

Univerzita Karlova

Filozofická fakulta

Ústav informačních studií a knihovnictví

Informační studia a knihovnictví

Diplomová práce

Bc. Helena Filipová

Informační chování žáků 8. a 9. tříd ve vztahu k ochraně vlastního soukromí na sociálních sítích

Information Behavior of the 8th and 9th Grade Pupils in Relation
to the Protection of Their Own Privacy on Social Networks

Praha 2020

Vedoucí práce: PhDr. Helena Lipková, Ph.D.

Na tomto místě bych velice ráda poděkovala zejména své vedoucí diplomové práce PhDr. Heleně Lipkové, Ph.D. za odborné vedení a cenné rady, které mi při zpracovávání a dokončení této diplomové práce velmi pomohly.

Dále bych ráda poděkovala žákům ze Základní školy a Mateřské školy Tábor, Husova 1570, za čas, který věnovali vyplnění dotazníku pro výzkumnou část této práce. Díky patří samozřejmě také vyučujícím, kteří svým žákům dotazník distribuovali.

V neposlední řadě děkuji také své rodině, příteli a přátelům bez jejichž podpory by bylo mnohem náročnější práci dokončit. Díky patří také mým kolegyním, z knihovny, které mě nejen podporovaly, ale často mi i poskytovaly velice užitečné rady.

Prohlášení:

Prohlašuji, že jsem diplomovou práci vypracovala samostatně, že jsem řádně citovala všechny použité prameny a literaturu a že práce nebyla využita v rámci jiného vysokoškolského studia či k získání jiného nebo stejného titulu.

V Praze dne 18. 12. 2020

.....

Helena Filipová

Identifikační záznam: FILIPOVÁ, Helena. *Informační chování žáků 8. a 9. tříd ve vztahu k ochraně vlastního soukromí na sociálních sítích*. Praha, 2020. Diplomová práce. Univerzita Karlova, Filozofická fakulta, Ústav informačních studií a knihovnictví. Vedoucí diplomové práce PhDr. Helena Lipková Ph.D.

Abstrakt

Tato diplomová práce se zabývá informačním chováním žáků 8. a 9. tříd základních škol ve vztahu k ochraně jejich vlastního soukromí na sociálních sítích Facebook a Instagram. Cílem práce je zjistit:

- jak se žáci zajímají o problematiku ochrany svého soukromí na těchto sítích a odkud čerpají tyto informace (rodiče, škola),
- zda jsou si vědomi asociovaných rizik a jak je ve svém chování zohledňují,
- jestli znají nástroje, které jsou jim na těchto sítích k dispozici,
- jak výše uvedené ovlivňuje jejich vystupování na vybraných sociálních sítích z pohledu obsahu a formy sdílených informací.

Teoretická část práce se zabývá především charakteristikou vybraných sociálních sítí Facebook a Instagram z hlediska možností ochrany soukromí vůči možným hrozbám. Praktická část prezentuje výsledky kvantitativního výzkumu, který byl realizován formou dotazníku mezi žáky 8. a 9. tříd základních škol.

Klíčová slova

Dospívající, teenageři, sociální sítě, sociální média, soukromí, ochrana soukromí, Facebook, Instagram

Abstract

This diploma thesis deals with the information behavior of the pupils in the 8th and 9th grades of primary schools in relation to the protection of their own privacy on the social networks Facebook and Instagram. The aim of the work is to find out:

- how pupils are interested in the issue of protecting their privacy on these networks and where they get this information from (parents, school),
- if they are aware of the associated risks and how they take them into account in their behavior,
- whether they know the tools available to them on these networks,
- how the above affects their manners on selected social networks in terms of content and form of shared information.

The theoretical part of the thesis deals mainly with the characteristics of selected social networks Facebook and Instagram in terms of privacy protection against possible threats. The practical part presents the results of quantitative research, which was carried out in the form of a questionnaire among 8th and 9th grade elementary school students.

Key words

Teenagers, social network, social media, privacy, privacy protection, Facebook, Instagram

Obsah

Předmluva.....	8
1 Úvod.....	9
2 Sociální sítě.....	10
2.1 Začátky sociálních sítí.....	12
2.2 Facebook.....	12
2.3 Instagram.....	13
3 Ochrana soukromí na sociálních sítích.....	14
3.1 Soukromí.....	14
3.1.1 Soukromí v online době.....	15
3.1.2 Soukromí na sociálních sítích.....	16
3.2 Ochrana soukromí na Facebooku.....	17
3.2.1 Smluvní podmínky Facebooku ve vztahu k soukromí uživatelů.....	18
3.2.2 Zásady komunity Facebook.....	20
3.2.3 Zásady používání dat na Facebooku.....	21
3.2.4 Možnosti nastavení profilu na Facebooku týkající se soukromí.....	23
3.3 Ochrana soukromí na Instagramu.....	25
3.3.1 Podmínky použití Instagramu ve vztahu k soukromí uživatelů.....	25
3.3.2 Zásady komunity Instagram.....	27
3.3.3 Zásady používání dat na Instagramu.....	27
3.3.4 Možnosti nastavení profilu na Instagramu týkající se soukromí.....	28
4 Teenageři ve světě sociálních médií.....	30
4.1 Související statistiky.....	33
4.2 Specifika chování teenagerů (nejen na sociálních sítích).....	36
4.3 Dopady používání sociálních sítí.....	39
4.3.1 Přínosy sociálních sítí.....	39

4.3.2	Asociovaná rizika a možné hrozby na sociálních sítích.....	40
4.4	Zdroje a programy.....	45
4.5	Stávající stav výzkumu o chování teenagerů na sociálních sítích ve vztahu k ochraně soukromí	46
5	Informační chování žáků 8. a 9. tříd ve vztahu k ochraně vlastního soukromí na sociálních sítích	52
5.1	Cíle výzkumu, hypotézy.....	52
5.2	Dotazník (kvantitativní výzkum)	52
5.3	Účastníci výzkumu.....	53
5.4	Postup výzkumu.....	53
5.5	Výsledky dotazníkového šetření	54
5.5.1	Odpovědi na otázky týkající se sociálních sítí všeobecně	54
5.5.2	Odpovědi na otázky týkající se Instagramu	58
5.5.3	Odpovědi týkající se Facebooku	61
5.5.4	Odpovědi týkající se digitální stopy a rizik sociálních sítí	67
5.6	Interpretace výsledků výzkumu	72
6	Závěr	76
	Seznam použité literatury a zdrojů.....	79
	Seznam tabulek	85
	Seznam grafů.....	86
	Přílohy	i
	Seznam příloh.....	i
	Příloha 1 – Dotazník.....	ii
	Příloha 2 – E-mail rodičům	xviii

Předmluva

Předkládaná diplomová práce si klade za cíl popsat informační chování teenagerů ve věku žáků 8. a 9. tříd, a to především ve vztahu k ochraně vlastního soukromí na sociálních sítích. Toto téma bylo zvoleno zejména z důvodu jeho aktuálnosti, jelikož sociální sítě většinu z nás provází téměř každodenně a obzvláště pro teenagery musí být občas náročné se v tomto světě orientovat natolik, aby svým chováním na sítích například omylem neohrozili hlavně sami sebe. Diplomová práce je dále zaměřena zejména na dvě sociální sítě, Facebook a Instagram, protože Facebook je v současnosti nejrozšířenější sociální síť obecně a Instagram patří k nejoblíbenějším sociálním sítím právě v cílové skupině teenagerů ve věku žáků 8. a 9. tříd základních škol.

Hlavním cílem této práce bylo zjistit, jak vlastně žáci 8. a 9. tříd vnímají problematiku vlastního soukromí, odkud čerpají potřebné informace a zda jsou si plně vědomi, že jim na sociálních sítích hrozí i řada různých rizik. Tyto informace byly zjišťovány prostřednictvím kvantitativního výzkumu – dotazníku, který byl zaslán na Základní školu a Mateřskou školu Tábor, Husova 1570.

Vzhledem ke komplikované současné situaci, kdy se nejenom Česká republika potýká s epidemií koronaviru a s tím souvisejícím nouzovým stavem, kdy byly téměř celý podzim všechny školy zavřené a výuka probíhala pouze distančně, byl bohužel dotazník respondentům zaslán prostřednictvím vyučujícího pouze e-mailem, což pravděpodobně vedlo k tomu, že poměrně velká část žáků svou odpověď neodeslala. Přestože má tedy v současné době vybraná základní škola pro pilotní výzkum k dispozici cca 170 žáků v 8. a 9. třídách, dotazník vyplnilo pouze 111 z nich. Je pravděpodobné, že kdyby jim dotazník mohl vyučující zadat přímo ve výuce, obdrželi bychom více odpovědí. Vyplněné dotazníky nicméně i tak pomohly k získání odpovědí na otázky týkající se ochrany soukromí na sociálních sítích.

Veškeré informace jsou platné k datu 18. 12. 2020.

Tato práce čítá od předmluvy po závěr 22 878 slov, tj. přibližně 90,5 normostran.

1 Úvod

Sociální sítě jsou tu s námi již několik let a jsou mezi lidmi stále rozšířenější, jelikož postupně nahrazují většinu dřívějších způsobů komunikace – umožňují nám nejenom sdílet fotky, videa a své myšlenky, ale také chatovat s ostatními, a na některých sociálních sítích jsou k dispozici dokonce i hlasové a video hovory. Spolu se stále se rozvíjejícími technologiemi, v čele s chytrými telefony s připojením na internet, sociální sítě začínají v mnohých případech nahrazovat dříve běžná telekomunikační spojení.

Zároveň s tím, že jsou sociální sítě stále rozšířenější mezi lidmi, kteří na nich často sdílejí i mnohé informace ze svého soukromého života, je potřeba řešit i otázku bezpečnosti a ochrany sebe a svých dat. Vždy je důležité myslet na to, co o sobě na sociální sítě píšeme, kdo se k těmto informacím může dostat a jak je může zneužít. A o těchto problémech je potřeba nejenom vědět, ale také o nich mluvit, zejména s osobami, které jsou v tomto prostředí noví a nezkušení, tj. děti, teenageři nebo například senioři.

Tato diplomová práce se zaměřuje právě na tuto problematiku, a to ve vztahu k teenagerům ve věku žáků 8. a 9. tříd. Rozdělena je do čtyř hlavních kapitol, které se postupně snaží obsáhnout zkoumanou problematiku.

Tématem kapitoly 2 jsou sociální sítě obecně, snaží se je definovat a krátce popsat jejich začátky. Zároveň je zde uvedena základní charakteristika vybraných sociálních sítí – Facebooku a Instagramu.

Kapitola 3 se zabývá ochranou soukromí na sociálních sítích. Definuje soukromí, soukromí v online době a soukromí na sociálních sítích. Zároveň zde detailně popisuje ochranu soukromí na Facebooku a Instagramu v souvislosti s jejich smluvními podmínkami a možnostmi nastavení uživatelských profilů na těchto sociálních sítích.

Předmětem kapitoly 4 jsou teenageři ve světě sociálních médií. Kapitola se zabývá jejich specifickým chováním na sociálních sítích, popisuje některé vybrané statistiky, jež se vztahují k této problematice, a v neposlední řadě se v tomto směru věnuje rizikům, která teenagerům mohou hrozit. V souvislosti s tím jsou zde uvedeny vybrané zdroje a programy, ze kterých mohou teenageři čerpat informace ohledně bezpečnosti na internetu a sociálních sítích. V závěru kapitoly je popsán současný stav výzkumu v této oblasti.

Kapitola 5 obsahuje praktickou část této diplomové práce, je zde tedy popsán prováděný výzkum, který byl uskutečněn ve formě dotazníku, mezi žáky 8. a 9. tříd, jeho výsledky a vyhodnocení.

Práce je vhodná zejména pro zorientování se v tématu ochrany soukromí teenagerů na sociálních sítích a podání základního pohledu do problematiky.

2 Sociální sítě

Sociální síť lze definovat jako „*webovou službu, která uživatelům umožňuje vytvářet veřejné či polo-veřejné profily v rámci uzavřeného systému*“ (boyd¹, Ellison, 2007, s. 2). Jsou to nástroje, na kterých se mohou lidé prezentovat prostřednictvím personalizovaných osobních profilů (Ševčíková et al., 2014, s. 23), a vystupují zde zpravidla pod svým vlastním jménem, jež využívají i v běžném životě (Ševčíková et al., 2014, s. 59). Podle těchto profilů se pak mohou jednotliví uživatelé navzájem vyhledávat a vytvářet mezi sebou vztahy – takzvaná přátelství (Ševčíková et al., 2014, s. 23). Se svými „přáteli“ mají na sociální síti možnost sdílet různorodý obsah, od svých zážitků a fotografií, přes oblíbenou hudbu až například po své politické názory (Kirkpatrick, 2010, s. 31). Jak uvádí David Kirkpatrick ve své knize *Pod vlivem Facebooku: „Předávání informací masám bylo dříve doménou elektronických médií – rádia a televize. Facebook efekt však poskytl možnost zapojit se i běžným jedincům. Nemusíte umět nic navíc ani být odborníky na cokoliv.“* (Kirkpatrick, 2010, s. 8).

Obrovský rozmach tohoto nového komunikačního kanálu můžeme pozorovat již několik posledních let. Ve velké míře jím bylo nahrazeno dříve hojně využívané e-mailové a telefonní spojení (Kirkpatrick, 2010, s. 16). Před více než deseti lety byla sociální média považována spíše jen za nějakou technologickou vymoženost, která byla určena pouze několika vybraným, technicky zdatnějším jedincům (boyd, 2017, s. 18), ale od té doby prošla společnost obrovským vývojem a informační a komunikační technologie se v čele se sociálními sítěmi staly téměř nezbytnou součástí každodenního života (Ševčíková et al., 2014, s. 9). Realitou se postupně stávají spekulace z dob, kdy internet teprve začínal, tedy to, že „*jednou tam bude mít každý svou vlastní stránku*“ – dnes většina z nás svou stránku na některé sociální síti má (Kirkpatrick, 2010, s. 16). Lidé jsou na službách sociálních sítí, které jim mnohdy výrazně zlehčují život, často téměř doslova závislí. Sociální média by se dala dokonce považovat za symbol současné společnosti a kultury (boyd, 2017, s. 20). A je očividné, že vývoj technologií v čele se sociálními sítěmi a mobilními aplikacemi nezpomaluje, ba právě naopak (Uhls, 2018, s. 61). Toto celé je úzce spjato s výzvou, které musíme v současnosti čelit – s otázkou bezpečnosti a eliminování hrozeb, které mohou internet a sociální sítě přinášet (Ševčíková et al., 2014, s. 9).

¹ Jméno **danah boyd** se píše s malými písmeny, vysvětlení je k dispozici na jejích webových stránkách: <http://www.danah.org/name.html>

V současné komunikaci jsou nejvýznamnější a nejpoužívanější sociální sítě jako je Facebook, Instagram, YouTube² nebo Twitter (Karlíček, 2016, s. 196). Celkově nejrozšířenější a nejoblíbenější sociální sítí je již několik let Facebook. V dubnu 2020 na něm bylo registrováno 2,498 mld. účtů, následuje ho YouTube s 2,000 mld. účty. Na dalších pozicích jsou služby takzvaného Instant Messaging – WhatsApp, Facebook Messenger a Wechat. Instagram zabírá šesté místo s 1,000 mil. účty. Čínská sociální síť TikTok je nejnovějším trendem a v žebříčku oblíbenosti se zařadila na sedmou pozici s počtem 800 mil. účtů. (Novotný, 2020).

Hlavním důvodem pro používání sociálních sítí je pro většinu uživatelů jednoznačně možnost jednoduchého udržování kontaktu s přáteli a známými. Již není nezbytné, aby si lidé mezi sebou vyměňovali poštovní adresy, telefonní čísla či e-mailové kontakty jako tomu bylo ještě před několika lety (Karlíček, 2016, s. 196). Tyto asynchronní cesty komunikace, z nichž většina neumožňovala komunikaci v reálném čase, byly v současné době téměř úplně nahrazeny právě sociálními sítěmi (Uhls, 2018, s. 101) a přátelstvím na Facebooku, kde je možné uživatele jednoduše vyhledat a kontaktovat pouze díky znalosti jména (Karlíček, 2016, s. 196). Rozvoj chytrých mobilních telefonů a mobilních sítí umožňuje postupné nahrazení klasického telefonování a posílání SMS zpráv právě komunikací přes internet prostřednictvím aplikací sociálních sítí. V případě Facebooku se jedná zejména o aplikaci Messenger (Karlíček, 2016, s. 196), která umožňuje jak textovou, tak i hlasovou a video komunikaci. A rozvoj mobilních technologií a vývoj aplikací pro sociální sítě rozhodně nezpomaluje, spíše naopak se novinky v těchto odvětvích vyvíjejí stále rychleji (Uhls, 2018, s. 61). Díky tomu se socializace v posledních letech stala téměř nezávislá na prostoru a čase (Uhls, 2018, s. 13). Internet spolu se sociálními médii zároveň ovlivnil i masovou komunikaci, která již nadále není pouze jednosměrná, ale publikum může i reagovat a vyjadřovat své názory pomocí komentářů pod příspěvky na sociálních sítích. (Uhls, 2018, s. 101).

Není pochyb o tom, že sociální média od základů změnila informační a komunikační ekosystém (boyd, 2017, s. 18) a související technologie budou i nadále zásadně ovlivňovat život většiny lidí. Bez mobilních zařízení připojených k internetu se pravděpodobně v běžném životě blízké budoucnosti jen těžko obejdeme (Uhls, 2018, s. 61).

² **YouTube** je známý především jako internetový server pro sdílení videí. V současné době je ale často zařazován i mezi sociální sítě, jelikož uživatelé si tam mohou vytvářet své vlastní kanály, na která mohou nahrávat svá videa, která jim následně mohou ostatní hodnotit (lajkovat) a komentovat.

2.1 Začátky sociálních sítí

V knize Johna A. Barnese *Class and Committees in Norwegian Island Parish* z roku 1954, ve které se autor zabývá sociálními vztahy v rybářské vesnici, byl poprvé použit termín *sociální síť* právě ve významu vztahové sítě mezi jednotlivými lidmi (Barnes, 1954).

Ke službám, které sociálním sítím předcházely, můžeme zařadit například internetové diskusní servery nebo online fotogalerie, kde mohli uživatelé již tehdy sdílet a publikovat omezené množství vlastního obsahu. To jim ale brzy přestalo stačit, chtěli s ostatními i komunikovat, což vedlo k tomu, že se začaly objevovat služby, jejichž hlavní náplní bylo právě spojování uživatelů. A to je vlastně to hlavní, na čem stojí i dnešní sociální sítě – na vztazích mezi jednotlivými uživateli a obsahu, který si tvoří z velké části sami (Bednář, 2011, s. 10).

Jedním z předchůdců Facebooku byla sociální síť Friendster, která byla založena v roce 2002. Zásadní novinkou, která vedla k její popularitě, byla možnost vkládání vlastních fotografií. Ale uživatelé si zde začali ve velkém množství vytvářet falešné identity, což nebylo původním záměrem této platformy. Toho brzy využila síť MySpace, která byla založena v roce 2003. Tato sociální síť byla mnohem benevolentnější a uživatelé si zde mohli zakládat profily například i pro své mazlíčky nebo třeba pohádkové postavy. Dalším faktorem, jenž vynesl MySpace na vrchol byla paradoxně chyba v programování stránky, díky které mohli uživatelé na své profily nahrávat vlastní HTML kód. Profily většiny uživatelů tak brzy „zářily jako náměstí Times Square“ a strohý Friendster upadl v zapomnění (Kirkpatrick, 2010, s. 30).

2.2 Facebook

Sociální síť Facebook byla spuštěna v roce 2004 Markem Zuckerbergem na Harvardské univerzitě. V té době Facebook fungoval pouze pro studenty této univerzity a od tehdy nejrozšířenější sítě MySpace ho odlišoval velice minimalistický styl (Kirkpatrick, 2010, s. 23). Jeho název vznikl na základě letáček, takzvaných „*Facebooks*“, které jsou rozšířené ve Spojených státech mezi studenty na univerzitách a slouží k jednoduššímu vzájemnému seznamování (Blažek, 2015).

Netrvalo dlouho a úspěch Facebooku rychle stoupal, což vedlo k jeho postupnému rozšíření i na další univerzity. Velice rychle se z něho stal naprostý fenomén. Do konce roku 2004 dosáhl 1,5 mil. uživatelů, v následujícím roce byl zpřístupněn i středoškolákům

a jenom o rok později dokonce celé široké veřejnosti (Kirkpatrick, 2010, s. 89). Připojit se od té doby mohl (a dodnes může) každý, komu je více než 13 let (Janouch, 2010, s. 241).

Funkce označování přátel na sdílených fotografiích, se kterou přišel Facebook jako první, je dodnes považována za tu vůbec nejoblíbenější, kterou tato sociální síť nabízí. I přesto, že Facebook ukládá nahrávané fotografie ve značně zhoršené kvalitě, je dodnes díky této funkci nejoblíbenějším nástrojem pro sdílení fotografií (Kirkpatrick, 2010, s. 156).

2.3 Instagram

Velice rozšířenou sociální sítí je v poslední době Instagram, na který se přesouvá pozornost především mladší generace uživatelů (Hofreitr, 2015). Tato sociální síť byla v roce 2010 původně vytvořena pouze jako mobilní aplikace, primárně určená pro chytré telefony (Vesecký, 2016). Slouží především ke sdílení fotografií upravených různými filtry v typickém čtvercovém formátu (v dnešní době lze nahrát i fotografie jiných rozměrů) s tzv. *hashtagy*, označovanými symbolem křížku (#) (Warchar, 2015), které fungují jako identifikátory, štítky nebo klíčová slova, pomocí nichž lze jednoduše dohledávat podobný a související typ obsahu na této sociální síti (Svobodová, 2016, s. 19). A jelikož je aplikace Instagram určena primárně pro používání na chytrých telefonech, souvisí s ním i prudké rozšíření tzv. *selfies*. Lidé dnes častěji fotí sami sebe na přední kamery svých mobilních telefonů než své okolí (Uhls, 2018, s. 141).

Poprvé byl Instagram spuštěn v roce 2010 a netrvalo dlouho, než dosáhl 5 mil. uživatelů. O dva roky později byl koupen majitelem Facebooku Markem Zuckerbergem (Warchar, 2015) a v současné době je právě Instagram oblíbenou platformou, která láká děti a dospívající (Uhls, 2018, s. 103). Hlavním důvodem je pravděpodobně i to, že na Facebooku jsou dnes registrováni „starší“ uživatelé a teenageři na sociálních sítích nechtějí potkávat své rodiče a učitele (Hofreitr, 2015).

3 Ochrana soukromí na sociálních sítích

3.1 Soukromí

Slovník sociální práce Oldřicha Matouška definuje soukromí jako: „*potřebu a právo každého člověka chránit si vlastní území, vlastní čas, vlastní tělo, vlastní prožitky, informace o sobě před zveřejňováním a před zneužíváním.*“ (Matoušek, 2016, s. 208). Fred Cate ve své publikaci *Privacy in the Information Age* (1997) shrnuje definice soukromí podle různých autorů a několik z nich se zde shoduje, že soukromí je vlastně uměle vytvořenou sociální potřebou. V publikaci *Děti a dospívající online* definují autoři soukromí například na základě publikací Irwina Altmana, podle nějž je soukromí procesem „*udržování interprofesionální hranice, v níž jedinec či skupina reguluje interakci s ostatními*“, nebo Sandry Petronio která soukromí popisuje jako regulaci toho, co o sobě a komu sdělíme (Ševčíková et al., 2014, s. 57). Alan Westin (1967) hovoří o tzv. informačním soukromí, které podává jako požadavek jedinců rozhodovat o tom, jaké informace o nich budou poskytovány. V publikaci od Karla Knapa a kol. (2004) je soukromí definováno jako „*právo fyzické osoby rozhodnout podle vlastního uvážení zda, popř. v jakém rozsahu a jakým způsobem mají být skutečnosti jejího osobního soukromí zpřístupněny jiným a zároveň se bránit (vzepřít) proti neoprávněným zásahům do této sféry ze strany jiných osob s rovným právním postavením.*“

Abychom dokázali porozumět tomu, co je soukromí, je potřeba vysvětlit tři pojmy: osobní, veřejný a státní. To, co je označováno za **osobní**, náleží konkrétní osobě, konkrétnímu jedinci, ale nemusí to nutně znamenat, že je to soukromé – „*co je osobní, nemusí být zároveň soukromé, a naopak, co je soukromé, nemusí být vždy osobní.*“ **Veřejné** znamená patřící nebo otevřené všem, a je to tedy opak soukromí. To, co je **státní**, patří státu nebo vládě (Dědečková, 2012, s. 13–14).

Adéla Dědečková ve své diplomové práci (2012) shrnuje několik různých pojetí soukromí: Alan Westin (1967) člení soukromí na čtyři typy, tj. na samotu, odstup, důvěrnost a anonymitu, Fred Cate (1997) soukromí spojuje zejména s tématy samoty, autonomie, izolace a tajemství, ale zároveň poukazuje na to, že to určitě nejsou synonyma. Patricie B. Newell (1995) rozepisuje typologii soukromí, kde definuje samotu, izolaci, anonymitu, odstup, intimitu, tajemství i fantazii. **Samota** je stav, kdy je člověk sám, a často bývá používána jako základní znak definující (prostorové) soukromí – „*jedinec je sám a není vidět.*“ Ale důležitým znakem pro samotu je to, že je to chtěný stav, díky kterému se jedinec snaží ostatním uniknout. Na opačné straně stojí **izolace**, která nastává v moment, kdy jedinci není umožněn kontakt s ostatními, přestože to tak sám nechce. **Anonymita** je stav, který umožňuje

jedinci pohyb ve veřejném prostoru, aniž by mu ostatní věnovali pozornost. Anonymitu ztrácí zpravidla pouze veřejně známé osoby, celebrity, politici apod. **Odstup** je naopak spíše psychický stav, kdy si jedinec vytváří mentální bariéry proti vyrušování ze strany ostatních lidí. **Intimita** označuje touhu po blízkém a osobním vztahu mezi jedinci založeném právě na dostatku soukromí. Sporným typem soukromí je **tajemství**, které někteří autoři ani nechtějí mezi typy soukromí řadit, jelikož ho často pojí s nemorálními činy. Na posledním místě je v typologii zmiňována **fantazie** jako typ soukromí, který je definován jako jakýsi únikový mechanismus, kterým se jedinec snaží soukromí dosáhnout (Dědečková, 2012, s.13).

3.1.1 Soukromí v online době

Jednadvacáté století s sebou kromě neustálého vývoje digitálních technologií a internetu přináší i obrovské změny, co se týče soukromí a jeho ochrany (Uhls, 2018, s. 212). Pro internet je charakteristické to, že se data a informace, která na něj nahrajeme, se mohou šířit obrovskou rychlostí k nepředstavitelnému množství dalších lidí, a navíc cokoliv nahrané na internet již nikdy nelze úplně odstranit (Ševčíková et al., 2014, s. 56). Na internetu je často diskutováno i to, co by běžně člověk držel v tajnosti, čímž se zásadně proměňuje samotná povaha soukromí (Dědečková, 2012, s. 20). A v souvislosti s tím se ztráta soukromí právě v prostředí internetu stává stále častějším problémem (Uhls, 2018, s. 212).

V začátcích internetu se toto médium dalo považovat za relativně anonymní už jenom z toho důvodu, že tehdy tam lidé nepřispívali buď vůbec, nebo pouze se skrytou identitou. V současnosti ale na internet nahráváme nejenom ty nevinné informace (sdílení oblíbeného filmu, receptu apod.), ale často i své osobní údaje, jako je jméno, telefonní číslo, adresa (například při objednávání zboží z e-shopu), nebo dokonce sdílíme svou aktuální polohu. A s tím samozřejmě přicházejí i rizika zneužití těchto údajů (Ševčíková et al., 2014, s. 56), kterým nemusí zabránit ani to, že uživatelé své profily nastavují jako soukromé, popřípadě omezují přístup na ně jen pro vybrané okruhy ostatních uživatelů. A přestože jsou uživatelé často přesvědčeni, že své údaje dostatečně chrání, měli by si zároveň uvědomovat, že nikdy nelze mít nad sdílenými informacemi absolutní kontrolu (Dědečková, 2012, s. 22).

S rozvojem technologií a stále většího vlivu internetu a sociálních sítí na životy lidí, je každopádně téměř nemožné některé informace nesdílet, aniž bychom nepřišli o výhody, které s sebou online komunikace přináší. Nesmíme však zapomínat na to, že na internetu nelze nikdy plně uhlídat, kdo se může ke sdíleným datům dostat (Ševčíková et al., 2014, s. 56–57).

3.1.2 Soukromí na sociálních sítích

S příchodem sociálních médií se do jisté míry mění i nároky na ochranu vlastního soukromí a každý z nás má mnoho možností, jak svou identitu na sociálních sítích bude vytvářet, jak bude sám sebe prezentovat (Svobodová, 2016, s. 28). Přesto bylo zjištěno, že na sociálních sítích je většina příspěvků zaměřena na své pisatele, kteří informují o svých aktuálních činnostech a zážitcích příspěvkem jako: „*Právě teď jsem...*“ (Uhls, 2018, s. 105).

Všichni, kdo sociální sítě alespoň částečně využívají mohou vidět, že s postupem času je stále intenzivněji cíleno na to, aby jejich uživatelé sdíleli více a více obsahu. V současné době jsou velice rozšířené takzvané *stories* neboli příběhy, které jsou nejčastěji využívány na Instagramu, ale obdobná funkce je i na Facebooku. Tyto *stories* mohou obsahovat fotografie nebo krátká videa a jejich specifickým oproti klasickým příspěvkům je to, že je ostatní uživatelé uvidí pouze 24 hodin. To může uživatele vést k myšlence, že budou přes tuto funkci zveřejňovat více detailů ze svého života – vždyť to přeci za chvíli zase zmizí!

Adéla Dědečková ve své diplomové práci (2012) zmiňuje studii z roku 2008 R. Langeho a C. Lampeho, ve které se snaží zjistit, jaký mají uživatelé Facebooku vztah ke svému soukromí. Zmiňuje zde například to, že své jméno a profilovou fotografii uživatelé často nechávají na svých profilech veřejně viditelné, ale ostatní informace obvykle dovoluují zobrazit pouze přátelům. V současné době je toto nastavení – tedy veřejně zobrazené jméno a profilová fotografie – výchozím nastavením Facebooku, které nelze změnit, takže pokud uživatelé chtějí tuto síť využívat, nemohou tyto informace skrýt před veřejností. Z výsledků zmiňované studie dále plyne, že uživatelé často na sociální síti zveřejňují osobní fotografie a místo (město) bydliště, díky čemuž je mohou ostatní uživatelé dohledat. Naopak většinou nezveřejňují své telefonní číslo a konkrétní adresu. Tato data se shodují i s výsledky dalších podobných výzkumů (Dědečková, 2012).

Sociální sítě Facebook a Instagram nabízejí i různé možnosti, jak si své soukromí chránit. Na Facebooku je to nastavení jednotlivých sdílených příspěvků, které lze sdílet veřejně, pouze s přáteli či pouze s vybranou skupinou přátel. Zároveň je na této sociální síti dostupná funkcionality *seznamů přátel*, kde je možné rozdělit sledující do skupin podle toho, zda s nimi chceme sdílet více nebo méně. Instagram má nastavení soukromí poněkud omezenější, uživatel si v podstatě může vybrat pouze ze dvou možností – buď bude mít profil *veřejný*, kde všichni uvidí všechno, nebo *soukromý*, kde se ke sdíleným příspěvkům dostanou pouze jeho sledující. Detailněji se možnostmi nastavení soukromí na těchto sociálních sítích zabývají kapitoly 3.2 (*Ochrana soukromí na Facebooku*) a 3.3 (*Ochrana soukromí na Instagramu*).

3.2 Ochrana soukromí na Facebooku

Ač se to může zdát na první pohled poměrně snadné, nastavení soukromí na Facebooku mohou být občas poměrně nejasná a matoucí, a to především z důvodu, že se často mění. Obecně můžeme předpokládat, že nás na Facebooku sledují hlavně naši *přátelé*, ale při některých nastaveních profilu to mohou být i úplně jiní, cizí lidé. V záplavě příspěvků se navíc může některý „ztratit“ a vlastně ho ani předpokládání sledující z řad *přátel* nemusí zaznamenat (boyd, 2017, s. 49).

Na Facebooku si uživatel každopádně může ve svém profilu nastavit, které informace a které příspěvky zpřístupní veřejnosti, které pouze svým přátelům, které jen některým vybraným osobám a které pouze sám sobě (Svobodová, 2016, s. 13). Ohledně zajištění ochrany a bezpečí existuje stručný průvodce³ s rozcestníkem na detailnější informace vytvořený přímo společností Facebook, který má uživatelům přehledně a jednoduše pomoci se zabezpečením uživatelského účtu.

V první řadě je zde popsáno, jak si vytvořit bezpečné a silné heslo tak, aby se (nejenom) k účtu na této sociální síti nedostal nikdo cizí. Heslo má být jedinečné, dobře zapamatovatelné, ale zároveň dostatečně dlouhé a složené z různých typů znaků. Je doporučováno nepoužívat stejné heslo na různých webových stránkách, jelikož v případě, že by ho někdo odcizil, je více než pravděpodobné, že ho zkusí použít i jinde.

Facebook nabízí možnost zvolit si tzv. důvěryhodné kontakty, které bude možné kontaktovat v případě, kdy uživatel ztratí přístup ke svému účtu. V nastavení *Zabezpečení a přihlášení* pak lze zvolit minimálně tři a maximálně pět přátel, kteří v případě, že to bude potřeba, dostanou oddělené části kódu, pomocí něhož bude možné získat zpět přístup k profilu.

Další zajímavou a velice užitečnou možností, kterou Facebook nabízí, je sledování toho, na kterých zařízeních je uživatel přihlášen, jelikož každé přihlášení vytváří samostatnou aktivní relaci. K těmto údajům se uživatel opět dostane v nastavení přes možnost *Zabezpečení a přihlášení* v sekci *Kde jste přihlášení*. Pokud zde objeví záznam o přihlášení, o kterém si je jistý, že to není on sám, například z neznámého prohlížeče nebo zařízení, může ho nahlásit pomocí tlačítka *Nejste to vy?*. Zároveň zde lze nastavit upozornění na e-mail, Facebook nebo Messenger o nerozpoznaném přihlášení.

³ Zajištění ochrany a zabezpečení. 2020. Facebook [online]. [cit. 2020-07-14]. Dostupné z: <https://www.facebook.com/about/basics/stay-safe-and-secure>

Pro zvýšení ochrany uživatelského účtu na Facebooku si mohou uživatelé zapnout funkci takzvaného dvoufázového ověření. To znamená, že budou při každém dalším přihlašování z nového zařízení kromě vyplnění hesla vyzváni ještě k zadání schvalovacího kódu, který jim bude doručen buď SMS zprávou, nebo v mobilní aplikaci Facebook.

Pokud uživatel používá Facebook pouze na svém soukromém zařízení, na které nemá přístup nikdo jiný, není nezbytně nutné, aby se vždy odhlašoval. Důležité je to ale v tom případě, že se k Facebooku připojuje přes zařízení, která využívají i jiní lidé – ve škole, v zaměstnání apod.

Facebook se prezentuje tím, že k zajištění ochrany informací a dat svých uživatelů používá špičková bezpečnostní opatření. Aktivita uživatelů je šifrována a osobní údaje bez svolení uživatelů, nesdílí – více viz v kapitole 3.2.1. Údaje o uživatelích si však mohou vyžádat úřady v rámci vyšetřování, zejména během trestních řízení. Ve většině případů je uživatel informován o tom, že byly tyto informace o jeho aktivitě vyžádány. Výjimkou jsou například případy vyšetřování zneužívání dětí.

Každý uživatel, který chce využívat služeb Facebooku musí při registraci potvrdit, že souhlasí se *Smluvními podmínkami*. Ty se dělí na několik částí, které se postupně zabývají poskytovanými službami, financováním poskytovaných služeb, závazky uživatelů vůči Facebooku a jeho komunitě a dalšími ujednáními a podmínkami. Tyto smluvní podmínky však nejsou jediné, které se mohou uživatelů týkat. Tato práce se ještě zaměří na *Zásady komunity* v kapitole 3.2.2 a *Zásady používání dat* v kapitole 3.2.3.

3.2.1 Smluvní podmínky Facebooku ve vztahu k soukromí uživatelů

*Smluvní podmínky*⁴ Facebooku se týkají nejenom používání Facebooku, ale také například Messengeru a dalších propojených produktů a služeb poskytovaných společností *Facebook Ireland Limited*. Výjimkou jsou pouze ty služby, které mají vlastní smluvní podmínky – jako je například Instagram (viz kapitolu 3.3.1). *Smluvní podmínky* Facebooku se dělí na několik částí – poskytované služby, financování poskytovaných služeb, závazky uživatelů vůči Facebooku a jeho komunitě a další ujednání a podmínky. V této kapitole se zaměříme pouze na ty části *Smluvních podmínek*, které souvisejí s ochranou soukromí.

⁴ Smluvní podmínky, 2020. *Facebook* [online]. [cit. 2020-12-14]. Dostupné z: <https://www.facebook.com/legal/terms>

V úvodu *Smluvních podmínek* Facebooku je popsáno financování jejich služeb, které je bezplatné, ale tím, že uživatel tyto služby využívá, souhlasí s tím, aby mu byl zobrazován reklamy. Reklamy jsou jednotlivým uživatelům zobrazovány na základě porovnání požadavků inzerentů a osobních údajů uživatelů. Samotní inzerenti však k těmto osobním údajům přístup nemají, o tom, komu budou reklamy zobrazeny rozhoduje Facebook a inzerent dostane pouze report o úspěšnosti své reklamy.

Závazkem uživatele vůči Facebooku je dle těchto podmínek povinnost používat „stejně jméno jako v běžném životě“ a „poskytnout o své osobě přesné informace“. Každá osoba smí vytvořit pouze jeden uživatelský účet a nesmí ho převádět na jinou osobu než na sebe. Facebook zároveň nesmí používat osoby mladší 13 let, lidé odsouzení za sexuální delikvenci nebo někdo, komu byl v minulosti účet zablokovan z důvodu porušení *Smluvních podmínek*.

Produkty a služby Facebooku nesmí být využívány pro nic, co porušuje *Smluvní podmínky*, *Zásada komunity* ani jiné související dokumenty. Zároveň je zakázáno na Facebooku provádět cokoli „nezákonného, diskriminujícího nebo podvodného“, co by mohlo nějak narušovat práva ostatních. Současně se uživatel nesmí pokoušet dostat k datům, ke kterým nemá oprávnění.

Potvrzením *Smluvních podmínek* uživatel uděluje Facebooku také několik oprávnění, například oprávnění k používání uživatelem vytvořeného a sdíleného obsahu. V podmínkách je uvedeno, že vlastníkem práv k duševnímu vlastnictví zůstává uživatel, který obsah vytvořil a sdílel, ale Facebook si nárokuje oprávnění (licenci) k používání tohoto obsahu. Ve smluvních podmínkách je doslova napsáno, že sdílením, zveřejněním nebo nahráním obsahu „udělujete nám (pozn. Facebooku) nevýhradní, převoditelnou, dále licencovatelnou, bezplatnou a celosvětovou licenci k hostování, používání, distribuci, úpravě, spouštění, kopírování, veřejnému předvádění nebo vystavování, překladu a vytváření odvozených děl k vašemu obsahu“. Toto se dá částečně upravit v nastavení soukromí. Je to z důvodu „poskytování a vylepšování produktů a služeb“, jako je například přizpůsobování prostředí sociální sítě každému jednotlivému uživateli dle jeho voleb, nastavení a používání Facebooku nebo sdílení obsahu s ostatními uživateli. Na základě těchto dat může Facebook svým uživatelům zároveň doporučovat další obsah – členství ve skupinách, události, přátelství s dalšími uživateli apod. Facebook má taktéž oprávnění k používání „jména, profilového obrázku a informací o vašich interakcích“, což znamená, že může tyto údaje používat třeba tím způsobem, že přátelům daného uživatele ukáže, které stránky „olajkoval“, o kterou naplánovanou událost má zájem apod.

Ve smluvních podmínkách se ale Facebook zavazuje k tomu, že platnost výše zmíněné licence končí okamžikem odstranění daného obsahu z jeho systémů (a to buď po jednotlivých položkách, nebo odstraněním celého účtu). Z technických důvodů se však může stát, že k okamžitému odstranění nedojde. V takovém případě se Facebook zavazuje k tomu, že daný obsah bude odstraněn nejpozději do 90 dnů. Odstranění obsahu může bránit i například to, že ho použily jiné osoby (např. ho sdílely). Dokud ho také nesmažou, tak nebude možné daný obsah odstranit. Zároveň zde existuje podmínka, že Facebook musí vyhovět žádosti ze strany soudního, správního nebo jiného podobného orgánu, pokud si vyžádají uchovat data po dobu trestního šetření.

Co se týče ochrany soukromí, tak *Smluvní podmínky* Facebooku slibují, že osobní údaje (například jméno a e-mailovou adresu) nejsou nikterak sdíleny ani prodávány třetím stranám, a to zejména zmiňovaným inzerentům, kteří využívají Facebook jako platformu pro reklamu. Pokud chce inzerent zobrazovat svou reklamu určité cílové skupině uživatelů na Facebooku, má pouze možnost zadat požadované parametry (pohlaví, věk apod.) a Facebook na základě toho vyhodnotí, kterým uživatelům reklamu zobrazí. Inzerent následně získá report o úspěšnosti, ale konkrétní data o uživatelích znát nebude.

3.2.2 Zásady komunity Facebook

*Zásady komunity*⁵ popisují, co je a co není na Facebooku povolené. Cílem používání Facebooku má být vytvoření místa, kde lidé dostanou svůj hlas. Facebook ve svých zásadách deklaruje, že chce dosáhnout čtyř základních hodnot – autentičnosti obsahu, bezpečnosti, ochrany soukromí a důstojnosti ve vzájemném chování uživatelů. *Zásady komunity* jsou dále rozděleny na šest částí: násilí a kriminální chování, bezpečnost, nepřijatelný obsah, integrita a autentičnost, respektování duševního vlastnictví a žádosti související s obsahem.

S tématem této diplomové práce souvisí částečně kapitola *Integrita a autentičnost*, která se mimo jiné zabývá také falešnou identitou a *zvěčnění* účtu. Facebook od svých uživatelů vyžaduje, aby na síti vystupovali pod svým pravým jménem, které využívají i v běžném životě, což má napomoci vytvoření bezpečného a důvěryhodného prostředí. To znamená, že by zde měl každý vystupovat sám za sebe a nemělo by se stávat ani to, že někdo při registraci vyplní

⁵ Zásady komunity. 2020. *Facebook* [online]. [cit. 2020-07-14]. Dostupné z: <https://www.facebook.com/communitystandards/>

například jiné datum narození (svůj věk často zvyšují děti, jelikož dokud jsou mladší 13 let, nemohou se na Facebooku registrovat).

O zveřejnění účtu může být požádáno přáteli a rodinnými příslušníky osoby, která zemřela. Každý uživatel má právo vybrat v nastavení svého profilu, zda si přeje po své smrti účet odstranit nebo může označit osobu, která se bude po jeho smrti o daný facebookový účet starat a budou tam tak zachovány všechny sdílené informace a příspěvky.

I část týkající se duševního vlastnictví souvisí s ochranou soukromí. Facebook se zde zavazuje, že obsah, který uživatelé na této sociální síti sdílí, zůstává ve vlastnictví uživatelů a to, jak bude moci být dále sdílen je ovlivněno na základě jejich vlastního nastavení. Na oplátku po svých uživatelích vyžaduje, aby sdíleli jen ten obsah, ke kterému mají sami právo.

3.2.3 Zásady používání dat na Facebooku

*Zásady používání dat*⁶ je dokument týkající se dat, která Facebook, Facebook Messenger a další související služby zpracovávají a shromažďují. Je zde popsáno, jaké druhy informací Facebook zaznamenává, jak je následně používá, jak data uchovává atd. Důvody ke zpracování dat, které jsou v dokumentu uvedeny, souvisí s plněním podmínek používání služby Facebook a vždy je to podmíněno souhlasem uživatele, který to potvrdil při registraci. Tyto zásady jsou rozděleny na několik částí, jež se týkají například tohoto:

- jaké informace jsou o uživatelích shromažďovány,
- jak jsou tyto informace použity,
- jak jsou tyto informace sdíleny,
- jak lze uplatnit svá práva nebo
- jak jsou uchovávána data při deaktivaci účtu.

Úvodní část *Zásad používání dat* se zabývá tím, jaká data jsou o uživatelích shromažďována. Je to obsah, který uživatelé poskytují při používání Facebooku – jedná se například o vyplněné údaje v profilu, metadata o poskytovaném obsahu (fotografie) a zároveň o automaticky zpracováváný obsah komunikace, který může být dále použit pro účely

⁶ Zásady používání dat. 2020. *Facebook* [online]. [cit. 2020-07-14]. Dostupné z: <https://www.facebook.com/about/privacy>

přizpůsobení obsahu (reklamy aj.). Pokud to uživatel povolil, může Facebook sbírat data i o jeho lokalitě (poloha zařízení, IP adresa). I na základě těchto údajů pak bude přizpůsobován další obsah, který Facebook uživateli zobrazí. Nasbíraná data Facebook využívá také pro průzkumy a vývoj či vylepšování produktů. Data o uživatelích jsou sbírána napříč produkty Facebooku, které uživatelé používají, tj. na základě sledovaných účtů na Instagramu může být uživatelům například doporučena stránka nebo skupina na Facebooku apod.

Facebook dále shromažďuje data o síti kontaktů jednotlivých uživatelů. Patří sem jak informace o lidech, tak i o stránkách a skupinách, se kterými uživatel nějakým způsobem interaguje. Pokud uživatel své adresáře z mobilního zařízení synchronizuje se svým účtem na Facebooku, jsou shromažďována i data o těchto kontaktech a shromažďována jsou i data týkající se používání dalších produktů a aplikací Facebooku. Pokud uživatel provádí finanční transakce (například ve hrách, v příspěvcích na charitu apod.), bude zaznamenána informace o platbě, kam patří číslo platební karty, informace o účtu, podrobnosti o fakturaci aj. V neposlední řadě jsou uchovávána i data a informace, která o uživateli na Facebook přidávají ostatní uživatelé – například někdo sdílí fotku, kde označí dalšího uživatele.

Dále jsou shromažďovány informace o zařízeních, která uživatelé používají při interakci s produkty Facebooku. Na základě těchto dat pak může být uživateli přizpůsobován obsah, jenž se mu zobrazuje na notebooku například podle toho, jakým způsobem používal Facebook na mobilním telefonu. Shromažďována jsou data o vlastnostech zařízení, jako je informace o operačním systému, verzi hardwaru, softwaru, typu prohlížeče apod. Uchovávají se i informace o operacích a chování při používání Facebooku na daném zařízení, například pohyby myši nebo zda je okno Facebooku v popředí či nikoli. Dále to mohou být signály, které zařízení vysílá, data o některých nastaveních, o síti a stavu připojení a soubory cookies.

V neposlední řadě Facebook shromažďuje data od svých partnerů, kteří využívají sociální pluginy od Facebooku. To může být například možnost přihlášení se na webovou stránku prostřednictvím svého facebookového účtu nebo implementované tlačítko *To se mi líbí* na webu.

Druhá část *Zásad používání dat* popisuje, jak jsou shromážděné informace používány. Jak již bylo řečeno výše, tak prvním důvodem pro shromažďování dat je možnost následného přizpůsobení a vylepšování produktů společnosti Facebook. Uživatelům na základě získaných dat zároveň chodí přizpůsobené marketingové nabídky. Dále lze tyto informace využít pro různé analýzy, které například pomohou inzerentům zjistit účinnost jejich reklamy. Shromážděné informace Facebook využívá také z bezpečnostních důvodů, zejména při ověřování uživatelských účtů.

Třetí část se zabývá tím, jak jsou nashromážděné informace dále sdíleny. Na Facebooku si uživatel volí, s kým bude svůj obsah sdílet (např. s veřejností, s přáteli, s vybranou skupinou přátel apod.). Zároveň by měl každý uživatel myslet na to, že obsah, který zveřejňuje, mohou všichni ti, se kterými ho sdílí, znovu sdílet s dalšími lidmi. V externě integrovaných aplikacích (např. hrách) mohou jejich zástupci (vývojáři, zástupci webu apod.) sledovat aktivitu a získat přístup k profilu uživatele.

Údaje o uživateli jsou uchovávány do té doby, dokud jsou jim poskytovány služby nebo do momentu odstranění uživatelského účtu. Delší dobu mohou být informace o uživateli uchovávány v tom případě, že jsou předmětem „*právně podložené žádosti či povinnosti, oficiálního policejního vyšetřování nebo vyšetřování možného porušení podmínek a zásad (Facebooku)*“. Zároveň jsou ponechána po dobu jednoho roku data uživatelů, jejichž účty byly deaktivovány z důvodu porušení podmínek, aby bylo zabráněno opakování zneužití nebo porušení.

Poslední bod, který je v *Zásadách používání dat* popsán a souvisí s ochranou soukromí, se týká globálního sdílení dat uživatelů interně v rámci společnosti Facebook, ale také externě s jeho partnery a uživateli, a to za účelem poskytování služeb.

3.2.4 Možnosti nastavení profilu na Facebooku týkající se soukromí

Facebook pro své uživatele připravil online průvodce nastavením soukromí jejich profilů s názvem *Základy soukromí*.⁷

Průvodce *Základy soukromí* je rozdělen do několika částí. Hned po úvodních ilustracích doplněných lákavými slogany je rozcestník hlavních témat, kde mají být v podstatě shrnuty nejčastější dotazy týkající se nastavení soukromí příspěvků, profilu, seznamu přátel, reakcí a komentářů, označování a odeírání z přátel a blokování. V následující části nazvané *Je to ve vašich rukou* se pak uživatel dozví více o tématech správy soukromí, zvýšení zabezpečení účtu, nastavení reklam a navazování spojení – detailněji to popisuje zbytek této kapitoly.

Správa vlastního soukromí na Facebooku je něco, co si může uživatel v mnohém přizpůsobit. Může si nastavit, kdo uvidí jeho příspěvky, fotky a další sdílený obsah, má možnost zjistit, jak se jeho profil zobrazuje ostatním a kdo uvidí seznam jeho přátel, může si upravit, kdo uvidí jeho reakce a komentáře, kdo uvidí fotky, na kterých je označený a mnohé další.

⁷ Základy soukromí na Facebooku. 2020. *Facebook* [online]. [cit. 2020-07-14]. Dostupné z: <https://www.facebook.com/about/basics>

Nastavit **soukromí u jednotlivých příspěvků** mohou uživatelé při zveřejňování těchto příspěvků. Tuto volbu lze kdykoli později změnit. Sdílet své příspěvky mohou uživatelé se svými přáteli (což je nejčastěji využívaná varianta), veřejně nebo s konkrétní skupinou osob. Upravit konkrétní okruh skupiny uživatelů lze za pomoci takzvaných *seznamů přátel*, díky kterým je možné přátele na Facebooku roztrždit. K této možnosti se lze dostat v levém menu na hlavní stránce, kde je (pravděpodobně skrytá pod volbou *Zobrazit další*) položka *Seznamy přátel*. Příspěvky pak mohou uživatelé sdílet zvláště například pro rodinu nebo kolegy z práce. Tyto seznamy přátel si může každý uživatel vytvářet libovolně podle svých potřeb, ale pro začátek jsou zde tři přednastavené. Seznam s názvem *Blízcí přátelé* by měl sloužit pro ty přátele, se kterými chce daný uživatel sdílet obsah přednostně, a seznam *Známí* je pro ty, se kterými naopak nechce sdílet tolik. Při sdílení příspěvku lze dokonce zvolit variantu *sdílet s: Přátelé kromě známých*. Třetí přednastavený seznam nese titulek *Omezeno* a je určen pro ty osoby, které sice má uživatel v přátelích, ale obsah s nimi sdílet nechce. Osobám na tomto seznamu se pak bude zobrazovat pouze *veřejně* sdílený obsah. Důležité je, že se přátelé nedozví, ve kterém seznamu je má uživatel zařazené.

S nastavením soukromí jednotlivých příspěvků pak souvisí také to, co bude zobrazováno **na profilové stránce** daného uživatele. Uživateli, který něčí profil navštíví se zobrazí ty příspěvky, které odpovídají jeho zařazení v příslušném *seznamu přátel*. V nastavení Facebooku v sekci *Timeline a označování* si může každý uživatel nastavit, co bude na jeho profilu zobrazováno, jak se budou zobrazovat příspěvky, které přidali přátelé na jeho profil nebo na kterých je označen. Jsou však informace, které jsou na profilu nastaveny jako veřejné vždy, což znamená, že to uvidí kdokoli z Facebooku i mimo něj. Je to jméno, *profilová fotka*⁸ a *úvodní fotka*⁹.

Uživatel si může také nastavit, kdo další uvidí na jeho profilu seznam přátel. K tomuto nastavení se dostane na profilu v sekci *Přátelé*, kde je pak vpravo nahoře možnost *Upravit soukromí*. I přes to, že má pak uživatel na svém profilu seznam přátel skrytý, může být jeho

⁸ **Profilová fotka** na Facebooku je snímek, kterým uživatel identifikuje svůj profil. Uživatelé zde často používají fotografie, kde jsou vyobrazeni oni sami – fotografie a selfies svých obličejů, postav aj. Profilová fotografie má zároveň daného uživatele identifikovat všude v prostředí Facebooku – kdykoli sdílí nějaký příspěvek, napíše nějaký komentář apod., bude u toho ostatním uživatelům zobrazena kromě jména právě i profilová fotografie. Tato fotografie je vždy veřejná pro všechny.

⁹ **Úvodní fotka** na Facebooku je fotografie, kterou si uživatel může vložit do záhlaví svého profilu. I tato fotografie je vždy nastavena jako veřejná pro všechny ostatní uživatele, kteří si profil daného uživatele zobrazí.

jméno zobrazeno v seznamu přátel jeho přátel – samozřejmě záleží na nastavení profilu jeho přítele.

Na Facebooku je uživatelům k dispozici funkce **Zobrazit jako**, která slouží k tomu, že si uživatel může svůj profil prohlédnout z pohledu veřejnosti (tedy osob, které nemá v přátelích) a zkontrolovat si tak nastavení svého soukromí. Tuto možnost lze nalézt v profilu, přes tři tečky v pravém dolním rohu úvodní fotky.

3.3 Ochrana soukromí na Instagramu

Jelikož je sociální síť Instagram ve vlastnictví stejné společnosti jako Facebook, tak se ochrana soukromí na této sociální síti příliš neliší a v zásadě lze říci, že většina základních možností je obdobná, jako na Facebooku – například nutnost nastavení silného hesla, možnost nastavení dvoufázového ověření při přihlašování a sledování neoprávněných pokusů o přihlášení se k uživatelskému účtu. Drobné odlišnosti, kterými Instagram disponuje pak vychází z rozdílů těchto dvou sociálních sítí.

3.3.1 Podmínky použití Instagramu ve vztahu k soukromí uživatelů

Při registraci na sociální síť Instagram musí každý uživatel potvrdit svůj souhlas s *Podmínkami použití*¹⁰, které představují smlouvu mezi daným uživatelem a společností *Facebook Ireland Limited*. Pokud uživatel nebude tyto podmínky dodržovat, může mu být na základě těchto podmínek odebrán příslušný nevhodný obsah nebo dokonce zablokován celý uživatelský účet. Poslední verze *Podmínek použití* Instagramu byla zveřejněna na konci listopadu 2020 a budou účinné od 20. prosince 2020¹¹.

V úvodní části je v *Podmínkách použití* popsáno, jaké služby Instagram svým uživatelům poskytuje a hned následně je čtenáři sděleno, že s poskytovanými službami samozřejmě souvisí i sběr a používání informací uživatelů. To je detailněji specifikováno v dokumentu s názvem *Zásady používání dat*, kterému se věnuje kapitola 3.3.3. Následuje část zaměřená na financování Instagramu, kde je uvedeno, že uživatelé za používání Instagramu nic neplatí, ale tím, že službu využívají souhlasí také s tím, že jim bude zobrazována relevantní

¹⁰ Podmínky použití Instagramu, 2020. *Facebook* [online]. [cit. 2020-12-14]. Dostupné z: https://help.instagram.com/1215086795543252?helpref=page_content

¹¹ pozn. Nové *Podmínky použití* Instagramu vejdou v účinnost 2 dny po odevzdání této diplomové práce, v této kapitole je popsáno již jejich nové znění.

reklama. Inzerenti mohou požadovat, jakým okruhům uživatelů chtějí své produkty nabízet. Instagram potom na základě údajů, které o sobě uživatelé na této sociální síti zveřejní, vyhodnocuje, komu danou reklamu zobrazí. Inzerentům nejsou osobní údaje uživatelů sdělována.

Závazkem ze strany uživatele je podle *Podmínek použití* dodržení několika faktorů – toho, že je uživatel osoba starší 13 let, že není trestně stíhaná jako sexuální delikvent a její účet na Instagramu nebyl v minulosti zablokován z důvodu porušení zákona nebo zásad Instagramu. Uživatel sice nemusí na Instagramu vystupovat pod svým jménem, ale nesmí toho využívat k vydávání se za někoho jiného. Tomu má zamezit povinnost poskytování přesných a aktuálních informací, jako je například registrační e-mailová adresa. Uživatelé se zkrátka souhlasem s těmito podmínkami zavazují k tomu, že nebudou dělat nic, co by mohlo nějakým způsobem narušovat nebo zhoršovat fungování služeb Instagramu.

V souvislosti se soukromím je důležitá další část, týkající se oprávnění, která každý uživatel Instagramu uděluje. Stejně jako na Facebooku, ani na Instagramu se nahráním obsahu uživatel nevzdává jeho vlastnictví. Ale tím, že obsah na této sociální síti zveřejní uděluje Instagramu „nevýhradní, bezplatnou, převoditelnou, dále licencovatelnou a celosvětovou licenci k hostování, používání, distribuci, úpravě spouštění, kopírování, veřejnému předvádění nebo vystavování, překladu a vytváření odvozených děl“. Pokud chce uživatel tuto licenci ukončit, může nahraný obsah ze svého účtu odstranit. Ale stejně jako na Facebooku je to i zde ovlivněno tím, zda mezitím tento obsah nesdílel někdo další. V takovém případě bude tento obsah i nadále zobrazován.

Dále každý uživatel na základě těchto podmínek poskytuje Instagramu oprávnění k používání profilového obrázku a informací o akcích nebo vztazích (tzn. označování příspěvků ostatních *To se mi líbí* nebo sledování jiných účtů).

Instagram si dále vyhrazuje právo odebírat obsah sdílený uživateli, který porušuje *Podmínky použití* nebo *Zásady komunity Instagram* (viz kapitolu 3.3.2). Pokud uživatel porušuje podmínky opakovaně nebo společnost Facebook vystavuje např. riziku trestního stíhání, může mu být zablokován přístup ke službě Instagram nebo k jejím částem.

Pokud uživatel požádá o odstranění svého uživatelského účtu, může tento proces trvat až 90 dnů. Po tuto dobu již není obsah viditelný ostatním uživatelům Instagramu, ale ještě je dostupný v zálohách pro případnou obnovu dat. Delší dobu může být obsah uživatelského účtu uchovávan pouze z důvodů technických omezení nebo pokud by jeho odstranění mohlo ohrozit průběh vyšetřování nelegální činnosti nebo porušení *Podmínek použití*.

3.3.2 Zásady komunity Instagram

Používáním Instagramu uživatel souhlasí nejen s *Podmínkami použití*, o kterých se zmiňuje předchozí kapitola, ale také se *Zásadami komunity*¹². Tyto *Zásady* určují pravidla, která musí uživatelé dodržovat, pokud chtějí Instagram používat. Hned na prvním místě je zde nutnost vlastnictví práv k obsahu, který uživatel na síti sdílí. Dále je zde uživatel seznámen s tím, že nesmí zveřejňovat nevhodný obsah, jako jsou snímky odporující zákonným opatřením, například obhajování terorismu, holokaustu, nabízení sexuálních služeb apod.

Instagram se zde zavazuje k tomu, že bude chránit a respektovat své uživatele. Pokud někdo z nich poruší tyto zásady například tím, že na této sociální síti někoho obtěžuje či mu vyhrožuje, Instagram daný příspěvek odebere a dotyčný uživatel může být zablokován. Zároveň zde prosí své uživatele, aby takto nevhodný obsah nahlašovali, jelikož ne vždy se to správcům podaří odhalit okamžitě.

Zásady upozorňují také na to, že se může stát, že některý z uživatelů bude sdílet něco, co se jinému uživateli z nějakého důvodu nelíbí, ale *Zásady komunity* to neporušuje. V takovémto případě je doporučováno, aby uživatel přestal nechtěný obsah sledovat, případně si druhou osobu zablokoval.

3.3.3 Zásady používání dat na Instagramu

*Zásady Instagramu ohledně používání dat*¹³ jsou také velmi podobné *Zásadám používání dat na Facebooku* (kapitola 3.2.3). Shromažďován je veškerý obsah, který uživatelé poskytují při používání Instagramu – tj. údaje uvedené při registraci, při sdílení obsahu nebo komunikaci s ostatními uživateli. Ukládána jsou i metadata poskytovaného obsahu a data o síti kontaktů, kterou si uživatelé tvoří svou aktivitou na Instagramu. Zároveň jsou ukládány i informace o tom, jaké informace o uživateli sdílí ostatní. Stejně jako při používání Facebooku, jsou i u Instagramu shromažďována data o zařízeních, ze kterých uživatelé k aplikaci přistupují – vlastnosti zařízení, informace o prováděných informacích, identifikátory zařízení,

¹² Zásady komunity Instagram. 2020. *Instagram* [online]. [cit. 2020-07-14]. Dostupné z: [https://www.facebook.com/help/instagram/477434105621119/?helpref=hc_fnav&bc\[0\]=Nápověda%20pro%20instagram&bc\[1\]=Centrum%20soukrom%C3%AD%20a%C2%A0bezpečnosti](https://www.facebook.com/help/instagram/477434105621119/?helpref=hc_fnav&bc[0]=Nápověda%20pro%20instagram&bc[1]=Centrum%20soukrom%C3%AD%20a%C2%A0bezpečnosti)

¹³ Zásady Instagramu ohledně používání dat. 2020. *Instagram* [online]. [cit. 2020-07-15]. Dostupné z: [https://www.facebook.com/help/instagram/519522125107875/?helpref=hc_fnav&bc\[0\]=Nápověda%20pro%20instagram&bc\[1\]=Centrum%20soukrom%C3%AD%20a%C2%A0bezpečnosti](https://www.facebook.com/help/instagram/519522125107875/?helpref=hc_fnav&bc[0]=Nápověda%20pro%20instagram&bc[1]=Centrum%20soukrom%C3%AD%20a%C2%A0bezpečnosti)

informace o připojení k síti atd. Jsou shromažďována data i od partnerů, kteří využívají některé funkcionality, např. plugin tlačítka *To se mi líbí* aj.

Shromážděné informace jsou využívány, stejně jako na Facebooku, k poskytování, přizpůsobování a zlepšování produktů Instagram. Uživatelské informace jsou spojeny napříč všemi produkty Facebooku, aby je bylo možné ještě lépe využívat k přizpůsobování obsahu. Toto je využíváno i pro přizpůsobování reklamních nabídek.

Každý uživatel si volí cílovou skupinu, se kterou bude sdílet svůj obsah – na Instagramu lze nastavit profil jako *veřejný* nebo *soukromý* (viz kapitolu 3.3.4). Veřejné informace jsou pak dostupné všem jak v rámci Instagramu, tak i všem mimo něj. Příspěvky uživatele mohou ostatní uživatelé (ti, kteří k tomuto obsahu mají přístup) dále sdílet i se svými sledujícími.

3.3.4 Možnosti nastavení profilu na Instagramu týkající se soukromí

Tipy, jak zabezpečit uživatelský účet na Instagramu jsou shrnuty v příručce *Tipy k zabezpečení*¹⁴, která je dostupná v centru nápovědy Instagramu. Tato kapitola shrnuje to nejpodstatnější.

Stejně jako kdekoli jinde je i na Instagramu důležité nastavení bezpečného hesla, které bude natolik unikátní a bude obsahovat dostatečně různorodé znaky, že bude velice těžko prolomitelné. S nastavením hesla úzce souvisí nastavení přihlašování se za pomoci dvoufázového ověření. To zde funguje obdobně, jako u Facebooku, takže při každém přihlašování do aplikace Instagram z nového zařízení bude kromě hesla vyžadováno ještě vyplnění kódu, který uživatel obdrží SMS zprávou.

Tím nejzákladnějším, co může uživatel udělat pro ochranu soukromí na svém instagramovém účtu, je to, že si ho v nastavení přepne z *veřejného* na *soukromý*. Při takovémto nastavení uvidí obsah jeho profilu jenom ti sledující, které sám schválí. Naopak pokud by nechal svůj profil jako *veřejný*, bude jeho sdílený obsah viditelný pro všechny uživatele Instagramu.

Ochrana soukromí na Instagramu se od Facebooku liší hlavně v tom, že zde platí jedno nastavení zpravidla na všechno, co uživatel sdílí. Tj. pokud nastaví svůj profil jako *veřejný*, budou všechny jím sdílené příspěvky i příběhy veřejné. Nemůže si zvolit pro každý jednotlivý

¹⁴ Tipy k zabezpečení. 2020. *Instagram* [online]. [cit. 2020-07-15]. Dostupné z: [https://www.facebook.com/help/instagram/377830165708421/?helpref=hc_fnav&bc\[0\]=Nápověda%20pro%20Instagram&bc\[1\]=Centrum%20soukrom%C3%AD%20a%20a%20A0bezpečnosti](https://www.facebook.com/help/instagram/377830165708421/?helpref=hc_fnav&bc[0]=Nápověda%20pro%20Instagram&bc[1]=Centrum%20soukrom%C3%AD%20a%20a%20A0bezpečnosti)

příspěvek jiné nastavení. Jedinou možností, kterou může uživatel na Instagramu využít, je sdílení *stories* (příběhů) pouze se skupinou *blízkých přátel*, které si v nastavení sám vybere. Tato funkce je ale dostupná pouze pro jednotlivé příběhy, zbytek profilu a příspěvků se sdílí všem sledujícím uživatelům. Sledující zařazení v seznamu blízkých přátel nicméně nikde nevidí, že jsou v takovémto seznamu zařazení. To je jim odkryto až v případě, kdy s nimi uživatel sdílí svůj příběh – tak se dozví, že je ten daný příběh pouze pro blízké přátele, a je tedy zřejmé, že jsou do tohoto seznamu zařazení.

4 Teenageři ve světě sociálních médií

Internet a sociální média jsou v současnosti (nejenom) ve světě teenagerů obrovským trendem, ze kterého mohou být jejich rodiče poněkud znepokojeni, jelikož v mnoha případech nejnovějším technologiím sami úplně nerozumí a zároveň se obávají ztráty kontroly nad tím, k jakým mediálním zdrojům se takto jejich děti mohou dostat (Uhls, 2018, s. 14). To je naprosto pochopitelné, současní rodiče ještě zažili svět „před internetem“, jejich dětství a dospívání rozhodně nebylo technologiemi zasaženo do takové míry, jako je tomu u dnešních dětí (Whitty a Young, 2017, s. 73). A přestože rodiče mohou ztrácet nad novými technologiemi kontrolu, jejich děti jsou těmi, kteří se do tohoto „světa digitálních technologií“ narodily a celý jejich život jimi bude ve velké míře ovlivňován. Život bez mobilního telefonu a internetu je pro tyto děti téměř nepředstavitelný (Ševčíková et al., 2014, s. 19).

Taková situace nenastala v historii lidstva poprvé. Už Sokrates byl známý svými obavami z toho, že abeceda a schopnost psát budou v budoucnu negativně ovlivňovat lidskou paměť a schopnost učit se (boyd, 2017, s. 28). Na konci 19. století zase měli rodiče obavy, když začaly vycházet paperbackové romány od autorů jako je Jane Austenová. Toto tehdy nové médium bylo symbolem neseriózní zábavy a plýtvání času. Nadměrný zájem dětí a dospívajících o tyto romantické příběhy je děsil, obávali se, že kvůli tomu půjde „celá příští generace rovnou do pekla.“ Teenageři, stejně jako dnes, názoru dospělých vzdorovali a tyto romány četli, jak jen mohli. V současnosti je tvorba Jane Austenové paradoxně považována za kvalitní literaturu. A podobná situace nastala později i s příchodem rádia, filmu, televize, počítače a samozřejmě i již zmíněného internetu. Přestože se tento vzorec chování evidentně opakuje, i ve 21. století generace dospělých trvá na tom, že „tentokrát jde opravdu o něco jiného“ (Uhls, 2018, s. 11–12).

V každé době se dospívající lidé, teenageři, snaží najít a získat své místo ve společnosti (boyd, 2017, s. 21). Co se týče celého procesu socializace, kdy se lidé učí, jak se stát hodnotnými a produktivními členy společnosti, běžně v něm napomáhá několik různých faktorů – rodiče, vrstevníci, učitelé apod. Nyní se se nejčastějším zdrojem pro osvojování si společenských a kulturních hodnot poprvé v historii stala digitální média, k čemuž přispělo několik faktorů – mobilní telefony, sociální média a dotyková technologie (Uhls, 2018, s. 33). Existence sociálních médií přesunula snahu socializovat se do světa takzvané *online veřejnosti*. Pojem *online veřejnost* označuje technologiemi tvořený prostor pro sdílení, ale také komunitu, která v sobě pojí jak technologie, tak běžné chování lidí. A důvody, které vedou teenagery k tomu, aby se zapojovali do online veřejnosti jsou v podstatě stejné, jako tomu bylo kdykoli

dříve, když se snažili vstupovat do společenského života v parcích, obchodních centrech a podobných místech – chtějí se stát součástí světa, propojit se s dalšími lidmi a prohlubovat své vztahy s nimi (boyd, 2017, s. 21). Dokonce i Abraham Maslow staví potřebu sounáležitosti ve své pyramidě potřeb na důležité místo hned za potřebu potravy a bezpečí. Není proto divu, že je pro děti a teenagery komunikace s vrstevníky tak důležitá (Uhls, 2018, s. 104). Již výzkum *Oxford Internet Survey* z roku 2011 zjistil, že opravdu téměř všechny děti ve věku od 14 do 17 let používají internet (Whitty a Young, 2017, s. 73). A je důležité zmínit, že ač to dospělí vnímají často naprosto odlišně, pro děti neexistuje rozdíl mezi svou „osobností v online a offline světě“ (Uhls, 2018, s. 106).

Oproti klasickým veřejným prostorům má však online veřejnost jiné vlastnosti. Definují ji následující čtyři znaky – **stálost** online obsahu, **zobrazování** obsahu potenciálnímu publiku, snadné **rozšiřování** obsahu a jednoduché (znovu) **vyhledávání** sdíleného obsahu (boyd, 2017, s. 24).

Z toho vyplývá, že sociální média a naše *digitální stopa*¹⁵, která na internetu vzniká, v zásadní míře změnila sociální situaci. Šíření pomluv a fám je například umocněno, zefektivněno rychlostí šíření prostřednictvím sociálních sítí. Nejen teenageri jsou tak schopni vyhledáváním dat o ostatních tzv. „stalkovat“ jeden druhého. Sociální sítě takto mohou přitáhnout pozornost k začínající kapele a zviditelnit ji, ale stejně dobře mohou šířit pomluvy a eskalovat konflikty mezi lidmi (boyd, 2017, s. 26).

Internet bohužel i dnes používá velké množství lidí, kteří si neuvědomují existenci nějaké digitální stopy. Toto může často ovlivňovat budoucí život například při nástupu na vysokou školu nebo při hledání zaměstnání. A v momentu, kdy si toto neuvědomují ani dospělí, nastává problém v tom, co o sobě jejich děti mnohdy sdílí, aniž by je kdokoli upozornil na nějaké možné důsledky. Na jedné straně problému tedy stojí samotná aktivita dětí a teenagerů, a na straně druhé pak aktivita „hrdých rodičů“, kteří sdílí fotky svých dětí již od jejich útlého věku (Uhls, 2018, s. 119).

S tím souvisí fenomén *sharentingu* (do češtiny se tento termín nepřekládá). Termín vznikl složením slov *share*, česky sdílet, a *parenting*, tedy rodičovství. Také se v obdobném významu používá termín *oversharenting*, tedy spojení slov přehnané

¹⁵ **Digitální stopa** je soubor informací, které po sobě uživatel zanechává v prostředí internetu. Rozlišujeme aktivní a pasivní digitální stopu: ta aktivní zahrnuje vše, co o sobě uživatel sdílí vědomě (příspěvky na sociálních sítích, e-mailů...), a ta pasivní je souborem informací, které se o uživateli ukládají jenom tím, že provádí nějakou interakci v prostředí internetu (IP adresa, vyhledávané výrazy, informace o času stráveném na nějaké stránce apod.) (Digitální stopa, ©2013).

sdílení a rodičovství. Tento fenomén popisuje současný trend, kdy rodiče sdílí na sociálních sítích fotky a informace o svých dětech, a to často hned po jejich narození. *Digitální identita a stopa* těchto dětí je tedy tvořena již od jejich útlého dětství. Rodiče tak činí bez souhlasu svých dětí – až děti vyrostou, nemusí být spokojeni s tím, co o sobě na internetu a sociálních sítích najdou. Tito rodiče se brání tím, že také mají právo pochlubit se svými potomky, ale zatím se stále diskutuje o tom, zda je jejich jednání správné, či nikoli. Většinou panuje shoda, že by mělo dojít k nějakému kompromisu – rodiče by například vždy měli dobře promyslet, které informace o svých dětech sdílet, aby se za to nemusela ani jedna strana později stydět (Steinberg, 2016).

Yalda Uhls v úvodu své knihy *Mediální mámy a digitální tátové* zmiňuje průzkum nadace Kaiser Foundation (Rideout et al., 2010), která v průběhu deseti let měřila používání médií dětmi mezi 8 a 18 lety – v roce 1999, 2004 a 2010. Celkový čas, který děti trávily s médii, vzrostl, a to téměř na osm hodin denně, sedm dní v týdnu z čehož lze jednoduše odvodit, že je to stejně nebo i mnohem více času, než kolik tráví průměrné dítě ve škole nebo s rodiči (Uhls, 2018, s. 13). Další průzkum, který Yalda Uhls zmiňuje se zabývá tím, jak moc mají „teenageři svá zařízení rádi“, a zjišťuje, že v USA a ve Velké Británii by dali přednost svým mobilním zařízením, které je spojuje s kamarády, například před kapesným, novým oblečením nebo večeří v restauraci (Uhls, 2018, s. 62). Pro teenagery je *online veřejnost* s offline světem natolik propojená a neoddělitelná, že na používání sociálních sítí závisí jejich zapojení do společnosti, ovlivňuje to „oblíbenost“ jednotlivců ve skupině (zejm.) vrstevníků. (Uhls, 2018, s. 91). Není tak divu, že se snaží sdílet své názory a zážitky s ostatními a získávat na sociálních sítích obdiv – *lajky* a *followery* (Uhls, 2018, s. 126).

Ale není to pouze o *lajcích*. Pro teenagery jsou sociální sítě důležité i z praktického hlediska. Využívají je při komunikaci ohledně školy a skupinových úkolů, domlouvají si na nich setkání v offline světě a následně tam zveřejňují fotky z míst, kde společně trávili čas (Ševčíková et al., 2014, s. 59).

Dalším z důvodů, proč tráví teenageři na sociálních často tolik času, je strach ze zmeškání něčeho důležitého. Když se teenager dříve nezúčastnil například nějakého večírku, byl pak další den nucen poslouchat skvělé historky a zážitky ostatních. Dnes tyto zážitky vidí téměř okamžitě na sociálních sítích, a navíc v mnohem větší míře. Je to zároveň úzkost, která vzniká při porovnávání svého života s životy ostatních, což je něco, čemu se na sociálních sítích lze jen velice těžko vyhnout. Tomuto stavu se říká zkráceně *FOMO*, z anglického *fear of missing out* (Uhls, 2018, s. 139). Toto se pak může týkat i těch teenagerů, kteří sociální sítě až tak aktivně nepoužívají a příliš po tom ani netouží, ale aby „drželi krok s děním“,

účet tam založený mají a alespoň sledují aktivitu svých přátel a známých (Ševčíková et al., 2014, s. 60).

4.1 Související statistiky

Tato podkapitola se zabývá statistikami týkajícími se toho, jak moc je v českých a evropských domácnostech rozšířené vlastnictví počítačů a připojení k internetu, což jsou základní podmínky pro to, aby děti vůbec mohly používat sociální sítě. Zmíněna jsou většinou jak data týkající se všech českých domácností, tak i data zaměřená na domácnosti, ve kterých je alespoň jedno dítě. Pro zajímavost jsou zmíněna i data domácností s jedním dítětem a domácností se dvěma a více dětmi, kde je však rozdíl minimální. V další části jsou pak ukázána data o počtech jednotlivců v ČR, kteří vlastní počítač a internet, a statistiky osob v České republice, jež používají sociální sítě. V závěru jsou zmíněna data porovnávající státy na úrovni celé Evropské unie. Data byla převzata od Českého statistického úřadu (dále jen ČSÚ). Porovnáván je vždy současný stav z konce roku 2020 (případně 2019, pokud v době dokončování této práce ještě nebyla zveřejněna aktuálnější data) s údaji deset let starými, tj. z roku 2010. Do tabulek byla zároveň doplněna i data za období 2017–2019, aby byl alespoň částečně naznačen postupný vývoj i v kratších časových úsecích.

	2010	2017	2018	2019	2020
Celkem	59,3	76,3	78,4	77,9	78,7
Domácnosti s dětmi celkem	84,8	94,6	95,8	94,2	95,8
Domácnosti s 1 dítětem	85,3	95,1	95,8	95,8	96,2
Domácnosti se 2 a více dětmi	83,8	94,1	95,7	92,2	95,2

Tabulka 1 – Statistika ČSÚ: Domácnosti v ČR s počítačem, vybrané údaje z tabulky (v %, podíl z celkového počtu domácností v dané skupině)¹⁶

Podle statistiky ČSÚ z listopadu roku 2020 (viz *tabulka 1*) vlastní 78,7 % všech domácností v České republice počítač. V domácnostech, kde žije alespoň jedno dítě, má v současné době počítač dokonce 95,8 % z nich. O deset let dříve, tedy v roce 2010 vlastnilo

¹⁶ ČSÚ, 2020. *Domácnosti v ČR s počítačem – vývoj v čase* [tabulka]. [cit. 2020-11-29]. Dostupné z: <https://www.czso.cz/documents/10180/122362692/0620042013.pdf/2c205a15-7a6e-439f-866d-df330e9ea76b?version=1.1>

počítač pouze 59,3 % domácností, ale pokud hovoříme o domácnostech, ve kterých žilo alespoň jedno dítě, mělo již v roce 2010 počítač 84,8 % z nich. V průběhu let můžeme sledovat postupný nárůst k současnemu stavu.

Další ze statistik ČSÚ (viz *tabulka 2*) se zaměřuje na počet domácností s připojením k internetu. Těch bylo před deseti lety, v roce 2010, 56,0 %, v současnosti je to 81,7 %. Z domácností, ve kterých žije alespoň jedno dítě, bylo již v roce 2010 k internetu připojeno 79,8 %, nyní, o deset let později, je to 98,5 % domácností.

	2010	2017	2018	2019	2020
Celkem	56,0	77,2	80,5	81,1	81,7
Domácnosti s dětmi celkem	79,8	95,2	97,8	97,2	98,5
Domácnosti s 1 dítětem	80,9	96,6	97,9	97,5	99,2
Domácnosti se 2 a více dětmi	77,0	95,1	97,7	96,9	97,7

Tabulka 2 – Statistika ČSÚ: Domácnosti v ČR s připojením k internetu, vybrané údaje z tabulky (v %, podíl z celkového počtu domácností v dané skupině)¹⁷

Následující část se zaměřuje na data ČSÚ, která popisují jednotlivé osoby, jež v českých domácnostech žily v roce 2019, vlastnily počítač a měly připojení k internetu. Zároveň je zde ještě rozděleno, kolik osob vlastní stolní počítač a kolik notebook nebo tablet (viz *tabulka 3*).

Data v této tabulce jsou dále rozdělena podle čtyř různých kritérií – podle pohlaví, dosaženého vzdělání, ekonomické aktivity a věkové skupiny. Pro účely této práce byla použita poslední zmíněná část zaměřená na věkové skupiny. Je patrné, že mezi dětmi a dospívajícími (věkové kategorie 10–15 let a 16–24 let) většina z nich vlastní jak počítač, tak disponuje připojením k internetu. Konkrétně 1 058 tis. z nich vlastní počítač a 1 389,2 tis. má připojení k internetu. Ve všech měřených kategoriích se hodnoty pohybují nad 90 %, pouze v případě stolních počítačů se procento pohybuje okolo 50 %. Z toho je patrné, že děti a dospívající častěji vlastní nějaké přenosné zařízení (notebook, tablet), které si mohou brát s sebou do školy, ke kamarádům apod.

¹⁷ ČSÚ, 2020. *Domácnosti v ČR s internetem – vývoj v čase* [tabulka]. [cit. 2020-11-29]. Dostupné z: <https://www.czso.cz/documents/10180/122362692/0620042014.pdf/e1d043ea-4b41-4b3c-8149-149ac9410343?version=1.1>

Pro porovnání je ještě třeba zmínit, že i v kategorii dospělých (25–54 let, v tabulce rozepsáno ve věkových skupinách po deseti letech) jsou sledována čísla obdobná těm u dětí a dospívajících. Ve všech kategoriích kromě té zaměřené na stolní počítače se tedy čísla pohybují nad 90 %. Změny lze pozorovat až u osob starších 55 let, kdy hodnoty všech sledovaných parametrů postupně klesají (často až pod hranici 50 %), takže lze jednoznačně říci, že starší osoby vlastní počítač a připojení k internetu mnohem méně často než mladší.

	Počítač (celkem)	Stolní počítač	Přenosný počítač (notebook či tablet)	Internet
Celkem	82,6 %	39,3 %	72,8 %	85,3 %
10–15 let	90,7 %	45,9 %	85,9 %	96,4 %
16–24 let	95,9 %	51,0 %	92,5 %	97,8 %
75+	35,8 %	19,0 %	25,2 %	35,0 %

Tabulka 3 – Statistika ČSÚ: Jednotlivci v ČR žijící v domácnostech s počítačem a internetem, 2019, vybrané údaje z tabulky (v %, podíl z celkového počtu jednotlivců v dané socio-demografické skupině)¹⁸

Na webových stránkách ČSÚ je možné dohledat i statistiku, která porovnává domácnosti zemí v Evropské unii na základě toho, kolik z nich má připojení k internetu.¹⁹ Tato data zatím nejsou aktuální z letošního roku, nejnovější informace o domácnostech s internetem je z roku 2019. Ale i na základě toho si lze představit, jak je na tom Česká republika v porovnání s ostatními zeměmi.

Co se týče domácností v zemích EU s internetem, tak průměrně mělo v roce 2019 internet 90,5 % domácností. Česká republika je jen těsně pod tímto průměrem s 87,0 %. Nejlépe je na tom Nizozemsko s 98,4 %, následováno Dánskem s 95,4 %, Lucemburskem s 95,2 % a Finskem s 94,4 %. Nejnižší počet domácností s připojením k internetu je pak v Bulharsku, kde je to pouhých 75,1 %.

¹⁸ ČSÚ, 2019. *Jednotlivci v ČR žijící v domácnostech s počítačem a internetem* [tabulka]. [cit. 2020-07-29]. Dostupné z: <https://www.czso.cz/documents/10180/90577057/062004190114.pdf/d67b508f-a51c-4933-b165-b57062146d5a?version=1.1>

¹⁹ ČSÚ, 2019. *Domácnosti v zemích EU s internetem – vývoj v čase* [tabulka]. [cit. 2020-11-29]. Dostupné z: <https://www.czso.cz/documents/10180/122362692/062004200113.pdf/29a6bb28-53c5-4dc1-ae45-eeb29b935d5e?version=1.1>

Další tabulka ČSÚ se zabývá počtem osob v ČR, které používají sociální sítě.²⁰ Zde je uvedeno, že v současné době, tj. v roce 2020, používá sociální sítě 53,8 % osob starších 16 let. O rok dříve to bylo o něco málo více, tedy 54,0 %. Velký nárůst je vidět zejména v porovnání s rokem 2010, kdy v České republice používalo sociální sítě pouze 9,4 % osob starších 16 let.

Dle statistik Evropské unie (viz *tabulka 4*) používá sociální sítě v České republice 58,9 % osob ve věku mezi 16 a 74 lety, což je nad evropským průměrem, který činí 56,6 % osob. Nejvyšší čísla má Dánsko, kde sociální sítě používá 80,8 % obyvatel, na druhém místě je Belgie se 75,5 %, na třetím Velká Británie se 73,1 % a na čtvrtém Švédsko se 72,2 % obyvatel. Na druhém konci žebříčku se umístila Francie s Itálií – v obou těchto zemích používalo v roce 2019 sociální sítě 42,3 % obyvatel. V roce 2011 (starší data nebyla v tabulce od ČSÚ dostupná) byla čísla ve všech zmíněných státech nižší (viz *tabulka 4*). V Evropské unii tehdy používalo sociální sítě průměrně 37,7 % obyvatel.

	2011	2017	2018	2019
Celkem	37,7	54,3	55,8	56,6
ČR	26,7	48,3	55,6	58,9
Dánsko	55,4	75,5	78,6	80,8
Belgie	39,5	72,0	72,6	75,5
Velká Británie	49,7	71,2	69,7	73,1
Švédsko	53,6	70,8	70,4	72,2
Francie	35,5	42,8	41,9	42,3
Itálie	26,3	43,4	46,5	42,3

Tabulka 4 – Statistika ČSÚ: Osoby v zemích EU používající sociální sítě – vývoj v čase, 2019, vybrané údaje z tabulky (v %, podíl z celkového počtu osob ve věku 16-74 let v daném státě)²¹

4.2 Specifika chování teenagerů (nejen na sociálních sítích)

Jelikož současní teenageři žijí ve světě, kterému technologie včetně sociálních sítí dominují, je logické, že si na ně zvykli lépe a rychleji než dospělí (boyd, 2017, s. 27). I z toho důvodu se objevily dva nové pojmy, které tyto dvě skupiny uživatelů technologií rozdělují –

²⁰ ČSÚ, 2020. *Osoby v ČR používající sociální sítě*, [tabulka]. [cit. 2020-11-29]. Dostupné z: <https://www.czso.cz/documents/10180/122362692/0620042052.pdf/76f76896-4758-480a-8856-9d6658534cba?version=1.1>

²¹ ČSÚ, 2019. *Osoby v zemích EU používající sociální sítě – vývoj v čase* [tabulka]. [cit. 2020-11-29]. Dostupné z: <https://www.czso.cz/documents/10180/122362692/0620042055.pdf/59e558f6-ba0b-4156-84ad-8f0fec616308?version=1.1>

digitální přistěhovalci (v angličtině *digital immigrants*) a *digitální rodáci/domorodci* (v angličtině *digital natives*) (Uhls, 2018, s. 26). Tyto pojmy poprvé použil na začátku tisíciletí americký pedagog a publicista Marc Prensky. Pojmem *digital natives* označil generaci těch, kteří se narodili po roce 1980, tedy ty, kteří se již od útlého dětství setkávali, jako se samozřejmou součástí života, s technologiemi jako jsou počítač a internet (Spitzer, 2012, s. 185). Dnešní děti již téměř neznají život, ve kterém by neměly k dispozici mobilní telefon a internet (Ševčíková et al., 2014, s. 19).

Socializování dnešních dětí a teenagerů se velmi zásadně odlišuje od toho, jak tomu bylo u jejich rodičů a prarodičů. Je tomu zcela očividně proto, že je ovlivňuje elektronické komunikování skrze e-maily a zejména pak prostřednictvím sociálních sítí, hlasových a video hovorů, ale také každodenní hraní videoher a mnohá další specifika této doby. Marc Prensky ve svém článku *Do They Really Think Differently?* z roku 2001 hovoří o tom, že již jeho současná generace na základě výše zmíněných podnětů skutečně myslí jinak, a že to dokonce způsobuje změny na jejich mozcích a v souvislosti s tím od života také očekávají něco jiného než předchozí generace (Prensky, 2001, s.1).

Kromě označení *digital natives* se pro tuto generaci vžilo i označení *generace Y*, *millenials* (česky *mileniálové*) nebo také *net generation* (česky *síťová generace*) (Spitzer, 2012, s. 185). Osvojení dovedností spojených s využíváním technologií a sociálních sítí se pro děti a teenagery stalo dokonce nutným předpokladem (boyd, 2017, s. 27). Jejich osobnosti jsou formovány na základě odlišných zkušeností, než tomu bylo u jejich rodičů.

Dle Dona Tapscotta existuje několik faktorů, které tuto síťovou generaci tolik odlišují od těch předchozích. Prvním je jejich všeobecná touha po svobodě ve všem, což souvisí hned s druhým bodem, který se týká jejich touhy moci si všechno přizpůsobit svým potřebám. Vše zkoumají, vyžadují poctivost a chtějí se bavit. Jsou zvyklí vzájemně spolupracovat, jsou rychlí v komunikaci i získávání informací a milují inovace – ať už se sami pokouší něco vytvářet a vylepšovat nebo jen využívají nejnovější funkce a technologie (Tapscott, 2009, str. 35).

Internet do jejich života vstoupil s mnohým pozitivním, ale přinesl s sebou i řadu nových rizik, se kterými se musí generace dnešních dětí vypořádat (Whitty a Young, 2017, s. 84). Již pro ně neexistuje rozdíl mezi „reálným“ a „online“ životem – jejich online identita zdánlivě odpovídá té reálné a jejich aktivita online s ostatními se vztahuje i ke vztahům z běžného života (Uhls, 2018, s. 106). Prostě a jednoduše: teenageři se snaží být součástí tohoto nového světa a na rozdíl od předchozích generací se tento svět nesnaží tolik analyzovat

a porovnávat s tím předchozím. Pro teenagery je zásadní ona online veřejnost, pro dospělé spíše samotná online technologie (boyd, 2017, s. 27). Z výzkumu, který prováděla v rámci své diplomové práce Lucie Svobodová vyplynulo, že hlavním důvodem pro to, aby teenageři využívali sociální sítě, je právě komunikace s přáteli a prohlubování a zachovávání vazeb, které mezi sebou mají z „reálného světa“ (Svobodová, 2016, s. 57).

Teenageři se často nebojí sdílet na internetu množství osobních informací (Uhls, 2018, s. 110) a pravděpodobně si často neuvědomují nebo zapomínají, že sice sdílejí to, co se bude líbit jejich vrstevníkům, spolužákům a kamarádům, ale mohou to vidět i dospělí. Mállokterí jsou schopni vůbec odhadnout, kolik lidí se k jejich příspěvkům může dostat (Uhls, 2018, s. 118). Bývá doporučováno to, aby rodiče sledovali své děti na sociálních sítích, například aby si je přidali na Facebooku *do přátel*, a mohli tak alespoň částečně kontrolovat, jak se tam děti chovají a co vlastně sdílejí online (Mullen, 2016, s. 165–172). Tomu se však děti často aktivně brání. A většinou jim vadí i jenom to, že se jim rodiče občas pokouší koukat přes rameno, když si píšou s kamarády, natož aby si prohlíželi jejich profily (boyd, 2017, s. 73). Není až tak překvapivé, že přílišná snaha rodičů sledovat veškeré chování svých potomků může narušit jejich vzájemný vztah. Děti mohou považovat onu *žádost o přátelství* na Facebooku jako něco, co vlastně nemohou odmítnout, protože by si rodiče mohli myslet, že na síti dělají něco špatného. Ale zároveň ji většinou ani nechtějí přijmout, protože považují sociální sítě spíše za prostor pro budování vztahů s vrstevníky (Mullen, 2016, s. 165–172).

Yalda Uhls ve své knize *Mediální mámy a digitální tátové* z roku 2018 poukazuje na to, že 71 % adolescentů uvádí na internetu název své školy a místo bydliště., 53 % svou e-mailovou adresu a 20 % své telefonní číslo (Uhls, 2018, s. 110). Ve výzkumu od společnosti McAfee, která se orientuje právě na bezpečnost na internetu a poskytuje mimo jiné i antivirové programy, bylo zjištěno, že až 46 % dětí a mladých dospělých (do 21 let) by změnilo své počínání na sociálních sítích, kdyby věděli, že jejich příspěvky mohou vidět rodiče (Uhls, 2018, s. 118).

Pro to, aby se děti a teenageři dokázali vyrovnat s nástrahami internetu a sociálních médií potřebují především od rodičů, ale také ve škole vedení k *digitální a informační gramotnosti* (Uhls, 2018, s. 185). Nesmíme zapomínat, že ač se zdá, že děti a teenageři se vše související s technologiemi učí rychleji než cokoli dalšího, nemusí nutně hned pochopit pravidla související s digitální gramotností, a je proto nezbytné, aby jim s tím dospělí pomohli. Teenageři by měli být schopni zamýšlet se a kriticky zhodnotit jak to, co na internetu a sociálních sítích konzumují, tak i to, co tam sami vytváří a sdílí s ostatními (boyd, 2017, s. 216). Potřebují se naučit fungovat ve světě, který bude jejich součástí po celý život a orientace v něm je nutným předpokladem. (boyd, 2017, s. 27). Potřebují vědět, jak chránit

svou bezpečnost, jak funguje *digitální stopa* a jak se vůbec na internetu prezentovat. Zároveň potřebují poradit, jak se vyhnout různým dalším rizikům – měli by například znát alespoň základní pravidla související s autorskými právy a dokázali se tak vyvarovat například s plagiátorstvím (Uhls, 2018, s.185).

4.3 Dopady používání sociálních sítí

Je nezpochybnitelné, že internet a sociální sítě jsou pro dospívající velice lákavé a nabízejí jim množství skvělých příležitostí a možností. Sociální sítě přináší řadu výhod spojených se socializací. V současné době jsou k dispozici různé nástroje pro komunikaci – od e-mailu, přes chatovací aplikace až po nástroje, které umožňují videohovory. Uživatelé internetu mohou být neustále ve spojení s ostatními, zároveň mohou technologie využívat i pro zábavu a vzdělávání – k dispozici jsou jim různé kreativní nástroje, díky kterým se mohou dospívající mnohé naučit, ale také spousta zábavných her. V neposlední řadě může být obsah na internetu pro děti a dospívající i zdrojem informací, jelikož je zde množství jak odborných článků, tak také rad od ostatních.

Na druhou stranu je ale nezbytné nezapomínat, že zároveň přináší i rizika, ke kterým je záhodno přistupovat zodpovědně a před kterými by děti měly být varovány svými rodiči a učiteli. A jelikož jsou technologie něčím, co bude tyto děti skutečně provázet celým jejich životem, nejsou řešením těchto rizik například zákazy používání internetu. Mnohem přínosnější je komunikace a edukace, která dětem osvětlí, proč by se měly toho daného rizika obávat a jak se před ním ochránit (Whitty a Young, 2017, s. 76).

4.3.1 Přínosy sociálních sítí

Moderní technologie v čele s internetem a sociálními sítěmi a schopnost s nimi pracovat jsou pro současné teenagery téměř nezbytností a zároveň jsou velmi přínosné pro budoucí život, jelikož téměř v každé oblasti, ve které se budou pohybovat a pracovat, budou alespoň částečně tyto technologie využívat. Tyto schopnosti a dovednosti jsou užitečné i z toho důvodu, že rozvíjejí způsob myšlení a schopnosti jako je *informační* a *mediální gramotnost*, které jsou v dnešní době nezbytné (Whitty a Young, 2017, s. 76).

Mezi hlavní výhody a přínosy, které sociální sítě svým uživatelům nabízejí patří (Sociální sítě, 2012):

- jejich schopnost spojovat lidi a udržovat kontakty,
- možnosti snadného získávání nových přátel,

- rychlá, jednoduchá a časově neomezená komunikace a
- neomezený a nepřetržitý přístup k informacím.

Hlavní výhodou sociálních sítí je jejich schopnost spojovat velké skupiny lidí a pomoc při udržování kontaktů. Nikdy dřív nebylo jednodušší spojit se například se vzdáleným příbuzným, s bývalými spolužáky, s přítelem z dětství, který se odstěhoval na druhý konec republiky apod. Sociální sítě umožňují nejen uchovávat kontakty na tyto osoby, ale jejich uživatelé také mohou sledovat aktivitu ostatních, díky čemuž již nebude takovým problémem dohledat například spolužačku, která si po svatbě změnila jméno. Sociální sítě jsou zároveň místem, kde lze najít nové přátele z celého světa, a to například na základě členství ve stejné skupině. Na Facebooku například existuje velké množství skupin zaměřených na rozmanité koníčky, obory či sdílení zkušeností, díky čemuž je opravdu jednoduché seznámit se s někým, kdo má podobné zájmy. Komunikace s ostatními je navíc na sociálních sítích velice rychlá, jednoduchá a časově neomezená (Sociální sítě, 2012).

Další výhodou je nepřetržitý a neomezený přístup k informacím z celého webu, které jsou na sociálních sítích propojovány (Sociální sítě, 2012). V současnosti již není třeba procházet řadu zpravodajských webových stránek. Na Facebooku například stačí, když uživatel sleduje svá oblíbená média a jejich příspěvky se mu budou zobrazovat přímo na hlavní stránce. Pokud je uživatel-teenager dostatečně informačně a mediálně gramotný, může být toto nepřehledné množství informací i dobrým vzdělávacím zdrojem. (Whitty a Young, 2017, s. 76). Tyto informace mohou být díky sociálním sítím uživateli jednoduše a efektivně sdíleny ostatním (Sociální sítě, 2012).

4.3.2 Asociovaná rizika a možné hrozby na sociálních sítích

Kromě přínosů a výhod jsou sociální sítě bohužel spojeny i s řadou rizik, která mohou velmi negativně ovlivnit životy a budoucnost nejenom teenagerů, ale také dospělých. Internet a sociální sítě sice mohou být zdrojem mnohých užitečných informací, nesmíme však zapomínat na to, že jsou zároveň plné zkreslených informací a dezinformací, které mohou být pro děti a dospívající často velmi těžko rozpoznatelné. Je proto nezbytné, aby se již ve škole setkali s výukou *mediální a informační gramotnosti*, které jim mohou pomoci tyto dezinformace rozpoznat (Whitty a Young, 2017, s. 76). Důležité je si uvědomit, že každé sdílení osobních údajů, myšlenek, fotografií apod. většinou nemusí být možné vzít zpět.

Bývá doporučováno například „nezveřejňovat o sobě na internetu to, co byste nezveřejnili na sloupu veřejného osvětlení“ (Sociální sítě, 2018).

Sdílení velkého množství údajů o sobě může stále častěji vést k různým rizikům, která by si uživatelé internetu a sociálních sítí měli uvědomovat. Některé publikované informace mohou následně vést k rozepřím a narušit vztahy, ale stále častěji se hovoří i o tom, že *digitální stopa* na internetu může být překážkou k přijetí na vysokou školu, úspěchu při hledání nového zaměstnání nebo představuje podnět k výpovědi. Některé údaje mohou vést k vydírání či vyhrožování. V prostředí škol se stále častěji mluví o takzvané kyberšikaně (Ševčíková et al., 2014, s. 56). Jsou známé také případy, kdy si lupiči vytipovali byty nebo domy na základě sdílení fotografií interiérů, oznámení cesty na dovolenou apod. (Sociální sítě, 2018).

Děti a teenageri jsou na internetu často terčem podvodného jednání, jelikož bývají snáze ovlivnitelní. Za příslib videohry zdarma často bez přemýšlení vyplní osobní informace, které mohou být následně zneužity. Monica Whitty a Garry Young ve své knize popisují několik názorných situací, jak mohou být informace následně zneužity. Popisují zde například, jak bývají podváděni prarodiče těchto dětí, a to právě na základě zcizených údajů svých vnuků a vnuček. Tito podvodníci se vydávají právě za děti a teenagery, kontaktují „své“ prarodiče s prosbou o peníze, jelikož „ztratili peněženku“ apod. (Whitty a Young, 2017, s. 79).

V publikaci *Děti a dospívající online: vybraná rizika používání internetu* Anna Ševčíková spolu s kolegy popisuje například rizika nadměrného užívání a závislosti na internetu, ale především rizika související s navazováním kontaktů v online světě a s tím spojeným obtěžováním a kyberšikanou, ale také se sebe-odhalováním se a ztrátou soukromí (Ševčíková et al., 2014, s. 5). Online rizika pro děti a dospívající zde autoři dále rozdělují do přehledné tabulky podle autorek *Sonie Livingstone* a *Leslie Haddon* z roku 2009. Typy rizik jsou zde rozděleny do čtyř kategorií, z nichž každá je pak v tabulce rozepsána podle toho, jaká rizika se objevují v případě, že je *dítě příjemcem, účastníkem* nebo „*pachatelem*“. Tato tabulka (viz v *tabulce 5*) je sice zaměřena zejména na rizika pro děti a dospívající, ale obdobná rizika mohou hrozit i ostatním uživatelům internetu a sociálních sítí. Vždy je to závislé především na zkušenostech a znalostech prostředí online světa, ale také na prostředí, ve kterém člověk žije – v jaké sociální skupině se pohybuje, jak často má přístup k internetu, co na internetu sleduje a jaké webové stránky používá, s kým tam komunikuje apod.

Na základě této tabulky lze i určit, které ze zmíněných rizik souvisí se sledovanou problematikou soukromí. Svým způsobem mohou soukromí ovlivnit všechny čtyři sledované kategorie rizik, tedy komerční, násilné, sexuální i rizika související s osobními hodnotami.

Typ rizika	Obsah: dítě jako příjemce	Kontakt: dítě jako účastník	Počínání: dítě jako pachatel
Komerce	reklama, spam, nabádání k poskytování peněžní podpory	získávání a uchovávání osobních údajů	gambling, nelegální stahování, hackování
Násilí	násilí, nenávistný či děsivý obsah	oběť kyberšikany, online obtěžování a pronásledování	pachatel kyberšikany, online obtěžování či pronásledování
Sexualita	pornografie a jiný sexuálně zraňující obsah	setkávání s neznámými lidmi z internetu, sexuální zneužívání	vytváření a nahrávání pornografických materiálů
Hodnoty	rasistické a jiné zkreslené, zavádějící informace či rady (př. drogy)	sebepoškozování, přesvědčování a manipulace ze strany druhých	poskytování (zavádějících) rad např. ohledně hubnutí nebo sebevraždy

Tabulka 5 – Klasifikace online rizik (Ševčíková et al., 2014, s.10)

Rizika z kategorie **komerce** ohrožují soukromí zejména v tom smyslu, že na základě získávání a uchovávání osobních údajů na stránkách, kde je uživatel registrovaný (např. na Facebooku), mu mohou být následně zobrazovány personalizované reklamy. Právě na zmiňovaném Facebooku jsou například uživatelům zobrazovány reklamy na základě uvedeného věku, místa bydliště, aktuální lokality a podobně. Zároveň může být sledována aktivita na webu, na jejímž základě se budou zobrazovat relevantní reklamy. Není tedy neobvyklé, že pokud uživatel shání nějaký produkt a vyhledává ho v nabídkách e-shopů, budou se mu následně zobrazovat reklamy právě na hledaný druh sortimentu.

Druhá kategorie se zabývá rizikem **násilí**, kdy se dítě (nebo i jiná osoba) může stát obětí kyberšikany, tedy se zamýšleného a opakovaného ubližování, které je způsobováno komunikací přes moderní technologie. Kyberšikana může přicházet jak ze strany osob, se kterými se oběť zná i z běžného života (např. spolužáci), tak i od úplně neznámých osob. Oběť bývá nejenom obtěžována nenávistnými zprávami, ale také o ní často bývají veřejně vystavovány i soukromé informace a fotografie.

Děti a teenageři se s kyberšikanou na sociálních sítích setkávají stále častěji. Mohou to být například zlomyslné poznámky nebo dokonce vydírání ze strany druhých osob, což často vede k tomu, že se na sociální síť dostanou velice nepříjemné informace týkající se soukromí, například fotografie, které dotyčný nikdy nechtěl sdílet s ostatními apod. A anonymita internetu a sociálních sítí kyberšikanu bohužel spíše podporuje a bývá velice obtížné se s ní vypořádat

(Whitty a Young, 2017, s. 78). Ač často bývá kyberšikanována často způsobována spolužáky, které šikanované děti znají i z offline života, hrozí jim na sociálních sítích i nebezpečí ze strany lidí, které ani nemusejí osobně znát. V poslední době se u nás značně diskutuje o sexuálním zneužívání dětí po internetu, a to hlavně v souvislosti s premiérou filmu *V síti*, který poukazuje právě na tuto problematiku.

Monica Whitty a Garry Young ve své knize rozlišují vytváření a sdílení dětských pornografických materiálů, oslovování dětí na sítích a vyžadování fotografií a dalšího kontaktu s nimi (Whitty a Young, 2017, s. 170). Právě výše zmíněný film velmi názorně poukázal na to, kolik lidí na sociálních sítích oslovuje děti třeba jen na základě fotografie a informací o věku.

Co se týče další kategorie nazvané **sexualita**, která úzce souvisí s předchozím bodem, tak i ta může zasahovat do soukromí uživatelů, a to zejména v případě, že se dítě (oběť) s neznámým člověkem z internetu či sociálních sítí setká osobně. V tom případě mu může hrozit sexuální zneužití. Může být také donuceno k vytváření a zasílání pornografických materiálů, což může zasáhnout do soukromí ovlivnit i budoucí život, zejména v tom případě, pokud druhá osoba tyto materiály dále zveřejní.

I kategorie **hodnot** popisuje rizika, která mohou soukromí ovlivnit, a to v tom smyslu, že oběti těchto rizik mohou být manipulovány ze strany druhých osob například k sebepoškozování, k nenávisti nebo dokonce k sebevraždě.

Ve publikaci *Děti a dospívající online* pak následuje překlad modelu *EU Kids Online*,²² který popisuje propojení rizik se způsoby, jakými děti a dospívající internet používají. Tento výzkum byl uskutečněn v roce 2010²³ s podporou Evropské komise díky programu *Safer Internet*. Do výzkumu se včetně České republiky se zapojilo dvacet pět evropských zemí.

V modelu *EU Kids Online* jsou odděleny tři úrovně vlivů, které děti a jejich chování na internetu ovlivňují. První úroveň je individuální a zahrnuje to, jak psychosociální charakteristika dítěte působí na jeho chování na internetu. Do druhé úrovně pak patří blízké okolí dítěte, jako jsou rodiče, škola a vrstevníci, kteří také mají zásadní vliv na způsob jeho jednání v online světě. Poslední, nejvyšší úroveň obsahuje ovlivňující faktory na národní

²² LIVINGSTONE, Sonia, Leslie HADDON, Anke GÖRZIG, and Kjartan ÓLAFSSON, 2011. *Risks and safety on the internet: the perspective of European children: full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries*. EU Kids Online: London [online]. [cit. 2020-07-03]. Dostupné z: <http://eprints.lse.ac.uk/33731/>

²³ Výzkum *EU Kids Online* je pravidelně opakován. Jeho poslední verze je zmíněna v kapitole 4.5 *Stávající stav výzkumu o chování teenagerů na sociálních sítích ve vztahu k ochraně soukromí*.

úrovni a patří sem socioekonomická stratifikace, informační a komunikační infrastruktura, právní rámec, vzdělávací systém a kulturní hodnoty a postoje.

V modelu je zároveň jasně znázorněno, že způsoby chování jednotlivce jsou velice úzce navázány na potenciální rizika. Blízké okolí může do jisté míry ovlivňovat, jak budou děti a dospívající internet používat, mohou regulovat čas, který touto činností stráví. Toto všechno je však ovlivněno vlivy na národní úrovni (viz výše), které se liší jak v jednotlivých státech, v některých případech i v jednotlivých regionech či menších celcích. Z tohoto modelu vyplývá, že při zkoumání online rizik by neměl být opomíjen i kontext, který může vést k lepšímu porozumění, proč jsou v některých oblastech rozšířenější jiná rizika než jinde. Děti a dospívající kteří jsou nějakým způsobem znevýhodněni v běžném životě, se mohou s online riziky setkávat častěji. Zároveň čím více mohou děti internet a sociální sítě používat, tím je vyšší pravděpodobnost, že se s některým rizikem setkají (Ševčíková et al., 2014, s. 12).

Na serveru *Internetem bezpečně* (internetembezpecne.cz) je dostupné „Desatero bezpečného užívání sociální sítě“, které ve dvanácti bodech přehledně shrnuje základní pravidla, jak by se měli (nejenom) teenageři na sociálních sítích chovat (Sociální sítě, 2018):

1. *„Přečtěte si podmínky užívání sociální sítě před registrací a zjistěte, jak bude nakládáno s Vašimi osobními údaji ze strany provozovatele (zda nebudou poskytovány třetím stranám).*
2. *Čím méně toho o sobě při registraci vyplníte, tím je menší riziko, že se vám něco stane.*
3. *Naučte se nastavovat různá práva svým přátelům – např. svým spolupracovníkům (pozn. v případě teenagerů například spolužákům) nastavte nižší než členům rodiny.*
4. *Nesdílejte své intimní fotografie. Mohou být zneužity.*
5. *Nesdílejte komentáře ani statusy, které mohou být použity proti vám – např. pomlouvat nadřízeného v pracovní době.*
6. *Pokud pojedete na delší dobu mimo své obydlí, nesdílejte tuto skutečnost, leda až po návratu.*
7. *Zapněte kontrolu obsahu a příspěvků, kde jste označeni.*
8. *Neposkytujte hrám a dalším aplikacím obsaženým v sociálních sítích své osobní údaje – např. informace o poloze nebo seznam přátel.*
9. *Pravidelně v nastavení zabezpečení kontrolujte, na jakém zařízení jste přihlášení – zda jste se někde (např. ve škole nebo v práci) nezapomněli odhlásit.*

10. *Potvrzujte přátelství pouze osobám, které znáte.*
11. *Cokoliv vložíš na sociální síť, již zpravidla nelze vymazat!*
12. *Neužívejte funkci přihlášení do jiných online služeb pomocí svého účtu na sociální síti – např. přihlášení do internetového obchodu pomocí FB účtu – předáváte své přihlašovací údaje třetí osobě!!!“*

4.4 Zdroje a programy

Aby se teenageři dokázali orientovat ve světě internetu a sociálních sítí a chránit tam své soukromí, potřebují pomoc, která by měla pocházet zejména ze strany rodičů a učitelů. Často se však může stát, že rodiče a učitelé sami nemají dostatek zkušeností, a je tedy potřeba, aby teenageři získali tyto informace i jinde. Tato kapitola se zaměřuje právě na vybrané zdroje a programy, které mají za cíl vzdělávání (nejenom) dětí a teenagerů ohledně bezpečnosti na internetu a sociálních sítích. Všechny se snaží nějakým způsobem radit a vysvětlovat, jaká rizika dětem a teenagerům hrozí, a hlavně jak se jim mohou bránit. Zdroje a programy jsou řazeny abecedně, a byly vybrány zejména na základě českého původu, a tedy srozumitelnosti pro teenagery z našeho prostředí, na které se zaměřuje praktická část této práce.

Bud' safe online (budsafeonline.cz) je projekt technologické firmy Avast a influencer²⁴ Jirky Krále. Funguje pod záštitou Ministerstva školství, mládeže a tělovýchovy (dále jen MŠMT), je nevýdělečný a zaměřuje se na žáky základních škol a jejich vzdělávání a prevenci v oblasti bezpečnosti na internetu. Projekt získal již řadu ocenění, například Cen SDGs 2019, Effie Awards 2019 a WebTop100. Pořádají pro děti interaktivní workshopy a na konkrétních příkladech jim vysvětlují, jak předcházet rizikům souvisejícím s používáním moderních technologií. Zároveň mají přehledné webové stránky, kde sdílejí články a videa zaměřená na jednotlivé typy hrozeb. Od roku 2020 poskytují také interaktivní online kurz, který je dostupný na webu a učitelé ho mohou využívat ve výuce.

Portál **E-bezpečí** (e-bezpeci.cz) provozuje Centrum prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci. Zaměřuje se především na problémy spojené s rizikovým chováním na internetu, na kyberšikanu, ale také na rizika sociálních sítí a zneužívání osobních údajů. Jejich cílovou skupinou jsou nejen žáci a studenti, ale i jejich učitelé a rodiče, včetně metodiků prevence, vychovatelů a policistů.

²⁴ **Influencer** je pojem, který označuje člověka, jenž dokáže ovlivnit velké množství lidí. Nejčastěji se tento pojem pojí s youtubery a instagramery, kteří mají vliv na své fanoušky a firmy jim často platí za marketingovou propagaci svých produktů (Rostecký, 2018).

Hlavním partnerem projektu E-bezpečí je telekomunikační společnost O₂, která sama provozuje portál zaměřený na internetovou bezpečnost a mediální gramotnost – **O₂ Chytrá škola** (o2chytraskola.cz). Je to také portál pro děti, rodiče i pedagogy, který jim pomáhá získat přehled v digitálním světě.

V poslední době je společným a nejdiskutovanějším projektem E-bezpečí a O₂ Chytré školy filmový dokument *V síti*, který měl premiéru 27. února 2020 a zaměřuje se na sexuální hrozby, se kterými se děti mohou v internetovém prostředí setkat.

Projekt **bezpecnyinternet.cz** se snaží ukazovat rizika spojená s používáním internetu a možnosti obrany proti nim. Zaměřuje se na několik oddělených skupin uživatelů – na začátečníky, na pokročilé, na rodiče, na děti a na školy – a pro každou z nich poskytuje na svém webu relevantní informace. Hlavními partnery tohoto projektu jsou společnosti Česká spořitelna, Microsoft a Seznam.cz.

Další vybraný projekt se nazývá **Zvol si info** (zvolsi.info). Je to projekt studentů Masarykovy univerzity v Brně a je zaměřen především na mediální gramotnost a boj proti dezinformacím. Je orientován mimo jiné i na žáky základních škol, kterým pomáhá s kritickým myšlením a nástrahami sociálních sítí.

4.5 Stávající stav výzkumu o chování teenagerů na sociálních sítích ve vztahu k ochraně soukromí

Již od dob prvních sociálních médií vzniká obrovské množství literatury a výzkumů na toto téma, ale nesmíme zapomínat na fakt, že se jedná o velice rychle se rozvíjející technologii, tudíž pouze literaturu a výzkumy z posledních několika málo let lze považovat za relevantní. Ve spojení s problematikou ochrany soukromí (nejen) dětí a teenagerů na internetu a sociálních sítích je toto navíc v posledních letech diskutovaným a velice důležitým tématem.

Vybrané zdroje pocházejí například z těchto databází: ERIC, Political Science Complete, SocINDEX, SPORTDiscus with Full Text. Získané výsledky na základě klíčových slov byly následně omezeny obdobím mezi lety 2014 a 2020 a dostupností v anglickém a českém jazyce. Procházeny potom byly od nejnovějších po nejstarší a byly vybírány podle relevance s tématem této diplomové práce. Z těchto důvodů jsou zdroje použité pro tuto kapitolu pouze reprezentativním výběrem zejména za období od roku 2014 do současnosti. Některé vybrané výzkumy se zároveň zabývají i vyšší věkovou skupinou, než do které patří teenageři. Seřazené jsou vzestupně od nejstarších.

Významnou autorkou a výzkumnicí, která se zaměřuje na tuto problematiku je americká akademička danah boyd. V letech 2007 až 2010 provedla celkem 166 formálních polostrukturovaných rozhovorů s americkými teenagery, rodiči a učiteli, díky kterým se snažila porozumět způsobům, jak teenageři žijí v online světě. Své výsledky shrnula v publikaci z roku 2014 s názvem *It's complicated: The Social Lives of Networked Teens* (v českém překladu vyšla až v roce 2017 pod názvem *Je to složitější: sociální život teenagerů na sociálních sítích*). Hned v úvodu autorka uvádí, že si je vědoma toho, že v moment, kdy publikace vyšla, jsou již některé informace, které v ní uvádí zastaralé, jelikož vývoj sociálních sítí postupuje kupředu nesmírnou rychlostí. Zároveň si však myslí, že základní principy se až tolik nezmění, tudíž i v pozdější době bude mít její výzkum nějaký význam. Autorka se nejenom v této knize, ale i ve svých předchozích publikacích zabývá právě tématem sociálních sítí a informačního chování dětí a teenagerů. Ve zmíněné publikaci (boyd, 2017) se věnuje tématu soukromí teenagerů a jejich potřebě zveřejňovat informace o sobě celou kapitolu. Staví se zde kriticky k tvrzení, že dnešní teenageři se nezajímají o své soukromí. Zmiňuje zde souvislost se základní povahou sociálních sítí, tedy tím, že jejich primární funkcí je sdílet příspěvky veřejně s celou skupinou přátel. A teenageři jsou zvyklí sdílet s vědomím, že jejich příspěvky na Facebooku uvidí velké množství lidí. To ale neznamená, že by se o své soukromí nezajímali. Spíše zkrátka nechtějí vynakládat úsilí k tomu, aby omezili viditelnost svých příspěvků. Nemají důvod nezveřejnit přání k narozeninám a běžné rutinní komunikace, ale pokud spolu chtějí řešit něco, co má být soukromé, tak si zkrátka zvolí jiný komunikační kanál. boyd zde zároveň popisuje způsob, jakým dospívající píšou své příspěvky a zprávy. Ty jsou totiž mnohdy psané „šifrovaně“ tak, aby nezasvěcený člověk (rodič, učitel) nepoznal, čeho se týkají.

To přímo souvisí s dalším faktorem, který je v zde popisován. danah boyd píše o tom, jak se rodiče na jednu stranu snaží dětem vštěpovat nutnost chránit si své soukromí, ale na druhou stranu sami chtějí o svých dětech vědět vše, aniž by jim poskytovali prostor, kde děti soukromí mohou mít. Fakt, že dospívající většinou nechtějí mít na sociálních sítích v přátelích své rodiče, přirovnává k nalepení cedule *Nevstupovat* na dveře dětských pokojíčků. Snaha chránit své soukromí před dospělými tu byla již před příchodem sociálních sítí, nyní jen nabrala jiného rozměru. V další kapitole se zaměřuje na to, že mnozí teenageři (ale je to strategie i slavných osobností) o sobě sdílejí informace právě proto, aby ochránili své soukromí. Došli totiž k závěru, že když o sobě sdílí alespoň něco, případně to sdílí tak, aby to vypadalo, že sdílí to důležité ze svého života, zajistí si, že o nich nebude kolovat žádná jiná informace – sdílí tedy proto, aby nad nimi ostatní ztratili moc (boyd, 2017).

Další významné výzkumy ve zkoumané oblasti provedla společnost *Livingston Research*. V roce 2014 uskutečnili dva výzkumy, první z nich pod názvem *Developing Social Media Literacy* a druhý ve spolupráci s *EU Kids Online* a *Net Children Go Mobile* zaměřený na téma rizik a příležitostí v online světě pro děti. Obou těchto výzkumů se účastnili děti a teenageři ve věku mezi 9 a 16 lety. Počet účastníků prvního výzkumu nebyl uveden, druhého se zúčastnilo formou rozhovorů téměř 29 tis. respondentů z různých národů a regionů Evropské unie. Zaměřen byl nejenom na sociální sítě, ale i na používání internetu. Z těchto výzkumů vyplývá, že pouze 43 % dětí mělo v té době nastaveny profily na svých sociálních sítích tak, že jimi sdílený obsah viděli pouze jejich *přátelé* (tj. schválení sledující). Profily 28 % z nich mohli sledovat i přátelé jejich přátel a 26 % dětí mělo podle výše zmíněných výzkumů profil nastavený jako veřejně dostupný pro kohokoliv. Pouze 9 % dětí ve věku 11 až 16 let pak uvedlo, že jejich data byla někdy zneužita. Výzkum z roku 2014 zjišťuje například to, že 79 % teenagerů ve věku od 14 do 16 let ví, jak nastavovat a měnit nastavení soukromí na svých sociálních sítích (Willoughby, 2019).

Z roku 2014 stojí za zmínku ještě jeden výzkum od skupiny autorů mimo jiné i z Masarykovi univerzity, a to od Lenky Dědkové, Aleny Černé, Kateřiny Janasové a Kristiana Danebacka s názvem *Meeting online strangers offline*. Výzkum byl zaměřen na setkávání se dívek ve věku mezi 15 a 18 lety s neznámými lidmi z prostředí online světa (Willoughby, 2019). Tato setkání dle výzkumu představují jedno z nejméně rozšířených, ale zároveň také nejobávanějších online rizik pro teenagery. Na základě čtrnácti rozhovorů s českými dívkami, jež hovořily o znepokojujících setkáních s cizími lidmi, které poznaly online, studie identifikuje zejména nesoulad mezi očekáváním a realitou jako hlavní příčinu negativních pocitů (Dedkova et al., 2014)²⁵.

Na Fakultě sociálních věd Univerzity Karlovy udělala Lucie Svobodová v roce 2016 výzkum v rámci své diplomové práce na téma *Facebook a Instagram jako součást životního stylu mládeže*. Zde se formou polostrukturovaných rozhovorů s deseti respondenty ve věku mezi 15 a 19 lety snažila zjistit, co je motivací teenagerů k používání sociálních sítí. Její zjištění jsou obdobná tomu, co popisuje ve svých textech danah boyd – tedy to, že teenageři používají sociální sítě zejména k udržování vztahů s vrstevníky a ke komunikaci s nimi. Zároveň se Svobodová ve svém výzkumu ptala i na povědomí teenagerů o bezpečnosti v tomto prostředí a od svých respondentů zjistila především to, že i přesto, že sociální sítě používají,

²⁵ Jelikož výzkum vyšel v angličtině, jsou i jejich jména a příjmení v citaci psána bez diakritiky, viz např. <https://www.degruyter.com/view/journals/comm/39/3/article-p327.xml>

tak je nepovažují za příliš bezpečné. Někteří zde zmiňovali, že si občas přidají do přátel i někoho, koho úplně neznají. Další otázky se zaměřovaly například na sdílení polohy, kde byly odpovědi dost rozdílné – někdo sdílí častěji, někdo vůbec. Zároveň zde respondenti dochází ke shodě, že nastavení soukromí mají odlišné na Facebooku a Instagramu už jen z toho důvodu, že každá z těchto sítí funguje na trochu jiném principu (Svobodová, 2016).

V roce 2018 vznikl výzkum na Univerzitě Severní Karolíny v Charlotte na téma *Používání sociálních médií studenty „Middle schools“*, tedy dětmi přibližně ve věku mezi 12 a 15 lety. Zúčastnilo se celkem 593 studentů, kteří odpovídali na otázky související se sociálními médii a digitálními stopami. 72,85 % respondentů tohoto výzkumu používá sociální síť Instagram. Daleko za ním a za YouTube, Snapchatem, Vine a Pinterestem je se svými 31,19 % Facebook. To jasně souvisí s tím, že děti a teenageři nechtějí sdílet tolik obsahu na takových sítích, kde mohou potkat i více osob starší generace – zejména rodiče a učitele. Nejčastěji se na tyto sítě připojují přes své chytré telefony nebo laptopy. Mezi jejich nejoblíbenější aktivitu na sítích pak patří jednoznačně sdílení fotografií. Většina z nich začala sociální sítě používat mezi 10 a 12 lety a z výzkumu lze také vyvodit, že v dřívějším věku začaly sociální sítě používat dívky. Na otázku, zda přijímají nabídky přátelství a sledování od osob, které neznají, sice odpověděla většina, že ne, ale přesto tu zbylo 239 respondentů, kteří takovéto nabídky přátelství přijímají. To, co mají tito respondenti na sociálních sítích jako společný zájem, je záliba ve sledování ostatních, zejména toho, co dělají kamarádi, a pak komunikování s nimi. Mezi nejméně oblíbené vlastnosti sociálních sítí pak patří znepokojující a nevhodný obsah, zlí lidé a hrozba kyberšikany a ztráty soukromých informací (Martin et al., 2018).

Česká společnost *AMI Digital Index* zveřejnila v roce 2020 výzkum, který byl zaměřený na používání sociálních sítí. Zúčastnilo se ho 301 respondentů ve věku od 15 do 59 let. 92 % z nich používá sociální sítě, 79 % z nich je na sociálních sítích denně. Z nejmladší skupiny respondentů (mezi 15 a 29 lety) používá sociální sítě 95 % z nich dokonce denně. Tato věková skupina přidává příspěvky na sociální síť Facebook méně často než starší respondenti, naopak na Instagramu jsou aktivnější. Toto přímo souvisí s tím, které sociální sítě respondenti vůbec navštěvují opakovaně. U Facebooku se jednotlivé věkové skupiny příliš nelišili, ale u Instagramu byl vidět mnohem zásadnější rozdíl, jelikož tuto sociální sítě opakovaně navštěvují nejvíce právě respondenti ve věku mezi 15 a 29 lety. Ze starších respondentů Instagram navštěvuje minimum z nich. V tomto výzkumu byly zjišťovány i důvody, které respondenty vedou k používání sociálních sítí – nejčastěji je důvodem kontakt s přáteli, zábava a používání sociálních sítí jako zdroje informací (Crha, Marešová, 2020).

EU Kids Online je nadnárodní výzkumná síť, která se zabývá povědomím evropských dětí ve věku od 9 do 16 let o příležitostech, rizicích a bezpečnosti na sociálních sítích. Na jejich výzkumech se podílí i čeští vědci z Masarykovy univerzity v Brně. Nejnovější výsledky byly získávány v letech 2017–2019 a publikovány byly v roce 2020. Zúčastnilo se celkem 25 101 dětí z 19 zemí Evropy. Co se týče českých dětí, které se tohoto výzkumu zúčastnily, tak 84 % z nich denně používá svůj chytrý telefon pro přístup na internet. Právě chytrý telefon je u této věkové skupiny nejrozšířenější technologií, kterou pro účely sledování internetu a sociálních sítí používají. Obecně lze z tohoto výzkumu soudit, že starší děti používají internet častěji než mladší, s čímž souvisí i fakt, že se mnohem častěji setkávají s online riziky. Zajímavým poznatkem tohoto výzkumu je, že české děti setkání s rizikem na internetu příliš nerozruší. Každopádně z výzkumu také vyplynulo, že dívky se mnohem častěji setkávají s rizikovým obsahem, který např. podporuje poruchy příjmu potravy, a častěji jsou oslovovány s žádostmi o sdílení soukromých/důvěrných informací. Chlapci se naopak častěji setkávají s počítačovými viry a přehnaným utrácením v aplikacích a online hrách. Komunikace a dobré vztahy s rodiči jsou podle tohoto výzkumu nejčastější faktory, které dětem pomáhají s prevencí a případným vyrovnáváním se s riziky v online světě (Smahel et al., 2020).

V září roku 2020 prezentovala na konferenci *Instameet* společnost *Kantar* svůj nejnovější výzkum týkající se Čechů na sociálních sítích. Jejich výzkumu se zúčastnilo přes 2 000 osob starších 16 let. 91 % všech respondentů tohoto výzkumu používá Facebook, 56 % YouTube a 49 % Instagram. Ostatní zmíněné sociální sítě (Pinterest, Twitter, Snapchat, LinkedIn a Tiktok) používá pod 50 % respondentů. Pro další porovnání byly z celkových výsledků následně vybrány pouze odpovědi respondentů ve věku mezi 16 a 24 lety. I zde se na prvním místě umístil Facebook s 99 %, ale byl mnohem těsněji následován sítí YouTube (88 %) a Instagram (82 %). I všechny ostatní vybrané sociální sítě v této věkové skupině měli větší zastoupení. Obecně zde shrnují, že hlavně mladší generaci v posledních letech přestává bavit Facebook a mnohem aktivněji používají Instagram. I když i zde 36 % z respondentů odpovědělo, že nepřidává žádné příspěvky na svůj profil a 50 % z nich nepřidává ani žádné příběhy (*stories*) (Pflanzer, 2020).

Během roku 2020 také vyšel související výzkum mezi stovkou respondentů z řad teenagerů na téma ochrany soukromí na Instagramu z indonéského města Surabaya. I v tomto výzkumu vyšlo, že dívky se na ochranu svého soukromí zaměřují více než chlapci, ale ten rozdíl nebyl až tak velký jako u předchozího zmíněného výzkumu. Čím jsou zároveň teenageři starší, tím aktivněji se snaží své soukromí chránit. Z tohoto výzkumu celkově vychází, že čím více

mají teenageři povědomí o možných nebezpečích, tím více své soukromí chrání a naopak, pokud případná rizika neznají, jsou jejich obavy minimální (Widiyaningsih, 2020).

Výzkum Ralfa de Wolfa z roku 2020 se zabývá tím, jak teenageři spravují své osobní a mezilidské soukromí na sociálních sítích. Zúčastnilo se dvanáct škol, celkem 2 681 respondentů z regionů belgických Flander. Výzkum odhalil, že více o ochranu svého soukromí na sociálních sítích dbají dívky než chlapci. V tomto výzkumu mimo jiné zmínilo 44,25 % respondentů, že o nich na sociálních sítích, zejména na Facebooku, sdílí informace jejich rodiče (tzv. *sharenting*). Více než polovina z nich odpověděla, že s tímto sdílením nesouhlasili (Wolf, 2020).

V závěru této kapitoly můžeme jednoznačně shrnout, že ve světě rychle se rozvíjejících technologií, internetu a sociálních sítí jsou velice ohroženou skupinou děti a teenageři, a to zejména proto, že sociální sítě jejich životy ovlivňují mnohem více než kteroukoli z předchozích generací – a to v tom pozitivním, tak i v negativním slova smyslu. Zároveň je nutné nezapomínat, že do světa internetu a sociálních sítí vstupují ve velice nízkém věku, kdy je pro ně složité uvědomovat si veškeré aspekty těchto online platform. Proto je potřeba, aby i rodiče a učitelé drželi krok s vývojem a zejména s hrozícími riziky a snažili se děti a teenagery v co největší míře informovat, varovat a chránit.

5 Informační chování žáků 8. a 9. tříd ve vztahu k ochraně vlastního soukromí na sociálních sítích

5.1 Cíle výzkumu, hypotézy

Tato diplomová práce se zabývá informačním chováním žáků 8. a 9. tříd základních škol ve vztahu k ochraně vlastního soukromí na sociálních sítích Facebook a Instagram. Cílem práce je zjištění:

- jak se žáci zajímají o problematiku ochrany svého soukromí na těchto sítích a odkud čerpají tyto informace (rodiče, škola),
- zda jsou si vědomi asociovaných rizik a jak je ve svém chování zohledňují,
- jestli znají nástroje, které jsou jim na těchto sítích k dispozici,
- jak výše uvedené ovlivňuje jejich vystupování na vybraných sociálních sítích z pohledu obsahu a formy sdílených informací.

Na základě literatury, která byla popsána v předchozích kapitolách, a tématu práce byly pro výzkum zvoleny tyto hypotézy:

1. Více než polovina žáků 8. a 9. tříd má účet alespoň na jedné sociální síti.
2. Žáci 8. a 9. tříd čerpají informace o bezpečnosti na sociálních sítích zejména z internetových zdrojů a programů.
3. Více než polovina respondentů ví, jak si nastavit svůj profil na Facebooku a Instagramu s ohledem na své soukromí – ví, s kým sdílejí své příspěvky, kdo vidí jejich obsah atd.
4. Nejméně polovina respondentů má v přátelích na Facebooku nebo ve sledování Instagramu minimálně jednoho člověka, kterého neznají i osobně.
5. Více než 50 % žáků 8. a 9. tříd zná pojem *digitální stopa*.

5.2 Dotazník (kvantitativní výzkum)

Na základě zadání této diplomové práce a souvisejících výzkumných otázek byl vytvořen dotazník, který se skládal z těchto částí: sociální sítě všeobecně, nepoužívání sociálních sítí, Instagram, Facebook, ostatní sociální sítě, digitální stopa a rizika sociálních sítí.

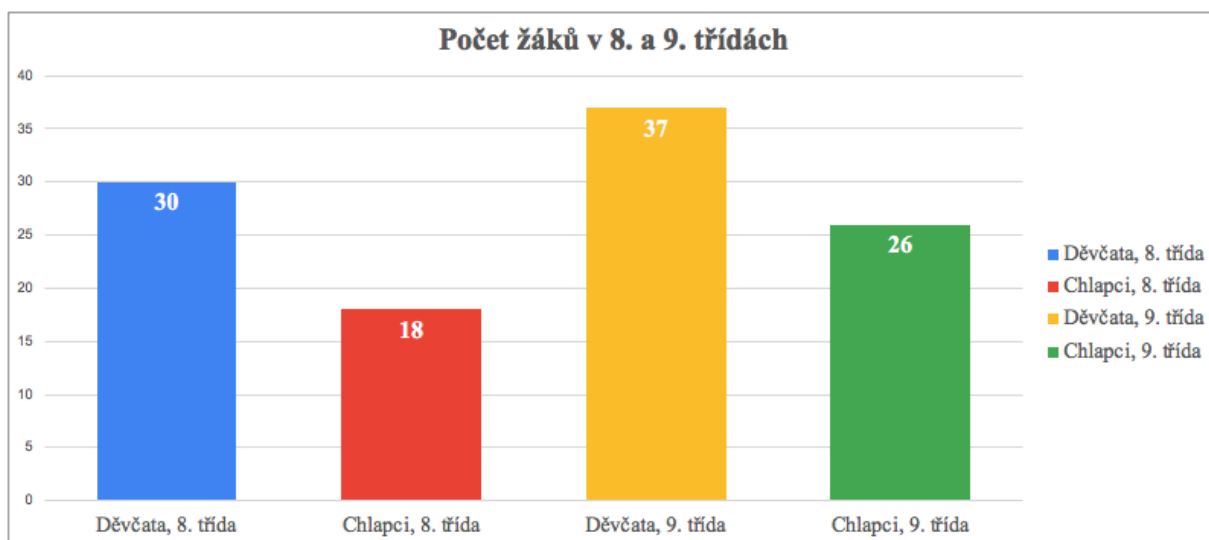
Nejrozsáhlejšími částmi dotazníku byly ty zaměřené na Instagram a Facebook, které se respondentů ptaly zejména na otázky související s nastavením jejich osobních profilů právě se zaměřením na ochranu soukromí – např. *veřejné* nebo *soukromé* nastavení profilu,

přidávání přátel a sledujících, které osobně neznají, sdílení polohy, četnost sdílení vlastních příspěvků apod. Další části se zajímaly o to, zda respondenti znají pojem *digitální stopa* a mají přehled o tom, s jakými riziky se na sociálních sítích mohou setkat. Kromě toho bylo zkoumáno, z jakých zdrojů žáci 8. a 9. tříd vůbec získávají informace o bezpečnosti na internetu a sociálních sítích, o chování na nich a o prevenci před možnými riziky. Celé znění dotazníku je dostupné v příloze č. 1.

5.3 Účastníci výzkumu

V rámci této diplomové práce byl uskutečněn pilotní výzkum prostřednictvím dotazníku, který byl detailněji popsán v předchozí kapitole. Zúčastnilo se ho celkem 111 žáků 8. a 9. tříd ze ZŠ a MŠ Husova Tábor. Na této základní škole mají v současné době (školní rok 2020/2021) 3 osmé a 4 deváté třídy, celkem tedy přibližně 170 žáků. Dotazník vyplnilo 65,3 % z nich.

Dle získaných odpovědí v části dotazníku zaměřené na demografické údaje se vyplňování zúčastnilo 67 děvčat a 44 chlapců. 48 z nich navštěvuje momentálně 8. třídu a 63 z nich chodí do 9. třídy (viz *graf 1*).



Graf 1 – Počet žáků v 8. a 9. třídách

5.4 Postup výzkumu

Po dokončení dotazníku byl jeho obsah předložen dvěma osobám ve věku respondentů. Tyto osoby byly vybrány z rodinných příslušníků a dalších známých autorky této práce. Jejich pomoc spočívala zejména v posouzení srozumitelnosti předkládaných otázek a odpovědí. Pokud jim nebyl význam jednotlivých částí dotazníku dostatečně jasný, byla s nimi konzultována úprava znění tak, aby byla zajištěna srozumitelnost pro respondenty výzkumu.

Týden před samotným rozesláním dotazníku žákům poslal jejich vyučující informační e-mail rodičům, ve kterém je seznámil s tím, že se jejich syn nebo dcera zúčastní vyplňování anonymního dotazníku, který se týká zejména ochrany soukromí na sociálních sítích. V případě, že by některý z rodičů nesouhlasil s účastí svého potomka, mohl se obrátit na příslušného vyučujícího a jeho syn/dcera dotazník nedostal/a. Celé znění e-mailu rodičům je dostupné v příloze č. 2.

Odkaz na dotazník (celé znění dotazníku je dostupné v příloze č. 1), který byl vytvořený v prostředí internetové aplikace *Formuláře* od společnosti *Google*, byl žákům rozeslán prostřednictvím e-mailu. Na vyplnění dotazníku měli celý týden (7 dní). Po uplynutí doby, kterou měli žáci na vyplnění dotazníku byl dotazník uzavřen a byly zpracovány výsledky.

5.5 Výsledky dotazníkového šetření

V následující části textu jsou popsány výsledky jednotlivých částí dotazníku. Výsledky jsou rozděleny do několika podkapitol z důvodu přehlednosti a jednodušší orientace. První část se zabývá obecnými otázkami, které se týkaly používání, popř. nepoužívání sociálních sítí. Druhá část obsahuje odpovědi na otázky týkající se Instagramu, třetí část se zabývá Facebookem a čtvrtá část obsahuje výsledky otázek týkajících se digitální stopy a rizik sociálních sítí.

5.5.1 Odpovědi na otázky týkající se sociálních sítí všeobecně

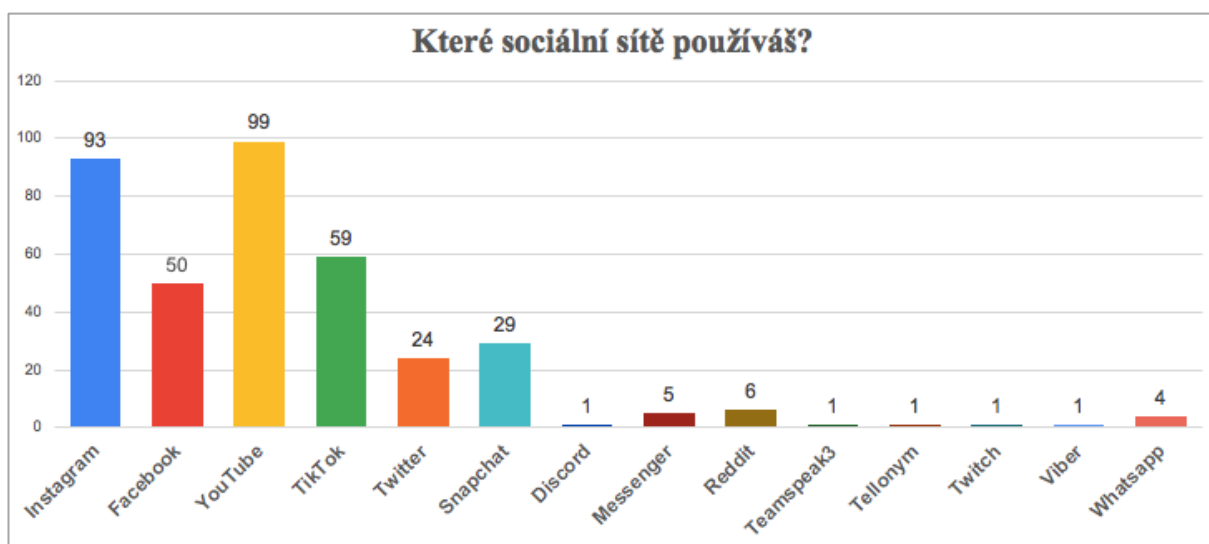
První otázka pro respondenty se zajímala, zda vůbec nějaké sociální sítě používají. Pokud odpověděli *ano*, dostali se v dalších částech na otázky týkající se už konkrétních sociálních sítí. Pokud odpověděli *ne*, dostali se do části, která se dotazovala na důvody proč sociální sítě nepoužívají a následně přeskočili rovnou na sekci o digitální stopě a rizicích na sociálních sítích.

Jak je patrné z grafu níže (viz *graf 2*), naprostá většina respondentů (97,3 %) odpověděla, že sociální sítě používá, pouze 3 z nich odpověděli negativně. Všichni 3 respondenti, kteří uvedli, že sociální sítě nepoužívají, tak činí jednoduše proto, že nechtějí. Pouze 1 z nich svou odpověď dále specifikoval a uvedl, že sociální sítě nepoužívá, protože si myslí, že čím více informací o sobě zveřejní, tím spíše hrozí, že je někdo zneužije.



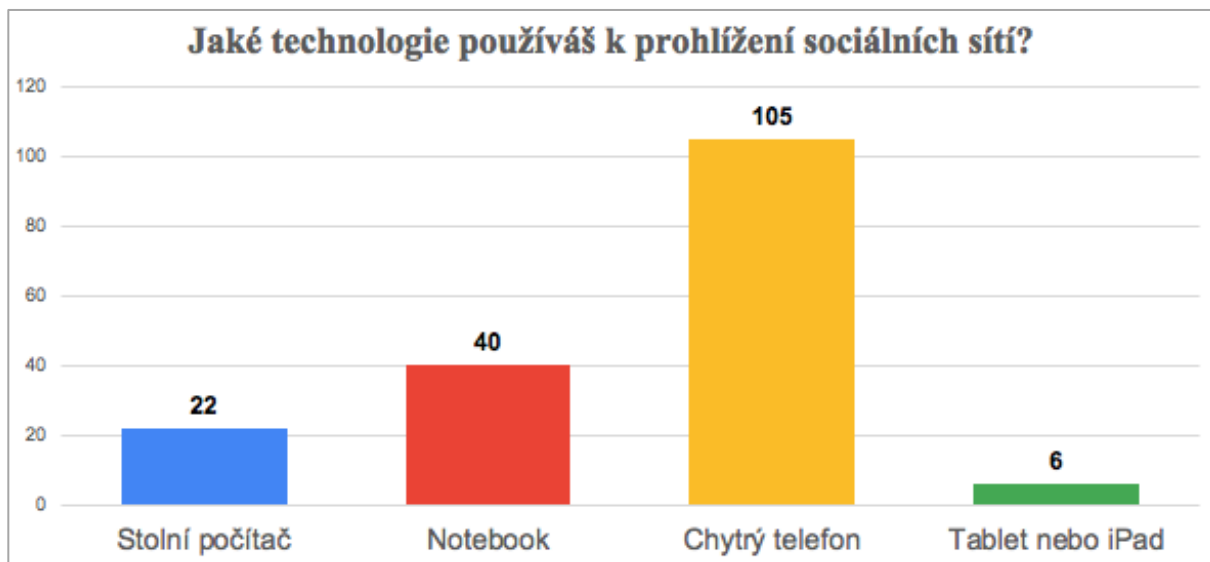
Graf 2 – Odpovědi na otázku: „Používáš nějaké sociální sítě?“

Další otázky se respondentů tázaly na to, jaké sociální sítě používají. Nejvíce z nich, 99 respondentů, zvolilo Youtube, na druhé pozici se umístil Instagram. Na třetím místě skončila sociální síť TikTok a na čtvrtém Facebook. Na pátém místě skončil Snapchat a šesté místo obsadil Twitter. Další sociální sítě, které jsou k vidění v *grafu 3* doplňovali respondenti ručně jako další sítě, které také sledují. Několikrát doplnili například Messenger, což je komunikační aplikace napojená na Facebook, takže to není sociální síť jako taková, navíc ji pravděpodobně používá i většina z těch respondentů, kteří odpověděli, že používají Facebook. Níže (*graf 3*) jsou v grafu shrnuty veškeré odpovědi na otázku používaných sociálních sítí.

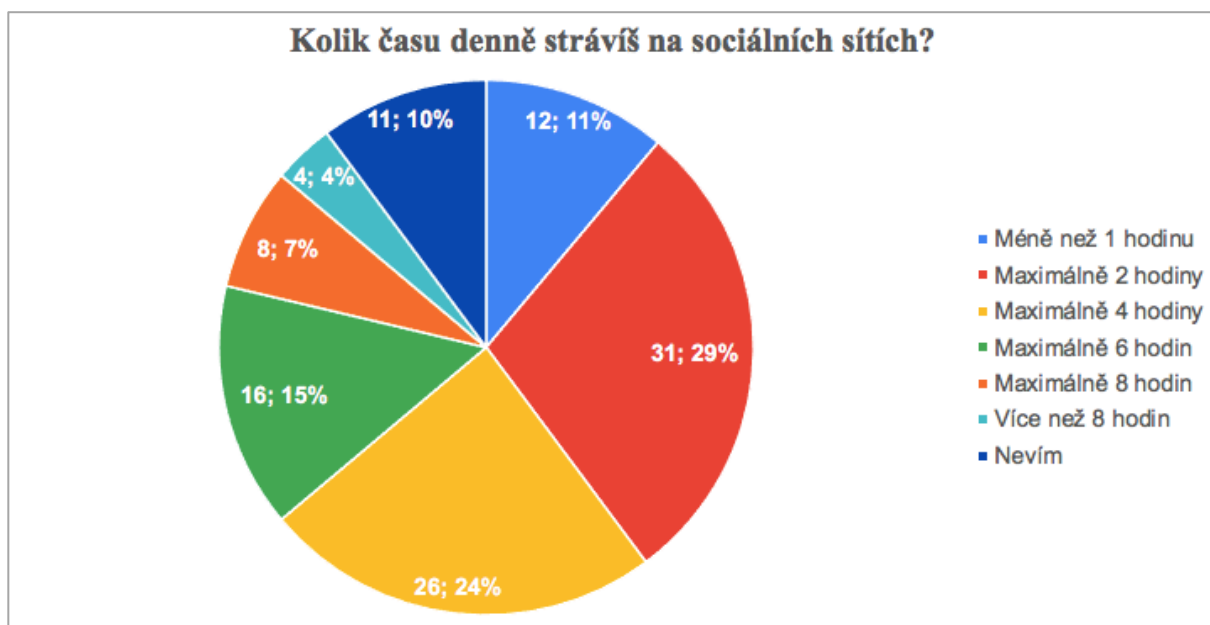


Graf 3 – Sociální sítě, které respondenti používají

Nejčastější odpovědí na otázku, které technologie respondenti používají k prohlížení sociálních sítí (viz graf 4), byl jednoznačně chytrý telefon. Tuto odpověď nezvolili pouze 3 respondenti. Daleko za chytrým telefonem se umístil notebook a stolní počítač. Tablet nebo iPad zvolilo pouze 6 respondentů.



Graf 4 – Zařízení, která respondenti používají k prohlížení sociálních sítí

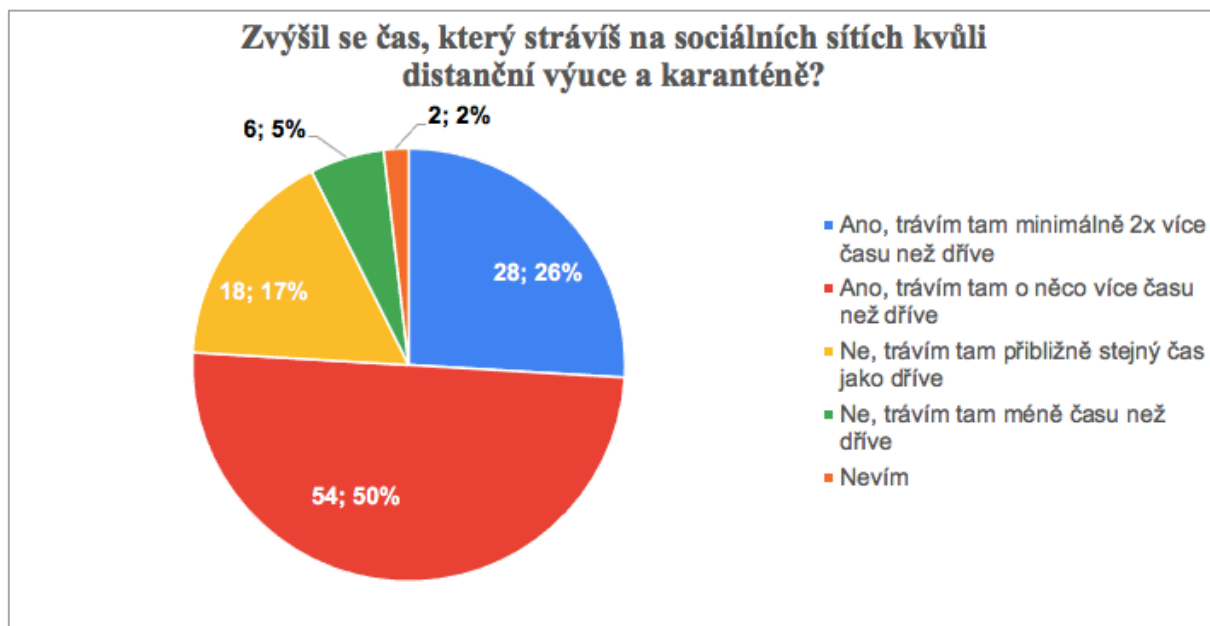


Graf 5 – Čas, který respondenti stráví na sociálních sítích

Do dotazníku byly zařazeny i tři otázky týkající se času stráveného na sociálních sítích, jelikož i to může souviset s ochranou soukromí a vystavování se rizikům sociálních sítí – čím více času tam tráví, tím více o sobě mohou sdílet apod. 54,6 % respondentů odpovědělo, že si čas strávený na sociálních sítích nijak neměří, zbylých 45,4 % z nich používá ke sledování nějaký nástroj nebo aplikaci ve svém zařízení. Dále respondenti uváděli nebo odhadovali,

kolik času na sociálních sítích skutečně stráví. Největší část z nich, 29 %, uvedla, že tam tráví maximálně 2 hodiny denně. Velké zastoupení měla také skupina těch, kteří tráví na sociálních sítích maximálně 4 hodiny (24 %) a maximálně 6 hodin (15 %). 8 respondentů uvedlo, že tam tráví maximálně 8 hodin a 4, že dokonce více než 8 hodin. Detailně jsou výsledky zobrazeny v grafu 5.

Poslední otázka související s časem stráveným na sociálních sítích se respondentů tázala na to, zda se nějak změnila doba, kterou na sociálních sítích tráví z důvodu distanční výuky a karanténních opatření, která byla v letošním roce zavedena z důvodu epidemie koronaviru. Zde naprostá většina z respondentů odpověděla, že nyní na sociálních sítích tráví více času než dříve. 26 % z nich dokonce uvedlo, že je to minimálně 2× více než dříve. Detailní výsledky jsou uvedeny v grafu 6.

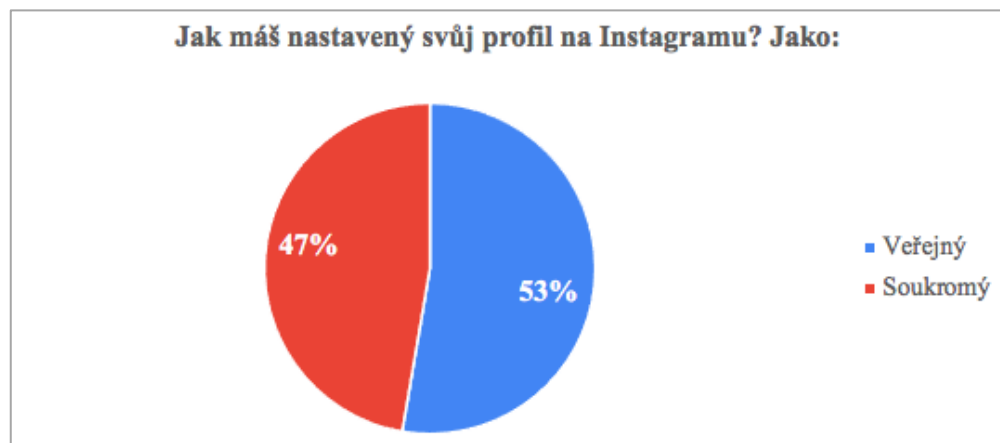


Graf 6 – Čas strávený na sociálních sítích v karanténě

5.5.2 Odpovědi na otázky týkající se Instagramu

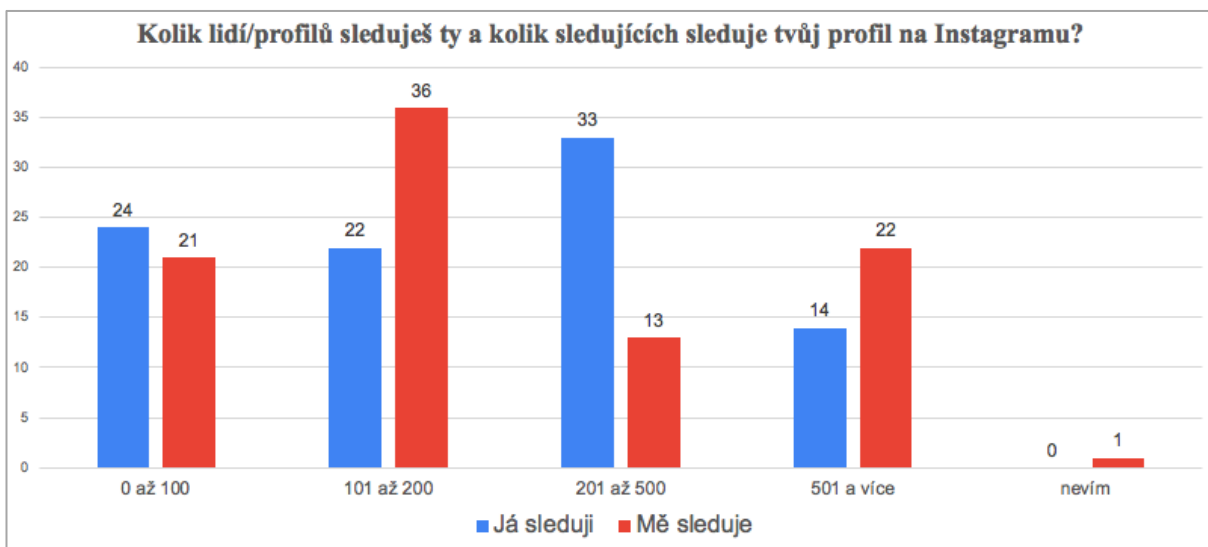
Z celkového počtu 108 respondentů, kteří používají sociální sítě, uvedlo 93 z nich, že používá sociální síť Instagram. Na všechny následující otázky ohledně této sociální sítě odpovídali pouze ti respondenti, kteří sociální síť Instagram používají.

První otázka se respondentů tázala na to, zda mají svůj profil na Instagramu nastavený jako *veřejný* nebo *soukromý*. A výsledek je velmi vyrovnaný, 53 % z nich má profil *soukromý*, zbylých 47 % veřejně přístupný pro kohokoli (viz *graf 7*).



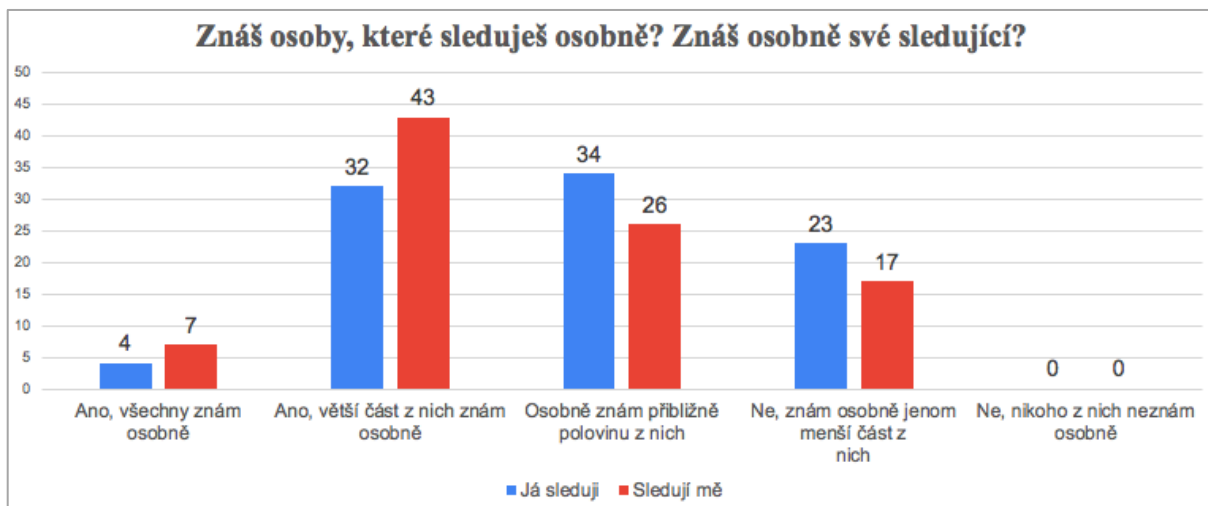
Graf 7 – Odpovědi na otázku ohledně nastavení soukromí profilu na Instagramu

Druhá otázka se týkala počtu sledovaných profilů a počtu sledujících. Největší počet respondentů odpovědělo, že je sleduje mezi 101 a 200 uživatelů. Odpovědi na otázku, kolik profilů respondenti sledují byly více vyrovnané, ale přeci jen největší počet z nich odpověděl, že sledují 201 až 500 jiných profilů. Detailně jsou výsledky zobrazeny na *grafu 8*.



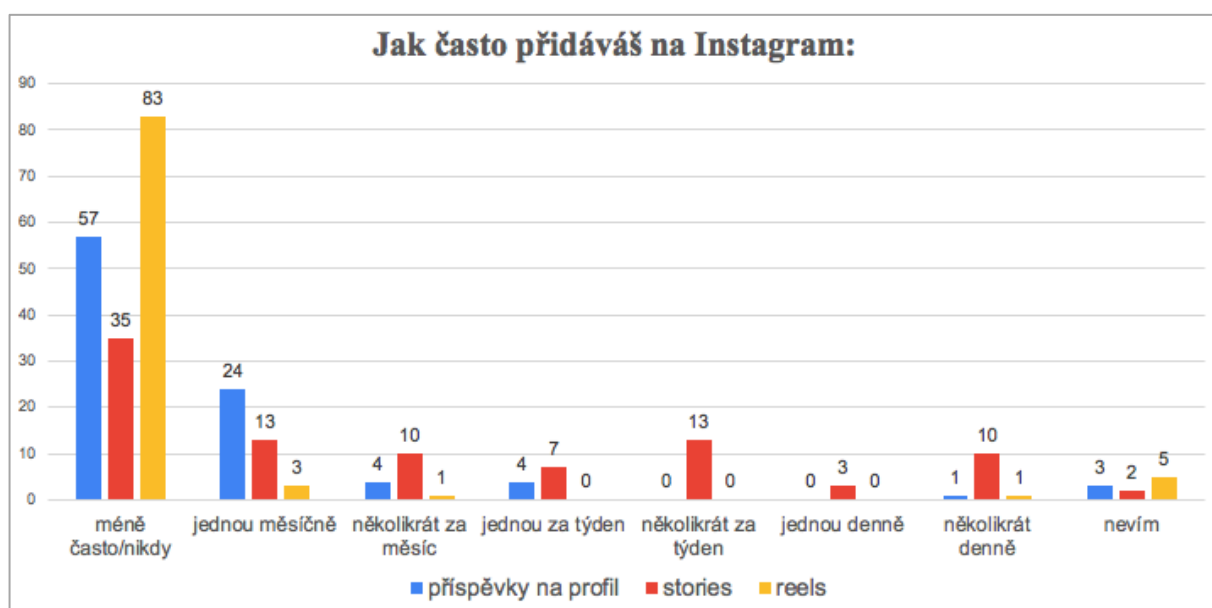
Graf 8 – Počty sledovaných a sledujících na Instagramu

Následovaly dvě otázky, které se zaměřovaly na to, zda respondenti osobně znají ty osoby, jejichž profily sledují a zda znají vlastníky profilů, které sledují je. V obou otázkách byly stejné dvě nejčastější odpovědi – tedy že znají buď většinu z nich, nebo přibližně polovinu (viz graf 9).



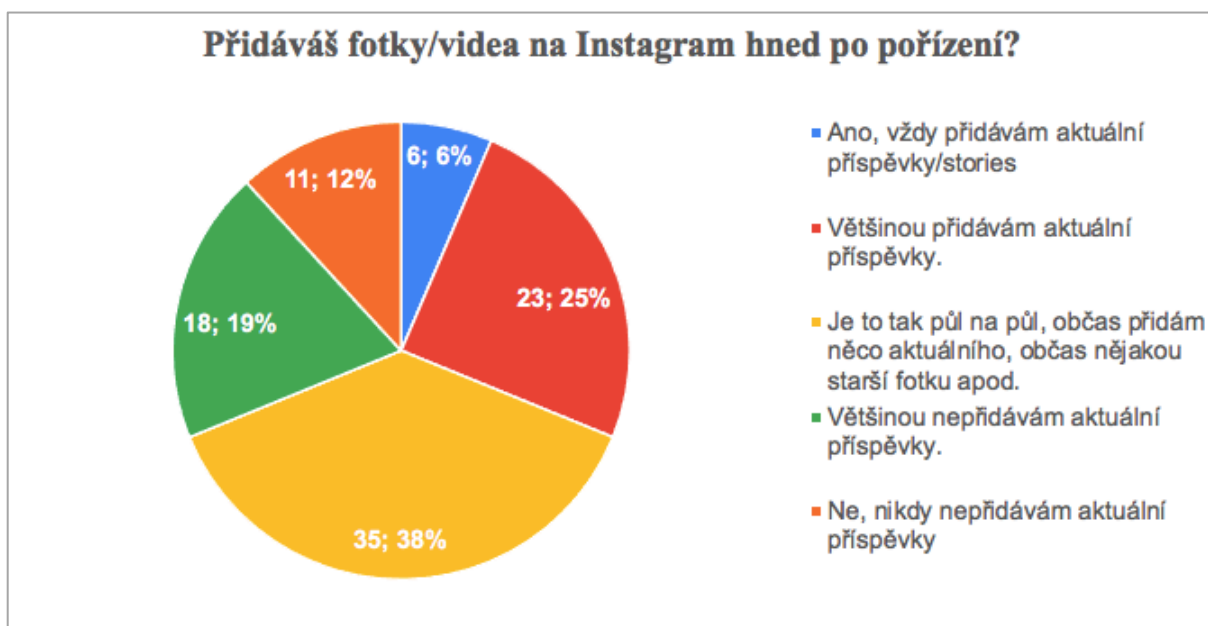
Graf 9 – Sledování a sledující, znají je respondenti osobně?

S ochranou soukromí také úzce souvisí fakt, jak často uživatel sociální sítě zveřejňuje své příspěvky. A právě toho se týkala další otázka, která navíc odlišovala četnost přidávání běžných fotografií na profil, *stories* (příběhy) a *reels* (krátká videa). Z výsledků téměř jednoznačně vyplývá, že většina žáků 8. a 9. tříd na Instagram nepřidává příspěvky nikdy nebo téměř nikdy. A pokud už někdo přidává příspěvky častěji, tak je to formou příběhů, které po 24 hodinách zmizí. Detailně je to znázorněno v grafu 10.



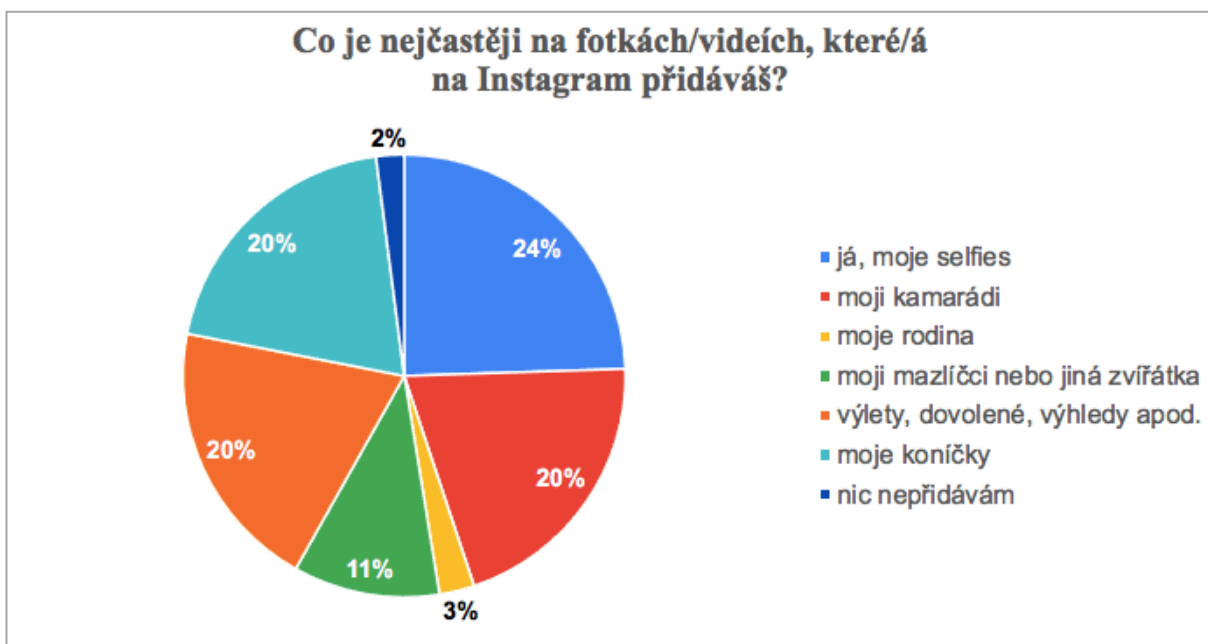
Graf 10 – Četnost přidávání příspěvků na Instagram

S četností přidávaných příspěvků úzce souvisí i následující otázka, která se ptala na to, zda respondenti přidávají na Instagram své příspěvky hned po pořízení. I zde jsou odpovědi víceméně půl napůl, viz *graf 11*.



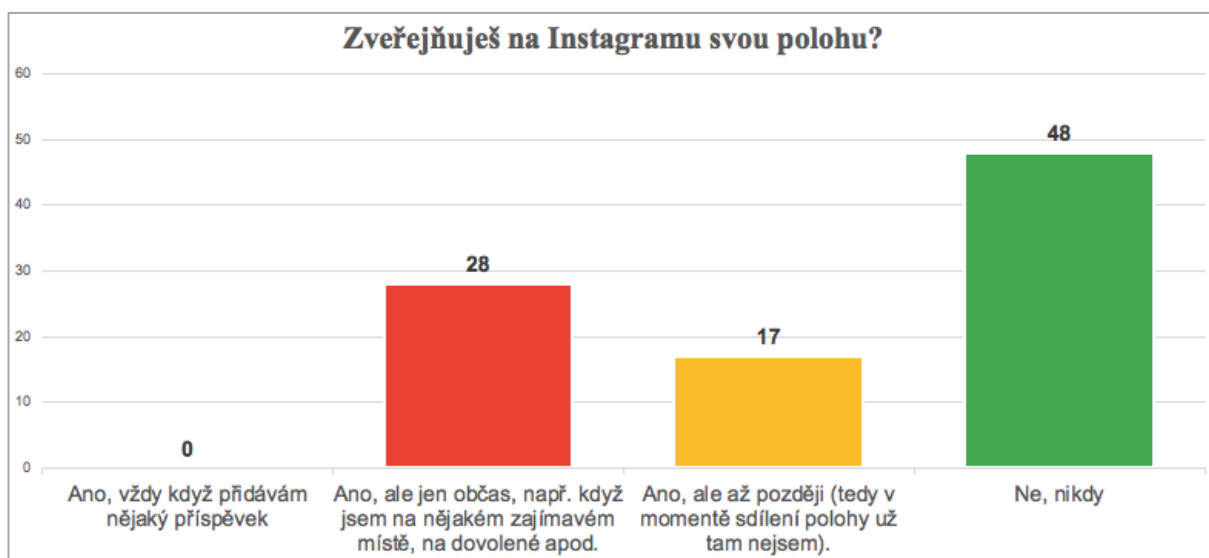
Graf 11 – Aktuálnost přidávaných příspěvků

Další otázka se zaměřovala na to, co vlastně děti ve věku žáků 8. a 9. tříd na Instagramu nejčastěji sdílí. Výsledkem je, že s největší frekvencí zveřejňují fotky sami sebe a svých kamarádů. Často ale přidávají i záběry z různých výletů a dovolených nebo příspěvky vztahující se k jejich koníčkům. Naopak skoro nikdo z respondentů nepřidává příspěvky se svou rodinou (viz *graf 12*).



Graf 12 – Obsah příspěvků na Instagramu

S tím souvisela i následující otázka, která se týkala toho, zda u sdílených příspěvků respondenti uvádějí i svou polohu. Zde odpovědělo 48 z nich, že polohu nesdílí nikdy, ostatní volili, že jenom občas, například když jsou na nějakém zajímavém místě, u kterého lze předpokládat, že jej chtějí právě sdílením na Instagramu ostatním doporučit, pochlubit se apod., viz *graf 13*.



Graf 13 – Zveřejňování polohy na Instagramu

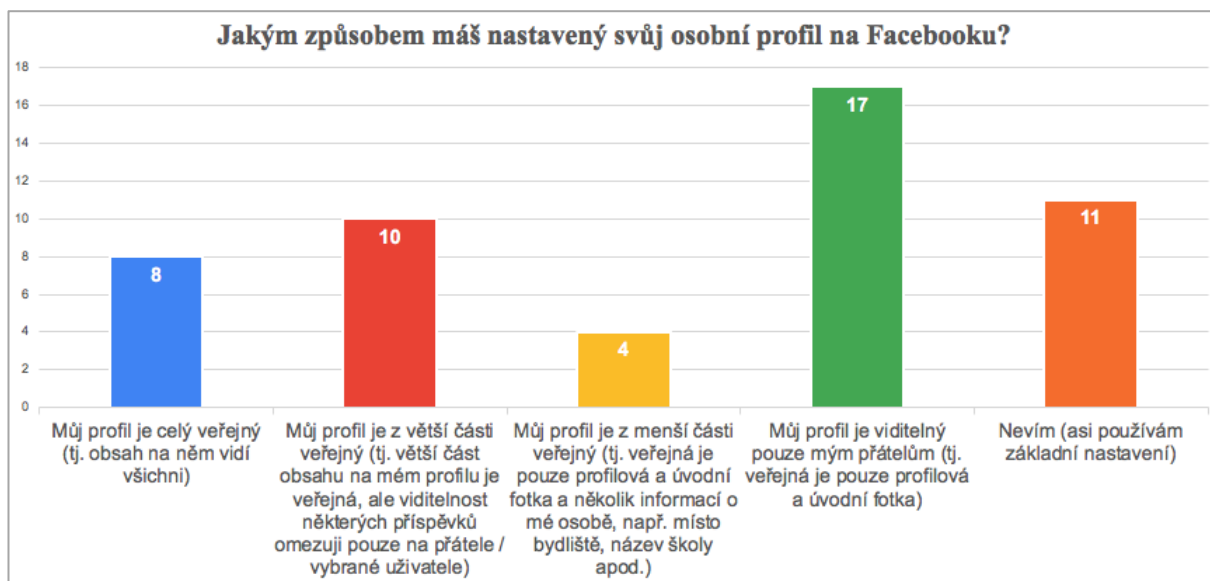
Na závěr otázek týkajících se Instagramu byla umístěna otevřená otázka, která se respondentů dotazovala na to, zda se někdy setkali na Instagramu s něčím, co by přímo ohrozilo jejich soukromí. Většina z nich odpověděla, že ne, občas někdo zmínil, že se mu někdo cizí ukradl uživatelský účet (např. odhalil heslo, změnil obsah profilu a přístupové údaje). Jedna respondentka zmínila, že jí jedna z jejích (bývalých) kamarádek založila falešný účet, kde bez dovolení sdílela její fotografie – celé to bylo vůči respondentce zaměřeno velmi nenávistně. Nezkrácené znění odpovědí na tuto otázku naleznete v *příloze č. 3*.

5.5.3 Odpovědi týkající se Facebooku

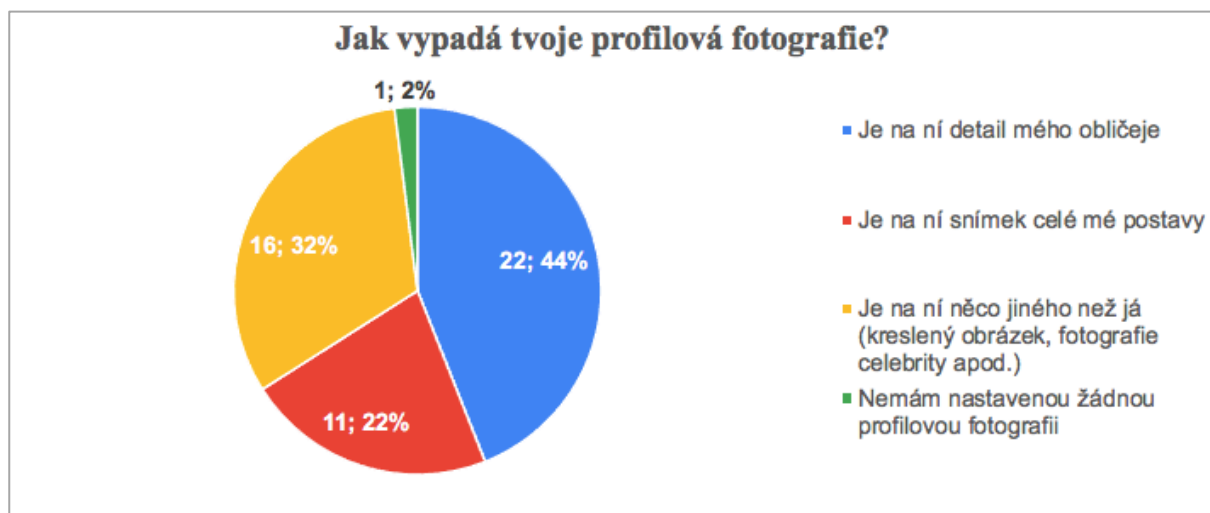
50 z celkového počtu 108 respondentů, kteří používají sociální sítě, uvedlo, že používá sociální síť Facebook. Na všechny následující otázky ohledně této sociální sítě odpovídali pouze ti respondenti, kteří sociální síť Facebook používají.

Hned první otázka se zajímala o to, jak mají žáci 8. a 9. tříd nastavené své profilové stránky na Facebooku. Nastavení se totiž může různit a oproti Instagramu mají uživatelé mnohem více možností, jak ovlivnit nastavení svého profilu pro ostatní uživatele. Důležitá je zejména volba těch informací, které ponechají jako veřejné – tedy těch, které uvidí i ty osoby,

jež nemají v přátelích. Zde většina respondentů zvolila možnost, že jejich profil je viditelný pouze těm uživatelům, které mají v přátelích, což znamená, že kdokoli jiný na jejich profilu uvidí pouze jejich profilovou a úvodní fotografii – pokud tedy mají nějakou nastavenou. 11 respondentů nevědělo, jak má profil nastavený, 10 z nich vybralo variantu, že je jejich profil veřejný ve větší míře a jenom některé své příspěvky omezují jen pro své přátele. Pouze 8 respondentů odpovědělo, že mají profil veřejně dostupný úplně pro všechny. Celé znění odpovědí je zřejmé v *grafu 14*.



Graf 15 – Nastavení profilu na Facebooku respondenty

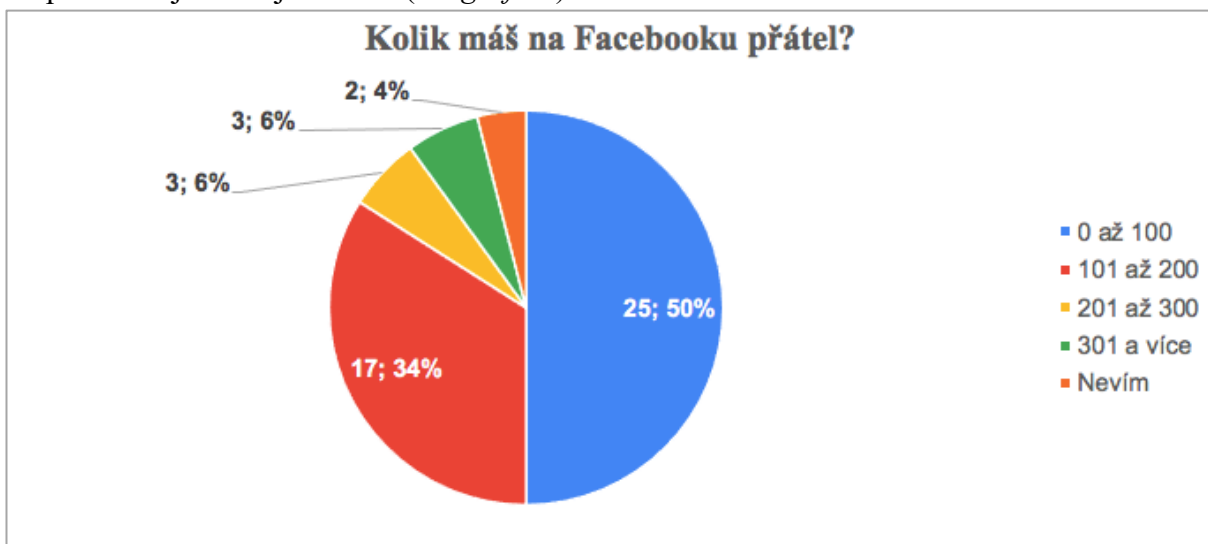


Graf 14 – Profilová fotografie na Facebooku

S nastavením profilu na Facebooku úzce souvisí profilová fotografie, jelikož ta je veřejná pro ostatní uživatele vždy. Výsledky odpovědí na otázku týkající se profilové fotografie jsou v *grafu 15*. Pouze 1 respondent odpověděl, že profilovou fotografii nastavenou nemá.

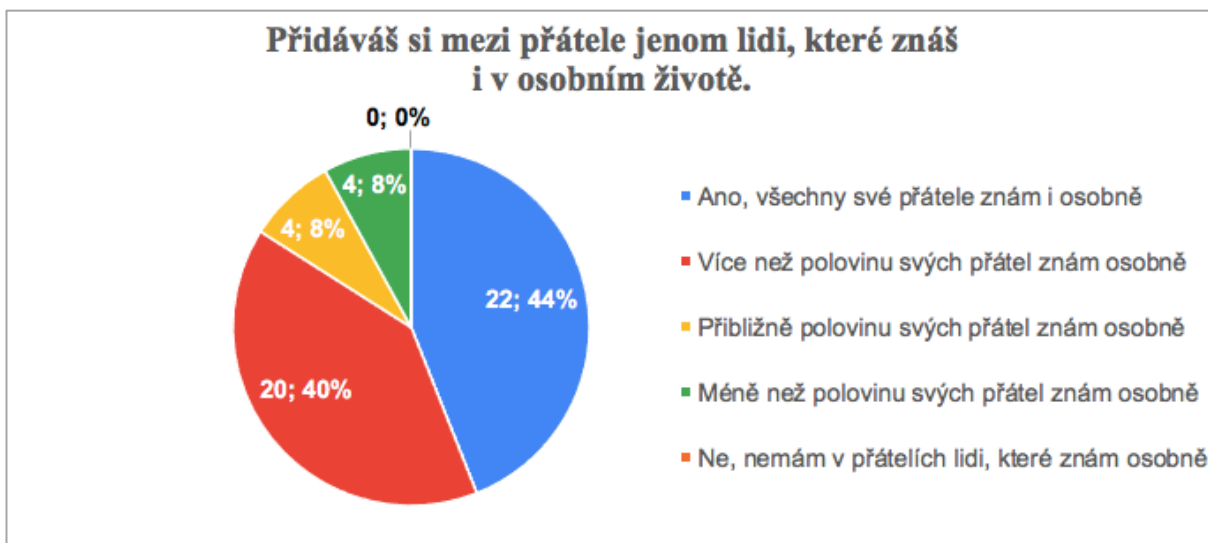
Většina ostatních na ní má detailní snímek svého obličeje nebo celé své postavy. Jenom 16 respondentů má na profilové fotografii vyobrazeno něco jiného než sami sebe.

Další část dotazníku se zabývala přáteli na Facebooku – kolik jich žáci 8. a 9. tříd mají, podle čeho se rozhodují, že žádost o přátelství schválí a zda jsou ochotni přijmout přátelství na Facebooku i od někoho, koho osobně neznají. Přesně 50 % respondentů odpovědělo, že mají na Facebooku maximálně 100 přátel, dalších 34 % má maximálně 200 a jen minimum zbylých respondentů jich má ještě více (viz graf 16).



Graf 16 – Počet přátel na Facebooku

Na otázku, zda si respondenti přidávají do přátel i osoby, které osobně neznají největší část z nich odpověděla negativně – buď znají osobně všechny své přátele (44 %) nebo více než polovinu z nich (40 %). Pouze 4 respondenti odpověděli, že znají osobně méně než polovinu ze svých přátel (viz graf 17).



Graf 17 – Znají respondenti své přátele osobně?

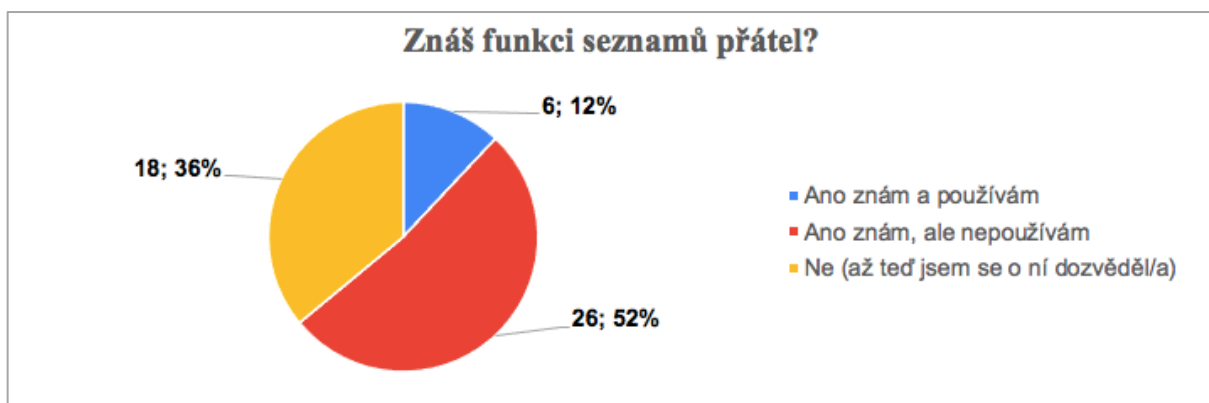
Následující dvě otázky se obě zabývaly schvalováním *žádosti o přátelství*. První z nich nabízela výběr odpovědí na otázku kritérií, podle kterých se žáci 8. a 9. tříd rozhodují, že schválí *žádost o přátelství*. Jak je vidět v *grafu 18*, byla jednoznačně nejčastější odpověď, že kritériem pro schválení je fakt, zda se s danou osobou znají osobně. Na druhém místě skončilo kritérium společných přátel na Facebooku. Pouze 4 respondenti odpověděli, že nepřemýšlí o tom, kdo daná osoba, která jim žádost o přátelství poslala, je a žádost automaticky schvalují.



Graf 18 – Kritéria respondentů pro schválení přítele

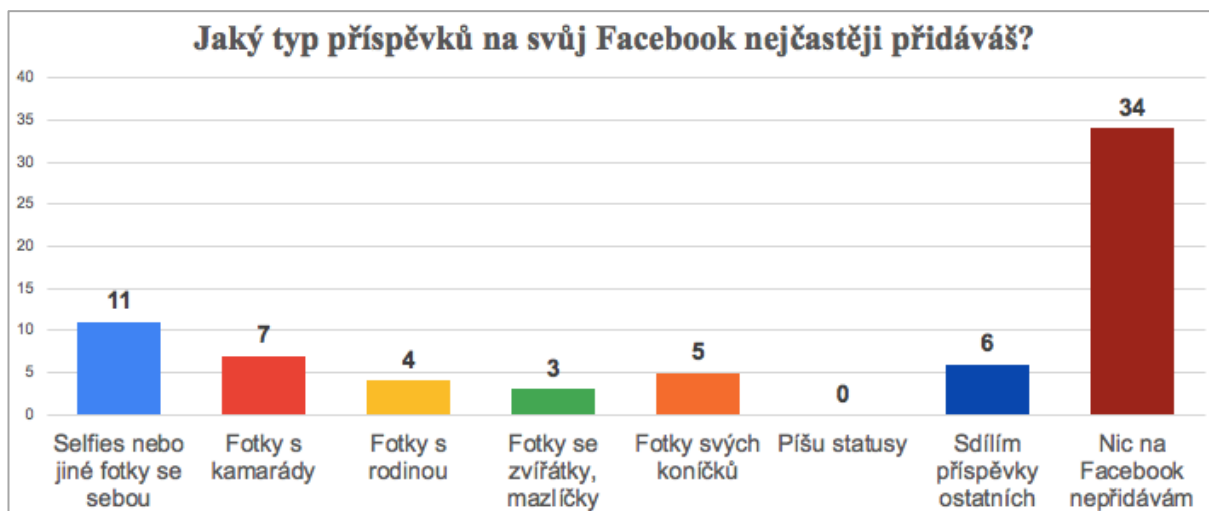
Navazující otázka se týkala konkrétněji toho, jak se respondent zachová, pokud mu přijde záležitost o přátelství od někoho, koho nezná. Na tuto otázku mohli respondenti odpovídat v delší samostatně psané odpovědi. Celé znění těchto odpovědí naleznete v *příloze 3*. Většina respondentů odpověděla, že takovou žádost nepřijímají a rovnou ji odmítají. Několik z nich se shodlo v tom, že se nejprve podívají na profil žadatele o přátelství a následně se rozhodnou podle sympatií a věku – je-li to zřejmé z profilové fotografie. Zároveň je často zajímavá, zda mají s danou osobou nějaké společné přátele, což je také kritérium, díky kterému by byli často ochotni takovou žádost o přátelství přijmout.

Další otázka se týkala seznamů přátel, které umožňují rozdělení přátel podle různé úrovně přátelství. Připravené jsou seznamy *blízcí přátelé*, *známí* a *omezeno*, ale uživatel si může vytvořit i vlastní. Facebook potom automaticky sdílí například více obsahu s lidmi v seznamu *blízkých přátel* nebo nezobrazí sdílený obsah těm, kteří jsou v seznamu *omezeno*. Pouze 6 respondentů odpovědělo, že tuto funkci používá, 26 z nich ji sice zná, ale nepoužívá a zbytek respondentů funkci neznalo – viz *graf 19*.

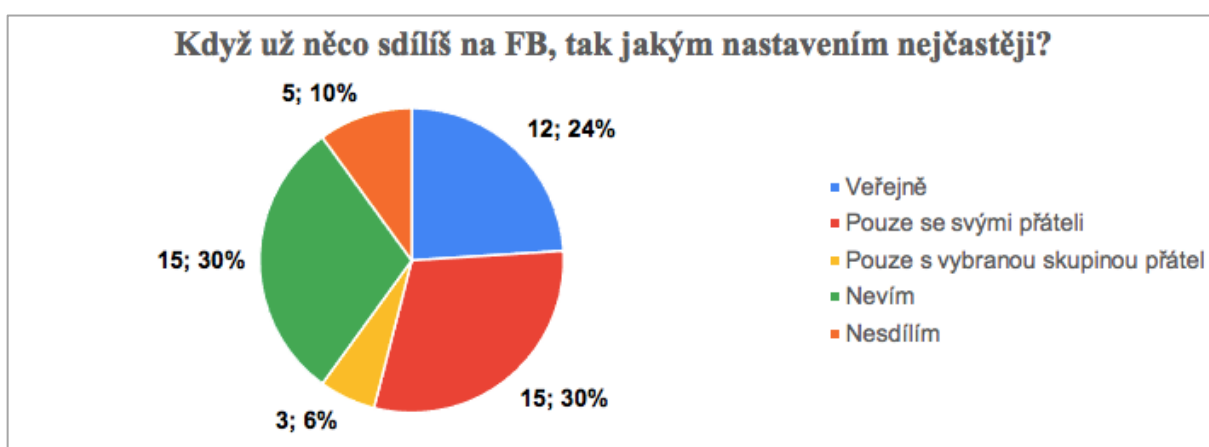


Graf 19 – Znalost funkce seznamů přátel

Na otázku, co respondenti na Facebook přidávají, naprostá většina z nich odpověděla, že nic. Pokud už někdo z nich něco sdílí, tak to jsou většinou *selfies* nebo jiné fotky sebe sama, případně fotky s kamarády (viz graf 20).



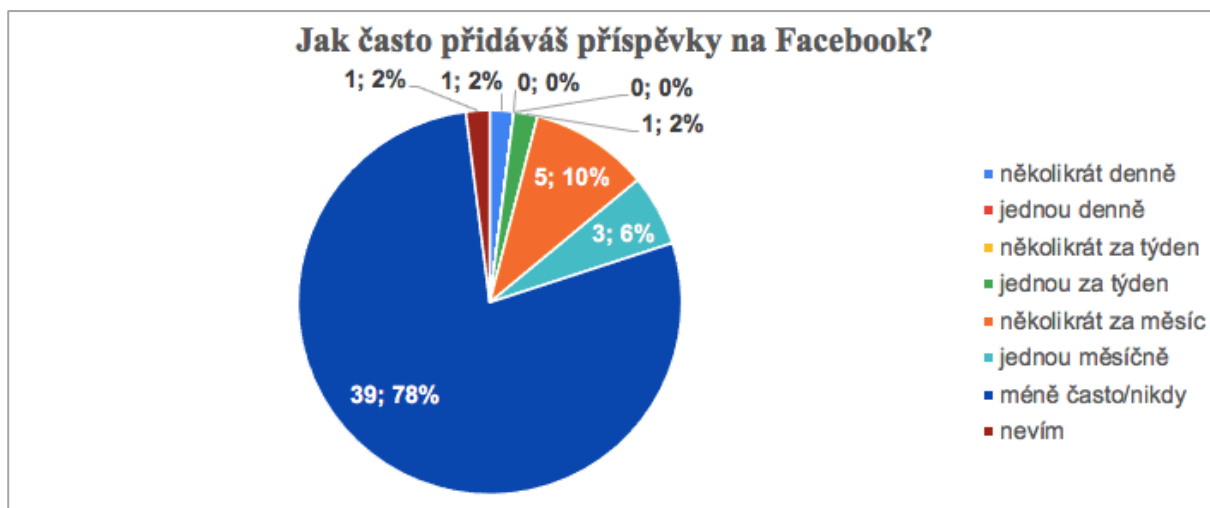
Graf 20 – Obsah sdílených příspěvků na Facebook



Graf 21 – Nastavení sdílených příspěvků na Facebook

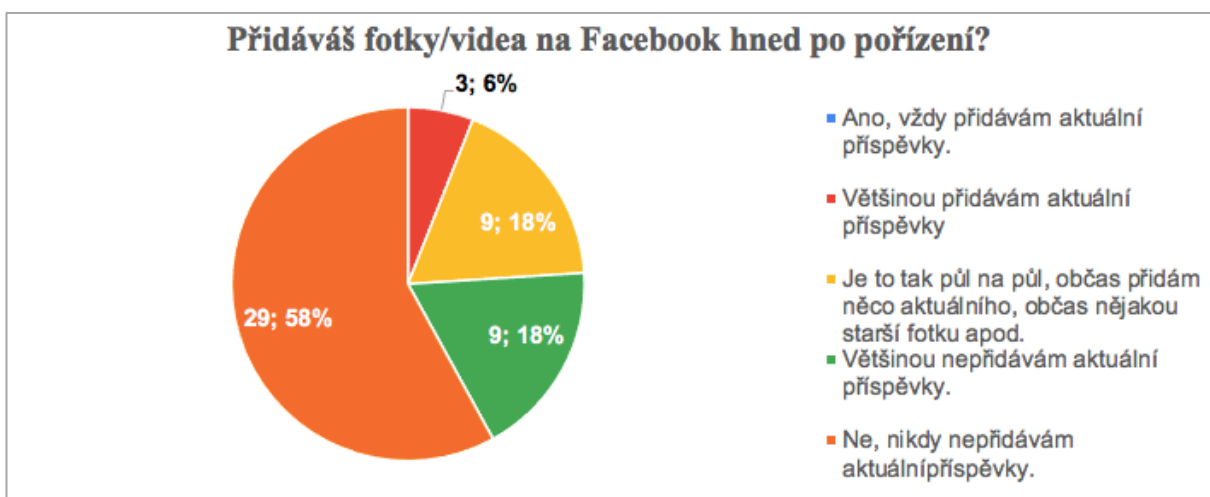
Když už někteří z respondentů něco na Facebook přidávají, tak je to ve 30 % případů sdíleno pouze s přáteli. Ale hned za touto volbou byla často volena i varianta, že sdílí veřejně, konkrétně ve 24 % případů. Detailně viz v *grafu 21*.

Odpovědi na následující otázku (viz *graf 22*), která se týkala toho, jak často respondenti na Facebook přidávají příspěvky, odpovídaly tomu, co jsme se již dozvěděli u těch předchozích. 78 % z nich odpovědělo, že nikdy nebo málo často. A pokud už někdo něco sdílí, tak to jsou spíše výjimky. Pouze 1 respondent odpověděl, že přidává na Facebook příspěvky denně.



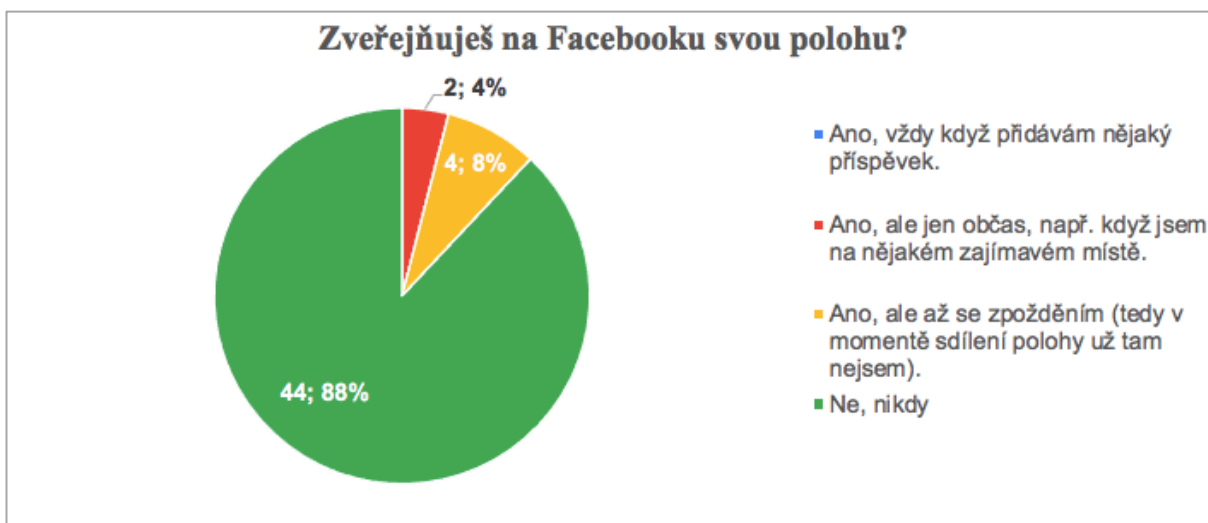
Graf 22 – Četnost přidávání příspěvků na Facebook

Na otázku, zda přidávají na Facebook aktuální příspěvky (např. fotografii hned po jejím pořízení), odpověděla většina respondentů, že *ne*, pouze 6 % z nich odpovědělo, že většinou přidává aktuální příspěvky – viz *graf 23*.



Graf 23 – Aktuálnost přidávaných příspěvků na Facebook

Zveřejňování polohy je něco, co respondenti na Facebooku většinou vůbec nedělají. Pravděpodobně to úzce souvisí i s tím, že na Facebooku moc příspěvků nesdílí. Detailně zobrazeno v *grafu 24*.



Graf 24 – Zveřejňování polohy na Facebooku

Na závěr části otázek týkajících se Facebooku byla ještě otevřená otázka, kde se mohli respondenti vyjádřit, pokud se na Facebooku setkali s něčím, co ohrozilo jejich soukromí. Většina z nich se s ničím takovým nesetkala, pouze 2 odpověděli, že se oni nebo jejich kamarádi stali obětí zcizení účtu.

5.5.4 Odpovědi týkající se digitální stopy a rizik sociálních sítí

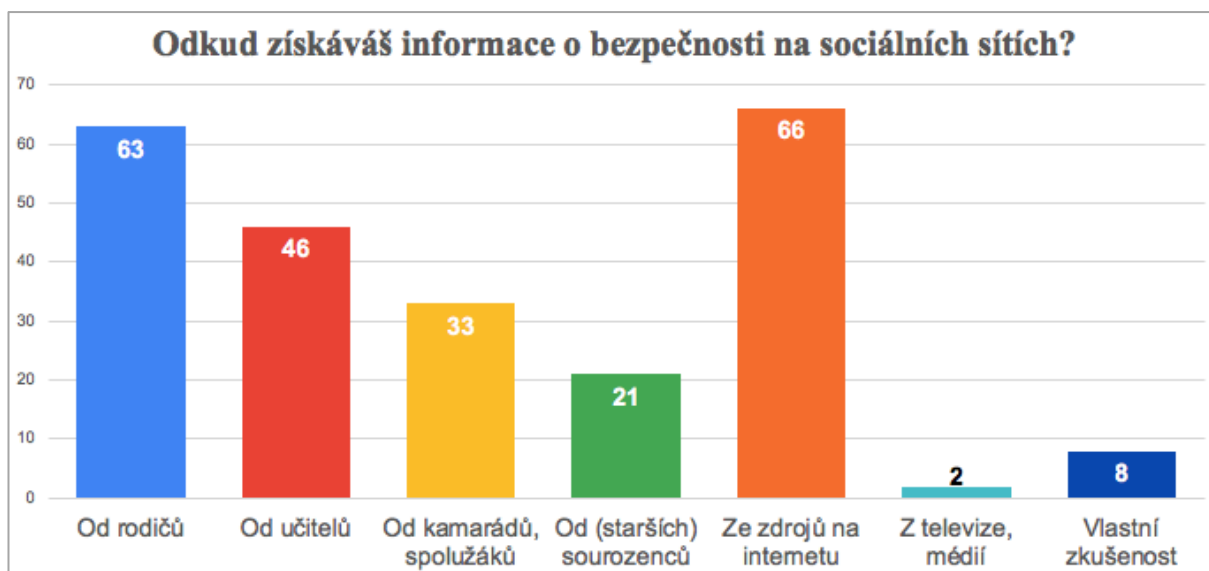
Na otázku, zda respondenti znají pojem digitální stopa, sice kladně odpověděla větší část z nich, ale pouze 24,3 % z nich si myslelo, že zná i význam tohoto pojmu. 41,4 % z nich nevědělo, co tento pojem znamená – viz *graf 25*.

Dále měli respondenti vlastními slovy zkusit vysvětlit, co pojem znamená – pokud v předchozí otázce zvolili, že pojem neznají, měli si alespoň tipnout. Podle odpovědí, které odeslalo 47 z celkových 111 respondentů (otázka, kde měli pojem zkusit vysvětlit nebyla povinná), většina z nich ví nebo správně tuší, co to digitální stopa je – tedy, že je to něco, co po sobě v prostředí internetu zanechávají. Ostatní spíše vůbec neví. Někteří se význam snažili různě odhadovat a pravděpodobně ze slova *stopa* si odvodili, že pojem souvisí se sledování polohy zařízení apod. Detailní odpovědi jsou k dispozici v *příloze č. 3*.



Graf 26 – Znalost pojmu digitální stopa

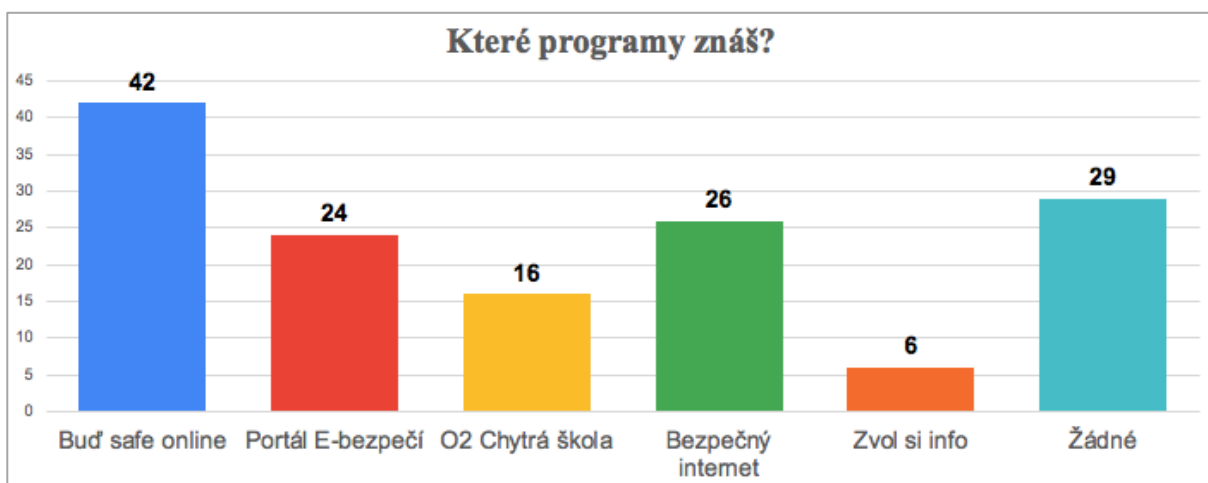
V otázce odkud vlastně čerpají informace o bezpečném chování na sociálních sítích, se nejvíce respondentů shodlo na tom, že od rodičů (63 odpovědí) a ze zdrojů na internetu (66 odpovědí). Své zastoupení ale v odpovědích získaly i ostatní nabízené varianty – 46 respondentů zvolilo, že informace získávají od svých učitelů, 33 od kamarádů a spolužáků a 21 od sourozenců. 8 z nich ještě doplnilo, že se řídí hlavně vlastní zkušeností a 2 čerpají informace také z televize. Detailně je to rozepsáno v *grafu 26*.



Graf 25 – Zdroje čerpání informací o bezpečnosti na sociálních sítích

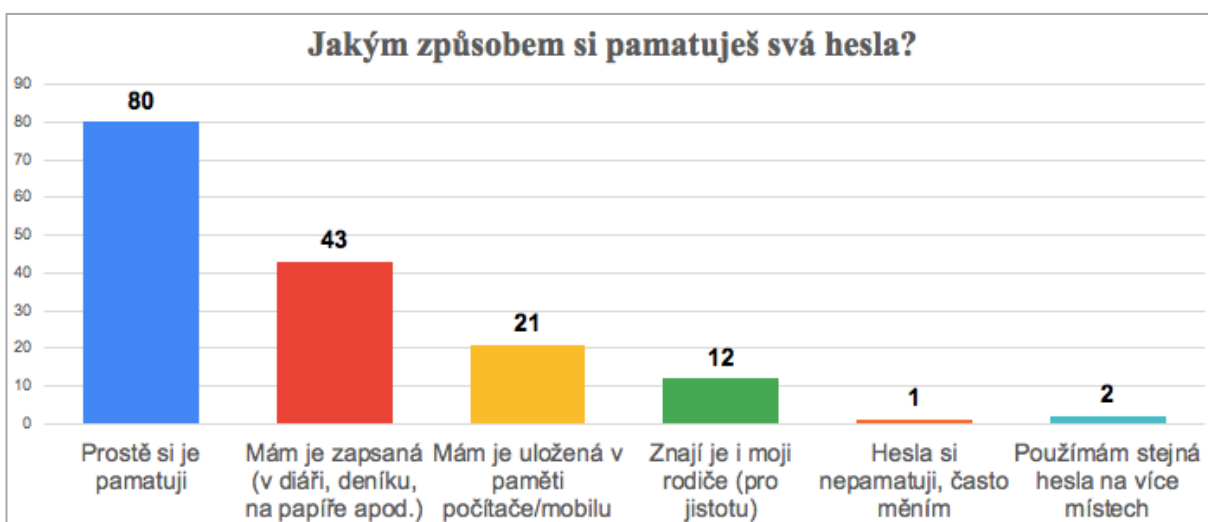
Nejznámějším programem, který se zabývá bezpečím na internetu a sociálních sítích, je mezi respondenty jednoznačně *Bud' safe online*, ale i ostatní vybrané platformy mají v odpovědích své zastoupení – viz *graf 27*. 29 respondentů odpovědělo, že žádný ze zmíněných

programů nezná – lze předpokládat, na základě předchozí otázky, že čerpají informace spíše od rodičů nebo učitelů.



Graf 27 – Znalost programů zabývajících se bezpečností na internetu a sociálních sítích

Co se týče hesel, tak si je většina respondentů (80) prostě pamatuje. Ale značná část z nich vybrala i variantu, že je mají někde zapsaná (43) nebo jejich heslo zná ještě někdo jiný (12). Pouze 21 respondentů odpovědělo, že pro správu hesel používá paměť svého zařízení. Dvě osoby přiznaly, že ve skutečnosti používají jenom několik málo hesel pro všechny aplikace a nástroje (viz graf 28).



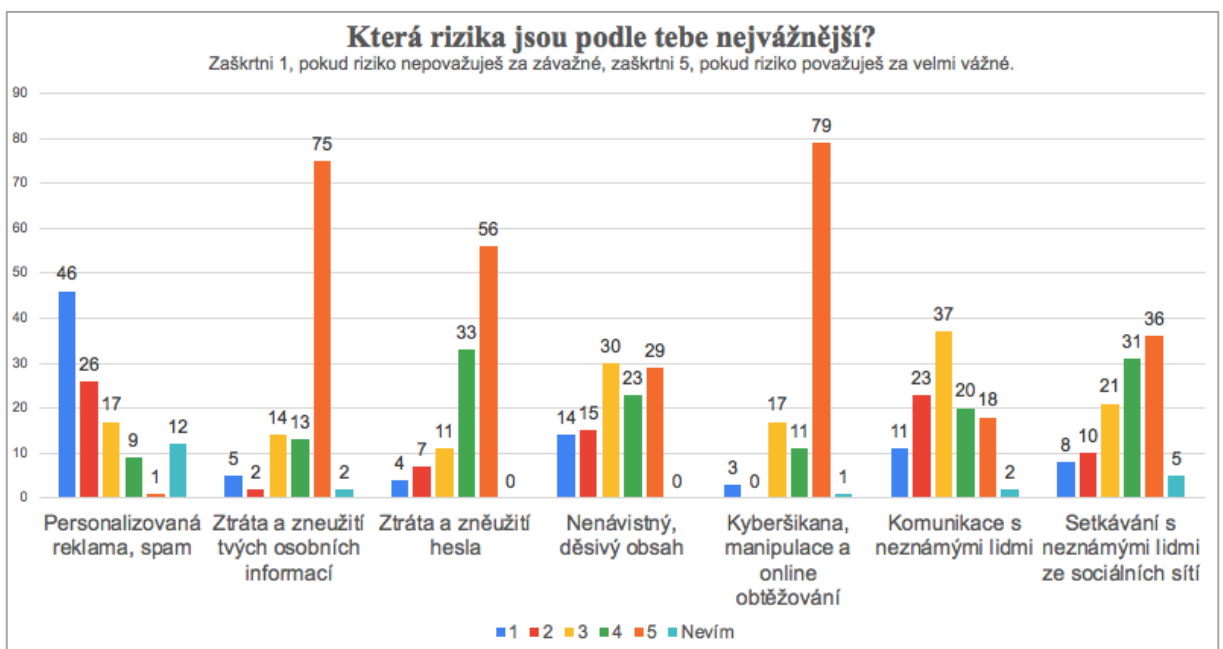
Graf 28 – Způsoby pamatování si hesel

Co se týče ochrany zařízení, která používají respondenti pro přístup k sociálním sítím, nejčastěji je mají chráněna heslem, pinem nebo gestem. Pouze dvanáct respondentů odpovědělo, že zařízení nemá nijak chráněno (viz graf 29).



Graf 29 – Zabezpečení zařízení

V následující otázce měli respondenti ohodnotit vybraná rizika podle jejich vážnosti. Volili mezi hodnotami 1 až 5, přičemž volba 1 znamenala nejnižší riziko a 5 velmi vážné riziko. Jako nejvážnější ohodnotili téměř shodně *kyberšikanu, manipulaci a online obtěžování a ztrátu a zneužití osobních informací*. Na třetím místě by se umístila *ztráta a zneužití hesla*. Nejméně vážné je podle nich *personalizovaná reklama a spam*. Ostatní vybraná rizika skončila s víceméně nerozhodnými odpověďmi (viz graf 30).



Graf 30 – Závažnost rizik

Dále měli respondenti prostor pro to, aby doplnili další rizika, která jim mohou na sociálních sítích hrozit. Většina z 50 odpovědí (tato otázka nebyla pro respondenty povinná) odpověděla, že je nic dalšího nenapadá. Ostatních rizika, která byla zmiňována by se dala zařadit do kategorií v předchozí otázce. Přesto je zde výběr několika nejčastěji zmiňovaných odpovědí na tuto otázku (odpovědi jsou doslovné, zaznamenané přesně tak, jak je respondenti napsali, bez jakýchkoli dalších úprav):

- „Zveřejňování nepravdivých informací o někom i když víme že jim to může ublížit“
- „Závislost“
- „psaní si po sociálních sítích s lidmi kteří jsou poměrně starší a domlouvat si zchůzky na neveřejných místech“
- „posílání nahých fotek“
- „Hacknutí počítače a zneužití bankovního účtu“
- „Sexuální obtěžování.“

Poslední otázka v dotazníku se respondentů ptala na to, zda se někdy na internetu nebo sociálních sítích setkali s něčím, co jim bylo nepříjemné nebo je to nějak ohrožovalo a měli strach. Odpověď na tuto otázku nebyla pro respondenty povinná, ale přesto jich odpovědělo 72. Většina z nich psala, že žádnou negativní zkušenost nemá, ale přesto se v odpovědích několik krátkých příběhů objevilo. Zde na ukázkou zmíníme několik z nich (odpovědi jsou doslovné, zaznamenané přesně tak, jak je respondenti napsali, bez jakýchkoli dalších úprav):

- „Napsali mi cizí lidé že jsem prý moc pěkná jestli bych jim neposlala nahé fotky. Me už od mala rodiče učili abych to nedělala tak jsem jim napsala že ne nesmím a že je to hrozna vec a blokády jsemsi je.“
- „22letý kluk po mne chtěl nahé fotky.Řešila jsem to tím způsobem že jsem to tak že jsem to nejdříve řekla mému kamarádovi který ho znal a hned potom rodičům“
- „Na Instagramu mi začal psát jeden kluk, zdál se jako fajn kluk. Po dlouhé době jsem měla pocit že s ním jsem šťastná. Jenomže zdání klame. Asi po měsíci začal chtít moje fotky. On mi poslal sebe (obličej), nejdřív jsem nechtěla, ale když jsem ho znala už docela dobře, řekla jsem si vlastně proč ne. Byla to chyba. Nezůstalo to jen u fotky obličej. Chtěl po mě víc a víc. Naštěstí jsem mu neposlala žádnou fotku kde by bylo něco vidět. No a tak jsem si ho zablokovala

a vymazala. On si založil další a další účet a začlo to na novo. Svěřila jsem se s tím mojí nejlepší kamarádce, strašně moc se mi ulevilo a věděla jsem, že jsme na něho dvě. Prostě jsem ho začla ignorovat a asi po měsíci to skončilo. Tohle celé se stalo asi tak před rokem, jsem ráda, že už to mám za sebou.“

- „Ano, hlavně když byl kamarádovi zcizen účet. Snažil jsem mu pomoci, a jeho účet jsem si pro jistotu odebral.“
- „Psaní s pedofilem : v tu dobu mi bylo 11 a začal mi psát nějaký chlapek nechutné a sprostě věci tsť jsem si ho zablokovala tak jsem to resila :)“
- „Když se mi někdo naboural na účet na instagramu. Řešila jsem to s mojí starší sestrou, která mi pomohla se nějak rozumněji zachovat. Můj bývalý účet jsme zablokovali, zpětně si myslím, že jsme to mohli vyřešit lépe. Poté jsme udělali nový účet a dali těžší heslo.“

5.6 Interpretace výsledků výzkumu

Při zhodnocení a interpretaci výsledků výzkumu je zde na prvním místě důležité znovu zmínit, že se jednalo o pilotní výzkum, kterého se zúčastnilo jen poměrně malé množství respondentů. Získané výsledky tudíž nelze aplikovat obecně na všechny žáky 8. a 9. tříd, jelikož je více než pravděpodobné, že kdyby se jich zúčastnilo větší množství, podíl jednotlivých odpovědí na otázky by byl odlišný. Tato kapitola se pokusí zhodnotit a interpretovat výsledky provedeného výzkumu v souvislosti s hypotézami a cíli výzkumu, které byly definovány v kapitole 5.1 *Cíle výzkumu, hypotézy*.

Hypotéza č. 1: **Více než polovina žáků 8. a 9. tříd má účet alespoň na jedné sociální síti.**

Již na základě výsledků jiných výzkumů, které byly zmíněny v kapitole 4.5 zaměřené na stávající stav výzkumu, bylo očividné, že pro teenagery jsou sociální sítě důležitou součástí života. Toto potvrdil i výzkum, který byl uskutečněn v rámci této diplomové práce, kde pouze 3 respondenti odpověděli, že žádné sociální sítě nepoužívají.

Obliba sociálních sítí u teenagerů jistě souvisí s dobou, ve které vyrůstají a s technologiemi, které jsou jim dostupné. Jedna z dalších otázek se jich v souvislosti s tím tázala, na kterých zařízeních k sociálním sítím nejčastěji přistupují. Největší množství respondentů (105) zvolilo *chytrý telefon*. Tato volba se jeví jako poměrně logická, jelikož chytré telefony nemusí být pro jejich rodiče tak drahé, navíc jejich prostřednictvím mohou udržovat kontakt se svými dětmi a pokud mají třeba menší byt, nezabere chytrý telefon tolik místa,

jako například stolní počítač. Právě chytrý telefon s připojením k internetu, což je technologie stará pouze něco málo přes 10 let, poskytuje ideální podmínky pro používání sociálních sítí. Například sociální síť Instagram ještě do nedávna nebylo možné používat jinak, a i dnes má její rozhraní v internetových prohlížečích na počítači omezené funkcionality.

Hypotéza č. 2: Žáci 8. a 9. tříd čerpají informace o bezpečnosti na sociálních sítích zejména z internetových zdrojů a programů.

Druhá hypotéza se zaměřovala na to, odkud vlastně žáci 8. a 9. tříd čerpají informace o sociálních sítích a bezpečnosti na nich. Ve výsledcích výzkumu sice potvrdil, že tyto znalosti čerpají z internetových zdrojů, ale skoro stejný počet hlasů získala i odpověď, že je čerpají od svých rodičů. V otázce, která se zajímala o znalost konkrétních programů zabývajících se bezpečností na internetu a sociálních sítích, se však ukázal i fakt, že 29 z celkových 111 respondentů nezná žádný ze zmíněných programů. Někteří z nich uváděli v detailních odpovědích, že sice neznají tyto konkrétní programy, ale když něco neví, tak si to dokážou vyhledat. Několik z nich se vyjádřilo i tak, že se většinu naučili vlastně sami – buď si informace dokázali najít nebo věděli, koho se zeptat. Každopádně je zcela zřejmé, že důležitým zdrojem jsou pro žáky 8. a 9. tříd hlavně jejich rodiče, kteří by je měli ve směru bezpečnosti na internetu a sociálních sítích vést a případně jim radit a doporučovat, kde se o této problematice mohou dozvědět více.

V související otázce týkající se toho, které konkrétní zdroje a programy respondenti znají, získala nejvíce hlasů služba *Bud' safe online*. V tomto programu se aktivně angažuje i jeden z nejznámějších českých influencerů, bývalý youtuber²⁶ Jirka Král, který byl v době, kdy aktivně natáčel videa na YouTube, u dětí oblíbený zejména proto, že ve svých videích hrál a ukazoval počítačové hry. Lze tedy předpokládat, že právě díky němu je tato služba mezi respondenty známější než ty ostatní.

Hypotéza č. 3: Více než polovina respondentů ví, jak si nastavit svůj profil na Facebooku a Instagramu s ohledem na své soukromí – ví, s kým sdílejí své příspěvky, kdo vidí jejich obsah atd.

Třetí hypotéza říkala, že „Více než polovina z nich ví, jak si nastavit svůj profil na Facebooku a Instagramu s ohledem na své soukromí – ví, s kým sdílejí své příspěvky, kdo vidí jejich

²⁶ **Youtuber** je člověk, který pravidelně natáčí videa, která následně nahrává na server YouTube. V těchto videích točí zejména sám sebe a své zájmy.

obsah atd.“ Všichni respondenti výzkumu v rámci této diplomové práce, kteří používají Instagram, věděli, zda mají profil *veřejný* nebo *soukromý*. Přesto, že toto nastavení znali, tak 53 % z nich odpovědělo, že má profil nastavený jako *veřejný* – tzn. každý, komu se daný profil zobrazí, vidí veškerý jeho obsah. Nabízí se vysvětlení, že tito respondenti mají profil takto nastavený, jelikož chtějí získávat více *lajků* a komentářů ke svým příspěvkům. Ale podle odpovědí na další otázky lze soudit, že většina respondentů na Instagram moc příspěvků nepřidává a když už někdo z nich přidává něco častěji, tak jsou to tzv. *stories*, které se sledujícím zobrazují pouze 24 hodin. Je tedy možné, že mají profil nastavený jako *veřejný* prostě proto, že tam nesdílí moc často a když ano, tak to není nic, u čeho by jim vadilo, že to uvidí úplně kdokoli.

Naopak na Facebooku má většina respondentů profil nastavený tak, aby byl jeho obsah zobrazován pouze přátelům. Na Facebook ale také většina z nich nepřidává vůbec žádné příspěvky ani nesdílí polohu. Je tedy možné, že i když někteří z nich mají profil otevřený veřejnosti, moc informací se tam o nich nikdo nedozví. Funkci seznamů přátel na Facebooku více než polovina respondentů znala, ale většina z nich ji nepoužívá. Každopádně lze soudit, že se hypotéza potvrdila. I když někdo odpověděl, že má profil nastavený jako *veřejný*, věděla většina respondentů, že to tak je, tudíž lze předpokládat, že podle toho se i rozhodují, co na sociálních sítích zveřejní.

Hypotéza č. 4: Nejméně polovina respondentů má v přátelích na Facebooku nebo ve sledování Instagramu minimálně jednoho člověka, kterého neznají i osobně.

Čtvrtá hypotéza se týkala přátel na Facebooku, sledujících a sledovaných na Instagramu a toho, zda respondenti tyto osoby znají i osobně, v *offline životě*.

Na Facebooku si největší podíl respondentů (44 %) přidává do přátel pouze ty osoby, která zná i osobně, ale i zde byla řada odpovědí (40 %), kdy respondenti znají osobně pouze větší polovinu svých přátel, a další (8 %), kdy znají osobně pouze polovinu z nich.

Na Instagramu více než polovina z nich sleduje i profily lidí, které osobně neznají. Toto je ale v případě Instagramu poměrně logická volba, jelikož sledování se tam nemusí být vzájemné. Instagramové účty navíc mohou sloužit i jako stránky různých firem, slavných osobností, influencerů apod. (na Facebooku je tento typ účtů nazván *stránka* a funguje jiným způsobem než běžné *přidávání do přátel*). Respondenti znají přibližně polovinu osob, jejichž profily sledují. Sledující, kteří sledují naše respondenty, jsou ve většině případů osoby, se kterými se respondenti znají i osobně. V odpovědích vyšlo, že větší část svých sledujících osobně znají.

Problematika přátel a sledujících však úzce souvisí i s tím, co bylo zmíněno výše pod hypotézou 3. Většina respondentů uvedla, že ani na Instagramu ani na Facebooku příspěvky nesdílí příliš často, tudíž by teoreticky až tak nevadilo, že je sledují i cizí lidé, když se na jejich profilu příliš informací o nich nedozví.

Hypotéza č. 5: Více než 50 % žáků 8. a 9. tříd zná pojem *digitální stopa*.

Poslední hypotéza se týkala digitální stopy. Většina z respondentů pojem znala, ale pouze menší část z nich byla schopna vysvětlit přesný význam. Ze získaných odpovědí lze každopádně soudit, že polovina z nich alespoň přibližně tuší, že tento pojem souvisí s něčím, co po sobě na internetu zanechávají. Někteří se význam snažili různě odhadovat a pravděpodobně ze slova *stopa* si odvodili, že pojem souvisí se sledováním polohy zařízení apod. Hypotéza, že více než 50 % z respondentů pojem zná, se spíše nepotvrdila. Jelikož přesný význam tohoto pojmu není respondentům úplně jasný, je velice důležité s dětmi i o této konkrétní problematice dále mluvit, aby přemýšlely o tom, co na internetu a sociálních sítích zveřejňují.

Každopádně je důležité podívat se na tuto otázku i v souvislosti s ostatními dotazy, které byly respondentům v dotazníku položeny. Jak již bylo představeno v kapitole 5.5, tak větší část respondentů na sociální síť Facebook a Instagram příspěvky příliš často nepřidává. Zároveň většina z nich jen málokdy zveřejňuje u sdílených příspěvků i svou polohu. Z toho lze soudit, že sice možná neznají úplně přesně konkrétní pojem *digitální stopa* a neví, s čím si ho spojit, ale vědí, že to, co na internet jednou nahrají, to tam zůstane (tedy znají obsah pojmu *digitální stopa*), a proto toho nesdílí příliš mnoho.

V závěru této kapitoly by ještě stálo za to zmínit, že dle získaných odpovědí lze soudit, že žáci 8. a 9. tříd spíše vědí, jak se na sociálních sítích chovat tak, aby své soukromí neohrozili. Přestože má velké množství z nich profily nastavené jako veřejné, většina z nich příliš příspěvků s ostatními nesdílí, tudíž o sobě moc soukromých informací nesdělují. A z konkrétních, respondenty popsaných případů, kdy se s něčím ohrožujícím na sociálních sítích setkali, lze soudit, že spíše vědí, že s některými osobami se raději nemají moc bavit, nemají jim posílat žádné své fotografie apod. Většina z nich také uvedla, že ví, jak zablokovat profily těch osob, které je nějakým způsobem obtěžují.

6 Závěr

Tato diplomová práce měla za cíl nastínit problematiku informačního chování žáků 8. a 9. tříd základních škol zejména ve vztahu k ochraně jejich vlastního soukromí. Cílem práce bylo zjistit, jak se vlastně k celé problematice staví, zda se o ochranu svého soukromí na sociálních sítích zajímají a zda jsou si vědomi i asociovaných rizik, která jim v tomto prostředí mohou hrozit. V kvantitativním výzkumu bylo také zjišťováno, jak výše uvedené ovlivňuje jejich chování na vybraných sociálních sítích Facebook a Instagram, zda znají funkcionality, kterými mohou ovlivnit nastavení svých profilů apod.

V práci bylo také nastíněno, že v současnosti je pro teenagery trendem mezi sociálními sítěmi Instagram. Facebook již není pro tuto věkovou skupinu tolik atraktivní, jako tomu bylo ještě před několika lety – lze předpokládat, že je to z velké části také proto, že na Facebooku je dnes aktivní hlavně ta „dospělá generace“, kterou současní teenageři na svých sociálních sítích tolik potkávat nechtějí. V budoucnosti se pravděpodobně do podobného postavení dostane i Instagram, jelikož i jeho uživatelé budou postupně stárnout. Částečně už se to možná děje, jelikož hlavně v letošním roce se dostává na výsluní stále poměrně nová sociální síť – TikTok.

Hlavním problémem sociálních sítí obecně je jejich neuvěřitelně rychlý rozvoj, kdy není neobvyklé, že se během velice krátké doby například úplně změní uživatelské rozhraní aplikací těchto sociálních sítí, což jejich uživatelům může značně snížit orientaci na dané sociální síti obecně, ale hlavně i v možnostech nastavování různých funkcionalit, včetně těch, které souvisejí s ochranou soukromí. Zároveň se stále rozvíjí i potenciální hrozby, které mohou nejenom uživatele sociálních sítí ohrožovat. Proto je důležité, aby právě cílové skupině výzkumu z této diplomové práce bylo s orientací v tomto světě sociálních sítí pomáháno. A to nejenom ze strany rodičů a učitelů, ale měli by být seznámeni i s různými jinými zdroji, které jim mohou v orientaci v této problematice pomáhat a které možná často budou moci teenagerům poskytnout aktuálnější informace – zejména, pokud rodiče nebo učitelé, kteří o tomto se svými dětmi a žáky mluví, sami sociální síť příliš nepoužívají.

Výzkum, který byl proveden v rámci této diplomové práce, byl pouze pilotním šetřením, které by jistě stálo za to uskutečnit i ve větším měřítku – například v rámci celého kraje nebo celé České republiky. Takovéto rozšíření by jistě dodalo přesnější výsledky, které by lépe popisovaly charakteristiku chování této sociální skupiny na sociálních sítích ve vztahu k ochraně vlastního soukromí. Zároveň by mohlo být zajímavé, zaměřit konkrétní otázky i na některé další sociální síť, zejména na velmi rozšířený YouTube a TikTok. Kromě toho by jistě bylo možné tento dotazník rozšířit i na další věkové skupiny. Starší teenageři používají

sociální zcela jistě podobně aktivně jako žáci 8. a 9. tříd. Často jsou to i mladší děti, s jejichž účty se na sociálních sítích můžeme setkat (přestože dle smluvních podmínek sociálních sítí Facebook a Instagram se tam nesmí registrovat nikdo, kdo je mladší než 13 let). Současně by jistě stálo za zvážení dotazník rozšířit i o otázky zaměřené na sharenting a názor respondentů na to, když rodiče sdílí fotky a informace o svých dětech. Případně na to, zda s tímto mají konkrétní zkušenosti a jak se k tomu staví. Výstupy této práce tedy mohou posloužit také jako podklady pro případná další zkoumání této problematiky.

Nejvýraznějším omezením, které výzkum v rámci této diplomové práce provázal, byla jednoznačně komplikovaná situace související se stále probíhající epidemií koronaviru, což mimo jiné způsobilo uzavření všech škol téměř na celé jaro a podzim v roce 2020. Výuka probíhala distančně, a proto byl i dotazník vytvořený v rámci této diplomové práce žákům 8. a 9. tříd distribuován pouze elektronicky. Kdyby žáci mohli dotazníky vyplňovat ve škole během výuky, bylo by pravděpodobně vybráno větší množství odpovědí. Jak již bylo popsáno v předchozích kapitolách, osloveno bylo 170 žáků 8. a 9. tříd ze Základní školy a Mateřské školy Tábor, Husova 1570, ale odpovědí bylo získáno pouze 111.

Možná je škoda, že nebyly ve v dotazníku zahrnuty i otázky týkající se komunikace na Facebooku a Instagramu prostřednictvím soukromých zpráv a komunikace s těmi přáteli, které respondenti osobně neznají – jestli s nimi vůbec nějak komunikují, o čem apod. Někteří respondenti v detailních odpovědích zmiňovali, že pokud jim přijde žádost o přátelství od někoho takového, tak mu napíše zprávu, aby zjistili, kdo to je, jestli se znají nebo jestli je ta osoba prostě sympatická natolik, aby přátelství schválili.

Problematika informačního chování žáků 8. a 9. tříd základních škol zejména ve vztahu k ochraně jejich vlastního soukromí, která byla popsána v této diplomové práci, je stále se rozvíjejícím a aktuálním tématem. Sociální sítě jsou nástroje, které lze považovat za symbol současné doby a stále větší počet lidí se s nimi setkává v každodenním životě. Děti a teenageri nejsou výjimkou. Jejich životy jsou sociálními sítěmi provázeny od velmi útlého věku a pravděpodobně tu s nimi budou i nadále. Proto je důležité, aby byli obeznámeni nejenom s přínosy, které pro ně sociální sítě mohou mít, ale také s hrozícími riziky.

V současné době se navíc stále častěji objevuje další fenomén, který spojuje děti a sociální sítě – *sharenting*. Tato práce ho zmínila jenom velmi okrajově, ale je to něco, co pravděpodobně ovlivní generaci osob, která se narodila v době sociálních sítí. Jelikož se spousta pyšných rodičů na sociálních sítích rádi chlubí svými potomky, sahá digitální stopa těchto dětí mnohem dál, než tomu bylo u předchozích generací. Každopádně toto není

nic, co by mohly ovlivnit sami děti, toto je problematika, která souvisí zejména s informačním chováním jejich rodičů.

Sociální sítě, jak již bylo řečeno, se staly neodmyslitelnou součástí dnešní doby a většinu z nás opravdu provází každodenním životem. Tato práce se zaměřovala zejména na ochranu soukromí dětí a teenagerů, ale zapomínat by na svou bezpečnost neměli ani starší uživatelé sociálních sítí. A kromě ochrany svého vlastního bezpečí by nikdo neměl ohrožovat svým chováním ani ostatní. Je důležité, aby se děti, teenageři i dospělí chovali na sociálních sítích zodpovědně a společně tam vytvářeli prostor, kde se jim rizika budou v ideálním případě úplně vyhýbat.

Seznam použité literatury a zdrojů

1. BARNES, John A., 2016. Class and Committees in a Norwegian Island Parish. *Human Relations* [online]. 7(1), 39-58 [cit. 2020-11-29]. ISSN 0018-7267. Dostupné z: doi:10.1177/001872675400700102
2. BEDNÁŘ, Vojtěch, 2011. *Marketing na sociálních sítích: prosad'te se na Facebooku a Twitteru*. Brno: Computer Press. ISBN 978-80-251-3320-0.
3. BLAŽEK, Zdeněk, 2015. Vznik a historie Facebooku. *Zdeněk Blažek: Marketingový konzultant* [online]. [cit. 2019-09-19]. Dostupné z: <http://www.zdenekblazek.cz/vznik-a-historie-facebooku/>.
4. BOYD, danah, 2008. *Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life*. The MIT Press, Cambridge, Dostupné z: https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=1518924
5. BOYD, danah, 2017. *Je to složitější: sociální život teenagerů na sociálních sítích*. Praha: Akropolis. ISBN 978-80-7470-165-8.
6. BOYD, danah a Nicole ELLISON, 2007. Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication* [online]. 13(1) [cit. 2020-04-11]. Dostupné z: <http://www.danah.org/papers/JCMCIntro.pdf>
7. BOYD, danah a Alice MARWICK, 2014. How Teenagers Negotiate Context in Social Media. *New Media and Society* [online]. 16(7), 1051–1067 [cit. 2020-08-27]. Dostupné z: <https://journals.sagepub.com/doi/10.1177/1461444814543995>
8. CATE, Fred H., 1997. *Privacy in the Information Age*. Brookings Institution Press. ISBN 9780815713159.
9. CRHA, Vladan a Kateřina MAREŠOVÁ. 2020. *AMI Digital Index 2020*. AMI Digital Index. [online]. [cit. 2020-12-15]. Dostupné z: https://index.amidigital.cz/wp-content/uploads/2020/10/ADI-2020_klienti_FINAL-1.pdf
10. ČSÚ, 2020. *Domácnosti v ČR s počítačem – vývoj v čase* [tabulka]. [cit. 2020-11-29]. Dostupné z: <https://www.czso.cz/documents/10180/122362692/0620042013.pdf/2c205a15-7a6e-439f-866d-df330e9ea76b?version=1.1>
11. ČSÚ, 2020. *Domácnosti v ČR s internetem – vývoj v čase* [tabulka]. [cit. 2020-11-29]. Dostupné z: <https://www.czso.cz/documents/10180/122362692/0620042014.pdf/e1d043ea-4b41-4b3c-8149-149ac9410343?version=1.1>

12. ČSÚ, 2019. *Domácnosti v zemích EU s internetem – vývoj v čase* [tabulka]. [cit. 2020-11-29]. Dostupné z:
<https://www.czso.cz/documents/10180/122362692/062004200113.pdf/29a6bb28-53c5-4dc1-ae45-eeb29b935d5e?version=1.1>
13. ČSÚ, 2019. *Jednotlivci v ČR žijící v domácnostech s počítačem a internetem* [tabulka]. [cit. 2020-07-29]. Dostupné z:
<https://www.czso.cz/documents/10180/90577057/062004190114.pdf/d67b508f-a51c-4933-b165-b57062146d5a?version=1.1>
14. ČSÚ, 2020. *Osoby v ČR používající sociální sítě*, [tabulka]. [cit. 2020-11-29]. Dostupné z:
<https://www.czso.cz/documents/10180/122362692/0620042052.pdf/76f76896-4758-480a-8856-9d6658534cba?version=1.1>
15. ČSÚ, 2019. *Osoby v zemích EU používající sociální sítě – vývoj v čase* [tabulka]. [cit. 2020-11-29]. Dostupné z:
<https://www.czso.cz/documents/10180/122362692/0620042055.pdf/59e558f6-ba0b-4156-84ad-8f0fec616308?version=1.1>
16. DE WOLF, Ralf, 2020. Contextualizing how teens manage personal and interpersonal privacy on social media. *NewMedia & Society* [online]. **22**(6), 1058-1075 [cit. 2020-11-30]. ISSN 1461–4448. Dostupné z: doi:10.1177/1461444819876570
17. DEDKOVA, Lenka, Alena CERNA, Katerina JANASOVA a Kristian DANEBACK, 2014. Meeting online strangers offline: The nature of upsetting experiences of adolescent girls. *Communications* [online]. **39**(3) [cit. 2020-11-30]. ISSN 1613-4087. Dostupné z: doi:10.1515/commun-2014-0115
18. DĚDEČKOVÁ, Adéla, 2012. *Paradoxní zveřejňování soukromí v prostředí Facebooku*. Praha. Diplomová práce. Univerzita Karlova, Pedagogická fakulta, Katedra psychologie. Vedoucí práce PhDr. Miroslav Klusák, CSc. Dostupné z:
<http://hdl.handle.net/20.500.11956/49550>
19. Digitální stopa, ©2013. *Wikisofia* [online]. [cit. 2020-11-30]. Dostupné z:
https://wikisofia.cz/wiki/Digitáln%C3%AD_stopa
20. Dospívání, ©2020. *WikiSkripta* [online]. [cit. 2020-08-18]. Dostupné z:
<https://www.wikiskripta.eu/index.php?title=Dosp%C3%ADván%C3%AD&oldid=439375>
21. HOFREITR, Jiří, 2015. Marketing na Instagramu? Jde to a velmi dobře! *Clipsan: Platforma pro digitální marketing a efektivní prodej* [online]. [cit. 2020-01-15]. Dostupné z: <https://clipsan.com/blog/marketing-na-instagramu-jde-velmi-dobre/>

22. JANOUC, Viktor, 2010. *Internetový marketing: prosad'te se na webu a sociálních sítích*. Brno: Computer Press. ISBN 978-80-251-2795-7.
23. KARLÍČEK, Miroslav, 2016. *Marketingová komunikace: jak komunikovat na našem trhu*. 2., aktualizované a doplněné vydání. Praha: Grada Publishing. ISBN 978-80-247-5769-8.
24. KIRKPATRICK, David, 2011. *Pod vlivem Facebooku: příběh z nitra společnosti, která spojuje svět*. Brno: Computer Press. ISBN 978-80-251-3573-0.
25. KNAP, Karel, 2004. *Ochrana osobnosti podle občanského práva*. 4., podstatně přeprac. a dopl. vyd. Praha: Linde. ISBN 80-720-1484-6.
26. LIVINGSTONE, Sonia, Leslie HADDON, Anke GÖRZIG, and Kjartan ÓLAFSSON, 2011. *Risks and safety on the internet: the perspective of European children: full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries*. EU Kids Online: London [online]. [cit. 2020-07-03]. Dostupné z: <http://eprints.lse.ac.uk/33731/>
27. MARTIN, Florence, Chuang WANG, Teresa PETTY, Weichao WANG a Patti WILKINS. 2018. Middle School Students' Social Media Use. *Educational Technology* [online]. **21**(1), 213-224 [cit. 2020-10-11]. ISSN 14364522. Dostupné z: https://www.jstor.org/stable/26273881?seq=1#metadata_info_tab_contents
28. MATOUŠEK, Oldřich, 2016. *Slovník sociální práce*. Vydání třetí. Praha: Portál. ISBN 978-80-262-1154-9.
29. MULLEN, Caron a Nicola FOX HAMILTON, 2016. Adolescents' response to parental Facebook friend requests: The comparative influence of privacy management, parent-child relational quality, attitude and peer influence. *Computers in Human Behavior* [online]. **60**, 165-172 [cit. 2020-11-30]. ISSN 07475632. Dostupné z: doi:10.1016/j.chb.2016.02.026
30. NOVOTNÝ, Michal, 2020. Žebříček TOP 10: Nejoblíbenější sociální sítě. *Markomu.cz* [online]. [cit. 2020-11-30]. Dostupné z: <https://www.markomu.cz/nejoblibenejsi-socialni-site/>
31. PFLANZER, Tomas. 2020. Instameet 2020 [online] [cit. 2020-12-10]. Dostupné z: <https://www.slideshare.net/gizmax/instameet-2020>
32. Podmínky použití Instagramu, 2020. *Facebook* [online]. [cit. 2020-12-14]. Dostupné z: https://help.instagram.com/1215086795543252?helpref=page_content
33. PRENSKY, Marc a Bruce D. BERRY, 2001. *Do they really think differently* [online]. **9**(6) [cit. 2020-12-04]. Dostupné z:

<https://faculty.ontariotechu.ca/kay/courses/educ5303g/resources/Prensky/Chapter%205%20-%20Digital%20Immigrants%20Digital%20Natives%20-%20Part%202.pdf>

34. RIDEOUT, Victoria J., Ulla G. FOEHR a Donald F. ROBERTS. © 2010. *Generation M²: Media in the Lives of 8–18 Year-Old*. California. Henry J. Kaiser Family Foundation. Dostupné z: <https://www.kff.org/wp-content/uploads/2013/04/8010.pdf>
35. ROSTECKÝ, Jiří, 2020. Kdo je to influencer? *MladýPodnikatel.cz* [online]. [cit. 2020-02-28]. Dostupné z: <https://mladypodnikatel.cz/stitek/influencer>
36. SMAHEL David, Hana MACHACKOVA, Giovanna MASCHERONI, Lenka DEDKOVA, Elisabeth STAKSRUD, Kjartan ÓLAFSSON, Sonia LIVINGSTONE a Uwe HASENBRINK. 2020. EU Kids Online 2020: Survey results from 19 countries. EU Kids Online. Dostupné z: <https://irtis.muni.cz/media/3218267/eu-kids-online-2020-16march2020.pdf>
37. Smluvní podmínky, 2020. *Facebook* [online]. [cit. 2020-12-14]. Dostupné z: <https://www.facebook.com/legal/terms>
38. Sociální sítě, 2018. *Internetem bezpečně* [online]. [cit. 2020-08-11]. Dostupné z: <https://www.internetembezpecne.cz/internetem-bezpecne/socialni-media/socialni-site/>
39. Sociální sítě, ©2012. *WikiKnihovna.cz* [online]. [cit. 2020-08-06]. Dostupné z: http://wiki.knihovna.cz/index.php?title=Sociáln%C3%AD_s%C3%ADtĕ
40. Sociální sítě. ©2012. *WikiKnihovna.cz* [online]. [cit. 2020-08-06]. Dostupné z: http://wiki.knihovna.cz/index.php?title=Sociáln%C3%AD_s%C3%ADtĕ
41. SPITZER, Manfred, 2014. *Digitální demence: jak připravujeme sami sebe a naše děti o rozum*. Brno: Host. ISBN 978-807-2948-727.
42. STEINBERG, Stacey B., 2016. Sharenting: Children's Privacy in the Age of Social Media. *Emory Law Journal* [online]. **66**(4), 839-884 [cit. 2019-01-24]. ISSN 0094-4076. Dostupné z: <https://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1796&context=facultypub>
43. SVOBODOVÁ, Lucie, 2016. *Facebook a Instagram jako součást životního stylu mládeže – kvalitativní výzkum o způsobu chování teenagerů na sociálních sítích*. Praha. Diplomová práce. Univerzita Karlova, Fakulta sociálních věd, Katedra mediálních studií. Vedoucí práce PhDr. Lenka Vochocová, Ph.D. Dostupné z: <http://hdl.handle.net/20.500.11956/83052>
44. ŠEVČÍKOVÁ, Anna et al., 2014. *Děti a dospívající online: vybraná rizika používání internetu*. Praha: Grada. ISBN 978-80-210-7527-6.

45. TAPSCOTT, Don, 2009. *Grown up digital: how the net generation is changing your world*. New York: McGraw-Hill. ISBN 978-0-07-150863-6.
46. Tipy k zabezpečení. 2020. *Instagram* [online]. [cit. 2020-07-15]. Dostupné z: [https://www.facebook.com/help/instagram/377830165708421/?helpref=hc_fnav&bc\[0\]=Nápověda%20pro%20Instagram&bc\[1\]=Centrum%20soukrom%C3%AD%20a%C2%A0bezpečnosti](https://www.facebook.com/help/instagram/377830165708421/?helpref=hc_fnav&bc[0]=Nápověda%20pro%20Instagram&bc[1]=Centrum%20soukrom%C3%AD%20a%C2%A0bezpečnosti)
47. UHLS, Yalda T., 2018. *Mediální mámy a digitální tátové: rady, které na internetu nenajdete*. Praha: Portál. ISBN 978-80-262-1317-8.
48. VESECKÝ, Zdeněk, 2016. #Instagram. Obrázky se může skvěle prezentovat architekt i zedník. *Podnikatel.cz: Průvodce vašim podnikáním* [online]. [cit. 2020-01-15]. Dostupné z: <https://www.podnikatel.cz/clanky/instagram-obrazky-se-muze-skvele-prezentovat-architekt-i-zednik/>
49. WARCHAR, Petr, 2015. Jak vznikl Instagram? Od nuly až k Facebooku. *Instagram CZ: Recenze tipy a triky* [online]. [cit. 2020-01-15]. Dostupné z: <http://www.instagram.cz/jak-vznikl-instagram-od-nuly-az-k-facebooku/362>
50. WESTIN, Alan F. 1967. *Privacy and freedom*. London: The Bodley Head. ISBN 068-91-0289-5.
51. WHITTY, Monica a Gary YOUNG, 2017. *Cyberpsychology: the study of individuals, society and digital technologies*. Chichester: Wiley. ISBN 978-0-470-97562-6.
52. WILLOUGHBY, Mark, 2019. A review of the risks associated with children and young people's social media use and the implications for social work practice. *Journal of Social Work Practice* [online]. **33**(2), 127-140 [cit. 2020-10-04]. Dostupné z: doi:10.1080/02650533.2018.1460587
53. WIDIYANINGSIH, Yohana, Helmy P. YUWINANTO a Fitri MUTIA. 2020. Privacy Protection Behavior of Instagram Users in Middle School Students in Surabaya City. *Talent Development* [online]. **12**(2), 443-451 [cit. 2020-10-11]. ISSN 1869-0459. Dostupné z: <https://iratde.com/index.php/jtde/article/view/204>
54. Zajištění ochrany a zabezpečení. 2020. *Facebook* [online]. [cit. 2020-07-14]. Dostupné z: <https://www.facebook.com/about/basics/stay-safe-and-secure>
55. Zásady Instagramu ohledně používání dat. 2020. *Instagram* [online]. [cit. 2020-07-15]. Dostupné z: [https://www.facebook.com/help/instagram/519522125107875/?helpref=hc_fnav&bc\[0\]=Nápověda%20pro%20Instagram&bc\[1\]=Centrum%20soukrom%C3%AD%20a%C2%A0bezpečnosti](https://www.facebook.com/help/instagram/519522125107875/?helpref=hc_fnav&bc[0]=Nápověda%20pro%20Instagram&bc[1]=Centrum%20soukrom%C3%AD%20a%C2%A0bezpečnosti)

56. Zásady komunity. 2020. *Facebook* [online]. [cit. 2020-07-14]. Dostupné z: <https://www.facebook.com/communitystandards/>
57. Zásady komunity Instagram. 2020. *Instagram* [online]. [cit. 2020-07-14]. Dostupné z: [https://www.facebook.com/help/instagram/477434105621119/?helpref=hc_fnav&bc\[0\]=Nápověda%20pro%20Instagram&bc\[1\]=Centrum%20soukrom%C3%AD%20a%C2%A0bezpečnosti](https://www.facebook.com/help/instagram/477434105621119/?helpref=hc_fnav&bc[0]=Nápověda%20pro%20Instagram&bc[1]=Centrum%20soukrom%C3%AD%20a%C2%A0bezpečnosti)
58. Zásady používání dat. 2020. *Facebook* [online]. [cit. 2020-07-14]. Dostupné z: <https://www.facebook.com/about/privacy>
59. Základy soukromí na Facebooku. 2020. *Facebook* [online]. [cit. 2020-07-14]. Dostupné z: <https://www.facebook.com/about/basics>

Seznam tabulek

Tabulka 1 – Statistika ČSÚ: Domácnosti v ČR s počítačem, vybrané údaje z tabulky (v %, podíl z celkového počtu domácností v dané skupině).....	33
Tabulka 2 – Statistika ČSÚ: Domácnosti v ČR s připojením k internetu, vybrané údaje z tabulky (v %, podíl z celkového počtu domácností v dané skupině)	34
Tabulka 3 – Statistika ČSÚ: Jednotlivci v ČR žijící v domácnostech s počítačem a internetem, 2019, vybrané údaje z tabulky (v %, podíl z celkového počtu jednotlivců v dané socio-demografické skupině).....	35
Tabulka 4 – Statistika ČSÚ: Osoby v zemích EU používající sociální sítě – vývoj v čase, 2019, vybrané údaje z tabulky (v %, podíl z celkového počtu osob ve věku 16-74 let v daném státě)	36
Tabulka 5 – Klasifikace online rizik (Ševčíková et al., 2014, s.10)	42

Seznam grafů

Graf 1 – Počet žáků v 8. a 9. třídách	53
Graf 2 – Odpovědi na otázku: „Používáš nějaké sociální sítě?“	55
Graf 3 – Sociální sítě, které respondenti používají	55
Graf 4 – Zařízení, která respondenti používají k prohlížení sociálních sítí	56
Graf 5 – Čas, který respondenti stráví na sociálních sítích	56
Graf 6 – Čas strávený na sociálních sítích v karanténě	57
Graf 7 – Odpovědi na otázku ohledně nastavení soukromí profilu na Instagramu	58
Graf 8 – Počty sledovaných a sledujících na Instagramu	58
Graf 9 – Sledovaní a sledující, znají je respondenti osobně?	59
Graf 10 – Četnost přidávání příspěvků na Instagram	59
Graf 11 – Aktuálnost přidávaných příspěvků	60
Graf 12 – Obsah příspěvků na Instagramu	60
Graf 13 – Zveřejňování polohy na Instagramu	61
Graf 14 – Nastavení profilu na Facebooku respondenty	62
Graf 15 – Profilová fotografie na Facebooku	62
Graf 16 – Počet přátel na Facebooku	63
Graf 17 – Znají respondenti své přátele osobně?	63
Graf 18 – Kritéria respondentů pro schválení přítele	64
Graf 19 – Znalost funkce seznamů přátel	65
Graf 20 – Obsah sdílených příspěvků na Facebook	65
Graf 21 – Nastavení sdílených příspěvků na Facebook	65
Graf 22 – Četnost přidávání příspěvků na Facebook	66
Graf 23 – Aktuálnost přidávaných příspěvků na Facebook	66
Graf 24 – Zveřejňování polohy na Facebooku	67
Graf 25 – Znalost pojmu digitální stopa	68
Graf 26 – Zdroje čerpání informací o bezpečnosti na sociálních sítích	68
Graf 27 – Znalost programů zabývajících se bezpečností na internetu a sociálních sítích	69
Graf 28 – Způsoby pamatování si hesel	69
Graf 29 – Zabezpečení zařízení	70
Graf 30 – Závažnost rizik	70

Přílohy

Seznam příloh

Příloha 1 – Dotazník

Příloha 2 – E-mail rodičům

Příloha 3 – Odpovědi respondentů

Příloha 1 – Dotazník

Soukromí na sociálních sítích?

08.11.20 16:14

Soukromí na sociálních sítích?

Dotazník, který se právě chystáš vyplňovat, se zaměřuje na sociální sítě Instagram a Facebook, zejména s ohledem na ochranu tvého soukromí. Nemusíš se bát odpovídat naprosto pravdivě, všechny odpovědi jsou úplně anonymní :-). A nezapomínej, že zde nejsou správné a špatné odpovědi.

Výsledky dotazníku budu zpracovávat ve své diplomové práci na Univerzitě Karlově, kde studuji obor zaměřený na informační vědu. A opravdu mi tvé odpovědi velmi pomohou. Takže ti ještě jednou moc děkuji. Navíc je dost možné, že se v dotazníku dovíš i něco nového :-)

Helena

P.S. Tento dotazník je určen pouze žákům 8. a 9. tříd.

***Povinné pole**

1. Používáš nějaké sociální sítě? *

Označte jen jednu elipsu.

Ano Přeskočte na otázku 4

Ne Přeskočte na otázku 2

**Nepoužívání
sociálních sítí**

Jelikož jsi v první otázce odpověděl/a, že sociální sítě nepoužíváš, tak jsi byl/a přeměrován/a na tuto sekci.

2. Proč nepoužíváš sociální sítě? *

Označte jen jednu elipsu.

Nechci.

Nemám počítač, chytrý telefon apod.

Rodiče mi to zakázali.

Nevím

Jiné: _____

3. Zde máš prostor popsat detailněji, proč sociální sítě nepoužíváš - pokud tedy chceš :-)

Přeskočte na otázku 33

Sociální sítě všeobecně

První část dotazníku se zaměřuje na sociální sítě obecně

4. Jaké technologie používáš k prohlížení sociálních sítí? *

Můžeš vybrat více možností.

Zaškrtněte všechny platné možnosti.

Stolní počítač

Notebook

Chytrý telefon

Tablet nebo iPad

Jiné: _____

5. Sleduješ přes nějaký nástroj, kolik času na sociálních sítích denně strávíš? *

Označte jen jednu elipsu.

Ano.

Ne, čas pouze odhaduji.

6. Kolik času denně strávíš na sociálních sítích? *

Stačí přibližně :-)

Označte jen jednu elipsu.

- Méně než 1 hodinu
- Maximálně 2 hodiny
- Maximálně 4 hodiny
- Maximálně 6 hodin
- Maximálně 8 hodin
- Více než 8 hodin
- Nevím

7. Zvýšil se čas, který strávíš na sociálních sítích kvůli distanční výuce a karanténě? *

Označte jen jednu elipsu.

- Ano, trávím tam minimálně 2x více času než dříve
- Ano, trávím tam o něco více času než dříve
- Ne, trávím tam přibližně stejný čas jako dříve
- Ne, trávím tam méně času než dříve
- Nevím

Instagram

Další část dotazníku se zaměřuje na sociální síť Instagram. Pokud ale odpovíš na následující otázku "ne", budeš přesměrován/a rovnou na další sekci.

8. Používáš sociální síť Instagram? *

Označte jen jednu elipsu.

- Ano *Přeskočte na otázku 9*
- Ne *Přeskočte na otázku 18*

Instagram

Jelikož jsi v předchozí otázce odpověděl/a, že sociální síť instagram používáš, mám tu teď pro tebe připraveno několik otázek právě o Instagramu.

9. Jak máš nastavený svůj profil na Instagramu? *

Označte jen jednu elipsu.

- Jako veřejný
 Jako soukromý

10. Kolik lidí/profilů sleduješ ty a kolik sledujících sleduje tvůj profil na Instagramu? Vyber: *

Označte jen jednu elipsu na každém řádku.

	0 až 100	101 až 200	201 až 500	501 a více	Nevím
Já sleduji:	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mě sleduje:	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

11. Sleduješ na Instagramu pouze ty uživatele, které znáš i v „offline životě“? *

= ty, které sleduješ ty

Označte jen jednu elipsu.

- Ano, všechny znám osobně
 Ano, větší část z nich znám osobně
 Osobně znám přibližně polovinu z těch lidí, které sleduji
 Ne, znám osobně jenom menší část z nich
 Ne, nikoho z nich neznám osobně

12. Znáš osobně své sledující? *

= ty, kteří sledují tebe

Označte jen jednu elipsu.

- Ano, všechny své sledující znám osobně.
- Ano, větší část z nich znám osobně
- Osobně znám přibližně polovinu z těch lidí, kteří mě sledují
- Ne, znám osobně jenom menší část z nich
- Ne, nikoho z nich neznám osobně

13. Jak často přidáváš na Instagram: *

1 = méně často/nikdy, 2 = jednou měsíčně, 3 = několikrát za měsíc, 4 = jednou za týden, 5 = několikrát za týden, 6 = jednou denně, 7 = několikrát denně

Označte jen jednu elipsu na každém řádku.

	1	2	3	4	5	6	7	Nevím
příspěvky na profil	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
stories	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
reels	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

14. Přidáváš fotky/videa na Instagram hned po pořízení? *

Označte jen jednu elipsu.

- Ano, vždy přidávám aktuální příspěvky/stories.
- Většinou přidávám aktuální příspěvky.
- Je to tak půl na půl, občas přidám něco aktuálního, občas nějakou starší fotku apod.
- Většinou nepřidávám aktuální příspěvky.
- Ne, nikdy nepřidávám aktuální příspěvky.

15. Co je nejčastěji na fotkách/videích, které/á na Instagram přidáváš? *

Můžeš vybrat více možností.

Zaškrtněte všechny platné možnosti.

- já, moje selfies
- moji kamarádi
- moje rodina
- výlety, dovolené apod.
- moji mazlíčci nebo jiná zvířátka
- moje koníčky

Jiné: _____

16. Zveřejňuješ na Instagramu svou polohu? *

Označte jen jednu elipsu.

- Ano, vždy když přidávám nějaký příspěvek.
- Ano, ale jen občas, např. když jsem na nějakém zajímavém místě, na dovolené apod.
- Ano, ale až později (tedy v momentě sdílení polohy už tam nejsem).
- Ne, nikdy

17. Setkal/a jsi se někdy na Instagramu s něčím, co přímo ohrozilo tvé soukromí?

Facebook

Následující část dotazníku se zaměřuje na sociální síť Facebook. Pokud ale odpovíš na následující otázku "ne", budeš přesměrován/a rovnou na další sekci.

18. Používáš sociální síť Facebook? *

Označte jen jednu elipsu.

- Ano *Přeskočte na otázku 19*
- Ne *Přeskočte na otázku 32*

Facebook

Jelikož jsi v předchozí otázce odpověděl/a, že sociální síť Facebook používáš, mám tu teď pro tebe připraveno několik otázek právě o Facebooku.

19. Jakým způsobem máš nastavený svůj osobní profil na Facebooku? *

Označte jen jednu elipsu.

- Můj profil je celý veřejný (tj. obsah na něm vidí všichni)
- Můj profil je z větší části veřejný (tj. větší část obsahu na mém profilu je veřejná, ale viditelnost některých příspěvků omezují pouze na přátele/vybrané uživatele)
- Můj profil je z menší části veřejný (tj. veřejná je pouze profilová a úvodní fotka a několik informací o mé osobě, např. místo bydliště, název školy apod.)
- Můj profil je viditelný pouze mým přátelům (tj. veřejná je pouze profilová a úvodní fotka)
- Nevím (asi používám základní nastavení)

20. Jak vypadá tvoje profilová fotografie? *

Označte jen jednu elipsu.

- Je na ní detail mého obličeje
- Je na ní snímek celé mé postavy
- Je na ní něco jiného než já (kreslený obrázek, fotografie celebrity apod.)
- Nemám nastavenou žádnou profilovou fotografii

21. Kolik máš na Facebooku přátel?

*

Označte jen jednu elipsu.

- 0 až 100
- 101 až 200
- 201 až 300
- 301 a více
- Nevím

22. Přidáváš si mezi přátele jenom lidi, které znáš i v osobním životě. *

Označte jen jednu elipsu.

- Ano, všechny své přátele znám i osobně
- Více než polovinu svých přátel znám osobně
- Přibližně polovinu svých přátel znám osobně
- Méně než polovinu svých přátel znám osobně
- Ne, nemám v přátelích lidi, které znám osobně

23. Podle jakých kritérií vyhodnocuješ zda schválíš žádost o přátelství? *

Můžeš vybrat více možností.

Zaškrtněte všechny platné možnosti.

- známe se osobně
- máme na Facebooku společné přátele
- má sympatickou profilovou fotku
- nejprve té osobě pošlu zprávu, abych zjistil/a, kdo to je
- nepřemýšlím o tom, automaticky žádost schvaluju
- nevím

Jiné: _____

24. Pokud ti přijde žádost o přátelství od někoho, koho osobně neznáš, jak se zachováš?

Seznamy přátel na Facebooku

Na Facebooku si můžeš své přátele rozdělit do seznamů podle toho, jak moc je znáš. Facebook pak podle toho sdílí více ne méně tvých příspěvků s osobami z těchto seznamů.

Připravené jsou seznamy „blízcí přátelé“, „známí“ a „omezeno“, ale vytvořit si můžeš i vlastní. Facebook potom automaticky sdílí například více tvého obsahu s lidmi v seznamu „blízkých přátel“ nebo nezobrazí tvůj obsah těm, které máš v seznamu „omezeno“.

25. Znáš funkci seznamů přátel? *

Označte jen jednu elipsu.

- Ano znám a používám.
- Ano znám, ale nepoužívám.
- Ne (až teď jsem se o ní dozvěděl/a)

26. Jaký typ příspěvků na svůj Facebook nejčastěji přidáváš? *

Můžeš vybrat více možností.

Zaškrtněte všechny platné možnosti.

- Selfies nebo jiné fotky se sebou
- Fotky s kamarády
- Fotky s rodinou
- Fotky se zvířátky, mazlíčky
- Fotky svých koníčků
- Píšu statusy
- Sdílím příspěvky ostatních
- Nic na Facebook nepřidávám

27. S jakým nastavením nejčastěji sdílíš své příspěvky na Facebook? *

Označte jen jednu elipsu.

- Veřejně
- Pouze se svými přáteli
- Pouze s vybranou skupinou přátel
- Nevím
- Jiné: _____

28. Jak často přidáváš příspěvky na Facebook? *

Označte jen jednu elipsu.

- několikrát denně
- jednou denně
- několikrát za týden
- jednou za týden
- několikrát za měsíc
- jednou měsíčně
- méně často/nikdy
- nevím

29. Přidáváš fotky/videoa na Facebook hned po pořízení? *

Označte jen jednu elipsu.

- Ano, vždy přidávám aktuální příspěvky.
- Většinou přidávám aktuální příspěvky.
- Je to tak půl na půl, občas přidám něco aktuálního, občas nějakou starší fotku apod.
- Většinou nepřidávám aktuální příspěvky.
- Ne, nikdy nepřidávám aktuální příspěvky.

30. Zveřejňuješ na Facebooku svou polohu? *

Označte jen jednu elipsu.

- Ano, vždy když přidávám nějaký příspěvek.
- Ano, ale jen občas, např. když jsem na nějakém zajímavém místě.
- Ano, ale až se zpožděním (tedy v momentě sdílení polohy už tam nejsem).
- Ne, nikdy

31. Setkal/a jste se někdy na Facebooku s něčím, kdy jsi měl/a pocit, že by něco mohlo ohrozit tvé soukromí?

Ostatní sociální sítě

32. Které další sociální sítě používáš? (Kromě Instagramu a Facebooku) *

Můžeš vybrat více možností.

Zaškrtněte všechny platné možnosti.

- YouTube
- TicTok
- Twitter
- Snapchat
- Žádnou další sociální síť nepoužívám

Jiné: _____

Přeskočte na otázku 33

Digitální stopa

33. Znáš pojem "digitální stopa"? *

Označte jen jednu elipsu.

- Ano znám a vím, co to znamená
- Ano znám, ale nevím, co to znamená
- Ne neznám

34. Zkus pojem "digitální stopa" krátce vysvětlit. Pokud nevíš, co to znamená, zkus si alespoň tipnout. *

Digitální stopa (vysvětlení)

Digitální stopa je informace zanechaná uživatelem v prostředí internetu nebo jako součást souborů. Digitální stopa se dále dělí na aktivní a pasivní digitální stopu.

Aktivní digitální stopa zahrnuje veškeré informace, které o sobě uživatel dobrovolně a vědomně zveřejní prostřednictvím různých služeb - profily a následné příspěvky zanechané na sociálních sítích, emaily, sms, historie chatu, různé úřední údaje...

Pasivní digitální stopa zahrnuje informace, které bez našeho přímého záměru vznikají při interakci v prostředí internetu - IP adresa, vyhledávané výrazy na internetu, údaje o času stráveném na určité webové stránce (cookies), poskytovatel připojení, lokace...

V dnešní době může být jakákoliv aktivita v online prostředí zaznamenána a uložena a může mít určitou vypovídací hodnotu o uživateli, který je zanechal. A jak Vám jistě již došlo, tyto informace lze různými způsoby zneužívat (krádež dat, kyberšikana, kyberstalking,...).

Pokud by Vás zajímalo více, můžete se podívat například zde: https://wikisofia.cz/wiki/Digitáln%C3%AD_stopa

Rizika sociálních sítí

V této části se zaměříme na rizika, která ti na sociálních mohou hrozit. Opět se nemusíš bát odpovídat pravdivě, veškeré odpovědi jsou anonymní. Zároveň se zde dozvíš i něco málo o tom, kde hledat informace o prevenci a obraně proti těmto rizikům.

35. Odkud získáváš informace o bezpečnosti na sociálních sítích? *

Můžeš vybrat více možností.

Zaškrtněte všechny platné možnosti.

- Od rodičů
- Od učitelů
- Od kamarádů, spolužáků
- Od (starších) sourozenců
- Ze zdrojů na internetu

Jiné: _____

36. Zaškrtni programy, které znáš: *

Můžeš vybrat více možností.

Zaškrtněte všechny platné možnosti.

- Bud' safe online (budsafeonline.cz)
- Portál E-bezpečí (e-bezpeci.cz)
- O2 Chytrá škola (o2chytraskola.cz)
- Bezpečný internet (bezpecnyinternet.cz)
- Zvol si info (zvolsi.info)

Jiné: _____

37. Jakým způsobem si pamatuješ svá hesla? *

Můžeš vybrat více možností.

Zaškrtněte všechny platné možnosti.

- Prostě si je pamatuji
- Mám je zapsaná (v diáři, deníku, na papíře apod.)
- Mám je uložena v paměti počítače/mobilu
- Znají je i moji rodiče (pro jistotu)

Jiné: _____

38. Máš nějak zabezpečené zařízení (počítač, telefon apod.), ze kterého k sociálním sítím přistupuješ? *

Označte jen jednu elipsu.

- Ano, zařízení je chráněno heslem/pinem
- Ne
- Nevím
- Jiné: _____

39. Která rizika jsou podle tebe nejzávažnější? *

Zaškrtni 1, pokud riziko nepovažuješ za závažné, zaškrtni 5, pokud riziko považuješ za velmi vážné.

Označte jen jednu elipsu na každém řádku.

	1	2	3	4	5	Nevím
Personalizovaná reklama, spam	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ztráta a zneužití tvých osobních informací	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ztráta a zneužití hesla	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Nenávistný, děsivý obsah	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Kyberšikana, manipulace a online obtěžování	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Komunikace s neznámými lidmi	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Setkávání s neznámými lidmi ze sociálních sítí	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

40. Napadají tě ještě nějaká další rizika, která jsem v předchozí otázce nezmínila? Napiš je prosím sem:

41. Setkal/a jsi se někdy na internetu nebo sociálních sítích s něčím, co ti bylo nepříjemné nebo tě to nějak ohrožovalo a měl/a jsi strach? Poděliš se prosím i o tuto zkušenost? Jak jsi to řešil/a?

Demografické údaje

Tak už jsi skoro na konci, teď už prosím jenom vyplň pár údajů o sobě, které mi pomohou s vyhodnocováním všech předchozích odpovědí :-)

42. Jsi: *

Označte jen jednu elipsu.

holka

kluk

43. Do jaké třídy chodíš? *

Označte jen jednu elipsu.

do 8.

do 9.

Obsah není vytvořen ani schválen Googlem.

Google Formuláře

Příloha 2 – E-mail rodičům

Vážení a milí rodiče,

do výuky předmětu [xy]²⁷ jsme se pro žáky 8. a 9. tříd rozhodli zakomponovat dotazník zaměřený na ochranu soukromí na sociálních sítích, který vytvořila naše absolventka Helena Filipová v rámci své diplomové práce na Univerzitě Karlově. Dotazník je zcela anonymní (děti neuvádějí ani své jméno ani žádné své kontaktní údaje). Získané výstupy nám poskytnou zajímavé podklady pro diskuzi o otázkách soukromí v další výuce. Otázky jsou zaměřeny zejména na sociální sítě Instagram a Facebook a snaží se děti vést k zamyšlení se nad vlastní bezpečností a ochranou osobních informací na sociálních sítích.

Vyplnění dotazníku není povinné! Pokud souhlasíte s tím, že Váš syn/ Vaše dcera tento dotazník vyplní, nemusíte na tento e-mail nikterak reagovat. V případě, že z nějakého důvodu **nesouhlasíte**, aby se Váš syn/ Vaše dcera vyplňování dotazníku účastnil/a, dejte nám prosím vědět nejpozději do [XX].11.2020 na e-mailové adrese [kontakt na vyučujícího, který bude dotazník rozesílat], dotazník mu/ jí zasílat nebudeme.

S pozdravem

[]

²⁷ červeně a v hranatých závorkách označená místa v textu si vyučující na ZŠ doplnil sám, podle potřeby