VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

RIZIKA VIRTUÁLNÍHO SVĚTA U ŽÁKŮ ZÁKLADNÍCH ŠKOL V MARIÁNSKÝCH LÁZNÍCH

Autor práce: Ladislav Sidorják, DiS

Studijní program: Bezpečnostně právní činnost

Forma studia: Kombinovaná

Vedoucí práce: Mgr. Milan Kocík, MBA

Katedra: Katedra právních oborů a bezpečnostních studií

2022

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.
Žižkova tř. 6, 370 01 České Budějovice

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Ladislav Sidorják, DiS

Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Místo studia: Příbram

Název bakalářské práce: Rizika virtuálního světa u žáků základních škol v Mariánských Lázních

Název bakalářské práce v anglickém jazyce: Risks of the virtual world in primary school pupils in Mariánské Lázně

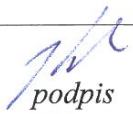
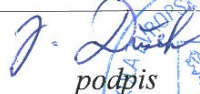
Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce (jméno a příjmení, titul): Mgr. Milan Kocík, MBA

Datum zadání bakalářské práce (měsíc, rok):

Cíl bakalářské práce: Cílem práce je zanalyzovat, do jaké míry je schopnost žáků základních škol, čelit rizikům kyberprostoru, především pak kybergroomingu, ovlivněna prostředím, ve kterém se pohybují. K dosažení hlavního cíle budou zvoleny cíle dílčí: Určit, do jaké míry jsou děti obeznámeny s riziky virtuálního světa z domácího prostředí, v jakém rozsahu pomáhají v orientaci školní vzdělávací aktivity a jak žáci chápou problematiku kyberkriminality.

Student: Ladislav Sidorják, DiS	6. 11. 2021 *datum*	 *podpis*
Vedoucí práce: Mgr. Milan Kocík, MBA	6. 11. 2021 *datum*	 *podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	6. 12. 2021 *datum*	 *podpis*
Prorektor pro studium a vnitřní záležitosti: Doc. PhDr. Miroslav Sapík, PhD.	8. 12. 2021 *datum*	 *podpis*
Pověřený rektor: doc. Ing. Jiří Dušek, Ph.D.	14. 12. 2021 *datum*	 *podpis*

Prohlašuji, že jsem bakalářskou práci vypracoval(a) samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce v elektronické podobě ve veřejně přístupné části infodisku VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucí(ho) a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Děkuji vedoucí(mu) bakalářské práce Mgr. Milanovi Kocíkovi, MBA za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

SIDORJÁK, L. *Rizika virtuálního světa u žáků základních škol v Mariánských Lázních: bakalářská práce*. České Budějovice: Vysoká škola evropských a regionálních studií, 2022. 59 s. Vedoucí bakalářské práce: Mgr. Milan Kocík, MBA

Klíčová slova: rizika, virtuální svět, online, žáci základních škol.

Práce pojednává o rizicích virtuálního světa u žáků základních škol. Teoretická východiska nám definují pojmy internet, realita, virtuální realita, digitální stopa, sociální síť. Druhá kapitola teoretické části se zaměřuje na fundamentální hrozby, kterým běžný uživatel internetu může čelit. Jedná se o problematiku kyberšikany, sextingu a kyberstalkingu. Kapitola čtyři je věnována hrozbě zvané kybergrooming, a to jak z pohledu oběti, tak i z pohledu trestního zákoníku. Důležitý prostor je v páté kapitole otevřen přehledu Rámcového vzdělávacího programu pro základní vzdělávání a vzdělávacím programům základních škol, které jsou zaměřeny na informační a komunikační technologie pro žáky prvního a druhého stupně základních škol. Cílem práce bylo stanoveno zjistit, do jaké míry jsou žáci základních škol v Mariánských Lázních znalí rizik virtuálního prostředí. Pro objasnění problému, jak žáci šestých tříd základních škol v Mariánských Lázních vnímají rizikovost online prostředí, byly zvoleny tři cíle: Určit, do jaké míry jsou děti obeznámeny s riziky virtuálního světa z domácího prostředí, od rodičů. Zjistit, v jakém rozsahu s orientací v rizicích kyberprostoru pomohlo prostředí školy a školní vzdělávací aktivity. Zmapovat, v jakém rozsahu se žáci orientují v oblasti kyberkriminality. K dosažení všech vytyčených cílů bylo použito dotazníkové šetření, kdy byly žákům šestých tříd základních škol v Mariánských Lázních kladeny otázky, zaměřené na danou problematiku. Pozitivním zjištěním bylo, že se dětem v oblasti hrozeb virtuálního světa věnují jak rodiče, tak i učitelé. Ovšem dosažené znalosti jsou mnohdy povrchní a děti tak nejsou schopny, v případě hrozby, zanalyzovat situaci tak, aby správnou reakcí ochránily sebe a své soukromí. Podobný závěr je možné vyvodit také z rozhovoru s pedagogickým pracovníkem, což v tomto případě byla kvalitativní část průzkumného šetření. V závěru jsou výsledky průzkumného šetření shrnuty a na základě analýzy bylo vyvozeno několik doporučení pro praxi.

ABSTRACT

SIDORJÁK, L. *Risks of the Virtual World for Primary School Pupils in Mariánské Lázně: Bachelor's Thesis.* České Budějovice: University of European and Regional Studies, 2022. 59 pp. Thesis supervisor: Mgr. Milan Kocík, MBA

Key words: risks, virtual world, online, primary school students.

The thesis deals with the risks of the virtual world for primary school students. Theoretical background defines the terms internet, reality, virtual reality, digital footprint, social network. The second chapter of the theoretical part focuses on the fundamental threats that the average Internet user may face. This is an issue of cyberbullying, sexting and cyberstalking. Chapter four is devoted to the threat called cybergrooming, both from the perspective of the victim and from the perspective of the Criminal Code. An important area in the fifth chapter is open to an overview of the Framework Educational Program for Primary Education and primary school educational programs, which are focused on information and communication technologies for primary and secondary school pupils. The aim of the work was to find out to what extent primary school students are aware of the risks of the virtual environment. To clarify the problem of how sixth graders perceive the riskiness of the online environment, three goals were chosen: To determine the extent to which children are familiar with the risks of the virtual world from the home environment, from their parents. To find out to what extent the environment of the school and school educational activities helped with orientation in the risks of cyberspace. To map the extent to which primary school students are oriented in the field of cybercrime. To achieve all the set goals, a questionnaire survey was used, when the pupils of the sixth grades of primary schools were asked questions focused on the given issue. A positive finding was that both parents and teachers care about children in the area of virtual world threats. However, the knowledge gained is often superficial and children are not able, in the event of a threat, to analyze the situation so that they can protect themselves and their privacy with the right response. A similar conclusion can also be drawn from an interview with a pedagogical worker, which in this case was a qualitative part of the survey. In conclusion, the results of the survey are summarized and based on the analysis, several recommendations for practice were derived.

Obsah

Úvod

V dnešní době, kdy se většina z nás pohybuje současně v několika paralelních světech, kdy jeden je skutečný a ostatní jsou virtuální, je potřeba se zamyslet nad tím, do jaké míry jsou tyto světy provázané, jakým způsobem se vzájemně ovlivňují, jakým způsobem nám prospívají a jakým způsobem nás mohou ohrozit.

Tématem bakalářské práce byla zvolena rizika virtuálního světa u žáků základních škol v Mariánských Lázních. Motivací byla vlastní zkušenost s prací s dětmi na základních školách v oblasti prevence kyberkriminality, dále zjištění, jak snadno se děti a dospívající mohou stát obětmi predátorů kyberprostoru a jak důležité je preventivní působení na zmíněné skupiny v oblasti rizik online prostředí. V teoretických východiscích byly charakterizovány s tématem související základní pojmy, jako je internet, realita a virtuální realita. Dále byly definovány činnosti i hrozby v online prostředí, specifikována pravidla netikety a identifikovány tváře kyberkriminality. Ve vztahu k žákům byl věnován prostor rámcovému vzdělávacímu programu a školským vzdělávacím programům jednotlivých základních škol. K orientaci v dané problematice bylo využito studium literárních, internetových a jiných zdrojů, jakými jsou například statistická data. Cílem práce bylo stanoveno zanalyzovat, do jaké míry je schopnost žáků základních škol v Mariánských Lázních, čelit rizikům kyberprostoru, především pak kybergroomingu, ovlivněna prostředím, ve kterém se pohybují. Pro objasnění problému, jak žáci šestých tříd vnímají rizikovost online prostředí, byly zvoleny dílčí cíle: Určit, do jaké míry jsou děti obeznámeny s riziky virtuálního světa z domácího prostředí, od rodičů. Zjistit, v jakém rozsahu s orientací v rizicích kyberprostoru pomohlo prostředí školy a školní vzdělávací aktivity. Zmapovat, v jakém rozsahu se žáci základních škol orientují v oblasti kyberkriminality.

V dnešní době, kdy prevalence kybernetických útoků a kriminálních činů má stále rostoucí charakter, je zcela žádoucí se věnovat analytickým činnostem a s relevantními výsledky pak investovat čas preventivní osvětě ohrožených skupin. Je zcela zřejmé, že rizika v online prostředí mohou být hrozbou pro každého uživatele, a to v jakémkoliv věku, napříč celou společností. Většina rodičů dětí a dospívajících má pocit, že své děti znají, že plně kontrolují náplň jejich volnočasových aktivit, že mají přehled o jejich pohybu virtuálním světem. Ale ani ten nejdůslednější rodič nemá šanci na absolutní kontrolu, pokud si to jeho dítě nepřeje. Právě děti jsou díky své psychické a sociální

nezralosti pro kybernetické predátory skupinou velmi snadno ovladatelnou a manipulovatelnou. Je potřeba jim být nápomocni v rozlišování zla a dobra. Cesta, jak nevnímat internet jako hrozbu, jak různé druhy kriminality internetového prostředí minimalizovat, je zařazení programů zaměřených na prevenci. Schopnost pohybovat se virtuálním světem bezpečně, informovaně a uživatelsky zodpovědně nám zajistí pocit, že internet je úžasný zdroj informací, zábavy a komunikace, který nám do života přinese novou úroveň seberealizace.

1 CÍL A METODIKA BAKALÁŘSKÉ PRÁCE

Cílem práce je zanalyzovat, do jaké míry jsou žáci vybraných základních škol v Mariánských Lázních schopni rozpoznat rizika kyberprostoru, především pak kybergroomingu.

Průzkumným problémem je vliv online prostředí, ve kterém se žáci základních škol pohybují, na jejich orientaci v online světě a s tím související schopnost čelit negativním hrozbám kyberprostoru.

1.1 Dílčí průzkumné cíle

1. Cíl průzkumu: Určit, do jaké míry jsou děti obeznámeny s riziky virtuálního světa z domácího prostředí.
2. Cíl průzkumu: Zjistit, v jakém rozsahu s orientací v rizicích kyberprostoru pomohlo prostředí školy a školní vzdělávací aktivity.
3. Cíl průzkumu: Zmapovat, v jakém rozsahu se žáci základních škol orientují v oblasti kyberkriminality.

1.2 Metodika průzkumu

K uskutečnění průzkumného šetření byla zvolena kvantitativní metoda v podobě dotazníkového šetření a kvalitativní metoda v podobě anonymizovaného řízeného rozhovoru.

Kvantitativní metoda, dotazníkové šetření bylo prioritně zaměřeno na znalosti a orientaci žáků základních škol v online prostředí, zároveň byly popsány základní pojmové znaky. Jelikož se jednalo o průzkum cílený, byl pro sběr empirických dat vytvořen anonymní, polostrukturovaný dotazník. Vzhledem k přetrvávající pandemické situaci a aktuálním omezujícím opatřením byla složitá osobní distribuce dotazníků v tištěné formě. Z tohoto důvodu byla zvolena forma vytvoření online dotazníku, kdy bylo této služby využito na webu Click4Survery.cz. Vytvoření konečné verze dotazníku předcházel pilotážní průzkum s cílem zjistit, jsou-li ve vytvořeném dotazníku otázky formulovány srozumitelně, jasně a zda odpovědi naplní podstatu průzkumného šetření. V rámci pilotážní studie bylo ve druhé polovině měsíce listopadu 2021 distribuováno 20 dotazníků mezi žáky šestých tříd základních škol v Mariánských Lázních. Návratnost

vyplněných dotazníků byla 13, tedy 65%, což bylo dostačující k posouzení, že je dotazník sestaven tak, aby splňoval námi požadovanou funkci. Na základě ústního souhlasu ředitelů základní školy Jih a základní školy Úšovice z Mariánských Lázní bylo zahájeno průzkumné šetření. S pomocí třídních učitelů šestých ročníků základních škol byl distribuován odkaz na elektronický dotazník s požadavkem na jeho vyplnění v rámci plnění zadání domácího úkolu. Celkem se jednalo o distribuci 154 dotazníků, z nichž 84 byly distribuovány žákům základní školy Úšovice a 70 žákům základní školy Jih. Průzkumné šetření bylo realizováno v období od listopadu 2021 do března 2022.

Kvalitativní metoda, anonymizovaný řízený rozhovor byl veden s pedagogem základní školy, který se věnuje výuce informačních a komunikačních technologií. Cílem rozhovoru bylo získat pohled pedagoga na problematiku kyberkriminality, především pak kybergroomingu u žáků základních škol a zároveň zjistit, do jaké míry se školní prostředí podílí na prevenci kyberkriminality a pomoci případným obětem predátorů online prostředí. Anonymizace byla zvolena z důvodu získání pravdivých, plnohodnotných a ucelených informací, které budou vypovídající o reálné skutečnosti. Před začátkem rozhovoru byl pedagog seznámen s předem připravenými dotazy, kterých bylo celkem sedm.

1.3 Charakteristika zkoumaného vzorku

Kvantitativní metoda, dotazníkové šetření – výběr zkoumaného vzorku byl systematický a záměrný. Respondenti byli voleni mezi žáky základních škol v Mariánských Lázních a kritérium výběru byl věk 11 – 12 let, což odpovídá stupni vzdělávání v šestých třídách základních škol. Zkoumaný vzorek byl složen z 56 respondentů ze Základní školy Jih, kam bylo distribuováno 70 dotazníků, návratnost dotazníků tedy odpovídala 80 % a z 61 respondenta ze Základní školy Úšovice, kam byly distribuovány 84 dotazníky, z nichž se k vyhodnocení navrátil 61 dotazník, což odpovídá 72,6% návratnosti. Celkem byly tedy distribuovány 154 dotazníky, k vyhodnocení se jich vrátilo 117 plnohodnotně vyplněných, což odpovídá 76% návratnosti. Respondentů bylo celkem 117, z toho 55 chlapců a 62 dívek.

Tabulka 1 Přehled složení průzkumného vzorku celkem (Zdroj: Autor)

Skupiny respondentů	Absolutní počet (n)	Relativní počet (%)
Chlapci	55	47%
Dívky	62	53%

Průzkumný vzorek byl složen ze 117 respondentů. Chlapců bylo 55, což odpovídá 47 % z celku. Dívky byly 62, což tvoří 53 % z celku.

Kvalitativní metoda, anonymizovaný řízený rozhovor – respondent byl zvolen jeden, jednalo se o pedagogického pracovníka s dlouholetou praxí v oboru výpočetní technologie a komunikace pro žáky základních škol.

2 INTERNET

K pojmu Internet bychom našli celou řadu definic, více či méně zaměřených na dílčí činnosti, konkrétní funkce a možnosti využití. Na Internet bychom mohli hledět jako na datovými linkami celosvětově propojené stále spuštěné počítače. Dle Dostála jde o „*celosvětovou síť propojující menší počítačové sítě, která se neustále po stránce geografické rozšiřuje a je omezena velikostí Země*“[1]. Do internetové sítě jsou počítače zapojeny buď jako servery, které své služby poskytují, nebo jako klientské stroje, které tyto služby využívají[2].

Název Internet má původ v anglickém a latinském jazyce. Vznikl z anglického slova network (síť), podle něhož tak byly tvořeny koncovky názvů amerických počítačových sítí a latinské předpony inter (mezi). Slovo Internet tak vyjadřuje absorbování, případně propojení všech starších, dílčích a lokálních sítí. Internet je prostředek předávání informací a poskytování služeb, mezi které patří elektronická pošta, chat, katalogizace, sdílení souborů, webové stránky a podobně[3].

Samotná historie vzniku internetu sahá do poloviny šedesátých let minulého století, kdy americká armáda hledala způsob, jak by bylo možné propojit důležité vojenské základny, strategická místa a zajistit tak funkční výměnu informací, a to především v situaci válečného konfliktu. Podmínkou bylo zachování informačního systému i v případě selhání a odříznutí některé za zainteresovaných základen. Pomocí metody trasování tak v roce 1969 vznikla první síť ministerstva obrany USA, nazvaná dle pracoviště Advanced Reseaech Project Agency – ARPANET. Tato síť byla navržena bez hlavního řídícího centra. Teprve mnohem později, v devadesátých letech dvacátého století, dochází ke komercializaci internetu a příliv peněz ze soukromého sektoru tak zajistil jeho exponenciální rozvoj. Dnes je internet každodenní součástí života a je důležité si uvědomit, že nemá vlastníka, nikdo jej tedy direktivně neřídí[4].

[1] DOSTÁL, J. 2011. *Internet druhé generace pro učitele*. 1. vydání. Olomouc: Univerzita Palackého v Olomouci. 2011. 70 s. ISBN 978-80-244-2779-9, str.7.
[2] DOSTÁL, J. 2011. *Internet druhé generace pro učitele*. 1. vydání. Olomouc: Univerzita Palackého v Olomouci. 2011. 70 s. ISBN 978-80-244-2779-9.
[3] PROCHÁZKA, D. 2010. *První kroky s internetem.* 3. aktualizované vydání. Praha: Grada Publishing, a.s. 2010. 112 s. ISBN 978-80-247-3255-8.
[4] DOSTÁL, J. 2011. *Internet druhé generace pro učitele*. 1. vydání. Olomouc: Univerzita Palackého v Olomouci. 2011. 70 s. ISBN 978-80-244-2779-9.

Tak, jako jsou součástí běžného společenského života pravidla chování neboli etiketa, tak se nedílnou součástí pohybu v online prostředí staly zásady chování na internetu neboli netiketa. Nejedná se přímo o ucelený přesný seznam pravidel, jedná se spíše o výčet doporučení, která nejsou v žádném ohledu právně vymahatelná, ale kterými by se měli uživatelé řídit proto, aby bylo prostředí přátelské a přívětivé.

Netiketě se ve své knize věnovala Virginia Shea, která jednotlivá pravidla definovala:

- Prvním pravidlem je docela určitě ohleduplnost k člověku, se kterým komunikujeme.
- Druhé pravidlo vyzývá ke slušnosti a neporušování zákonů.
- Třetí pravidlo upozorňuje na důležitost rozlišit, kde se v kyberprostoru nacházíme.
- Čtvrté pravidlo hovoří o respektu k času ostatních lidí.
- Páté pravidlo klade důraz na vybudování si dobré online pověsti.
- Šesté pravidlo vyzývá ke sdílení odborných znalostí.
- Sedmým pravidlem pomáhají uživatelé držet pod kontrolou flame wars.
- Osmé pravidlo zdůrazňuje respekt soukromí ostatních lidí.
- Deváté pravidlo žádá, aby nikdo nezneužíval své síly.
- Desáté pravidlo je výzvou k odpuštění chyb jiných.

Toto desatero můžeme zcela jistě chápat jako jistý kodex slušnosti v online prostředí a budeme-li se jím řídit, budeme součástí nekonfliktního prostředí, přínosného pro všechny zúčastněné[5].

S rozšířením internetu, s jeho snadnou přístupností a s nutností využívání jeho informačních kanálů se začíná hovořit o jeho nadužívání. Vzniká nejistota ohledně povahy závislosti na internetu, její konceptualizace. Ne zcela jasná interpretace klinických a teoretických východisek komplikuje pak výzkumy, kdy není zcela jasné, jaké nástroje měření je vhodné použít k měření prevalence v populaci, v souvislosti s mapováním problematických vzorců používání internetu. Různí autoři pak kladou důraz na různá diagnostická kritéria. V čem se však většina odborníků shodne, je rozdělení hodnotících škál do dvou základních kategorií. První kategorie měří obecnou závislost na internetu, do které patří excesivní, kompulzivní nebo patologické používání internetu a

[5] RECMANOVÁ, A. 2017. [online]. *Pravidla netikety*. [citováno 2021-10-10]. Dostupné na internetu: <https://medium.com/edtech-kisk/pravidla-netikety-ea92f7c3e58b>.

druhou kategorií hodnotících škál je měřena specifická online závislost, se zaměřením na problematické hraní online her, kybersex a závislost na online sociálních sítích[6].

2.1 Realita a virtuální realita

Abychom mohli hovořit o virtuální realitě, nejprve si vyjasníme, jak chápeme realitu. Realita je nám známý svět, který vnímáme pomocí smyslů. Všechny smyslové vstupy, spolu se speciálním zpracováním smyslových informací mozkem, nám zajišťuje bohatý tok informací z našeho prostředí do naší mysli. Hovoříme tak o zkušenosti, kterou jsme si osahali, ochutnali, slyšeli, viděli nebo cítili. Taková zkušenost je pro nás základním stavebním kamenem chápání reálného prožitku. Ve chvíli, kdy prezentujeme naše smyslové vnímání v prostředí vygenerovaném počítačem, hovoříme již o prostředí virtuálním neboli virtuální realitě. Virtuální realitu bychom tedy mohli definovat jako trojrozměrné, počítačem generované prostředí, které může být uživatelem prozkoumáno a takovému uživateli je umožněno se v jistém slova smyslu stát jeho součástí. V dnešní době je virtuální realita velmi často implementována za pomoci počítačové technologie, kdy použitím speciálních rukavic nebo např. vícesměrového běžeckého pásu jsou stimulovány uživatelovy smysly a tím dojde k vytvoření iluze reality[7].

Výpočetní technika, interaktivita a internet nabídli zcela jiný druh komunikace, ve které dochází ke ztrátě mimoverbálního vnímání. Dochází k vytváření nesmrtelných virtuálních hrdinů, ke snadným přesunům mezi komunitami a není potřeba přemýšlet nad kompromisy. Vzniká nový kybernetický svět, pro mnohé snesitelnější a příjemnější než svět reálný. Ovšem také kybersvět nabývá všech společenských atributů, jako jsou obchodní, kultovní, náboženské nebo emocionální a politické. Také zde jsou kyberprofesionálové, kyberamatéři, kybermoralisti i kyberzločinci. Kyberprostor se stal pátou dimenzí života společnosti, ve které, aby lidé přežili, je potřeba stará pravidla chování přizpůsobit, nová pravidla vytvořit, nové modifikace nebezpečí pochopit a naučit se je akceptovat nebo najít způsob, jak se s nimi vypořádat[8].

Virtuální realita, kyberprostor, internet, online prostředí, to všechno jsou termíny označující prostor mimo fyzickou realitu a tento prostor nám dává možnost neustálé

[6] BLINKA, L. a kol. 2015. *Online závislosti.* 1. vydání. Praha: Grada Publishing, a.s. 2015. 200 s. ISBN 978-80-247-5311-9.
[7] VRS. 2020. *Co je virtuální realita?* [online]. [citováno 2021-12-17]. Dostupné na internetu: <https://www.vrs.org.uk/virtual-reality/what-is-virtual-reality.html>.
[8] JIROVSKÝ, V. 2007. *Kybernetická kriminalita*. 1. vydání. Praha: Grada Publishing, a.s. 2007. 284 s. ISBN 978-80-247-1561-2.

propojenosti s ostatními. Máme možnost být téměř nepřetržitě nablízku lidem, na kterých nám záleží, ale zároveň se tak téměř nepřetržitě, pokud ztratíme jistou ostražitost, vystavujeme některým rizikům. Jedním z nich je situace, kdy se k nám někteří lidé dostanou blíže, než jsme původně plánovali. Většina dětí a dospívajících vnímá pobyt online jako nezbytný v navazování vztahů, hledání si přátel, komunikaci s lidmi z celého světa. Dává jim pocit sounáležitosti a neomezeného čerpání informací, které se internetem šíří neuvěřitelně rychle a jednoduše. Dovednost obstát v mezilidském kontaktu, třeba jen virtuálním, jim dodává sebejistotu a pocit samostatnosti. Online prostředí umožňuje účastníkům se prezentovat tak, jak chtějí, aby je ostatní viděli. Pro děti a dospívající je pak interakce s realitou často těžká, složitá a nezvládnutelná a únik od reality k virtuální realitě je tak pro některé jediným východiskem[9].

Život v kyberprostoru konstruuje kybersociabilitu, která způsobuje erozi přirozeného sociálna v reálném časoprostoru a rozvoj kybersociálna. Jedná se o stav, kdy dochází k přebírání postojů a názorů „lajkováním“ a sdílením, bez uplatnění jakékoliv analýzy a nutnosti zapojení vlastních myšlenkových pochodů. Vzniká tak prostor, ve kterém si kybernetický predátor svou oběť najde velmi snadno[10].

Dnešní děti jsou ovlivněny virtuálním světem již od batolecího věku. Sledují své rodiče, jak neustále tisknou mobilní telefony k uchu, jak brouzdají po internetu. Mobily a sítě tak děti nepřipravují jen o dětství, strávené s kamarády na hřišti, ale také o rodiče. Virtuální svět, připojení k sociálním sítím, nereálný život prožívaný pomocí vytvořeného avatara se stává normou a pouto dítěte s rodičem ztrácí svou sílu. V takovém okamžiku je dítě nejzranitelnější. Nalezená blízkost, náklonnost, radost, kterou mu najednou nabízí nový, virtuální kamarád, je pro něj tak důležitá, že je ochotno jí obětovat vše, i svou vlastní bezpečnost[11].

2.2 Digitální stopa

Internet není v žádném případě anonymním prostředím. Digitální stopou nazýváme soubor informací, který obsahuje různorodé záznamy o činnostech uživatele v online prostředí. Součástí takového souboru jsou záznamy z počítače, chytrých hodinek,

[9] ČERNÁ, A. a kol. 2013. *Kyberšikana, průvodce novým fenoménem*. 1. vydání. Praha: Grada Publishing, a.s. 2013. 152 s. ISBN 978-80-247-4577-0.
[10] SAK, P. 2018. *Úvod do teorie bezpečnosti: nekonvenční pohledy na minulost, přítomnost a budoucnost lidstva*. 1. vydání: Petrklíč. 2018. 271 s. ISBN 978-80-7229-652-1.
[11] DOČEKAL, D. a kol. 2019. *Dítě v síti.* 1. vydání: Mladá fronta. 2019. 208 s. ISBN 978-80-204-5145-3.

chytré televize, mobilního telefonu, dále pak příspěvky na sociálních sítích, blogy, nákupy na internetu. Digitální stopa vypovídá o vlastním digitálním „já“ a každá z těchto informací je velmi snadno zneužitelná. Kybernetičtí predátoři tak dokáží ukrást osobní údaje, hesla, e-mailové účty. Při krádeži profilu na sociální síti mohou spáchat protiprávní jednání, kterým je podvod, vydírání, phishingový útok a jiné. Neopatrní uživatelé virtuálního světa mohou být velmi snadno, díky digitální stopě, vystaveni kyberšikaně[12].

Každý uživatel online prostředí má svou digitální stopu a s tím spojenou digitální pověst. Potřeba sdílet radostné zážitky na sociálních sítích může mít ovšem dlouhodobý negativní dopad na naši trvalou digitální stopu. Ne vždy si uvědomujeme, že to, co na internetu zveřejníme, zůstane naší součástí bez možnosti změny a takovým způsobem se představíme novým přátelům, spolužákům ve škole, kolegům v zaměstnání. Naprosto ochotně tak nabízíme digitální nekonečnost bez jakéhokoliv sledovacího nástroje[13].

Digitální stopu můžeme rozdělit do tří základních kategorií. První kategorií jsou stopy, které uživatel vytváří sám, vlastní činností. Zde se jedná o stopu vědomou, která je zanechána interakcí na sociálních sítích, příspěvky v diskuzních fórech, mailovou komunikací nebo využíváním internetových úložišť fotografií. Zároveň však vzniká stopa nevědomá, kterou jsou soubory cookies, údaje o poskytovateli připojení, IP adresa, nebo lokační údaje. Druhou kategorií jsou digitální stopy zanechané přáteli, které vznikají např. označením přítele v příspěvku nebo na fotografii. Třetí kategorií jsou digitální stopy zanechané nepřáteli, kdy o každém uživateli je možné v online prostředí zanechat nepravdy, které údaje zkreslují s cílem uživatele poškodit či jinak kompromitovat. Je důležité vědět, že jakékoliv informace, které se do internetového prostředí vloží, již prakticky není možné odstranit[14].

Ovšem je důležité vědět, že není třeba digitální stopu vnímat pouze negativně. Pokud uživatel chápe celý proces jejího vzniku, lze si takovou stopu cíleně pěstovat a umožnit tak informačně-knihovnické komunitě náhled do soukromí v rozsahu, který si uživatel sám zvolí. Jedná se o informace, které pak lze následně nabídnout možnému budoucímu zaměstnavateli s tím, že si může udělat představu o uživatelových

[12] Internetem bezpečně. 2020. [online]. *Digitální stopa*. [citováno 2020-10-22]. Dostupné na internetu: <https://www.internetembezpecne.cz/internetem-bezpecne/dobre-vedet/digitalni-stopa/>.
[13] FIELDINGOVÁ, O. 2018. *Digitální detox*. 1. vydání. Praha: Albatros Media a.s. 2018. 120 s. ISBN 978-80-264-1980-8.
[14] KOHOUT, R. 2017. *Internetem bezpečně: Jak se nestát obětí virtuálního predátora.* Karlovy Vary: You conneected. 2017. 68 s. ISBN 978-80-270-2897-9.

schopnostech v oblasti grafiky, mentorování, řečnictví, případně v oblasti managementu či názorového zaměření[15].

2.3 Sociální sítě

Sociální síť je internetová služba, umožňující svým registrovaným členům vytvářet uzavřené, veřejné, nebo firemní profily, diskuzní fóra a prezentace, sdílet videa a fotografie. Uživatelé pak svými příspěvky, chaty a veřejnou komunikací vytváří většinu obsahu sociálních sítí. Rozmach sociálních sítí v České republice nastal zároveň s příchodem neomezeného internetu. Mezi uživateli jsou zastoupeny všechny věkové kategorie[16].

Sociální sítě je možné rozdělit do dvou základních skupin, a to na všeobecné a oborové. Všeobecné sítě jsou určeny běžnému uživateli, registrace není podmíněna žádnými kritérii, jsou tedy dostupné bez rozdílu všem. Příkladem takové všeobecné sociální sítě je Facebook. Druhou skupinou jsou sociální sítě oborové, ve kterých se sdružují uživatelé se stejnými zájmy, případně zabývající se stejným oborem v zaměstnání či studiu. Zde bychom mohli hovořit o sociálních sítích profesionálních, hobby sociálních sítích a sociálních sítích studentských[17].

Internet je zdrojem možností vstřebat a tvořit cokoliv a kdykoliv. Díky síle sociálních sítí si může každý užít svých pět minut slávy zveřejněním jednoho videa na YouTube, zveřejněním poutavého článku na blogu, na statusu na Facebooku. Zveřejnit jakoukoliv informaci není složité a běžný uživatel to zvládne bez větších potíží. Ten, komu zmiňovaných pět minut slávy nestačí, si pak pravidelnými příspěvky vytváří určitou komunitu fanoušků, skupinu sledujících. Ovšem být úspěšný na sítích není vůbec jednoduché. Je třeba nad sítěmi přemýšlet. Většina uživatelů neví, jakou skupinu lidí svými příspěvky osloví a neuvědomuje si, jaké důsledky takový zveřejněný příspěvek může mít. Každý uživatel sociálních sítí má možnost se vyjádřit bez jakéhokoliv omezení,

[15] HLEDÁNÍ FLOW. 2008. *Hledání flow.* 1. vydání. Brno: Tribun EU. 2008. 152 s. ISBN 978-80-7399-623-9.
[16] KOŽÍŠEK, M. – PÍSECKÝ, V. 2016. *Bezpečně na internetu, průvodce chováním ve světě online.* 1. vydání. Praha: Grada Publishing, a.s. 2016. 176 s. ISBN 978-80-247-5595-3.
[17] BLÁHA, J. a kol. 2016. *Řízení lidských zdrojů, nové trendy*. 1. vydání. Praha: Albatros Media a.s. 2016. 240 s. ISBN 978-80-726-1434-9.

má ve svých rukách sílu na sebe strhnout pozornost celého světa. Nemusí být úspěšný, ale všechny potřebné nástroje k tomu má[18].

Sociální sítě rozlišujeme české a zahraniční. Počet uživatelů českých sociálních sítí se stále snižuje. Důvodem je jednoznačně rostoucí popularita sociálních sítí mezinárodních, kde díky lokalizaci služeb došlo k odbourání jazykové bariéry a byly vytvořeny intuitivní mobilní verze, kde se využívají nové trendy a technologie. Ale zde by si měl každý uživatel uvědomit, že to, že je sociální síť lokalizována do českého jazyka neznamená, že se jedná o českou službu, která podléhá českým zákonům. Všechny podmínky se řídí právem státu, ve kterém je síť zaregistrována. Domoci se tak, v případě potřeby, spravedlnosti, bývá mnohdy složité a časově náročné. Na sociálních sítích má uživatel možnost zveřejnit celou řadu informací o sobě. Ovšem zde je potřeba se zamyslet, která z těchto informací by mohla být zneužita. Z tohoto důvodu je doporučováno jedno důležité pravidlo – na sociálních sítích zveřejňovat jen ty informace, které by byl uživatel ochoten vyvěsit na autobusové zastávce, nebo školní nástěnce[19].

[18] LOSEKOOT, M. a kol. 2019. *Jak na sítě: Ovládněte čtyři principy úspěchu na sociálních sítích*. 1. vydání. Brno: Jan Melvil Publishing. 2019. 328 s. ISBN 978-80-7555-085-9.
[19] KOŽÍŠEK, M. – PÍSECKÝ, V. 2016. *Bezpečně na internetu, průvodce chováním ve světě online.* 1. vydání. Praha: Grada Publishing, a.s. 2016. 176 s. ISBN 978-80-247-5595-3.

3 RIZIKA NA INTERNETU

Internet je již celou řadu let nedílnou součástí našeho života. Je to prostředek komunikace, práce, zábavy. Bez ohledu na věk uživatele je důležité dodržovat zásady bezpečného chování na internetu a sociálních sítích, neboť k interakci dochází velmi často s lidmi neznámými. Značné nebezpečí se skrývá za používáním sociálních sítí, kdy nejohroženější skupinou jsou dle statistických údajů děti, především pak dívky ve věku 12 až 15 let[20].

Dnes, kdy jsou jednotlivá zařízení připojena k internetu téměř nepřetržitě, stává se pro většinu uživatelů téměř nehmatná hranice mezi soukromým a veřejným prostorem. Uživatelé, nacházející se v prostoru veřejném, mají tendenci chovat se, jako by byli v soukromí, což může vést ke zneužití zveřejněných informací, což může vést k nepříjemnostem v mnoha ohledech[21].

Online rizika je důležité chápat v kontextu určitých charakteristických rysů, kterými jsou zcela jistě druhy činností prováděných uživateli online prostředí a druhou významnou veličinou je počet internetových aktivit. Čím vyšší je míra aktivit, tím vyšší je míra rizika. Druhým hodnotícím kritériem rizikovosti je věk uživatele. Čím starší uživatel je, tím rozmanitější je způsob využívání internetu. To přináší značnou nepřehlednost a ztíženou orientaci v hodnocení, co je bezpečné a co již uživatele vystavuje riziku. Velmi náročné je z tohoto hlediska období adolescence, které je typické budováním vlastní autonomie a oproštěním se od rodičovské autority a rodičovské kontroly. Třetím kritériem, vycházejícím ze zkušenosti, je zjištění, že čím výraznější je újma, tím méně často je možné se s daným rizikem setkat[22].

Rodiče jsou ti, kteří by měli své děti jako první poučit o zásadách bezpečného chování na internetu. Zcela jistě by děti neměly komunikovat s cizí osobou, která je na sociálních sítích vyhledala a oslovila. Dítě by nemělo neznámé osobě sdělovat důvěrné informace o sobě a své rodině, jako je adresa bydliště, školy, telefonní číslo, případně hesla, používaná na internetu. Velmi nebezpečné je pak posílání fotografií a jejich

[20] Policie České republiky. *Kyberkriminalita.* [online]. [citováno 2020-11-17]. Dostupné na internetu: < https://www.policie.cz/clanek/kyberkriminalita.aspx>.
[21] RECMANOVÁ, A. 2017. [online]. *Pravidla netikety*. [citováno 2021-10-10]. Dostupné na internetu: <https://medium.com/edtech-kisk/pravidla-netikety-ea92f7c3e58b>.
[22] ŠEVČÍKOVÁ, A. a kol. 2014. *Děti a dospívající online, vybraná rizika používání internetu*. 1. vydání. Praha: Grada Publishing, a.s. 2014. 184 s. ISBN 978-80-247-5010-1.

ukládání na sociálních sítích. Každé dítě by mělo vědět, že pokud mu někdo bude posílat obtěžující a neslušné zprávy, je třeba toto sdělit svým rodičům, učiteli ve škole nebo jinému dospělému člověku. Důvěra dítěte ve známou dospělou autoritu zde hraje zásadní roli. V neposlední řadě by děti měly používat webovou kameru pouze ke komunikaci se svými kamarády, nikdy při komunikaci s cizím člověkem. A pokud by bylo dítě vyzváno osobou, se kterou se seznámilo na chatu nebo na sociálních sítích, k osobnímu setkání, mělo by toto odmítnout a opět se svěřit svému rodiči[23].

Rizik, která v kyberprostoru číhají, je celá řada. Je potřeba je umět identifikovat, abychom jim uměli čelit. Nejčastěji řešená je kyberšikana, kybergrooming, stalking, kyberstalking, spam a hoax, phishing a sociální inženýrství, sexting, webcam trolling. Jsou to rizika, kterým jsou nejčastěji vystaveny děti, protože právě ony tráví výraznou část svého času virtuální komunikací, navazováním sociálních vztahů pod rouškou anonymity a zveřejňováním citlivých dat a fotografií[24].

3.1 Vývoj kriminality na internetu

Pokud se hovoří o kriminalitě na internetu, zcela jistě se setkáme s pojmem kybernetická kriminalita. Tento pojem je odvozen od pojmu kyberprostor. Problematice kybernetické kriminality se věnuje stále větší pozornost, neboť dynamický rozvoj informačních technologií s sebou přináší zcela nová společensky škodlivá jednání. Nebezpečnost spočívá ve virtuálním prostředí, které nezná hranice, nemá omezení a jen velmi těžko se zde uplatňuje kontrola. Dle Jirovského „*je nutno si uvědomit, že veškeré dosud známé nelegální aktivity probíhaly ve fyzickém prostoru, kde každý z aktérů byl lehce popsatelný a postižitelný. Tak tomu není v kyberprostoru, kde se setkáváme pouze s projekcemi pachatelů, s jejich virtuálním obrazem, který může být od skutečných rysů pachatele na hony vzdálen.*“[25] Policie České republiky sleduje počet trestných činů v kyberprostoru již od roku 2011 a je zcela zjevná stále rostoucí prevalence. V roce 2011

[23] Policie české republiky. [online]. [citováno 2021-11-30]. Dostupné na internetu: <https://www.policie.cz/clanek/uzemni-odbor-praha-venkov-zapad-zpravodajstvi-nebezpeci-na-internetu.aspx>.
[24] KOŽÍŠEK, M. – PÍSECKÝ, V. 2016. *Bezpečně na internetu, průvodce chováním ve světě online.* 1. vydání. Praha: Grada Publishing, a.s. 2016. 176 s. ISBN 978-80-247-5595-3.
[25] JIROVSKÝ, V. 2007. Kybernetická kriminalita. 1. vydání. Praha: Grada Publishing, a.s. 2007. Přímá citace s 16. ISBN 978-80-247-1561-2.

zaznamenala Policie České republiky 1502 případů trestných činů kybernetické kriminality, v roce 2019 se již jednalo o 8417 případů[26].

Hovořit o kyberkriminalitě je stejně důležité, jako hovořit o bezpečnosti online prostředí. Bezpečnost virtuálního světa má dvě dimenze. První dimenzí je bezpečnost sociální, která je zároveň dimenzí klíčovou. Dojde-li k jejímu ohrožení, je narušeno sociální vnímání a narušena je vlastní lidská civilizace a civilizovanost. Druhou dimenzí je informační kyberbezpečnost. Jedná se o informační a komunikační technologie, které kyberprostorem přenáší informace a jsou tak nositeli procesů, které v lidské společnosti vytváří budoucnost, fantastické možnosti, ale i netušené hrozby[27].

Počítačové systémy, fenomén jejich bezpečnosti, informatizace společnosti, to jsou témata, která si získávají stále větší popularitu. Existují desítky firem, které za přesně stanovenou částku zabezpečí počítačovou a komunikační infrastrukturu před napadením. Zároveň najde i běžný uživatel na internetu stovky návodů, jak tato bezpečnostní opatření obejít. Bezpečnostní opatření se tak stala obchodním produktem, který kalkuluje se strachem z rizika a nutí firmy i běžného uživatele online prostředí k řešení v rámci kterého je potřeba vynakládat nemalé prostředky[28].

Nejčastější kybernetickou trestnou činností jsou různé druhy podvodného jednání, jako např. porušování autorských práv, sociální inženýrství nebo falešné e-shopy. Dále se velmi často setkáváme s napadením škodlivým softwarem – malwarem, mezi které řadíme různé druhy virů, červů nebo botnet. Běžný uživatel může čelit útokům na sociálních sítích v podobě kybergroomingu, kyberšikany nebo krádeže identity. Čtvrtým typem nejrozšířenější kybernetické trestné činnosti je pak sofistikovaný kybernetický útok v podobě hackingu, crackingu nebo pharmingu[29].

Studium kybernetické kriminality, nazývané kybernalita, se snaží o projekci pohledu na jedince i společnost do kyberprostoru. Nedílnou součástí kybernality jsou také společenské vědy, jako je psychologie, právní věda nebo sociologie, které poukazují na významné změny chování jedince ve společnosti. Současné chápání kybernetického

[26] Policie české republiky. [online]. [citováno 2022-02-15]. Dostupné na internetu: <https://www.policie.cz/clanek/kyberkriminalita.aspx>.
[27] SAK, P. 2018. *Úvod do teorie bezpečnosti: nekonvenční pohledy na minulost, přítomnost a budoucnost lidstva*. 1. vydání: Petrklíč. 2018. 271 s. ISBN 978-80-7229-652-1.
[28] JIROVSKÝ, V. 2007. *Kybernetická kriminalita*. 1. vydání. Praha: Grada Publishing, a.s. 2007. 284 s. ISBN 978-80-247-1561-2.
[29] KOHOUT, R. – ŠTOCHL, J. 2018. *Kybernetická kriminalita, příručka pro policisty*. První vydání. Karlovy Vary: You connected. 2018. 146 s.

trestného činu, kde jen velmi obtížně hledáme klasické atributy, se zatím opatrně formuje a stávající standardizované metody policejního vyšetřování tak často naráží na rychlost, s jakou jsou kybernetické trestné činy provedeny, na rychlost zahlazování stop a z takového vyšetřování se pak stává komplikované honění duchů. Je důležité si uvědomit, že v kyberprostoru se setkáváme pouze s projekcí pachatele, s obrazem, který se skutečnými rysy pachatele nemusí mít zcela nic společného. Kybernalitou rozumíme takovou činnost, kterou je porušován zákon, případně není v souladu s morálními pravidly společnosti[30].

Kyberkriminalita je trestná činnost, páchána za pomoci informačních technologií. Právě v případě kybernality se zcela jasně potvrzuje téze, že entita je sama sobě největší hrozbou. Sám jedinec je sám sobě zdrojem rizika, a to ve velmi širokém spektru. Zveřejňováním soukromých citlivých dat na internetu zvyšuje jedinec riziko kyberútoku na vlastní osobu. Oběť, kterou si predátor v kyberprostoru vyhlédne, většinou dlouhou dobu ani netuší, že se stala obětí a materiály, kterými je později vydíratelná a tlačena k extrémním řešením, tak většinou agresorovi vydá sama a dobrovolně[31].

Současné platné právní normy neumí nový typ zločinů v kyberprostoru taxativně vyjmenovat, je tedy legislativní vágnost velmi často součástí probíhajících soudních řízení. Řešením je tedy přípustnost určité analogie, kdy je možné použít právní normy, které postihují delikty podobné charakteristiky. Ovšem některé analogie, s ohledem na nutnou přesnost vyjádření v zákoně, nelze použít[32].

3.2 Kyberšikana

Kyberšikanou rozumíme určitý typ šikany, který přímo souvisí s informačními a komunikačními technologiemi, které jsou využívány k ublížení druhé osobě. Může se jednat o obtěžování, vydírání, zastrašování, zesměšňování, ohrožování. Aktérem kyberšikany je vždy agresor, oběť a velmi často také publikum. Dopad kyberšikany na dítě je mnohem závažnější než u šikany klasické, a to z několika důvodů. Oběť sama většinou ani neví kdo a z jakého důvodu jí ubližuje. Velmi často se do šikany v kyberprostoru zapojí hned několik agresorů. Anonymita dodává agresorovi značné

[30] JIROVSKÝ, V. 2007. *Kybernetická kriminalita*. 1. vydání. Praha: Grada Publishing, a.s. 2007. 284 s. ISBN 978-80-247-1561-2.
[31] SAK, P. 2018. *Úvod do teorie bezpečnosti: nekonvenční pohledy na minulost, přítomnost a budoucnost lidstva*. 1. vydání: Petrklíč. 2018. 271 s. ISBN 978-80-7229-652-1.
[32] JIROVSKÝ, V. 2007. *Kybernetická kriminalita*. 1. vydání. Praha: Grada Publishing, a.s. 2007. 284 s. ISBN 978-80-247-1561-2.

sebevědomí. Oběť je vystavena stálému stresu, neboť ponižující příspěvek je na internetu vystaven stále a ponížení oběti tak může sledovat velké množství uživatelů internetu. Oběť má pak pocit bezmoci a bezvýchodnosti[33].

Kyberšikaně začala být věnována intenzivní pozornost jen nedávno. Výzkumníci, kteří se problematice kyberšikany věnují, neustále bojují s rychlostí, jakou se vyvíjí informační a komunikační technologie. S rychlým rozvojem technologií tak rostou možnosti kyberšikany. Jedním ze smyslů průzkumných šetření je zjistit, jaká je prevalence případů kyberšikany. Jsou to data, která jsou různými zdroji rozdílně interpretována. Svět mladé online generace je dospělým velmi často neprůhledný a nepochopitelný. To je jeden z důvodů, proč jednotlivé zdroje mají nejednotné pojetí a vymezení, co to kyberšikana vlastně je[34].

Velmi často se můžeme setkat s tím, že jednotlivé zdroje nerozlišují kyberšikanu od online obtěžování, případně vrstevnického škádlení a tím dochází k nadhodnocení četnosti a obvyklosti kyberšikany. Takto alarmující zprávy pak mohou způsobit morální paniku a vyvolat zavedení opatření, která nejsou adekvátní skutečnému stavu. Takto zavedená preventivní a intervenční opatření pak bývají neefektivní a neúčinná. Je tedy účelné se v rozdílech mezi kyberšikanou a online obtěžováním dobře orientovat. Na rozdíl od kyberšikany je pro online obtěžování typický jednorázový atak v podobě urážek, který se dále neopakuje. Druhým definujícím znakem je agresivita nezáměrná, není cílena na poškození konkrétní osoby. Třetím příkladem online obtěžování je případ, kdy osoba, která je cílem útoku, nevnímá takové jednání jako poškozující[35].

Rozpoznat kyberšikanu není vůbec jednoduché a velmi často si závažnost jednání i samotní aktéři neuvědomují ihned. Kyberšikana má určité znaky:

- Útočník se velmi často chybně domnívá, že je anonymní.
- Publikum napomáhá útočníkovi v šíření kyberšikany.
- V internetovém prostředí nerozhoduje fyzická síla, slabší může šikanovat silnějšího.
- Není možné odhadnout čas a místo útoku.
- Není jednoduché rozpoznat dopad kyberšikany na oběť.

[33] Internetem bezpečně. 2021 [online]. *Kyberšikana.* [citováno 2020-12-12]. Dostupné na internetu: <https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/>.
[34] ČERNÁ, A. a kol. 2013. *Kyberšikana, průvodce novým fenoménem*. 1. vydání. Praha: Grada Publishing, a.s. 2013. 152 s. ISBN 978-80-247-4577-0.
[35] ŠEVČÍKOVÁ, A. a kol. 2014. *Děti a dospívající online, vybraná rizika používání internetu*. 1. vydání. Praha: Grada Publishing, a.s. 2014. 184 s. ISBN 978-80-247-5010-1.

- Kyberšikana může začít jako nepovedený vtip.
- Kyberšikana je velmi často spojena s šikanou tradiční.

Každé dítě, každý dospívající, každý uživatel internetu, který se s kyberšikanou setká, by měl vědět, že takovou zkušenost je třeba oznámit. Dětská oběť by měla mít možnost se svěřit rodiči, pedagogovi, případně jinému dospělému, ke kterému má důvěru. Může se také obrátit na bezplatnou telefonní Linku bezpečí 116111, nebo na policii, na linku 158[36].

V souvislosti s kyberšikanou, což je jakékoliv jednání s cílem ublížit, poškodit, ohrozit nebo zastrašit oběť pomocí informačních technologií, vyvstává otázka, je-li dostupný způsob, jak agresora potrestat. Zcela jistě bychom obrátili pozornost k trestnímu zákoníku, kde bychom ovšem kyberšikanu jako skutek definovánu nenašli. Tento fakt neznamená, že nebude potrestána. Celý skutek kyberšikany je nutné rozčlenit na jednotlivé projevy, kterými jsou např. vydírání nebo vyhrožování, což v trestním zákoníku je definovaným skutkem a tyto skutky jsou pak předmětem trestního stíhání[37].

3.3 Sexting

Možnou definicí sextingu by bylo dobrovolné sdílení intimních fotografií a videí s jinými uživateli v kybernetickém prostoru. Jedná se o fenomén, který je celosvětově na vzestupu. Sexting je velmi úzce provázaný s kybergroomingem, kdy zveřejněné intimní informace mohou být nástrojem vydírání a predátor tak svoji oběť může donutit k osobnímu setkání, se všemi důsledky, které z takového činu vyplynou[38].

Sexting sice není zákonem definovaná trestná forma jednání, ale judikáty soudů jej hodnotí jako určitou formu autopornografického díla, které dokáží děti velmi snadno vytvořit a sdílet. Právní rámec vychází z toho, že osoby starší patnácti let sex mít mohou, ale nesmí se při sexuálním styku natáčet nebo fotografovat. Pokud k takovému jednání

[36] KOHOUT, R. 2017. *Internetem bezpečně: Jak se nestát obětí virtuálního predátora.* Karlovy Vary: You conneected. 2017. 68 s. ISBN 978-80-270-2897-9.
[37] KOŽÍŠEK, M. – PÍSECKÝ, V. 2016. *Bezpečně na internetu, průvodce chováním ve světě online.* 1. vydání. Praha: Grada Publishing, a.s. 2016. 176 s. ISBN 978-80-247-5595-3.
[38] O2 chytrá škola. 2021. [online]. [citováno 2021-11-22]. Dostupné na internetu: <https://www.o2chytraskola.cz/data/files/sexting-dfjl8pi7x6.pdf>.

dojde, je takový čin chápán, dle Zákona č. 40/2009 Sb., trestní zákoník (dále jen trestní zákoník) § 192, jako výroba a nakládání s dětskou pornografií[39].

Je velmi žádoucí, zaměřit se na preventivní chování, a protože sexting řadíme mezi závažné rizikové aktivity, je nezbytné pracovat s tímto tématem také v prostředí základních škol. Výukové aktivity se zaměřují především na zodpovědný přístup žáků k internetu a snaží se o vybudování zdravého postoje k práci s osobními údaji. Každé dítě, které se v online prostředí pohybuje, by mělo být seznámeno s riziky zneužití zveřejněných osobních informací na internetu[40].

K sextingu dochází při výměně lechtivých zpráv mezi partnery, nebo pak mezi neznámými lidmi, kteří takovýto typ komunikace vyhledávají. Na nabídku sextingu může uživatel internetu narazit na celé řadě serverů. Nejčastěji jsou tyto materiály měněny pomocí e-mailů, případně přes komunikační kanály typu Skype, messenger nebo pomocí aplikace typu Snapchat. Aplikace Snapchat dává účastníkům takové komunikace falešný pocit bezpečí a anonymity, neboť odeslaný obsah se příjemci zobrazí pouze po dobu, kterou určí sám odesílatel. Ovšem každý ze zúčastněných by si měl uvědomit, že tato nastavená dočasnost může být celou řadou programů ohrožena vytvořením screenshotu obrazovky. Takto získané fotografie se mohou stát předmětem vydírání, kdy si je dospělý predátor velmi dobře vědom, jak citlivé je takové téma pro dětský věk a období adolescence. Nejčastější výhrůžkou je zveřejnění zaslaných materiálů, případně jejich zaslání přátelům a rodičům. Sexting je vysoce rizikovou činností, obzvlášť jedná-li se o komunikaci mezi cizími lidmi, případně za účasti dětí[41].

3.4 Kyberstalking

Kyberstalking je nebezpečné pronásledování, kdy útočník využívá ke stupňovanému kontaktování a obtěžování informační a komunikační technologie. Cílem útočníka je vyvolat v oběti strach o své zdraví, život, o vlastní soukromí. Nejběžnější formou kyberstalkingu je zasílání sms, opakované prozvánění, komentování příspěvků oběti na sociálních sítích, krádež identity a následné zneužití profilu ke kompromitaci

[39] E–bezpečí. 2021. [online]. *Sexting a právo*. [citováno 2021-11-28]. Dostupné na internetu: <https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/sexting/1681-sexting-a-pravo>.
[40] O2 chytrá škola. 2021. [online]. [citováno 2021-11-22]. Dostupné na internetu: <https://www.o2chytraskola.cz/data/files/sexting-dfjl8pi7x6.pdf>.
[41] KOŽÍŠEK, M. – PÍSECKÝ, V. 2016. *Bezpečně na internetu, průvodce chováním ve světě online.* 1. vydání. Praha: Grada Publishing, a.s. 2016. 176 s. ISBN 978-80-247-5595-3.

oběti, vkládání příspěvků do profilu oběti. Motivací kyberstalkera je demonstrace vlastní síly, poškození oběti před společností, vyhrožování, obtěžování a vydírání oběti, nebo pokus o znovunavázání vztahu po odmítnutí[42].

Pokud se uživatel internetu setká s nevhodným chováním, je potřeba takovou skutečnost řešit. Není nutné se okamžitě obrátit na policii, je možné podat oznámení administrátorovi služeb, který taková oznámení shromažďuje a po následném vyhodnocení oznamuje polici. Oznámení, založená na důkazech pak vedou k blokování, případně stíhání útočníka. Proti stalkerům je možné se do určité míry bránit. Oběť by v první řadě měla stalkera vyzvat, aby svých intervencí zanechal, že jeho zájem je nežádoucí. Oběť by měla změnit své zvyky, měla by se svěřit svým přátelům, rodině. V žádném případě by neměla na ataky, zprávy, prozvánění reagovat a při pocitu ohrožení by měla neprodleně kontaktovat policii[43].

Kyberstalking je možné, za konkrétních podmínek, kvalifikovat dle trestního zákoníku, § 354, jako trestný čin Nebezpečné pronásledování. Je-li takový čin páchán na dítěti, hovoříme, dle § 354, odst. 2, písmeno a) trestního zákoníku, o okolnostech přitěžujících[44].

[42] Internetem bezpečně. 2021. [online]. *Kyberstalking*. [citováno 2021-11-01]. Dostupné na internetu: <https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kyberstalking/>.

[43] KOŽÍŠEK, M. – PÍSECKÝ, V. 2016. *Bezpečně na internetu, průvodce chováním ve světě online.* 1. vydání. Praha: Grada Publishing, a.s. 2016. 176 s. ISBN 978-80-247-5595-3.

[44] Internetem bezpečně. 2021. [online]. *Kyberstalking*. [citováno 2021-11-01]. Dostupné na internetu: <https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kyberstalking/>.

4 HROZBA ZVANÁ KYBERGROOMING

Pokud bychom kybergrooming chtěli definovat, budeme hovořit o manipulativním chování predátora k oběti, kdy je oběť pomocí informačních komunikačních technologií vylákána pomocí falešné identity ke schůzce, za účelem zneužití. Útočník si svou oběť zpravidla vytipuje na základě údajů, uvedených na internetu[45].

Kybergrooming je založen na tom, že si predátor vytvoří několik identit, které využívá k přesvědčení oběti, že je jeho identita pravá. Takto vytvoření fiktivní přátelé pak mohou bez problému potvrdit oběti, že nový kamarád na internetu je skutečný. Při hledání nových přátel v online prostředí existuje několik varovných indicií, které se mohou objevit u fiktivních identit. Velmi často je profil založen jen krátce, přátelé jsou stejného pohlaví a věku, v popiscích jsou velmi často dvojsmysly se sexuálním podtextem, zveřejněné fotografie jsou dokonalé, vyumělkované a z jedné série, jméno kontaktu je zvláštní a kontakt se vždy vyhne audiovizuálnímu kontaktu pod různými záminkami[46].

Kybergrooming je termín, se kterým se setkáváme stále častěji v souvislosti s hraním online her. Velmi nebezpečným se jeví pocit rodičů, že prostředí virtuálních her nepředstavuje riziko přítomnosti dospělých predátorů, kteří by byli schopni se do komunity dětských hráčů začlenit. Byly zveřejněny případy, kdy právě v takovém prostředí došlo k rizikové komunikaci a pomocí virtuálních dárků došlo k prohloubení vztahu mezi predátorem a obětí. Útočník pak následně dosáhl osobního setkání, při kterém došlo k sexuálnímu zneužití a je znám i případ, který skončil vraždou oběti. Účinnou obranou proti takovým dopadům online komunikace je především prevence. Každé dítě by mělo být rodiči nebo pedagogem seznámeno se zásadami správné online komunikace a jejími riziky[47].

Nejčastějšími obětmi kybergroomingu jsou děti ve věku 11 – 17 let. Skupiny dívek a chlapců jsou většinou rovnoměrně zastoupené. Jen ze 3 % byly predátorem osloveny děti, které na svém online profilu nezveřejnily svoji fotografii, naopak většina

[45] KOŽÍŠEK, M. – PÍSECKÝ, V. 2016. *Bezpečně na internetu, průvodce chováním ve světě online.* 1. vydání. Praha: Grada Publishing, a.s. 2016. 176 s. ISBN 978-80-247-5595-3.
[46] tamtéž
[47] KOPECKÝ, K. 2017. [online]. E-bezpečí. [citováno 2021-12-22]. Dostupné na internetu: <https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/kybergrooming/1222-minecraft-kybergrooming>.

oslovených chlapců ve svém profilu zveřejňovala fotografie v plavkách, částečně odhaleni do půl těla. U dívek se obětí staly většinou blondýnky ve věku 13 a 14 let. Obětmi se stávají děti s nízkou sebedůvěrou, s emocionálními problémy a pocitem osamělosti, děti dospívající, které jsou ochotny si o své sexualitě povídat. Kybergroomeři mají rádi svou anonymitu a hlídají si své teritorium. Bylo zjištěno, že ze vzorku nahlášených podvodných identit asi 16 % nahlásili sami podvodníci. Každý dospělý by měl vědět, jak děti jemu svěřené, před kybergroomingem chránit. Počítač by měl být umístěn na místě, kde je možné činnost dítěte kontrolovat. Každé dítě by mělo být o rizicích na internetu poučeno. Je vhodné, aby mělo dítě ve svém mobilním telefonu nastavený paušál, je zde snazší kontrola činností. Internet by dítě doma mělo mít dostupný, pokud bude internet hledat u kamarádů, jen těžko bude rodič dohlížet na jeho zájmy. Je velmi důležité, aby rodiče u svého dítěte byli schopni zaregistrovat změnu v chování, nenadálou uzavřenost nebo podrážděnost. Může to být známka toho, že se mu stalo něco, s čím si neví rady. A to něco může být útok kybernetického predátora[48].

Groomeři, díky anonymitě a dostupnosti digitální technologie, přistupují k více dětem najednou. Pravděpodobnost, že se jim podaří oběť získat, se tak jednoznačně zvyšuje. Samotný kybergrooming může proběhnout velmi rychle, ale dopad na oběť, na její psychiku může být dlouhodobá. Dítě si velmi často celý incident dává za vinu, má pocit, že si to zaslouží a jen velmi těžko získává zpět své sebevědomí. Kybernetický grooming je považován za bránu k mnohem závažnějším trestným činům sexuálního vykořisťování dětí. Klíčová je zde mezinárodní legislativa, která kriminalizuje všechny typy groomingu.[49]

4.1 Fáze kybergroomingu

Na kybergrooming je možné nahlížet jako na proces, který probíhá v několika stádiích. V první fázi se predátor snaží o získání důvěry a pokouší se oběť izolovat od rodičů a kamarádů. Zároveň od již zmanipulovaného dítěte získává fotografie a citlivé informace, které využívá k vydírání. Ve druhé fázi dochází k podplácení dárky, kterými jsou peníze, počítačové hry, hračky nebo oblečení. Třetí fází vzniká emoční závislost

[48] KOŽÍŠEK, M. – PÍSECKÝ, V. 2016. *Bezpečně na internetu, průvodce chováním ve světě online.* 1. vydání. Praha: Grada Publishing, a.s. 2016. 176 s. ISBN 978-80-247-5595-3.
[49] ChildSafeNet. 2022. [online]. Cyber Grooming. [citováno 2022-02-12]. Dostupné na internetu: <https://www.childsafenet.org/new-page-15>.

oběti na útočníkovi. Zde predátor zneužívá sílu sdíleného tajemství, exkluzivního kamarádství. Dále následuje poslední fáze a tou je osobní setkání se všemi důsledky[50].

V první fázi používá útočník typicky metodu mirroringu, tedy zrcadlení. Ve chvíli seznamování s obětí využívá predátor již předem zjištěné informace a je tak schopen dítěti nabídnout pochopení, podporu a sounáležitost, sdílí s ním společné názory a myšlenky a ukazuje mu, že se potýká se stejnými problémy. Důvěru nezkušeného a naivního dítěte tak predátor získá velmi rychle a dítě se k takovému pocitu přátelství snadno upne[51].

Druhá fáze je o budování kamarádského vztahu. Luring, neboli vábení je založeno na uplácení oběti dárky. Predátor nabízí dítěti peníze, lístky na koncert, do kina a podobně a na oplátku požaduje intimní fotografie, citlivé informace. V tuto chvíli dítě není schopno vyhodnotit, jak závažnou se situace stává. Má pocit, že získalo kamaráda, který mu dává pocit bezpečí a důvěry[52].

Ve třetí fázi se oběť stává emočně závislou na predátorovi. Velmi rychle se emočně závislými stávají děti ze sociálně slabšího prostředí, kdy dítě získává falešný, ale silný pocit, že pouze kontakt s agresorem ho naplňuje pocitem síly a spokojenosti. Materiální závislost může vést až k prostituci[53].

Čtvrtá fáze je ve znamení osobního setkání. Na tuto fázi se predátor připravuje v průměru 3 měsíce, ovšem může uběhnout i více než jeden rok, než k setkání skutečně dojde. Velmi často je místem setkání kybergroomerův byt, případně jiné místo, odkud nemá oběť šanci uniknout nebo se dovolat pomoci[54].

K osobnímu setkání nedojde vždy, ale pokud k němu dojde, je to známka toho, že je vytvořený vztah ze strany oběti brán vážně[55].

---

[50]BĚLÍK, V. a kol. 2017. Slovník sociální patologie. 1. vydání. Praha: Grada Publishing, a.s. 2017. 120 s. ISBN 978-80-271-0599-1.

[51] MÁČELOVÁ, K. 2021. [online]. Učení v pohodě. [citováno 2021-12-12]. Dostupné na internetu: <https://www.uceni-v-pohode.cz/faze-kybergroomingu-podezrele-chovani-virtualnich-pratel/>.

[52] KOPECKÝ, K. 2021. [online]. Kybergrooming. [citováno 2021-12-12]. Dostupné na internetu: <http://www.kybergrooming.cz/#kybergrooming>.

[53] MÁČELOVÁ, K. 2021. [online]. Učení v pohodě. [citováno 2021-12-12]. Dostupné na internetu: <https://www.uceni-v-pohode.cz/faze-kybergroomingu-podezrele-chovani-virtualnich-pratel/>.

[54] KOŽÍŠEK, M. – PÍSECKÝ, V. 2016. *Bezpečně na internetu, průvodce chováním ve světě online.* 1. vydání. Praha: Grada Publishing, a.s. 2016. 176 s. ISBN 978-80-247-5595-3.

[55] MÁČELOVÁ, K. 2021. [online]. Učení v pohodě. [citováno 2021-12-12]. Dostupné na internetu: <https://www.uceni-v-pohode.cz/faze-kybergroomingu-podezrele-chovani-virtualnich-pratel/>.

V páté fázi dochází k výrazné manipulaci, sexuálnímu obtěžování a zneužívání. Oběť, pokud se ve vztahu s agresorem v této fázi ocitne, potýká se s traumatem, zradou a zklamáním a jen velmi zřídka tuto událost nahlásí. Jedná se o fázi vystřízlivění[56].

4.2 Prevence kybergroomingu

Neposkytovat osobní citlivé údaje a kompromitující materiály jakéhokoli charakteru nikomu, koho znám jen z online prostředí, je tou nejspolehlivější ochranou proti predátorům, kybergroomům. Ovšem dětská osobnost je důvěřivá a bez získané zkušenosti je možné jen velmi těžko chtít, aby bylo schopno detekovat nebezpečí, hrozbu. K tomu, aby se dětský uživatel sociálních sítí snáze zorientoval ve svých virtuálních přátelích, může posloužit několik otázek, nad kterými by se samo dítě mělo zamyslet:

- Proč se mnou nekomunikuje přes webovou kameru?
- Proč nesmím o našem vztahu nikomu říct?
- Proč mi dává tolik intimních otázek?
- Neprotiřečí si u některých informací?
- Je v pořádku, že mi nabízí dárky a chce za to mé fotografie?[57]

V otázkách předcházení kybergroomingu je zcela zásadní aktivita rodičů. Každý rodič by měl být důsledný při kontrole činností svých dětí v online prostředí a předsudky o narušování soukromí dítěte je na místě odložit. Ovšem dle Kožíška ani *„ten nejpečlivější rodič není schopen kontrolu nad užíváním internetu svého dítěte zajistit. Není to jen kontrola domácích zařízení a kontroly jejich užívání, musíme si uvědomit, že děti mají běžně přístup k internetu ve většině škol, případně u spolužáků, kamarádů.“*[58] Proto je třeba své dítě poučit o rizicích spojených s internetem a mluvit s ním o jeho přátelích, o tom, s kým tráví svůj volný čas. Když dítě začne o svých kamarádech a aktivitách lhát, může se jednat o signál, že něco není v pořádku a že se v jeho životě objevila hrozba. O pomoc se mohou jak rodiče tak děti obrátit hned na několik institucí:

- Bílý kruh bezpečí
- E-Bezpečí
- Pomoc online

[56] KOŽÍŠEK, M. – PÍSECKÝ, V. 2016. *Bezpečně na internetu, průvodce chováním ve světě online.* 1. vydání. Praha: Grada Publishing, a.s. 2016. 176 s. ISBN 978-80-247-5595-3.
[57] NEBUĎ OBĚŤ! Rizika internetu a komunikačních technologií, z. s. [online]. [citováno 2021-12-04]. Dostupné na internetu: <http://www.nebudobet.cz/?cat=kybergrooming>.
[58] KOŽÍŠEK, M. – PÍSECKÝ, V. 2016. *Bezpečně na internetu, průvodce chováním ve světě online.* 1. vydání. Praha: Grada Publishing, a.s. 2016. Přímá citace 10 s. ISBN 978-80-247-5595-3.

- Národní centrum bezpečnějšího internetu
- Policie ČR[59]

Obranu i ochranu před potencionálními pachateli lze účinně zvýšit posílením osvěty, sociálně – psychologických aspektů a právního vědomí. Prevenci je nutné zaměřit také na práci s pachatelem, kde je důležité se zaměřit na oblast resocializace. Riziko recidivy u těchto pachatelů je značně vysoké[60].

4.3 Právní rámec kybergroomingu

Každá, ať již fyzická nebo právnická osoba, která dítěti mladšímu patnácti let, navrhne osobní setkání s cílem spáchat na něm trestný čin výroby pornografie, pohlavního zneužití, případně jiný trestný čin se sexuální pohnutkou, naplňuje objektivní stránku trestného činu navazování nedovolených kontaktů s dítětem. Předmětný trestný čin je upraven § 193b trestního zákoníku. Možnosti trestně – právního řešení fenoménů, které v oblasti kyberkriminality, tedy i kybergroomingu, virtuální prostor umožňuje a mnohdy i umocňuje, je jednoznačným základem pro prevenci a pro bezpečnost každého uživatele[61].

Zákon č. 40/2009 Sb., trestní zákoník (dále jen trestní zákoník) § 193b – Navazování nedovolených kontaktů s dítětem hovoří o tom, že kdo navrhne setkání dítěti mladšímu patnácti let v úmyslu spáchat trestný čin podle § 187 odst. 1, § 192, 193, § 202 odst. 2 nebo jiný sexuálně motivovaný trestný čin, bude potrestán odnětím svobody až na dvě léta. Dále dle trestního zákoníku, § 187 odst. 1 – Pohlavní zneužití, trest odnětí svobody na jeden až osm let, § 192, 193 – Výroba a jiné nakládání s dětskou pornografií, odnětí svobody na 6 měsíců až šest let, § 202 odst. 2 – Svádění k pohlavnímu styku, odnětí svobody až na dvě léta[62].

[59] Záchranný kruh. [online]. Kybergrooming. [citováno 2021-11-12]. Dostupné na internetu: <https://www.zachranny-kruh.cz/osobni-bezpeci/dalsi-nebezpeci/kybergrooming/kybergrooming.html>.
[60] HAMBERGER, T. Prevence kriminality 2021. [online]. Kybergrooming. [citováno 2021-11-10]. Dostupné na internetu: <https://prevencekriminality.cz/kybergrooming/>.
[61] HAMBERGER, T. Prevence kriminality 2021. [online]. Kybergrooming. [citováno 2021-11-10]. Dostupné na internetu: <https://prevencekriminality.cz/kybergrooming/>.
[62]Zákon číslo 40/2009 Sb. Trestní zákoník.

5 RÁMCOVÝ VZDĚLÁVACÍ PROGRAM PRO ZÁKLADNÍ VZDĚLÁVÁNÍ

Od roku 1989 probíhá reforma českého školství a vzdělávání, kterou řídí Ministerstvo školství, mládeže a tělovýchovy, jež pověřuje svá resortní pracoviště přípravou kurikulárních dokumentů. Základní koncepční materiály, kterými jsou jistě Budoucnost vzdělání školství v obnovené demokratické společnosti a ve sjednocující se Evropě, Svoboda ve vzdělávání a česká škola a Program transformace vzdělávací soustavy, upozorňují na to, že funkcí školy je především rozvoj osobnosti žáka. Následně se nejdůležitějším koncepčním dokumentem stal Národní program rozvoje vzdělávání v České republice, tak zvaná Bílá kniha. V Bílé knize byl vymezen systém více úrovní vzdělávacích programů, kde rámcové vzdělávací programy měly formulovat učební plán a pravidla školních vzdělávacích programů. Je kladen důraz na komplexnost tvorby obsahu vzdělávání a možnost modifikace obsahu vzdělání dle individuálních potřeb jednotlivých typů škol, regionů, požadavků učitelů, žáků a jejich rodičů[63].

Rámcový vzdělávací program, cíle, forma a stanovená délka vzdělávání je dána zákonem číslo 561/2004 Sb. o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon). Zákon zároveň vymezuje povinnosti i práva jak fyzických, tak i právnických osob, které se na vzdělávání podílejí. Rámcové vzdělávací programy stanovují členění obsahu dle jednotlivých období, případně ročníků, přizpůsobují obsah danému oboru, organizuje podmínky průběhu a ukončení vzdělání. Ministerstvo školství, mládeže a tělovýchovy po projednání s Ministerstvem zdravotnictví určí podmínky ochrany zdraví pro uskutečňování vzdělávání. Rámcové vzdělávací programy vycházejí z nejnovějších poznatků vědních disciplín, pedagogiky a psychologie s ohledem na vhodnost využití pro konkrétní věkovou kategorii[64].

5.1 Vzdělávací program předmětu Informační a komunikační technologie pro první stupeň základních škol

Rámcový vzdělávací program Ministerstva školství, mládeže a tělovýchovy pro základní vzdělávání se zaměřením na vzdělávací oblast Informační a komunikační

[63] FIALOVÁ, L. a kol. 2015. *Vzdělávací oblast Člověk a zdraví v současné škole.* 1. vydání. Praha: Univerzita Karlova v Praze, Nakladatelství Karolinum. 2015. 197 s. ISBN 978-80-246-2885-1.
[64] Zákon číslo 561/2004 Sb. o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon).

technologie pro první stupeň základních škol stanovuje minimální časovou dotaci učebního plánu na dvě hodiny týdně. Obsah vzdělávání je zde vymezen do čtyř okruhů. První okruh je zaměřen na data, informace a modelování. Jedná se o základní ovládání počítače a práce s daty. Modelové znázorňování skutečnosti včetně porovnávání a vysvětlování jevů kolem žáka. Druhý okruh je zaměřen na algoritmizaci a programování. Edukativní činnost je cílena na objevování a experimentování v programovacím prostředí včetně porozumění kroků postupů v algoritmu. Třetí okruh je cílen na informační systémy a jejich vzájemné působení. Čtvrtý okruh je vymezen na digitální technologie a jejich účel. Konkrétně na hardware, software, počítačové sítě a pravidla bezpečné práce s digitálními zařízeními, hesly a účty[65].

Školní vzdělávací program základní školy Jih Mariánské Lázně vymezuje výuku Informačních a komunikačních technologií ve 4. a 5. ročníku v časové dotaci dvou vyučovacích hodin týdně, kde v 5. ročníku s jednou disponibilní hodinou týdně. Výuka pro 4. ročník je obsahově vymezena na učivo základního ovládání počítače, obecné ovládání programů pod Windows, vytváření jednoduchých dokumentů v textovém editoru a vkládání obrázků z webu, seznámení se s internetem a programy umožnujíc internetovou komunikaci, vysvětlení pojmu kyberšikany, webové prohlížeče a vyhledávání požadovaných informací. V 5. ročníku je učivo vymezeno na základní údržbu počítače včetně řešení běžné problematiky s hardwarem a softwarem, operační systémy a jejich základní funkce, zásady bezpečnosti práce s počítačem proti zneužití dat a virového napadení, autorský zákon a legální software, práce se soubory, vytváření jednoduchých prezentací a jejich prezentování[66].

Školní vzdělávací program základní školy Úšovice Mariánské Lázně vymezuje výuku Informačních a komunikačních technologií ve 4. ročníku v časové dotaci dvou vyučovacích hodin týdně. Pro 1.-3. ročník je předmět Informatika integrován do předmětu Český jazyk a literatura, kde je obsahem cíleno na seznámení se s počítačem a jeho základními funkcemi. Ve 4. ročníku je učivo vymezeno na pravidla práce s počítačem, legálnost softwaru, práci se soubory, základní ovládání programu Word, práce s textem a jeho formátování, tisk dokumentů a jejich ukládání na lokální disk, ovládání

[65] MŠMT [online]. [citováno 2021-12-04]. Dostupné na internetu: <https://www.msmt.cz/file/56005/>.
[66] Základní škola Jih Mariánské Lázně. [online]. *Dokumenty školy*. [citováno 2021-11-28]. Dostupné na internetu: <https://skolajih.cz/?sekce=skola&stranka=dokumenty_skoly>.

internetového prohlížeče a vyhledávací portály, využívání SMS brány a chatu, práce s emailem, práce s výukovými programy a rastrovými obrázky[67].

5.2 Vzdělávací program předmětu Informační a komunikační technologie pro druhý stupeň základních škol

Rámcový vzdělávací program Ministerstva školství, mládeže a tělovýchovy pro základní vzdělávání se zaměřením na vzdělávací oblast Informační a komunikační technologie pro druhý stupeň základních škol stanovuje minimální časovou dotaci učebního plánu na čtyři hodiny týdně. Obsah výuky je rozdělen do čtyř okruhů. První okruh je cílen na data, informace a modelování. Zahrnuje přehled ve vyhledávání a ukládání dat obecně a počítači, přenosu dat, tvorbu základních grafových úloh a vývojových diagramů. Druhý okruh je zaměřen na algoritmizaci a programování. Jedná se o základní programovací prostředí, tvorba a zápis algoritmů, autorství a licence programů. Třetí okruh učební náplně je vymezen na informační systémy. Vysvětlení účelu běžně používaných informačních systémů. Čtvrtý okruh je vymezen na digitální technologie. Konkrétně na nebezpečné aplikace a systémy, zabezpečení zařízení a dat, digitální stopu, správa souborů a instalace aplikací, postupy při řešení problémů s digitálním zařízením.[68].

Školní vzdělávací program základní školy Jih Mariánské Lázně vymezuje výuku Informačních a komunikačních technologií v 6. až 9. ročníku v časové čtyř vyučovacích hodin týdně, kde v 7. až 9. ročníku ještě navíc po jedné disponibilní hodině týdně. V 6. ročníku je obsah učiva zaměřen na dělení počítačů (PC, Notebook, Netbook atd.) a jejich komponenty, operačním systémy a jejich funkce, ovládání systému Windows, datová média, softwary a jejich využití, kopírování a přesouvání souborů, počítačová grafika, webové prohlížeče a zásady vyhledávání informací, způsoby internetové komunikace a obsluha e-mailové schránky, zásady bezpečnosti práce s výpočetní technikou. Učivo v 7. ročníku je zaměřeno na práci s dokumenty a editace textů. Vkládání grafiky, tabulek, rovnic a speciálních znaků do dokumentu. Práce s hromadnou korespondencí. V 8. ročníku je výuka zaměřena na práci s tabulkovým kalkulátorem. Obsahem je vytvoření nového sešitu v tabulkovém kalkulátoru, práce s listy, editace obsahu buněk a jejich formátování, tvorba základních vzorců, vkládání grafů a jejich editace včetně tisku

[67] Základní škola Úšovice. [online]. *Dokumenty ke stažení*. [citováno 2021-11-28]. Dostupné na internetu: <https://www.zsusovice.cz/index.php/domu/ke-stazeni>.
[68] MŠMT [online]. [citováno 2021-12-04]. Dostupné na internetu: <https://www.msmt.cz/file/56005/>.

vytvořeného listu. Učivo 9. ročníku obsahuje základy webových stránek a jazyka kódování internetových stránek, práce s digitální fotografií, ovládání prezentačního programu a vytváření prezentací, práce s vektorovým editorem[69].

Školní vzdělávací program základní školy Úšovice Mariánské Lázně vymezuje výuku Informačních a komunikačních technologií v 6.-9. ročníku v časové dotaci čtyř vyučovacích hodin týdně. Zde je obsah učiva stanoven všeobecně pro všechny ročníky druhého stupně. Jedná se o zaměření na internet a komunikaci skrze internet, vývojové trendy informačních technologií, ovládání textových a grafických editorů, počítačová grafika, práce s tabulkovým editorem, vytváření tabulek a jednoduchých vzorců, tvorba prezentací na uživatelské úrovni v textové, grafické a multimediální formě[70].

[69] Základní škola Jih Mariánské Lázně. [online]. *Dokumenty školy*. [citováno 2021-11-28]. Dostupné na internetu: <https://skolajih.cz/?sekce=skola&stranka=dokumenty_skoly>.
[70] Základní škola Úšovice. [online]. *Dokumenty ke stažení*. [citováno 2021-11-28]. Dostupné na internetu: <https://www.zsusovice.cz/index.php/domu/ke-stazeni>.

6 VÝSLEDKY PRŮZKUMU

Práce byla zaměřena na vyhodnocení schopností žáků šestých tříd pohybovat se ve virtuálním prostředí. Cílem práce bylo stanoveno zjistit, do jaké míry jsou žáci základních škol znalí rizik virtuálního prostředí. V následujících kapitolách byly vyhodnocovány odpovědi na jednotlivé otázky z dotazníků a rozhovoru a výsledky byly analyzovány také v celkovém kontextu.

K dosažení cíle byly vedle průzkumných cílů nadefinovány průzkumné otázky:

1. Průzkumná otázka: V jaké míře komunikují rodiče se svými dětmi na téma využívání internetu?

2. Průzkumná otázka: Do jaké míry se rodiče zabývají kontrolou činností svých dětí ve virtuálním prostředí?

3. Průzkumná otázka: V jakém rozsahu se školní aktivity podílejí na dobré orientaci dětí ve virtuálním prostředí?

4. Průzkumná otázka: Do jaké míry jsou žáci základních škol schopni vyhodnotit závadové chování na internetu?

5. Průzkumná otázka: S jakou jistotou dokáží žáci základních škol identifikovat známky a hrozby kybergroomingu?

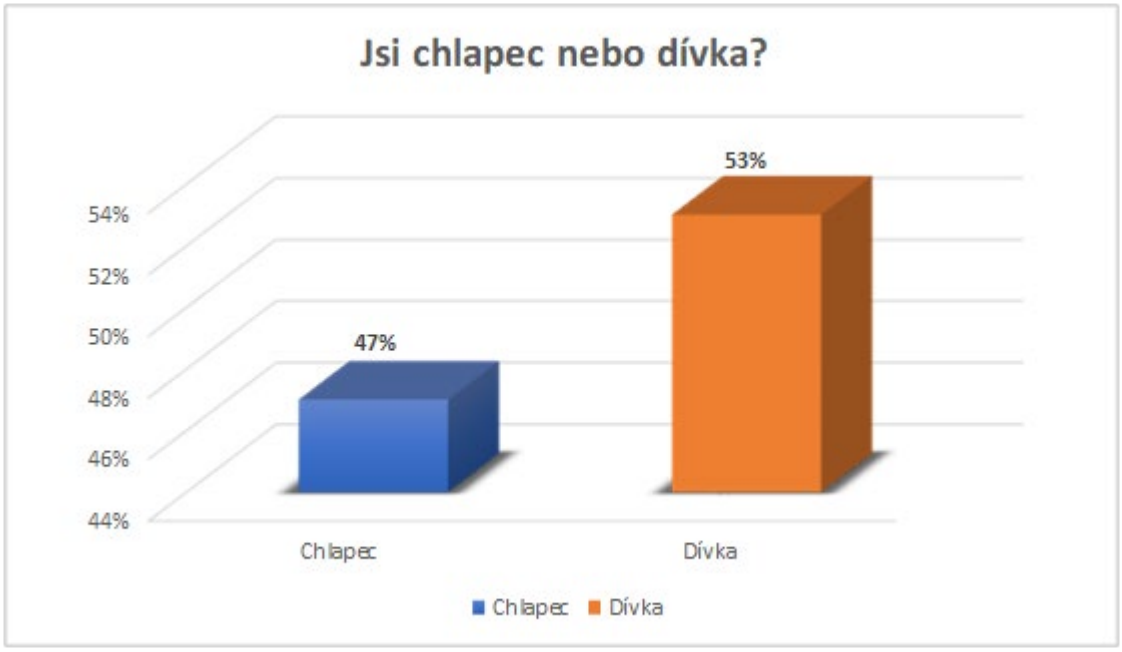
6. Průzkumná otázka: Vyhodnotit, jsou-li a případně v jakém rozsahu, rozdíly v orientaci ve virtuálním světě mezi chlapci a dívkami.

6.1 Interpretace výsledků průzkumu kvantitativní metodou

Dotazník obsahoval celkem 15 otázek, z nichž jedna byla kategorizační položka, týkající se pohlaví. Dále byly použity tři otázky polouzavřené, v rámci kterých bylo zjišťováno, na kterých sociálních sítích jsou respondenti registrováni, jakým činnostem se nejvíce v online prostředí věnují a jestli jsou rodiče zdrojem informací o rizicích virtuálního světa. Jedenáct otázek bylo uzavřených a byly zaměřeny na zjištění, kolik času tráví respondenti na internetu, jestli se rodiče zajímají o chování svých dětí v online prostředí, jestli je školní prostředí zdrojem informací k virtuálnímu prostředí, jestli již respondenti měli osobní zkušenost s riziky kyberprostoru, jestli se setkali s kybergroomingem a jestli respondenti vědí, na koho se obrátit v případě podezření na rizikové jednání. Tři polytomické otázky byly zaměřeny na to, čemu se respondenti na internetu věnují, jaké sociální sítě používají a s jakou situací mají osobní zkušenost. Jeden

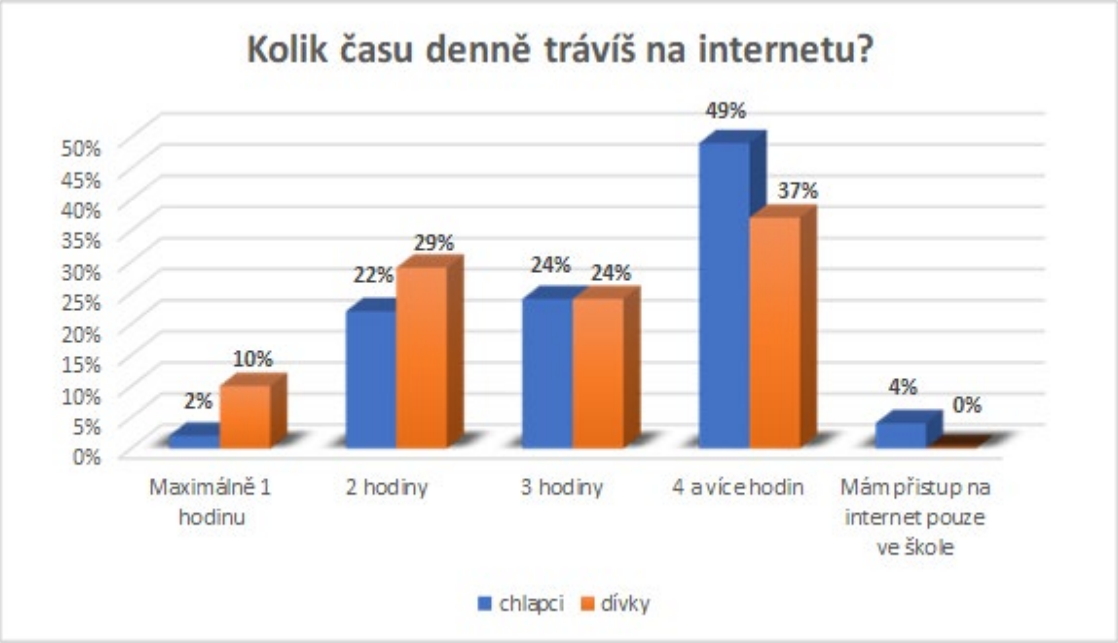
dotaz se vztahoval ke znalosti terminologie a jedna otázka zjišťovala, jestli mají respondenti pocit ohrožení tím, že zveřejňují informace o sobě v online prostředí. Šest dichotomických otázek bylo umístěno do střední části dotazníku, byly jasné a jednoduché a respondenti zde volili pouze jednu odpověď – ano/ne. Každá otázka byla vyhodnocena tak, aby bylo možné porovnat rozdíly v odpovědích chlapců a dívek. Získané odpovědi byly uloženy v PC. Údaje, získané dotazníkovým šetřením, byly zpracovány pomocí počítačového programu Microsoft Excel. Výsledky nejsou všeobecné a vztahují se pouze k námi zkoumanému vzorku respondentů, kteří byli záměrně vybráni mezi žáky základních škol v Mariánských Lázních. Odpovědi respondentů byly po vyhodnocení zobrazeny pomocí grafů. Každý graf se vztahuje k jedné dotazníkové otázce. V případě vyhodnocení otázky, vztahující se k pohlaví respondenta, bylo použito vyhodnocení relativního počtu, neboť tyto dvě skupiny nejsou složeny ze stejného počtu respondentů a námi zvoleným postupem bylo dosaženo objektivních výsledků, které bylo možné, v porovnání mezi jednotlivými skupinami, použít.

Graf č. 1: Vymezení vzorku (Zdroj: Autor, 2022)



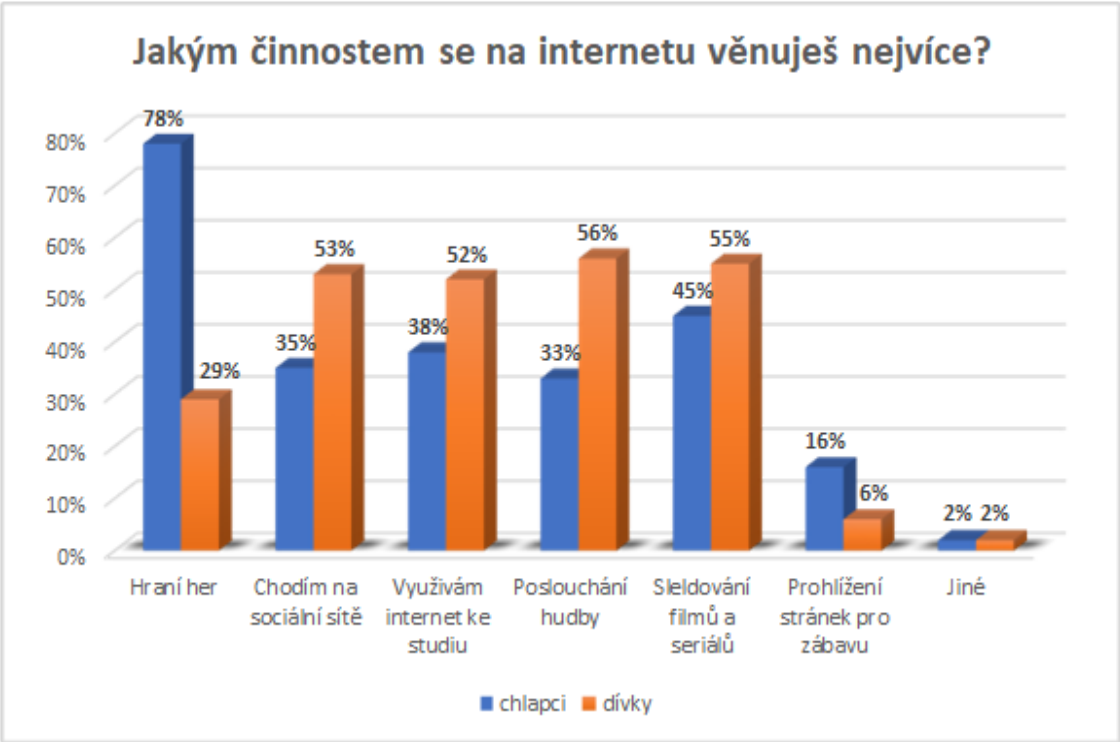
První otázka byla kategorizační **„jsi chlapec nebo dívka“** a byla položena s cílem zjistit, jaký podíl průzkumného vzorku tvoří chlapci a jaký dívky. Průzkumný vzorek byl složen ze 117 respondentů. Chlapců bylo 55, což odpovídá 47 % z celku. Dívky byly 62, což tvoří 53 % z celku.

Graf č. 2: Upřesnění doby užívání internetu (Zdroj: Autor, 2022)



Odpovědi respondentů na dotaz **„kolik času denně trávíš na internetu“**, kdy respondenti mohli volit jednu z pěti možností – 1 hodinu, 2 hodiny, 3 hodiny, 4 hodiny a více, mám přístup na internet pouze ve škole – jsme hodnotili také s ohledem na to, jestli odpovídá chlapec nebo dívka. Pouze **hodinu na internetu denně** tráví 1 chlapec, což odpovídá 2 % z celkového počtu chlapců a 6 dívek, což odpovídá 10 % z celkového počtu dívek. **2 hodiny denně** na internetu tráví 12 chlapců, což odpovídá 22 % z celkového počtu chlapců a 18 dívek, což odpovídá 29 % z celkového počtu dívek. **3 hodiny denně** na internetu tráví 13 chlapců, což odpovídá 24 % z celkového počtu chlapců a 15 dívek, což odpovídá shodě s chlapci, 24 % z celkového počtu dívek. **4 hodiny a více denně** na internetu tráví 27 chlapců, což odpovídá 49 % z celkového počtu chlapců a 23 dívky, což odpovídá 37 % z celkového počtu dívek. Pouze 2 chlapci, což odpovídá 4 % z celkového počtu chlapců, odpověděli, že **mají přístup na internet pouze ve škole** a v odpovědi tuto možnost nevyužila ani jedna dívka. Z výsledků jednoznačně vyplývá, že největší procento dětí tráví na internetu 4 a více hodin denně. Z celkového počtu 117 respondentů tuto odpověď zvolilo 50 dětí, což odpovídá 42,7 % z celku.

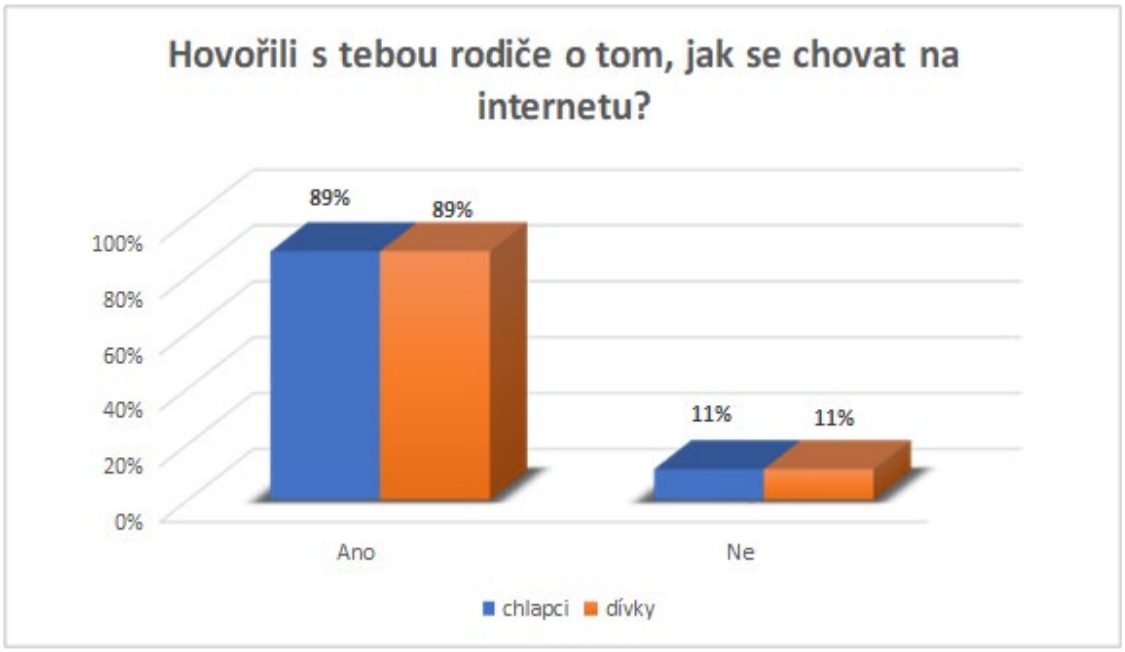
Graf č. 3: Využití internetu (Zdroj: Autor, 2022)



Odpovědi respondentů na dotaz **„jakým činnostem se na internetu věnuješ nejvíce“**, kdy respondenti mohli volit až tři ze šesti možností – hraní her, chodím na sociální sítě, využívám internet ke studiu, poslouchání hudby, sledování hudby a seriálů, prohlížení stránek pro zábavu, jiné (zde měli respondenti možnost doplnit vlastní text) – jsme hodnotili také s ohledem na to, jestli odpovídá chlapec nebo dívka. **Hraní her** se věnují 43 chlapci, což odpovídá 78 % z celkového počtu chlapců a 18 dívek, což odpovídá 29 % z celkového počtu dívek. **Chození na sociální sítě** se věnuje 19 chlapců, což odpovídá 35 % z celkového počtu chlapců a 33 dívky, což odpovídá 55 % z celkového počtu dívek. **Internet ke studiu** využívá 21 chlapec, což odpovídá 38 % z celkového počtu chlapců a 32 dívky, což odpovídá 52 % z celkového počtu dívek. **Poslouchání hudby** se věnuje 18 chlapců, což odpovídá 33 % z celkového počtu chlapců a 35 dívek, což odpovídá 56 % z celkového počtu dívek. **Sledování filmů a seriálů** se věnuje 25 chlapců, což odpovídá 45 % z celkového počtu chlapců a 34 dívky, což odpovídá 55 % z celkového počtu dívek. **Prohlížení stránek pro zábavu** se věnuje 9 chlapců, což odpovídá 16 % z celkového počtu chlapců a 4 dívky, což odpovídá 6 % z celkového počtu dívek. Odpověď **jiné** zvolil 1 chlapec, tedy 2 % z celkového počtu chlapců a zároveň doplnil, že na internetu hledá zajímavosti a odpověď **jiné** také zvolila 1 dívka, což odpovídá 2 % z celkového počtu dívek a zároveň doplnila, že se věnuje distanční výuce. Výsledky nám jednoznačně definují, že oblast zájmu činností ve virtuálním světě je

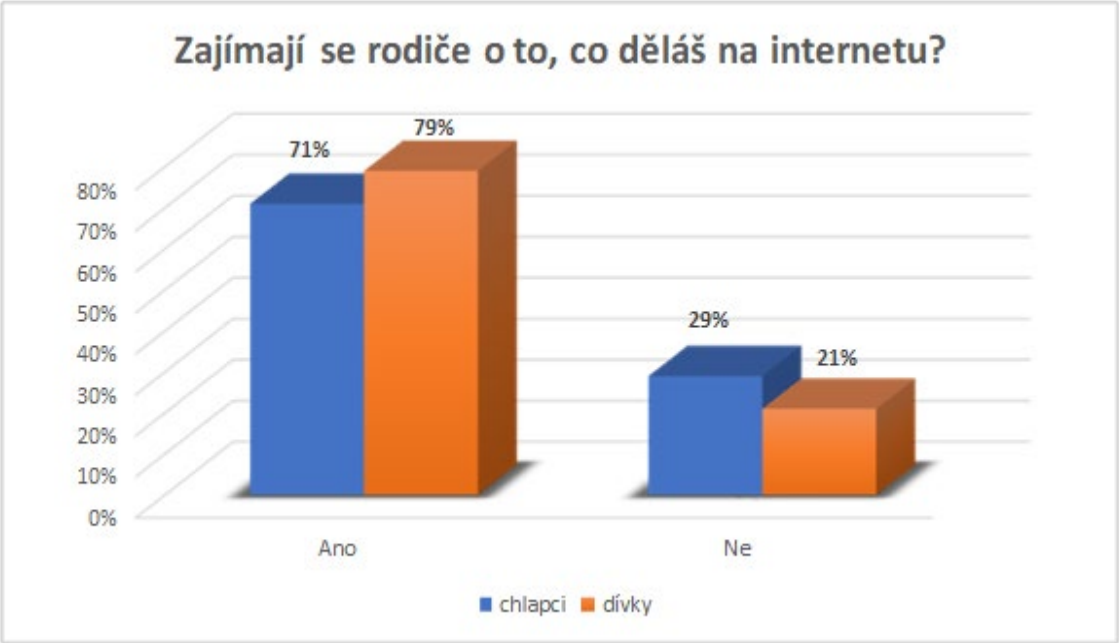
rozdílná u chlapců a dívek. Chlapci svůj čas tráví převážně hraním her, na rozdíl od dívek, které svůj čas na internetu věnují hudbě, filmům a sociálním sítím.

Graf č. 4: Rady od rodičů, jak se chovat na internetu (Zdroj: Autor, 2022)



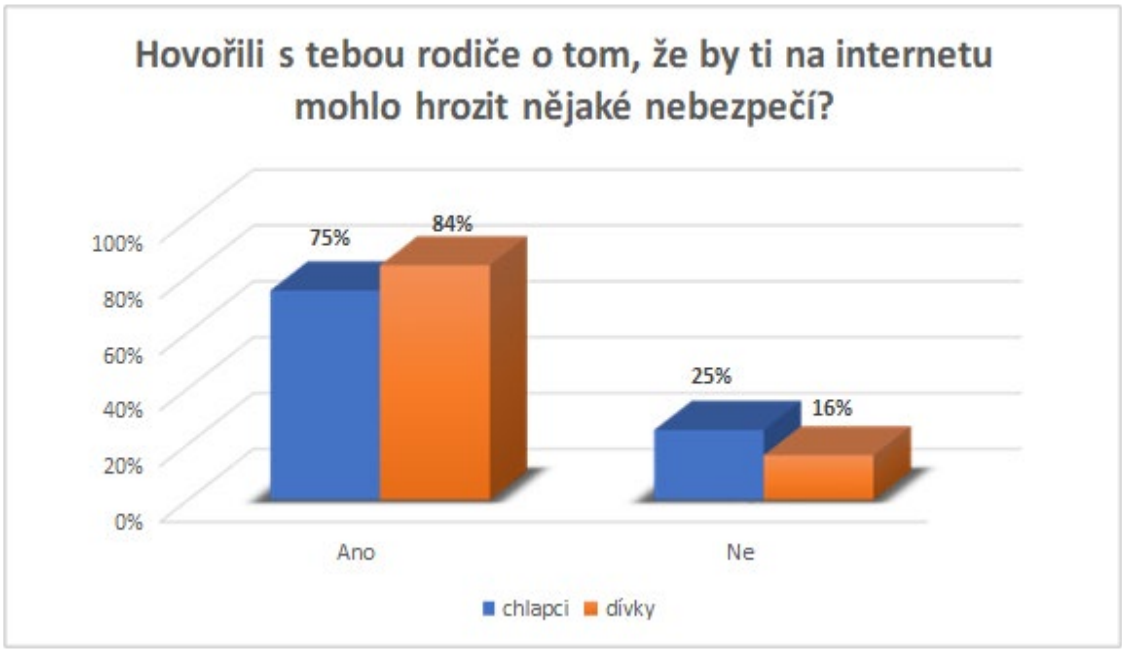
Odpovědi respondentů na dotaz **„hovořili s tebou rodiče o tom, jak se chovat na internetu“**, kdy respondenti volili mezi odpovědí ano / ne, jsme hodnotili také s ohledem na to, jestli odpovídá chlapec nebo dívka. V případě této otázky došlo ke shodě v relativním počtu odpovědí chlapců a dívek. **Ano** odpovědělo 49 chlapců, což odpovídá 89 % z celkového počtu chlapců a 55 dívek, což odpovídá 89 % z celkového počtu dívek. **Ne** odpovědělo 6 chlapců, což odpovídá 11 % z celkového počtu chlapců a 7 dívek, což odpovídá 11 % z celkového počtu dívek. Z celkového počtu 117 respondentů odpovědělo 104 děti ano, že s nimi rodiče hovoří o tom, jak se chovat na internetu, což odpovídá 88,9 % z celkového počtu respondentů, se 13 dětmi, což je 11,1 % z celku, rodiče o chování na internetu nehovoří.

Graf č. 5: Kontrola rodičů (Zdroj: Autor, 2022)



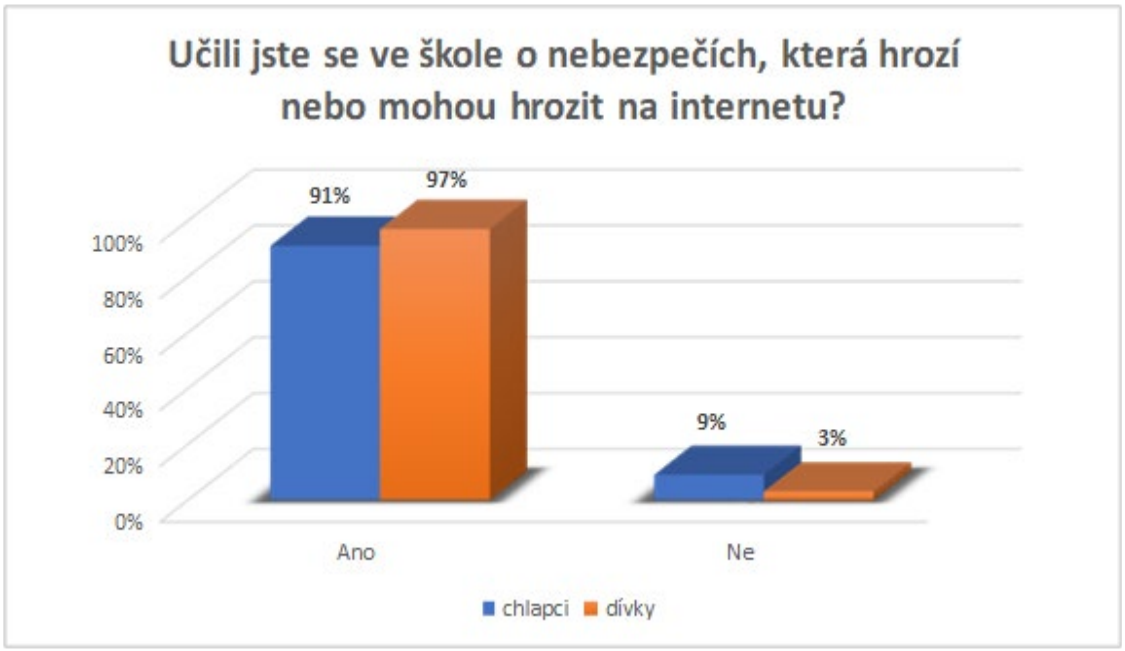
Odpovědi respondentů na dotaz **„zajímají se rodiče o to, co děláš na internetu“**, kdy respondenti volili mezi odpovědí ano / ne, jsme hodnotili také s ohledem na to, jestli odpovídá chlapec nebo dívka. **Ano** odpovědělo 39 chlapců, což odpovídá 71 % z celkového počtu chlapců a 49 dívek, což odpovídá 79 % z celkového počtu dívek. **Ne** odpovědělo 16 chlapců, což odpovídá 29 % z celkového počtu chlapců a 13 dívek, což odpovídá 21 % z celkového počtu dívek. Z celkového počtu 117 respondentů odpovědělo 88 dětí ano, že se rodiče zajímají o to, co dělají na internetu, což odpovídá 75,2 % z celkového počtu respondentů, ale stále je zde 29 dětí, což je 24,8 % z celku, u kterých se rodiče o činnosti svých dětí na internetu nezajímají.

Graf č. 6: Upozornění od rodičů na internetová rizika (Zdroj: Autor, 2022)



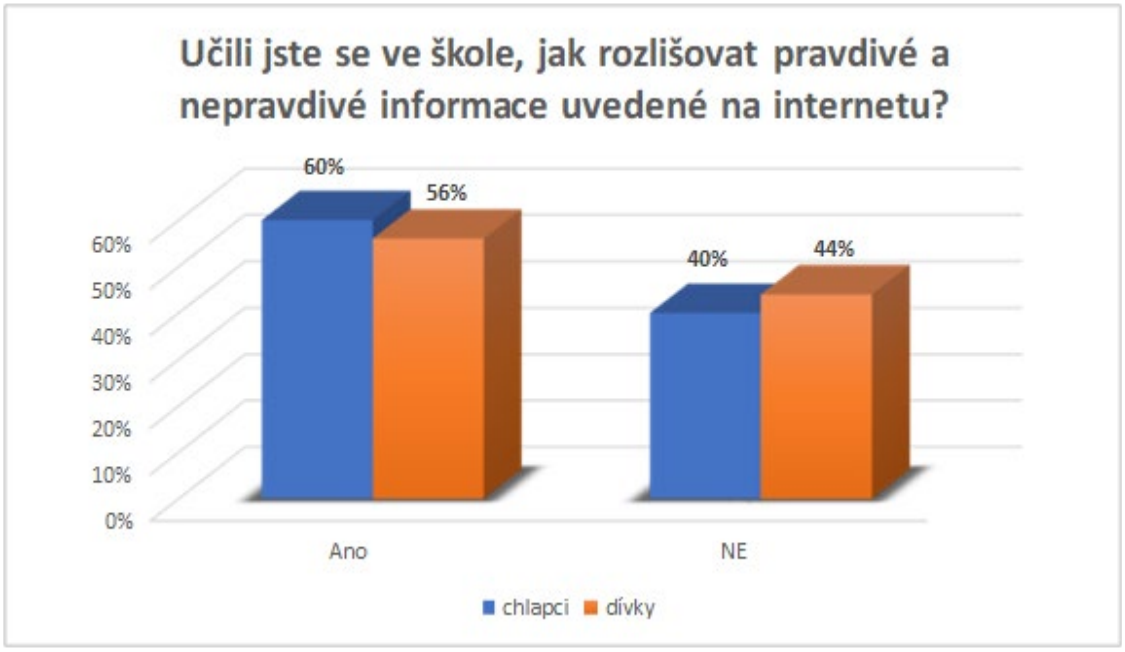
Odpovědi respondentů na dotaz **„hovořili s tebou rodiče o tom, že by ti na internetu mohlo hrozit nějaké nebezpečí“**, kdy respondenti volili mezi odpovědí ano/ne, jsme hodnotili také s ohledem na to, jestli odpovídá chlapec nebo dívka. V případě odpovědi ano mohli respondenti konkretizovat odpověď vlastním textem. **Ano** odpověděl 41 chlapec, což odpovídá 75 % z celkového počtu chlapců a 52 dívek, což odpovídá 84 % z celkového počtu dívek. **Ne** odpovědělo 14 chlapců, což odpovídá 25 % z celkového počtu chlapců a 10 dívek, což odpovídá 16 % z celkového počtu dívek. V případě kladné odpovědi chlapci nejčastěji textem doplnili, že je rodiče **varovali před činnostmi na sociálních sítích a před pedofily**. U dívek byly odpovědi textem podobné, jen se ještě objevilo **varování před zveřejněním soukromých informací a před kontakty s falešnou identitou**. Z celkového počtu 117 respondentů odpověděly 93 děti ano, že s nimi rodiče hovoří o konkrétních nebezpečích na internetu, což odpovídá 79,5 % z celkového počtu respondentů, ale stále jsou zde 24 děti, což je 20,5 % z celku, se kterými rodiče o nebezpečích na internetu nehovoří.

Graf č.7: Výuka rizik na internetu ve škole (Zdroj: Autor, 2022)



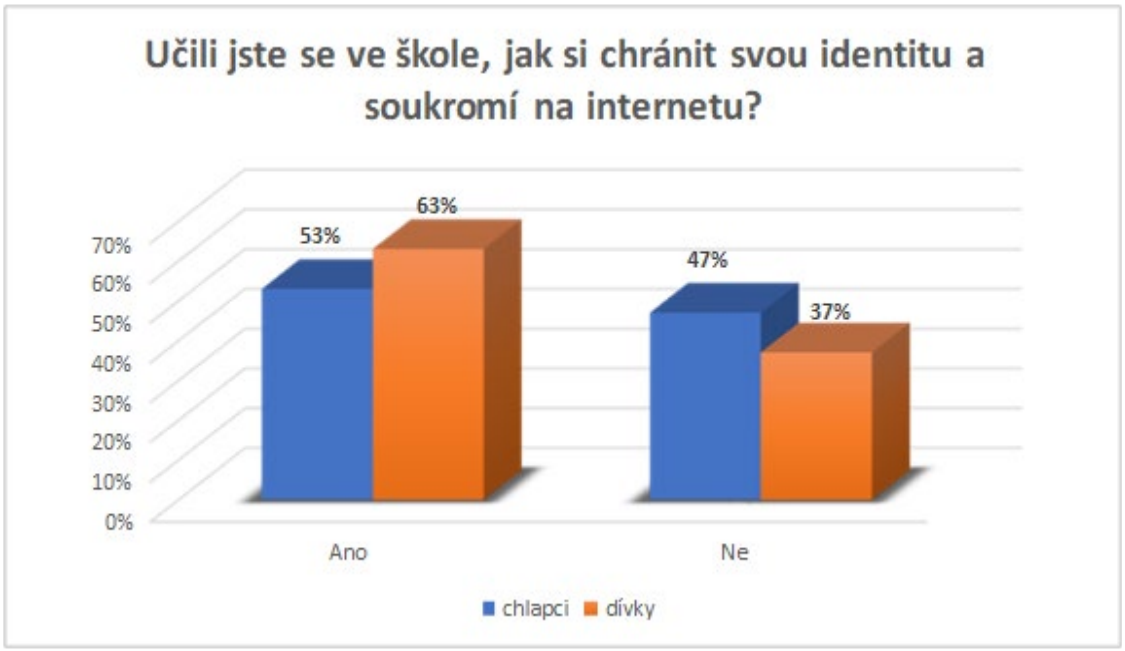
Odpovědi respondentů na dotaz **„učili jste se ve škole o nebezpečích, která hrozí nebo mohou hrozit na internetu“**, kdy respondenti volili mezi odpovědí ano / ne, jsme hodnotili také s ohledem na to, jestli odpovídá chlapec nebo dívka. **Ano** odpovědělo 50 chlapců, což odpovídá 91 % z celkového počtu chlapců a 60 dívek, což odpovídá 97 % z celkového počtu dívek. **Ne** odpovědělo 5 chlapců, což odpovídá 9 % z celkového počtu chlapců a 2 dívky, což odpovídá 3 % z celkového počtu dívek. Z celkového počtu 117 respondentů odpovědělo 110 dětí ano, že se ve škole o nebezpečích virtuálního světa učily, což odpovídá 94 % z celkového počtu respondentů a 7 dětí, což odpovídá 6 % z celku, odpovědělo, že se ve škole o rizicích na internetu neučily.

Graf č. 8: Analyzování informací uvedených na internetu ve školním prostředí (Zdroj: Autor, 2022)



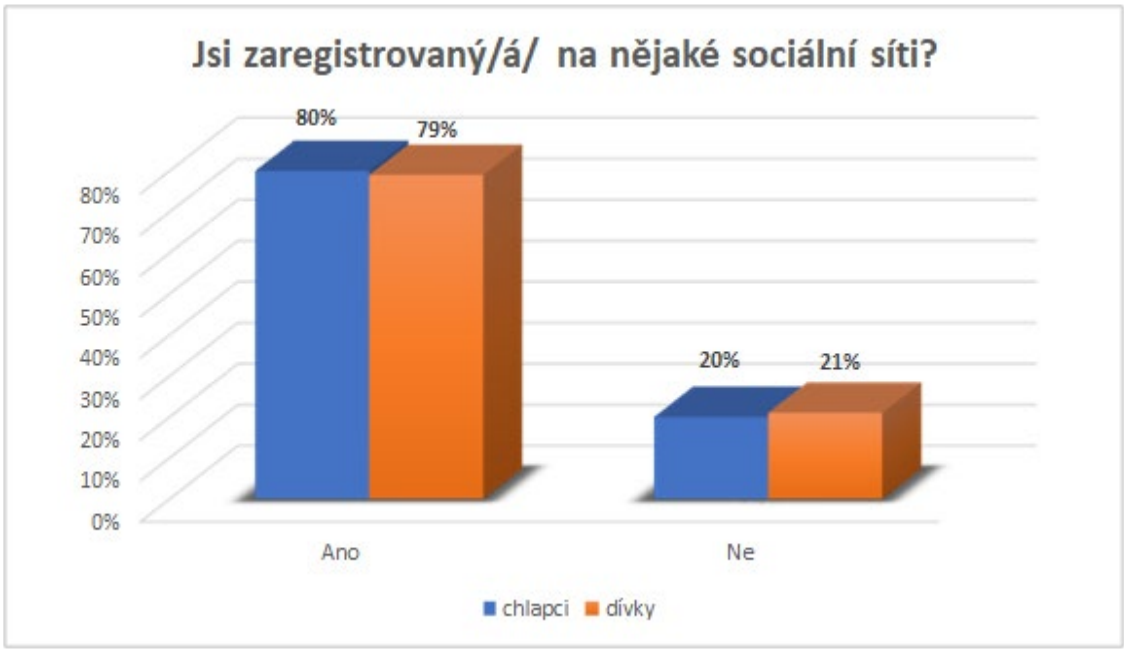
Odpovědi respondentů na dotaz **„učili jste se ve škole, jak rozlišovat pravdivé a nepravdivé informace uvedené na internetu“**, kdy respondenti volili mezi odpovědí ano / ne, jsme hodnotili také s ohledem na to, jestli odpovídá chlapec nebo dívka. **Ano** odpověděli 33 chlapci, což odpovídá 60 % z celkového počtu chlapců a 35 dívek, což odpovídá 56 % z celkového počtu dívek. **Ne** odpověděli 22 chlapci, což odpovídá 40 % z celkového počtu chlapců a 27 dívek, což odpovídá 44 % z celkového počtu dívek. Z celkového počtu 117 respondentů odpovědělo 68 dětí ano, že se ve škole učili, jak rozlišovat pravdivé a nepravdivé informace ve virtuálním světě, což odpovídá 58 % z celkového počtu respondentů a 49 dětí, což odpovídá 42 % z celku, odpovědělo, že se ve škole o rozpoznávání pravdivých a nepravdivých informací na internetu neučili.

Graf č. 9: Ochrana své identity v internetovém prostředí (Zdroj: Autor, 2022)



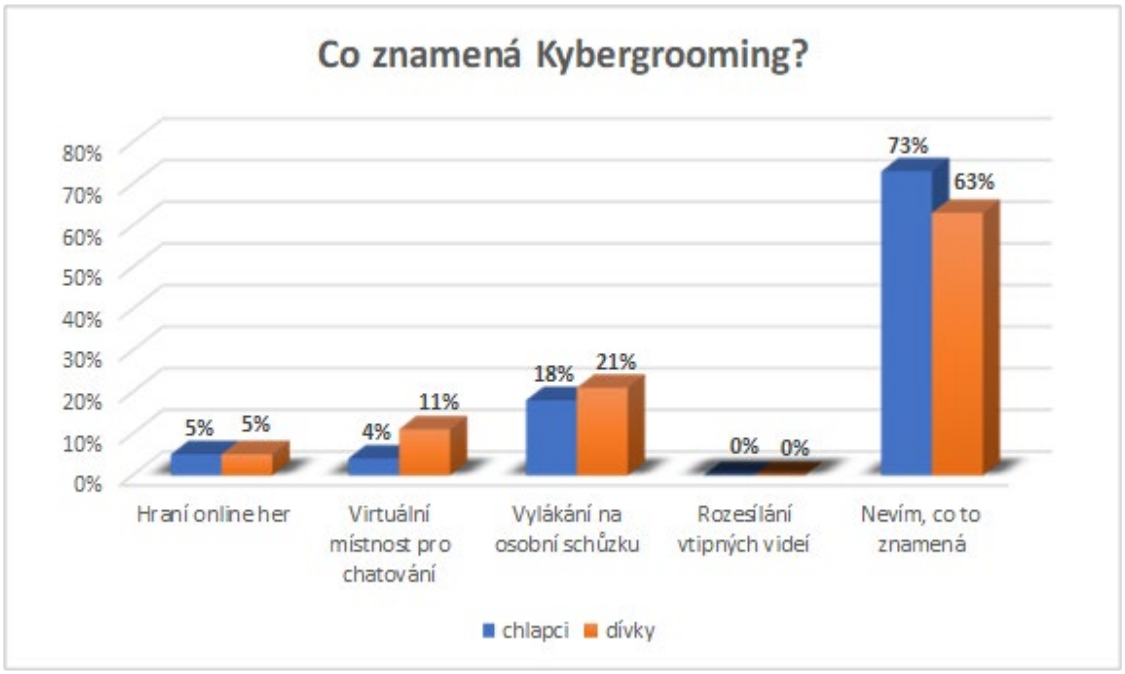
Odpovědi respondentů na dotaz „**učili jste se ve škole, jak si chránit svou identitu a soukromí na internetu“**, kdy respondenti volili mezi odpovědí ano / ne, jsme hodnotili také s ohledem na to, jestli odpovídá chlapec nebo dívka. **Ano** odpovědělo 29 chlapců, což odpovídá 53 % z celkového počtu chlapců a 39 dívek, což odpovídá 63 % z celkového počtu dívek. **Ne** odpovědělo 26 chlapců, což odpovídá 47 % z celkového počtu chlapců a 23 dívek, což odpovídá 37 % z celkového počtu dívek. Z celkového počtu 117 respondentů odpovědělo 68 dětí ano, že se ve škole učili, jak si chránit své soukromí ve virtuálním světě, což odpovídá 58 % z celkového počtu respondentů a 49 dětí, což odpovídá 42 % z celku, odpovědělo, že se ve škole o ochraně vlastního soukromí na internetu neučili. Výrazně větší podíl kladných odpovědí byl vyhodnocen u dívek.

Graf č. 10: Využití sociálních sítí (Zdroj: Autor, 2022)



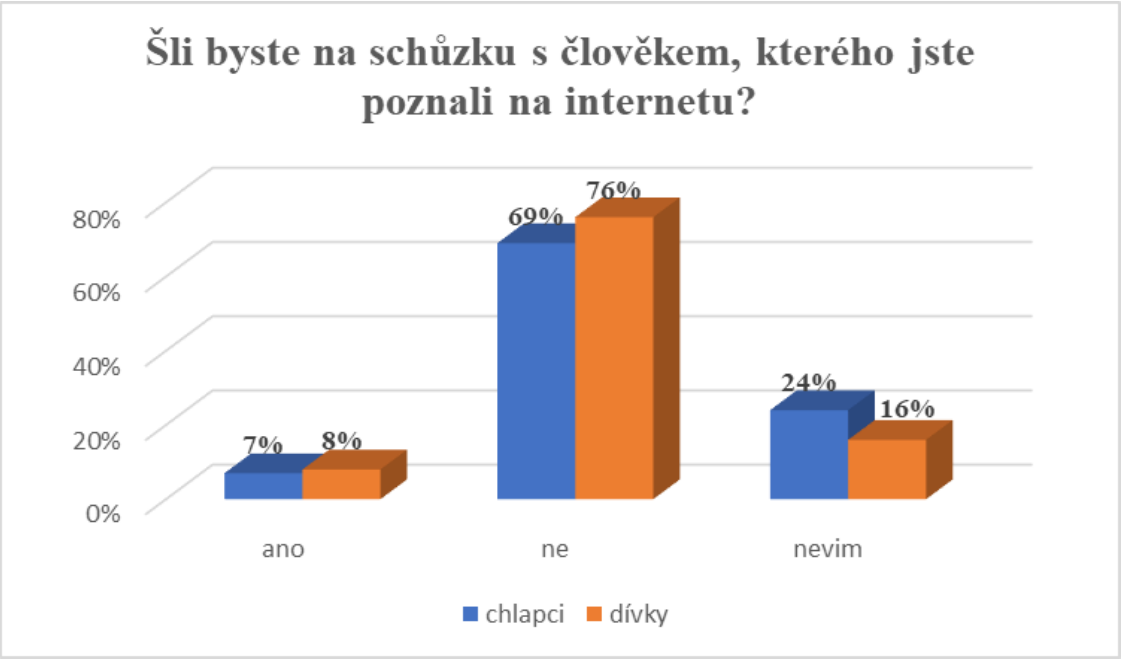
Odpovědi respondentů na dotaz **„jsi zaregistrovaný/á na nějaké sociální síti“**, kdy respondenti volili mezi odpovědí ano / ne, jsme hodnotili také s ohledem na to, jestli odpovídá chlapec nebo dívka. V případě odpovědi ano mohli respondenti konkretizovat odpověď vlastním textem. **Ano** odpověděli 44 chlapci, což odpovídá 80 % z celkového počtu chlapců a 49 dívek, což odpovídá 79 % z celkového počtu dívek. **Ne** odpovědělo 11 chlapců, což odpovídá 20 % z celkového počtu chlapců a 13 dívek, což odpovídá 21 % z celkového počtu dívek. V případě kladné odpovědi textem chlapci i dívky shodně nejčastěji doplnili, že **jsou registrováni na Facebook, Instagram, Youtube a Tik tok, a to z důvodu komunikace s kamarády, sledování vtipných videí a hraní her**. Z celkového počtu 117 respondentů jsou na sociálních sítích zaregistrovány 93 děti, což odpovídá 79,5 % z celkového počtu respondentů a bez registrace na sociálních sítích byly 24 děti, tedy 20,5 % z celkového počtu respondentů.

Graf č. 11: Internetový pojem Kybergrooming (Zdroj: Autor, 2022)



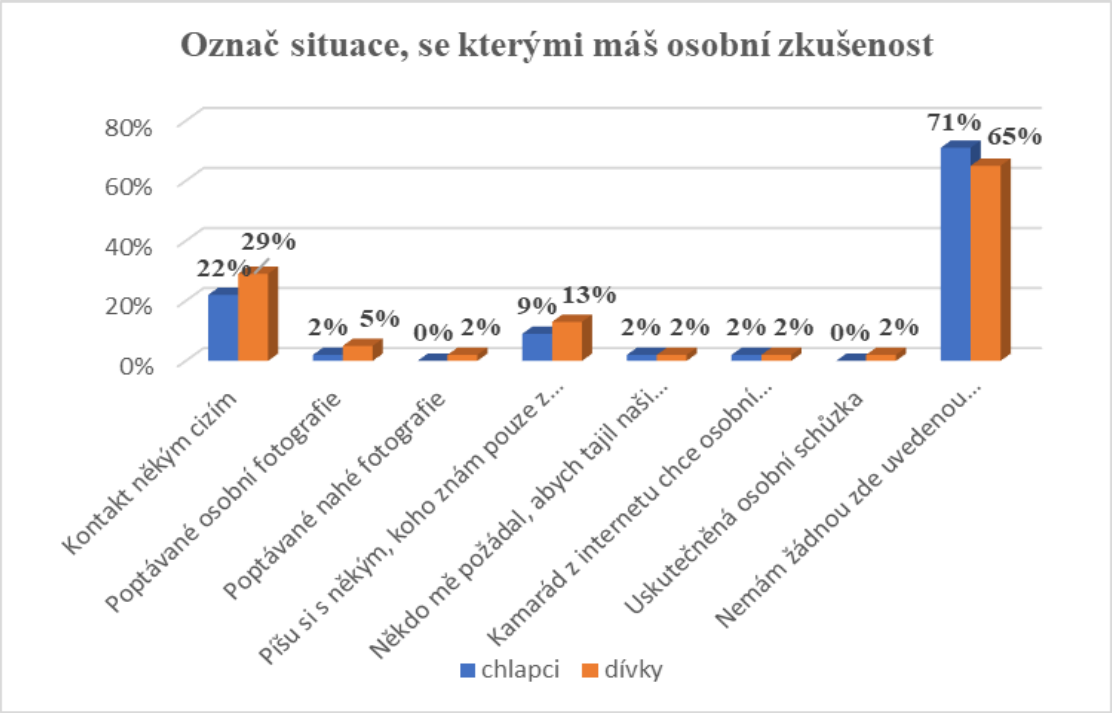
Odpovědi respondentů na dotaz **„co znamená Kybergrooming“**, kdy respondenti mohli volit jednu z pěti možností – hraní online her, virtuální místnost pro chatování, vylákání na osobní schůzku, rozesílání vtipných videí, nevím, co to znamená – jsme hodnotili také s ohledem na to, jestli odpovídá chlapec nebo dívka. **Hraní online her** – odpověděli 3 chlapci, což odpovídá 5 % z celkového počtu chlapců a 3 dívky, což odpovídá 5 % z celkového počtu dívek. **Virtuální místnost pro chatování** – odpověděli 2 chlapci, což odpovídá 4 % z celkového počtu chlapců a 7 dívek, což odpovídá 11 % z celkového počtu dívek. **Vylákání na osobní schůzku** – odpovědělo 10 chlapců, což odpovídá 18 % z celkového počtu chlapců a 13 dívek, což odpovídá 21 % z celkového počtu dívek. **Rozesílání vtipných videí** – neodpověděl ani jeden chlapec, ani jedna dívka, tedy 0 % z celku. **Nevím, co to znamená –** odpovědělo 40 chlapců, což odpovídá 73 % z celkového počtu chlapců a 39 dívek, což odpovídá 63 % z celkového počtu dívek. Výsledky jednoznačně ukazují na to, že většina respondentů, což je v tomto případě 94 dětí a zároveň 80,3 % z celku, nezná, nebo si špatně vykládá význam termínu Kybergrooming. Celkem 23 dětí, což je 19,7 % z celkového počtu 117 respondentů význam kybergroomingu chápe.

Graf č. 12: Osobní schůzka s člověkem, kterého jste poznali na internetu (zdroj: autor, 2022)



Odpovědi respondentů na dotaz **„šli byste na schůzku s člověkem, kterého jste poznali na internetu“**, kdy respondenti volili mezi odpovědí ano/ne/nevím, jsme hodnotili také s ohledem na to, jestli odpovídá chlapec nebo dívka. **Ano** – odpovědělo 38 chlapců, což odpovídá 69 % z celkového počtu chlapců a 47 dívek, což odpovídá 76 % z celkového počtu dívek. **Ne** – odpověděli 4 chlapci, což odpovídá 7 % z celkového počtu chlapců a 5 dívek, což odpovídá 8 % z celkového počtu dívek. Odpověď **Nevím** – zvolilo 13 chlapců, což odpovídá 24 % z celkového počtu chlapců a 10 dívek, což je 16 % z celkového počtu dívek. Většina chlapců i dívek, v tomto případě celkem 85 dětí, což odpovídá 72,6 % z celkového počtu respondentů, je přesvědčena, že by s člověkem, kterého poznali na internetu, na osobní schůzku nešla.

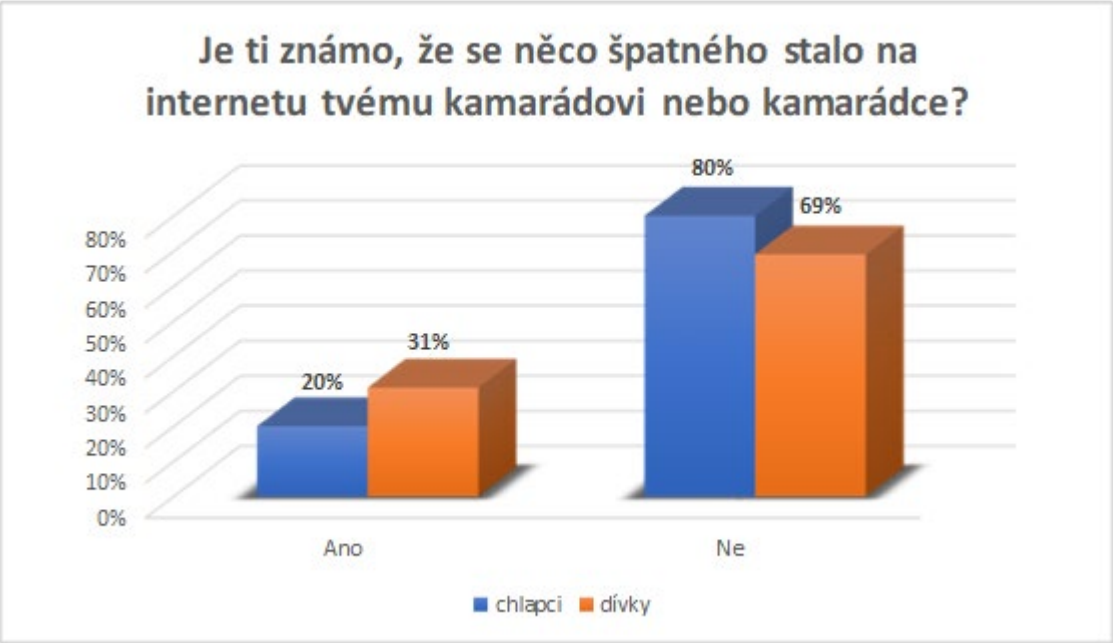
Graf č. 13: Nepříjemné osobní zkušenosti z internetového prostředí (Zdroj: Autor, 2022)



Odpovědi respondentů na dotaz **„označ situace, se kterými máš osobní zkušenost“**, kdy z osmi uvedených odpovědí mohli respondenti zaškrtnout i více možností, jsme hodnotili také s ohledem na to, jestli odpovídá chlapec nebo dívka. **Někdo cizí mě kontaktoval přes internet** – odpovědělo 12 chlapců, což odpovídá 22 % z celkového počtu chlapců a 18 dívek, což odpovídá 29 % z celkového počtu dívek. **Někdo po mně chtěl, abych mu poslal/a svoji fotografii** – odpověděl 1 chlapec, což odpovídá 2 % z celkového počtu chlapců a 3 dívky, což odpovídá 5 % z celkového počtu dívek. **Někdo po mně chtěl, abych mu poslal/a fotografii, na které jsem nahý/á** – žádný z chlapců tuto možnost nezvolil, dívka odpověď zvolila 1, což odpovídá 2 % z celkového počtu dívek. **Píšu si s někým, koho znám pouze z internetu** – odpovědělo 5 chlapců, což odpovídá 9 % z celkového počtu chlapců a 8 dívek, což odpovídá 13 % z celkového počtu dívek. **Někdo mě požádal, abych tajil naši společnou konverzaci** – odpověděl 1 chlapec, což odpovídá 2 % z celkového počtu chlapců a 1 dívka, což odpovídá 2 % z celkového počtu dívek. **Dostal/a jsem návrh na osobní schůzku od uživatele, kterého znám pouze z internetu** – odpověděl 1 chlapec, což odpovídá 2 % z celkového počtu chlapců a 1 dívka, což odpovídá 2 % z celkového počtu dívek. **Šel/šla jsem na osobní schůzku s uživatelem, se kterým jsem se seznámil/a na internetu** – žádný z chlapců tuto možnost nezvolil, dívka odpověď zvolila 1, což odpovídá 2 % z celkového počtu dívek. **Nemám žádnou zde uvedenou zkušenost** – odpovědělo 39

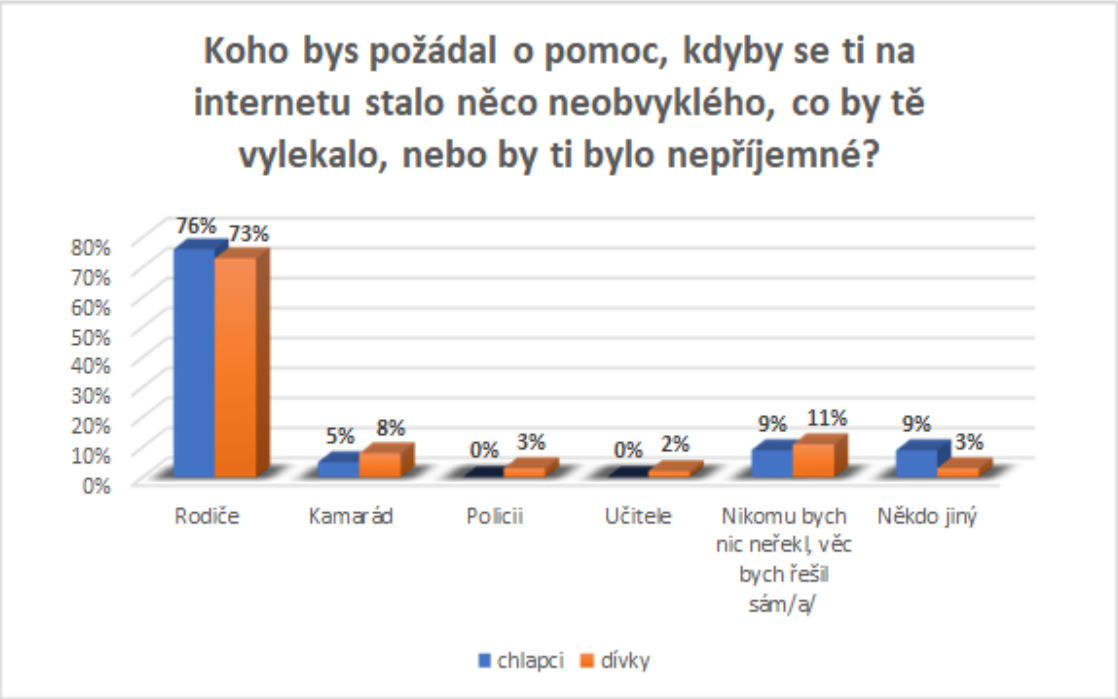
chlapců, což odpovídá 71 % z celkového počtu chlapců a 40 dívek, což odpovídá 65 % z celkového počtu dívek.

Graf č. 14: Špatné zkušenosti blízkých osob (Zdroj: Autor, 2022)



Odpovědi respondentů na dotaz **„je ti známo, že se něco špatného stalo na internetu tvému kamarádovi nebo kamarádce“**, kdy respondenti volili mezi odpovědí ano/ne, jsme hodnotili také s ohledem na to, jestli odpovídá chlapec nebo dívka. **Ano** – odpovědělo 11 chlapců, což odpovídá 20 % z celkového počtu chlapců a 19 dívek, což odpovídá 31 % z celkového počtu dívek. **Ne** – odpověděli 44 chlapci, což odpovídá 80 % z celkového počtu chlapců a 43 dívky, což odpovídá 69 % z celkového počtu dívek. Z celkového počtu 117 respondentů odpovědělo 87 dětí, což odpovídá 74,3 % z celku, že neví o tom, že by se nějakému jejich kamarádovi stalo něco špatného na internetu. Kamarádi 30 respondentů, což je 25,7 %, však nějakou špatnou zkušenost již měli.

Graf č. 15: Vyhledání pomoci (Zdroj: Autor, 2022)



Odpovědi respondentů na dotaz **„koho bys požádal o pomoc, kdyby se ti na internetu stalo něco neobvyklého, co by tě vylekalo nebo by ti bylo nepříjemné“**, kdy respondenti mohli volit jednu ze šesti možností – rodiče, kamaráda, policii, učitele, nikomu bych nic neřekl/a, věc bych řešil/a sám/a, někoho jiného (zde měli respondenti možnost doplnit vlastní text) – jsme hodnotili také s ohledem na to, jestli odpovídá chlapec nebo dívka. **Rodiče** – zvolili 42 chlapci, což odpovídá 76 % z celkového počtu chlapců a 45 dívek, což odpovídá 73 % z celkového počtu dívek. **Kamaráda –** by zvolili 3 chlapci, což odpovídá 5 % z celkového počtu chlapců a 5 dívek, což odpovídá 8 % z celkového počtu dívek. **Policii** – by nezvolil žádný chlapec, což odpovídá 0 % z celkového počtu chlapců a tuto možnost by si vybraly 2 dívky, což odpovídá 3 % z celkového počtu dívek. **Učitele** – by nezvolil žádný chlapec, což odpovídá 0 % z celkového počtu chlapců, ale učitele by oslovila 1 dívka, což odpovídá 2 % z celkového počtu dívek. **Nikomu bych nic neřekl/a, věc bych řešil/a sám/a,** tuto možnost by zvolilo 5 chlapců, což odpovídá 9 % z celkového počtu chlapců a 7 dívek, což odpovídá 11 % z celkového počtu dívek. **Někoho jiného** by o pomoc požádalo 5 chlapců, což odpovídá 9 % z celkového počtu chlapců a volili by mezi svými staršími sourozenci a v jednom případě by oslovili babičku a 2 dívky, což odpovídá 3 % z celkového počtu dívek. Také dívky by hledaly pomoc u svých sourozenců. Většina respondentů, v tomto případě celkem 87 dětí, což odpovídá 74,4 % z celku, by o pomoc požádala rodiče.

6.2 Interpretace výsledků průzkumu kvalitativní metodou

Rozhovor obsahoval sedm otázek. První otázka se vztahovala k délce praxe v oboru vzdělávání dětí v informačních technologiích, kdy cílem bylo vyhodnotit, je-li možné od respondenta získat odpovědi na všechny připravené dotazy. Dvě otázky měly přímý vztah k obsahu výukových osnov na základní škole, dvě otázky se vztahovaly k vývoji kyberkriminality, jeden dotaz byl směrován na informovanost dětí o možných centrech pomoci a jedním dotazem byla zjišťována osobní zkušenost pedagoga s případy, kdy jemu svěřené děti byly konfrontovány s predátory online prostředí.

Respondent pedagog – přepis anonymizovaného řízeného rozhovoru:

Dotaz č. 1: Jak dlouho působíte jako pedagogický pracovník na základní škole, se zaměřením na informační a komunikační technologie?

Odpověď č. 1: Na základní škole učím již 24 let a po celou dobu vyučuji informační a komunikační technologie. V posledních 5 letech dokonce také na prvním stupni.

Dotaz č. 2: Zaměřují se výukové osnovy na základní škole na rizika online prostředí, s akcentem na kybergrooming a sexting? Pokud ano, tak jak velký prostor je těmto tématům vymezen?

Odpověď č. 2: Bohužel je čas vymezený předmětu informační a komunikační technologie velmi omezený a každý učitel musí zvládnout naučit žáky uživatelsky potřebné dovednosti jako je např. práce s Excelem, Wordem a podobně. Co musíme žáky naučit je dáno školními osnovami a prevence nikde stanovena není. Je tedy na každém pedagogovi, jak k celé problematice přistupuje a do jaké míry, z časového hlediska, ji zvládne do svých vyučovacích hodin zahrnout. Je ale pravda, že se v letošním roce budou učební osnovy měnit a informačním a komunikačním technologiím by mělo být věnováno výrazně více času. Já osobně se snažím o hrozbách na internetu se svými žáky hovořit pravidelně, chápu prevenci jako důležitou součást výuky.

Dotaz č. 3: Jsou žáci v hodinách informační a komunikační technologie obeznámeni s tím, kam se mohou v případě osobní negativní zkušenosti z online prostředí obrátit o pomoc? Pokud ano, upřesněte, s jakým postupem a možnostmi jsou žáci obeznámeni.

Odpověď č. 3: Ano, žáci vědí, že škola je jim vždy s pomocí otevřena. Vědí, že se mohou obrátit na kteréhokoliv pedagoga, ve kterého mají důvěru. Samozřejmě jsme je seznámili s tím, že pokud jejich problém vyhodnotíme jako hrozbu, budeme muset celý

případ předat Policii ČR k prošetření. Rodiče na rodičovských schůzkách jsou informováni o možnosti obrátit se na školu s řešením případů i z domácího prostředí.

Dotaz č. 4: Sledujete vývoj závadového jednání v internetovém prostředí ve vztahu k mladistvým?

Odpověď č. 4: Aktivně vývoj kriminality online prostředí nesleduji, ale pokud někde v médiích nebo na sociálních sítích zaznamenám, že se někde něco takového stalo, snažím se zjistit co nejvíce faktů, abychom s případem své žáky mohli seznámit.

Dotaz č. 5: Dokážete na základě Vaší zkušenosti vyhodnotit podíl a vývoj kybernetických rizik, kde hlavní roli sehrává internetový predátor?

Odpověď č. 5: Rizika jsou obrovská a já mám pocit, že minulé dva roky, v době kovidové, měli internetoví predátoři skutečně velké příležitosti si své oběti najít. A bohužel opětovným přechodem na distanční výuku těch příležitostí neubylo. Děti se s životem v online prostředí natolik sžily, že to vysoké riziko stále přetrvává.

Dotaz č. 6: Máte osobní zkušenosti jako pedagogický pracovník s řešením situace, kdy se některý z vašich žáků stal obětí kybergroomera?

Odpověď č. 6: Ano, zkušeností mám hned několik, a to jak z působení na střední, tak i na základní škole. Zrovna nedávno, na začátku roku, se na mě obrátili rodiče jedné mé žákyně šesté třídy, že při kontrole domácího pc zjistili, že již došlo mezi jejich dcerou a neznámou osobou na druhé straně k výměně nějakých fotografií, dokonce jí byly doručeny i nějaké fotografie nahé. Na základě domluvy s rodiči byla k případu přivolána Policie ČR a ta si celý případ převzala.

Dotaz č. 7: Myslíte si, že jsou stávající výukové osnovy z oblasti informačních a komunikačních technologií na základních školách dostačující pro zajištění osobní bezpečnosti žáků před internetovými predátory?

Odpověď č. 7: Dostačující určitě nejsou, bylo by vhodné zařadit nějakou formu pravidelné intervence dětského psychologa, který je školen na komunikaci s dětmi a umí si lépe poradit s naivitou, důvěřivostí a snadnou manipulovatelností dětí. Domnívám se, že pravidelnou intervencí je možné dosáhnout toho, že dítě nebude dávat úplně cizímu člověku svoji domácí adresu nebo číslo účtu, ale v silách běžného pedagoga není zvládnout vysvětlit, jak pozná „dobro“ a „zlo“…no. Občas s tím má problém i dospělý člověk.

6.2.1 Shrnutí a výsledek rozhovoru

Na základě rozhovoru s respondentem ze školského prostředí je možné chápat rizika online prostředí pro žáky základních škol jako nezanedbatelná, hodná pozornosti. Sám pedagog vnímá, že kybernetičtí predátoři jsou skutečnou hrozbou, neboť čas, po který se děti v internetovém prostředí pohybují, je stále delší a osvěta, vztahující se ke kyberkriminalitě a závadovému jednání, je ve školním prostředí nedostatečně ošetřena.

ZÁVĚR

Průzkumné šetření bylo zaměřeno na žáky šestých tříd základních škol v Mariánských Lázních, kdy cílem bylo zjistit, do jaké míry jsou žáci znalí rizik virtuálního prostředí. Průzkumný vzorek čítal 117 respondentů, z nichž chlapci, s počtem 55, tvořili 47% podíl a dívky, v počtu 62, pak tvořily 53 % z celku.

Zcela shodných výsledků bylo dosaženo u dotazu, jestli rodiče hovoří se svými dětmi o tom, jak se chovat na internetu. Chlapců i dívek odpovědělo 89 % – že ano, že s nimi o chování na internetu rodiče hovoří. Přibližné shody bylo dosaženo při porovnání odpovědí chlapců a dívek také u dotazu, jestli se rodiče zajímají o to, co respondenti dělají na internetu. Většina chlapců (71 %) a většina dívek (79 %) odpověděla kladně. Podobného výsledku bylo dosaženo u dotazu, jestli se svými dětmi hovoří o rizicích na internetu. Také zde většina chlapců (75 %) a většina dívek (84 %) zvolila kladnou odpověď. V případě kladné odpovědi zde respondenti uvedli, před čím je rodiče varovali. Děti shodně odpovídaly „před úchyly, cizími lidmi, podvodníky, pedofily“. Zde je ovšem třeba si uvědomit, že dítě vůbec nemusí po celou dobu kontaktu poznat, že se o případného predátora jedná. Těmito výsledky bylo dosaženo naplnění **1. průzkumného cíle, kterým bylo určit, do jaké míry jsou děti obeznámeny s riziky virtuálního světa z domácího prostředí, od rodičů**.

Také v rámci školy je míra informovanosti dětí v oblasti rizik virtuálního světa naplněna. 91 % chlapců a 97 % dívek odpovědělo, že se o problematice ve škole učili. Ovšem dle školní výuky zvládne rozeznat pravdivé od nepravdivých informací pouze 60 % chlapců a 56 % dívek a ochránit si své soukromí zvládne 53 % chlapců a 63 % dívek. Ostatní děti odpověděly, že se daného tématu školní výuka netýkala. Vyhodnocením odpovědí na uvedené dotazníkové otázky bylo dosaženo **2. průzkumného cíle, kterým bylo zjistit, v jakém rozsahu s orientací v rizicích kyberprostoru pomohlo prostředí školy a školní vzdělávací aktivity.**

Bylo zjištěno, že obě skupiny, jak chlapci (49 %), tak i dívky (37 %) se věnují činnostem na internetu přibližně stejný počet hodin. Nejčastěji se jedná o čtyři hodiny a více. Zároveň bylo dosaženo zjištění, že 80 % chlapců a 79 % dívek je aktivních na sociálních sítích. Vzhledem k tomu, kolik času tráví respondenti aktivně v online prostředí, bylo překvapivé zjistit, jak málo rozumí terminologii a činnostem, které mají spojitost s riziky virtuálního světa. 76 % chlapců a 73 % dívek nerozumí termínu

Kybergrooming. Důležitým zjištěním bylo, že většina respondentů, 71 % chlapců a 65 % dívek, zkušenost s kyberkriminalitou v roli oběti nemá. Ovšem zde je vhodné vzít v úvahu fakt, že ne vždy je dítě schopno okamžitě rozpoznat, že to, co se mu děje, není v pořádku a může se obětí predátora kyberprostoru stát. Tyto výsledky naplnily dosažení **3. průzkumného cíle, kterým bylo zmapovat, v jakém rozsahu se žáci základních škol orientují v oblasti kyberkriminality.**

Odpovědi respondentů byly vyhodnocovány vždy s ohledem na to, jedná-li se o chlapce nebo dívku. Výsledky ukazují jen nepatrné rozdíly v postoji chlapců a dívek, a to převážně v dotazech zaměřených na zájmové činnosti. Na první rozdíl při porovnávání výsledků obou skupin jsme narazili u dotazu, jakým činnostem se respondenti na internetu věnují nejvíce. Zatímco chlapci se ze 78 % věnují hraní her, dívky hrají hry pouze z 29 % a naopak dívky nejvíce, z 56 % poslouchají hudbu, zatímco chlapci se o hudbu zajímají jen z 33 %. Je možné se domnívat, že právě znalost rozdílů v zájmech dívek a chlapců usnadňuje predátorům v kyberprostoru navazování nových kontaktů a manipulaci oběti.

Rozhovorem s pedagogickým pracovníkem bylo možné získat na celou problematiku kybernetických hrozeb ještě jeden pohled. Dle respondenta je kriminalitu v online prostředí možné vnímat jako problém se stále rostoucím charakterem, ovšem školní osnovy na tento vývoj nereflektují, nebo jen velmi vlažně. Respondent chápe důležitost prevence, snaží se ji ve svých hodinách aplikovat, ale cítí, že to není pro děti dostačující. Z rozhovoru bylo ale zároveň možné vyčíst, že ani pedagog nemá všechny informace o možnostech, kam se oběť útoku může obrátit. Veškerá nabízená pomoc je tak směrována do školského zařízení a informace, že potvrzený útok bude dále vyšetřovat Policie ČR, může oběť dětského věku natolik vystrašit, že raději nikomu nic neřekne.

Na základě výsledků uskutečněného průzkumného šetření bylo možné vyvodit některá **doporučení pro praxi, pro školská zařízení v Mariánských Lázních:**

- Umožnit externím specialistům z oboru prevence kyberkriminality pravidelné přednášky na základních školách v rámci výuky.
- Navázat spolupráci s dětskými psychology, kteří by byli ochotni a schopni proaktivně, v pravidelných konzultacích, s dětmi o kybernetických predátorech hovořit.
- Pro pedagogické pracovníky a rodiče organizovat vzdělávací semináře, zaměřené na internetové hrozby a zároveň zvýšení povědomí o možné pomoci

díky různým organizacím, jako je E-bezpečí, Buď safe online, Nebojte se internetu, Internetem bezpečně, Linka bezpečí.

- Pro lepší pochopení terminologie zatraktivnit výuku informačních a komunikačních technologií pouštěním filmů s danou problematikou.
- Proaktivně vyhledávat akce zaměřené na kyberkriminalitu s ohledem na věk dítěte.
- Umožnit aktivní zapojení rodičů v dané problematice.
- Využívat vzdělávací programy a metodiky Národního úřadu pro kybernetickou a informační bezpečnost.

Doporučení pro praxi budou v nejbližším možném termínu komunikována s řediteli základních škol v Mariánských Lázních, na kterých bylo průzkumné šetření uskutečněno.

SEZNAM POUŽITÝCH ZDROJŮ

Literární zdroje

1. BĚLÍK, V. a kol. 2017. *Slovník sociální patologie.* 1. vydání. Praha: Grada Publishing, a.s. 2017. 120 s. ISBN 978-80-271-0599-1.
2. BLÁHA, J. a kol. 2016. *Řízení lidských zdrojů, nové trendy*. 1. vydání. Praha: Albatros Media a.s. 2016. 240 s. ISBN 978-80-726-1434-9
3. BLINKA, L. a kol. 2015. *Online závislosti.* 1. vydání. Praha: Grada Publishing, a.s. 2015. 200 s. ISBN 978-80-247-5311-9.
4. ČERNÁ, A. a kol. 2013. *Kyberšikana, průvodce novým fenoménem*. 1. vydání. Praha: Grada Publishing, a.s. 2013. 152 s. ISBN 978-80-247-4577-0.
5. DOČEKAL, D. a kol. 2019. *Dítě v síti.* 1. vydání: Mladá fronta. 2019. 208 s. ISBN 978-80-204-5145-3.
6. DOSTÁL, J. 2011. *Internet druhé generace pro učitele*. 1. vydání. Olomouc: Univerzita Palackého v Olomouci. 2011. 70 s. ISBN 978-80-244-2779-9.
7. FIELDINGOVÁ, O. 2018. *Digitální detox*. 1. vydání. Praha: Albatros Media a.s. 2018. 120 s. ISBN 978-80-264-1980-8.
8. FIALOVÁ, L. a kol. 2015. *Vzdělávací oblast Člověk a zdraví v současné škole.* 1. vydání. Praha: Univerzita Karlova v Praze, Nakladatelství Karolinum. 2015. 197 s. ISBN 978-80-246-2885-1.
9. HLEDÁNÍ FLOW. 2008. *Hledání flow.* 1. vydání. Brno: Tribun EU. 2008. 152 s. ISBN 978-80-7399-623-9.
10. JIROVSKÝ, V. 2007. *Kybernetická kriminalita*. 1. vydání. Praha: Grada Publishing, a.s. 2007. 284 s. ISBN 978-80-247-1561-2.
11. KOHOUT, R. 2017. *Internetem bezpečně: Jak se nestát obětí virtuálního predátora.* Karlovy Vary: You conneected. 2017. 68 s. ISBN 978-80-270-2897-9.
12. KOHOUT, R. – ŠTOCHL, J. 2018. *Kybernetická kriminalita, příručka pro policisty*. První vydání. Karlovy Vary: You connected. 2018. 146 s.
13. KOŽÍŠEK, M. – PÍSECKÝ, V. 2016. *Bezpečně na internetu, průvodce chováním ve světě online.* 1. vydání. Praha: Grada Publishing, a.s. 2016. 176 s. ISBN 978-80-247-5595-3.
14. LOSEKOOT, M. a kol. 2019. *Jak na sítě: Ovládněte čtyři principy úspěchu na sociálních sítích*. 1. vydání. Brno: Jan Melvil Publishing. 2019. 328 s. ISBN 978-80-7555-085-9.

15. PROCHÁZKA, D. 2010. *První kroky s internetem.* 3. aktualizované vydání. Praha: Grada Publishing, a.s. 2010. 112 s. ISBN 978-80-247-3255-8.
16. SAK, P. 2018. *Úvod do teorie bezpečnosti: nekonvenční pohledy na minulost, přítomnost a budoucnost lidstva*. 1. vydání: Petrklíč. 2018. 271 s. ISBN 978-80-7229-652-1.
17. ŠEVČÍKOVÁ, A. a kol. 2014. *Děti a dospívající online, vybraná rizika používání internetu*. 1. vydání. Praha: Grada Publishing, a.s. 2014. 184 s. ISBN 978-80-247-5010-1.

Elektronické zdroje

1. E–bezpečí. 2021. [online]. *Sexting a právo*. [citováno 2021-11-28]. Dostupné na internetu: <https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/sexting/1681-sexting-a-pravo>.
2. HAMBERGER, T. Prevence kriminality 2021. [online]. Kybergrooming. [citováno 2021-11-10]. Dostupné na internetu: <https://prevencekriminality.cz/kybergrooming/>.
3. ChildSafeNet. 2022. [online]. Cyber Grooming. [citováno 2022-02-12]. Dostupné na internetu: <https://www.childsafenet.org/new-page-15>.
4. Internetem bezpečně. 2021. [online]. Digitální stopa. [citováno 2021-10-22]. Dostupné na internetu: <https://www.internetembezpecne.cz/internetem-bezpecne/dobre-vedet/digitalni-stopa/>.
5. Internetem bezpečně. 2021. [online]. *Kyberstalking*. [citováno 2021-11-01]. Dostupné na internetu: <https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kyberstalking/>.
6. Internetem bezpečně. 2021 [online]. *Kyberšikana.* [citováno 2021-12-12]. Dostupné na internetu: <https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/>.
7. KOPECKÝ, K. 2021. [online]. Kybergrooming. [citováno 2021-12-12]. Dostupné na internetu: <http://www.kybergrooming.cz/#kybergrooming>.
8. KOPECKÝ, K. 2017. [online]. E-bezpečí. [citováno 2021-12-22]. Dostupné na internetu: <https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/kybergrooming/1222-minecraft-kybergrooming>.

9. MÁČELOVÁ, K. 2021. [online]. Učení v pohodě. [citováno 2021-12-12]. Dostupné na internetu: <https://www.uceni-v-pohode.cz/faze-kybergroomingu-podezrele-chovani-virtualnich-pratel/>.
10. MŠMT [online]. [citováno 2021-12-04]. Dostupné na internetu: <https://www.msmt.cz/file/56005/>.
11. NEBUĎ OBĚŤ! Rizika internetu a komunikačních technologií, z. s. [online]. [citováno 2021-12-04]. Dostupné na internetu: <http://www.nebudobet.cz/?cat=kybergrooming>.
12. O2 chytrá škola. 2021. [online]. [citováno 2021-11-22]. Dostupné na internetu: <https://www.o2chytraskola.cz/data/files/sexting-dfjl8pi7x6.pdf>.
13. Policie České republiky. Kyberkriminalita. [online]. [citováno 2022-02-25]. Dostupné na internetu: <https://www.policie.cz/clanek/kyberkriminalita.aspx>.
14. Policie české republiky. [online]. [citováno 2021-11-30]. Dostupné na internetu: <https://www.policie.cz/clanek/uzemni-odbor-praha-venkov-zapad-zpravodajstvi-nebezpeci-na-internetu.aspx>.
15. RECMANOVÁ, A. 2017. [online]. Pravidla netikety. [citováno 2021-10-10]. Dostupné na internetu: <https://medium.com/edtech-kisk/pravidla-netikety-ea92f7c3e58b>.
16. Záchranný kruh. [online]. *Kybergrooming*. [citováno 2021-11-12]. Dostupné na internetu: <https://www.zachranny-kruh.cz/osobni-bezpeci/dalsi-nebezpeci/kybergrooming/kybergrooming.html>.
17. Základní škola Jih Mariánské Lázně. [online]. Dokumenty školy. [citováno 2021-11-28]. Dostupné na internetu: <https://skolajih.cz/?sekce=skola&stranka=dokumenty_skoly>.
18. Základní škola Úšovice. [online]. Dokumenty ke stažení. [citováno 2021-11-28]. Dostupné na internetu: <https://www.zsusovice.cz/index.php/domu/ke-stazeni>.
19. VRS. 2020. Co je virtuální realita? [online]. [citováno 2021-12-17]. Dostupné na internetu: <https://www.vrs.org.uk/virtual-reality/what-is-virtual-reality.html>.

Legislativní dokumenty

1. Zákon číslo 40/2009 Sb. Trestní zákoník.
2. Zákon číslo 561/2004 Sb. o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon).

SEZNAM TABULEK A GRAFŮ

Tabulky:

Grafy:

PŘÍLOHY

Příloha 1 – dotazník

Strana 1 - První strana

Vážení studenti,
tímto se na Vás obracíme s žádostí o vyplnění dotazníku, který je **anonymní** se zaměřením na problematiku internetového prostředí. Data z dotazníku přispějí k poznání zkoumané problematiky, a proto Vás žádám o úplné a pravdivé informace.

Dotazník bude použit pro bakalářskou práci "Rizika virtuálního světa u žáků základních škol v Mariánských Lázních"

1. Jsi chlapec nebo dívka?

Poznámka: Vyberte jednu odpověď

( ) Chalpec

( ) Dívka

2. Kolik času denně trávíš na internetu?

Poznámka: Vyberte jednu odpověď

( ) Maximálně 1 hodinu

( ) 2 hodiny

( ) 3 hodin

( ) 4 a více hodin

( ) Mám přistup na internet pouze ve škole

3. Jakým činnostem se na internetu věnuješ nejvíce?

Poznámka: Vyberte jednu nebo více odpovědí. U možnosti "Jiné" můžete doplnit textem které

( ) Hraní her

( ) Chodím na sociální sítě

( ) Využívám internet ke studiu

( ) Poslouchání hudby

( ) Sledování filmů a seriálů

( ) Prohlížení stránek pro zábavu

( ) Jiné

4. **Hovořili s tebou rodiče o tom, jak se chovat na internetu?**

Poznámka: Vyberte jednu odpověď

( ) Ano

( ) Ne

5. **Zajímají se rodiče o to, co děláš na internetu?**

Poznámka: Vyberte jednu odpověď

( ) Ano

( ) Ne

6. **Hovořili s tebou rodiče o tom, že by ti na internetu mohlo hrozit nějaké nebezpečí?**

Poznámka: Vyberte jednu odpověď

( ) Ano

( ) Ne

Na co tě nejvíce upozorňovali - napiš textem:

.....

7. **Učili jste se ve škole o nebezpečích, která hrozí nebo mohou hrozit na internetu?**

Poznámka: Vyberte jednu odpověď

( ) Ano

( ) Ne

8. **Učili jste se ve škole, jak rozlišovat pravdivé a nepravdivé informace uvedené na internetu?**

Poznámka: Vyberte jednu odpověď

( ) Ano

( ) Ne

9. **Učili jste se ve škole, jak si chránit svou identitu a soukromí na internetu?**

Poznámka: Vyberte jednu odpověď

( ) Ano

( ) Ne

10.Jsi zaregistrovaný/á na nějaké sociální síti?

( ) Ano

( ) Ne

Napiš, na které sociální síti jsi zaregistrovaný:

.....

11.Víš co znamená kybergrooming?

Poznámka: Vyberte jednu odpověď

( ) Hraní online her

( ) Virtuální místnost pro chatování

( ) Vylákání na osobní schůzku

( ) Rozesílání vtipných videí

( ) Nevím, co to znamená

12.Šli byste na schůzku s člověkem, kterého jste poznali na internetu?

Poznámka: Vyberte jednu odpověď

( ) Ano

( ) Ne

( ) Nevím

13.Označ situace, se kterými máš osobní zkušenost:

Poznámka: Vyberte jednu nebo více odpovědí

( ) Někdo cizí mě kontaktoval přes Internet

( ) Někdo po mně chtěl, abych mu poslal/a svoji fotografii

( ) Někdo po mně chtěl, abych mu poslal/a fotografii, na které jsem nahý/á

( ) Píšu si s někým, koho znám pouze z internetu

( ) Někdo mě požádal, abych tajil naši společnou konverzaci

( ) Dostal/a jsem návrh na osobní schůzku od uživatele, kterého znám pouze z internetu

( ) Šel/šla jsem na osobní schůzku s uživatelem, se kterým jsem se seznámil/a na internetu

( ) Nemám žádnou zde uvedenou zkušenost

14. Je ti známo, že se něco špatného stalo na internetu tvému kamarádovi nebo kamarádce?

Poznámka: Vyberte jednu odpověď

( ) Ano

( ) Ne

15. Koho bys požádal o pomoc, kdyby se ti na internetu stalo něco neobvyklého, co by tě vylekalo, nebo by ti bylo nepříjemné?

Poznámka: Vyberte jednu odpověď

( ) Rodiče

( ) Kamaráda/ kamarádku

( ) Policii

( ) Učitele

( ) Nikomu bych nic neřekl/a - vyřešil/a bych situaci sám/sama

( ) Někdo jiný

Strana 2 - Poděkování a rozloučení

Děkujeme Vám za Vaše názory a čas, který jste věnovali vyplnění tohoto dotazníku.
