzické bezpečí, kdy mu dal radu nezkoušet vše, co na internetu uvidí, protože některými pokusy by si mohl způsobit různá zranění.

5.2 Vyhodnocení rozhovorů s vyučujícími

5.2.1 Otázka č. 1: Vyučujete na základní škole anebo víceletém gymnáziu?

Tabulka 21 - Vyučující – Typ školy

Škola	Počet	Podíl
Základní škola	12	80 %
Gymnázium	3	20 %

Výzkumu k diplomové práci v části pro vyučující se zúčastnilo celkem 15 respondentů. Z celkového počtu 80 % respondentů vyučuje druhý stupeň základních škol, a 20 % respondentů odpovídající ročníky víceletých gymnázií.

5.2.2 Otázka č. 2: Vaše odučené roky?

Tabulka 22 - Vyučující – Počet odučených let

Odučené roky	Počet	Podíl
0-9 let	6	40 %
10-19 let	4	27 %
20-29 let	2	13 %
30 a více let	3	20 %

Otázka č. 2 se dotazovala respondentů z řad pedagogů na počet odučených let. Nejvíce respondentů, 40 %, uvedlo praxi do 9 let, 27 % respondentů se ve školství pohybuje více než 10 ale méně než 20 let. Praxi více než 20 a méně než 30 let má 13 % respondentů. Délku svého působení více než 30 let uvedlo 20 % dotázaných vyučujících.

5.2.3 Otázka č. 3: V jakém vztahu jste ke třídám druhého stupně či odpovídajícím třídám víceletého gymnázia?

Tabulka 23 - Vyučující – Vztah ke třídám

Vztah k třídám	Počet	Podíl
Třídní učitel	7	47 %
Vyučující předmětů	7	47 %
Vyučující informatiky	3	20 %
Metodik prevence	3	20 %
Výchovný poradce	2	13 %

U otázky č. 3 uváděli oslovení vyučující více možností. Ve 47 % respondentů uvedlo, že pro některé z daných tříd jsou třídním učitele. Stejný podíl vyučujících vyučuje ve třídách druhého stupně a gymnázia některý z předmětů. Zde se často objevovaly předměty od chemie, fyziky a biologie, přes cizí jazyk, až po estetické předměty jako jsou hudební a výtvarná výchova. Vyučujících, kteří vyučují konkrétně informatiku a výpočetní techniku bylo mezi respondenty 20 %.

Mezi respondenty se našlo i 20 % vyučujících, kteří jsou školním metodikem prevence, a 13 % vyučující jež na škole figurují také jako výchovný poradce.

5.2.4 Otázka č. 4: Mají žáci ve škole přístup k internetu mimo hodiny informatiky? Jak?

Tabulka 24 - Vyučující – Přístup žáků k internetu

Přístup k internetu	Počet	Podíl
Ano	9	60 %
Ne	6	40 %

Na otázku č. 4, která zjišťovala, zda mají žáci ve škole přístup k internetu mimo hodiny informatiky, odpovědělo 40 % respondentů ne, ovšem většina dotázaných vyučujících (60 %) opověděla ano. Vyučujícím, kteří odpověděli kladně, byla položena doplňující otázka: Jak?

Tabulka 25 - Vyučující – Způsob přístupu žáků k internetu

Způsob	Počet	Podíl
V učebnách IVT	5	56 %
Vlastní data	3	33 %
Školní Wi-Fi	4	44 %

Na doplňující otázku k otázce č. 4 odpovědělo 56 % respondentů, že žáci mají mimo hodiny informatiky přístup k internetu v učebně informatiky a výpočetní techniky. Ovšem jejich přístup musí být schválen vyučujícím informatiky, kdy se jedná o jednorázový souhlas v daný moment.

Druhou nejčastější odpovědí na doplňující otázku (44 % respondentů) byl přístup žáků ke školní Wi-Fi síti, díky které mohou být o přestávkách připojeni neomezeně. Ovšem v hodinách žáci nesmí používat mobilní telefony, nejsou-li k tomu vyučujícím vyzváni.

Využívání žáků vlastní data zmínilo 33 % respondentů, dle kterých žáci přístup ke školní Wi-Fi síti nemají, proto využívají vlastní mobilní data. Všichni tito respondenti se shodují, že pokud má některý ze žáků neomezená mobilní data, vytváří svým spolužákům pomocí hotspotu v telefonu soukromou Wi-Fi síť.

5.2.5 Otázka č. 5: Prochází dostupný internetový obsah ve škole nějakou filtrací?

Tabulka 26 - Vyučující – Filtrace internetového obsahu

Filtrace obsahu	Počet	Podíl
Ano	6	40 %
Ne	6	40 %
Nevím	3	20 %

Nastaveno filtraci dostupného internetového obsahu pro žáky ve školách potvrdilo 40 % respondentů. Jedná se prý o blokaci některých nevhodných stránek. Jedna respondentka uvedla, že zakázaný obsah je blokován i na školních iPadech, které žáci používají během vyučování.

Stejný počet respondentů naopak odmítal jakoukoliv filtraci obsahu na školní síti. Tři respondenti (20 %) bohužel neměli informace, zda je ve škole zobrazovaný obsah nějak omezen, jelikož školní síť nemají na starost.

5.2.6 Otázka č. 6: Ukládají Vám učební osnovy vašeho předmětu probírat s žáky problematiku bezpečnosti na internetu?

Tabulka 27 - Vyučující – Osnovy

Osnovy	Počet	Podíl
Ano	10	67 %
Ne	5	33 %

Otázka č. 6 se respondentů dotazovala, zda jim učební osnovy jejich předmětu ukládají povinnost tématiku bezpečnosti na internetu s žáky probírat. Na tuto otázku odpovědělo 67 % respondentů Ano, v 33 % odpověděli vyučující Ne.

5.2.7 Otázka č. 7: Řešíte tuto problematiku s žáky nad rámec učebních osnov?

Tabulka 28 - Vyučující – Problematika nad rámec osnov předmětu

Problematika nad rámec osnov předmětu	Počet	Podíl
Ano	10	67 %
Ne	5	33 %

Dvě třetiny respondentů na otázku č. 7 odpovědělo, že s žáky problematiku bezpečnosti na internetu řeší nad rámec učebních osnov jejich předmětu.

Mezi těmito 67 % jsou tři vyučující, jímž osnovy povinnost toto téma řešit neukládají, ale činí tak dobrovolně.

Jedna třetina respondentů odpověděla, že problematiku s žáky nad rámec osnov neřeší. Mezi 33 % dotázaných vyučujících, kteří takto odpověděli, jsou 3 respondenti, kteří jsou dle školního vzdělávacího programu jejich předmětu povinni s žáky tuto problematiku probírat, a probírají ji v pouze v mezích osnov. Ostatní respondentům ze zmiňované jedné třetiny osnovy neukládají problematiku probírat, ani tak nečinní nad rámec osnov.

Někteří respondenti, kteří řeší problematiku nad rámec osnov uvádějí, že k takovým krokům přistupují v případě potřeby, např. když se v třídním kolektivu objeví problém z této oblasti. Jedná se většinou o varování.

Tři vyučující českého jazyka uvedli, že téma bezpečnosti řešili, když probírali téma sociálních sítí, či narazili na téma v textu nebo ukázce textu. Respondenti se v takových případech snažili žákům předat své zkušenosti, vyprávěli žákům příklady z praxe, a upozornili je na možné důsledky. Jeden z těchto tří respondentů také uvedl, že žáci na téma bezpečí na internetu tvořili v rámci českého jazyka myšlenkovou mapu a psali o tomto tématu úvahu.

Jeden vyučující informatiky nad rámec osnov přistupuje k vyprávění a rozebírání kazuistik případů, o kterých se dozvěděl při samostudiu.

5.2.8 Otázka č. 8: Řeší se problematika bezpečnosti na internetu v třídnických hodinách?

Tabulka 29 - Vyučující – Třídnické hodiny

Problematika v třídnických hodinách	Počet	Podíl
Ano	10	67 %
Ne	3	20 %
Nevím	2	13 %

Problematika bezpečnosti na internetu se v třídnických hodinách řeší dle 67 % dotazovaných pedagogů. Dle jedné respondentky se k tomuto kroku přistupuje, když si to žádají potřeby třídního kolektivu. Třídní učitelé mohou hledat oporu u školní metodičky prevence, která třídním učitelům poskytne potřebné materiály věnující se prevenci problematiky.

Další z vyučujících uvedla, že v rámci třídnické hodiny se se svými žáky dívala na dokument V Síti: Za školou, aniž by si to situace v třídním kolektivu žádala.

Celkem tři respondenti, tedy 20 %, odpověděli, že tuto problematiku v třídnických hodinách neřeší. Jeden respondent dodal, že na škole nejsou zavedeny třídnické hodiny, a v hodinách, kdy učí vlastní třídu, se žáky řeší organizační věci, jak např. omluvenky. Diskutovanou problematiku se svými žáky řeší v hodinách informatiky, a případně mimo vyučovací hodiny, pokud je někým ze žáků oslovena.

Dva respondenti (13 %) si nebyli jistí, zda se toto téma v třídnických hodinách řeší či nikoliv, jelikož nejsou třídními učiteli.

5.2.9 Otázka č. 9: Vzděláváte se nějakým způsobem v této problematice? Jak?

Tabulka 30 - Vyučující – Další vzdělávání v problematice

Další vzdělávání v problematice	Počet	Podíl
Ano	12	80 %
Ne	3	20 %

V problematice bezpečnosti dětí a nezletilých osob se dále vzdělává 80 % dotazovaných vyučujících, kterým byla položena doplňující otázka, zajímající se o způsob dalšího vzdělávání v problematice. Dvacet procent respondentů se již dále v problematice nevzdělává.

Tabulka 31 - Vyučující – Způsob dalšího vzdělávání

Způsob dalšího vzdělávání	Počet	Podíl
Samostudium	5	42 %
DVPP	6	50 %
Školení MP	1	8 %

Na doplňující otázku k otázce č. 9, která byla položena 12 respondentům, odpovědělo 42 % dotázaných vyučující, že k dalšímu vzdělávání v problematice bezpečnosti dětí na internetu, využívají samostudium. Jedna respondentka si vyhledává informace na internetu, většinou na webových stránkách, které se této problematice věnuji. Činí tak protože chce mít dostatek informací,

které by mohla poskytnout žákům, ale i protože se sama pohybuje v kyberprostoru a chce vědět, jak chránit i sebe.

Nejvíce respondentů, 50 %, uvedlo, že se v problematice vzdělávají díky DVPP – Dalšímu vzdělávání pedagogických pracovníků. Jak se shoduje několik respondentů, v nabídce jsou různé kurzy, semináře, webináře nebo odborné přednášky.

Jeden respondent uvedl jako další vzdělávání v problematice školení metodiků prevence.

5.2.10 Otázka č. 10: Probíhá ve škole prevence na téma této problematiky? Jak?

Na otázku č. 10 odpovědělo 100 % respondentů Ano. Následně jim byla položena otázka, jakým způsobem v jejich škole prevence probíhá?

Tabulka 32 - Vyučující – Způsob prevence ve školách

Způsob prevence	Počet	Podíl
Dokumenty, filmy	2	13 %
Besedy, přednášky	9	60 %
V rámci předmětu	5	33 %
Projektové dny	2	13 %
Plakáty	1	7 %

Při doplňující otázce uvedli někteří respondenti více možností prevence. Nejvíce respondentů (60 %) uvedlo, že prevence ve škole probíhá pomocí různých odborných přednášek a besed, které vedou odborní lektoři. Několik respondentů uvedlo, že ve škole proběhla na toto téma beseda s Policií ČR, která žáky opravdu bavila a velice se jim líbila. Dle dvou respondentů

tyto besedy a přednášky pro školy zajišťuje školní metodik prevence, který také sdružuje různé materiály, které slouží k dalším preventivním činnostem. Jedna z vyučujících se prý této tématice věnuje dlouhodobě, a sama dříve organizovala projekt, který se zaměřoval na prevenci ve školách. V rámci projektu proběhla série přednášek, které navštívilo přibližně 1 200 žáků základních škol.

Druhou nejčastější odpovědí, která zazněla od 33 % respondentů, je prevence probíhající v rámci různých předmětů. Vyjímaje informatiky a výpočetní techniky, vyučující také uváděli předměty jako je výchova ke zdraví, občanská nauka, a mediální výchova.

Celkem 13 % respondentů odpovědělo, že prevence probíhá i v rámci školních projektových dní. Stejný počet respondentů dále uvedlo různé filmy a dokumenty. Jeden z respondentů, který je ve vztahu k žákům školním metodikem prevence uvedl, že žáci víceletého gymnázia byli v kině na promítání dokumentu V Síti: Za školou. Promítání se kromě žáků do 15 let zúčastnili i starší studenti.

Pouze jeden z oslovených vyučujících odpověděl, že ve škole probíhá prevence pomocí různých plakátů a dalších informačních materiálů.

5.2.11 Otázka č. 11: Myslíte, že by zásady bezpečného internetu měl s dítětem řešit rodič, anebo škola? Proč?

Tabulka 33 - Vyučující – Zásady bezpečného internetu – rodič anebo škola

Kdo	Počet	Podíl
Rodič	4	27 %
Škola	0	0 %
Rodič i škola	11	73 %

Otázka č. 11 se zajímala o názor oslovených vyučujících, zda by problematiku bezpečného internetu měl s dítětem řešit rodič anebo škola. Nadpoloviční většina, celkem 73 % respondentů, opověděla, že by prevence měla vycházet jak ze strany rodiče, tak i školy. K doplňující otázce „Proč?“, se sešla spousta zajímavých názorů. Někteří respondenti zastávali názor, který říká, že prevence by měla vycházet od rodiče protože své dítě zná po osobní stránce, a ví, které webové stránky si dítě prohlíží, co dělá ve volném čase. Ze strany školy by měla vycházet teoretická část prevence.

Jeden respondent uvedl, že jedině působení stejným směrem od obou stran (rodiče i školy) může vést k úspěchu. Další odpověděl, že rodič s dítětem tuto problematiku probere po osobní stránce, a teorii, kterou se žák dozví ve škole, zase může prodiskutovat se svými spolužáky a vrstevníky. Díky tomu si bude moci utvořit vlastní celistvý názor na problematiku.

Dle další z dotázaných vyučujících je třeba součinnost rodiče i školy, protože si žáci myslí, že se je vyučující mnohdy snaží pouze „strašit“. Když ovšem o této problematice slyší z více zdrojů, nebo např. bohužel narazí na nějaký problém, zjistí, že se nejednalo o pouhé „strašení“.

Na důležitosti součinnosti školy a rodičů se shoduje i další respondent, který zastává názor, že by rodiče měli mít představu o činnosti dítěte na internetu, měli by jej upozornit na rizika a nebezpečí, ovšem vše ale záleží na vzájemné důvěře a komunikaci. Důležitým je dle respondentky také, aby byly zásady bezpečného internetu dětem opakovaně připomínány ať už doma nebo ve škole.

Že by měl zásady bezpečného internetu s dítětem řešit rodič uvedlo 27 % respondentů. Jeden z respondentů tento názor odůvodnil tím, že „rodina je základ, a měla by být základem i ve věcech prevence".

Další respondent uvedl, že nejvíce času na internetu tráví děti doma, proto by měl s dítětem řešit prevenci rodič. Ve škole se jedná o organizovanou činnost pod dohledem pedagogů.

Dva respondenti se shodli na názoru, že rodič zodpovídá za výchovu a bezpečí svého dítěte.

5.2.12 Otázka č. 12: Řešíte v rámci prevence problematiku bezpečnosti dětí na internetu nějakým způsobem s rodiči žáků?

Tabulka 34 - Vyučující – Komunikace školy s rodiči na dané téma

Komunikace o tématu s rodiči žáků	Počet	Podíl
Ano	5	33 %
Ne	10	67 %

Na otázku č. 12 odpovědělo 33 % respondentů kladně. Jedná se o respondenty, kteří problematiku s rodiči žáků řeší preventivně. Dva z nich uvedli, že se tato problematika řeší s rodiči opakovaně každý rok při rodičovských schůzkách na začátku školního roku. Případně jsou dle potřeby kvůli této problematice

kontaktování znovu. Další respondent, vyučující z víceletého gymnázia, také uvádí informování rodičů prvních ročníků na začátku školního roku, zejména o preventivním programu. V jednom případě jsou rodiče informováni o zákazu používání mobilních telefonů ve škole, a zároveň i upozorněni na danou problematiku.

Komunikaci mezi školou a rodiči v rámci prevence problematiky popírá 67 % respondentů. Z těchto respondentů polovina udala, že se problematika řeší v případě vzniklého problému.

5.2.13 Otázka č. 13: Řešil jste již nějaký problém týkající se zneužívání dětí na sociálních sítích v praxi? Svěřil se Vám žák s takovým problémem? Jak jste situaci řešil?

Tabulka 35 - Vyučující – Řešení již nastalého problému

Vzniklý problém	Počet	Podíl
Ano	4	27 %
Ne	11	73 %

Celkem 73 % dotázaných vyučujících uvedlo, že se během své praxe nesetkali s problémem, který by se týkal zneužívání dětí na sociálních sítích.

S nastalým problémem se dle výzkumu setkalo 27 % respondentů. Ve jednom případě se jednalo o problém v třídním kolektivu, kdy se spolužáci na Facebooku vzájemně pomlouvali a uráželi. Problém byl vyřešen domluvou žákům.

Jeden z respondentů uvedl, že se setkal s případem, kdy se cizí osoba snažila od dítěte vyloudit jeho fotografie. Dítě naštěstí vědělo, jak se má v takovém případě zachovat, druhou stranu si zablokovalo, a vše dobře dopadlo. Následně byli všichni žáci poučeni, jak se v podobných situacích chovat. Díky tomuto kolektiv probral i další různé situace, které mohou nastat.

Další respondent uvedl, že takové případy se na škole naštěstí řeší jen zřídka. Jde o případy, kdy žáci sdílí své fotografie a tím se dostanou do potíží, nebo jejich fotografie a videonahrávky bez jejich svědomí sdílí někdo jiný. V takových případech jsou vždy informování zákonní zástupci žáků. V závažnějších případech je rodičům doporučeno nahlásit skutečnost na Policii ČR.

6 DISKUZE

Tato část práce se bude věnovat hodnocení zjištěných dat a výsledků z praktické části práce, získaných pomocí metody smíšeného výzkumu.

Hlavním cílem práce bylo na základě provedeného výzkumu identifikovat slabá místa v preventivní činnosti škol a rodičů, a následně formulovat doporučení možných způsobů prevence zneužívání nezletilých osob v prostoru sociálních sítí pro rodiče, základní školy a víceletá gymnázia.

Pro získání potřebných dat byla zvolena metoda řízených rozhovoru s rodiči dětí ve věku 12-15 let, vyučujícími druhého stupně základních škol a vyučujícími odpovídajících ročníků víceletých gymnázií. Získaná dala byla vyhodnocena statistickým zpracováním a obsahovou analýzou.

Praktická část práce byla rozdělena na dvě části. První byla vyhodnocována část určená rodičům. Zde první část rozhovoru byla věnována obecným informacím o dětech dotazovaných rodičů. Mezi 15 respondenty bylo 53 % rodičů dívek a 47 % rodičů chlapců. Věkové rozpoložení dětí respondentů bylo 33 % dvanáctiletých, 20 % třináctiletých, 20 % čtrnáctiletých, a 27 % patnáctiletých dětí. Základní školu navštěvovalo 53 % dětí respondentů a víceleté gymnázium 47 % dětí respondentů. Rozložení respondentů mezi rodiči žáků základních škol a gymnázií bylo téměř vyrovnané, tudíž předpokládáme, že získaná data nejsou zaujata pouze na jednu kategorii.

Druhá část rozhovoru s rodiči byla zaměřena na přístup dětí respondentů k internetu. Otázkou č.4 bylo zjištěno, že přístup k internetu mají děti všech 15 respondentů (100 %). Nejvíce dětí se k internetu připojuje prostřednictvím mobilního telefonu (87 %), 47 % dětí prostřednictvím notebooku. Stolní počítač k připojení využívá 33 % dětí, stejně tak tablet, a 13 % dětí využívá herní konzoli.

Lze říct, že nejvíce rizikové zařízení je tedy mobilní telefon, který je nejčastější, a zároveň se díky jeho kompaktnosti a přenositelnosti nedá činnost dítěte na mobilním telefonu, na rozdíl od stolních zařízení, účinně uhlídat.

Většinu těchto zařízení získali děti od svých rodičů, a to v celých 87 % případů. Rodiče děti zařízeními obdarovaly ku příležitosti narozenin, Vánoc apod., v některých případech bylo zařízení zakoupeno z důvodu distanční výuky během pandemie COVID. Respondentů, kteří uvedli, že si dítě zakoupilo některé ze zařízení samo bylo 20 %. V dalších 20 % případů bylo některé zařízení již stávajícím zařízením domácnosti. Tato část rozhovoru se dotazovala také, zda rodiče nějakým způsobem limitují čas dítěte na internetu. Celých 87 % respondentů čas dítěte limituje, 13 % respondentů nikoliv. Z respondentů, kteří čas limitují tak 67 % činí verbálně a 33 % aplikačně. Z výpovědí respondentů je možné usuzovat, že verbální omezování času stráveného dítětem bývá leckdy neefektivní, jelikož není dítětem tolerováno. Mohlo by se zdát, že aplikační omezení je účinnější, avšak otázkou je, do jaké míry se děti umí s aplikačním přednastavením od rodičů po technické stránce vyrovnat a obejít jej.

Třetí část rozhovoru tvořena otázkami č. 8 a 9 zjišťovala, zda mají rodiče povědomí o činnosti dítěte na internetu. Dle výzkumu 93 % respondentů vědí o účtech dětí na sociálních sítích. Pouze jeden respondent (7 %) neví, zda má jeho dítě nějaký účet založený. Všech 100 % respondentů, kteří vědí o účtech svých dětí, uvedlo, že jejich dítě používá Facebook, 64 % respondentů dále uvedlo Instagram, 36 % Tik Tok, 14 % YouTube, 7 % Snapchat a 7% Twitter. V porovnání s výzkumem České děti v kybersvětě z roku 2019, jehož se účastnily děti ve věku 7-17 let, popularita Facebooku a Tik Toku u dětí vzrostla, naopak YouTube či Snapchat se propadli. Vysvětlením tohoto rozdílu může být fakt, že ve výzkumu z roku 2019 se pracovalo s mnohem širší věkovou skupinou dětí, ale i to, že rodiče nemají přehled o všech účtech dětí na sociálních sítích. [62]

V této části rozhovoru bylo dále zjištěno, že 53 % dotázaných rodičů své dítě na internetu nějakým způsobem kontroluje. Tito rodiče v 37,5 % případů využívají nahlížení do historie prohlížeče, 25 % rodičů své dítě kontroluje díváním se přes rameno dítěte na momentálně zobrazený obsah, taktéž 25 % vyžívá ke kontrole činnosti dítěte na internetu různé aplikace rodičovské kontroly. Pouze jeden respondent kontroluje přímo aktivitu na sociálních sítích. Někdo by kontrolování aktivity dítěte na internetu mohl považovat za narušení soukromí dítěte, ovšem i v tomto případě je nutné si uvědomit, že děti nemají dostatečné zkušenosti, aby rozpoznali, že se právě ocitli na internetu v nebezpečí. Jak bylo popsáno v teoretické části práce, v kapitole Sociální inženýrství, někteří útočníci, predátoři, používají velmi propracované metody, které není dítě schopno rozeznat. Rodič má v takovém případě větší šanci než dítě podvodníka odhalit. Někteří respondenti se u této otázky zdáli být lehce nervózní, přemýšleli nad svojí odpovědí. Tato náhlá změna mohla být vyvolána pocitem, že by za svoji odpověď mohli být tazatelem souzeni, jelikož sami částečně považují určité formy kontroly za narušování soukromí dítěte.

Další část rozhovoru s rodiči byla orientována na aplikace rodičovské kontroly, omezení přístupu a povoleného obsahu. Na otázku č. 10, která konkrétně zjišťovala znalost rodičů aplikací rodičovské kontroly, odpovědělo 73 % respondentů Ano, čímž byla potvrzena hypotéza 2. Z 11 respondentů, kteří odpověděli, že aplikace znají, je používá celých 55 %, především k blokaci nevhodného obsahu. Nevhodný obsah dle další výzkumné otázky z celkového počtu respondentů omezuje 53 % rodičů. Výzkumem nebyl zjišťován přímo věk respondentů, který by mohl mít vliv na četnost požívání aplikace. Zejména u respondentů vyššího věku nebo by mohly hrát roli obavy z instalace a nastavění aplikace, které by které plynou z nedostatečné edukovanosti práce s moderními technologiemi.

Dále se rozhovor zaměřoval na prevenci vycházející směrem od rodičů. Otázka č. 12 se dotazovala rodičů, zda si myslí, že na internetu dítěti hrozí nějaké nebezpečí. Bezpečným pro dítě internet shledalo 20 % respondentů, jeden respondent (7 %) si nebyl jistý, 73 % respondentů ovšem v internetu vidí, jak ukazuje tabulka 16, potencionální riziko pro jejich děti. Jedná se o nadpoloviční většinu rodičů, což potvrzuje hypotézu 3. Všech 15 dotázaných rodičů dále na otázku č. 13 uvedlo, že s dítětem jeho bezpečí na internetu řešili verbální formou.

Na otázku, zda my měla zásady bezpečného internetu s dítětem řešit škola anebo rodič odpověděl jeden respondent (7 %), že by otázka prevence měla být zásadně pouze v kompetenci rodičů. Naopak 93 % respondentů uvedlo, že by prevence měla vycházet z obou zmiňovaných směrů. Z toho vyplývá, že je důležitá vzájemná komunikace a spolupráce mezi rodiči a školou. Ovšem z další výzkumné otázky bylo zjištěno, že škola dle respondentů s rodiči komunikuje na téma bezpečnosti dětí na internetu pouze ve 40 % případů. Zbývajících 60 % odmítalo, že by komunikace na zmíněné téma někdy proběhla. V tomto případě je nutná úvaha nad způsobem sdělení, jelikož je možné, že někteří respondenti z řad rodičů nemuseli některou z forem považovat za podstatnou, a proto uvedli, že komunikace na dané téma neproběhla.

Rozhovor se rovněž zaměřoval také na důvěru mezi rodičem a dítětem. V této části rozhovoru důvěru k pohybu dítěte na internetu vyjádřilo 73 % respondentů z řad rodičů. Svým dětem v pohybu na internetu nedůvěřuje 20 % respondentů a jeden respondent (7 %) si není jistý. Důvěra byla tématem i otázky č. 16, která se respondentů tázala, zda by se jim jejich dítě svěřilo s problémem týkající se sociálních sítí. Na tuto otázku odpovědělo 33 % respondentů, že by se jim jejich dítě svěřilo, 47 % to předpokládalo, 13 % vědělo, že by se jim dítě nesvěřilo a 7 % si nebylo jistých. Nedůvěřivost rodičů směrem k pohybu dětí na internetu

pravděpodobně může pramenit z jiných oblastí života, kde se dítě mohlo projevit jako nezodpovědné, ale i z pochybnosti rodičů o vlastním preventivním vlivu na dítě.

Otázka č. 17 ukázala, že někteří respondenti již v takové situaci byli. Vzniklý problém týkající se sociálních sítí dítěte již řešilo 33 % (5) respondentů. Zbylých 67 % takový problém prozatím, naštěstí, ještě řešit nemuselo. I u této otázky na respondentech, kteří odpověděli, že již nějaký problém řešili, byla vidět jistá nervozita, pro kterou mohlo být důvodem možný pocit vlastního selhání v edukaci dítěte.

Poslední otázka, otázka č. 18 byla podrobena pouze obsahové analýze. Zjišťovala, jaké ponaučení dali rodiče svým dětem, když začali používat internet. Nejčastějším doporučením bylo nikomu nedávat adresu, nesdílet s nikým vlastní fotografie či fotografie vybavení domácnosti, nenavazovat kontakty s cizími lidmi, nepsat nikomu, že nikdo není doma. V porovnání s desaterem bezpečného internetu pro děti, které je k dostání na webových stránkách www.rodice-a-deti.cz, se rodiče s autorem desatera shodovali pouze ve třech bodech. Z toho lze usuzovat, že leckdy děti od rodičů nezískají v tématu bezpečného internetu všechny informace, které by zabezpečili jejich bezpečí. [63]

Dotazy na obecné informace začínal i rozhovor s vyučující druhého stupně základních škol a odpovídajících ročníků víceletého gymnázia. Tato část výzkumu ukázala, že mezi respondenty je 80 % vyučujících ze základních škol a 20 % vyučujících z víceletých gymnázií. Délka praxe nejvíce vyučujících se pohybovala v rozmezí 0-9 let (40 %), 27 % dotázaných vyučujících mělo praxi ve školství 10-19 let, 13 % 20-29 let, a 20 % více jak 30 let. V úvodu rozhovoru byli vyučující také dotázáni na jejich vztah k dětem ve vymezené věkové skupině. Mezi respondenty bylo 47 % třídních učitelů, dále 47 % vyučujících různých

předmětů. Respondenti byli vyučující předmětů téměř všech zaměření, např. biologie, fyzika, zeměpis, dějepis, cizí jazyky, matematika, český jazyk, výtvarná výchova, hudební výchova apod. Celkem 3 respondenti (20 %) byli vyučující informatiky a výpočetní techniky, stejně tak 20 % respondentů bylo školním metodikem prevence, a 13 % výchovných poradců. Díky různorodosti vztahů respondentu k žákům, bylo možné zjistit edukovanost všech vyučujících v řešené problematice.

Druhá část rozhovoru s vyučujícími se věnovala přístupu žáků k internetu a povolenému obsahu. Dle 40 % respondentů nemají žáci ve škole přístup k internetu mimo hodiny informatiky, podle 9 (60 %) respondentů ano. Těchto 9 respondentů bylo dále dotázáno jaké mají děti možnosti přístupu. Čtyři vyučující (44 %) uvedli, že je žákům k dispozici školní sít Wi-Fi, 33 % dotázaných uvedlo používání vlastních mobilních dat a vytváření hotspotu pro spolužáky, a 56 % respondentů se shodlo na možnosti pro žáky využívat po domluvě s vyučujícím počítače v učebnách informatiky a výpočetní techniky. Otázka č. 5 se vyučujících dotazovala, zda dostupný internetový obsah ve škole prochází nějakou filtrací. Ve 40 % případů respondenti uvedli, že je obsah ve škole filtrován od nevhodných stránek, stejně tak 40 % respondentů odpovědělo že obsah neprochází ve škole žádnou filtrací. Tři respondenti (20 %) bohužel o filtraci obsahu neměli informace.

Třetí část rozhovoru byla zaměřena na učební osnovy a problematiku bezpečnosti dětí na internetu. Osnovy předmětu udávají povinnost s žáky problematiku bezpečnosti na internetu řešit 67 % respondentů. Mezi těmi jsou vyučující informatiky, občanské výchovy a výchovy ke zdraví. Nad rámec osnov řeší tuto problematiku také 67 % respondentů, ovšem mezi nimi jsou i vyučující, kterým osnovy nepřikazují tuto problematiku řešit, a naopak někteří vyučující, kterým to osnovy přikazují, se pohybují pouze v rámci stanovených osnov.

Zda se problematika bezpečnosti dětí na internetu řeší v třídnických hodinách, se ptala otázka č. 8. Na tu kladně odpovědělo 67 % respondentů, 20 % respondentů uvedlo, že se v třídnických hodinách tato problematika neprobírá, a 13 % respondentů nemělo o tom informace. Zde pravděpodobně hraje roli četnost třídnických hodin, kdy někteří respondenti uvedli, že na jejich škole nic jako třídnické hodiny neexistuje. V některých případech vyučující uvedli, že jsou řešeny spíše organizační věci týkající se třídy, a je možné, že na řešení daného téma nezbývá čas.

Výzkum dále ukázal, že se v řešené problematice dále vzdělává 80 % respondentů (12), z nichž 42 % využívá samostudium, 50 % program dalšího vzdělávání pedagogických pracovníků, a 8 % se vzdělává v rámci školení metodiků prevence. Možností vzdělávání je tedy dostatek a vše záleží jen na přístupu jednotlivých vyučující.

Další část rozhovorů s vyučujícími byla věnována otázce prevence na školách. Sto procent respondentů uvedlo, že na školách nějakým způsobem prevence probíhá. Dle doplňující otázky se nejčastěji jedná o různé odborné besedy a přednášky s externisty (60 %), 33 % respondentů uvedlo probíhající prevenci v rámci určitých školních předmětů, 13 % prostřednictvím dokumentů a filmů, 13 % v rámci projektových dní, a jeden (7 %) respondent uvedl plakáty. Většina škol využívá kombinaci více výše zmiňovaných prvků prevence, čímž může být i dle mého názoru zvýšena efektivnost prevence.

Dle další výzkumné otázky si 73 % dotázaných vyučujících myslí, že by zásady bezpečného internetu měly být řešeny s dětmi školou i rodičem, 27 % respondentů uvedlo, že by tuto problematiku měli s dětmi řešit rodiče. Komparací výsledků otázky č. 11 z části pro vyučující a otázky č. 14 z části pro rodiče bylo zjištěno, že 25 respondentů z řad rodičů i vyučujících z celkových

30 zastává stejný názor, a to, že by tuto problematiku měla s dětmi řešit jak škola, tak i rodiče. Jedná se tedy o názor 83 % respondentů, čímž se potvrzuje hypotéza 1. Shoda mezi rodiči a vyučujícími vypovídá o předpokládané důležitosti spolupráce obou prvků prevence, která by dle mého názoru měla být více rozvíjena .

V části pro vyučující se rozhovor také věnoval komunikaci mezi školou a rodiči. Že škola komunikuje s rodiči o tématu bezpečnosti dětí na internetu uvedlo 33 % respondentů, 67 % respondentů uvedlo, že škola na toto téma s rodiči nekomunikuje preventivně. Komparací otázky č. 12 z části pro vyučující a otázky č. 15 z části pro rodiče bylo zjištěno, že 19 (63 %) respondentů z obou částí výzkumu se shodlo na absenci komunikace školy a rodiče na dané téma v rámci prevence, a pouze 11 respondentů z řad vyučujících i rodičů (37 %) komunikaci v rámci prevence potvrdilo. Touto komparací byla vyvrácena hypotéza 4.

Rozhovory s vyučujícími byly zakončeny otázkou, zda již během své praxe řešili problém týkající se zneužívání dětí na internetu, a zda se jim nějaký žák s takovým problémem svěřil. S žádným takovým problémem se nesetkalo 73 % respondentů, problém týkající se dětí a sociálních sítí řešilo 27 % respondentů. Někteří respondenti uvedli, že díky nastalému problému proběhla ve škole další forma prevence. Tento krok považuji za velice důležitý, jelikož dle mého názoru, si děti poučení na konkrétních případech zapamatují lépe, než jen při předkládání faktů.

Ačkoliv prevence ve školách a v rodinách probíhá, byly vytvořeny formulace doporučení pro rodiče a školy, ve kterých jsou zahrnuty návrhy na zlepšení preventivní činnosti.

6.1 Návrh doporučení pro rodiče

1. **Vzdělávejte se v problematice bezpečnosti na internetu**

Jedině pokud budete sami znát rizika, kterým může internet vystavit Vaše dítě, budete schopni vysvětlit Vašemu dítěti, jak se v kyberprostoru pohybovat bezpečněji.

2. **Kontrolujte činnost dítěte na internetu**

Včasným odhalením a řešením problému můžete Vaše dítě ušetřit zbytečného stresu a případného traumatu. Stejně jako byste hlídali své dítě na dětském hřišti, hlídejte jej na internetu. Mějte přehled, jaké webové stránky Vaše dítě navštěvuje, jaké osoby kontaktuje a jaké informace sdílí.

3. **Hlídejte množství času stráveného na internetu**

Věděli jste že i na internetu a sociálních sítích se dítě může stát závislým? Kontrolujte kolik času dítě na internetu tráví, a domluvte se společně na rozumném kompromisu.

4. **Vysvětlení dle věku a mentální úrovně dítěte**

Vysvětlete svému dítěti dle jeho věku či mentální úrovně, jaké nástrahy na něj mohou na internetu čekat. Poraďte mu, jak se na internetu orientovat, jaké věci může sdílet s ostatními uživateli, a které si má naopak raději nechat pro sebe. Dobrým pomocníkem Vám může být desatero bezpečného internetu dostupné na webových stránkách zabývajících se problematikou bezpečnosti na internetu, proberte s dítětem jednotlivé body desatera. Zkusit můžete i metodu, kdy dítě bude problematiku vysvětlovat Vám.

5. **Samostudium dítěte**

Nechejte dítě na internetu vyhledat rady od odborníků zabývající se problematikou bezpečnosti na internetu. Na webových stránkách věnující se prevenci problematiky může narazit na různé online kurzy pro děti, kvízy apod.

6. **Nezakazujte činnosti dítěte na internetu**

Pokud vysloveně nemusíte některou z činností dítěte na internetu zakázat, nedělejte to. Stejně jako v reálném světě by zakázaná činnost na internetu mohla být pro dítě více lákavá. Raději dítěti vysvětlete, proč by se měl určité činnosti vyvarovat, co a proč mu hrozí.

7. **Informujte se o problematice ve škole**

Pokud jste z řad rodičů, kteří se na internetu příliš nepohybují, a jejíchž dítě se na internetu vyzná lépe než rodič, zkuste se o problematice bezpečnosti dětí na internetu informovat ve škole Vašeho dítěte. Školní metodik prevence či třídní učitel dítěte Vám jistě rád poradí.

8. **Sledujte proměny nálad dítěte**

Proměny nálad Vašeho dítě Vám mohou hodně napovědět, zda dítě neřeší nějaký problém.

9. **Mluvte často s dítětem o problematice bezpečnosti na internetu**

Snažte se řešit problematiku bezpečnosti na internetu s dítětem opakovaně. Dítě si sice Vaše rady může pamatovat, ovšem někdy je dobré je čas od času připomenout.

10. Využívejte aplikační možnosti

Využívejte aplikace rodičovské kontroly. Tyto aplikace nabízí řadu možností nastavení. Od časového limitu, přes zakázaný zobrazovaný obsah, po kontrolu činnosti dítěte na internetu. Některé aplikace rodičovské kontroly jsou na internetu ke stažení zdarma, a jejich instalace není náročná.

6.2 Návrh doporučení pro školy

1. **Upozorňujte děti na nebezpečí na internetu**

Upozorňujte žáky na možná nebezpečí, na která mohou na internetu narazit, kdykoliv je to možné. Pokud v rámci svého předmětu narazíte na tuto tématiku, využijte této možnosti k preventivní činnosti. Vyzvěte žáky k tvoření různých projektů týkající se bezpečnosti dětí na internetu.

2. **Více komunikujte o problematice s rodiči**

Jedním z nedostatku v preventivních programech probíhajících na školách se dle výzkumu diplomové práce zdá být nedostatečná komunikace na téma prevence mezi rodiči a školou. Řešte s rodiči danou problematiku, informujte je o probíhající prevenci. Můžete je tím inspirovat k další prevenci ve směru od rodiče k dítěti.

3. **Filtrace dostupného obsahu ve škole**

Pokud mají žáci ve škole přístup k připojení k internetu, omezte žákům dostupný zobrazovaný obsah. Blokujte přístup k webovým stránkám s nevhodným obsahem.

4. **Pořádejte projektové dny na téma prevence**

Díky projektovým dnům na téma prevence nebezpečí na internetu probíhá mezi žáky vzájemná interakce na dané téma. Žáci si tématiku projektových dní zapamatují leckdy lépe než téma opakované během vyučovacích hodin. Zároveň se do programu prevence zapojí i více pedagogů.

5. **Informační materiály**

Vyvěste na nástěnky informační materiály jako plakáty a letáky. Žáci tak budou mít řešenou problematiku stále na očích.

7 ZÁVĚR

Cílem této diplomové práce věnující se problematice zneužívání dětí v prostoru sociálních sítí bylo na základě zjištěných výsledků formulovat doporučení možných způsobů prevence zneužívání nezletilých osob na sociálních sítích pro rodiče, základní školy a víceletá gymnázia.

Teoretická část práce se zabývala vymezením základním pojmů z oblasti kyberprostoru kybernetické kriminality a kybernetické bezpečnosti. Byly zde popsány nejčastější trestné činy páchané na dětech v prostoru sociálních sítí, a jejich dopad na děti. Kapitoly se zabývaly také chováním dětí na internetu, různými statistikami, prevencí a protiopatřeními zneužívání nezletilých na sociálních sítí, a osvětou. Na konci teoretické části byly shrnuty právní normy v kontextu kriminality páchané na dětech.

Empirická část práce byla věnována smíšenému výzkumu, který byl proveden pomocí časově náročných řízených rozhovoru s rodiči a vyučujícími druhého stupně základních škola a odpovídajících ročníků víceletých gymnázií. Získaná data byla statisticky zpracována a vyhodnocena obsahovou analýzou. Komparací získaných dat se podařilo potvrdit či vyvrátit všechny pro práci stanovené hypotézy.

Na podkladě výsledků výzkumu byla analyzována slabá místa probíhající prevence v rodinách a na školách, následně vytvořeny formulace návrhů doporučení pro rodiče a školy. Doporučení jsou obecná a mohou být využita pro inspiraci všech rodičů či škol.

V rámci práce také vznikl informační leták pro rodiče, který je součástí příloh práce, a který by případně mohl být poskytován rodičům na třídních schůzkách

jako upozornění na problematiku a případný návod pro prevenci. Dle názoru autora práce byly všechny cíle diplomové práce byly splněny.

8 SEZNAM POUŽITÝCH ZKRATEK

ARPA – Advanced Research Project Agency

BBN – Bolt, Beranek and Newman

CAN – Child Abuse and Neglect

CAS – Child Sexual Abuse

ČR – Česká republika

DVPP – Další vzdělávání pedagogických pracovníků

EU – Evropská unie

Europol – Evropský policejní úřad

FESNET – Federal Educational and Scientific Network

IMP – Interface Message Processor

IP – Internet Protocol

IVT – Informatika a výpočetní technika

MIT – Massachutsetts Institute of Technology

MŠMT – Ministerstvo školství, mládeže a tělovýchovy

NORSAR – Norwegian Seismic Array

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

Sb.- Sbírky

SMS – Short Message Service

ŠVP – Školní vzdělávací program

TCP – Transmission Control Protocol

USA – Spojené státy americké

WWW – World Wide Web

9 SEZNAM POUŽITÉ LITERATURY

1. KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7.
2. Historie internetu. *Jak na internet* [online]. [cit. 2022-01-24]. Dostupné z: https://www.jaknainternet.cz/page/1205/historie-internetu/
3. HOUSER, Pavel. Historie internetu v datech. *Sciencemag.cz* [online]. 2017 [cit. 2022-01-24]. Dostupné z: https://sciencemag.cz/historie-internetu-v-datech/
4. Co je to kyberprostor. *Správa sítě: Slovník pojmů* [online]. [cit. 2022-01-25]. Dostupné z: https://www.sprava-site.eu/kyberprostor/
5. KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7.
6. Zákon č. 181/2014 Sb. o kybernetické bezpečnosti
7. Slovník pojmů: Surface Web. *NejPřipojení.cz* [online]. [cit. 2022-01-26]. Dostupné z: https://nejpripojeni.cz/slovnik-pojmu/surface-web/
8. NETOLIČKA, Jan. Deep a Dark web - temná strana internetu: Surface Web. *IPure.cz* [online]. 3.9.2020 [cit. 2022-01-26]. Dostupné z: https://ipure.cz/archiv/magazin/deep-a-dark-web-temna-strana-internetu/
9. Slovník pojmů: Deep Web. *NejPřipojení.cz* [online]. [cit. 2022-01-27]. Dostupné z: https://nejpripojeni.cz/slovnik-pojmu/deep-web/
10. Slovník pojmů: Dark Web. *NejPřipojení.cz* [online]. [cit. 2022-01-27]. Dostupné z: https://nejpripojeni.cz/slovnik-pojmu/dark-web/
11. NCKB. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2022-02-01]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/
12. Kybernetická kriminalita. *Internetem bezpečně* [online]. [cit. 2022-02-01]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/dobre-vedet/kyberneticka-kriminalita/

13. KOŽÍŠEK, Martin a Václav PÍSECKÝ. *Bezpečně na internetu: průvodce chováním ve světě online*. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.
14. Sociální sítě. *Nebojte se internetu* [online]. [cit. 2022-02-01]. Dostupné z: https://www.nebojteseinternetu.cz/page/3396/socialni-site/
15. Facebook. *Idealab* [online]. [cit. 2022-02-01]. Dostupné z: https://idealab.cz/slovnik/facebook/
16. Facebook. *Aktuálně.cz* [online]. 2021 [cit. 2022-02-03]. Dostupné z: https://www.aktualne.cz/wiki/ekonomika/facebook/r~i:wiki:1064/
17. Podmínky používání služby. *Facebook* [online]. 2021 [cit. 2022-02-03]. Dostupné z: https://www.facebook.com/legal/terms
18. Twitter. *Aktuálně.cz* [online]. [cit. 2022-02-04]. Dostupné z: https://www.aktualne.cz/wiki/veda-a-technika/twitter/r~i:wiki:1441/
19. Instagram pro začátečníky? Máme tu návod pro Instagram, pokud ho postrádáte. *365tipů.cz* [online]. [cit. 2022-02-05]. Dostupné z: https://365tipu.cz/instagram-pro-zacatecniky-mame-tu-navod-pro-instagram-pokud-ho-postradate/
20. TikTok – průvodce pro rodiče. *Apple.com* [online]. [cit. 2022-02-07]. Dostupné z: https://apps.apple.com/cz/story/id1437295624?l=cs
21. ROSULEK, Martin. Co je TikTok a jak funguje? Vše, co musí vědět uživatel i marketák. *Digitální nomádství* [online]. 2.10.2020 [cit. 2022-02-07]. Dostupné z: https://digitalninomadstvi.cz/tiktok/
22. YouTube. *Aktuálně.cz* [online]. 14.1.2021 [cit. 2022-02-07]. Dostupné z: https://www.aktualne.cz/wiki/zahranici/youtube/r~i:wiki:1147/
23. JANDURA, Xaver. Snapchat: Mladými oblíbený, pro mnohé zábavný, ale zatraceně chaotický. *SMARTMANIA* [online]. [cit. 2022-02-07]. Dostupné z: https://smartmania.cz/snapchat-mladymi-oblibeny-pro-mnohe-zabavny-ale-zatracene-chaoticky/

24. Snapchat už nepřináší revoluční novinky, pouze rizika. *E-bezpečí* [online]. [cit. 2022-02-07]. Dostupné z: https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/socialni-site/1441-snapchat-uz-neprinasi-revolucni-novinky-pouze-rizika
25. Badoo. *Recenzer* [online]. 2.1.2022 [cit. 2022-02-07]. Dostupné z: https://www.recenzer.cz/seznamky/badoo/
26. Co je to Badoo?. *IT SLOVNÍK.CZ* [online]. [cit. 2022-02-07]. Dostupné z: https://it-slovnik.cz/pojem/badoo
27. Často kladené otázky: Vše o tvém profilu a propojeních. *Tinder* [online]. [cit. 2022-02-07]. Dostupné z: https://tinder.com/cs/faq
28. Co je tinder?. *Tinder* [online]. [cit. 2022-02-07]. Dostupné z: https://www.help.tinder.com/hc/cs/articles/115004647686-Co-je-Tinder-
29. SLÍŽEK, David. Lide.cz v půlce prosince definitivně končí, seznamka Seznamu si nevydělá na provo. *Lupa.cz* [online]. 18.11.2020 [cit. 2022-02-07]. Dostupné z: https://www.lupa.cz/aktuality/lide-cz-v-pulce-prosince-definitivne-konci-seznamka-seznamu-nevydelava/
30. KOPECKÝ, Kamil. Podvody s falešnými webkamerami. *E-bezpečí* [online]. 2013 [cit. 2022-02-16]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/sociotechnika/637-podvody-s-falenymi-webkamerami-
31. KOPECKÝ, Kamil, René SZOTKOWSKI a Pavla DOBEŠOVÁ. *Riziková komunikace a seznamování českých dětí v kyberprostoru*. Olomouc: Univerzita Palackého v Olomouci, 2021. ISBN 978-80-244-5914-1.
32. Co je kyberstalking. *02 - Chytrá škola* [online]. [cit. 2022-02-19]. Dostupné z: https://vyuka.o2chytraskola.cz/clanek/26/kyberstalking/
33. Kyberstalking. *Internetem bezpečně* [online]. [cit. 2022-02-19]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kyberstalking/

34. Co je to stalking a cyberstalking. *E-bezpečí* [online]. 2008 [cit. 2022-02-19]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/stalking-a-kyberstalking/66-23
35. ŠEVČÍKOVÁ, Anna. *Děti a dospívající online: vybraná rizika používání internetu*. Praha: Grada, 2014. Psyché (Grada). ISBN 978-80-247-5010-1.
36. BEDROŠOVÁ, M., HLAVOVÁ, R., MACHÁČKOVÁ, H., DĚDKOVÁ, L., & ŠMAHEL, D. EU Kids Online IV v České republice: *České děti a dospívající na internetu: Zpráva z výzkumu na základních a středních školách* [online]. Brno, 2018 [cit. 2022-03-29]. Dostupné z: https://irtis.muni.cz/media/3137006/eu_kids_online_report_2018_cz_main.pdf. Masarykova univerzita.
37. VÁGNEROVÁ, Marie a Lidka LISÁ. *Vývojová psychologie: dětství a dospívání*. Vydání třetí, přepracované a doplněné. Praha: Univerzita Karlova, nakladatelství Karolinum, 2021. ISBN 978-80-246-4961-0.
38. MACEK, Petr. *Adolescence*. Vyd. 2., upr. Praha: Portál, 2003. ISBN 80-717-8747-7.
39. VYBÍRAL, Zbyněk. *Psychologie komunikace*. Praha: Portál, 2005. ISBN 80-717-8998-4.
40. KOVÁŘOVÁ, Veronika a Kamil KOPECKÝ. *E-bezpečí: Fenomén – disinhibiční efekt* [online]. 1.6.2012 [cit. 2022-03-30]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/dali-rizika/485-fenomen-disinhibini-efekt
41. MACHKOVÁ, Alexandra. Mýty a fakta o sexuálním zneužívání dětí. *Šance dětem* [online]. 1.11.2012 [cit. 2022-03-30]. Dostupné z: https://sancedetem.cz/myty-fakta-o-sexualnim-zneuzivani-deti
42. DUNOVSKÝ, Jiří. *Týrané, zneužívané a zanedbávané dítě*. Praha: Grada, 1995. ISBN 80-716-9192-5.
43. Problematika sexuálního zneužívání. *Centrum Elektra* [online]. 20.10.2013 [cit. 2022-03-30]. Dostupné z: http://centrumelektra.cz/?p=35

44. LENDLEROVÁ, Denisa. *Osobní pohled dítěte na prožité sexuální zneužívání a jeho sociální dopad – rozbor monografie*. České Budějovice, 2017. Diplomová práce. Jihočeská univerzita v Českých Budějovicích. Vedoucí práce Prof. MUDr. Miloš Velemínský CSc., dr. h. c.
45. WEISS, Petr. *Sexuální zneužívání dětí*. Praha: Grada, 2005. Psyché (Grada). ISBN 80-247-0929-5.
46. V Síti: O filmu. *V Síti* [online]. [cit. 2022-04-01]. Dostupné z: https://vsitifilm.cz/o-filmu.html
47. KARBAN, Filip. Jak skončili sexuální predátoři z filmu V síti. *Seznam Zprávy* [online]. 13.3.2021 [cit. 2022-04-01]. Dostupné z: https://www.seznamzpravy.cz/clanek/jak-skoncili-sexualni-predatori-z-filmu-v-siti-146775
48. Online projekce filmu V síti přímo ve školách. *Aerofilms* [online]. 12.10.2020 [cit. 2022-04-01]. Dostupné z: https://www.aerofilms.cz/magazin/online-projekce-filmu-v-siti-primo-ve-skolach/?fbclid=IwAR3lgQIc5uEHe98Ld9PwJ6V8iRFCF9zwHxJj7IW3jYI3RrMta9jT_fxIxJw
49. Pro média: O projektu. *Bud' safe online* [online]. [cit. 2022-04-01]. Dostupné z: https://www.avast.com/cz/besafeonline/pro-media
50. RANDÁKOVÁ, Růžena. #SayNo! - Celoevropská kampaň proti zneužívání dětí online. *Policie ČR* [online]. 19.6.2017 [cit. 2022-04-01]. Dostupné z: https://www.policie.cz/clanek/sayno-celoevropska-kampan-proti-internetovemu-sexualnimu-natlaku-a-vydirani-deti-rekni-ne.aspx
51. Europol's 'Say No!' campaign travels to the Western Balkans. *Europol* [online]. [cit. 2022-04-01]. Dostupné z: https://www.europol.europa.eu/media-press/newsroom/news/europol's-'say-no'-campaign-travels-to-western-balkans-0
52. Together for a better internet. *Safer Internet Day* [online]. [cit. 2022-04-02]. Dostupné z: https://www.saferinternetday.org

53. TÝŘOVÁ, Zuzana. Den bezpečnějšího internetu 2022. *Policie ČR* [online]. 8.2.2022 [cit. 2022-04-02]. Dostupné z: https://www.policie.cz/clanek/uzemni-utvary-krajske-reditelstvi-policie-kvk-zpravodajstvi-den-bezpecnejsiho-internetu-2022.aspx
54. DLUBALOVÁ, Klára. Česko slaví Den bezpečnějšího internetu. *Ministerstvo vnitra České republiky* [online]. 8.2.2022 [cit. 2022-04-02]. Dostupné z: https://www.mvcr.cz/clanek/cesko-slavi-den-bezpecnejsiho-internetu.aspx
55. KOPECKÝ, Kamil. Rodičům: Jak s dítětem komunikovat o tématech spojených s online seznamováním a online abuzéry?. *E-bezpečí* [online]. 20.1.2020 [cit. 2022-04-02]. Dostupné z: https://www.e-bezpeci.cz/index.php/rodicum-ucitelum-zakum/1756-rodicum-jak-s-ditetem-komunikovat-o-tematech-spojenych-s-online-seznamovanim-a-online-abuzery
56. REZEK, Tomáš. Nejlepší návod, jak ochránit vaše dítě v online světě 2022. *VpnMentor* [online]. [cit. 2022-04-02]. Dostupné z: https://cs.vpnmentor.com/blog/ucelena-rodicovska-prirucka-pro-ochranu-vaseho-ditete-na-internetu/
57. Aplikace rodičovské kontroly (parental control), které vám mohou pomoci zajistit bezpečí vašich dětí v online prostředí. *E-bezpečí* [online]. 30.1.2022 [cit. 2022-04-02]. Dostupné z: https://www.e-bezpeci.cz/index.php/rodicum-ucitelum-zakum/2471-aplikace-rodicovske-kontroly-parental-control-ktere-vam-mohou-pomoci-zajistit-bezpeci-vasich-deti-v-online-prostredi
58. Norton Family. *Norton* [online]. [cit. 2022-04-02]. Dostupné z: https://cz.norton.com/norton-family?nortoncountry=cz&om_sem_cid=hho_sem_sy:cz:ggl:cs:e:br:kw0000061171:511537754614:c:google:12661635283:122798997280:kwd-11838054794&nortoncountry=CZ&gclsrc=aw.ds&gclid=Cj0KCQjw6J-

SBhCrARIsAH0yMZiJCHD6Nh6tqjejWj7Jxo6DoHWyOsvjmxz1sOrDt2QnJ2-_tu6W3fsaAv2CEALw_wcB

59. Google Family Link. *Google Play* [online]. [cit. 2022-04-03]. Dostupné z: https://play.google.com/store/apps/details?id=com.google.android.apps.kids.familylink&hl=cs&gl=US
60. Norton Family parental control. *Google Play* [online]. [cit. 2022-04-03]. Dostupné z: https://play.google.com/store/apps/details?id=com.symantec.familysafety&hl=cs&gl=CZ
61. Zákon č. 40/2009 Sb., trestní zákoník
62. *České děti v kybersvětě: Výzkumná zpráva* [online]. 2019 [cit. 2022-05-07]. Dostupné z: https://www.e-bezpeci.cz/index.php/ke-stazeni/vyzkumne-zpravy/117-ceske-deti-v-kybersvete/file
63. *Rodiče a jejich děti: Desatero bezpečného internetu* [online]. [cit. 2022-05-07]. Dostupné z: https://www.rodice-a-deti.cz/desatero-bezpecneho-internetu
64. *DESATERO DOBRÉHO „KYBERNETICKÉHO" RODIČE* [online]. [cit. 2022-05-11]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rodice/desatero-dobreho-kybernetickeho-rodice/

10 SEZNAM POUŽITÝCH OBRÁZKŮ

11 SEZNAM POUŽITÝCH TABULEK

12 SEZNAM PŘÍLOH

Příloha 1 - Informovaný souhlas s účastí na výzkumu

Informovaný souhlas s účastí na výzkumu

Informace o výzkumu:

Výzkum se zabývá problematikou zneužívání nezletilých osob na sociálních sítích, prevencí trestných činů páchaných na dětech a jejich protiopatření. V kvalitativním výzkumu bude prováděn rozbor mínění vyučujících druhého stupně základních škol, vyučujících odpovídajících ročníků víceletých gymnázií, a rodičů v dané problematice.

Prohlášení

Já níže podepsaný/-á potvrzuji, že

a) jsem se seznámil/-a s informacemi o cílech a průběhu výše popsaného výzkumu (dále též jen „výzkum“);

b) dobrovolně souhlasím s účastí své osoby v tomto výzkumu;

c) rozumím tomu, že se mohu kdykoli rozhodnout ve své účasti na výzkumu nepokračovat;

d) jsem srozuměn s tím, že jakékoliv užití a zveřejnění dat a výstupů vzešlých z výzkumu nezakládá můj nárok na jakoukoliv odměnu či náhradu, tzn. že veškerá oprávnění k užití a zveřejnění dat a výstupů vzešlých z výzkumu poskytuji bezúplatně.

Zároveň prohlašuji, že

a) souhlasím se zveřejněním anonymizovaných dat a výstupů vzešlých z výzkumu a s jejich dalším využitím;

b) rozhovor bude nahráván pro následný přepis, po kterém bude záznam smazán.

Výše uvedená svolení a souhlasy poskytuji dobrovolně na dobu neurčitou až do odvolání a zavazuji se je neodvolat bez závažného důvodu spočívajícího v podstatné změně okolností.
Vše výše uvedené se řídí zákony České republiky, s výjimkou tzv. kolizních norem, a bude v souladu s nimi vykládáno, přičemž případné spory budou řešeny příslušnými soudy v České republice.

Potvrzuji, že jsem převzal/a podepsaný stejnopis tohoto informovaného souhlasu.

Dne:

Jméno a příjmení:

Podpis:

Výzkumník: Bc. Dominika Kacetlová
ČVUT FBMI

Obrázek 6 - Informovaný souhlas s účastí na výzkumu

Příloha 2 - Otázky pro rodiče

1) Věk dítěte?
2) Navštěvuje Vaše dítě základní školu nebo víceleté gymnázium?
3) Pohlaví Vašeho dítěte?
4) Má Vaše dítě přístup k internetu? Z jakých zařízení?
5) Jak Vaše dítě získalo konkrétní zařízení?
6) Limitujete nějakým způsobem čas dítěte na internetu? Jak?
7) Věříte svému dítěti při pohybu na internetu?
8) Má Vaše dítě účet na nějaké sociální síti? Víte na Jaké?
9) Kontrolujete nějakým způsobem činnost dítěte na internetu? Pokud ano, jak?
10) Znáte aplikace rodičovské kontroly? Používáte je? Proč?
11) Omezujete nějakým způsobem obsah, ke kterému má Vaše dítě na internetu přístup?
12) Myslíte si, že Vašemu dítěti hrozí na internetu nějaké nebezpečí? Jaké?
13) Řešil jste nějakým způsobem s Vaším dítětem jeho bezpečí na internetu? Jak?
14) Myslíte si, že by měl zásady bezpečného internetu s dítětem řešit rodič, anebo škola? Proč?
15) Řešila s Vámi někdy škola Vašeho dítěte v rámci prevence problematiku bezpečnosti dětí na internetu?
16) Svěřilo by se Vám vaše dítě s problémem týkající se sociálních sítí?
17) Řešil jste již nějakým problém týkající se Vašeho dítěte a internetu?
18) Jaké ponaučení jste dal/a dítěti, když začalo používat internet?

Příloha 3 - Otázky pro vyučující

1) Vyučujete na škole anebo víceletém gymnáziu?
2) Vaše odučené roky?
3) V jakém vztahu jste ke třídám druhého stupně či odpovídajícím třídám víceletého gymnázia?
4) Mají žáci ve škole přístup k internetu mimo hodiny informatiky? Jak?
5) Prochází dostupný internetový obsah ve škole nějakou filtrací?
6) Ukládají Vám učební osnovy vašeho předmětu probírat s žáky problematiku bezpečnosti na internetu?
7) Řešíte tuto problematiku s žáky nad rámec učebních osnov?
8) Řeší se problematika bezpečnosti na internetu v třídnických hodinách?
9) Vzděláváte se nějakým způsobem v této problematice? Jak?
10) Probíhá ve škole prevence na téma této problematiky? Jak?
11) Myslíte si, že by zásady bezpečného internetu měl s dítětem řešit rodič, anebo škola? Proč?
12) Řešíte v rámci prevence problematiku bezpečnosti dětí na internetu nějakým způsobem s rodiči žáků?
13) Řešil jste již nějaký problém týkající se zneužívání dětí na sociálních sítích v praxi? Svěřil se Vám žák s takovým problémem? Jak jste situaci řešil?

Příloha 4 - Vzorový přepis rozhovoru

Tazatel: „Vyučujete na základní škole nebo víceletém gymnáziu?“
Respondent: „Vyučuji na základní škole.“

Tazatel: „Kolik let již učíte?“
Respondent: „Začala jsem hned po vysoké škole, takže to jsou už 3 roky.“

Tazatel: „Jaký vztah máte k těmto třídám? Jste třídní učitel?“
Respondent: „Jsem třídní učitel 6. třídy“

Tazatel: „Mají žáci ve škole přístup k internetu mimo hodiny informatiky?“
Respondent: „Ano mají.“
Tazatel: „Jak?“
Respondent: „Někteří mají neomezená data na svých mobilech a dělají hotspot svým spolužákům. Na školní síť, nebo školní Wi-Fi ale přístup mimo hodiny informatika nemají.“

Tazatel: „Prochází dostupný internetová obsah ve škole nějakou filtrací jako jsou zakázané stránky apod.?“
Respondent: „Ano, prochází, nevím přesně čím, ale i školní e-maily jsou hlídány.“

Tazatel: „Ukládají Vám učební osnovy Vašeho předmětu probírat s žáky problematiku bezpečnosti na internetu?“
Respondent: „Vzhledem k tomu, že neučím informatiku, tak úplně ne, ale na začátku školního roku děti upozorňujeme, aby si na internetu dávali pozor, a v průběhu roku, pokud je to možné, jsou pořádány různé workshopy, nebo přednášky, na toto téma“

Tazatel: „Řešíte tuto problematiku se studenty nad rámec učebních osnov?“
Respondent: „Já osobně ne.“

Tazatel: „Řeší se tato problematika v třídnických hodinách?“

Respondent: „Ano, pokud nastane nějaký problém, nebo je potřeba toto téma otevřít.“

Tazatel: „Vzděláváte se nějakým způsobem v této problematice?“
Respondent: „Ano.“
Tazatel: „Jakým způsobem?“
Respondent: „V rámci dalšího vzdělávání pedagogických pracovníků jsou v nabídce různé kurzy a semináře.“

Tazatel: „Probíhá ve škole prevence na téma této problematiky?“
Respondent: „Ano, pokud se podaří získat nějaký vzdělávací program, nebo přednášku.“

Tazatel: „Myslíte si, že by zásady bezpečného internetu měl s dítětem řešit rodič, anebo škola?“
Respondent: „Myslím si, že oba. Děti si mnohdy myslí, že se je snažíme pouze „strašit“, když to ale slyší od více zdrojů, nebo pak bohužel narazí na nějaký problém, zjistí i zbytek, že to nebylo pouhé upozorňování, ale že se to opravdu děje.“

Tazatel: „Řešíte v rámci prevence problematiku bezpečnosti na internetu nějakým způsobem s rodiči?“
Respondent: „Nevím o tom.“

Tazatel: „Řešil jste již nějaký problém týkající se zneužívání dětí na sociálních sítích v praxi? Svěřil se Vám žák někdy s takovým problémem?“
Respondent: „Ne, naštěstí ještě ne.“

Příloha 5 - Návrh informačního letáku pro rodiče

Obrázek 7 - Návrh informačního letáku pro rodiče

Obsah informačního letáku byl vytvořen na základě článku Desatero dobrého „kybernetického“ rodiče. [63] Leták může sloužit i jako propagační materiál pro webové stránky věnující se problematice bezpečnosti dětí v kyberprostoru.