Pedagogická fakulta
Faculty of Education
Jihočeská univerzita v Českých Budějovicích
University of South Bohemia in České Budějovice

JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH

Pedagogická fakulta

Katedra informatiky

Kompetence žáků základních škol při používání sociálních sítí

Bakalářská práce

Vypracoval: Radek Havlíček

Vedoucí práce: Mgr. Václav Šimandl, Ph.D.

České Budějovice 2017

Prohlášení

Prohlašuji, že svoji bakalářskou práci jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích dne 1.7.2017

Radek Havlíček

Abstrakt

Tato práce řeší rizika spojená s užíváním sociálních sítí u žáků základních škol z hlediska sdílení soukromých dat. Autor se zaměřuje na ochranu dat před zneužitím, na shromažďování informací a na sdílení osobních informací mladistvých. V práci dále popisuje podmínky užívání sociálních sítí, rizika užívání a porovnává sociální sítě z hlediska shromažďování dat. Cílem práce je zjistit, za pomocí výzkumu, jak mladiství přistupují k sociálním sítím, vytvořit si obraz o tom, jaká data sdílejí, proč je sdílejí a zda nedošlo k jejich zneužití. Autor využívá dotazníkové šetření, zvolenou problematiku vyhodnocuje použitím statistické metody Chí-kvadrát test. Zpracovaná data porovnává dle různých faktorů, ověřuje a analyzuje rozdíly mezi danými skupinami.

Klíčová slova

Sociální síť, dotazník, osobní data, ochrana soukromí, zneužití dat

Abstract

This bachelor thesis deals with the risk of connecting and using social network from the point of view of sharing private data by primary school students. The author focuses on data protection againts misuse, accumulation of information and sharing personal information of youthful. In this bachelor thesis he desribes requirements of using social networks, risks of using and comparing social networks with respect to data accumulation. The main aim is to figure out, with using a research, how youthful approach to social networks, find out what kinds of data they share, why they share them and whether data are not misused. The author uses a questionnaire survey and analyses chosen issues with using statistical method chi-square statistic. He also compares processed data to the variety of factors verify and analyses differences between separate groups.

Keywords

Social network, security questionnaire, personal data, privacy protection, data abuse

JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH
Fakulta pedagogická
Akademický rok: **2015/2016**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Radek HAVLÍČEK**
Osobní číslo:	**P14216**
Studijní program:	**B7507 Specializace v pedagogice**
Studijní obor:	**Informační technologie a e-learning**
Název tématu:	**Kompetence žáků základních škol při používání sociálních sítí**
Zadávající katedra:	**Katedra informatiky**

Zásady pro vypracování:

Cílem práce je z bezpečnostního hlediska zmapovat užívání sociálních sítí žáky základních škol a vytvořit obraz o jejich pohledu na tuto problematiku. Student sestaví dotazník, který bude zacílen na sdílení soukromých dat (osobní fotografie, videozáznamy, životní postoje ...) a osobních informací. Zaměří se také na uvědomování si možných rizik užívání sociální sítí respondenty, zda těmto rizikům již čelili a zda znají podmínky shromažďování informací jimi používanými sociálními sítěmi. Dotazníková data student vyhodnotí použitím statistických metod a použitím metody skórů lži ověří důvěryhodnost dat. Výsledky z dotazníků student porovná podle různých faktorů (věk, pohlaví, velikost školy, velikost obce) a zanalyzuje, zda se mezi danými skupinami objevují určité rozdíly. Práce bude obsahovat teoretickou část zaměřenou na rizika používání sociálních sítí, podmínky užívání, porovnání známých sociálních sítí ve shromažďování dat a známé případy jejich zneužití.

Rozsah grafických prací: **CD ROM**

Rozsah pracovní zprávy: **40**

Forma zpracování bakalářské práce: **tištěná**

Seznam odborné literatury:

1. **GAVORA, P. Úvod do pedagogického výzkumu. Brno: Paido, 2010. ISBN 978-80-7315-185-0.**
2. **CHRÁSTKA, M. Metody pedagogického výzkumu. Praha: Grada, 2007. ISBN 978-80-247-1369-4.**
3. **KULHÁNKOVÁ, H. a J. ČAMEK, 2010. Fenomén facebook. 1. vyd. Kladno: BigOak. ISBN 978-80-904764-0-0.**
4. **KIRKPATRICK, D., 2011. Pod vlivem Facebooku: příběh z nitra společnosti, která spojuje svět. Vyd. 1. Brno: Computer Press. ISBN 978-80-251-3573-0.**
5. **NEUBAUER, J., M. SEDLAČÍK a O. KŘÍŽ, 2012. Základy statistiky: aplikace v technických a ekonomických oborech. 1. vyd. Praha: Grada, 236 s. ISBN 978-80-247-4273-1.**
6. **OFCOM, 2015. Ofcom report on internet safety measures: Strategies of parental protection for children online [online]. [cit. 2016-03-15]. Dostupné z: http://stakeholders.ofcom.org.uk/binaries/internet/fourth_internet_safety_report.p**
7. **OFCOM, 2011. Children and parents: Media use and attitudes report [online]. [cit. 2012 04-15]. Dostupné z: http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/oct2011/Children_and_parents.pdf**

Vedoucí bakalářské práce: **Mgr. Václav Šimandl**
Katedra informatiky

Datum zadání bakalářské práce: **20. dubna 2016**

Termín odevzdání bakalářské práce: **28. dubna 2017**

Mgr. Michal Vančura, Ph.D.
děkan

L.S.

doc. PaedDr. Jiří Vaníček, Ph.D.
vedoucí katedry

V Českých Budějovicích dne 20. dubna 2016

Poděkování

Děkuji vedoucímu práce Mgr. Václavu Šimandlovi, Ph.D. za jeho pomoc, rady a připomínky při zpracování mé bakalářské práce. Rád bych poděkoval také mé rodině a blízkým za podporu při mém studiu.

Obsah

1 Úvod **10**

2 Cíle práce **11**

3 Metoda práce **12**

4 Sociální sítě **13**

4.1 Definice sociální sítě ... 13
4.2 Vývoj sociálních sítí ... 14
4.3 Typy sociálních sítí ... 15
4.3.1 Klasifikace podle záměru ... 16
4.3.2 Klasifikace podle funkcí ... 16
4.3.3 Klasifikace podle otevřenosti ... 17
4.3.4 Klasifikace podle úrovně spojení ... 17
4.3.5 Další klasifikace sociálních sítí ... 18
4.4 Nejpopulárnější moderní sociální sítě ... 18
4.4.1 Facebook ... 19
4.4.2 YouTube ... 19
4.4.3 Instagram ... 20
4.4.4 Linkedin ... 20
4.5 Rizika spojená s užíváním sociálních sítí ... 20
4.5.1 Kyberšikana ... 21
4.5.2 Kybergrooming ... 22
4.5.3 Kyberstalking ... 23
4.5.4 Další hrozby ... 23
4.5.5 Případy zneužití dat a informací ... 24
4.6 Bezpečnost na sociálních sítí ... 25
4.6.1 Pravidla pro bezpečné užívání sociálních sítí ... 26
4.7 Výhody sociálních sítí ... 26
4.8 Nevýhody sociálních sítí ... 27
4.9 Ochrana soukromí na sociálních sítí ... 27
4.10 Právní rámec ochrany soukromí ... 28
4.11 Podmínky používání ... 29
4.12 Zásady používání dat ... 30
4.13 Prohlášení o právech a povinnostech ... 33

4.14 Možnosti nastavení zabezpečení a soukromí účtu 35

5 Výzkumný záměr 38

5.1 Hlavní výzkumný problém a definice hypotéz 38

5.2 Cílová skupina respondentů 41

5.3 Návrh dotazníku 41

5.3.1 Ověření konzistentnosti odpovědí 42

5.4 Sběr dat 44

5.5 Statistická metoda Chí–kvadrát test - test nezávislosti 45

6 Výsledky výzkumu 46

6.1 Relační výsledky 46

6.1.1 Vliv věku na chování 46

6.1.2 Vliv pohlaví na chování 48

6.1.3 Vliv místa bydliště a počtu obyvatel na chování 51

6.1.4 Vliv nastavení soukromí na chování 52

6.1.5 Vliv znalostí a zkušeností na chování 53

6.2 Deskriptivní výsledky 54

6.2.1 Chování v oblasti sdílení dat 56

6.2.2 Chování v oblasti soukromí 58

6.2.3 Chování v oblasti vnímání informací 61

6.2.4 Chování v oblasti výběru kontaktů 62

6.2.5 Chování v oblasti znalosti zásad používání dat 63

6.2.6 Chování v oblasti znalostí rizik a zkušenosti se zneužitím dat 64

7 Shrnutí výsledků a diskuze 66

8 Závěr 68

Seznam obrázků 75

1 Úvod

V posledních několika letech se internet dostal do téměř každé domácnosti, a to po celém světě. Podle Českého statistického úřadu [1] internet v České republice využívá přibližně 73 % domácností, z toho 75 % uživatelů používá internet každý den. Nejčastěji jim slouží jako prostředek ke komunikaci, a to především prostřednictvím sociálních sítí.

Sociální sítě nám umožňují komunikovat, navazovat kontakty s novými lidmi, sdílet informace nebo se zapojovat do veřejných diskuzí. Lidé zde sdílí své zážitky, fotografie, videa nebo jen chatují. Podle nového průzkumu od Mediaguru [2] pouze 7,6 % uživatelů internetu v České republice nevyužívá sociální sítě, drtivá většina uživatelů internetu je aktivní alespoň na jedné sociální síti. Tři a více sociálních sítí využívá 69 % českých uživatelů, což je o 30 % více oproti minulému roku 2016.

V dnešní době jsou sociální sítě dostupné víceméně všem uživatelům internetu, a to bez ohledu na věk. Sociální sítě jsou populární především u „teenagerů“, avšak využívají je i dospělí. Převážná část sociálních sítí nepožaduje žádné ověření totožnosti, a tudíž registraci může provést kdokoliv, a to i věkově mladší jedinci. To potvrzuje i výzkumná zpráva Kopeckého [3], kde bylo zjištěno, že 59,3 % dětí mladších 13 let, kteří využívají internet, používá Facebook, a to i přes to, že tím porušují daná pravidla používání sociální sítě. S rostoucí tendencí dostupnosti a popularity sociálních sítí však rostou i rizika spojená s užíváním tohoto významného online nástroje. Zneužití dat a osobních informací, obtěžování, kyberšikana, stalking – to jsou pojmy, se kterými se každý uživatel sociálních sítí může setkat.

Ochrana soukromí na sociálních sítí je diskutovaným tématem. Znalost podmínek užívání, důvěryhodnosti identity uživatele, nastavení soukromí a zabezpečení účtů a znalost rizik spojených se sdílením dat se mnohdy vyplatí znát. Děti si často neuvědomují hrozby, které sdílení osobních dat přináší, přitom zneužití citlivých dat může mít špatné následky. Virtuální prostředí a online komunikace dává prostor útočníkům k narušení soukromí, a proto je třeba vyvarovat se nebezpečnému chování na sociálních sítí a mít základní znalosti v oblasti ochrany soukromí.

2 Cíle práce

Cílem práce je z bezpečnostního hlediska zmapovat užívání sociálních sítí žáky základních škol. Práce poskytne čtenáři detailní informace o problematice ochrany soukromí na sociálních sítí, sdílení informací, shromažďování dat a podmínkách užívání. Cílem je odhalit sdílení osobních dat (osobní fotografie, videozáznamy, životní postoje ...) a osobních informacích na sociálních sítí a zjistit, jak respondenti samotní hledí na tuto problematiku, zda si uvědomují možná rizika při používání sociálních sítí, jaká data sdílejí a v jaké míře. Dále zda se někdy setkali s prohlášením o zásadách používání dat a zda vědí, jakým způsobem sociální sítě shromažďují data a jak je využívají.

Cílem je také zmapovat jaké sociální sítě mladiství nejvíce využívají a ty v teoretické části porovnat z hlediska shromažďování dat a možnosti nastavení soukromí.

Práce by měla čtenáři rozšířit znalosti v této problematice. Hlavním přínosem práce budou samotné výsledky výzkumu, které budou podrobně popsány a pomocí nichž si čtenář udělá obraz o tom, jak respondenti ve věkovém rozmezí 12-15 let vnímají sociální sítě.

3 Metoda práce

Práci jsem si rozdělil na teoretickou a praktickou část. Jako první jsem si vyhledal a nastudoval potřebnou literaturu k tématu, kterou jsem využil v teoretické části. Problematiku ochrany soukromí jsem se snažil podpořit podobnými výzkumy, které byly vytvořeny. Studoval jsem také literaturu z oblasti metodologie výzkumu, tvorby dotazníků a statistického zpracování. Primárním zdrojem informací byly pro mě webové stránky a elektronické články.

V praktické části byl vytvořen vlastní výzkum zaměřený na ochranu soukromí na sociálních sítí. Nejdříve jsem si stanovil, na jakou cílovou skupinu se zaměřím a poté jsem si stanovil výzkumné otázky a hypotézy, které budu zpracovávat. Následně byl sestaven dotazník, který byl přizpůsoben věku respondentů. Před distribucí dotazníků do jednotlivých škol jsem provedl testování dotazníků s dětmi stejné věkové skupiny jako je moje cílová. V této fázi docházelo především k úpravám formulace otázek. Po zhotovení dotazníku jsem kontaktoval jednotlivé školy, v kontaktu jsem byl převážně s výchovnými poradci, kteří mi zajistili distribuci dotazníku. Dotazník byl dostupný jak elektronicky, tak v papírové podobě, a to kvůli tomu, že každá škola preferovala jiný způsob. Elektronickou verzi jsem realizoval za pomocí Google formuláře a papírová podoba byla realizována v MS Word 2016. Vyplněné dotazníky jsem následně přepisoval do MS Excel 2016 a zde jsem je také statisticky zpracovával a ověřoval důvěryhodnost odpovědí. Ke zpracování dat jsem využil statistickou metodu Chí-kvadrát test a data byla také graficky zpracována.

Výsledky výzkumu byly předány výchovným poradcům škol, které mě poprosily o zpětnou vazbu. Výsledkem je zmapování užívání sociálních sítí žáky základních škol.

4 Sociální sítě

V rámci této kapitoly je podkapitola 4.1 zaměřena na obecnou definici sociálních sítí, kapitola 4.2 stručně popisuje historii sociálních sítí. V podkapitole 4.3 je čtenář seznámen s typy a druhy sociálních sítí, se kterými se uživatelé internetu mohou setkat. V podkapitolách 4.4, 4.5 a 4.6 jsou vymezeny nejpoužívanější sociální sítě dnešní doby, možná rizika spojená s jejich užíváním a pojmy vztahující se k bezpečnosti na sociálních sítí. V podkapitolách 4.7 a 4.8 jsou porovnány výhody a nevýhody sociálních sítí. Zbylé podkapitoly této kapitoly jsou zaměřeny na ochranu soukromí na sociálních sítí, používané sociální sítě jsou porovnány z hlediska podmínek užívání a shromažďování dat. Prezentovány jsou také možnosti nastavení zabezpečení účtů a jaké možnosti mají uživatelé sociálních sítí při nastavení soukromí.

4.1 Definice sociální sítě

Sociální sítě jsou součástí každodenního života mnoha lidí po celém světě. Tomu nasvědčují i statistiky dostupných průzkumů zaměřených na nejvíce navštěvované stránky [4], kde přední příčky obsazují právě sociální sítě jako Facebook, YouTube, Twitter apod.

Můžeme je jednoduše definovat jako místo zábavy, prostředí k setkávání lidí, sdílení obsahu a zážitků. Lidé zde očekávají vzájemnou interakci s ostatními. Zajímavostí je poznatek, že sociální sítě (ať už reálné, nebo virtuální) jsou jedním z projevů lidství, protože člověk jako jedinec má potřebu se sdružovat, někam patřit a vyžaduje sociální podporu a bezpečí, a právě to sociální sítě nabízejí.

„Život člověka je vždy zajímavý, a tudíž se pokaždé najde někdo, koho zajímáme nebo kdo zajímá nás. Uživatelé sociálních sítí si mohou být zároveň zdrojem inspirace a zdrojem síly v těžkých životních situacích, protože vidíme, jak ostatní známí a přátelé překonali své temné časy [5].“

4.2 Vývoj sociálních sítí

Pojem sociální sítě byl zaveden dlouho před tím, než vznikl internet, a to londýnským sociologem Jamesonem Barnsonem v letech 1954 [6]. Ve druhé polovině 20. století se pak sociální sítě postupně začaly vyvíjet, a to jako vědecká koncepce. Historicky první sociální sítě tvořily skupiny lidí, kteří využívaly klasické maily, pro podporu sociálních vztahů. První odeslaný vzkaz na vzdálený počítač se uskutečnil 2. 10. 1971 a byl to první krok ke stvoření internetu a současných sociálních sítí. Dalším významným objevem bylo vytvoření komunikace IRC[1], které hrálo velkou roli při vývoji sociálních sítí. Za první uživatele sociálních sítí se považují „vojáci“ v síti ARPANET[2] [6].

Mnoho odborníků označuje za počátek vývoje sociálních sítí spíše systém BBS, který byl spuštěn v roce 1978. Jednalo se o elektronickou nástěnku, v „dosovské grafice“, kde si uživatelé mohli navzájem vyměňovat různé informace (textového druhu, nikoliv grafického). V té době však nebyly na světě modernější technologie pro komunikaci v reálném čase, a tudíž pouze jeden uživatel v jednu chvíli mohl být přihlášen do systému. Klasická konverzace o několika větách pak někdy trvala až 24 hodin a více a šlo o opravdu velmi pomalý proces [7].

Pokud bychom se zaměřili na moderní sociální sítě postavených na konceptu Web 2.0 – weby, kde registrovaní uživatelé vytváří a sdílí svůj obsah v reálném čase, tak bychom zjistili, že vůbec první takováto síť vznikla až v letech 1997 a nosila název sixDegrees.com [7].

Ta byla založena na myšlence šesti stupňů odloučení (anglicky six degrees of separation). Tato teorie předpokládá, že každý člověk je spojený s každým člověkem prostřednictvím řetězce šesti sobě navzájem známých lidí [8]. Síť přetrvala pouze 3 roky, poté byla služba ukončena (v dnešní době doména stále existuje, ale registrace je možná pouze na základě pozvánky). Podle svého zakladatele tento projekt „předběhl svou dobu“ a proto nebyl úspěšný. Je známo, že počet uživatelů internetu na konci devadesátých let byl nízký, a proto se můžeme domnívat, že tato síť zanikla [9]. Podle dostupných informací na vrcholu své slávy se cena této sociální sítě odhadovala na 125 milionů dolarů a měla milion registrovaných uživatelů [10].

[1] Internet Relay Chat - (česky chat přes internet) je systém pro komunikaci v reálném čase
[2] ARPANET - počítačová síť (spuštěná v roce 1969), kterou označujeme jako zárodek sítě Internet

Mezi podobné milníky historie můžeme zařadit také síť Friendster, která byla založena v roce 2002, kde hlavní myšlenkou bylo seznamovat „přátelé přátel“ s tím, že budou lépe navazovat kontakt než s úplně cizími lidmi. V roce 2003 společnost Google byla ochotna zaplatit 30 milionů dolarů za tuto úspěšnou síť, ale tvůrci odmítli. V dnešní době se již nejedná o seznamovací server, protože v roce 2009 upadající Friendster odkoupila firma MOL Global za 26, 5 miliónu dolarů. Web se poté zaměřoval na „online gaming“ [9] a od 14. 7. 2015 ukončil provoz.

V dnešní době běžní uživatelé sociálních sítí pravděpodobně tyto sociální sítě neznají, ale je třeba říci, že sociální sít sixDegrees byla předchůdcem a zárodkem již dnes světově známých sítí jako MySpace, Linkedin nebo Facebook.

4.3 Typy sociálních sítí

Řekněme, že nám sociální sítě nabízejí služby v prostředí sítě internet. Ty můžeme rozdělit do několika kategorií podle toho, jak jsou sítě strukturované a co uživatelům nabízejí. Ačkoliv typů sítí je hodně, troufnu si říci, že je všechny spojují stejné cíle, a to vybudovat lidské vztahy a poskytnout lidem určitý druh zábavy.

V podstatě sociální sítě lze rozdělit na dvě skupiny – nepřímé a přímé: [11]

Nepřímé sociální sítě. Zapůjčené služby v prostředí internetu, kde uživatel nemá svůj profil, ale hraje zde roli nějaká skupina, která kontroluje kroky uživatele a řídí např. témata v prostředí nějaké konkrétní oblasti. Do této skupiny patří blogy a fóra.

- Blog – služba, kterou obvykle spravuje pouze jeden nebo více autorů. Existuje zde chronologický zápis informací a obvykle bývají stránky aktualizovány svými autory. Je to jednoduchý způsob, jak se člověk může prezentovat. Podle zahraničních průzkumů více než polovina blogů byla vytvořena především mladými dívky, které blogy pojali jako jednoduchý a atraktivní deník [12]. Svojí největší slávu již mají za sebou.
- Fórum – služba, která v základě slouží expertům z různých specifických oblastí. Lze je považovat za informativní nástroj, který umožňuje výměnu a sdílení informací, názorů a poznatků. Umožňuje obousměrnou komunikaci v rámci fór (např. odpověď na předem položenou otázku).

Přímé sociální sítě. Zapůjčené služby v prostředí internetu, ve kterých je určitá spolupráce mezi skupinami lidí, které sdílí stejné zájmy. V tomto typu sociální sítě si uživatelé vytváří své uživatelské profily, které spravují a vytváří si vztahy s ostatními

uživateli. Do jaké míry ponechají přístup k osobním informacím na svém profilu je podmíněné nastavením soukromí, které uživatelé mohou spravovat.

Přímé sociální sítě pak můžeme klasifikovat dále podle formy zaměření, které jsem shrnul v následujících podkapitolách. Mezi přímé sociální sítě patří například Facebook, YouTube, MySpace, Linkedin, Xing aj.

4.3.1 Klasifikace podle záměru

Tento typ sítí se zaměřuje na konkrétní cíl. Tyto cíle by pak měly uživatele přesvědčit, aby do budoucna sociální síť i nadále využíval. Dále je můžeme rozdělit do dvou skupin: [11]

- Sociální sítě za účelem zábavy – Uživatelé zde hledají pouze formu nějaké zábavy. Dochází zde ke spojování s dalšími uživateli a navazování vztahů prostřednictvím výměny informací (komentáře, chat). Cílem je zlepšení vztahů mezi členy.
- Sociální sítě za profesionálním účelem – Primárním cílem uživatele je propagovat se na profesionální úrovni, kde se může zaměřit na rozšíření svých kontaktů v jeho pracovním (profesním) zaměřením.

4.3.2 Klasifikace podle funkcí

V tomto případě se jedná o procesy, které sociální sítě vytvářejí a orientují podle své formy prostřednictvím aktivit. Můžeme je rozdělit do třech kategorií [12].

- Obsahové sociální sítě – Jak plyne z názvu, uživatelé zde vytváří obsah, který může být buď psaný, nebo audiovizuální. Vytvořený obsah pak uživatelé sdílí s ostatními uživateli prostřednictvím sociální sítě. Zajímavostí je zde fakt, že obsah může vytvořit i neregistrovaný uživatel a může ho sdílet ostatním. Sdílený obsah obvykle prochází kontrolou, zda je neškodný, nebo není nevhodný, a až po schválení je možná jeho publikace.
- Sociální sítě založené na uživatelských a profesionálních profilech – Tento typ sítí je obecně velmi známý. Zde si uživatel musí vytvořit svůj profil (ať už se jedná o osobní, nebo profesionální) a až poté může využívat všechny funkce sociální sítě. Obvykle je účet doprovázen tzv. „profilovou fotkou“.

- Sociální sítě typu mikro blogy – Typ sítí, které umožňují uživateli publikovat krátké zprávy (většinou znakově omezeny) [13]. Zde obvykle uživatelé sdílí menší balíčky informací.

4.3.3 Klasifikace podle otevřenosti

U tohoto typu sítí se klade důraz především na možnost přístupu do sítí z hlediska uživatele. Mohou zde být definovány pravidla kdo může do sítě přistoupit [11]. Jsou dvě kategorie.

- Sociální sítě veřejné – Tyto sítě jsou tzv. otevřené, přístup do nich má jakýkoliv uživatel a neexistují zde žádná omezení přístupu. Uživatel se může do sítě přihlásit z jakéhokoliv přístroje a nemusí být žádným členem (uzavřené) skupiny nebo specifické organizace.
- Sociální sítě soukromé – Tento typ sítí není přístupným všem uživatelům a bývají zde definovaná pravidla a různá omezení přístupu. Uživatelem se obvykle může stát jen konkrétní člen nějaké skupiny nebo organizace, která sama financuje a spravuje svou síť. Uživatelé obvykle mají smluvní vztah s danou skupinou nebo organizací.

4.3.4 Klasifikace podle úrovně spojení

Jedná se o síť, která spojuje úroveň vzájemné souvislosti nebo zapojení do aktivit dle vlastní preference a profesionality [11]. Můžeme je rozdělit do dvou kategorií.

- Sociální sítě s vertikální integrací – Registrace do této sítě je většinou dostupná pouze přes pozvánku od jednoho z aktivních členů. Sdílený obsah zde bývá kontrolován a musí se schválit. Práce je zde vymezena v rámci využití určité skupiny uživatelů, které spojují aspekty jako profesní zaměření, vzdělání a zájmy. Můžeme se zde setkat i s placenými verzemi, kde uživatel sociální sítě hradí minimální poplatky na provoz.
- Sociální sítě s horizontální integrací – Tento druh sítě má stejné vlastnosti jako předchozí typ. Rozdíl je zde pouze ve vymezení práce, která většinou nebývá vymezena do určitých skupin dle jejich zájmů – tyto aspekty zde nehrají roli.

4.3.5 Další klasifikace sociálních sítí

Zmíním se o dalších klasifikacích sociálních sítí. Za zmínku určitě stojí např. dělení sociálních sítí na řízené a neřízené. Pod řízenými si můžeme představit „followery“ na Twitteru, „fan page“ na Facebooku nebo reakce na fórech. Neřízené vytvářejí obousměrnou komunikaci a vztahy mezi uživateli. Zde si můžeme představit klasické spojení přátelství dvou uživatelů na Facebooku, účastníky událostí nebo spoluautory různých blogových článků.

Tyto sítě můžeme dále dělit na explicitní a implicitní, přičemž explicitní deklarují vztahy (již zmíněné přátelství na Facebooku) a pod implicitními si můžeme představit například nákupy na E-bay [11].

4.4 Nejpopulárnější moderní sociální sítě

Každým rokem se popularita sociálních sítí mění. Méně známé sítě upadají, některým se zase dostává větší popularity. Sociální sítě se vyvíjejí, nabízejí lidem bohatější služby než v dřívějších letech. V této podkapitole shrnu nejznámější a nejnavštěvovanější sociální sítě celosvětové, ale zaměřím se také na nejvíce využívané sociální sítě v České republice.

Nové průzkumy ukázaly [14], že celosvětově nejpopulárnější sociální sítí dnešní doby je bezesporu Facebook, který odstartoval svou činnost v roce 2004. Na druhé místo se řadí Twitter, který v České republice není tolik populární, ale celosvětově je velmi využívaný. Třetí nejpopulárnější celosvětovou sítí je pak Linkedin, který je zaměřený jako profesní síť. Mezi dalšími deseti nejpopulárnějšími celosvětovými sociálními sítěmi jsou YouTube, Google+, Instagram, Pinteres, Snapchat, Reddit a Tumblr.

Pokud bychom porovnali novější průzkumy s průzkumy z dřívějších let [15], tak v minulých letech byly v popředí například sociální sítě jako DevianArt, LiveJournal nebo Tagged, které v dnešní době lehce ztratily na popularitě a domnívám se, že většina „teenagerů“ v České republice tyto sítě ani nezná. Bebo a Myspace byly také v minulých letech populárnější, než je tomu teď. Například sociální síť MySpace pak v letech 2004-2008 byla dokonce označena jako nejpopulárnější síť s největším počtem aktivních uživatelů, a ještě v roce 2012 podle průzkumu [16] byla v první pětici nejoblíbenějších. Postupem času však poměr aktivních uživatelů klesal a s tím klesala i popularita. V dnešní době ji využívají především uživatelé z Ameriky.

V České republice podle aktuálních průzkumů, zprostředkovaných společností Alexa [17], je nejnavštěvovanější sociální sítí YouTube společně s Facebookem. Můžeme se domnívat, že vysoká návštěvnost portálu YouTube je dána především kvůli rostoucí popularitě tzv. „Youtuberů“[3]. Mezi další populární sociální sítě v ČR patří například Instagram, překvapivě ruská sociální síť Vk nebo Linkedin. Twitter, jak jsem zmiňoval, není v ČR příliš populární jako ve světě, avšak své uživatele si také najde. České sociální sítě jako Libimseti, Spoluzaci, Xchat nebo Lide, začaly své uživatele ztrácet kolem roku 2009, kdy šel do popředí již zmiňovaný Facebook kam se čeští uživatelé sociálních sítí nejčastěji přesouvali [18]. Vzestup už tyto české sítě nepotkal. Na vrcholu byly v letech 2005-2008.

4.4.1 Facebook

Sociální síť sloužící ke komunikaci mezi uživateli, sdílení informací, fotografií a zážitků. Uživatelé zde mohou navazovat nová přátelství a mohou být jednoduše v kontaktu s lidmi po celém světě. Na Facebooku si uživatelé mohou psát statusy, účastnit se diskuzí ve skupinách a „živě“ komunikovat. Uživatelé zde mohou vést také videohovory, hrát hry a vytvářet si své stránky, ať už za zábavným nebo profesním účelem.

Facebook byl založen roku 2004 mladým studentem Harvardovy univerzity Markem Zuckerbergem. Původně byl systém pouze pro studenty Harvardovy univerzity, později byly připojeny další univerzity a pak celý svět [19].

Aktuálně má denně 1,28 miliardy aktivních uživatelů. Hlavní sídlo společnosti se nachází v Kalifornii. K roku 2017 počet zaměstnanců na plný úvazek se vyšplhal na 18770 [20].

4.4.2 YouTube

Největší internetový portál sloužící ke sdílení multimédií. Uživatelé zde mohou sdílet svá videa (zábavná, naučná, …), komentovat a sledovat videozáznamy jiných uživatelů. Objevují se zde také nové videoklipy slavných interpretů. Oblíbené tvůrce videozáznamů pak mohou ostatní uživatelé „odebírat“ a nahraná videa komentovat. V dnešní době YouTube velmi ráda využívá řada lidí jako nástroj pro vydělání si peněz prostřednictvím reklam, odběrů a různých spoluprací.

[3] YouTuber – osoba, která na portálu YouTube dlouhodobě nahrává svá videa s vlastním obsahem a sleduje ostatní videa.

YouTube je dostupný v 77 jazycích a není zde vyžadována registrace. Služba byla spuštěna v roce 2005, autoři byly zaměstnanci známého PayPalu. Nakonec byl YouTube odkoupen společností Google za 1,65 miliard dolarů [21].

4.4.3 Instagram

Instagram je sociální síť sloužící primárně pro sdílení fotografií. Uživatelé zde sdílí své zážitky a životní momenty. Na Instagramu si tak uživatelé tvoří alba fotografií, které mohou ostatní uživatelé vidět. Dostupnost fotografií je pak dána nastavením soukromí. Existují zde tzv. „foloweři“, kteří přihlášením odběru dávají najevo zájem o pozorování uživatelských profilů. Je zde možnost také komentovat fotografie či dávat obdiv k fotografiím. Přístup k síti zajišťuje mobilní aplikace dostupná na všech platformách a je zde možnost přímo upravovat nahrané fotografie pomocí dostupných filtrů.

Instagram je dostupný ve 33 jazycích a byl spuštěn v roce 2010 [22]. Aktuálně k roku 2017 je na této síti aktivních 700 milionů uživatelů [23].

4.4.4 Linkedin

Sociální síť, která propojuje profesionály po celém světě za účelem zvýšení produktivity a efektivity. Registrací uživatel dostane přístup k pracovním příležitostem, nebo třeba k novinkám a novým kontaktům ve své profesi [24].

V profilu uživatele se nachází životopis, kde se snadno zjistí položky jako hledaná pracovní místa, dosažené vzdělání, preference aj. Základní profil a funkce jsou registrovaným uživatelům dostupné zdarma, doplňkové funkce jsou za poplatky [25].

Linkedin byl poprvé spuštěn v roce 2003, aktuálně má 300 milionů uživatelů z 200 zemí a specializuje se ve 170 různých profesních odvětví. V roce 2016 byla sociální síť odkoupena společností Microsoft za 26,2 miliard dolarů [26].

4.5 Rizika spojená s užíváním sociálních sítí

Jak bylo řečeno, sociální sítě umožňují navazovat přátelství mezi lidmi z celého světa. Už při registraci (pokud je vyžadována) uživatel většinou zadává své jméno, příjmení, národnost a datum narození. U téměř všech sociálních sítí jsou pak zveřejněné informace dostupné ostatním uživatelům sociální sítě a podle nastavení soukromí je určeno

jaké informace, popřípadě kdo tyto informace bude vidět. Buď to může být pouze skupina lidí, kteří se označují většinou jako „přátelé nebo „followeři“, nebo jiné podskupiny uživatelů, nebo jakýkoliv uživatel sociální sítě a popřípadě také internetu. Nikdy v předchozích letech nebylo jednodušší si zjistit informace o lidech, které vlastně ani neznáme než dnes, a proto je nezbytné přemýšlet o tom, jak velké riziko zveřejnění sdílené informace nese a zamyslet se nad tím, komu chceme poskytnout informace. Informace, které pak mohou uživatelé, ale i nežádoucí lidé zjistit, jsou například bydliště, zájmy, koníčky, aktuální navštěvovaná škola, popřípadě zaměstnání, nebo třeba oblíbená navštěvovaná místa.

Mezi nejzranitelnější skupinou uživatelů sociálních sítí jsou bezesporu děti, kteří často mívají nižší smysl pro zodpovědnost, neuvědomují si tolik možné následky a méně často řeší soukromí svých profilů. Informace, které o sobě sdílí, je pak mohou také znevýhodnit či poškodit v budoucnu při hledání práce, protože v dnešní době je už běžné, že personalisté jednotlivých firem před nástupem prověřují uchazeče na internetu, a to zejména na sociálních sítí, které jsou bohatým zdrojem informací [27].

Sdílení informací pak může vést ke spoustě rizik. Rizikem může být například i neškodný příspěvek o odjezdu na dovolenou, který může přilákat potenciální zloděje. Zveřejněné údaje, především osobního charakteru, pak mohou vést také k vydírání a manipulování s obětí. S tím souvisí i možnost zakládat si účty na sociálních sítí pod jakoukoliv jinou osobností a tím si pak útočník může zajistit důvěru u oběti a následně ji někam vylákat. Při zveřejňování osobních fotografií pak může docházet k obtěžování, popřípadě zneužití fotografií [28].

Rizika spojená s užíváním sociálních sítí by měl znát každý uživatel a pokud se jedná o dítě, tak by zde měli především rodiče poskytnout základní informace o této problematice, popřípadě škola. Zavedení kurzů do základních škol o problematice bezpečnosti na sociálních sítí by bylo efektivním řešením a prevencí před hrozbami, které sociální sítě v sobě skrývají. V dalších podkapitolách shrnu hrozby a rizika, se kterými se nejčastěji můžeme setkat ve virtuálním prostředí.

4.5.1 Kyberšikana

Kyberšikanu lze definovat jako formu šikany, která probíhá prostřednictvím elektronických médií, jako jsou mobilní telefony, tablety a počítače, připojených do sítě internet, které slouží k agresivnímu a záměrnému poškození uživatele těchto médií [29].

Kyberšikana má s klasickou šikanou jednu společnou věc, a to cíl někoho poškodit nebo mu ublížit, jak psychicky, tak i fyzicky. Oběti kyberšikany neustále přibývají a potvrzují to i nejrůznější výzkumy. Nejčastějšími znaky kyberšikany jsou: [30]

- Anonymita útočníků
- Mění se profil útočníků a profil obětí
- Mění se místo a čas útoků
- Při kyberšikaně pomáhá útočníkovi publikum
- Dopady kyberšikany na oběť není lehké rozpoznat

Nejčastějšími projevy kyberšikany pak může být: [31]

- Zasílání urážlivých a zastrašujících zpráv
- Pořizování zvukových záznamů, videozáznamů či fotografií a jejich následné zveřejňovaní
- Vytváření internetových stránek za účelem zesměšnění oběti
- Vydírání pomocí mobilního telefonu nebo internetu
- Provokování uživatelů například ve veřejných diskuzí

Projevy kyberšikany se nejčastěji dějí za pomocí elektronických zařízení jako jsou počítače, tablety, mobilní telefony nebo herní konzole. Aplikace nebo služby, přes které komunikace probíhá jsou například e-mail, sociální sítě, MMS zprávy, telefonní hovory nebo diskuze na fórech.

4.5.2 Kybergrooming

Kybergrooming je jednání osoby, která se snaží vyhledat si oběť prostřednictvím internetu, získat si její důvěru, vybudovat si s ní vztah a následně ji donutit k osobní schůzce. Motivem bývá nejčastěji sexuální zneužití. Nejčastěji komunikace probíhá za pomocí online chatování, telefonování, nebo posílání zpráv na mobil.

Obvykle celý proces probíhá tak, že se útočník snaží vybudovat si důvěru u oběti a snaží se jí izolovat od okolního světa (přátel, rodiny, …). Následně oběť podplácí dárky nebo penězi a buduje si vztah. Pak získá nebezpečné materiály oběti (např. donutí oběť, aby poslala nahou fotografii) a začne fáze vydírání. Poté dojde k osobní schůzce, kde dochází ke zneužití, napadení a vydírání. Obvykle se násilník přetvařuje a vydává se za mladšího jedince. Komunikace pak může probíhat i několik měsíců, obvykle jsou násilníci velmi trpěliví [32].

4.5.3 Kyberstalking

Kyberstalking je pronásledování oběti, které může mít řadu různých forem a různou intenzitu. Nejčastěji jde o opakované obtěžování za pomocí elektronických prostředků, kde útočník převážně „bombarduje“ svou oběť SMS zprávami, telefonáty, emaily nebo i dárky. Základní projevy kyberstalkingu, jak jsem zmiňoval, jsou dlouhodobé a opakované nevyžádané pokusy kontaktovat oběť. Často se stalker označuje sám za oběť, aby vzbudil pocit viny. Mezi další znaky patří také záměrná destrukce majetku oběti, jako například poškrábané auto, rozbitá okna bytu nebo posílání virů s cílem získat osobní data oběti) [33]. Stalkerem pak může být osoba, která: [34]

- oběť osobně zná a ví, že ji pronásleduje
- osoba, kterou oběť osobně zná, ale neví, že ji pronásleduje
- osoba, kterou oběť osobně nezná

Existuje řada internetových stránek a telefonních čísel, kde se oběti mohou svěřit s problémy a popřípadě nahlásit, že se staly obětí pronásledování. Nahlášení je možné také u policie ČR nebo na lince bezpečí.

4.5.4 Další hrozby

Mezi další nebezpečné hrozby, se kterými se můžeme setkat na sociálních sítí jsou například sexting, flaming, hoax nebo phishing.

Sexting je elektronické zasílání zpráv se sexuálním obsahem, a to prostřednictvím telefonu (textových a multimediálních zpráv) nebo sociálních sítí. To je populární především u mladistvých a jejich začínajících vztahů. Často se pak intimní fotografie, především po ukončení vztahu, zveřejňují na internetu a tím dochází k jejich zneužití.

Flaming je opakované urážení a útočení na oběť. Objevují se zde vulgární slova a nadávky. Cílem je obhájit si svůj názor. Často se s flamingem můžeme setkat na fórech nebo v různých diskuzí, kde se vedou delší debaty, nebo na sociálních sítí a také v online hrách. Snadno se flaming může dostat z virtuálního prostředí do reality, kde pak bývá oběť často fyzicky napadena.

Hoax označuje falešnou zprávu, která má za úkol rozrušit uživatele a zmást ho. Varuje před nebezpečím, které neexistuje. Často je posílán textovou podobou prostřednictvím e-mailu, kde může obsahovat nebezpečná doporučení. Důvěřiví a neznalí je-

dinci pak mohou tato doporučení následovat a mohou si způsobit škody, např. v podobě ztráty dat apod. Ve zprávě se objevuje většinou výzva, která žádá uživatele pro rozeslání zprávy na další adresy.

Phishing je podvodný e-mail, jehož cílem je vylákat důvěrné informace uživatelů internetu. Nejčastěji to bývají piny a hesla k bankovním účtům, nebo jakékoliv přihlašovací údaje. Cílem útočníka je získat informace a zneužít je ve svůj prospěch. Nejčastěji se šíří jako příloha v e-mailu, nebo jako hypertextový odkaz [35].

V odkazech se pak často útočníci snaží napodobit internetové stránky známých bank, kde se pod vymyšlenou záminkou snaží donutit uživatele, aby se přihlásil přihlašovacím jménem a heslem stejným, jako do svého internetového bankovnictví. Útočník pak jednoduše získá cenné informace.

4.5.5 Případy zneužití dat a informací

V této podkapitole se zaměřím na případy zneužití informací, které se v ČR odehrály. Je důležité říct, že existuje mnoho případů, kde došlo ke zneužití především dětí, a to prostřednictvím sítě internet a sociálních sítí.

Jeden z nejznámějších případů [36] je případ skautských vedoucí z Ústí nad Labem, kteří zneužili 38 obětí ve věku od 12 do 18 let. Dopustili se trestných činů znásilnění, zneužití dětí, výroby dětské pornografie aj. Důležité je zde podotknout, že si své oběti získával především přes internet za pomocí falešných profilů na sociálních sítí. Obvykle se zde vydávali za dívky. Následně jim posílali fotografie nahých dívek, přičemž na oplátku chtěli zaslat také fotografie. Poté, co dvojice získala tyto fotografie pak pod falešným profilem začali oběti vydírat. Posléze je donutili ke schůzce.

Další z případů [37] je záznam o podvodném jednání, kde byly zneužití osobní informace a údaje na sociální sítí Facebook s cílem se obohatit, neboť po získání osobních údajů přišel poškozený o finanční prostředky, které pachatel získával prostřednictvím elektronických plateb přes mobilní zařízení. Celý proces probíhal tak, že se na facebookovém profilu od někoho ze svých přátel objevil vzkaz se žádostí o zpřístupnění osobních údajů. Důvody pro tuto žádost měl útočník předem nachystané a poměrně vždy byly věrohodné. Po získání telefonního čísla pak následovala konverzace, kde bylo cílem potvrdit zadanou platbu přes mobil. Pachatel se obvykle snažil na oběť tlačit, především časově, kde pod tlakem oběť potvrdila platbu, aniž by si přečetla obsah zprávy. Jeden pachatel měl na svědomí přibližně 40 takových případů.

Příkladem, ve kterém účinkuje kyberstaking, je případ zákazníka kroměřížské pizzerie [38] , který půl roku obtěžoval místní servírku. Využíval k tomu především psaní výhružných emailů, neustálé psaní SMS zpráv a pronásledování na sociálních sítí. Později pak oběť fyzicky napadl, ničil ji soustavně majetek a následně před domem zabil.

Podle ministerstva financí [39] mezi nejčastější způsob zneužití identity patří to, že pachatel získá osobní údaje jiné osoby na internetu, kde například inzeruje nebankovní půjčku. Od zájemce pak vyláká kopii občanského nebo řidičského průkazu a následné výpisy z účtů (vedené na jméno oběti). Získané kopie dokumentů pak zašle bance, u níž si chce založit účet na cizí jméno. Banka poté požaduje aktivaci účtu, kterou pachatel potvrdí provedením platby alespoň jedné koruny z existujícího účtu na nově založený. Ke splnění podmínky pak pachatel vyzve zájemce o nebankovní půjčku, aby poslal na nový účet pachatele alespoň korunu, a tím potvrdí svou shodu identifikačních údajů. Po připsání platby pak pachatel dostane uživatelské jméno a klíč k internetovému bankovnictví a ten pak využívá pod jinou identitou, než je jeho vlastní. Oběti podvodu pak sdělí, že mu nebyla poskytnuta půjčka a kontakt s ní přeruší.

4.6 Bezpečnost na sociálních sítí

Bezpečnost na sociálních sítí je diskutovaným tématem. Uživatelé sociálních sítí by si měli dávat pozor na to, jaká data sdílejí, jak je nastaveno jejich soukromí a také by měli dbát na to, s jakými neznámými uživateli budou v kontaktu. Rizika, které jsem v kapitole 4.5 shrnul pak mohou potkat každého uživatele, a to především ty uživatele, kteří se nechovají na sociálních sítí bezpečně. Přesto, že jsou sociální sítě dobrým nástrojem pro udržení kontaktů, mohou být nebezpečné.

V oblasti bezpečnosti na internetu pak existuje spousta internetových stránek, které seznámí zájemce v krátkých bodech s největšími hrozby a také jakému chování se mají vyvarovat. Je zvykem, že sociální sítě interpretují v podmínkách užívání body, zaměřené na problematiku bezpečnosti, kdy uživateli radí, jak se bezpečně chovat na jejich provozované sociální síti. Obvykle pak s potvrzením registrace uživatel souhlasí s tím, že v rámci bezpečnosti nikdy nesdělí jiným osobám své heslo, nebude vytvářet více než jeden účet, nebude zveřejňovat falešné osobní informace nebo nebude podnikat žádné kroky zasahující do práv jiných osob.

4.6.1 Pravidla pro bezpečné užívání sociálních sítí

Cenné rady a pravidla, jak se chovat bezpečně na sociálních sítí a na co si dávat pozor můžeme shrnout do několika bodů: [40], [41]

- Neuvádět na veřejném profilu telefonní číslo nebo adresu. Je zde riziko možnosti zneužití těchto informací. To může vést k vyhrožování, vydírání, pronásledování nebo také krádeži.
- Neposílat nikomu svoje intimní fotografie.
- Svá hesla od účtů v zásadě nikomu nesdělovat. Všechna používaná hesla by měla zůstat v tajnosti. Doporučuje se je nesdělovat ani svým blízkým přátelům.
- Nikdy neodpovídat na neslušné či vulgární zprávy.
- Nevěřit každé informaci, kterou můžeme na internetu získat.
- Komunikovat pouze s lidmi, se kterými chceme.
- Nedomlouvat si schůzku přes internet, aniž bychom pořádně nevěděli, jaká osoba sedí naproti. Obvykle se doporučuje také někomu o schůzce říct, aby mohl pomoci v případě, že by nastaly problémy.
- Nesdělovat informace typu „kdy jedu na dovolenou“ - může to přilákat zloděje a je zde riziko vykradení.
- Být obezřetný při používání webové kamery. Video může být nahráváno.
- Kontrola nastavení soukromí na používané sociální síti. Především pak informace, které může vidět veřejnost.
- Přečíst si podmínky užívání

V rámci bezpečnosti se doporučuje alespoň částečně dodržovat uvedené body. Samozřejmostí by mělo být utajení hesla, kontrola nastavení soukromí a obezřetnost při sdílení svých fotografií. Každý z uživatelů by si měl před vstupem na sociální síť důkladně pročíst podmínky užívání, ale z vlastních zkušeností a poznatků mohu tvrdit, že převážná část lidí se na to nezaměřuje.

4.7 Výhody sociálních sítí

Mezi největší výhody sociálních sítí patří možnost neomezené komunikace s velkou skupinou lidí. Výhodou je také to, že se uživatelé při komunikaci na sociálních sítí cítí příjemně, a to jak v osobní komunikaci s přáteli a blízkými, tak v marketingové komunikaci. Mezi další výhody patří efektivita a jednoduchost sdílení informací a možnost

předávat uživatelům informace o produktech nebo službách. Na vybraných sociálních síti je jednoduché prezentovat své dovednosti v rámci určitých skupin a „fun page“, kde se jedinec může lehce zviditelnit. V rámci skupin je možné vytvářet různé ankety, události nebo vyhlašovat soutěže. Na sociálních sítí si jsou všichni uživatelé rovnocenní a nezáleží zde na vzhledu, věku či výši přijmu, což můžeme brát také jako velikou výhodu. Komunikace mezi uživateli je obousměrná a efektivní, to se může často hodit při snaze získat okamžitou zpětnou vazbu [42].

Sociální sítě mohou být i naučné. Najdeme zde skupiny nadšenců, kteří mohou v rámci skupin nebo svých profilů sdílet zajímavé informace o tématech, které nás zajímají. Může také sloužit jako inzerce věcí. Profesně zaměřené sociální sítě pak pomáhají uživatelům zlepšovat se ve svém oboru a tvořit jejich kariéru.

4.8 Nevýhody sociálních sítí

Mezi největší nevýhodu bych zařadil možnost narušení soukromí a s tím spojené veškeré hrozby a rizika, které jsou podrobněji shrnuty v podkapitole 4.5. Jelikož sociální sítě jsou bezesporu určitou formou zábavy, tak často dochází k vytvoření závislosti, především u dospívajících dětí. Často zde tráví nepřiměřené množství času. Další nevýhodou můžou být nežádoucí reklamy, které se mohou objevit. Sociální sítě také mohou být zdrojem virů a podvodů s cílem poškodit uživatele.

4.9 Ochrana soukromí na sociálních sítí

V prostředí sociálních sítí se setkáváme ze spousty osobních informací. Obavy o své soukromí na sociálních sítí podle dostupného průzkumu od společnosti Intel [43] má většina Čechů a 60 % z nich pak uvádí, že se cítí být přehlceni osobními informacemi a daty, které se k nim na sociálních sítí dostávají. Ochrana soukromí je celosvětově diskutovaným tématem. Existuje spousta článků, průzkumů a dostupných informací s názory, že na internetu vlastně žádné soukromí neexistuje. Tyto články jsou založeny buď na domněnce autora, nebo jsou podloženy informacemi, které ale nemusí být pravdivé.

Zneužít, popřípadě využít osobní informace registrovaných uživatelů mohou jak uživatelé sociálních sítí (neoprávněně), tak i samotní autoři sociálních sítí, nebo aplikace či programy běžící na ní. To zajímavé na tom je, že při registraci na sociálních

sítí obvykle každý registrovaný uživatel souhlasí s podmínkami, kde se mimo jiné říká, jak sociální síť využívá data uživatelů. Bývá zde uvedeno, jak sociální sítě využívají osobní informace nebo aktivity uživatelů a na co si vyhrazují právo. Obvykle zde také bývá uvedena část, jaké informace shromažďují a za jakým účelem.

Ačkoliv sociální sítě tyto podmínky mají jasně stanovené, existuje řada kauz a informací, které nasvědčují tomu, že ze strany některých sociálních sítí dochází k úniku informací, popřípadě porušování ochrany soukromí uživatelů. Například v roce 2015 [44] tisíce rakouských uživatelů sociální sítě Facebook žalovalo síť kvůli špehování uživatelů a shromažďování jejich osobních dat bez souhlasu – a to třeba za účelem lépe cílené reklamy, tedy sledování lidí, jaké stránky navštěvují, a to ani nemusí být aktivní na sociální síti Facebook. Podle dalších žalob [45], [46] pak sociální síť Facebook porušuje evropské zákony především tím, že sleduje lidi bez jejich souhlasu a spolupracuje s americkými korporacemi. Za zmínku stojí také žaloba na společnost Google [47] o porušení ochrany dat při získávání dat pro službu Street View, kde bylo zjištěno, že mimo snímání měst pro panoramatické záběry Google také sbíral data z nezakódovaných sítí jako například e-maily, internetové adresy nebo přístupová hesla. Google sám tento čin potvrdil.

V rámci ochrany soukromí se v dalších podkapitolách zaměřím na zákon o ochraně soukromí a na podmínky používání tří vybraných sociálních sítí (Facebook, Instagram a Google+). Tyto sociální sítě byly vybrány vzhledem k výsledkům zpracovaného výzkumu, kde byly uváděny jako nejpoužívanější.

4.10 Právní rámec ochrany soukromí

Zákon, který reguluje ochranu osobních údajů v České republice, se nazývá Zákon o ochraně osobních údajů č. 101/2000 Sb.,. Rozlišují se zde osoby, které zpracovávají osobní údaje jiných lidí (správce nebo také zpracovatel osobních údajů) a osoby, jejichž osobní informace správce a zpracovatel zpracovávají (subjekty údajů). Správcům jsou přiřazeny povinnosti a subjektům práva [48]. Mezi některé povinnosti správců patří: [49]

- Stanovit účel, k němuž mají být osobní údaje zpracovány
- Stanovit prostředky a způsob zpracování osobních údajů
- Zpracovávat osobní údaje pouze se souhlasem subjektů údajů

- Informovat subjekty údajů v jakém rozsahu a pro jaký účel budou osobní údaje zpracovány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny
- Zpracovávat pouze přesné osobní údaje, které získal v souladu se zákonem
- Blokovat a likvidovat osobní údaje tehdy, pokud nejsou přesné
- Oznámit zpracování osobních údajů Úřadu pro ochranu osobních údajů
- Dbát, aby při zpracování osobních údajů subjekt údajů neutrpěl újmu na svých právech

Mezi práva subjektů patří: [50]

- Právo na přístup k informacím o zpracování osobních údajů
- Domáhat se ochrany osobních údajů podle norem trestního zákona
- Subjekt může požádat o informaci o zpracování svých osobních údajů a správce je povinen mu informaci předat
- Subjekt může vést občanskoprávní nebo trestní řízení při porušení povinností správce nebo nedodržení ustanovení
- Právo vědět za jakým účelem budou informace zpracovány
- Právo vědět předmět zpracování a příjemce

Výčet těchto práv a povinností není úplný. Celé znění zákona č. 101/2000 Sb., o ochraně osobních údajů je velmi rozsáhlé, a navíc obsahuje spoustu dalších norem a je spojen s dalšími zákony. V souhrnu se zde dále uvádí různé nástroje na ochranu soukromí, další právní předpisy, povinnosti a práva subjektů a správců, analýza žádostí, jako např. žádost o podání informace o zpracování osobních údajů aj. Jsou zde také vymezeny pojmy jako ochrana soukromí, citlivý údaj, anonymní údaj nebo evidence osobních údajů.

Při nedodržení nebo neplnění svých povinností, hrozí správci nebo zpracovateli osobních údajů sankce, a to ve formě přestupku nebo trestného činu v závislosti na typu prohřešku. Kontrolu plnění povinností provádí Úřad na ochranu osobních údajů, který také řídí sankce [48].

4.11 Podmínky používání

Každá internetová stránka, která nabízí nějaké služby s sebou nese podmínky užívání, které jasně stanovují pravidla používání a u sociálních sítí tomu není jinak. Ať už se jedná o stránky zaměřené na obchodní činnosti, herní portály, online hry nebo stránky

nabízející produkty, softwary či služby (email, inzerce, zájezdy, seznamky, aj…), tak se pokaždé setkáme s všeobecnými podmínky užívání. Pokud má uživatel možnost se registrovat, nebo stránka jakýmkoliv způsobem pracuje s osobními daty uživatelů, je povinností autorů vymezit ochranu soukromí, v nichž je mimo jiné uvedeno, jakým způsobem data shromažďují a jak je využívají.

U sociálních sítí jsou tyto podmínky poměrně podrobně rozepsány a jsou velmi rozsáhlé, což se dá předpokládat, vzhledem k možnostem, které nabízejí. Obvykle se v této sekci objevují prohlášení o právech a povinnostech uživatelů, dále se zde objevují zásady používání dat, kde je dopodrobna rozepsáno, jaké druhy informací konkrétní sociální síť shromažďuje, za jakým účelem, proč a jak mohou být informace využity. Součástí jsou také zásady a pravidla komunity a smluvní podmínky (registrací uživatel obvykle vytváří nějaký smluvní vztah ze společností poskytující dané služby). Dále se uvádí zabezpečení, popřípadě centrum bezpečnosti, kde je uživatel seznámen například s tím, jak nahlásit porušení podmínek užívání nebo zneužití informací a je seznámen s riziky, které s sebou nese využívání dostupných služeb.

Tyto uvedené body jsou základem podmínek používání a setkáme se s nimi u všech sociálních sítí. Další body podmínek používání se pak odvíjejí podle služeb, které sociální sítě nabízejí „navíc“. Může se jednat například o podmínky vztahující se k platbám, reklamám nebo využívání dalších aplikací či softwaru zprostředkovaných stejnou sociální sítí.

4.12 Zásady používání dat

Shrneme si stručně zásady používání dat u vybraných sociálních sítí, a to u Facebooku, Instagramu a Google+. Nejprve se podíváme na **Facebook.** Hned v úvodu Facebook upozorňuje, že zásady, které jsou k dispozici se vztahují pro všechny produkty a služby, které poskytují, pokud není výslovně řečeno, že tomu tak není. To je velmi důležitá informace. Jaké druhy informací tedy Facebook shromažďuje? [51]

- **Informace, které uživatelé sdílí**. Facebook má právo shromažďovat obsah, který uživatel poskytne při využívání jejich služeb. Patří sem například informace uvedené při registraci účtu, posílání nebo sdílení zpráv či jiné komunikace s ostatními uživateli. Také sem patří informace o obsahu, který na sociální síť uživatel nahraje, například místo a datum pořízení fotky, nebo datum vytvoření souboru. Facebook si vyhrazuje právo na shromažďování informací o tom, jak

uživatel využívá jejich služby, například typ veškerého obsahu, který si nejčastěji prohlíží, nebo se kterým je nějakým způsobem propojený. Patří sem také informace o frekvenci a době trvání aktivit na sociální síti. To platí i tehdy, pokud ostatní uživatelé například poskytnout informace o jiném uživateli nebo s ním sdílí fotku či komunikují přes zprávy.

- **Informace o spojení.** Pokud uživatel využívá synchronizaci kontaktů, tak i informace adresářů z konkrétního zařízení může Facebook shromažďovat. Také shromažďuje informace o lidech či skupinách, se kterými je uživatel ve spojení.
- **Informace o platbách.** Pokud uživatel provede jakoukoliv transakci na Facebooku nebo službách spojených s ním, tak automaticky dává Facebooku údaje o své kreditní nebo debetní kartě (číslo karty, informace o kartě, další informace o účtu a přístup k fakturaci platby). Také shromažďuje veškeré informace o nákupu.
- **Informace o zařízení.** Uživatel, který využívá na jakémkoliv zařízení Facebook a služby spojené s ním, dává souhlas ke shromažďování informací o tomto zařízení, jako je verze operačního systému, verze hardwaru, nastavení zařízení, názvy a typy souborů a softwaru, výkon baterie, síla signálu a identifikátory zařízení. Dále pak umístnění zařízení (přesné GPS souřadnice a poloha), signál WiFi či Bluetooth. Patří sem i veškeré informace o připojení (IP adresa, typ prohlížeče, číslo mobilního telefonu, aj.)
- **Informace z webů a aplikací, které využívají služby Facebooku.** Patří sem shromažďování informací při návštěvě webů nebo aplikací třetích stran, které využívají služby Facebooku.
- **Informace od externích partnerů**. Facebook získává informace od svých partnerů, a to o veškerých aktivitách uživatele na Facebooku, ale i mimo něj. Záměrně jsem se snažil najít nějaký seznam partnerů, se kterými Facebooku spolupracuje, ale bohužel jsem je nenašel.

Další sociální síť, kterou si shrneme je **Instagram**. Ten slouží primárně ke sdílení fotografií, a tudíž i zde je spousta informací, které systém shromažďuje. Jaké druhy údajů tedy Instagram shromažďuje? [52]

- **Údaje, které uživatel poskytne přímo.** Instagram má právo shromažďovat uživatelské jméno, heslo a e-mailovou adresu uvedenou při registraci. Dále pak informace uvedené v profilu (jméno, příjmení, telefonní číslo, …) a veškerý uživatelský obsah jako jsou fotky, komentáře a další materiály.
- **Analytické údaje.** Instagram využívá analytické nástroje třetích stran, které shromažďují informace odeslané ze zařízení, včetně navštívených webových stránek, doplňků a dalších informací.
- **Soubory cookie a podobné technologie.** Instagram má právo sledovat jakým způsobem uživatel používá služby Instagramu, a to za pomocí souborů cookies. Dále mohou požádat své partnery nebo inzerty, aby do zařízení uživatelů, na kterém využívají služeb Instagramu, umístily reklamu nebo poskytly jiné služby.
- **Identifikační údaje zařízení.** Tato část je víceméně stejná jako u sociální sítě Facebook. Navíc ale Instagram shromažďuje veškeré mobilní údaje, vyhrazuje si právo vzdáleně ukládat, monitorovat nebo přistupovat k zařízení uživatele. Identifikačními údaji jsou myšleny malé datové soubory nebo podobné datové struktury uložené na mobilním zařízení uživatele, které dané mobilní zařízení jedinečně identifikují. Mezi to patří data uložená ve spojení s hardwarem zařízení nebo data uložená v souvislosti s operačním systémem.

Poslední ze sítí, u které si shrneme shromažďování informací je **Google+.** I zde figuruje obrovské množství osobních dat a informací. Jak tyto data využívá společnost Google? [53]

- **Informace, které uživatelé sdělují.** Google si vyhrazuje právo na informace, které uživatel sám poskytne při registraci. Patří sem například jméno, příjmení, e-mailová adresa, telefonní číslo nebo platební karta.
- **Informace, které Google získává od uživatelů při používání služeb.** Google shromažďuje informace o službách, které uživatelé využívají, i jak je používají.
- **Informace o zařízení.** Stejně jako u předchozích sociálních sítí i Google si bere právo na shromažďování veškerých informací o zařízení uživatele (model hardwaru, verze operačního systému, údaje o mobilní síti a telefonní číslo).
- **Informace z protokolu.** Při využívání služeb si Google automatizovaně ukládá a shromažďuje informace do protokolů. Shromažďuje si do nich například podrobnosti o tom, jak uživatel službu použil, informace o telefonování, číslo

volajícího, čas a datum hovorů, trvání hovorů, údaje o směrování SMS zpráv a typy hovorů. Zde patří i soubory cookie, které si uchovávají informace o typu prohlížeči.

- **Informace o poloze**. Google shromažďuje také informace o poloze, jako jsou IP adresa, GPS souřadnice nebo přístupové body WiFi sítí a vysílače mobilních sítí.
- **Soubory cookie a podobné technologie.** Ty jsou využívány k identifikaci prohlížeče nebo zařízení. Tyto informace pak Google shromažďuje, ukládá a poskytuje jiným partnerům například pro reklamní služby.

Pokud si shrneme tyto dostupné informace, které obsahují podmínky užívání, tak je zřejmé, že veškerá aktivita na sociálních sítí je do značné míry monitorována a používána za dalšími účely. To samé platí i o sdílených informacích a osobních datech. Na zamyšlení je skutečnost, že tyto služby využívají i typy informací jako detailní informace o zařízení a poloze, síťové informace, nebo informace o pohybu mimo sociální sítě. Nejvíce překvapující je pro mě skutečnost, že Google využívá i veškeré informace a podrobnosti o telefonování. Snažil jsem se dohledat za jakým přesným účelem tyto informace o telefonování shromažďují, ale dopátral jsem se pouze k vysvětlení, že je to za účelem údržby, vylepšení a k ochraně systému. Je nutné opět dodat, že registrací uživatel souhlasí se všemi těmito podmínky a zpracováním dat.

4.13 Prohlášení o právech a povinnostech

Každá sociální síť má v podmínkách užívání smlouvu, která se zaměřuje na práva a povinnosti jak uživatelů, tak konkrétní sociální sítě. Bývají zde uvedeny obecné informace o soukromí, sdílení obsahu, bezpečnosti, postupy řešení při sporech a další ustanovení. Obvykle se zde objevují také různá doporučení, doplňující podmínky či různé nástroje (například nástroje pro nahlášení porušení práv, možnosti nastavení soukromí, aj.), které jsou uživateli k dispozici. Bývá zde i zobecnění všech práv sociální sítě, ať už se jedná o právo na shromažďování veškerých dat, které jsme si v kapitole 4.12 shrnuly, nebo práv na trestní stíhání uživatele při porušení jeho povinností.

Nejprve se zaměříme na **Facebook** a na jeho důležité body práv a povinností. Pokud se zaměříme konkrétněji na soukromí, tak zde Facebook uvádí právo na veškerý sdílený obsah a také má oprávnění využít používané aplikace uživatelů vzhledem k nastavení aplikací.

Povinností uživatelů, především kvůli bezpečnosti na sociální síti, je nezveřejňovat neautorizovaná komerční sdělení, neshromažďovat informace o jiných uživatelích, nezastrašovat jiné uživatele a nezveřejňovat nenávistné projevy a pornografii. Patří sem i zákaz používání chyb, tzv. „bugů“ stránek a také povinnost tyto chyby nahlásit. Další důležité body jsou nenapomáhat uživatelům k porušení Podmínek používání nebo zákaz nahrávání škodlivých souborů (PC viry a jiné škodlivé kódy) [54].

Mezi dalšími povinnostmi z hlediska bezpečnosti účtů je neposkytovat falešné osobní údaje, nevyužívat více účtů nebo nepoužívat služby Facebook, pokud je uživatel mladší 13 let. Patří sem i povinnost nikomu nesdělovat své osobní heslo k účtu či nepoužívat své účty za komerčním účelem. Při porušení těchto povinností má Facebook právo uživatelský účet odstranit [54].

Pokud se zaměříme na **Instagram,** tak se zde objevují stejné body jako u Facebooku. I zde platí, že sociální sít nesmí využívat osoby mladší 13 let. Je zakázané zveřejňovat fotografie se sexuálním kontextem, to platí i pro rasistický obsah a obecně obsah, který je v rozporu se zákonem daného státu. Patří sem také povinnost odpovědnosti za veškeré aktivity, které jsou spojeny s účty uživatelů. Povinností uživatelů je také nesdělovat hesla cizím osobám, nezneužívat fotografie a jiná data uživatelů a nepoužívat své účty k neoprávněným aktivitám [55].

Zajímavostí jde zde upozornění v úvodu prohlášení, že registrací uživatel souhlasí s tím, že pokud dojde ke zrušení účtu, tak veškeré spory mezi uživateli a službou Instagram budou řešeny pouze závazným individuálním řízením. Registrací se uživatel zříká práva na účasti při žalobě nebo skupinovém rozhodčím řízením proti službě Instagram [55].

Google+ je na tom obdobně jako předchozí sociální sítě. V prohlášení je jasně stanovena povinnost uživatele řídit se všemi zásady, které jsou v rámci služeb k dispozici. Uživatel nesmí zneužívat služby. Google má právo odstranit účet uživatele, pokud usoudí, že jeho jednání není v souladu s podmínky. Uživatel má právo nahlásit jiné uživatele, pokud porušují autorská práva nebo zneužívají informace. Stejně jako u předchozích sítí, i zde není možné sdílet obsah rasistický, sexuální či násilný.

Google se zříká své odpovědnosti za ušlý zisk, ztrátu tržeb, ztrátu dat, financí a za další škody, které mohou nastat při využívání jejich služeb a také jasně stanovuje způsoby, jakými uživatelé mohou služby využívat. Uživatel je povinen využívat aplikace Google pouze pro své účely. Aktivity, které na nich provádí, jsou k dispozici službám Google [56].

Pokud shrneme práva a povinnosti uživatelů a poskytovaných služeb, tak se vybrané sociální sítě téměř ve všem shodují a tyto podmínky mají stanoveny podobně. Zajímavým bodem je potvrzení, že vybrané sociální sítě jsou dostupné až od 13 let, přičemž podle průzkumů rozebíraných v kapitole 1, spousta dětí mladších 13 let tyto služby využívá a tím porušují pravidla užívání. Pokud by pak například sdílely informace v rozporu s dalšími ujednáními, nebo porušovaly prohlášení o právech a povinnostech, může dojít k právnímu stíhání ze strany poskytovatele služeb.

4.14 Možnosti nastavení zabezpečení a soukromí účtu

V rámci ochrany soukromí sociální sítě nabízejí uživatelům možnost chránit si soukromí, a to především před ostatními uživateli. V této části si uživatelé mohou přizpůsobit své účty tak, jak chtějí, ale pouze v závislosti na tom, co jim používané sociální sítě umožní. Opět si shrneme možnosti toho nastavení u vybraných sociálních sítí.

Zaměřme se na sociální síť **Facebook.** V části, která se nazývá centrum nápovědy je k dispozici nástroj pro základní nastavení soukromí. Zde jsou uživateli vysvětleny základní pojmy soukromí a možnosti správy. Všechny tyto nástroje jsou podpořeny obrázky pro lepší orientaci v celém nastavení. V nastavení účtu má pak uživatel možnost jednoduše přejít na nastavení soukromí, které se skládá z několika částí. Může zde nastavit osobní informace, do kterých patří jméno, příjmení, e-mailová adresa, uživatelské jméno nebo obecnou správu účtu, do které patří možnost deaktivace účtu, nebo je zde dokonce možnost vybrat si osobu, která bude v případě smrti uživatele spravovat účet. Také je zde možnost požádat o odstranění účtu po smrti uživatele.

K možnostem zabezpečení účtu patří oprávnění vybrat si tři uživatele sociální sítě, kteří se postarají o přístup k účtu, pokud bude mít uživatel problémy s přihlášením. Je zde také možnost propojení účtu s telefonem. Uživatel může k přihlašování využít dvoufázového ověření, například pomocí hesla a e-mailu, nebo hesla a kódu, který je možný zaslat na mobilní zařízení.

V části soukromí pak může uživatel nastavit, které osoby uvidí přidávané příspěvky, kdo uvidí seznam přátel, nebo kdo může uživatele kontaktovat a vyhledat. Pokud se zaměříme na přidávaný obsah a označování, tak je zde možnost přidávat obsah veřejně, soukromě, nebo pouze pro přátele a přátele přátel. Uživatel má možnost vypnout označení v příspěvcích, nebo vyžadovat kontrolu a povolení o označení. Může také vypnout zobrazení svých fotografií, videozáznamů a jiných multimédií pro

veřejnost. To samé platí i o zobrazení koníčků a zájmů, popřípadě osobních informací. Uživatel má možnost blokovat zprávy od nežádoucích uživatelů, pozvánky aplikací a událostí nebo blokovat celé aplikace a uživatele.

Další částí je možnost nastavení reklam a detailní informace o tom, jak reklamy fungují. Dále se zde objevují možnosti nastavení aplikací, plateb, kde je k dispozici správa a historie všech plateb, nebo videí. Také je zde možnost nahlášení uživatelů, za porušení podmínek.

Pokud se podíváme na nastavení **Instagramu**, tak zde má uživatel možnost nastavit soukromí svých fotografií. Defaultně je toto nastavení na veřejné, což znamená, že všichni uživatelé mají přístup ke všem fotografiím uživatelů s tímto nastavením. Uživatel může své fotografie nastavit soukromě, pouze pro své „followery". Instagram povoluje rovněž blokování nežádoucích osob. Soukromé nastavení je možné i u označení fotografií či komentářů, kde se jednoduše ve správě nastavení soukromí dá tato možnost přepínat. U komentářů je možné také vyfiltrovat nežádoucí komentáře pomocí klíčových slov, nebo je celkově skrýt, popřípadě je vypnout.

Uživatelé mají možnost svého sledujícího odebrat, pokud se tak rozhodnou. Instagram navrhuje podobné profily uživatelů, které mají něco společného. To je realizováno za pomocí shromažďování informací o uživatelích, a i zde je možnost vypnutí. Uživatelé také mohou, za pomocí návodu, odvolat udělení přístupu pro weby třetích stran. Tato možnost se využívá tehdy, pokud uživatel nechce, aby se jeho fotografie zobrazovaly ve vyhledávání Google. Instagram také nabízí dočasnou deaktivaci účtu nebo jeho odstranění, přičemž při úplném odstranění požaduje udání důvodu, většinou z předem předvyplněných možností.

Mobilní aplikace Instagramu dále umožňuje nastavit dvoufázové ověření, záložní kód, či možnosti upozornění a cestu uložení fotografií. Je zde také možnost vymazat veškeré údaje o historii prohlížení na Instagramu. K tomu je třeba dodat, že veškeré nastavení probíhá právě přes mobilní aplikaci. Pokud uživatel přistupuje k Instagramu přes webové rozhraní na počítači, tak nemá přístup k nástroji pro nastavení soukromí. Roli zde nehraje verze prohlížeče ani typ operačního systému.

Google+ nabízí tzv. ovládací prvky, pomocí nichž si uživatel může své soukromí spravovat. Uživatel může spravovat osobní informace jako jméno, příjmení, datum narození, e-mail nebo telefon. Dále pak může upravovat informace, které vidí jiní uživatelé, jako například určení, jaké údaje z profilu uživatelé uvidí, zobrazení příspěvků,

nastavení fotografií a videozáznamů. Je také možné zaznamenávat historii polohy, informace o zařízení a aktivity na webu do své profilové historie. Tyto údaje uvidí pouze konkrétní uživatel, nebo služba Google, pokud jim to uživatel povolí. Nechybí zde také nastavení reklam a vyhledávání, možnosti blokovat a nahlásit uživatele a nastavení upozornění a oznámení. V oznámeních si uživatel může vypnout například zasílání novinek, nových příspěvků, nových fotografií a událostí na e-mail. To samé platí pro oznámení na mobilní telefon.

I zde je možná správa příspěvků, kde uživatel může nastavit soukromí sdíleného obsahu. V rámci tohoto nastavení si pak může vytvořit také skupiny lidí, které budou mít možnost komentovat příspěvky a fotografie. Komentáře lze vypnout i pro všechny uživatele. Najdeme zde také nastavení, kde uživatel může povolit stažení svých fotografií dalším uživatelům. K tomu všemu patří i nastavení Google disku, především nastavení kopií dat, archivování, stažení a přenosu. Celý uživatelský účet je možné smazat a je také údajně možné smazat veškerá data a informace spojené s uživatelským účtem, ať se jedná o sdílená data, osobní informace, historii prohlížení a aktivit, informace o zařízení, připojení, typ sítě aj. Do jaké míry budou data spojená s účty uživatelů vymazána, je otázkou.

Vybrané sociální sítě nabízejí uživatelům velmi široké možnosti nastavení soukromí a zabezpečení účtů. Vzhledem k zaměření služeb to není příliš překvapivé. Uživatelé sociálních sítí by měli alespoň jednou projít celou konfiguraci soukromí a měli by možnosti nastavení znát. Zároveň by měli dbát na bezpečné užívání sociálních sítí a na všeobecná pravidla bezpečného užívání internetu. Nástroj nastavení soukromí a zabezpečení se většinou objevuje na viditelných místech, kterých si uživatel snadno všimne. Pokud však uživatel není schopen tento nástroj najít, je možné dohledat informace v nápovědě. Bývá zde uveden i obrázkový postup, jak se dostat do takového nastavení.

5 Výzkumný záměr

5.1 Hlavní výzkumný problém a definice hypotéz

V první řadě jsem si vymezil hlavní výzkumný problém a následně výzkumné otázky, na které jsem si chtěl odpovědět. Byly stanoveny také hypotézy výzkumu, které jsem pomocí statistické metody zpracoval. Celkem bylo stanoveno 22 výzkumných otázek a k tomu 19 hypotéz, kde jsem zjišťoval závislosti mezi veličinami.

Hlavní výzkumný problém:

- Jak přistupují žáci k problematice ochrany soukromí na sociálních sítí?

Zkoumané výzkumné otázky:

- Jaká data sdílejí žáci základních škol na sociálních sítí?
- Dokáží si žáci základní škol nastavit soukromí svého účtu?
- Znají žáci základních škol rizika při sdílení dat na sociálních sítí?
- Existuje rozdíl mezi žáky, kteří sdílí a kteří nesdílí svá data vzhledem k nastavení vkládaného obsahu na sociálních sítí a pohlavím?
- V jaké míře sdílí žáci základních škol svá data na sociálních sítí?
- S jakými typy pokusů o zneužití dat se žáci základních škol setkali?
- Je pro žáky základních škol důležité chránit si soukromí na sociálních sítí?
- Vnímají žáci základních škol sociální sítě jako zdroj osobních informací o svých přátelích/sledujících?
- Jakým způsobem nastavují žáci základních škol viditelnost sdíleného obsahu na sociálních sítí?
- Jsou žáci základních škol na sociálních sítí v kontaktu s lidmi, které neznají?
- Existuje vztah mezi věkem respondenta a znalostí nastavení soukromí svého účtu na používané sociální síti?
- Existuje vztah mezi zkušenostmi se zneužitím dat a neznalosti prohlášení o ochraně soukromí na používané sociální síti?
- Má pohlaví, místo bydliště nebo počet obyvatel místa bydliště vliv na sdílení soukromých informací (místo bydliště, telefonní číslo, věk, škola)?
- Má věk nebo místo bydliště vliv na uvědomování si rizik spojených se sdílením soukromých dat?
- Má pohlaví nebo věk vliv na znalost prohlášení o zásadách používání dat?

- Do jaké míry žáci základních škol věří sdíleným informacím na sociálních sítí?
- Existuje vztah mezi pohlavím a dovednosti nastavení zabezpečení a soukromí účtu na sociálních sítí?
- Existuje vztah mezi nastavením vkládaného obsahu, místem bydliště, pohlavím a sdílením osobních informací na sociálních sítí?
- Existuje vztah mezi znalostí nastavení zabezpečení soukromí svého účtu a sdílením osobních informací na sociálních sítí?
- Existuje vztah mezi sdílením svých fotografií a uvědomováním si rizik spojených se sdílením osobních dat na sociálních sítí?
- Existuje vztah mezi znalostí nastavení zabezpečení a soukromí svého účtu a pohlavím?
- Má věk nebo pohlaví vliv na sdílení svých fotografií na sociálních sítí?

Na základě uvedených výzkumných otázek byly stanoveny tyto hypotézy:

- H_{01}: Mezi znalostí nastavení zabezpečení a soukromí účtu na sociální síti a věkem neexistuje závislost.
- H_{A1}: Mezi znalostí nastavení zabezpečení a soukromí účtu na sociální síti a věkem existuje závislost.
- H_{02}: Mezi zkušeností se zneužitím dat a znalostí prohlášení o ochraně soukromí na používané sociální síti neexistuje závislost.
- H_{A2}: Mezi zkušeností se zneužitím dat a znalostí prohlášení o ochraně soukromí na používané sociální síti existuje závislost.
- H_{03}: Mezi sdílením osobních informací a pohlavím neexistuje závislost.
- H_{A3}: Mezi sdílením osobních informací a pohlavím existuje závislost.
- H_{04}: Mezi sdílením osobních informací a věkem neexistuje závislost.
- H_{A4}: Mezi sdílením osobních informací a věkem existuje závislost.
- H_{05}: Mezi sdílením osobních informací a počtem obyvatel v místě bydliště neexistuje závislost
- H_{A5}: Mezi sdílením osobních informací a počtem obyvatel v místě bydliště existuje závislost
- H_{06}: Mezi uvědomováním si rizik spojených se sdílením osobních dat a věkem neexistuje závislost.
- H_{A6}: Mezi uvědomováním si rizik spojených se sdílením osobních dat a věkem existuje závislost.

- H_{07}: Mezi uvědomováním si rizik spojených se sdílením osobních dat a místem bydliště neexistuje závislost.
- H_{A7}: Mezi uvědomováním si rizik spojených se sdílením osobních dat a místem bydliště existuje závislost.
- H_{08}: Mezi znalostí prohlášení o zásadách používání dat a pohlavím neexistuje závislost.
- H_{A8}: Mezi znalostí prohlášení o zásadách používání dat a pohlavím existuje závislost.
- H_{09}: Mezi znalostí prohlášení o zásadách používání dat na používané sociální síti a věkem neexistuje závislost.
- H_{A9}: Mezi znalostí prohlášení o zásadách používání dat na používané sociální síti a věkem existuje závislost.
- H_{010}: Dívky a chlapci se neliší v dovednosti nastavení zabezpečení a soukromí účtu na sociálních sítí.
- H_{A10}: Dívky a chlapci se liší v dovednosti nastavení zabezpečení a soukromí účtu na sociálních sítí.
- H_{011}: Mezi nastavením vkládaného obsahu a sdílením osobních informací neexistuje závislost.
- H_{A11}: Mezi nastavením vkládaného obsahu a sdílením osobních informací existuje závislost.
- H_{012}: Mezi znalostí nastavení zabezpečení soukromí svého účtu a sdílením osobních informací neexistuje závislost.
- H_{A12}: Mezi znalostí nastavení zabezpečení soukromí svého účtu a sdílením osobních informací existuje závislost.
- H_{013}: Mezi sdílením svých fotografií a uvědomováním si rizik spojených se sdílením osobních dat neexistuje závislost.
- H_{A13}: Mezi sdílením svých fotografií a uvědomováním si rizik spojených se sdílením osobních dat existuje závislost.
- H_{014}: Mezi sdílením dat a nastavením vkládaného obsahu neexistuje závislost.
- H_{A14}: Mezi sdílením dat a nastavením vkládaného obsahu existuje závislost.
- H_{015}: Mezi sdílením svých fotografií a pohlavím neexistuje závislost.
- H_{A15}: Mezi sdílením svých fotografií a pohlavím existuje závislost.
- H_{016}: Mezi sdílením svých fotografií a věkem neexistuje závislost.

- H_{A16}: Mezi sdílením svých fotografií a věkem existuje závislost.
- H_{017}: Mezi nastavením vkládaného obsahu a místem bydliště neexistuje závislost.
- H_{A17}: Mezi nastavením vkládaného obsahu a místem bydliště existuje závislost.
- H_{018}: Mezi sdílením dat a pohlavím neexistuje závislost.
- H_{A18}: Mezi sdílením dat a pohlavím existuje závislost.
- H_{019}: Mezi nastavením vkládaného obsahu a pohlavím neexistuje závislost.
- H_{A19}: Mezi nastavením vkládaného obsahu a pohlavím existuje závislost.

5.2 Cílová skupina respondentů

Jako cílovou skupinu respondentů jsem si vybral žáky základních škol ve věkovém rozmezí 12–15 let. Důvodem výběru této věkové kategorie respondentů byl fakt, že děti v tomto věkovém rozmezí bývají nejrizikovějšími uživateli sociálních sítí. Celkem bylo osloveno 6 základních škol, z toho 5 ze středočeského kraje (3 školy z okresu Příbram, 2 školy z hlavního města Praha) a 1 z jihomoravského kraje (základní škola v Brně). Celkem bylo sebráno 404 dotazníků.

5.3 Návrh dotazníku

Jako výzkumný nástroj jsem si zvolil metodu dotazníkového šetření. Dotazník obsahuje 22 otázek, přičemž zde využívám otevřené, uzavřené a polouzavřené otázky. Strukturu dotazníku jsem navrhnul tak, aby v úvodu dotazníku respondent odpovídal na jednodušší otázky a později na ty složitější, z důvodu udržení pozornosti. Dotazník obsahuje úvodní předmluvu, kde jsem žáky stručně seznámil s výzkumem a také obsahoval ujištění o anonymitě dat. Formulace otázek a odpovědí byla přizpůsobena věkové skupině respondentů, primárním cílem srozumitelnost.

Srozumitelnost dotazníku byla testována v předvýzkumu u věkově stejných dětí, jako je věk respondentů zpracovaného výzkumu. V předvýzkumu jsem se také kromě formulace otázek zaměřil na čas vyplňování, kde jsem se snažil o nepříliš velké množství otázek z důvodu udržení pozornosti. Také jsem se snažil o co nejstručnější formulaci otázek. Po vyplnění dotazníku jsem čekal na zpětnou vazbu vyplňujících, a na základě připomínek jsem dotazník přizpůsobil pro co nejlepší výsledek.

V rámci návrhu dotazníku se zaměřím na ukázky využitých typů otázek.

Ukázka otevřené otázky:

Máš nějakou osobní zkušenost se zneužitím dat na sociální síti? Pokud ano zkus se rozepsat :).

Dále zde bylo ohraničené pole, kde mohl uživatel volně sepsat svou odpověď. Tato otázka byla nepovinná a byla uvedena na konci dotazníku.

Ukázka uzavřené otázky:

Jsou pro tebe sociální sítě zdrojem osobních informací o Tvých přátelích?

- *Ano, díky sociální síti vím o mých přátelích vše*
- *Ano, sociální síť mi poskytuje některé osobní informace o mých přátelích*
- *Ano, ale nezajímám se o to*
- *Ne*

Tento typ otázek jsem využíval nejvíce. Mimo odpovědí, kde respondent musel vybrat pouze jednu z nabízených možností jsem využíval také typ odpovědí, kde mohl zaškrtnout jednu nebo více možností.

Ukázka polouzavřené otázky:

Kde bydlíš?

- *Město*
- *Vesnice*
- *Jiné …*

Tento typ otázky jsem využil pouze v jednom případě a to tehdy, když jsem se ptal na bydliště. Vzal jsem v úvahu, že může respondent odpovědět jinak, než je uvedeno, a proto jsem přidal možnost „Jiné“, kde měl respondent možnost odpovědět podle sebe.

5.3.1 Ověření konzistentnosti odpovědí

V dotazníku jsem využil metodu lži skóre, která má za úkol zjistit poctivost při vyplňování dotazníku. Předpokládal jsem, že by někteří respondenti mohli projevit nezájem o vyplnění dotazníků a mohli by vyplňoval schválně všechny otázky náhodně, a právě tyto záznamy by mohli zkreslit výsledky výzkumu, a proto jsem se je snažil zachytit a vyřadit.

Tuto metodu jsem realizoval tak, že jsem do výzkumu začlenil záměrně dvojice otázek, které byly významově totožné, ale byly jinak položeny a formulovány. Pozice

otázek byly záměrně co nejdále od sebe, aby respondent neměl pocit odpovídání na totožné otázky. Pokud na dvě významově stejné otázky odpověděl respondent rozdílně, tak se mu přičetl tzv. bod lži. Maximum bodů, které mohl získat byly 3, přičemž jsem si sám určoval škálu bodového ohodnocení. Záznamy, které získaly 1,4 bodu a více, byly automaticky vyhodnoceny jako nedůvěryhodné a byly vyřazeny z výzkumu.

Celý proces byl automatizován za pomocí funkcí, které jsem realizoval v programu MS Excel. Dotazník obsahoval tři dvojice, u kterých jsem zjišťoval míru lži.

Ukázka dvou otázek, u kterých jsem počítal body lži:

Víš, jak sociální síť nakládá s daty, která na ni uvedeš? (Můžeš zaškrtnout více odpovědí)

- *Ano, četl/a jsem celé zásady používání dat na sociální síti*
- *Ano, četl/a jsem částečně zásady používání dat na sociální síti*
- *Ano, něco málo o tom vím, ale zásady používání dat jsem nikdy nečetl/a*
- *Ano, bavil/a jsem se o tom s kamarády*
- *Ano, četl/a jsem o tom na internetu*
- *Ne, ale zajímalo by mě to*
- *Ne, nezajímá mě to*

Setkal/a jsi se někdy s nějakým prohlášením, jak sociální sítě nakládají s Tvými daty?

- *Ano, ale nevěnoval/a jsem tomu pozornost*
- *Ano a zaujalo mě to*
- *Nikdy jsem tomu nevěnoval/a pozornost*
- *Ne*

Jak můžeme vidět, obě otázky souvisí s tím, zda se někdy respondent setkal s nějakým prohlášením, které je zaměřené na zásady používání dat. Například pokud u první otázky odpoví, že se s prohlášením setkal, a dokonce četl celé zásady používá dat a u druhé otázky odpoví, že se s prohlášením nikdy nesetkal, je zřejmé, že neodpovídá podle pravdy. V tomto případě mu bude přičten bod lži. To samé platí naopak. Je zde několik kombinací odpovědí, které se kontrolují. Jedná se vždy o sadu podmínek, které otázky kontrolují.

Ukázky funkcí pro kontrolu pravdivosti odpovědi:

=KDYŽ(A(Q2=1;AL2=3);1;KDYŽ(A(Q2=1;AL2=1);0,6;KDYŽ(A(R2=1;AL2=3);1;KDYŽ(A(U2=1;AL2=3);0,8;KDYŽ(A(Q2=1;AL2=4);1;KDYŽ(A(R2=1;AL2=4);1;KDYŽ(A(W2=1;AL2=2);1;0)))))))

=KDYŽ(A(AJ2=1;COUNTIF(Y2:AE2;1)>6);1;KDYŽ(A(AJ2=1;COUNTIF(Y2:AE2;1)>5);0,8;KDYŽ(A(AJ2=1;COUNTIF(Y2:AE2;1)>4);0,6;KDYŽ(A(AJ2=1;COUNTIF(Y2:AE2;1)>3);0,4;KDYŽ(A(AJ2=1;COUNTIF(Y2:AE2;1)>2);0,2;KDYŽ(A(AJ2=5;COUNTIF(Y2:AE2;1)<2);1;KDYŽ(A(AJ2=5;COUNTIF(Y2:AE2;1)<3);0,8;KDYŽ(A(AJ2=5;COUNTIF(Y2:AE2;1)<4);0,6;KDYŽ(A(AJ2=5;COUNTIF(Y2:AE2;1)<5);0,4;KDYŽ(A(AJ2=5;COUNTIF(Y2:AE2;1)<6);0,2;0)))))))))

5.4 Sběr dat

Dotazník byl dostupný jak v papírové, tak elektronické podobě, přičemž oba uvedené způsoby obsahovaly totožné otázky a odpovědi. Důvodem realizace dvou podob dotazníků byl fakt, že každá škola preferovala jiný způsob vyplňování. Papírovou podobu jsem realizoval za pomocí MS Word 2016 a elektronickou v Google formulářích. Elektronický způsob vyplňování obsahoval mimo jiné větvení, které jsem využil na začátku dotazníku, kde jsem vyfiltroval respondenty na ty, kteří využívají sociální sítě, a kteří ne. Pro mě byl důležitý vzorek, který využívá sociální sítě, tudíž pro ty, co sociální sítě nevyužívají, byl dotazník ukončen. V elektronické podobě dotazníku jsem využil povinné otázky, díky kterým jsem zajistil úplnost odpovědí. Data z dotazníku se uložila až tehdy, pokud respondent došel na konec dotazníku a potvrdil stisknutím tlačítka své odpovědi. Pokud tedy respondent nedošel na konec dotazníku, tak jeho odpovědi nebyly uloženy.

5.5 Statistická metoda Chí–kvadrát test - test nezávislosti

V rámci analýzy dat a vyhodnocení závislostí mezi veličinami jsem využil statistické metody Chí–kvadrát test - test nezávislosti.

Chí–kvadrát test je nejpoužívanějším testem nezávislosti v kontingenčí tabulce. Test je založen na srovnání pozorovaných a očekávaných četností, které si kategorizujeme do kontingenční tabulky. Při výpočtu si stanovujeme nulovou a alternativní hypotézu, přičemž vycházíme z předpokladu, že platí nulová hypotéza. Nulová hypotéza nepředpokládá žádnou závislost mezi zkoumanými veličinami. Velikost rozdílů určujeme podle testové statistiky X^2. Při testování hypotézy si volíme hladinu významnosti, na které chceme testovat. Obvykle se volí hodnoty $\alpha = 0{,}05$ nebo $\alpha = 0{,}02$, což je pravděpodobnost, že zamítneme nulovou hypotézu. Následně se vypočítá hodnota testovacího kritéria p-value, kterou porovnáme s hladinou významnosti. Pokud je p-value menší než hladina významnosti, tak nulovou hypotézu zamítáme a přijímáme alternativní. V tomto případě prokazujeme závislost [57].

Předpokladem korektního použití tohoto testu je skutečnost, že alespoň 80 % buněk v kontingenčí tabulce má očekávanou četnost větší než 5 a zároveň všechny buňky tabulky mají očekávanou četnost větší než 0 [58].

6 Výsledky výzkumu

V této kapitole jsou prezentovány samotné výsledky výzkumu. Výsledky jsou rozčleněny do podkapitol, přičemž podkapitola 6.1 a její podkapitoly jsou zaměřeny na výsledky z testování hypotéz, které jsou členěny do logických souvislostí. Podkapitola 6.2 a její podkapitoly popisují výsledky procentuálního zastoupení v dané oblasti.

6.1 Relační výsledky

V rámci hledání závislostí mezi veličinami jsem testoval 19 hypotéz, přičemž jsem se zaměřil na různé faktory. Především mě zajímalo, jakou roli mají osobnostní faktory jako je pohlaví, věk, místo bydliště nebo počet obyvatel v místě bydliště na chování při sdílení osobních dat a informací a při nastavení soukromí. Zaměřil jsem se také na to, zda znalost zásad používání dat ovlivňuje chování při sdílení informací nebo při nastavení soukromí a zda je sdílení informací a nastavení soukromí závislé na znalostech rizik spojených se sdílením dat.

6.1.1 Vliv věku na chování

Ověřme si platnost nulové hypotézy H_{01} vzhledem k alternativní $H_{A1.}$

- H_{01}: Mezi znalostí nastavení zabezpečení a soukromí účtu na sociální síti a věkem neexistuje závislost.
- H_{A1}: Mezi znalostí nastavení zabezpečení a soukromí účtu na sociální síti a věkem existuje závislost.

Stanovil jsem si hladinu významnosti $\alpha = 0{,}05$, na které hypotézu testuji. Rozčlenil jsem si respondenty na ty, kteří si umí nastavit zabezpečení a soukromí účtu a na ty, kteří ne. Dále jsem si respondenty rozčlenil podle věku. Vytvořil jsem si kontingenční tabulku s četnostmi a vypočítal testovací kritérium X^2. Vypočítal jsem si hodnotu p-value = 0,238077. Tato hodnota je větší než hladina významnosti, a proto nezamítáme nulovou hypotézu – závislost nebyla prokázána.

Mezi znalostí nastavení zabezpečení a soukromí účtu na sociální síti a věkem neexistuje závislost.

Ověřme si platnost nulové hypotézy H_{04} vzhledem k alternativní H_{A4}.

- H_{04}: Mezi sdílením osobních informací a věkem neexistuje závislost.
- H_{A4}: Mezi sdílením osobních informací a věkem existuje závislost.

Stanovil jsem si hladinu významnosti $\alpha = 0{,}05$, na které hypotézu testuji. Rozčlenil jsem si respondenty na ty, kteří sdílí osobní informace (jméno, příjmení, věk, bydliště, telefonní číslo aj.) a na ty, kteří nesdílí osobní informace. Dále jsem si rozčlenil respondenty podle věku. Vytvořil jsem si kontingenční tabulku s četnostmi a vypočítal testovací kritérium X^2. Vypočítal jsem si hodnotu p-value = 0,047385. Tato hodnota je menší než hladina významnosti, a proto zamítáme nulovou hypotézu a přijímáme alternativní – závislost byla prokázána.

Mezi sdílením osobních informací a věkem existuje závislost.

Ověřme si platnost nulové hypotézy H_{06} vzhledem k alternativní H_{A6}.

- H_{06}: Mezi uvědomováním si rizik spojených se sdílením osobních dat a věkem neexistuje závislost.
- H_{A6}: Mezi uvědomováním si rizik spojených se sdílením osobních dat a věkem existuje závislost.

Stanovil jsem si hladinu významnosti $\alpha = 0{,}05$, na které hypotézu testuji. Rozčlenil jsem respondenty na ty, kteří si uvědomují rizika spojená se sdílením dat a na ty, kteří ne. Dále jsem si rozčlenil respondenty podle věku. Vytvořil jsem si kontingenční tabulku s četnostmi a vypočítal testovací kritérium X^2. Vypočítal jsem si hodnotu p-value = 0,323688433. Tato hodnota je větší než hladina významnosti, a proto nezamítáme nulovou hypotézu – závislost nebyla prokázána.

Mezi uvědomováním si rizik spojených se sdílením osobních dat a věkem neexistuje závislost.

Ověřme si platnost nulové hypotézy H_{09} vzhledem k alternativní H_{A9}.

- H_{09}: Mezi znalostí prohlášení o zásadách používání dat na používané sociální síti a věkem neexistuje závislost.
- H_{A9}: Mezi znalostí prohlášení o zásadách používání dat na používané sociální síti a věkem existuje závislost.

Stanovil jsem si hladinu významnosti $\alpha = 0{,}05$, na které hypotézu testuji. Rozčlenil jsem respondenty na ty, kteří četli prohlášení o zásadách používá dat a na ty, kteří ne. Seskupil jsem respondenty, kteří četli plné zásady používání dat a respondenty, kteří

alespoň částečně četly prohlášení o zásadách používání dat. Dále jsem si rozčlenil respondenty podle věku. Vytvořil jsem si kontingenční tabulku s četnostmi a vypočítal testovací kritérium X^2. Vypočítal jsem si hodnotu p-value = 0,90992217. Tato hodnota je větší než hladina významnosti, a proto nezamítáme nulovou hypotézu – závislost nebyla prokázána.

Mezi znalostí prohlášení o zásadách používání dat na používané sociální síti a věkem neexistuje závislost.

Ověřme si platnost nulové hypotézy H_{016} vzhledem k alternativní H_{A16}:.

- H_{016}: Mezi sdílením svých fotografií a věkem neexistuje závislost.
- H_{A16}: Mezi sdílením svých fotografií a věkem existuje závislost.

Stanovil jsem si hladinu významnosti $\alpha = 0,05$, na které hypotézu testuji. Rozčlenil jsem respondenty na ty, kteří sdílí své fotografie a na ty, kteří ne. Dále jsem si rozčlenil respondenty podle věku. Vytvořil jsem si kontingenční tabulku s četnostmi a vypočítal testovací kritérium X^2. Vypočítal jsem si hodnotu p-value = 0,06232. Tato hodnota je větší než hladina významnosti, a proto nezamítáme nulovou hypotézu – závislost nebyla prokázána.

Mezi sdílením svých fotografií a věkem neexistuje závislost.

6.1.2 Vliv pohlaví na chování

Ověřme si platnost nulové hypotézy H_{03} vzhledem k alternativní $H_{A3.}$

- H_{03}: Mezi sdílením osobních informací a pohlavím neexistuje závislost.
- H_{A3}: Mezi sdílením osobních informací a pohlavím existuje závislost.

Stanovil jsem si hladinu významnosti $\alpha = 0,05$, na které hypotézu testuji. Rozčlenil jsem respondenty na ty, kteří sdílí osobní informace (jméno, příjmení, věk, bydliště, telefonní číslo aj.) a na ty, kteří nesdílí osobní informace. Dále jsem si rozčlenil respondenty podle pohlaví. Vytvořil jsem si kontingenční tabulku s četnostmi a vypočítal testovací kritérium X^2. Vypočítal jsem si hodnotu p-value = 0,350971. Tato hodnota je větší než hladina významnosti, a proto nezamítáme nulovou hypotézu – závislost nebyla prokázána.

Mezi sdílením osobních informací a pohlavím neexistuje závislost.

Ověřme si platnost nulové hypotézy H_{08} vzhledem k alternativní H_{A8}.

- H_{08}: Mezi znalostí prohlášení o zásadách používání dat a pohlavím neexistuje závislost.
- H_{A8}: Mezi znalostí prohlášení o zásadách používání dat a pohlavím existuje závislost.

Stanovil jsem si hladinu významnosti $\alpha = 0{,}05$, na které hypotézu testuji. Rozčlenil jsem respondenty na ty, kteří četli prohlášení o zásadách používá dat a na ty, kteří ne. Seskupil jsem respondenty, kteří četli plné zásady používání dat a respondenty, kteří alespoň částečně četly prohlášení o zásadách používání dat. Dále jsem si rozčlenil respondenty podle pohlaví. Vytvořil jsem si kontingenční tabulku s četnostmi a vypočítal testovací kritérium X^2. Vypočítal jsem si hodnotu p-value = 0,53612821. Tato hodnota je větší než hladina významnosti, a proto nezamítáme nulovou hypotézu – závislost nebyla prokázána.

Mezi znalostí prohlášení o zásadách používání dat a pohlavím neexistuje závislost.

Ověřme si platnost nulové hypotézy H_{010} vzhledem k alternativní H_{A10}.

- H_{010}: Dívky a chlapci se neliší v dovednosti nastavení zabezpečení a soukromí účtu na sociálních sítí.
- H_{A10}: Dívky a chlapci se liší v dovednosti nastavení zabezpečení a soukromí účtu na sociálních sítí.

Stanovil jsem si hladinu významnosti $\alpha = 0{,}05$, na které hypotézu testuji. Rozčlenil jsem si respondenty na ty, kteří si umí nastavit zabezpečení a soukromí účtu a na ty, kteří ne. Dále jsem si respondenty rozčlenil podle pohlaví. Vytvořil jsem si kontingenční tabulku s četnostmi a vypočítal testovací kritérium X^2. Vypočítal jsem si hodnotu p-value = 0,724405024. Tato hodnota je větší než hladina významnosti, a proto nezamítáme nulovou hypotézu – závislost nebyla prokázána.

Dívky a chlapci se neliší v dovednosti nastavení zabezpečení a soukromí účtu na sociálních sítí.

Ověřme si platnost nulové hypotézy H_{015} vzhledem k alternativní H_{A15}.

- H_{015}: Mezi sdílením svých fotografií a pohlavím neexistuje závislost.
- H_{A15}: Mezi sdílením svých fotografií a pohlavím existuje závislost.

Stanovil jsem si hladinu významnosti $\alpha = 0,05$, na které hypotézu testuji. Rozčlenil jsem si respondenty na ty, kteří sdílí své fotografie a na ty, kteří ne. Dále jsem si respondenty rozčlenil podle pohlaví. Vytvořil jsem si kontingenční tabulku s četnostmi a vypočítal testovací kritérium X^2. Vypočítal jsem si hodnotu p-value = $2,91*10^{-8}$. Tato hodnota je menší než hladina významnosti, a proto zamítáme nulovou hypotézu a přijímáme alternativní – závislost byla prokázána.

Mezi sdílením svých fotografií a pohlavím existuje závislost.

Ověřme si platnost nulové hypotézy H_{018} vzhledem k alternativní H_{A18}.

- H_{018}: Mezi sdílením dat a pohlavím neexistuje závislost.
- H_{A18}: Mezi sdílením dat a pohlavím existuje závislost.

Stanovil jsem si hladinu významnosti $\alpha = 0,05$, na které hypotézu testuji. Rozčlenil jsem si respondenty na ty, kteří sdílí data (osobní informace, fotografie, zábavný obsah, obrázky, aj.) a na ty, kteří nesdílejí nic. Dále jsem si respondenty rozčlenil podle pohlaví. Vytvořil jsem si kontingenční tabulku s četnostmi a vypočítal testovací kritérium X^2. Vypočítal jsem si hodnotu p-value = 0,035105584. Tato hodnota je menší než hladina významnosti, a proto zamítáme nulovou hypotézu a přijímáme alternativní – závislost byla prokázána.

Mezi sdílením dat a pohlavím existuje závislost.

Ověřme si platnost nulové hypotézy H_{019} vzhledem k alternativní H_{A19}.

- H_{019}: Mezi nastavením vkládaného obsahu a pohlavím neexistuje závislost.
- H_{A19}: Mezi nastavením vkládaného obsahu a pohlavím existuje závislost.

Stanovil jsem si hladinu významnosti $\alpha = 0,05$, na které hypotézu testuji. Rozčlenil jsem si respondenty na ty, kteří sdílejí obsah veřejně a soukromě. Soukromě jsem si pak rozčlenil na další kategorie. Dále jsem si respondenty rozčlenil podle pohlaví. Vytvořil jsem si kontingenční tabulku s četnostmi a vypočítal testovací kritérium X^2. Vypočítal jsem si hodnotu p-value = 0,0185932. Tato hodnota je menší než hladina významnosti, a proto zamítáme nulovou hypotézu a přijímáme alternativní – závislost byla prokázána.

Mezi nastavením vkládaného obsahu a pohlavím existuje závislost.

6.1.3 Vliv místa bydliště a počtu obyvatel na chování

Ověřme si platnost nulové hypotézy H_{05} vzhledem k alternativní H_{A5}.

- H_{05}: Mezi sdílením osobních informací a počtem obyvatel v místě bydliště neexistuje závislost
- H_{A5}: Mezi sdílením osobních informací a počtem obyvatel v místě bydliště existuje závislost

Stanovil jsem si hladinu významnosti $\alpha = 0{,}05$, na které hypotézu testuji. Rozčlenil jsem si respondenty na ty, kteří sdílí osobní informace (jméno, příjmení, věk, bydliště, telefonní číslo aj.) a na ty, kteří nesdílí. Dále jsem si respondenty rozčlenil podle počtu obyvatel v místě bydliště. Vytvořil jsem si kontingenční tabulku s četnostmi a vypočítal testovací kritérium X^2. Vypočítal jsem si hodnotu p-value = 0,07927. Tato hodnota je větší než hladina významnosti, a proto nezamítáme nulovou hypotézu – závislost nebyla prokázána.

Mezi sdílením osobních informací a počtem obyvatel v místě bydliště neexistuje závislost

Ověřme si platnost nulové hypotézy H_{07} vzhledem k alternativní H_{A7}.

- H_{07}: Mezi uvědomováním si rizik spojených se sdílením osobních dat a místem bydliště neexistuje závislost.
- H_{A7}: Mezi uvědomováním si rizik spojených se sdílením osobních dat a místem bydliště existuje závislost.

Stanovil jsem si hladinu významnosti $\alpha = 0{,}05$, na které hypotézu testuji. Rozčlenil jsem si respondenty na ty, kteří si uvědomují rizika spojená se sdílením dat a na ty, kteří ne. Dále jsem si respondenty rozčlenil podle místa bydliště. Vytvořil jsem si kontingenční tabulku s četnostmi a vypočítal testovací kritérium X^2. Vypočítal jsem si hodnotu p-value = 0,04385438. Tato hodnota je menší než hladina významnosti, a proto zamítáme nulovou hypotézu a přijímáme alternativní – závislost byla prokázána.

Mezi uvědomováním si rizik spojených se sdílením osobních dat a místem bydliště existuje závislost.

Ověřme si platnost nulové hypotézy H_{017} vzhledem k alternativní H_{A17}.

- H_{017}: Mezi nastavením vkládaného obsahu a místem bydliště neexistuje závislost.

- H_{A17}: Mezi nastavením vkládaného obsahu a místem bydliště existuje závislost.

Stanovil jsem si hladinu významnosti $\alpha = 0{,}05$, na které hypotézu testuji. Rozčlenil jsem si respondenty na ty, kteří sdílejí obsah veřejně a soukromě. Soukromě jsem si pak rozčlenil na další kategorie. Dále jsem si respondenty rozčlenil podle místa bydliště. Vytvořil jsem si kontingenční tabulku s četnostmi a vypočítal testovací kritérium X^2. Vypočítal jsem si hodnotu p-value = 0,09942. Tato hodnota je větší než hladina významnosti, a proto nezamítáme nulovou hypotézu – závislost nebyla prokázána.

Mezi nastavením vkládaného obsahu a místem bydliště neexistuje závislost.

6.1.4 Vliv nastavení soukromí na chování

Ověřme si platnost nulové hypotézy H_{011} vzhledem k alternativní H_{A11}.

- H_{011}: Mezi nastavením vkládaného obsahu a sdílením osobních informací neexistuje závislost.
- H_{A11}: Mezi nastavením vkládaného obsahu a sdílením osobních informací existuje závislost.

Stanovil jsem si hladinu významnosti $\alpha = 0{,}05$, na které hypotézu testuji. Rozčlenil jsem si respondenty na ty, kteří sdílí osobní informace (jméno, příjmení, věk, bydliště, telefonní číslo aj.) a na ty, kteří nesdílí osobní informace. Dále jsem si respondenty rozčlenil na ty, kteří sdílejí obsah veřejně a soukromě. Soukromě jsem si pak rozčlenil na další kategorie. Vytvořil jsem si kontingenční tabulku s četnostmi a vypočítal testovací kritérium X^2. Vypočítal jsem si hodnotu p-value = 0,0323. Tato hodnota je menší než hladina významnosti, a proto zamítáme nulovou hypotézu a přijímáme alternativní – závislost byla prokázána.

Mezi nastavením vkládaného obsahu a sdílením osobních informací existuje závislost.

Ověřme si platnost nulové hypotézy H_{014} vzhledem k alternativní H_{A14}.

- H_{014}: Mezi sdílením dat a nastavením vkládaného obsahu neexistuje závislost.
- H_{A14}: Mezi sdílením dat a nastavením vkládaného obsahu existuje závislost.

Stanovil jsem si hladinu významnosti $\alpha = 0{,}05$, na které hypotézu testuji. Rozčlenil jsem si respondenty na ty, kteří sdílí data (osobní informace, fotografie, zábavný obsah, obrázky, aj.) a na ty, kteří nesdílejí nic. Dále jsem si respondenty rozčlenil na ty, kteří sdílejí obsah veřejně a soukromě. Soukromě jsem si pak rozčlenil na další kate-

gorie. Vytvořil jsem si kontingenční tabulku s četnostmi a vypočítal testovací kritérium X^2. Vypočítal jsem si hodnotu p-value = $1{,}68344*10^{-5}$. Tato hodnota je menší než hladina významnosti, a proto zamítáme nulovou hypotézu a přijímáme alternativní – závislost byla prokázána.

Mezi sdílením dat a nastavením vkládaného obsahu existuje závislost.

6.1.5 Vliv znalostí a zkušeností na chování

Ověřme si platnost nulové hypotézy H_{02} vzhledem k alternativní H_{A2}.

- H_{02}: Mezi zkušeností se zneužitím dat a znalostí prohlášení o ochraně soukromí na používané sociální síti neexistuje závislost.
- H_{A2}: Mezi zkušeností se zneužitím dat a znalostí prohlášení o ochraně soukromí na používané sociální síti existuje závislost.

Stanovil jsem si hladinu významnosti $\alpha = 0{,}05$, na které hypotézu testuji. Rozčlenil jsem si respondenty na ty, kteří mají osobní zkušenosti se zneužitím dat a na ty, kteří je nemají. Dále jsem si respondenty rozčlenil na ty, kteří projevili znalosti v prohlášení o ochraně soukromí a na ty, kteří ne. Vytvořil jsem si kontingenční tabulku s četnostmi. Získané četnosti měli velmi nízkou hodnotu, a proto jsem nemohl využít Chí-kvadrát test a ani jiný z testů.

Hypotézu nebylo možné ověřit.

Ověřme si platnost nulové hypotézy H_{012} vzhledem k alternativní H_{A12}.

- H_{012}: Mezi znalostí nastavení zabezpečení soukromí svého účtu a sdílením osobních informací neexistuje závislost.
- H_{A12}: Mezi znalostí nastavení zabezpečení soukromí svého účtu a sdílením osobních informací existuje závislost.

Stanovil jsem si hladinu významnosti $\alpha = 0{,}05$, na které hypotézu testuji. Rozčlenil jsem si respondenty na ty, kteří znají nastavení zabezpečení a soukromí svého účtu. Dále jsem si respondenty rozčlenil na ty, kteří sdílí data (osobní informace, fotografie, zábavný obsah, obrázky, aj.) a na ty, kteří nesdílejí nic. Vytvořil jsem si kontingenční tabulku s četnostmi a vypočítal testovací kritérium X^2. Vypočítal jsem si hodnotu p-value = 0,544793122. Tato hodnota je větší než hladina významnosti, a proto nezamítáme nulovou hypotézu – závislost nebyla prokázána.

Mezi znalostí nastavení zabezpečení soukromí svého účtu a sdílením osobních informací neexistuje závislost.

Ověřme si platnost nulové hypotézy H_{013} vzhledem k alternativní H_{A13}.

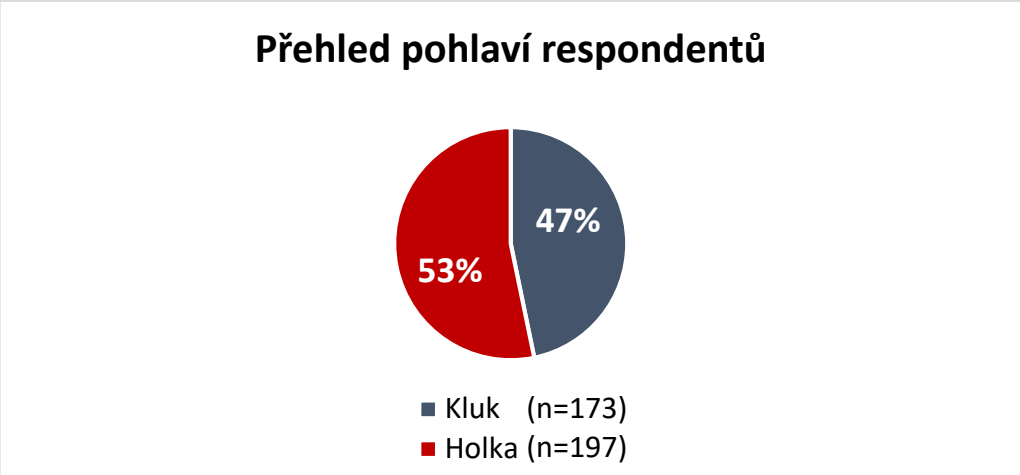
- H_{013}: Mezi sdílením svých fotografií a uvědomováním si rizik spojených se sdílením osobních dat neexistuje závislost.
- H_{A13}: Mezi sdílením svých fotografií a uvědomováním si rizik spojených se sdílením osobních dat existuje závislost.

Stanovil jsem si hladinu významnosti $\alpha = 0{,}05$, na které hypotézu testuji. Rozčlenil jsem si respondenty na ty, kteří si uvědomují rizika spojená při sdílení dat a na ty, kteří ne. Dále jsem si respondenty rozčlenil na ty, kteří sdílí své vlastní fotografie a na ty, kteří ne. Vytvořil jsem si kontingenční tabulku s četnostmi a vypočítal testovací kritérium X^2. Vypočítal jsem si hodnotu p-value = 0,6429423. Tato hodnota je větší než hladina významnosti, a proto nezamítáme nulovou hypotézu – závislost nebyla prokázána.

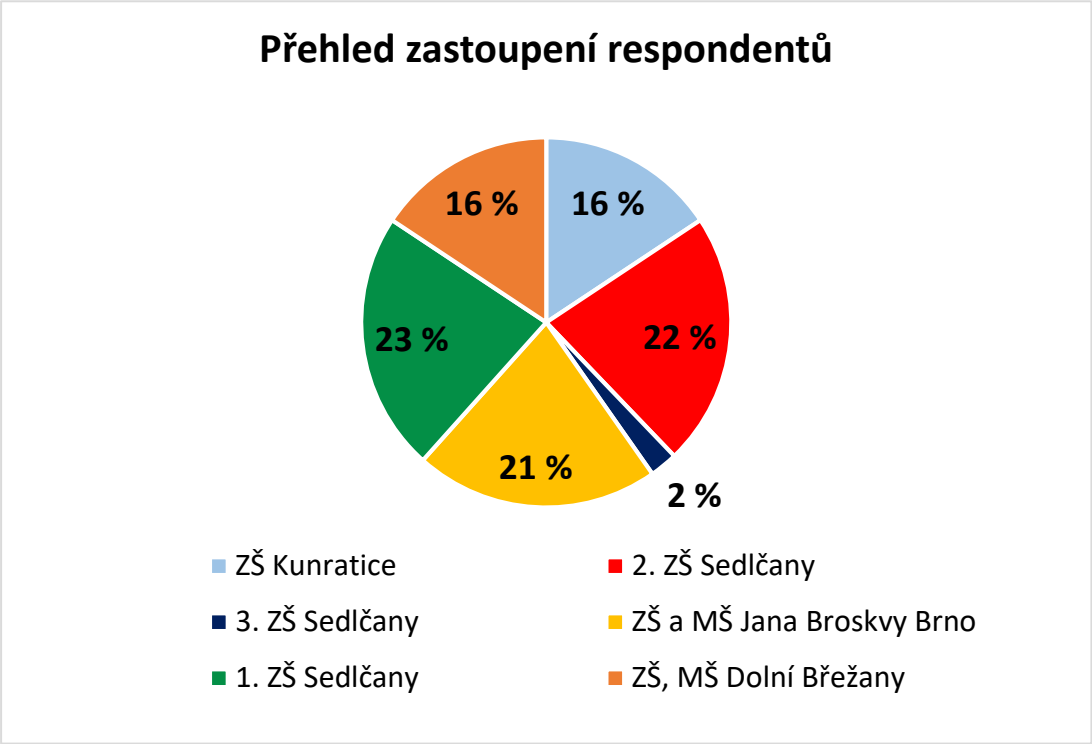
Mezi sdílením svých fotografií a uvědomováním si rizik spojených se sdílením osobních dat neexistuje závislost.

6.2 Deskriptivní výsledky

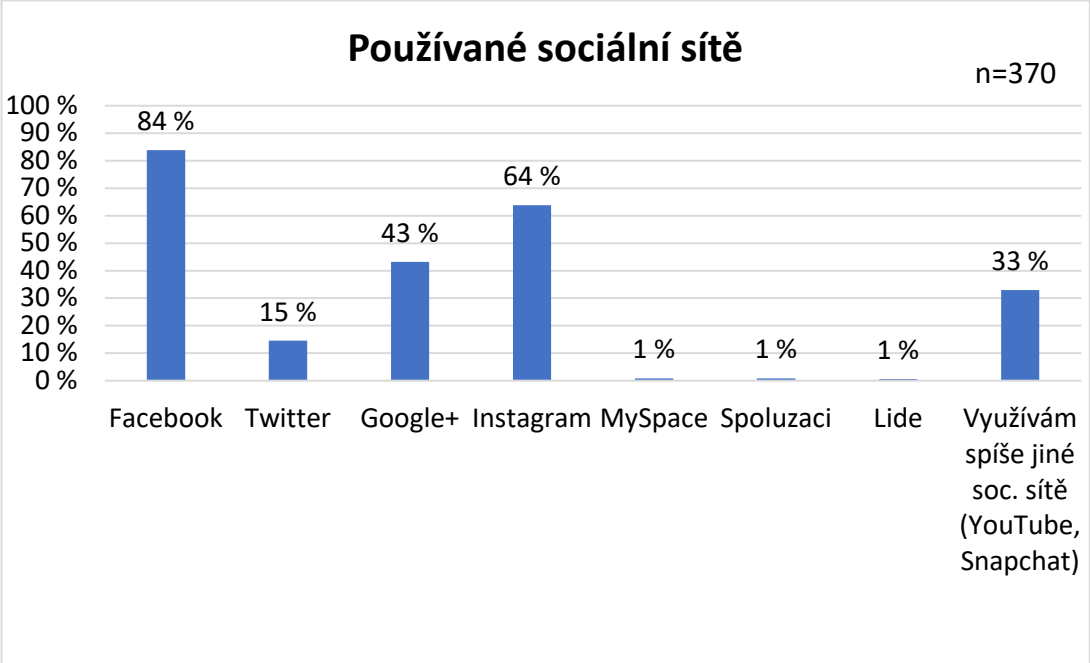
V této části se zaměřím především na procentuální vyjádření výsledků výzkumu. Zaměřme se na úvodní informace. Jak jsem již zmiňoval, výzkumu se zúčastnilo 404 respondentů. Celkem bylo vyřazeno 34 záznamů z různých důvodů. 21 respondentů nepoužívá sociální sítě, 6 dotazníků bylo špatně vyplněných a 7 dotazníků bylo označeno jako nedůvěryhodné. Dotazníky byly rozdány do 6 škol, přičemž pohlaví respondentů bylo přibližně ve stejném poměru.



Obr. 1: Zastoupení respondentů z hlediska pohlaví



Obr. 2: Zastoupení respondentů z hlediska navštěvované školy

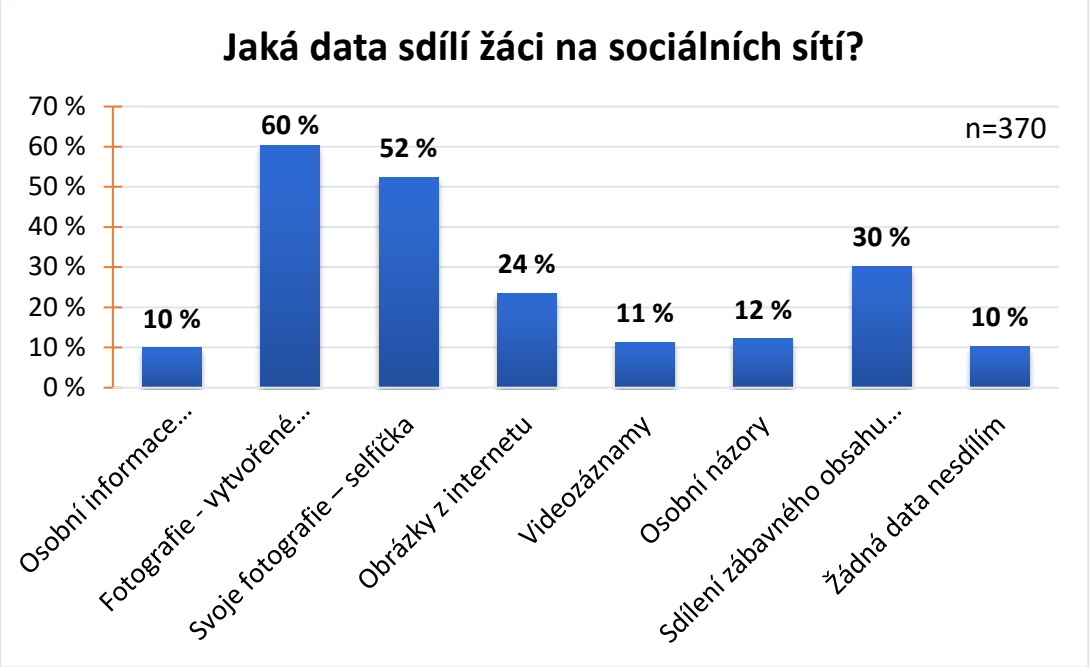


Obr. 3: Používané sociální sítě

Z grafu můžeme vidět, že většina respondentů používá sociální síť Facebook (84 %), kterou respondenti nejčastěji uváděli také jako jejich nejoblíbenější. Druhou nejpoužívanější sociální sítí je Instagram (64 %) a třetí Google+ (43 %).

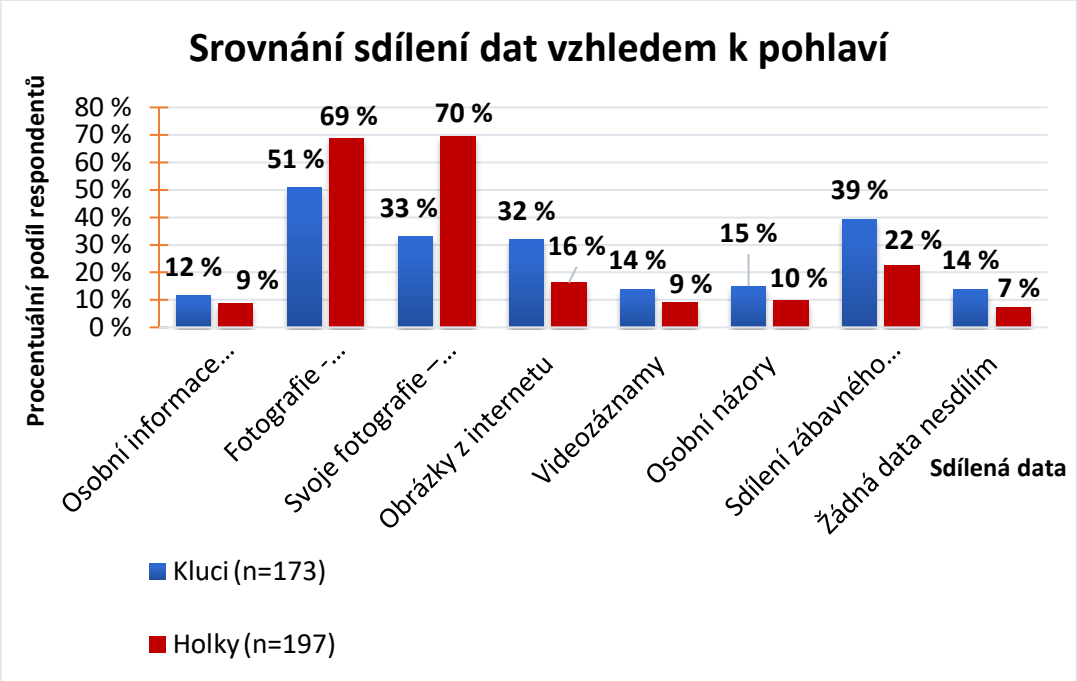
33 % respondentů uvedlo, že využívá jiné sociální sítě jako například YouTube a Snapchat. 15 % respondentů využívá Twitter a pouze 1 % respondentů využívá MySpace. Nejznámější české sociální sítě využívá jen 1 % respondentů, a i zde se potvrzuje, že v dnešní době se již české sociální sítě příliš nevyužívají.

6.2.1 Chování v oblasti sdílení dat



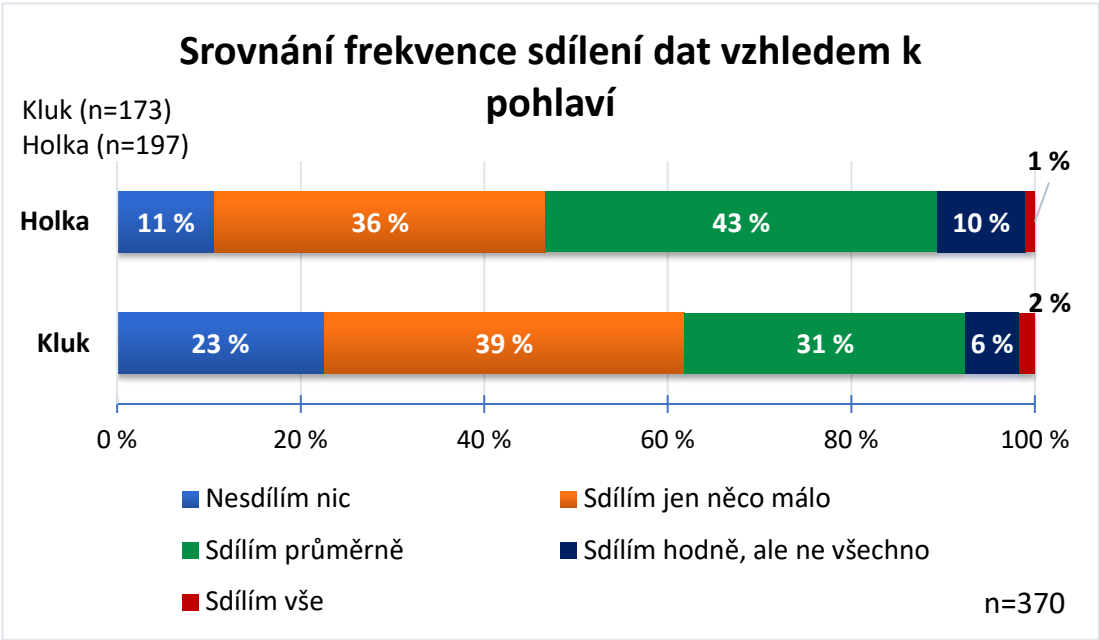
Obr. 4: Přehled dat, které žáci sdílí na sociálních sítí

Pokud se zaměříme na typ dat, který žáci základních škol sdílejí mezi ostatní uživatele na sociálních sítí, tak největší část respondentů sdílí především své fotografie. V 60 % se pak jedná o fotografie, které respondenti sami pořídili, jako například fotografie z dovolené, různých zážitků nebo každodenního života. 52 % respondentů uvádí, že sdílí tzv. selfíčka, které se staly v posledních několika letech fenoménem. Další oblíbený obsah, kteří respondenti sdílí je zábavný obsah (30 %), do kterého patří zábavná videa, zábavné obrázky a vtipy. S tím souvisí i sdílení videozáznamů (11 %) a obrázků (24 %) z internetu. 10 % respondentů uvedlo, že sdílí osobní informace jako bydliště, věk, telefonní číslo a název školy. Právě tato skupina respondentů je nejrizikovější, vzhledem k rizikám, které sdílení osobních informací přináší. Stejné procento respondentů uvádí, že nesdílí žádná data.



Obr. 5: Srovnání sdílení dat vzhledem k pohlaví

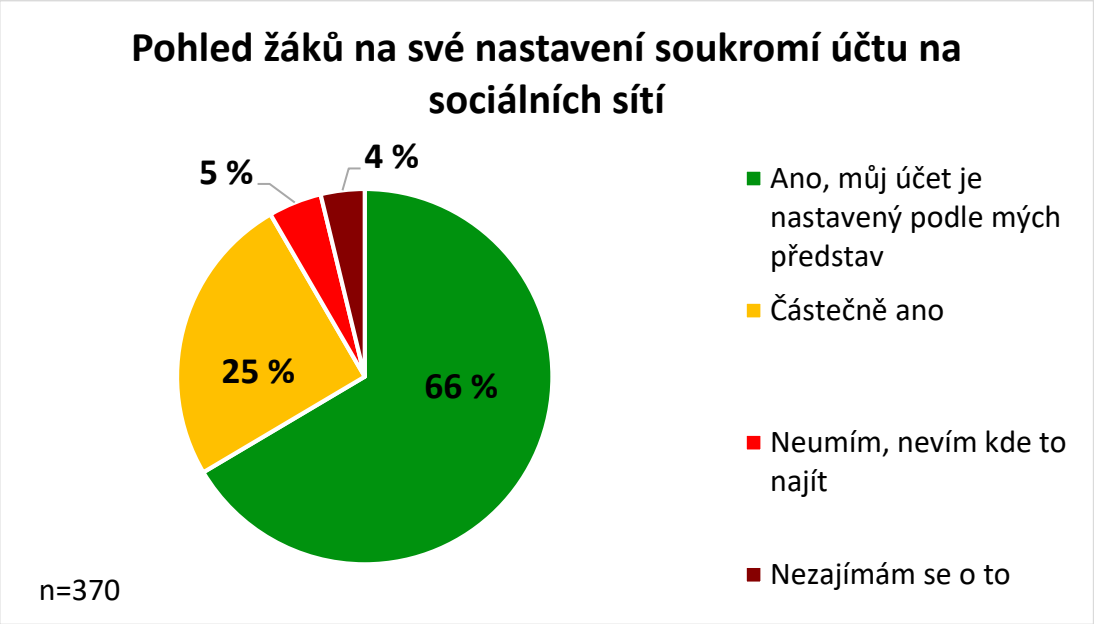
Pokud bychom porovnali sdílení dat vzhledem k pohlaví tak vidíme určité rozdíly u několika kategorií. Objevuje se zde velký rozdíl (37%) převážně ve sdílení svých tzv. selfie fotografií, kde se respondenti ženského pohlaví jeví mnohem aktivněji. Aktivněji se také jeví při sdílení fotografií každodenních. Naopak chlapci dávají přednost spíše sdílení obrázků a zábavného obsahu jako je herní obsah, zábavné obrázky, videozáznamy, vtipy aj. Sdílení osobních informací se v nepatrné míře ukázalo u chlapců ve větším množství než u opačného pohlaví.



Obr. 6: Srovnání frekvence sdílení dat vzhledem k pohlaví

Zajímala mě frekvence sdílení dat u respondentů vzhledem k pohlaví. Jak můžeme vidět, většina respondentů se ohodnotila jako průměrně sdílející až sdílející spíše méně než více. Chlapci pak ve 23 % volili možnost nesdílím nic, přičemž dívky pouze 11 %. Tato zjištění jsou úměrná zjištěním v předchozím grafu, kde chlapci skutečně projevili trochu větší zájem o nesdílení informací. Sdílím vše uvedla malá část respondentů.

6.2.2 Chování v oblasti soukromí

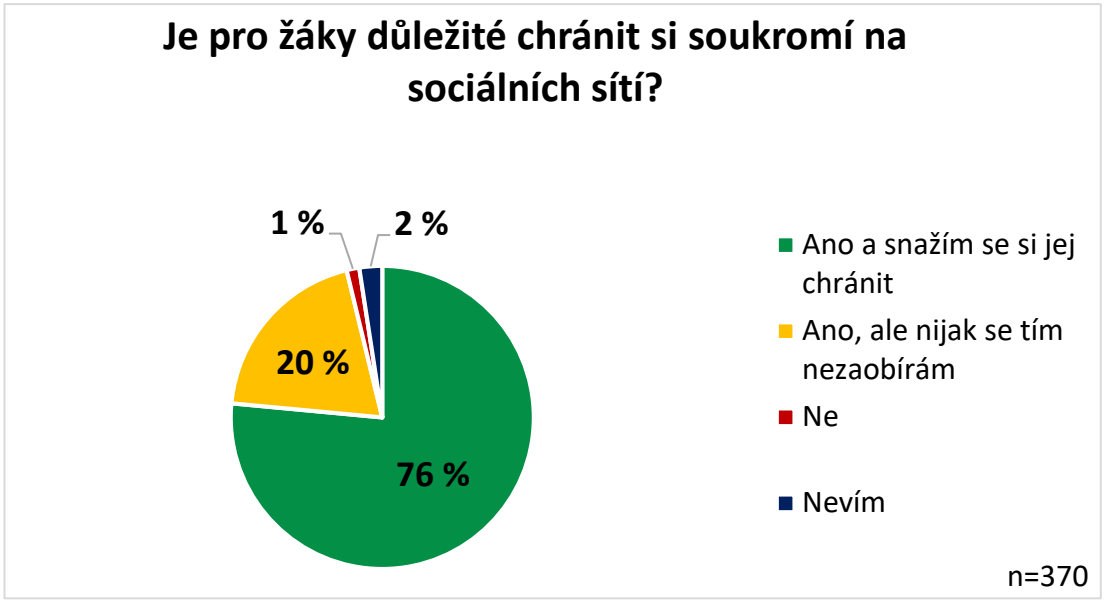


Obr. 7: Pohled na nastavení soukromí svého účtu

Zeptal jsem se respondentů, zda jsou schopni najít si nastavení soukromí a zabezpečení účtu na používané sociální síti a zda jim nedělá problém plně tento nástroj využít. 66 % respondentů uvedlo, že si umí nastavit soukromí a zabezpečení svého účtu a to tak, jak si oni sami představují. Z toho se můžeme domnívat, že tento nástroj dokáží plně využívat. 25 % respondentů uvedlo, že si umí nastavit soukromí, ale mají jisté mezery v dovednostech nastavení účtů. Celkem 9 % respondentů uvedlo, že si neumí nastavit soukromí, přičemž 5 % z nich odpovědělo, že neví, kde tato nastavení hledat a 4 % respondentů neprojevuje zájem o nastavení soukromí. Těchto 9 % můžeme zařadit do rizikové skupiny uživatelů sociálních sítí.

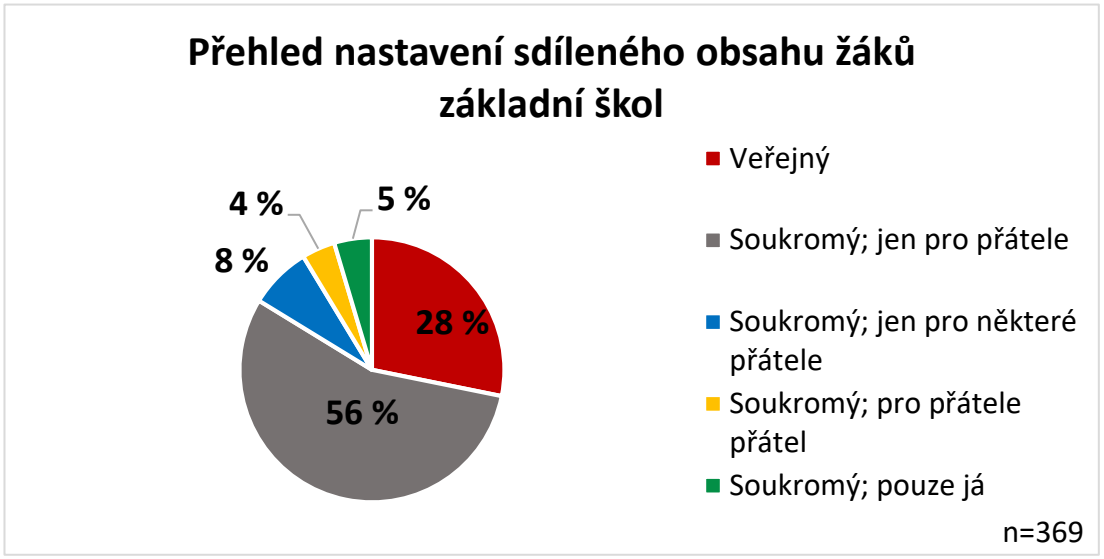
Zajímala mě skupina těchto 9 % respondentů. Chtěl jsem zjistit, zda skupina, která projevuje neznalost a nezájem v nastavení soukromí sdílí osobní informace, protože právě zde může docházet k větší pravděpodobnosti zneužití informací. Nicméně

v tomto případě pouze 3 % respondentů sdílí osobní informace a zároveň projevují neznalost v nastavení soukromí, tudíž zde nehrozí taková rizika.



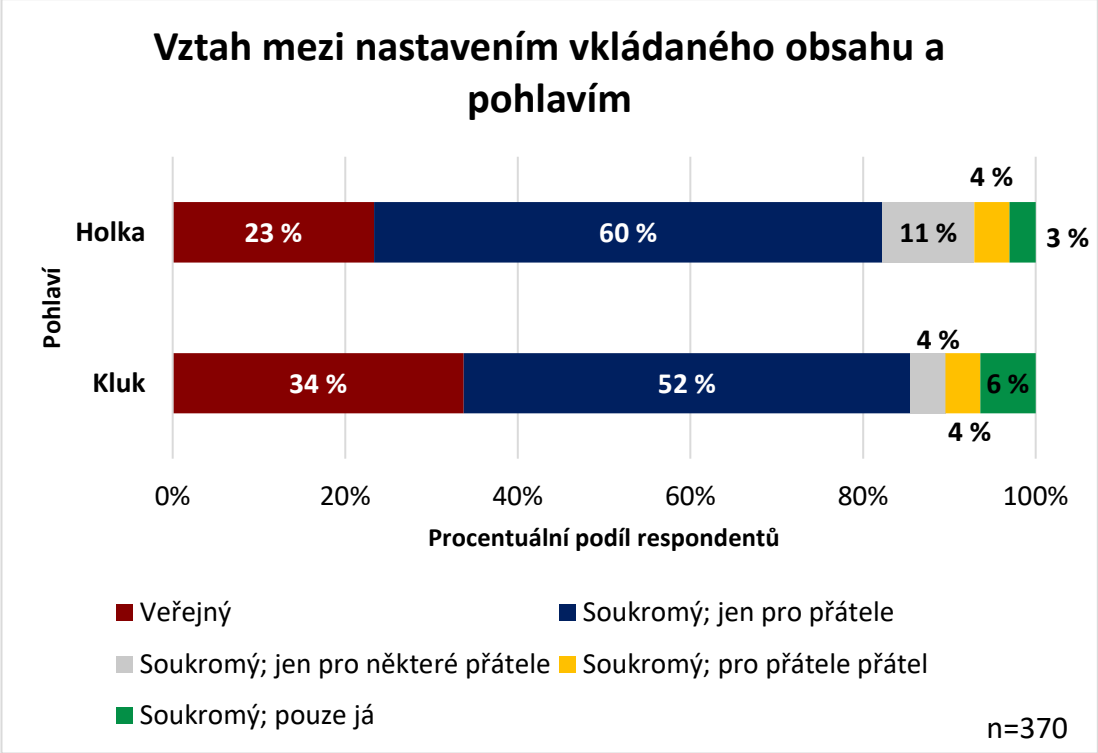
Obr. 8: Pohled na ochranu soukromí na sociálních sítí

Celkem 96 % respondentů uvedlo, že je pro ně důležité chránit si soukromí na sociálních sítí, z toho 76 % uvedlo, že se tím dokonce i více zaobírají a pro 20 % respondentů je soukromí důležité, avšak více informací si o tom nezjišťují. Takto velké procentuální zastoupení se ztotožňuje i s aktuálním již zmiňovaným výzkumem od Intel [43], kde se uvádí, že 96 českých občanů ze 100 lpí na ochranu soukromí na sociálních sítí a jsou si vědomi rizik spojených s užíváním. Česká republika patří v Evropě mezi země, kteří oblast ochrany soukromí velmi zajímá, a to se potvrzuje i v mém výzkumu mezi mladistvými.



Obr. 9: Přehled nastavení soukromí při sdílení obsahu

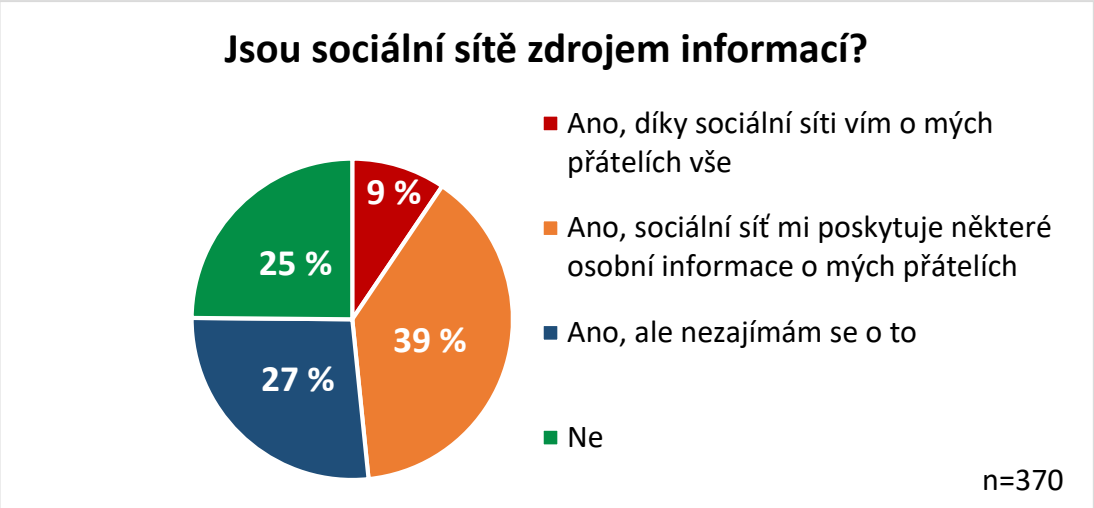
Z grafu je vidět, že 28 % respondentů sdílí svůj obsah veřejně a 72 % pak soukromě s různými omezeními. Nepříliš vhodné je nastavení soukromý, pro přátele přátel, protože sdílená data se mohou jednoduše dostat k lidem z druhého konce světa, které neznáme. Nejpoužívanější nastavení se ukázalo jako nastavení viditelnosti obsahu pouze pro přátele, odpovědělo tak 56 % respondentů.



Obr. 10: Nastavení soukromí vzhledem k pohlaví

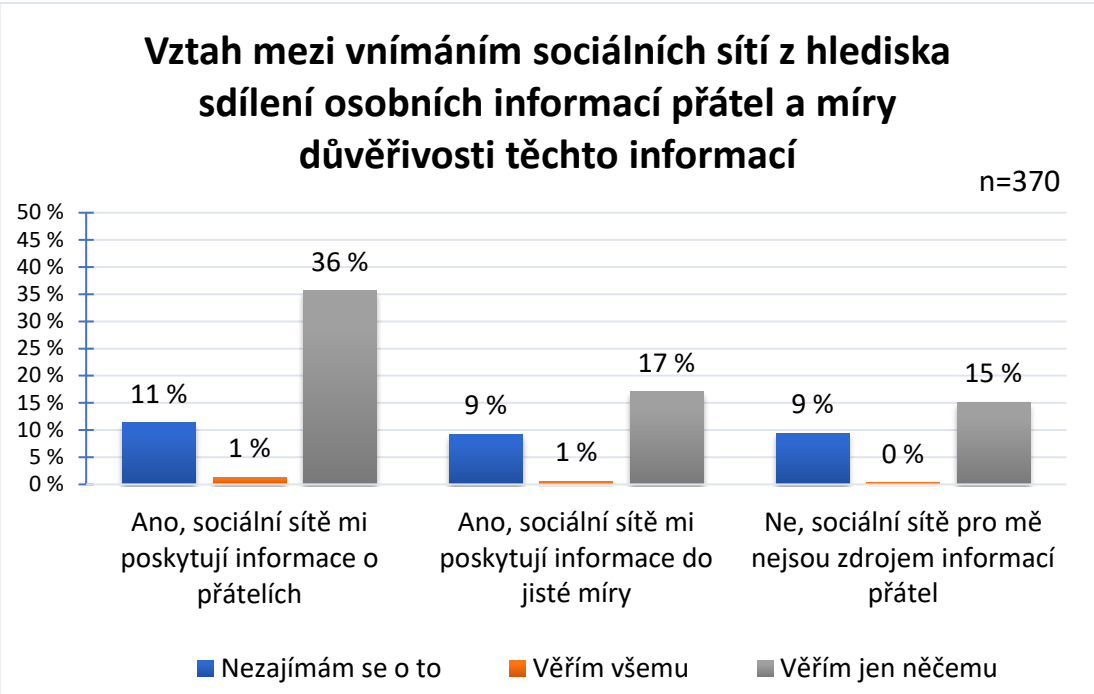
Pokud toto nastavení porovnáme vzhledem k pohlaví, tak největší rozdíl vidíme u veřejného nastavení sdílení obsahu. Chlapci se zde projevili jako ti, kteří sdílejí obsah veřejně více než dívky. Patrně za to může i fakt, že sdílí převážně zábavný obsah, což jsme si dokázali, a jsou si vědomi toho, že zde nehrozí žádná rizika. Může zde hrát roli také zmiňovaná neznalost nastavení soukromí a s tím spojená neznalost základního nastavení.

6.2.3 Chování v oblasti vnímání informací



Obr. 11: Pohled na sociální sítě jako na zdroj informací

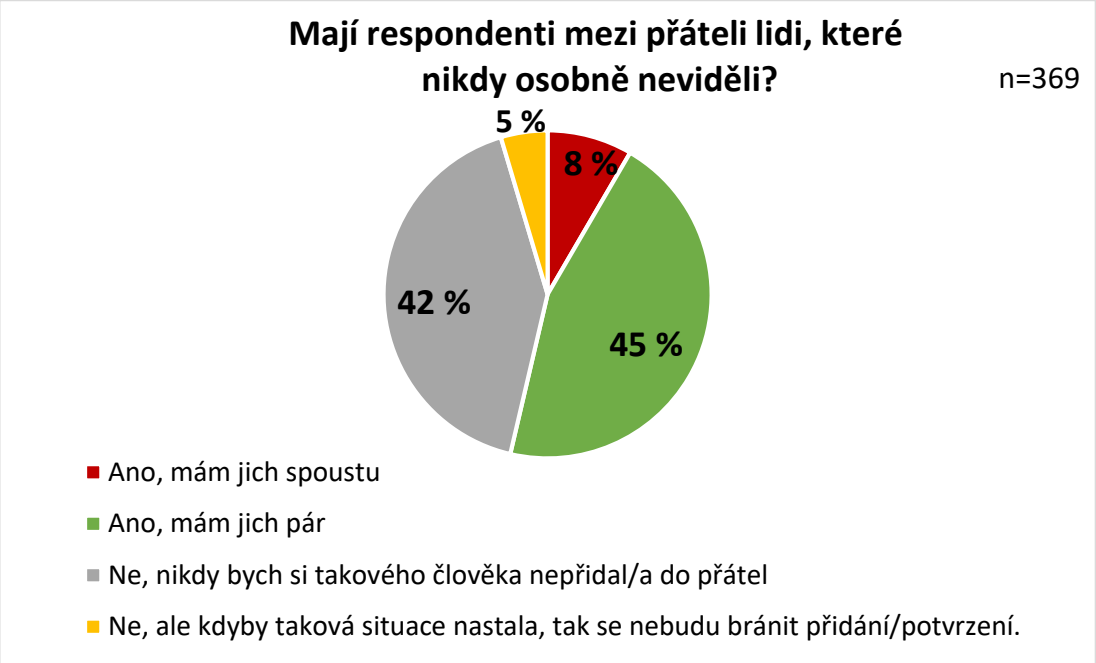
Zajímalo mě, jak respondenti hledí na sociální sítě z hlediska zdroje informací, kterých je na sociálních sítí spousta, a to především u svých přátel. Celkem 73 % respondentů uvedlo, že sociální sítě berou jako zdroj osobních informací o svých přátelích. Jaký konkrétní typ osobních informací respondenti nacházejí u svých přátel jsem však z výzkumu nezjistil. 25 % respondentů uvedlo, že sociální sítě nevnímají jako zdroj informací o svých přátelích. 27 % respondentů pak přiznává, že osobní informace přátel se na sociálních sítí objevují, avšak nijak se o to nezajímají.



Obr. 12: Míra důvěřivosti sdílených informací

Z grafu můžeme vidět, že respondenti, kteří přiznali, že sociální sítě jsou zdrojem osobních informací jejich přátel, tak převážně uváděli, že těmto informacím věří, avšak pouze do jisté míry. Všemu věří pouze 1 % respondentů. Zde se respondenti ukázali jako rozumní uživatelé sociálních sítí. Můžeme se domnívat, že mají přehled o problematice míře důvěryhodnosti uživatelů a sdílených dat, a proto se jevili spíše zdrženlivěji v této oblasti.

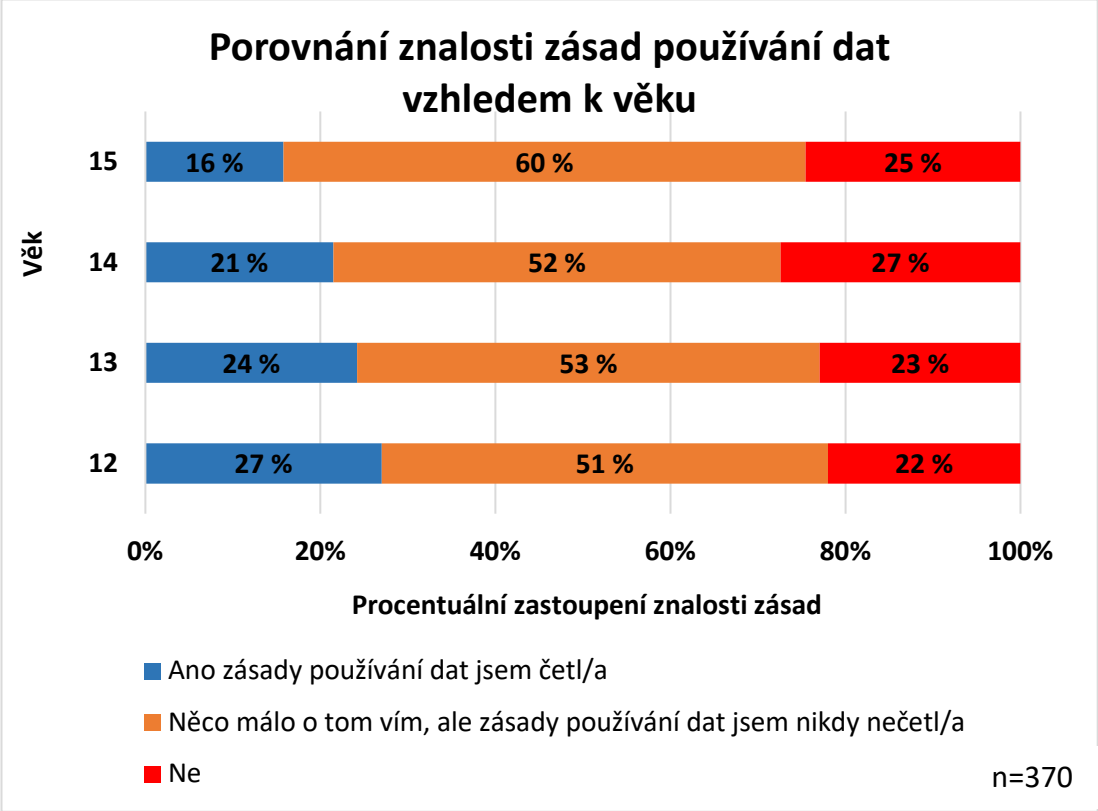
6.2.4 Chování v oblasti výběru kontaktů



Obr. 13: Pohled na neznámé kontakty na sociálních sítí

Celých 53 % respondentů uvedlo, že na sociálních sítí mají ve svých přátelích a sledujících lidi, které nikdy osobně neviděli. 8 % z nic pak uvedlo, že má takových kontaktů spoustu. Dalších 5 % pak uvedlo, že takové kontakty nemají, avšak by se nebránili tomu je mít. Myslím si, že je to velmi vysoké číslo, a právě přidávání si neznámých lidí a udržování kontaktů s nimi vede k většímu riziku kyberšikany a vydírání. Tyto výsledky se shodují i s jinými zprávami [59], kde se uvádí, že přibližně 54 % dětí ve věku 11-17 let jsou na sociálních sítí v kontaktu s neznámými lidmi, přičemž se zde u poloviny z nich objevila kyberšikana.

6.2.5 Chování v oblasti znalosti zásad používání dat



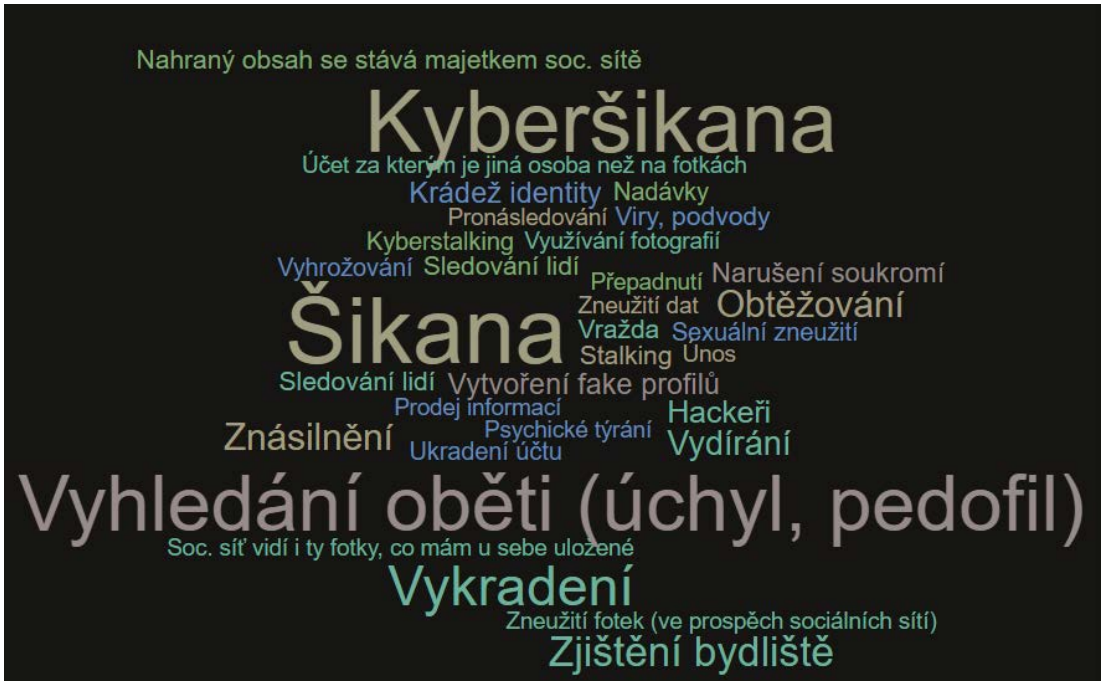
Obr. 14: Porovnání přehledu znalostí zásad

Můžeme vidět, že velká část respondentů uvedla, že zásady používání dat nikdy nečetla, avšak o této problematice něco ví. Respondenti zde nejčastěji uváděli, že četli různé články na internetu nebo se o tom bavili s kamarády. Do jaké míry jsou znalí v této oblasti, ačkoliv nečetli zásady používání dat, jsem z výzkumu nezjistil. Přibližně jeden ze čtyř respondentů pak zásady používání dat četl alespoň částečně. Zajímavé je zde srovnání z hlediska věku. Mladší respondenti jeví do jisté míry větší zájem o znalost zásad používání dat než starší jedinci. Vidíme zde rostoucí tendenci.

Pokud se zaměříme pouze na respondenty, kteří uvedli, že se s prohlášením o zásadách používání dat nikdy nesetkali a ani o tom nic nevědí (červeně označení), pak 60 % z nich uvádí, že by je tato problematika zajímala. 40 % z nich uvedlo, že je to nezajímá.

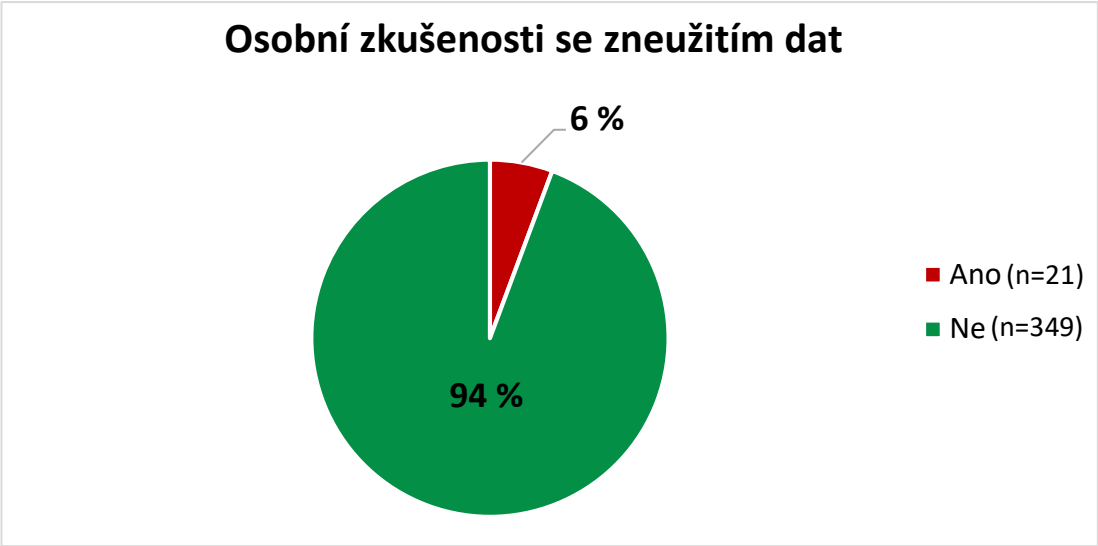
6.2.6 Chování v oblasti znalostí rizik a zkušenosti se zneužitím dat

Zajímalo mě, zda respondenti znají hrozby při sdílení dat na sociálních sítí. V rámci tohoto okruhu jsem se ptal na konkrétní hrozby, které respondenti reprodukovali. Následně jsem tyto hrozby stmelil do kategorií, pro přehlednější prezentaci výsledků. 61 % respondentů odpovědělo a vymyslelo několik zástupců rizik týkajících se sdílení dat. 39 % respondentů neodpovědělo.



Obr. 15: Hrozby při sdílení dat - prezentace znalostí respondentů

Jak můžeme vidět, nejznámějšími hrozby při sdílení dat a osobních informací na sociálních sítí jsou šikana, kyberšikana a riziko vyhledání si oběti kvůli dostupným osobním informacím prezentovaných na sociálních sítí. Často zde jako příklady respondenti uváděli především pedofily aj., kteří mohou zneužít osobní informace. Tyto záznamy měli nejvyšší zjištěnou četnost výskytu. Velmi často se zde objevovali hrozby jako nebezpečí zjištění bydliště a následné vykradení, zneužití dat (především fotografie) a s tím spojené vydírání, nebo obtěžování. Značná část respondentů si je také vědoma rizik spojených s e-bezpečností, kde uváděli, že sociální sítě jsou zdrojem virů a podvodných zpráv. Výhodou prostoru sociálních sítí je rychlé šíření mezi spousty uživatelů, čeho si jsou respondenti vědomi. Objevovali se zde také zajímavé odpovědi, že jakýkoliv sdílený obsah na sociálních sítí se stává majetkem sociální sítě a nevíme, kde naše data skončí. S tím do jisté míry lze souhlasit.



Obr. 16: Procentuální zastoupení osobní zkušenosti se zneužitím dat

Osobní zkušenosti se zneužitím dat má 6 % dotazujících. Záměrně jsem se nepovinnou otázkou ptal na tyto zkušenosti. Respondenti se setkali především se zneužitím fotografií, kde se často zmiňovalo zneužití intimních fotografií. Oběti posílali fotografie důvěřivé osobě, která je následně sdílela dál. Dále také uváděli zkušenosti s vydíráním, obtěžováním nebo zakládáním tzv. „fake“ účtů s jejich osobními informacemi a fotografiemi. V neposlední řadě pak uvádí, že se stali obětí hackerů a s tím spojených virů a podvodných zpráv.

Ukázky odpovědí na nepovinnou otázku zaměřenou na osobní zkušenosti se zneužitím dat:

„Někdo se snažil ze mě vylákat peníze, ale zablokoval jsem ho. Také mám zkušenosti s vyhrožováním.“

„Kamarádka poslala polonahou fotografii klukovi, který ji poslal ostatním a fotku vidělo hodně obcí kolem.“

„Jeden kluk poslal svou intimní fotku holce a ona ji rozeslala skoro všem co mohla až se to dostalo i do školy a k rodičům domů.“

„Ano, přátelé si zakládají fake účty.“

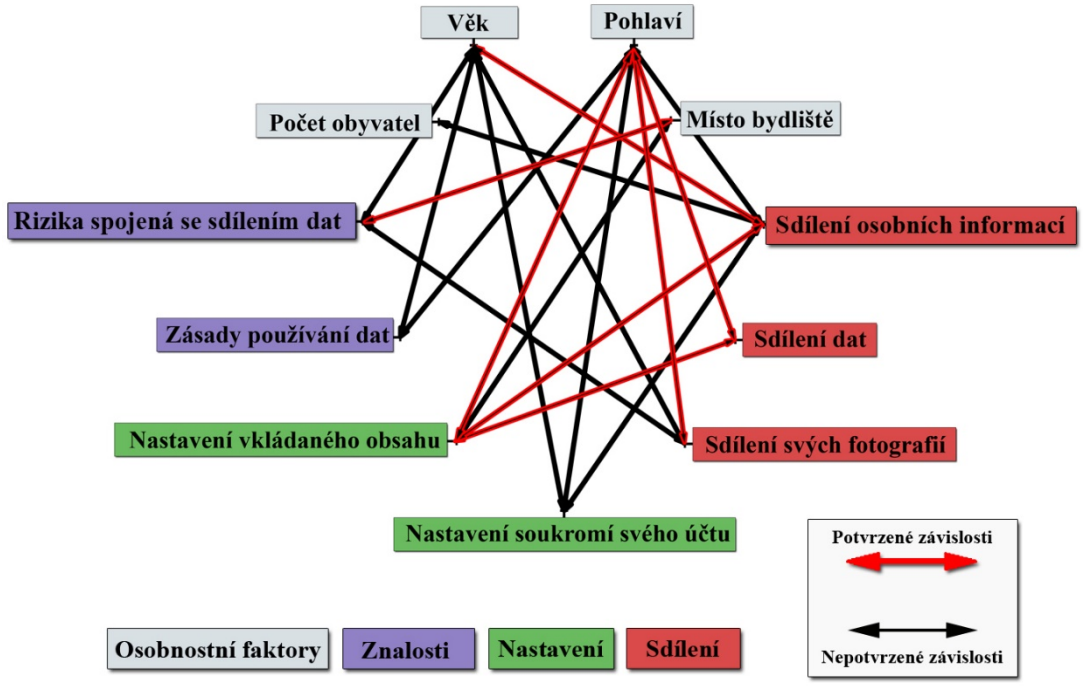
„Jednou se mi někdo cizí dostal na můj účet facebooku a psal tam špatné a nepravdivé informace o mých přátelích a příbuzných mých přátel. Facebookový účet jsem si zrušila.“

„Ano, mou sestru obtěžoval úchyl.“

„Napadení účtu hackerem.“

7 Shrnutí výsledků a diskuze

Podíváme se na shrnutí potvrzených a nepotvrzených závislostí. Pro přehlednost jsem tyto závislosti shrnul do jednoho obrázku a rozčlenil do kategorií.



Obr. 17: Přehled potvrzených a nepotvrzených závislostí

Pohlaví, z osobnostních faktorů, ovlivňuje především sdílení fotografií a sdílení dat (videozáznamy, osobní názory, vtipné obrázky aj.). Pohlaví také hraje roli v nastavení soukromí sdíleného obsahu. Věk ovlivňuje pouze sdílení osobních informací (jméno, příjmení, věk, bydliště, telefonní číslo aj.). Očekával jsem také potvrzení závislosti u sdílení svých fotografií vzhledem k věku, ale závislost se nepotvrdila. Věk neovlivňuje nastavení soukromí účtu ani znalosti zásad používání dat. I zde jsem očekával, že se věkově mladší jedinci projeví jako méně znalí a zkušení, ale to nemůžeme potvrdit. Z osobnostních faktorů jsem dále potvrdil závislost mezi místem bydliště a znalostí rizik spojených se sdílením dat.

Nastavení soukromí sdíleného obsahu ovlivňuje typ sdíleného obsahu. Závislost se zde prokázala jak u sdílení osobních dat, tak u typově jiných dat. Vliv na to může mít také fakt, že pro žáky je důležité chránit si soukromí a zároveň většina respondentů uvedla, že si soukromí sdíleného obsahu umí nastavit.

Očekával jsem, že počet obyvatel v místě bydliště bude mít vliv na sdílení osobních informací, kde jsem předpokládal, že respondenti mající kolem sebe větší počet přátel,

mají tendenci více na sebe poukazovat, ale to se nepotvrdilo. Můžeme se také domnívat, že respondenti záměrně nepřiznali, že sdílí své osobní informace, aby vypadali lépe a působili jako bezpeční uživatelé sociálních sítí.

Shrnutí získaných údajů:

- Chlapci na sociálních sítí sdílí převážně zábavný obsah.
- Dívky na sociálních sítí sdílí převážně své tzv. selfie fotografie a jiné obrázky.
- Věk neovlivňuje sdílení svých fotografií.
- Chlapci sdílejí osobní informace ve větší míře než dívky.
- Soukromí na sociálních sítí je pro žáky velmi důležité.
- Nejčastější způsob nastavení sdíleného obsahu je soukromý s různými omezeními.
- Chlapci sdílí svá data veřejně ve větší míře než dívky.
- Respondenti vnímají sociální sítě jako zdroj osobních informací o svých přátelích.
- Více než polovina respondentů je na sociálních sítí v kontaktu s lidmi, které osobně nikdy neviděli.
- Mladší respondenti projevují větší zájem o znalost zásad používání dat.
- Respondenti si jsou vědomi rizik, které přináší sdílení osobních dat.
- Osobní zkušenosti se zneužitím dat má 6 % respondentů.
- Pohlaví ovlivňuje typ sdílených dat a také nastavení soukromí sdíleného obsahu.
- Místo bydliště ovlivňuje znalosti rizik spojených se sdílením dat.
- Mezi věkem a dovednosti nastavení soukromí účtu neexistuje závislost.
- Podle typu sdílených dat respondenti nastavují soukromí těchto sdílených dat.
- Mezi pohlavím a znalostí zásad používá dat neexistuje závislost.

Pokud bych tyto výsledky shrnul do školní sféry a konkrétněji do výuky e-bezpečnosti na základních školách, tak vzhledem k zjištěným výsledkům, bych doporučoval například rozdělit výuku témat pro chlapce a dívky, protože se zde objevovali určité rozdíly. Věk respondentů zjevně nehraje roli ve znalostech rizik spojených se sdílením dat, ani dovednostech v nastavení účtů, a proto při výuce těchto témat bych navrhoval spojit ročníky, aby byla výuka e-bezpečnosti efektivnější. Žáci, kteří se projevili jako neznalí v oblasti ochrany soukromí, avšak uvedli, že mají zájem se o této problematice dozvědět více, tak právě jim bych umožnil přístup ke speciálním kurzům zaměřených na základní témata ochrany soukromí.

8 Závěr

Dotazníkovým šetřením jsem zjistil chování žáků základních škol na sociálních sítí. Zjistil jsem jejich pohled na problematiku ochrany soukromí, jaké sociální sítě využívají, jaký typ dat sdílí a v jaké míře. Dále jsem zjistil jejich znalosti a zkušenosti se zneužitím dat.

Použitím statistické metody jsem našel okolnosti, které ovlivňují chování respondentů. Nejvíce potvrzených závislostí jsem našel u pohlaví, které ovlivňuje především typ sdílených dat a nastavení soukromí sdíleného obsahu. Podle typu sdíleného obsahu pak respondenti nastavují soukromí těchto sdílených dat. Chování při sdílení osobních dat z osobnostních faktorů ovlivňuje pouze věk.

Překvapivé bylo zjištění, že se neprokázala závislost mezi znalostí zásad používání dat, znalostí rizik spojených se sdílením dat a věkem. Předpokládal jsem, že starší respondenti projeví více znalostí, ale to nebylo potvrzeno.

Hlavním přínosem práce je samotný výzkum, ve kterém pracuji s velmi aktuálním tématem. Zároveň je možné velmi dobře na tento výzkum navázat. Zajímavé by bylo zajistit distribuci dotazníků do více základních škol v České republice a porovnat samotné výsledky například z hlediska krajů a zjistit, zda se objevují určité rozdíly v chování a přístupu k ochraně soukromí. Jako návaznost výzkumu by mohl být realizován rozbor reálného chování na sociálních sítí, kde by byla provedena analýza profilů respondentů. Dále by se šlo také zaměřit na aktivity respondentů na sociálních sítí a porovnat je z hlediska bezpečnosti.

Použitá literatura a zdroje

[1] Počtem uživatelů internetu jsme přeskočili Evropu. *Czso.cz* [online]. 2015 [cit. 2017-06-14]. Dostupné z: https://www.czso.cz/csu/czso/poctem-uzivatelu-internetu-jsme-preskocili-evropu

[2] Počet používaných sociálních sítí na uživatele roste. *Mediaguru.cz* [online]. 2017 [cit. 2017-06-14]. Dostupné z: https://www.mediaguru.cz/2017/05/pocet-pouzivanych-socialnich-siti-na-uzivatele-roste/

[3] KOPECKÝ, Kamil. České děti a Facebook 2015. Výzkumná zpráva. Olomouc: univerzita Palackého v Olomouci, 2015.

[4] Top 15 Most Popular Websites | May 2017. *Ebizmba.com* [online]. 2017 [cit. 2017-06-16]. Dostupné z: http://www.ebizmba.com/articles/most-popular-websites

[5] DOBOSIOVÁ, Martina. Co to jsou sociální sítě. *Stremev.cz* [online]. 2015 [cit. 2017-06-16]. Dostupné z: https://www.stremev.cz/co-to-jsou-socialni-site/

[6] Historie sociálních sítí. *Socialnisite.estranky.cz* [online]. c2017 [cit. 2017-06-14]. Dostupné z: http://www.socialnisite.estranky.cz/clanky/historie-socialnich-siti.html

[7] Sociální sítě a jejich vývoj – pohled do historie. *Objevit.cz* [online]. 2013 [cit. 2017-06-16]. Dostupné z: http://objevit.cz/socialni-site-vyvoj-pohled-do-historie-t22280

[8] Sixdegrees. *Cs.wikipedia.org* [online]. 2015 [cit. 2017-06-16]. Dostupné z: https://cs.wikipedia.org/wiki/Sixdegrees

[9] Teorie masové komunikace jako specifika sociální komunikace. *Elearning.ujak.cz* [online]. 2012 [cit. 2017-06-16]. Dostupné z: http://2012.elearning.ujak.cz/mod/page/view.php?id=2185

[10] MIKLICA, Tomáš. Facebooky jiných dimenzí – sociální sítě, které svou šanci propásly. *Cnews.cz* [online]. 2012 [cit. 2017-06-16]. Dostupné z: http://www.cnews.cz/facebooky-jinych-dimenzi-socialni-site-ktere-svou-sanci-propasly/

[11] HALÍKOVÁ, Petra. Typy sociálních sítí. *Petrahalikova.com* [online]. 2016 [cit. 2017-06-17]. Dostupné z: http://www.petrahalikova.com/2016/08/06/typy-druhy-socialnich-siti/

[12] Víte, co je to BLOG? *Novinky.cz* [online]. 2003 [cit. 2017-06-17]. Dostupné z: https://www.novinky.cz/internet-a-pc/9928-vite-co-je-to-blog.html

[13] NÝVLTOVÁ, Táňa. Sociální sítě. *Wiki.knihovna.cz* [online]. 2010 [cit. 2017-06 17]. Dostupné z: http://wiki.knihovna.cz/index.php/Soci%C3%A1ln%C3%AD_s%C3%ADt%C4%9B

[14] MOREAU, Elise. The Top Social Networking Sites People Are Using. *Lifewire.com* [online]. 2017 [cit. 2017-06-19]. Dostupné z: https://www.lifewire.com/top-social-networking-sites-people-are-using-3486554

[15] Top 10 Most Popular Social Networks 2013. *Visual.ly* [online]. 2013 [cit. 2017-06-19]. Dostupné z: https://visual.ly/community/infographic/social-media/top-10-most-popular-social-networks-2013

[16] SORAV, Jain. 40 Most Popular Social Networking Sites of the World: Socialmediatoday.com. *Visual.ly* [online]. 2012 [cit. 2017-06-19]. Dostupné z: http://www.socialmediatoday.com/content/40-most-popular-social-networking-sites-world

[17] Top Sites in Czech Republic. *Alexa.com* [online]. 2017 [cit. 2017-06-19]. Dostupné z: http://www.alexa.com/topsites/countries/CZ

[18] DOČEKAL, Daniel. Vzestup a pád českých sociálních sítí. Justit.cz [online]. 2011 [cit. 2017-06-19]. Dostupné z: https://justit.cz/2011/04/02/vzestup-a-pad-ceskych-socialnich-siti/

[19] Facebook. *Wikipedia.org* [online]. 2011 [cit. 2017-06-19]. Dostupné z: https://cs.wikipedia.org/wiki/Facebook#cite_note-factsheet-3

[20] Company info - stats. *Newsroom.fb.com* [online]. 2017 [cit. 2017-06-19]. Dostupné z: https://newsroom.fb.com/company-info/

[21] YouTube. *En.wikipedia.org* [online]. 2015 [cit. 2017-06-19]. Dostupné z: https://en.wikipedia.org/wiki/YouTube

[22] Instagram. *En.wikipedia.org* [online]. 2014 [cit. 2017-06-19]. Dostupné z: https://en.wikipedia.org/wiki/Instagram

[23] Number of monthly active Instagram users from January 2013 to April 2017 (in millions). *Statista.com* [online]. 2017 [cit. 2017-06-19]. Dostupné z: https://www.statista.com/statistics/253577/number-of-monthly-active-instagram-users/

[24] Linkedin – O nás. *Press.linkedin.com* [online]. c2017 [cit. 2017-06-19]. Dostupné z: https://press.linkedin.com/cs-cz/about-linkedin

[25] Linkedln. *En.wikipedia.org* [online]. 2015 [cit. 2017-06-19]. Dostupné z: https://en.wikipedia.org/wiki/LinkedIn

[26] ROUSE, Margaret. LinkedIn. *Whatis.techtarget.com* [online]. 2016 [cit. 2017-06-19]. Dostupné z: http://whatis.techtarget.com/definition/LinkedIn

[27] Děti a rizika sociálních sítí. *Sancedetem.cz* [online]. 2014 [cit. 2017-06-20]. Dostupné z: http://www.sancedetem.cz/srv/www/content/pub/cs/clanky/deti-a-rizika-socialnich-siti-112.html

[28] Rizika sociálních sítí. *Jaknainternet.cz* [online]. c2017 [cit. 2017-06-20]. Dostupné z: https://www.jaknainternet.cz/page/1185/rizika-socialnich-siti/

[29] ČERNÁ, Alena, Lenka DĚDKOVÁ, Hana MACHÁČKOVÁ, Anna ŠEVČÍKOVÁ a David ŠMAHEL. KYBERŠIKANA. 1. Praha: Grada Publishing, a.s, 2013. ISBN 978-80-247-4577-0.

[30] Co je kyberšikana? *E-bezpeci.cz* [online]. 2009 [cit. 2017-06-20]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/kyberikana/17-cojekybersikana

[31] Víte, co je KYBERŠIKANA? *Policie.cz* [online]. 2011 [cit. 2017-06-20]. Dostupné z: http://www.policie.cz/clanek/vite-co-je-kybersikana.aspx

[32] Kybergrooming. *Nebudobet.cz* [online]. c2010-2017 [cit. 2017-06-20]. Dostupné z: http://www.nebudobet.cz/?cat=kybergrooming

[33] Co je to stalking a cyberstalking. *E-bezpeci.cz* [online]. 2008 [cit. 2017-06-20]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/stalking-a-kyberstalking/66-23

[34] PREVENCE – Stalking. Policie.cz [online]. c2017 [cit. 2017-06-20]. Dostupné z: http://www.policie.cz/clanek/prevence-stalking.aspx

[35] CO JE TO PHISHING. *Hoax.cz* [online]. c2000-2017 [cit. 2017-06-21]. Dostupné z: http://www.hoax.cz/phishing/co-je-to-phishing

[36] Skautští vedoucí zneužili 39 dětí. Soud jim potvrdil deset let vězení. *Ustecky.denik.cz* [online]. 2014 [cit. 2017-06-21]. Dostupné z: http://ustecky.denik.cz/zlociny-a-

soudy/vedouci-skautu-zneuzili-39-deti-soud-jim-potvrdil-deset-let-vezeni-20140708-17bb.html

[37] Zneužitím osobních údajů přišli o peníze. *Policie.cz* [online]. 2013 [cit. 2017-06-21]. Dostupné z: http://www.policie.cz/clanek/zneuzitim-osobnich-udaju-prisli-o-penize.aspx

[38] Kyberstalking - obtěžování po internetu. *Detskyklub.cz* [online]. c2008-2017 [cit. 2017-06-21]. Dostupné z: http://www.detskyklub.cz/c-kyberstalking-obtezovani-po-internetu.html

[39] JAKOB, Ondřej. Ministerstvo financí upozorňuje na množící se případy zneužití identifikačních údajů („ukradená identita"). *Mfcr.cz* [online]. 2012 [cit. 2017-06-21]. Dostupné z: http://www.mfcr.cz/cs/aktualne/tiskove-zpravy/2012/2012-05-03-tiskova-zprava-5110-5110

[40] Rady pro bezpečné používání sociálních sítí. *Bezpecnyinternet.cz* [online]. [cit. 2017-06-21]. Dostupné z: http://www.bezpecnyinternet.cz/zacatecnik/socialni-site/rady.aspx

[41] SKYBA, Mike. Bezpečnost sociálních sítí. Cz.norton.com [online]. c1995-2016 [cit. 2017-06-21]. Dostupné z: https://cz.norton.com/social-networking-safety/article

[42] 9 důvodů, proč být aktivní v sociálních sítích. *Sunmarketing.cz* [online]. c2011-2017 [cit. 2017-06-22]. Dostupné z: http://www.sunmarketing.cz/marketing-v-socialnich-sitich/9-duvodu-proc-byt-aktivni-v-socialnich-sitich

[43] ACHREMENKO, Michal. Problém sociálních sítí: ochrana soukromí, ale i záplava informací. *Denik.cz* [online]. 2012 [cit. 2017-06-27]. Dostupné z: http://www.denik.cz/ekonomika/problem-socialnich-siti-ochrana-soukromi-ale-i-zaplava-informaci-20121013.html

[44] BERGER, Vojtěch. Tisíce uživatelů žalují Facebook kvůli malé ochraně osobních údajů. Kauzu řeší soud ve Vídni. *Irozhlas.cz* [online]. 2015 [cit. 2017-06-27]. Dostupné z: https://www.irozhlas.cz/zpravy-svet/tisice-uzivatelu-zaluji-facebook-kvuli-male-ochrane-osobnich-udaju-kauzu-resi-soud-ve-vidni_201504091900_krohackova

[45] Facebook porušuje evropské zákony o ochraně soukromí, tvrdí belgická komise. *byznys.ihned.cz* [online]. 2015 [cit. 2017-06-27]. Dostupné z: http://byznys.ihned.cz/c1-64017500-facebook-porusuje-evropske-zakony-o-ochrane-soukromi-tvrdi-belgicka-komise

[46] Facebook je u soudu, kvůli špehování ho žaluje 25 000 lidí. *Zpravy.aktualne.cz* [online]. 2015 [cit. 2017-06-27]. Dostupné z: https://zpravy.aktualne.cz/zahranici/facebook-je-u-soudu-kvuli-spehovani-ho-zaluje-25-000-lidi/r~f85ee814de9b11e485d7002590604f2e/

[47] Google porušil zákon o ochraně dat, tvrdí Britové. *Archiv.ihned.cz* [online]. 2010 [cit. 2017-06-27]. Dostupné z: https://archiv.ihned.cz/c1-47734510-google-porusil-zakon-o-ochrane-dat-tvrdi-britove

[48] Klíč o ochraně osobních údajů. *Oou.cz* [online]. c2014 [cit. 2017-06-27]. Dostupné z: http://www.oou.cz/

[49] Povinnosti správce. *Oou.cz* [online]. c2014 [cit. 2017-06-27]. Dostupné z: http://www.oou.cz/povinnostispravcu

[50] Práva subjektů údajů osobních údaj. *Oou.cz* [online]. c2014 [cit. 2017-06-27]. Dostupné z: http://www.oou.cz/pravaapovinnosti/pravasubjektuudaju

[51] Zásady používání dat. *Facebook.com* [online]. c2017 [cit. 2017-06-28]. Dostupné z: https://www.facebook.com/about/privacy

[52] Zásady ochrany osobních údajů. *Facebook.com* [online]. 2013 [cit. 2017-06-28]. Dostupné z: https://www.facebook.com/help/instagram/155833707900388/?helpref=hc_fnav

[53] Vítejte v zásadách ochrany soukromí Google. *Google.cz* [online]. 2005 [cit. 2017-06-28]. Dostupné z: https://www.google.cz/intl/cs/policies/privacy/

[54] Prohlášení o právech a povinnostech. *Facebook.com* [online]. c2017 [cit. 2017-06-29]. Dostupné z: https://www.facebook.com/legal/terms

[55] Terms of Use. *Facebook.com* [online]. c2017 [cit. 2017-06-29]. Dostupné z: https://www.instagram.com/about/legal/terms/before-january-19-2013/

[56] Smluvní podmínky společnosti Google. *Google.com* [online]. 2007 [cit. 2017-06-29]. Dostupné z: https://www.google.com/intl/cs/policies/terms/

[57] Chí-kvadrát test. Biopedia.sk [online]. c2017 [cit. 2017-07-01]. Dostupné z: https://www.biopedia.sk/genetika/chi-kvadrat-test

[58] Testování nezávislosti (Pearsonův chí-kvadrát test). *Portal.matematickabiologie.cz* [online]. [cit. 2017-07-01]. Dostupné z: http://portal.matematickabiologie.cz/index.php?pg=aplikovana-analyza-klinickych-a-biologickych-dat--biostatistika-pro-matematickou-biologii--testovani-hypotez-o-kvalitativnich-promennych--analyza-kontingencnich-tabulek--testovani-nezavislosti-pearsonuv-chi-kvadrat-test

[59] Kyberšikana se týká každého druhého dítěte v Česku. *Novinky.cz* [online]. [cit. 2017-07-04]. Dostupné z: https://www.novinky.cz/internet-a-pc/428653-kybersikana-se-tyka-kazdeho-druheho-ditete-v-cesku.html

Seznam obrázků

Obr. 1: Zastoupení respondentů z hlediska pohlaví 54
Obr. 2: Zastoupení respondentů z hlediska navštěvované školy 55
Obr. 3: Používané sociální sítě 55
Obr. 4: Přehled dat, které žáci sdílí na sociálních sítí 56
Obr. 5: Srovnání sdílení dat vzhledem k pohlaví 57
Obr. 6: Srovnání frekvence sdílení dat vzhledem k pohlaví 57
Obr. 7: Pohled na nastavení soukromí svého účtu 58
Obr. 8: Pohled na ochranu soukromí na sociálních sítí 59
Obr. 9: Přehled nastavení soukromí při sdílení obsahu 59
Obr. 10: Nastavení soukromí vzhledem k pohlaví 60
Obr. 11: Pohled na sociální sítě jako na zdroj informací 61
Obr. 12: Míra důvěřivosti sdílených informací 61
Obr. 13: Pohled na neznámé kontakty na sociálních sítí 62
Obr. 14: Porovnání přehledu znalostí zásad 63
Obr. 15: Hrozby při sdílení dat - prezentace znalostí respondentů 64
Obr. 16: Procentuální zastoupení osobní zkušenosti se zneužitím dat 65
Obr. 17: Přehled potvrzených a nepotvrzených závislostí 66

Přílohy

Na přiloženém DVD se nachází:

- Plné znění bakalářské práce pod názvem BP_Havlíček_Radek.pdf.
- Zpracování hypotéz a grafů pod názvem BP_vyhodnoceni.xlsx

Dotazník

1. Jsem …

o Kluk

o Holka

2. Tvůj věk

—

3. Název školy

—

4. Kde bydlíš?

o Město

o Vesnice

o Jiné ...

5. Kolik obyvatel tam přibližně žije?

o 50 tisíc a více

o 50-20 tisíc

o 20-10 tisíc

o 10-5 tisíc

o 5-2 tisíce

o 2 tisíce a méně

6. Využíváš sociální sítě? (Můžeš zaškrtnout více odpovědí)

☐ Facebook

☐ Twitter

☐ Google+

☐ Instagram

☐ Myspace

☐ Spolužáci.cz

☐ Lidé.cz

☐ Využívám spíše jiné sociální sítě

☐ Nevyužívám žádné sociální sítě; Při této odpovědi byl respondent přesměrován na konec dotazníku.

7. Kterou používáš nejvíc?

—

8. Víš, jak sociální síť nakládá s daty, která na ni uvedeš? (Můžeš zaškrtnout více odpovědí)

☐ Ano, četl/a jsem celé zásady používání dat na sociální síti

☐ Ano, četl/a jsem částečně zásady používání dat na sociální síti

☐ Ano, něco málo o tom vím, ale zásady používání dat jsem nikdy nečetl/a

☐ Ano, bavil/a jsem se o tom s kamarády

☐ Ano, četl/a jsem o tom na internetu

☐ Ne, ale zajímalo by mě to

☐ Ne, nezajímá mě to

9. Když vkládáš nějaký příspěvek na sociální síť, viditelnost tohoto příspěvku nastavuješ obvykle jako:

O Veřejný

O Soukromý; jen pro přátele

O Soukromý; jen pro některé přátele

O Soukromý; pro přátele přátel

O Soukromý; pouze já

10. Jaká data na sociálních sítí sdílíš? (Vyber jednu nebo více možností)

☐ Osobní informace (bydliště, věk, telefonní číslo, škola)

☐ Fotografie - vytvořené mnou

☐ Svoje fotografie – selfíčka

☐ Obrázky z internetu

☐ Videozáznamy

☐ Osobní názory

☐ Sdílení zábavného obsahu (hry, vtipy, obrázky...)

☐ Žádná data nesdílím

11. Myslíš si, že Tvoje sdílená data může vidět i někdo, koho jsi nikdy osobně neviděl/a a nikdy nepotkal/a?

O Ano a vadí mi to

O Ano, ale nevadí mi to

O Ne

O Nevim

12. Tušíš, jaká rizika hrozí při sdílení dat na sociálních sítí?

O Ano, ale je mi to jedno

O Ano a dávám si na to pozor

O Ne, nezajímá mě to

O Nevím

13. Jaká rizika to podle tebe jsou? (Zkus nějaká vymyslet)

—

14. Jak hodnotíš své chování na sociální síti z pohledu sdílení dat? Vybarvi... (5 hvězdiček = sdílím vše, 1 hvězdička = nesdílím nic)

15. Myslíš si, že je důležité chránit si soukromí na sociálních sítí?

- O Ano a snažím se si jej chránit
- O Ano, ale nijak se tím nezaobírám
- O Ne
- O Nevím

16. Setkal/a jsi se někdy s nějakým prohlášením, jak sociální sítě nakládají s Tvými daty?

- O Ano, ale nevěnoval/a jsem tomu pozornost
- O Ano a zaujalo mě to
- O Nikdy jsem tomu nevěnoval/a pozornost
- O Ne

17. Jsi si vědom/a rizik, která přináší sdílení dat na sociální síti?

- O Ano a dávám si na to pozor
- O Ano, ale příliš se tím nezabývám
- O Ne
- O Je mi to jedno

18. Umíš si nastavit zabezpečení a soukromí svého účtu na sociální síti, kterou používáš?

- O Ano, můj účet je nastavený podle mých představ
- O Částečně ano
- O Neumím, nevím kde to najít
- O Nezajímám se o to

19. Máš mezi svými přáteli lidi, které jsi nikdy neviděl/a?

- O Ano, mám jich spoustu
- O Ano, mám jich pár
- O Ne, nikdy bych si takového člověka nepřidal/a do přátel

O Ne, ale kdyby taková situace nastala, tak se nebudu bránit přidání/potvrzení.

20. Jsou pro tebe sociální sítě zdrojem osobních informací o Tvých přátelích?

O Ano, díky sociální síti vím o mých přátelích vše

O Ano, sociální síť mi poskytuje některé osobní informace o mých přátelích

O Ano, ale nezajímám se o to

O Ne

21. Do jaké míry věříš tomu, co přátelé uvádí o sobě na sociálních sítí?

O Nezajímám se o to

O Věřím všemu

O Věřím jen něčemu

22. Máš nějakou osobní zkušenost se zneužitím dat na sociální síti? Pokud ano zkus se rozepsat :)

—