Soukromí jako nový druh aktiva

Bc. Roman Škarpa

Diplomová práce
2020

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektroniky a měření

Akademický rok: 2019/2020

ZADÁNÍ DIPLOMOVÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Roman Škarpa**
Osobní číslo:	**A18300**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**Kombinovaná**
Téma práce:	**Soukromí jako nový druh aktiva**
Téma práce anglicky:	**Privacy as a New Kind of Asset**

Zásady pro vypracování

1. Specifikujte, co je to soukromí a jak je obsahově a právně vymezeno.
2. Analyzujte příčiny a podstatu vzniku ochrany soukromí jako specifického druhu bezpečnosti. Co tvoří jeho aktiva.
3. Specifikujte a analyzujte základní hrozby, které ohrožují soukromí. Zaměřte se na fyzické a logické způsoby ohrožení soukromí. Analyzujte vybrané konkrétní případy narušení soukromí.
4. Na základě dotazníkového šetření specifikujte, jak si jednotlivé referenční objekty cení svého soukromí, jak je vnímají jako nové aktivum a jaké problémy spatřují v oblasti ochrany soukromí.
5. Navrhněte způsob řešení identifikovaných problémů v oblasti ochrany soukromí.

Rozsah diplomové práce:
Rozsah příloh:
Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. KERNIGHAN, Brian W. Jak porozumět digitálnímu světu: vše, co potřebujete vědět o internetu, bezpečnosti a soukromí. Praha: Argo, 2019. ISBN 978-80-7363-903-7.
2. MATEJKA, Ján. Internet jako objekt práva: hledání rovnováhy autonomie a soukromí. Praha: CZ.NIC, 2013. ISBN 978-80-904248-7-6.
3. Přehled judikatury ve věcech ochrany osobnosti. Praha: Wolters Kluwer ČR, 2016. ISBN 978-80-7552-074-6.
4. MATES, Pavel. Ochrana osobnosti, soukromí a osobních údajů. Praha : Leges, 2019. ISBN:978-80-7502-346-9.
5. PAVLÍČEK, Václav. Ústava a ústavní řád České republiky: komentář. Praha: Linde, 2003. ISBN 8072013912.
6. ŠULC, Vladimír. Kybernetická bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.
7. KOLOUCH, Jan a Pavel BAŠTA. CyberSecurity. Praha: CZ.NIC, 2019. ISBN 978-80-88168-31-7.
8. BARTÍK, Václav a Eva JANEČKOVÁ. Ochrana osobních údajů v aplikační praxi: vybrané otázky. Praha: Linde Praha, 2013. ISBN 978-80-86131-96-2.

Vedoucí diplomové práce: **doc. Ing. Luděk Lukáš, CSc.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **9. prosince 2019**
Termín odevzdání diplomové práce: **29. května 2020**

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Milan Navrátil, Ph.D.
ředitel ústavu

Ve Zlíně dne 9. prosince 2019

Jméno, příjmení: Bc. Roman Škarpa
Název diplomové práce: Soukromí jako nový druh aktiva
Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Bc. Roman Škarpa, v.r.

Ve Zlíně, dne 11.8. 2020

…….
podpis diplomanta

ABSTRAKT

Diplomová práce je zaměřena na ochranu soukromí. Zabývá se právním a obsahovým vymezením soukromí, včetně jeho aktiv. Analyzuje příčiny k ochraně soukromí, včetně jejich důsledků. Dále jsou v práci specifikovány hrozby, které ohrožují soukromí. Praktická část analyzuje na základě dotazníkového šetření, jak si respondenti cení svého soukromí a jaké problémy spatřují při jeho ochraně. Dotazník bude podpořen i názorem odborníků na tuto problematiku. Na identifikované problémy bude navrhnuto řešení.

Klíčová slova: soukromí, osobní údaje, ochrana, narušení, identita

ABSTRACT

The diploma thesis is focused on privacy protection. It deals with the legal and content definition of privacy, including its assets. Analyzes the causes of privacy, including their consequences. Furthermore, threats that threaten privacy are specified in the work. The practical part analyzes, based on a questionnaire survey, how respondents value their privacy and what problems they see in protecting it. The questionnaire will also be supported by the opinion of experts on this issue. A solution will be proposed for the identified problems.

Keywords: privacy, personal data, protection, disrupiton, identity

V první řadě bych chtěl poděkovat svému vedoucímu práce, panu doc. Ing. Luďkovi Lukášovi, CSc. Za odborné vedení diplomové práce, vstřícnost při konzultacích a cenné rady při zhotovování diplomové práce. Dále bych chtěl poděkovat všem lidem, kteří se podíleli na dotazníkovém šetření a interview.

Prohlašuji, že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Ochrana soukromí je v dnešní době aktuálním tématem. Ochrana osobních údajů, případy narušení soukromí a celkově zacházení s osobními údaji, se skloňuje mnohem více než dříve. Přelom v ochraně soukromí přinesly moderní telekomunikační prostředky. Pro všechny úkony již lidé používají internet. Všechny své osobní i pracovní záležitosti mají uložené ve svých počítačích a mobilech. Velká část úkonů, ke které byla dříve nutná osobní přítomnost člověka, dnes lze vyřídit online. Samozřejmě tyto online úkony šetří čas, ale dávají pachatelům prostor k tomu, aby mohli kopírovat něčí identitu za účelem obohacení se na úkor druhého člověka. K tomuto finančnímu obohacení zneužívají cizí identitu, na kterou si zakládají bankovní půjčky, nebo se snaží získat osobní údaje a údaje o platebních kartách k peněžním převodům. Ovšem pro soukromí není jedinou hrozbou krádež identity. Přechod do kybernetického prostoru napomohl i šíření kyberšikany, pokusům o zdiskreditování a manipulování lidí. Dalším problémem ochrany soukromí je to, že velké firmy jako Google a Facebook shromažďují o uživatelích velké množství osobní údajů, pro nejrůznější účely, převážně reklamní. I toto jednání se dá považovat za narušení soukromí. Jelikož aktuálně dochází k narušení soukromí převážně v kybernetickém prostoru, se tato diplomová práce bude zabývat převážně ochranou a problémy souvisejícími s narušením soukromí v kybernetickém prostoru.

Diplomová práce se dělí na část teoretickou a praktickou. Teoretická část se dělí na další 3 části. První část se zabývá obsahovým a právním vymezením soukromí. Z obsahové hlediska vymezí, co vše spadá pod soukromí a co si pod soukromím vše člověk může vyložit. Z právního vymezení soukromí se bude jednat o to, jak je soukromí v české legislativě vymezeno. Bude zde řešeno jaké zákony a vyhlášky slouží k ochraně soukromí a jak je právně vymahatelné narušení soukromí.

Druhá část se zabývá přímo ochranou soukromí jako nového druhu bezpečnosti. V této části práce jsou rozebrány hlavní příčiny k ochraně soukromí, které vedou k nutné vyšší ochraně soukromí. Následně budou rozebrány i dopady na soukromí, které plynou z daných příčin.

Třetí část se již zabývá přímo hrozbami, které narušují soukromí. Tyto hrozby jsou v práci klasifikovány podle dopadu na soukromí. Jedná se o hrozby logické a fyzické. Všechny hrozby narušující soukromí budou popsány, včetně doporučení jak se těmto hrozbám vyvarovat, nebo snížit jejich riziko. Poslední část teoretické části spočívá v analyzování

dvou skutečných případů narušení soukromí, aby bylo více transparentní, že případy narušení soukromí můžou mít vážný psychický, fyzický, nebo peněžní dopad.

Praktickou část tvoří analýza veřejného mínění o tom, jak se lidé cení svého soukromí. Respondenti budou odpovídat na nejrůznější otázky týkajících se soukromí, jestli vnímají ochranu soukromí za dostatečnou a kde se nejvíce obávají o své soukromí. Toto dotazníkové šetření poslouží jako podklad k identifikování problémů souvisejících se soukromím. Dotazníkové šetření bude doplněno o rozhovory s policistou a právníkem, kteří potvrdí, nebo vyvrátí, že identifikované problémy jsou opravdové.

Poslední část práce se zabývá návrhem řešení identifikovaných problémů. Každý problém bude podrobněji vyspecifikován, včetně návrhu řešení daného problému. Bude se jednat o soubor o doporučení, jak lze tyto problémy v současné situaci minimalizovat, s vlastním návrhem nového řešení problému.

I. TEORETICKÁ ČÁST

1 SOUKROMÍ

Člověk má své soukromí a mělo by být jen na něm, jak moc dovolí okolnímu světu do něj nahlédnout. Najdou se i lidé, kterým svým způsobem na soukromí nezáleží. Nejspíše si kladou otázku, proč bych měl „já“ někoho zajímat, k čemu by okolnímu světu „mé“ údaje sloužily a jak by mi mohlo ublížit, když tyto informace zjistí. Ale i přesto je v dnešní době čím dál více lidí, kteří si své soukromí snaží uchránit. Nechtějí, aby měl okolní svět přístup k jeho fotografiím, osobním údajům a dokumentům, které uchovává ve svém soukromí. Když chce být viděn a něco o sobě sdělit, tak to udělá vědomě a měl by si být vědom, jaké následky to může přinášet. Tato kapitola se bude zabývat právě soukromím, co vše do něj spadá a jak je v České republice právně vymezeno.

V právních normách je výraz „soukromí“ používán mnoho století. Po dlouhou dobu bylo soukromí bráno jako adjektivum k vyjádření něčeho co patří jen určité osobě, na co má nárok, který musí být respektován. To znamená, že garantována byla pouze dílčí práva (např. nedotknutelnost obydlí, důstojnost osoby), nikoliv právo na soukromí jako specifické a samostatné právo. Ústava ani jiné zákony pojem soukromí nechránily ani nepoužívaly, i přesto, že obsah soukromí jak ho chápeme dnes, byl chráněn. [1]

V původním pojetí bylo „soukromí“ vymezeno jako sféra člověka, do níž se nesmí zasahovat bez jeho souhlasu, nebo pokud k tomu neexistuje zákonem daný důvod. Dále oblast, o níž nejsme povinni podávat žádné informace a všem je zakázáno tyto informace získávat a dále je používat, pokud to dotyčný neumožnil, nebo k tomu nebyl zákonem daný důvod. Postupně se doktrína i judikatura propracovaly k širšímu pojmu soukromí, než je jen soukromí čtyř stěn. Soukromí nyní již není omezeno jen na vnitřní kruh, v němž jedinec může žít osobní život, ale je do něj zahrnuto i právo vytvářet a budovat vztahy k ostatním lidem, zejména k rodině. Dále by soukromí mělo představovat možnost navazovat sociální a individuální vztahy na pracovišti. [1]

Podobně na soukromí nahlíží i Ústavní soud České republiky. Podle něj má právo na soukromí dvě složky, pozitivní a negativní. Složka pozitivní obsahuje právo fyzické osoby svobodně rozhodovat, zda a v jaké míře a jakým způsobem mají být skutečnosti z jeho života zpřístupněny. Negativní složka vyjadřuje právo se bránit neoprávněnému zasahování do soukromého života. Soukromí se ale nemůže omezovat pouze na ochranu proti neoprávněnému získávání informací a skutečností ze soukromého života a jeho šíření. Tím by se právo zúžilo a nezahrnovalo by i ostatní aspekty soukromí jako vztahy rodinné,

sociální, ale i materiální. Ústavní soud klade důraz na to, aby tyto vztahy mohly fungovat a rozvíjet se. [1]

Ovšem všichni, kteří se právem na soukromí odborně zabývají, se shodují na tom, že pojem právo na soukromí nelze přesně definovat, zejména z důvodu, že okruh hodnot, které spadají pod soukromí, se neustále vyvíjí. Evropský soud pro lidská práva prohlásil, že neshledává nutným pokoušet se o přesnou definici slova soukromý život, právě s ohledem na jeho strukturovanou a dynamickou povahu. [2]

Pro zachování soukromí není rozhodující, kde se člověk nachází. Právo na soukromí se neztrácí ani ve veřejném prostoru o čemž svědčí množství právních aktů týkajících se pořizováním kamerových záznamů v komerčních prostorách, nebo na ulicích. [2]

O soukromí lze hovořit jen ve vztahu k fyzickým osobám. Soukromím se nerozumí jen subjektivní nahlížení na vniknutí do čtyř stěn. Jedná se i o právo na osobní anatomii, osobní vývoj, právo na rozvíjení vztahů s lidmi, vztahy které jsou obchodní a profesionální. Do soukromého života spadá rovněž interakce s dalšími osobami i přesto že je uskutečňována ve veřejném kontextu, nebo jako součást obchodních aktivit. [2]

Stát je povinen přijmout opatření na ochranu soukromí, u služeb institucí, bez kterých se nedá v moderním světě obejít. Jedná se o banky a jiné finanční instituce, dopravní podniky a poskytovatelé telekomunikačních služeb a mobilní operátoři, protože zde může docházet k zásahům do soukromí, aniž si to můžou dotyční lidé uvědomovat. [2]

1.1 Právní vymezení soukromí

Právní ochrana soukromí spočívá zejména v tom vytvořit si možnost, co ze svého soukromého života budu sdílet s ostatními a svým okolím a co nikoliv. Ochranou soukromí se zabývá obecné ustanovení §81 Občanského zákoníku a dále je upravena v ustanovení §86 téhož zákona. [2]

Soukromí je chráněno zároveň i nad zákonnými právními předpisy, zejména článkem 7 a 10 Listiny základních práv a svobod. Postihy a sankce za narušení soukromí člověka vymezuje Trestní zákoník. [2]

1.1.1 Listina základních práv a svobod

Listina základních práv a svobod je součást ústavního pořádku České republiky. Vznikla na základě federální shromáždění návrhů České národní rady a Slovenské národní rady,

uznávající neporušitelnost přirozených práv člověka. Česká a Slovenská federativní republika ji schválila 16. prosince 1992. [3]

Soukromí je v listině základních práv a svobod zakotveno hned ve dvou článcích, konkrétně v článku 7, který zaručuje nedotknutelnost osoby a jejího soukromí a v článku 10, který garantuje právo na ochranu proti neoprávněným zásahům do soukromého a rodinného života. [1]

Článek 7 je vykládán tak, že se jedná o generální klauzuli, jíž je chráněno soukromí všeobecně. Tento výklad se opírá o ochranu osoby a v širokém slova smyslu po všech jejích stránkách (tělesné, duševní, psychické a profesních aktivit). Toto ustanovení je navíc zesíleno o pojem nedotknutelnost. Z toho plyne, že garantem tohoto práva je stát, který je povinen zabránit nepovolaným zásahům do soukromí ze strany veřejné moci i jednotlivců. [1]

Konkrétní znění článku 7:

„(1) Nedotknutelnost osoby a jejího soukromí je zaručena. Omezena může být jen v případech stanovených zákonem.

(2) Nikdo nesmí být mučen ani podroben krutému, nelidskému nebo ponižujícímu zacházení nebo trestu.“ [3]

Článek 10 chrání soukromí osoby v užším slova smyslu se zaměřením na intimní hodnoty (tělo, podoba, sexualita, rodinné vztahy atd.). Zde je ovšem interpretační problém, že v odstavci jedna je chráněna osobnost člověka a její projevy, které ale tvoří část soukromí. Dále v odstavci 2 je zvlášť garantovaný rodinný život, který také spadá do soukromí. Zde můžeme vidět, že snaha zákonodárce, který chtěl vyložit právo na soukromí co nejvíce komplexně, vedla k překrývání pojmů a některá práva a hodnoty jsou garantovány vícekrát. [1]

Konkrétní znění článku 10:

„(1) Každý má právo, aby byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a chráněno jeho jméno.

(2) Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života.

(3) Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.“ [3]

Vedle článku 7 a 10 dále Listina základních práv a svobod garantuje další jednotlivé atributy, které taktéž spadají pod soukromí. Konkrétně v článku 6 (ochrana lidského života), článku 9 zákaz nucených prací a služeb, článku 12 (nedotknutelnost obydlí), článku 13 (tajemství listovní, písemnosti a zpráv podávaných telekomunikačními prostředky) a článku 14 (svoboda pobytu a pohybu)

Pro pojem soukromí jako nový druh aktiva se nás nejvíce týká článek 13 tajemství listovní, písemnosti a zpráv podávaných telekomunikačními prostředky. [1]

„Nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon. Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením.“ [3]

A článek 12, který se zabývá nedotknutelnosti obydlí

„(1) Obydlí je nedotknutelné. Není dovoleno do něj vstoupit bez souhlasu toho, kdo v něm bydlí.
(2) Domovní prohlídka je přípustná jen pro účely trestního řízení, a to na písemný odůvodněný příkaz soudce. Způsob provedení domovní prohlídky stanoví zákon.
(3) Jiné zásahy do nedotknutelnosti obydlí mohou být zákonem dovoleny, jen je-li to v demokratické společnosti nezbytné pro ochranu života nebo zdraví osob, pro ochranu práv a svobod druhých anebo pro odvrácení závažného ohrožení veřejné bezpečnosti a pořádku. Pokud je obydlí užíváno také pro podnikání nebo provozování jiné hospodářské činnosti, mohou být takové zásahy zákonem dovoleny, též je-li to nezbytné pro plnění úkolů veřejné správy.“ [3]

Listina základních práv a svobod nám zaručuje ochranu soukromí jako celku. Dává nám právo na to, že nikdo by nás neměl ponižovat, pomlouvat urážet a jinak narušovat naše soukromí. Vedle toho chrání i aktiva spojené se soukromím. Zaručuje nám nedotknutelnost odesílaných zpráv a ochranu veškerých dokumentů uchovávaných v soukromí. Za což lze považovat jakékoliv dokumenty ať už pracovní záležitosti v počítači, fotografie, cenné papíry apod.

Velmi důležitou pro ochranu našich aktiv je i nedotknutelnost obydlí, která zaručuje, že nikdo bez našeho souhlasu nemá právo vstoupit do našeho obydlí. Není tím myšleno jen náš dům, ale i hotelový pokoj, karavany apod.

Dále nikomu nedává právo shromažďovat o nás jakékoliv osobní údaje, které by nás pomohly identifikovat. Najít údaje o kterékoliv osobě není náročné a je zde více zdrojů těchto dat. Samostatně nemusí být tyto údaje pro narušení soukromí nebezpečné, ale pokud někdo dá informace dohromady, lze poskládat i celou identitu člověka, což už nebezpečné je.

1.1.2 Občanský zákoník

Občanský zákoník je zákon č.89/2012 Sb, který byl přijat Parlamentem České republiky v roce 2012. Hned v úvodu zákonné úpravy je zakotveno právo na ochranu cti a důstojnosti. [2]

„§ 81

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

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

Následuje ustanovení o možnosti obrany proti porušení práva.

§ 82

„(1) Člověk, jehož osobnost byla dotčena, má právo domáhat se toho, aby bylo od neoprávněného zásahu upuštěno nebo aby byl odstraněn jeho následek.

(2) Po smrti člověka se může ochrany jeho osobnosti domáhat kterákoli z osob jemu blízkých.“

§ 83

„(1) Souvisí-li neoprávněný zásah do osobnosti člověka s jeho činností v právnické osobě, může právo na ochranu jeho osobnosti uplatnit i tato právnická osoba; za jeho života však jen jeho jménem a s jeho souhlasem. Není-li člověk schopen projevit vůli pro nepřítomnost nebo pro neschopnost úsudku, není souhlasu třeba.

(2) Po smrti člověka se právnická osoba může domáhat, aby od neoprávněného zásahu bylo upuštěno a aby byly odstraněny jeho následky.“ [4]

Podoba a soukromí

Ustanovení §84 OZ stanovuje, že jakékoliv zachycení podoby člověka je možné jen se souhlasem zachyceného člověka. Vztahuje se již na možnost vyfotografování člověka. Souhlas člověka se zachycením podoby může být vyjádřen jakkoliv. Jak ústně tak písemně nebo jen mlčky. [2]

„§ 84

Zachytit jakýmkoli způsobem podobu člověka tak, aby podle zobrazení bylo možné určit jeho totožnost, je možné jen s jeho svolením.“ [4]

Ustanovení§ 85 OZ dále obdobně upravuje podmínku souhlasu k šíření podobizny. [2]

§ 85

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

(2) Svolí-li někdo k zobrazení své podoby za okolností, z nichž je zřejmé, že bude šířeno, platí, že svoluje i k jeho rozmnožování a rozšiřování obvyklým způsobem, jak je mohl vzhledem k okolnostem rozumně předpokládat.“ [4]

Ustanovení §86 OZ obsahuje široký rozsah ochrany soukromí člověka, především narušení soukromí člověka a záznamu soukromých prostor. Tato ustanovení se vztahují i na zákaz záznamu o soukromém životě a písemnosti osobní povahy. [2]

„§ 86

Nikdo nesmí zasáhnout do soukromí jiného, nemá-li k tomu zákonný důvod. Zejména nelze bez svolení člověka narušit jeho soukromé prostory, sledovat jeho soukromý život nebo pořizovat o tom zvukový nebo obrazový záznam, využívat takové či jiné záznamy pořízené o soukromém životě člověka třetí osobou, nebo takové záznamy o jeho soukromém životě šířit. Ve stejném rozsahu jsou chráněny i soukromé písemnosti osobní povahy.“ [4]

Udělený souhlas s šířením podobizny a písemnosti osobní povahy lze odvolat.

„§ 87

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

(2) Bylo-li svolení udělené na určitou dobu odvoláno, aniž to odůvodňuje podstatná změna okolností nebo jiný rozumný důvod, nahradí odvolávající škodu z toho vzniklou osobě, které svolení udělil.“ [4]

Výjimky pro zachycení podoby a užití podobizny bez souhlasu

„§ 88

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

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

§ 89

Podobizna nebo zvukový či obrazový záznam se mohou bez svolení člověka také pořídit nebo použít přiměřeným způsobem též k vědeckému nebo uměleckému účelu a pro tiskové, rozhlasové, televizní nebo obdobné zpravodajství.“ [4]

Pro všechny výjimky platí omezující podmínka, že je možné výjimku použít jen přiměřeným způsobem.

„§ 90

Zákonný důvod k zásahu do soukromí jiného nebo k použití jeho podobizny, písemnosti osobní povahy nebo zvukového či obrazového záznamu nesmí být využit nepřiměřeným způsobem v rozporu s oprávněnými zájmy člověka.“ [4]

Občanský zákoník rozšiřuje soukromí i o podobiznu člověka. Jedná se o jakýkoliv obrazový či zvukový záznam. Toto je velmi důležité, například při tom, kdy se za nás chce někdo vydávat, falešně nás pomlouvat, vytvářet s naší podobiznou a osobními údaji falešné doklady atd. [2]

Dalším důležitým bodem je i narušení soukromí. Nikdo nemá právo náš soukromí život ani nikterak sledovat a zasahovat do něj bez našeho svolení. [2]

1.1.3 Trestní zákoník

Postihy a sankce za narušení soukromí člověka vymezuje Trestní zákoník. Jedná se o předpis trestního práva hmotného. Stanovuje, které chování je trestné a jak za ně bude viník

potrestán. Trestnými činy proti narušení práva na ochranu soukromí a osobnosti se zabývá v druhé části Hlavy 2, dílu 2. Konkrétně v paragrafech §180 - §184. [2]

Trestné činy proti právům na ochranu osobnosti, soukromí a listovního tajemství

Neoprávněné nakládání s osobními údaji je podle trestního zákoníku právo na ochranu před nedovoleným zveřejňováním osobních údajů a jejich zneužíváním. Jedná se se tedy o ochranu části osobnosti člověka, která se pojí s právem na soukromí. [2]

„*§180*

Neoprávněné nakládání s osobními údaji

(1) *Kdo, byť i z nedbalosti, neoprávněně zveřejní, sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje, které byly o jiném shromážděné v souvislosti s výkonem veřejné moci, a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají, bude potrestán odnětím svobody až na tři léta nebo zákazem činnosti.*

(2) *Stejně bude potrestán, kdo, byť i z nedbalosti, poruší státem uloženou nebo uznanou povinnost mlčenlivosti tím, že neoprávněně zveřejní, sdělí nebo zpřístupní třetí osobě osobní údaje získané v souvislosti s výkonem svého povolání, zaměstnání nebo funkce, a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají.“* [5]

U poškození cizích práv, jsou objektem nemajetková práva subjektu. Trestný čin spočívá v spáchání vážné újmy na právech jinému tím, že někoho uvede v omyl nebo jeho omylu využije. Pokud se jedná o uvedení v omyl, jedná se o jednání, kdy pachatel předstírá okolnosti, kteří neodpovídají skutečné věci. O využití omylu se jedná v případě, že pachatel nikoho sám v omyl neuvedl, ale poznal, že dotyčný jednal v omylu a využil ho k poškození dotyčného. [2]

„§181

Poškození cizích práv

(1) *Kdo jinému způsobí vážnou újmu na právech tím, že*

a) *uvede někoho v omyl, nebo*

b) *využije něčího omylu,*

bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti.“ [5]

Porušení tajemství dopravovaných zpráv, se týká jen zpráv zaslaných poštou, dopravním zařízením, nebo telefonem. Ochrana je poskytována bez ohledu na hodnotu této zprávy. Zprávy, které již byly doručeny adresátovi, této ochraně nepodléhají. [2]

„*§182*

Porušení tajemství dopravovaných zpráv

1) *Kdo úmyslně poruší tajemství*

a) *uzavřeného listu nebo jiné písemnosti při poskytování poštovní služby nebo přepravované jinou dopravní službou nebo dopravním zařízením,*

b) *datové, textové, hlasové, zvukové či obrazové zprávy posílané prostřednictvím sítě elektronických komunikací a přiřaditelné k identifikovanému účastníku nebo uživateli, který zprávu přijímá, nebo*

c) *neveřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému, přenášejícího taková počítačová data, bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti.“* [5]

Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí. Objektem trestné činnosti jde zde ochrana písemností, záznamů, nejrůznějších počítačových dat ukrytých v soukromí. Vztahuje se na písemnosti a data soukromé i profesní povahy. Trestný čin spočívá v jednání pachatele, který poruší tajemství listiny, nebo písemnosti fotografie, videa či jiného záznamu, počítačových dat a dokumentů uchovaných v soukromí, tím že informace zpřístupní nebo je jiným způsobem použije. [2]

Další možností je, že pachatel tento trestný čin spáchá za účelem získat tyto informace pro sebe, nebo pro někoho jiného a získat tím majetkový nebo jiný prospěch. Dále způsobit jinému škodu, nebo ohrozit jeho společenskou vážnost. [2]

„§183

Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí

(1) *Kdo neoprávněně poruší tajemství listiny nebo jiné písemnosti, fotografie, filmu nebo jiného záznamu, počítačových dat anebo jiného dokumentu uchovávaného v soukromí jiného tím, že je zveřejní, zpřístupní třetí osobě nebo je jiným způsobem použije, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci.“* [5]

Objekt tohoto trestného činu je čest, dobrá pověst a vážnost člověka. Stránka trestného činu spočívá v tom, že pachatel o jiném sdělí nepravdivou informaci, která značnou měrou ohrozí dotyčného společenskou vážnost, ohrozí jej v zaměstnání, naruší jeho rodinné vztahy, nebo způsobí jinou právní újmu. K naplnění podmínek trestné činnosti se nevyžaduje, aby došlo k ohrožení vážnosti u spoluobčanů, postačí, že tato informace je nepravdivá. [2]

„§184

Pomluva

***(1)** Kdo o jiném sdělí nepravdivý údaj, který je způsobilý značnou měrou ohrozit jeho vážnost u spoluobčanů, zejména poškodit jej v zaměstnání, narušit jeho rodinné vztahy nebo způsobit mu jinou vážnou újmu, bude potrestán odnětím svobody až na jeden rok.*

***(2)** Odnětím svobody až na dvě léta nebo zákazem činnosti bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem.“* [5]

Trestní zákoník vymezuje tresty za narušení soukromí, přesněji než Listina základních práv a svobod. Občanský zákoník vymezuje, co je prohřeškem proti soukromí. Ošetřuje neoprávněné nakládání s osobními údaji a už jen jejich sdělení nebo umístění na veřejný prostor je trestným činem.

Vymezuje i to, že nikdo nemá právo nijak získat listiny, počítačové dokumenty apod. uchovávané v soukromí. Trestným činem není jen jejich použití za nějakým účelem obohacení se, ale i jejich zveřejnění, nebo snaha o to je nějakým způsobem získat.

Dalším důležitým prvkem pro ochranu soukromí je to, že se zabývá i ctí člověka. Pomluvy a nepravdivé výroky můžou mít veliký dopad na život člověka a jedná se o narušení jeho soukromí. V dnešní době sociálních sítích je šíření pomluv velice jednoduché a nese sebou veliké následky. Lidi využívají pomluvy zejména ze msty, za účelem člověka zdiskreditovat, nebo při nekalém konkurenčním boji.

1.1.4 General data protection regulation

Ochrana soukromí a soukromých informací je velmi obsáhlá a esenciální, vedle Listiny základních práv a svobod, Občanského zákoníku a Trestního zákoníku je dále soukromí upravováno dalšími speciální právní předpisy. Zejména je potřeba zmínit General Data Protection Regulation (GDPR), které se zabývá ochranou osobních údajů. GDRP naplňuje ochranu soukromí tím, že každý jedinec se může rozhodnout, s kým své soukromí bude

sdílet. To platí i pro ochranu osobních údajů, které jsou významnou podmnožinou ochrany soukromí. [2]

GDPR je „Obecné nařízení o ochraně osobních údajů“ zejména při jejich zpracování firmami. Toto nařízení představuje nový právní rámec ochrany osobních údajů v celém prostoru Evropské unie. Autorem tohoto nařízení je Evropský parlament a Evropská rada. Nařízení bylo schváleno 27. května 2016 a v České republice je platným od 25. května 2018. Nařízení nahradilo zákon č. 101/2000 Sb. o ochraně osobních údajů, který byl následně 24. dubna 2019 zrušen a plně nahrazen obecným nařízením GDPR. [6]

Důvodem k nahrazení zákona č. 101/200 sb. o ochraně osobních údajů, bylo, že již byl zastaralý a neodpovídal současné době. Zejména pokud se jedná o prostředky, které jsou při zpracování osobních údajů využívány. Dále zpracování osobních údajů je mnohem komplexnější, než tomu bylo dříve. Dalším důležitým aspektem k vytvoření jednotného nařízení bylo sjednocení právní úpravy což před platností GDPR správcům osobních údajů jednotlivých zemí činilo problémy. Cílem tohoto nařízení je přizpůsobení právního rámce dnešní době a dosažení jednoty právního rámce, v celém Evropském prostoru. [7]

Osobními údaje, které GDPR chrání, chápeme jako veškeré informace o fyzické osobě, díky kterým ji lze přímo či nepřímo identifikovat. Mezi tyto údaje řadíme zejména:

- Jméno a příjmení
- Datum narození
- Věk
- Pohlaví
- Rodinný stav
- E-mail
- Telefon
- Fotografie
- Genetické údaje
- Biometrické údaje
- Obrazové a zvukové záznamy, lokační údaje a další charakteristiky

- IP adresu, která, je osobním údajem od okamžiku, kdy ji lze konkrétním člověkem
- Podobně cookies a veškeré další údaje o chování uživatele na webu v případě, že je cíleně monitorován [8]

GDPR dává člověku právo vědět, jak s těmito údaji bude nakládáno. Těmito právy jsou zejména právo na přístup, opravu, výmaz, právo být zapomenut, právo na omezení zpracování a právo vznést námitku. Každý občan bude mít právo být informován o tom, za jakým účelem se jeho osobní údaje zpracovávají, po jakou dobu budou tyto informace uchovány a také musí znát příjemce svých osobních údajů. [9]

GDPR také ukládá firmám povinnost správně zpracovávat osobní údaje. Firmy jsou zodpovědné a povinné zavést technická a organizační opatření za účelem prokázaní, že veškeré zpracování osobních dat je v souladu s GDPR. Týká se to zejména těchto oblastí:

- *„implementace záměrné a nezbytné ochrany dat*
- *vypracování posouzení vlivu na ochranu osobních údajů, v angličtině DPIA neboli Data Protection Impact Assessment*
- *jmenování pověřence pro ochranu osobních údajů neboli DPO (Data Protection Officer)*
- *zavedení tzv. pseudonymizace osobních údajů*
- *vedení záznamů o činnostech zpracování*
- *konzultace s dozorovým orgánem před samotným zpracováním osobních údajů“*

„Výjimky z povinnosti vést záznamy o činnostech zpracování lze uplatnit pro organizaci s méně než 250 zaměstnanci, pokud zpracování osobních údajů není jejich hlavní činností, neexistuje u nich riziko pro práva a svobody osob a tyto organizace nezpracovávají citlivé údaje.“ [10]

GDPR také nařizuje sankce za porušení nařízení. Týká se nejen porušení, ale i nezavedení či nepřipravenosti nařízení vykonávat. GDPR nedopadá na fyzické osoby a příslušné orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů. [9]

1.2 Dílčí závěr

Každý z nás má právo na své soukromí. Jedná se o jedno ze základních lidských práv, v České republice to dokládá například Listina základních práv a svobod, kde je právo na soukromí ukotveno hned ve dvou článcích. V článku 7, který zaručuje nedotknutelnost osoby a jejího soukromí a v článku 10, který zaručuje právo na ochranu soukromého života.

Další dílčí práva jsou garantovány občanským zákoníkem, kde jsou jednotlivá dílčí práva na ochranu soukromí a osobnosti vymezeny poměrně obecně. Ochrana soukromí se dynamicky vyvíjí, zejména kvůli masivnímu používání moderních technologií, nejrůznějších telekomunikačních prostředků a sociálních sítí. Jednotlivé zákony v Občanském Zákoníku nenaplňovaly právo na soukromí, jako ho vnímáme dnes.

Zejména kvůli tomu jak se soukromí vyvíjelo spolu s moderními technologiemi, bylo zapotřebí vyvinout i právní nařízení na ochranu soukromí, které by odpovídalo současným trendům. Právě kvůli tomu, že ochrana soukromí a zejména osobních údajů neodpovídala dnešní době, bylo přijato nařízení GDPR, které má sloužit k lepší ochraně soukromí a osobních údajů v moderním světě. S GDPR se zlepšila informovanost lidí, jak je s jejich osobními údaji zacházeno a manipulováno. Ovšem prozatím nezvýšilo ochranu soukromí, protože osobní údaje o uživatelích mohou být stále shromažďovány, pokud s tím uživatel souhlasí ve smluvních podmínkách. S těmito smluvními podmínkami ovšem uživatel „musí“ souhlasit, pokud chce dané služby nadále používat.

2 OCHRANA SOUKROMÍ JAKO SPECIFICKÝ DRUH BEZPEČNOSTI

Soukromí člověka a to převážně ve virtuálním světě, je mnohem přístupnější než dříve. Téměř každý člověk používá internet, nakupuje online, využívá sociální sítě a komunikuje přes emaily. Všechny tyto aktivity za sebou zanechávají soukromé údaje o uživatelích. Těmto údajům se říká digitální stopy. Jedná se digitální stopy po našich aktivitách v kybernetickém prostoru. Tyto stopy za sebou uživatel zanechává vědomě, formou vyplnění profilu na sociálních sítích, aktivitou v diskuzích, vyplňováním registračních karet při online nakupování, nebo registrací na různé weby. Ovšem ne všechny digitální stopy jsou zanechané vědomě, ale i nevědomě, například ukládáním cookies apod. Údaje, které za sebou uživatel zanechá vědomě vlastní činností, například vyplnění profilu osobními údaji, jsou dobře dohledatelné a snadno zneužitelné, například pro kopii identity člověka. Digitální stopy, které jsou zanechány nevědomě aktivitou na internetu, bývají často prodávány společnostem, například pro reklamní účely.

2.1 Příčiny k ochraně soukromí

Nejdůležitější příčinou k ochraně soukromí je snadné zneužití identity a velmi jednoduché vyhledávání osobních údajů, zejména na internetu. Osobní údaje absolutně nahradily osobní přítomnost člověka. Ke komunikaci používáme sociální sítě, které obsahují naše osobní údaje, při nakupování na internetu rovněž vyplňujeme registrační karty s osobními údaji. Zásadní příčiny k ochraně soukromí jsou zejména:

- Zanechávání digitálních stop
- Snadný přístup k digitálním stopám
- Neopatrnost na sociálních sítích
- Snadné zjištění polohy, IP adresy apod.
- Nezabezpečené internetové stránky s osobními údaji uživatelů
- Snadný přístup k digitálním stopám (soukromým údajům)
- Jednoduché zneužití digitálních stop
- Možnost vytvoření hodnověrné verze identity jinou osobou

Dříve bylo zjištění a následné zneužití osobních údajů mnohem složitější. Pokud někdo chtěl získat osobní údaje, musel se vloupat do nějakých státních registrů na úřadech, nebo fyzicky zasáhnout do fyzického života osoby a osobní údaje ukrást, například krádeží občanského průkazu. Dnes jsou tyto informace dostupné na internetu, formou digitálních stop, kterou za sebou zanechává každý uživatel internetu. S jednodušším přístupem k osobním údajů souvisí i jejich snadnější zneužití. U mnoha úkonů již není potřeba osobní přítomnost jedince, tudíž stačí jeho virtuální identita, která je díky výčtu příčin výše snadno zneužitelná.

2.2 Zanechávání digitálních stop

Jakákoliv činnost v kyberprostoru za sebou zanechává stopu, v tomto případě digitální stopy. Jedná se o informace o uživateli, které za sebou zanechává při surfování na internetu, vyhledávání na Googlu, prohlížení si Facebooku, nebo online nakupování. Zkrátka při kterékoliv činnosti, vykonané ve virtuálním prostoru. Jedná se o záznamy o činnosti uživatele ve virtuálním prostředí, které nazýváme digitální stopa. [11]

Tyto digitální stopy se ukládají jak v zařízení, které uživatel používá (PC, mobilní telefon, tablet apod.), tak i ve virtuálním prostředí formou příspěvků na sociálních sítích, prostřednictvím webových stránek, diskuzí pod internetovými články, vlastních vlogů a blogů, ale i při online nákupech. Tyto údaje jsou často ukládaný, bez přímého souhlasu uživatele. O tyto digitální stopy je důležité se zajímat, protože tvoří počítačovou identitu každého uživatele internetu a jsou mnohdy snadno dohledatelné a zneužitelné. [11]

2.2.1 Dělení digitálních stop

Digitální stopy dělíme do několika kategorií, zejména podle toho kdo digitální stopu vytvořil.

Vlastní

Jedná se digitální stopu, kterou za sebou uživatel za sebou zanechal vlastní aktivitou ve virtuálním prostředí. Jedná se o nejčastější případ zanechání digitální stopy. Digitální stopu za sebou můžeme zanechat vědomě, respektive vědomou činností. Mezi takové činnosti patří:

- Aktivita na sociálních sítích
- Přispívání do internetových diskuzí a fór
- Vkládání fotografií do fotobank a sociálních sítí

- Emailová komunikace a posílání zpráv přes aplikace [11]

Nevědomá

Vzniká společně s vědomou digitální stopou. Jedná se o digitální stopy, které jsou ukládány bez činnosti uživatele a jeho vědomého přímého uložení, ukládají se automaticky. Jedná se o údaje o našem zařízení, z kterého přistupujeme k internetu, počítačové sítě a užívané online služby.

- Vyhledávané výrazy na internetu
- Údaje o činnosti na webové stránce a strávený čas na webové stránce (cookies)
- IP adresa
- Naše lokace, poskytovatel připojení apod. [11]

2.2.2 Digitální informace zanechána cizím uživatelem

I přesto, že uživatel si dobře chrání své soukromí a záměrně nikde sám nedává příspěvky, své fotografie s geografickou polohou apod., může být označen na fotografii někoho ze svých přátel na sociálních nebo být zmíněn v některém jeho příspěvku. Tímto o nás může prozradit například naši geografickou polohu, nebo s kým se nacházíme. Dále může i další přátele a narušit naše soukromí tím, že se tyto informace rozšíří mimo okruh našich přátel. [11]

Digitální stopy nemusí šířit jen známí a přátelé, ale i uživatelé internetu s cílem druhého poškodit. Můžou kdekoliv na internetu psát nepravdy, podávat zkreslené informace o druhých, nebo jinak poškozovat dobré jméno druhého. Všechny informace, které jsou jednou na internetu zveřejněné, už nelze absolutně odstranit. [11]

Všechny tyto digitální informace lze dále dělit podle toho, jak je lze dohledat.

- Veřejné (informace, které může kdokoliv vyhledat, například pomocí vyhledávače)
- Neveřejné (informace, které vyhledá jen okruh lidí, které určíme)
- Skryté (cookies a ostatní informace o zařízení, poskytovateli internetu apod. [11]

2.2.3 Metadata

Metadata jsou data o datech. Jakýkoliv soubor, který uživatel vytvoří, sebou nese o sobě informace, respektive metadata. Jedná se o soubor údajů, v nichž je zapsáno, kdy a kým byl

soubor vytvořen, kdy a zda byl soubor nějak upraven, mnohdy i kým byl vytvořen. Tato metadata obsahují i všechny fotografie a obrázky. Metadata ve fotografiích jsou uložena v EXIF tabulce a lze z nich vyčíst model fotoaparátu, výrobce fotoaparátu, citlivost ISO, ale i GPS souřadnice, nebo užití blesku. [11]

Metadata ovšem neobsahují jen fotografie a soubory, ale i například emailová zpráva. Emailová hlavička obsahuje údaje o IP adrese odesílatele a příjemce a údaje o dalších serverech, kterými zpráva prošla. Všechny tyto údaje jsou součástí digitální stopy uživatele. [11]

2.2.4 Veřejně dostupné osobní údaje

Nyní jsou osobní údaje pro všechny mnohem přístupnější. Ať už se jedná údaje, které o sobě dobrovolně vystavíme sami například na sociálních sítích, nebo údaje, které jsou dostupné na různých webových stránkách, kde je velké množství osobních údajů snadno dohledatelných.

Klíčové je chránit si takové osobní údaje, které se dají nahlásit do různých smluv při kontrole identity, například revizorům, bankovním účtům apod. Důležitá je ochrana rodného čísla, adresy trvalého bydliště, a pokud je to možné i jména a příjmení. Někteří občané, zejména podnikatelé, mají v tomto situací značně ztíženou kvůli aktivitám Ministerstva spravedlnosti a Ministerstva průmyslu a obchodu. Jejich osobní údaje jako adresa bydliště, nebo datum narození jsou volně dostupné v živnostenském rejstříku. [12]

Nejčastěji se zadávají osobní údaje při online nakupování, věrnostních programech apod. Uživatel by měl dávat dobrý pozor, jestli webové stránky používají šifrování při zadávání údajů do registračních formulářů. [12]

Nejnebezpečnější je právě shromažďování těchto osobních údajů, kdy je pachatel schopný z několika zdrojů poskládat celou identitu člověka.

Všechny tyto digitální stopy, které jsou volně dostupné, nebo jsou součástí cookies webových stránek. Jsou to soukromé informace, které jsou často využívány bez vědomí uživatele. Jedná se o absolutní ztrátu soukromí, kdy z jednotlivých částí těchto digitálních stop, může být vytvořena celistvá identita uživatele. Ovšem krádež identity není jediný způsob, jak jsou tyto stopy zneužívány. Tyto digitální stopy, cookies a metadata slouží k mnoha dalším účelům.

2.3 Důsledky zneužití digitálních stop

Soukromí má obrovský markentingový potenciál a jsou to velmi ceněné informace, které dokáží doslova hýbat s moderním světem manipulace. Ve většině případů se nejedná o sběr údajů s cílem uživateli nějak uškodit, minimálně co se týká po fyzické a psychické stránce, nejčastěji je zajímají pouze naše finance, respektive vůle peníze utratit. Ale jsou využívány i pro určitý druh psychické manipulace, ale samozřejmě zneužívány i jednotlivci za účelem někoho pošpinit, nebo mu jinak způsobit újmu.

2.3.1 Reklamní účely

Jedná se o nejčastější sběr osobních údajů, kterého si určitě všiml, každý uživatel internetu. Pokud do vyhledávače zadáme například dětské hračky, systém sběru informaci automaticky vyhodnotí, že ve svém okolí máme malé dítě a začne nám v reklamních banerech automaticky podbízet dětské hračky, dětské oblečení a vše spojené s dětmi. Ovšem okruh tohoto reklamního zájmu je obrovský. Snaží se dělat i určité databáze lidí, tříděných podle jejich potřeb. Vyhodnotí například, že ten kdo si koupí levnější mobil, nebude prahnout po drahém a luxusním oblečení a automaticky mu ho nenabízí, ale nabídne mu to, co si nejčastěji kupovali uživatelé mobilního telefonu daného typu. Možná to působí neškodně, ale je to obrovský monitoring masy lidí. Odborný název pro tento druh reklamy je behaviorální reklama. Nejedná se o nic jiného než o sběr osobních informací a jejich využití za účelem prodeje produktů. [13]

Některé webové stránky používají i nástroj zvaný Google Analytics, která jeho uživatelům poskytuje další osobní informace o uživatelích. Lze se dozvědět i z které stránky uživatel navštívil danou stránku, jak dlouho se na webu zdrželi, nebo klíčová slova použitá při vyhledávání. Můžeme se z aplikace dozvědět i AP adresu návštěvníka, jeho přibližnou polohu, nebo i poskytovatele internetu a jméno prohlížeče. [13]

2.3.2 Nekalé úmysly

Sběr informací bohužel neslouží jen pro reklamní účely. Zde se již nejedná o souhrnné sbírání informací veliké masy lidí, ale o vybrané jedince. Může se jednat například o cílené sledování, diskreditaci, omezování, nebo o nekalou konkurenci a v krajních mezích i přímo vydírání. Speciálním příkladem vydírání může být i stále více častější kyberšikana, která je z velké části založena na tom, že dotyčný má nějaký soukromý materiál na poškozeného a pomocí něho ho vydírá a nutí k nejrůznějším věcem. [13]

Ke sběru soukromých údajů mohou být použity i soukromé agentury, nebo takzvaná soukromá očka. Ať už se jedná o zjištění toho, jestli je zákazníkova manželka nevěrná, nejrůznější konkurenční boj, nebo například i politický zájem. [13]

2.3.3 Státní zájem

Jedná se o sledování na státní úrovni vykonávané policií, nebo zpravodajskými službami. Zde se jedná například o sledování potenciálních teroristů, mapování jejich pohybu, kontaktů, trávení volného času atd. Dále nejrůznější mapování zločineckých kruhů, prodeje drog atd. Toto sledování má samozřejmě vesměs pozitivní dopad, ale může vyústit třeba jako ve Francii listopadu 2015 v domovní prohlídky bez soudního příkazu. Tyto domovní prohlídky nastaly po sérii teroristických útoků. Nejrůznější zákazy vycházení v určitých hodinách a podobné zákroky mohou ovlivnit soukromé životy všech. Ovšem nutno přijmout, že toto narušení soukromí je nutné pro naši bezpečnost. [13]

2.3.4 Volební kampaně

Politické strany, předsedové stran, ale například i kandidáti na prezidenty potřebují před volbami rozjet vhodnou politickou kampaň. Vytypovat si svou zájmovou skupinu a zjistit co zajímá, čím se zabývají, co netolerují a na čem si zakládají. Jaké mají prostředí, cokoliv. Všechny volební kampaně jsou založeny na mapování soukromí jejich voličů, aby věděli jak svou kampaň postavit. Snaží se nejrůzněji s psychikou manipulovat, aby volič dal hlas právě jim. Jedná se o podobný systém mapování soukromí jako při behaviorální reklamě, s tím rozdílem, že jejich cílem není, aby se nakoupilo zboží prodejce, ale aby získali nové voliče. [14]

2.4 Ochrana soukromí

Česká legislativa disponuje mnoha zákony a nařízeními, které může použít při ochraně osobních údajů, zejména jejich zpracováváním. Nejvyšší úroveň má na tomto vyhláška GDPR, která nahradila zákon o ochraně osobních údajů. Ovšem i přes tyto nařízení dochází k narušení soukromí. Jako příklad lze uvést použití soukromí uživatele pro inteligentní reklamu.

Google pomocí své služby Google Analytics cíleně zneužívá soukromí uživatelů pro inteligentní reklamu. Cíleně sleduje záliby uživatelů, co vyhledávají, monitoruje jejich lokaci dokonce i IP adresy uživatelů a s těmito údaji dále obchoduje. Samozřejmě pokud si všimneme smluvních podmínek Googlu, tak s tímto plně souhlasíme a je veřejně dostupné,

jak toto shromažďování osobních údajů funguje. Při instalaci Google chrome, ale při prvním použití Googlu, souhlasíme se smluvními podmínkami. Kdy dovolujeme Googlu tyto informace použít, výměnou za to, že tyto služby budeme využívat. [15]

Google shromažďuje následující údaje:

- Aktivita (vyhledávané dotazy, informace o zvuku při používání služeb, aktivita na webech, historie prohlížení chromu)
- Informace o poloze pomocí GPS, IP adresy, senzorů ze zařízení apod. (rozsah zjištění polohy lze ovlivnit například vypnutím zjišťování polohy zařízení)
- Informace z veřejně dostupných zdrojů (například jméno v novinách, kdy Google bude tento článek indexovat a poskytne ho někomu, kdo do vyhledávače zadá jméno tohoto uživatele) [16]

Ke shromažďování používá nejrůznější technologie jako cookie, pixelové značky, webové prohlížeče, mezipaměť dat a aplikací, databáze protokolů. S tímto vším uživatel souhlasí, při smluvním potvrzení, které Google vyžaduje při používání jeho služeb. Google dále ve smluvních podmínkách varuje, abychom při vyhledávání nijak nepoužívali své vlastní osobní údaje, aby nedošlo k jejich uložení a následnému použití. Pokud uživatel někdo tyto osobní zadává, tak na vlastní nebezpečí. Tato data jsou používána zejména pro reklamní účely. Google sám o sobě naše osobní údaje neprodává, protože klienti (firmy) platí za to, aby mohly na Google reklamu umístit a pak Googlu, který tyto údaje vlastní rozhoduje, který obsah kterému uživateli ukáže. [16]

Reklama není hrozba pro uživatele, ale není zcela zřejmé, že tyto údaje, které jsou shromažďovány, nebudou nikdy zneužity. Dalším problémem je to, zda ti co údaje shromažďují, je dokáží uchránit před ostatními. Únik soukromých údajů je obrovskou hrozbou.

2.5 Ochrana soukromí jako druh bezpečnosti

V tomto případě lze ochranu lze jen velmi obtížně řídit. Uživatelé s tímto používáním osobních údajů souhlasí. Při registraci na sociální sítě, při schválení licence Googlu apod. Jediným řešením absolutní ochrany soukromí na internetu by bylo internet nepoužívat vůbec, což je v dnešním světě nereálné. Lze zde jen dbát doporučení a své osobní údaje nezveřejňovat nikde, kde to není nutné, nebo o nich dokonce na sociálních sítích apod. lhát.

Nezveřejňovat své fotografie se snadnou lokalizací a neusnadňovat tím nikomu snáze se dostat do našeho soukromého života.

2.5.1 Opatření pro ochranu soukromí

Kontrola vlastní digitální stopy

Digitální stopu za sebou nejde úplně zamést, pokud chceme používat internet pohodlně a plnohodnotně. Existují nástroje pro minimalizaci digitální stopy, jako jsou anonymní proxy servery, prohlížeče, anonymní režimy, pluginy do prohlížeče, které se snaží digitální stopu uživatele nevytvářet, mazat cookies po každém kroku atd. Ale ani tato opatření nedokáží digitální stopu zcela odstranit. [11]

Kontrola smluvních podmínek

Při ochraně soukromí je důležité kontrolovat smluvní podmínky. Pokud chceme něco na internetu používat, je potřeba si pročíst všechny smluvní podmínky, abychom se ujistili, že s našim soukromím budou nakládat, tak, jak si to představujeme.

Opatrnost na sociálních sítích

Sociální sítě jsou pravděpodobně na začátku každého narušení soukromí. Pokud chce pachatel oběť sledovat, nejprve začne na sociálních sítích. Na sociálních sítích mají lidé i osobní údaje, fotografie s místem kde se nachází, kde bydlí a podobně. Pro ochranu soukromí je naprosto důležité, dát na sociálně sítě jen to, co nebude nikdo moci použít proti nám. [17]

Vyplňování osobních údajů

Kamkoliv se registrujeme, nebo si něco objednáváme, musíme si být jisti, že jsou tyto webové stránky spolehlivé a bezpečné. Nikdy nevyplňovat žádné osobní údaje do formulářů, které nám chodí například přes emaily. Tyto podvodné emaily často slouží ke krádežím identity apod. [17]

Testování

Nejjednodušší možnost jak otestovat soukromí a jeho zabezpečenost, je zkusit vyhledat sama sebe. Pokud pomocí vyhledávače o sobě uživatel nalezne velké množství osobních údajů, které by se daly následně zneužít, měl by se to pokusit vyřešit. Pokud je to možné měl by sám zkusit tyto údaje odstranit. Pokud k těmto údajům nemá přístup, zkusit využít práva být zapomenut. [17]

2.6 Atributy soukromí a jeho aktiva

Soukromí je velmi těžké vymezit a určit co vše do něj spadá. Neexistuje žádný zákon, ani nařízení, které by jej přímo vymezovalo. Zde jsou nejdůležitější atributy, které tvoří soukromí osoby. Vybrány byly zejména ty atributy soukromí, které mají pro člověka nějakou hodnotu a při jejich narušení může nastat nějaký fyzický, nebo psychický dopad na člověka. Dále se jedné o ty údaje, které mají pro člověka, nebo pro pachatele určitou finanční hodnotu a tyto údaje lze nadále zneužít v pachatelův finanční prospěch.

2.6.1 Osobní údaje

Definicí a tím co spadá do osobních údajů, se tato práce zabývá již v kapitole o GDPR. Jedná se o údaje, podle kterých lze identifikovat danou osobu. Lze jsem zařadit i například emailovou adresu, telefonní číslo, ale i nejrůznější identifikační údaje vydané státem. [2]

2.6.2 Soukromé prostory

Soukromý prostor je prostor, který je ve vlastnictví soukromých osob. Přístup a pohyb je omezený na souhlas vlastníka. Patří do našeho soukromí a nikdo nemá právo v těchto prostorech narušovat naše soukromí. [2]

2.6.3 Soukromý život

Mezi důležitý atribut našeho soukromí patří i soukromý život, o kterém nelze pořizovat zvukové a obrazové záznamy a ty dále šířit nebo s nimi neoprávněně nakládat [2]

2.6.4 Fotografie

Všechny fotografie, na kterých je zachycena naše podobizna, nesmějí být nijak použity bez našeho svolení. To samozřejmě platí i o zvukových záznamech. Nezáleží na tom, zda je zvukový záznam přímo z našeho soukromého života, nebo například zachycený pracovní pohovor nebo rozhovor na ulici. Ve všech případech se jedná o část našeho soukromí a nesmí být bez našeho souhlasu nijak využíván. [2]

2.6.5 Soukromé písemnosti osobní povahy a tajemství listovní

Pojmově do této skupiny nespadají písemnosti například pracovního charakteru, ale podle Listiny základních práv a svobod je ochrana písemnosti chráněna i tam kde korespondence má pracovní charakter. To samé platí i pro zvukové projevy osobní povahy. Projevy osobní povahy jsou také součástí soukromí. S ustanovením §87 mohou být písemnosti osobní

povahy šířeny jen se souladem autora. Písemnosti osobní povahy jsou chráněny i ustanovením trestního zákoníku §182 Porušení tajemství dopravovaných zpráv a dále ustanovením §183 Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí. [2]

2.6.6 Písemnosti, dokumenty, počítačová data uchovávaná v soukromí

Jedná se o všechna data, která uchováváme u sebe. Může se jednat o nejrůznější fotogalerie, textové dokumenty jakékoliv povahy, videa. Samozřejmě se to nevztahuje jen na data v počítači, ale i na písemnosti, které uchováváme v soukromí. Může se jednat o nejrůznější plány, smlouvy, ale třeba i deník. [2]

2.6.7 Předávání zpráv telekomunikačními prostředky

Předávání zpráv telekomunikačními prostředky zajišťuje, že zpráva musí dojít jen příjemci, kterému byla odeslána a nebude nijak změněna její podoba. Platí to i pro číslo mobilního telefonu a IP adresu. [2]

2.6.8 Nedotknutelnost obydlí

Nedotknutelnost obydlí nezahrnuje pouze byt a dům v osobním vlastnictví nebo v pronájmu a místo kde žijeme, ale i například hotelové zařízení, karavany, ale i místa kde jsou vykonávány pracovní aktivity. Nejedná se jen o nepovolený vstup do těchto prostor, ale i nehmotné imise, které narušují možnost poklidně obydlí užívat. [2]

2.7 Dílčí závěr

Tato kapitola se skládá z příčin proč, by měla být ochrana soukromí brána jako nový druh bezpečnosti. Hlavní příčinou k ochraně soukromí je snadné zneužití identity, například k bankovním podvodům. Snadné zneužití identity spočívá zejména v tom, že je jednoduché dohledat osobní údaje o uživatelích, které se dají použít k sestavení identity. Dohledatelné jsou díky digitální stopě, kterou za sebou uživatel zanechává při každém úkonu v kyberprostoru, nebo při používání všech zařízení, která jsou připojena k internetu. Dále jsou v této kapitole rozebrány dopady, které za sebou nese zanechávání digitální stopy.

Nutno říct, že pro vyšší ochranu soukromí, je důležité, aby se každý uživatel, který používá moderní technologie, choval zodpovědně a opatrně. Každá ochrana soukromí by byla zbytečná, pokud by uživatelé nedbaly o své soukromí a nadále dobrovolně zveřejňovali své osobní údaje na sociálních sítích a různých webových stránkách.

Poslední část se zabývá tím, co tvoří aktiva soukromí. Jedná se o jednotlivé složky soukromí, které mají pro člověka nějakou hodnotu a jejich zneužití může mít finanční dopad. Jedné se zejména o osobní údaje, fotografie a dokumenty uchovávané v soukromí, převážně soubory v počítačích a mobilech.

3 OHROŽENÍ SOUKROMÍ

S vývojem technologií přichází i nové hrozby. Svět se změnil, u většiny informačních činností již není zapotřebí osobní přítomnost osoby. Platby probíhají online, registrace, online nákupy. Všechny tyto činnosti jsou vykonávány v digitální podobě. Jako ověření pro tyto úkony neslouží naše osobní přítomnost, ale osobní údaje, které nás nutí zadávat téměř při každém úkonu na internetu, čehož využívají pachatelé.

Příkladem může být krádež identity. V dnešní době je velice snadné vydávat se za někoho cizího. Stačí ze sociálních sítí stáhnout fotografie, shromáždit osobní údaje a vyplnit těmito informacemi falešný profil. I toto stačí ke krádeži identity. V dnešní době je to velice častý jev. Nejvíce se tyto profily využívají k šíření pomluv nebo vydírání.

Krádež osobních údajů ovšem může zajít mnohem dál a být provedena mnohem profesionálněji. Zde už nebude poškozena jen naše čest, ale může to těžce přímo poškodit náš majetek. Může se jednat o nejrůznější falešné objednávky na naše, pokusy využívat naše bankovní účty atd.

3.1 Typologie hrozeb z pohledu ohrožení soukromí

Ve vztahu k narušení soukromí dělíme hrozby do základních skupin, podle toho za jakým účelem a jakým způsobem pachatel narušuje soukromí objektu. Základní typy hrozeb jsou:

- Přímý útok na subjekt (přímé narušení soukromí)
- Shromažďování osobních údajů (a následné zneužití)
- Přímý útok na soukromé údaje subjektu (s následným zneužitím)

Tyto hrozby se dále dělí podle metody provedení, kterou pachatel využije k narušení soukromí na:

- Logické hrozby

Pod pojem logické hrozby řadíme všechny hrozby, které mohou narušit soukromí jedince bez fyzického kontaktu útočníka s obětí, nebo fyzickým narušení jeho soukromé života. Jedná se o nejrůznější formy vytváření nátlaku na uživatele internetu formou vyhrožování, okradení, krádeže jeho virtuální identity, nebo zdiskreditování a zesměšnění osoby.

- Fyzické hrozby

Fyzické hrozby se vyznačují přímým kontaktem pachatele s obětí. Dochází zde ke konfrontacím s obětí, nebo hmotnými aktivy oběti. Jedná se zde převážně o přímé sledování oběti, nebo krádež věcí, které obsahují osobní údaje a soukromé materiály.

3.2 Přímý útok na subjekt

Jedná se o přímý útok na soukromí oběti, kdy pachatel narušuje soukromí jednotlivce za účelem ho sledovat, poškodit jeho pověst, nebo mu způsobit psychické problémy.

3.2.1 Logické hrozby

Logickou hrozbou když pachatel přímo útočí na oběť, jsou nejrůznější formy kyberšikany.

Kyberšikana

Moderní technologie využívá čím dál více lidí, zejména mladistvých, kteří jsou nejčastější obětí kyberšikany. Útočníkům tento prostor poskytuje pocit anonymity, nadvlády a nedotknutelnosti. V krajních případech může kyberšikana vést až k úplné ztrátě soukromí, pocitu lhostejnosti a v nejkrajnějších případech i k sebevraždě. [18]

Pachatelé se při kyberšikaně snaží získat choulostivé údaje o oběti, aby ji mohli následně vydírat, nebo jí způsobit jinou újmu. [18]

Kyberšikana je druh šikany, kdy se pachatel snaží svou oběť psychicky týrat a nějakým způsobem jí ublížit prostřednictvím internetu. Nejčastějšími prostředky kyberšikany jsou sociální sítě, SMS, MMS, interaktivní online hry, jakýkoliv komunikace prostřednictvím internetu (viber, messenger apod.) a emaily. Dále se s kyberšikanou můžeme setkat na různých webových stránkách nebo blozích. Nebezpečí kyberšikany spočívá i v tom, že nemá dopad jen virtuální život ale i osobní život. Následky kyberšikany se prolínají i do osobního a společenského života a můžou vyústit i v klasickou šikanu. Například, že se spolužáci smějí osobně tomu, co o oběti zveřejnili na sociálních sítích. Kyberšikana se na rozdíl od šikany vyznačuje anonymitou, absencí fyzické konfrontace a nezávislostí na místě a čase. [18]

Průběh kyberšikany může být různý, v závislosti na jejím druhu. Začíná většinou velmi nenápadně, protože pachatel si potřebuje získat důvěru své oběti. Většinou se jedná o nejrůznější komentáře fotografií, nezávazným psaním při kterém se nám svěřuje, abychom dotyčnému věřili. Dotyčný ovšem tyto kroky dělá za účelem získání nejrůznějších osobních údajů, soukromých materiálů, nejčastěji intimních fotografií apod. Pachatel si je dobře

vědom, že tyto soukromé informace je velmi jednoduché rozšít do okolního a můžou dotyčnému značně ovlivnit společenský a osobní život. Kyberšikana má více a pachatelé mají s obětí nejrůznější záměry a jejich cíle se různí. [18]

Kyberstalking

Kyberstalking je jedna z nejčastějších hrozeb v kyberprostoru od 1. ledna 2010 je klasifikován jako trestný čin. Je charakteristický tím, že pachatel v tomto případě stalker, neustále obtěžuje svou oběť a sleduje všechny její kroky, může vyústit až k nejrůznějším formám vyhrožování. [18]

Stalker je většinou oběti nějak blízký, například bývalý přítel kamarád apod. Tudíž o obětí ví poměrně hodně soukromých informací, které mu pomáhají v chronickém sledování oběti. Kyberstalking může zajít do krajních mezí, oběti hrozí absolutní ztráta soukromí, ztráta pocitu bezpečí, vyúsťující k pocitům nejistoty a strachu. Oběť se cítí neustále v nebezpečí a začne selhávat i v běžných věcech, které ovlivňují kvalitu jejího každodenního života. [18]

Pro oběť je nejdůležitější rozvázat s dotyčným veškeré kontakty, vyhýbat se mu pokud je to možné a shromažďovat všechny materiály, které by mohly sloužit jako důkazy kyberstalkingu (kopie výhružných zpráv, výpisy hovorů apod.). [18]

Kyberooming

Jeden z druhů kybešikany, při které se agresor snaží nejrůznějšími způsoby manipulovat se svou obětí. Agresor ze začátku opět působí velmi nenápadně a snaží se získat důvěru své obětí dostat se to okruhu blízkých přátel. Poté co se mu to povede, se svou oběť snaží vylákat na osobní schůzku za účelem zneužití oběti (krádež, znásilnění, fyzické napadení apod.). [18]

Kyberooming má několik fází a většina útoků probíhá více méně podobně. Nejdříve si pachatel vybírá svou oběť podle viditelných osobních informací. Zranitelnější jsou lidé, o kterých může získat nejvíce osobních informací. Ty mu pomáhají v druhé fázi, kdy se snaží s obětí navázat kontakt a získat její důvěru. Poté co získá důvěru, následuje třetí fáze a to získání intimních fotografií, nebo soukromých materiálů, pomocí kterých svou oběť může vydírat a nabádat k osobní schůzce, což je čtvrtá fáze. [18]

Nejlepší obranou proti kyberoomingu je nikomu za žádných okolností nezasílat osobní informace a intimní fotografie. Pokud už jsme nějaké osobní materiály poskytli a dotyčný se nás snaží vylákat na schůzku, tak v žádném případě na ni nejít a nereagovat na výhružky

agresora. Dobrým rozpoznávacím znakem těchto agresorů je, že se v průběhu konverzace snaží ujistit, že o konverzaci nikomu neřekneme. [18]

Flaming

Flaming je označení pro agresivní chování, charakteristické urážkami, nadáváním a vyhrožováním. Setkáváme se s ním téměř všude, u fotografií, v diskuzích, nebo přímo v osobní konverzaci. Jediným cílem flamingu je dotyčného anonymně naštvat a ponížit, bez jakéhokoliv trestu. Díky anonymitě se s flamingem na internetu setkáváme 4x častěji než v běžném osobním životě. [18]

Nejlepším způsobem obrany, je na tyto zprávy a komentáře nereagovat. Útočníkovi nejde o naše argumenty, ale pouze o vyvolání hádky a zesměšnění oběti. Nejlepší prevencí je se nezapojovat do vyhrocených diskuzí a udržovat si nadhled. [18]

Sexting

Jedná se o rozesílání vlastních intimních fotografií či videí s intimních obsahem. Ti, kteří se účastní těchto komunikací, riskují zneužití svých intimních materiálů a může opět dojít k vydírání nebo jinému poškození dotyčné osoby. [18]

Obrana je zde stejná jako o kyberoomingu. Za žádných okolností nesmíme nikomu zaslat své intimní fotografie nebo videa, která by dotyčný mohl použít proti nám. [18]

Manipulace za účelem podvodné platby

Internetové bankovnictví nám mnohdy dokáže velmi často zjednodušit život. K zaplacení čehokoliv nám stačí přístup k internetu a mobilní telefon, kterým platbu potvrzujeme. Odpadají potíže s nošením hotovosti, cesty na poštu k vypsání složenky, jednoduše se jedná o velmi jednoduchý a pohodlný platební úkon. Bohužel není jednoduchý jen pro nás, ale i pro pachatele, kteří se díky naší důvěřivosti a znalosti našich osobních údajů snaží obohatit. Velmi zajímavé na těchto případech je, že se nejedná zneužití osobních dat, pouze jednoho člověka nýbrž ve většině případu rovnou dvou.

Pachatelé cílí na osobní údaje, které jsou zapotřebí k přístupu do bankovnictví oběti, které následně zneužije a jménem oběti provádí tyto podvodné platby. [19]

Většinou to probíhá tak, že pachatel zkopíruje profil některého přítele, kterého známe, nebo se nějakým způsobem dostane na originální profil našeho známého. Z tohoto profilu potom chce po poškozených zaslat osobní údaje včetně mobilního telefonu. Většinou svým blízkým věříme, navíc tito lidé jsou velmi vynalézaví a vždy si najdou způsob, aby jejich žádost o

naše osobní údaje vypadala věrohodně. Poté pachatel použije naše telefonní číslo k internetové platbě. Aby mohl tuto provést, je zapotřebí potvrzovací kód, který přijde poškozenému na mobilní telefon. [19]

Pachatelé se v tento moment snaží dostat poškozeného do časové tísně, aby jednal zbrkle v časové tísni a platbu potvrdil. Další možností je, že se snaží o potvrzení pomocí klamu, například že kód potřebují do hry, do které nás chtějí pozvat apod. [19]

3.2.2 Fyzické hrozby

Jedná se o hrozby, kdy pachatel přímo pod nejrůznějšími účelem sleduje svou oběť. Jde o přímo narušení soukromí, kdy pachatel svou oběť sleduje, fotí si ji, zjišťuje, kde se pohybuje, co dělá apod.

3.2.3 Sledování

Sledování, pronásledování, slídění anglicky stalking. Platí zde stejná pravidla jako u kyberstalkingu. Pouze s tím rozdílem, že zde už dochází k fyzickému kontaktu mezi útočníkem a obětí a dochází v něm reálném prostředí. Stalking většinou začíná právě ve virtuální prostředí, prostřednictvím kyberstalkingu, kdy postupně přejde v sledování oběti i mimo virtuální svět a přenáší se do reálného života, kdy dochází k fyzickým kontaktům. Všechny formy stalkingu jsou od 1. ledna 2010 trestným činem. Jedná se o narušení soukromí, kdy pachatel se za každou cenu snaží řídit soukromí oběti. Zajímá ho vše, co oběť dělá, s kým se stýká, kdy a kam chodí apod. [20]

Pachatel stalkingu může být kdokoliv, většinou se převážně jedná o osobu, kterou známe, bývalý přítel, zhrzený kamarád, rozvedený manžel apod. Ovšem když kyberstalking přechází ve stalking, může se stát, že oběť pachatele vůbec nemusí znát, protože pachatel si ji vybral na internetu, nebo se mu oběť zalíbila na ulici apod. Ovšem ve většině případů stalkingu se oběť s pachatelem zná. Což nijak neznevažuje situaci, naopak to dělá věc mnohdy mnohem závažnější, protože stalker zná denní návyky oběti. Zná místa, kde se oběť pohybuje, zná místo kde bydlí, mají společné přátele. [21]

Stalkeři právě svou oběť nejčastěji vyhledávají na místech, kde jsou si jisti, že se pohybuje. Jedná se o její domov, zaměstnání, školu, oblíbenou restauraci apod. Většinou se pachatel snaží se svou obětí navázat fyzická kontakt, nabídnout jí doprovod, nebo jinou pomoc, ale nemusí to být pravidlo. Někteří stalkeři svou oběť, sledují pouze z dálky, popřípadě pořizují její fotografie, nebo poslouchají její rozhovory. Stalkeři často svým obětím i vyhrožují,

například ublížením na zdraví jim, nebo jejich blízkým, usmrcením domácího mazlíčka a dalších forem vyhrožování. [21]

Stalking je ve většině případů dlouhodobá záležitost, která přechází až k vyhrožování. Vyhrožování i stalking jsou trestnými činy, dochází při nich k narušení psychiky osoby, absolutní ztrátě soukromí, kdy oběť ztrácí pocit bezpečí, kdekoliv se pohybuje. Stalking má na oběť zdrcující dopad. Při ztrátě soukromí, dochází ke strachu o svůj život, životy svých blízkých a mnohdy končí absolutním psychickým zhroucením oběti, nebo sebevraždou. [21]

3.3 Shromažďování osobních údajů

Pachatel systematicky shromažďuje osobní údaje o uživateli. Pachatel vyhledává digitální stopy, které po sobě uživatel zanechal na internetu a snaží se je nejrůznějšími způsoby použít ve svůj vlastní prospěch. Pomocí takto získaných údajů může s obětí nejrůzněji manipulovat (kyberšikana, vydírání), nebo se může za uživatele, o kterém shromáždil osobní údaje vydávat. Jedná se o krádež identity za nejrůznějšími účely. Nejčastějším příkladem je krádež identity za účelem nejrůznějších bankovních podvodů.

3.3.1 Krádež identity

Ve vztahu k logickým hrozbám, narušující soukromí se jedná o krádež virtuální identity oběti. Způsobů ke krádeže virtuální identity je více. První z nich je ukradení celého profilu oběti, jeho účtu nebo emailové adresy. Krádež spočívá v zjištění přihlašovacích údajů a následného prolomení hesla k těmto účtům. Největší výhodou tohoto způsobu krádeže identity je, že tyto falešné identity působí velice věrohodně, protože tyto účty a profily vytvořila sama oběť. Pachatel tudíž má přístup ke všem přátelům obětí, osobním údajům na profilu zkrátka vše. Pomocí ukradeného profilu se může pachatel jednoduše vydávat za cizí osobu a manipulovat přátele oběti, například k zaslání peněz na svůj účet apod. [22]

Druhým způsobem krádeže identity je zkopírování profilu, nebo účtu uživatele. Z volně dostupných zdrojů, pomocí digitálních stop a jiných zdrojů osobních údajů, fotografií dostupných na internetu pachatel vytvoří přesnou kopii uživatelského účtu a následně se za svou oběť vydává. Tuto falešnou identitu následně využívá k nejrůznějším činnostem s úmyslem se obohatit, nebo poškodit svou oběť. [22]

Nejčastější využití cizí identity:

- Zdiskreditování oběti (komunikace s jeho přáteli, psaní nevhodných komentářů apod.)

- Získání dat od blízkých oběti
- Vykonávání trestné činnosti jménem oběti
- Zasílání malwerů a phisingových zpráv blízkým oběti
- Získávání informací
- K přístupu do dalších služeb [22]

3.3.2 Krádež identity za účelem bankovních podvodů

Pachatel se zaměřuje na osobní údaje, které jsou zapotřebí k půjčkám, nebo bankovním převodům. Pachatel shromáždí na internetu osobní údaje oběti, založí s jejími údaji bankovní konta, vyrobí falešné doklady identity (občanský průkaz, řidičský průkaz atd.). Na tyto bankovní účty dále jménem oběti uzavře nejrůznější půjčky, které pomocí falešných dokladů vybere a dále nesplácí. Jedná se o krádež identity za účelem obohacení se na úkor oběti. Oběti nemají tušení o tom, že jejich jménem někdo tyto půjčky, někdo založil a vznikají jim tím další problémy se splácením, vymáháním půjček apod. Identity k bankovním podvodům nejsou zneužívány jen pro falešné půjčky. Pachatelé mnohdy zakládají účty na cizí jméno z důvodu praní špinavých peněz. [23]

3.3.3 Manipulace

Dalším důvodem sběru osobních informací, může být manipulace nebo vydírání. Pachatel o oběti shromáždí množství informací za účelem ji k něčemu přimět nebo ji ovlivnit. Může se jednat i o shromažďování informací za účelem nekalé konkurence. [22]

3.3.4 Vydírání

Pachatel sbírá nejrůznější osobní informace o své oběti, jedná se nejčastěji o choulostivé fotografie, informace o blízkých, rodině, záležitostech s dětmi, milenkách apod. Tyto informace následně používá k vydírání oběti. Vytváří na oběť nátlak tím, že vyhrožují vypuštěním těchto informací, nebo je sdělí jeho osobám, před kterými tyto informace tají. Nutí oběť následně dělat činnosti proti své vůli, nebo oběť nutí k poslání peněž. [22]

3.4 Přímý útok na soukromé údaje subjektu

Pachatel přímo útočí na soukromé údaje a materiály oběti. Nejedná se o sběr informací z veřejných zdrojů, ale přímo napadení soukromých údajů oběti, kdy pachatel logicky, nebo fyzicky zaútočí na zdroje osobních údajů a soukromých materiálů. Těmito zdroji je převážně

osobní počítač, mobilní telefon, nebo osobní doklady, které můžou být použity. Pachatel tyto soukromé údaje shromažďuje pro svou vlastní potřebu, vytvoření nátlaku na oběť, nebo je jednoduše získává pro někoho dalšího.

3.4.1 Logické hrozby

Mezi logické hrozby řadíme nejrůznější kybernetické útoky na zařízení oběti za účelem odcizení soukromých materiálů. Tyto útoky jsou prováděny vzdáleně a cílí na počítače a mobilní telefony. Tyto ukradené materiály mohou být dále použity pro krádež identity, nekalý konkurenční boj, nebo manipulaci obětí.

3.4.2 Kybernetické hrozby

Většinu svého soukromí uchováváme ve svých počítačích a mobilních telefonech. Máme v nich uložené své osobní kontakty, soukromé fotografie, dokumenty, zkrátka data našeho mobilního telefonu a počítače tvoří naše soukromí. Kybernetické útoky se netýkají jen naší virtuální identity jako u předešlých hrozeb, ale jedná se přímo o útok na naše aktiva (fotografie, dokumenty, přihlašovací údaje) v našich mobilních telefonech a počítačích. Zkrátka pachatel se snaží získat vzdálený přístup do zařízení oběti a odcizit její soukromé soubory, fotografie, zkrátka vše co se nachází v zařízení. Dalším hrozbou kromě odcizení dat z počítače pro narušení soukromí je nelegální odposlouchávání telefonu, nebo získaní videí pomocí naší webkamery. K výkonu těchto činností k narušení našeho soukromí pachatel používá nejrůznější počítačové viry. [24]

Virus je program, který kopíruje sám sebe do různých spustitelných souborů a dokumentů, které si libovolně upravuje (mění, maže). Nakažení virem není nic příjemného, narušuje programy, zahlcuje operační systém, a sám se šíří a tím dochází ke zhroucení operačního systému a ztrátě dat. Viry se nejčastěji šíří s falešnými přílohami k emailu, v přenosných zařízeních (hry), nebo pomocí webových stránek s pochybným obsahem. [24]

Nejčastější druhy virů:

- Trojský kůň (program, který umožňuje útočníkovi proniknout do PC, působí jako neškodný program, na rozdíl od klasických virů a červů se nekopíruje, sbírá přístupová hesla, jména, čísla k účtům atd)
- Červ (červ nebo anglicky worm se nepozorovaně dostane do našeho PC, bez zásahu uživatele, spouští vzdálené programy a požívá je jako přenašeče)

- Spyware (zaznamenává data o našem pohybu na internetu, projevuje se vyskakováním nežádoucích oken, popřípadě změny domovské stránky)
- Keylogger (běží na pozadí systému, čeká, až vejdeme na stránky, kde zadáváme hesla, a čte jednotlivé klávesy, když zadáváme heslo)
- Phishing (vylákání hesla od nic netušícího uživatele, například emailem)
- Malware (obecný název pro jakýkoliv škodlivý program) [24]

K získání soukromých informací používají pachatelé nejrůznější nástroje. Nejčastějším nástrojem pro tyto účely je sociální inženýrství. Sociální inženýrství je snaha podvodným jednáním od uživatele získat citlivé informace jako jsou hesla, osobní informace, nebo právě přístup k počítači. Sociální inženýrství využívá nejčastěji různých podvodných emailů se závadným obsahem, které nás nutí vyplnit osobní údaje nebo odkazují na stažení nějakého škodlivého programu (malwere, ransormware) pomocí kterého následně pachatel může odcizit naše data. [25]

3.4.3 Fyzické hrozby

Fyzické hrozby se vyznačují přímým kontaktem pachatele s obětí, dochází zde ke konfrontacím s obětí, nebo hmotnými aktivy oběti. Zde se jedná krádeže mobilních telefonů a počítačů za stejným účelem jako byly kybernetické útoky, nebo o krádeže osobních dokladů, díky kterým se za nás může pachatel vydávat, konat naším jménem trestnou činnost apod.

3.4.4 Krádež mobilního telefonu a počítače

Jedná se o stejný princip jako při vzdáleném útoku na počítače a mobilní telefony, pouze s tím, rozdílem že se jedná o přímou krádež zařízení s následným prolomením jeho zabezpečení. Ke vztahu k narušení soukromí a krádeži osobních informací je tato metoda určitě méně používaná, než vzdálené útoky na data v těchto zařízeních. Na druhou stranu může k narušení našich soukromých dat dojít, jako vedlejší produkt krádeže zařízení pro účel prodeje, kdy pachatele primárně nezajímala data v zařízeních, ale přímo zařízení.

3.4.5 Odcizení občanského průkazu a jiných dokladů s osobními údaji

Na občanském průkazu se nachází téměř všechny naše údaje a jedná se o jeden ze způsobů, jak naši identitu lze zneužít. Nejedná se jen o notoricky známé případy, kdy si někdo na nás vezme půjčku, která je vedena na naše jméno. Je zde mnoho způsobů, jak lze osobní doklady

zneužít. Dalšími častými případy zneužití osobních dokladů je například neplacení nejrůznějších drobných pokut například v dopravních prostředích, kdy pachatelé nechávají pokuty psát na cizí občanský průkaz. [26]

3.5 Konkrétní případy narušení soukromí

Narušení soukromí má mnoho podob a případy nejsou ojedinělé ani v České republice. V této kapitole se zaměříme na konkrétní případy narušení soukromí, které se skutečně staly a mohou sloužit jako modelové příklady, proč by si každý měl chránit své soukromí a jak velké dopady může mít narušení soukromí v reálném v životě ve skutečných případech.

3.5.1 Krádež identity a bankovní podvody

V tomto případu figuruje osm mužů z Ostravska, kteří kradli lidem identity za účelem nejrůznějších bankovních podvodů. Případ není nijak jedinečný svým provedením, ale jeho rozsahem. Došlo zde k 189 doloženým krádežím identit a následným podvodům. [27],[28]

Pachatelé odcizovali identity za účelem bankovních podvodů, jménem cizí osoby. Pachatelé vytvořili falešnou identitu, na kterou následně zakládali bankovní účty a přijímali cizím jménem půjčky. Pachatelé si předem zjišťovali, jak velké částky si můžou jménem cizích lidí vypůjčit, aby nemuseli podstoupit detailnější prověrku finančních společností. Při každém jednotlivém podvodu používali pachatelé novou SIM kartu. [27],[28]

Pachatelé své oběti vybírali náhodně na internetu, ale mezi okradenými byli i jejich známí, tudíž měli jednodušší přístup k jejich osobním údajům. Průběh krádeže identity probíhal nejdříve vybráním konkrétní osoby. Všechny údaje o postihnutých pachatelé nacházeli na internetu, kde tyto údaje byly volně dostupné (sociální sítě, veřejné registry apod.). Na základě těchto odcizených údajů pachatelé vyráběli falešné občanské průkazy, zdravotní karty, nebo i řidičské průkazy. Pachatelé dále padělali i výpisy z potvrzení o příjmu a bankovní výpisy. Pomocí osobních údajů a padělaných průkazů zakládali pod jménem obětí bankovní účty s falešnou emailovou adresou. [27],[28]

Na vytvořené bankovní účty pachatelé poté uzavírali úvěry, které pomocí zfalšovaných dokladů vybírali pěšáci této organizované skupiny a následně předali hlavním členům zločinecké skupiny. Na jednoho člověka s ukradenou identitou vytvářeli více půjček, o kterých neměl původní majitel identity potuchy. [27],[28]

Tímto si pachatelé přišli na 6,5 milionů korun a dalších 3,5 milionu se nadále pokoušeli neúspěšně získat. Všech osm hlavních organizátorů se podařilo Policii ČR vypátrat. Hlavě

této skupiny, která byla zapojena do všech dokázaných podvodů, byl vyměřen trest na 6,5 roku nepodmíněně. Další z kompliců byli poslání za mříže na 6 let. Dalším dvěma komplicům byly uloženy tresty ve výši 3 roky a 10 měsíců. Ostatní členové skupiny dostali pouze podmíněné tresty. Do krádeží identit a následných bankovních podvodů bylo nejspíše zapojeno více lidí, které se Policii ČR nepodařilo vypátrat. [27],[28]

3.5.2 Stalking

Druhým analyzovaným případem je případ stalkingu, který se odehrával na Slovensku v letech 2013-2016, jako podklad pro analýzu případu byl vybrán soudní usnesení slovenského soudu Okresný súd Spišská Nová Ves. [29]

Jedná se o nejčastější model stalkingu, kdy se oběť s pachatelem znala. Vedli spolu 3 měsíční vztah, který se rozhodla poškozená roku 2011 ukončit. Posléze se snažili udržet kamarádský vztah, ovšem obžalovaný v tomto případě stalker navyšoval své nároky a proto se s ním oběť rozhodla roku 2013 veškerý osobní kontakt ukončit, protože poprvé pocítila strach a pachatel se začal chovat agresivněji. Po rozvázání osobního kontaktu se pachatel snažil kontaktovat její známé a rodinné příslušníky a vulgárně se vyjadřoval na její adresu. Dále se ji snažil nejrůzněji kontaktovat na sociálních sítích, sledoval ji a znepříjemňoval jí život. Po tomto tlaku se oběť přistoupila k osobnímu setkání, ale pachatel se opět choval agresivně a situace se tím pouze vyostřila. Po osobní schůzce se jí nadále snaží kontaktovat přes sociální sítě, ale i osobně. Vyhledává osoby z jejího okolí, šíří o obžalované pomluvy a vyjadřuje se o ní vulgárně. [29]

Po rozvázání kontaktu ji stalker nadále pronásledoval například i na služební cestě. Stalker ji pronásledoval autem a následně se s obětí setkal v obchodním domě, kde se dožadoval dalšího setkání a po odmítnutí ji fyzicky napadl, oběť uchopil a začal s ní třást. [29]

Situace nadále eskalovala až do bodu kdy stalker přišel přímo k ní domů a oběť mu otevřela. Poté ji vtlačil do bytu, byl agresivní, násilím ji držel a třásl s ní. Po naléhaní a hrozbou zavolání policie, pachatel odešel z domu v moment, kdy se domů vrátil syn oběti. [29]

Obtěžování nadále pokračovalo i na pracovišti oběti, kdy pachatel vícekrát vnikl do kanceláře oběti. Po častém opakování, kdy pachatel způsoboval v kanceláři scény a choval se agresivně, se oběť svěřila spolupracovníkům a poprosila je, aby nadále pachatele nadále nepouštěli dovnitř. [29]

Když stalker nemohl nadále obtěžovat oběť v místě pracoviště, čekal jí před budovou pracoviště, kde jí násilím vzal klíčky od auta a nedovolil oběti odejít. Chtěl jí sebrat i mobilní telefon, ovšem oběť stihla zavolat policii, pachatel před příjezdem policie ovšem odešel. Cestou i incidentu domů si oběť všimla násilníkova auta a bylo jí jasné, že ji nadále pronásleduje. Přesto si šla nakoupit, kde ji násilník opět osobně konfrontoval a slovně jí vyhrožoval, že si na něj dovolila zavolat policii. [29]

Pachatel se často zdržoval v kavárně blízko bydliště oběti, odkud mohl lehce zpozorovat pohyb a předpovídat trasu oběti, v kavárně býval muž spatřen i několikrát denně. Když se pachatel nenacházel v kavárně, snažil se oběť pronásledovat vozidlem, kroužil kolem ní, nebo parkoval blízko jejího bydliště, aby měl výhled na balkón. Tímto jednáním se podle žalobkyně muž snažil dosáhnout toho, aby oběť nemohla navázat další kontakty a měl ji plně pod svým dohledem. Pokud se v blízkosti oběti objevil muž, nezáleželo, jestli jej oběť znala nebo ne, začal se pachatel vždy chovat agresivněji jak vůči oběti, tak vůči třetím osobám, kteří přišli s obětí do styku. [29]

Pachatel shromažďoval osobní informaci o oběti i o jejích blízkých, aby jim mohl následně nejrůznějšími případy znepříjemňovat život. Pachatel získával informace od svého kamaráda z policejního sboru, kdy například poskytnul informace o majiteli vozidla apod. Příslušník policejního sboru byl za toto jednání disciplinárně potrestán. [29]

Pachatel se snaží co nejčastěji oběť osobně konfrontovat, například jí vozidlem zablokuje cestu, pokud ji zadrží na místě bez svědků, z auta vystoupí a nadává jí. Dále ji například strká v noci zápalku do zvonku od jejího bytu, aby zvonek neustále zvonil, volá jí po nocích z neznámých čísel, sedne si bez dovolení do jejího auta a odmítá ho opustit, nebo ji bezdůvodně nadává před známými oběti. Oběť přitom nijak pachatele nekontaktuje, ani nijak neprovokuje, pouze chce mít od pachatele klid. [29]

Z důvodu stupňování agresivity pachatele a čím dál častějších osobních kontaktů se oběť v prosinci roku 2015 rozhodla podat trestní oznámení. I přes trestní řízení se ovšem útoky nadále stupňovaly a zašly do bodu, kdy se oběť bála opustit sama svůj byt.

Posledním útok se odehrál 7. srpna 2016, kdy útočník, zastavil v autě vedle oběti a i přes přítomnost svědka (kamarádky oběti), ji nadále slovně nadával, vyhrožoval a opakovaně plivl do obličeje. Během celého incidentu seděl útočník v autě a jel v protisměru a ohrožoval tak i ostatní účastníky silničního provozu. [29]

Způsoby útoků se nadále stupňovali a útoky přesahovali rámec snesitelnosti. Pronásledování a obtěžování se nadále stupňovalo do míry, kdy už to bylo nesnesitelné a začali se projevovat na duševním rozpoložení a zdraví oběti, z důvodu strachu o svůj život. [29]

Soud se shodl na tom, že nebezpečné sledování neboli stalking vysokou měrou ovlivňuje život oběti a jejího blízkého okolí a nezřídka končí sebevraždou oběti, nebo vraždou oběti. Po podání všech důkazů a s přihlídnutím na to, že pachatel byl již v minulosti trestně stíhán za narušení domovní svobody, ublížení na zdraví a výtržnictví ve prospěch oběti. [29]

3.6 Dílčí závěr

Kapitola se zabývá ohrožením soukromí, konkrétně typologií hrozeb podle narušení soukromí. Jedná se o hrozby fyzické a logické. V dnešní době kybernetického světa se setkáváme více s hrozbami logickými, protože pro pachatele je jednodušší nalézt osobní údaje, nebo jinak narušit soukromí člověka skrze internet, sociální sítě, nebo za pomocí nejrůznějších kybernetických útoků. Nejčastější logické hrozby jsou kyberšikana a krádež identity za účelem bankovních podvodů. Z fyzických hrozeb zejména stalking a nejrůznější krádeže osobních dokladů.

V závěru kapitoly jsou analyzovány dva skutečné případy narušení soukromí. Prvním případem byla analýza logické hrozby a to krádeže identity. Pachatelé kopírovali identity obětí a na tyto zkopírované identity si následně brali bankovní půjčky. V tomto případu je skvěle vidět, jak snadné je vyhledat na internetu osobní údaje a pomocí nich padělat doklady a vydávat se za někoho jiného. Druhý případ byla fyzická hrozba konkrétně stalking (nebezpečné sledování). Tyto případy ukazují, že k narušení soukromí opravdu dochází a může se s nimi setkat každý.

II. PRAKTICKÁ ČÁST

4 ANALÝZA OCHRANY SOUKROMÍ Z POHLEDU RESPONDENTŮ

Cílem dotazníkového šetření bylo zjistit, jak si respondenti cení svého soukromí, jak ho berou jako nové aktivum a zda si jej dostatečně chrání. Bez znalostí mínění respondentů by bylo složité podnikat kroky pro lepší ochranu soukromí, jelikož by se nebylo možné zaměřit na nejrůznější sektory soukromí a ochrana by nemusela být cílená přímo na běžné občany. Toto šetření umožnilo vnést lepší náhled do toho, jak respondenti o svém soukromí uvažují, kde ho cítí nejohroženější a pomohlo nám chránit soukromí tam, kde je to nejvíce potřebné.

4.1 Dotazník

Samotný dotazník obsahoval 26 otázek, týkajících se soukromí respondentů. Otázky se skládaly z několika bloků otázek. Účelem prvního bloku bylo rozdělení respondentů do určitých kategorií podle pohlaví, věku a vzdělání. Toto rozdělení bylo nápomocné k tomu, aby dotazník obsahoval odpovědi od co nejširší skupiny respondentů a nepřevažovaly zde odpovědi pouze od jedné skupiny respondentů.

Následující blok otázek týkajících se přímo soukromí respondentů. Jeho úkolem bylo zjistit, jak respondenti nakládají se svým soukromím a zda jeho narušení považují za hrozbu, zda vůbec mají o ochranu soukromí zájem a své soukromí si chrání.

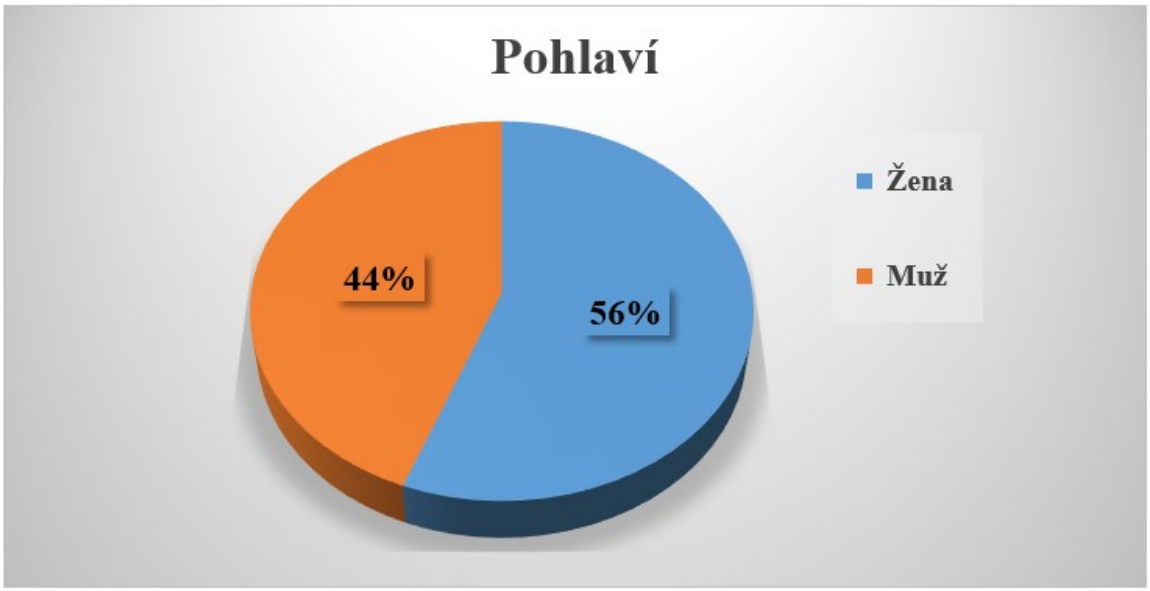
Další blok otázek se týkal narušení soukromí. Je velmi důležité pro další práci s ochranou soukromí zjistit, kde a z jaké strany cítí respondenti své soukromí nejvíce ohrožené.

Poslední blok otázek se týkal ochrany soukromí, kdy byli respondenti tázaní, jak své soukromí chrání a co považují jako dostatečnou ochranu svého soukromí. Pro ochranu soukromí je také důležité, jak si respondenti svého soukromí cenní a do jaké míry ho berou jako nové aktivum a jakou má pro respondenty soukromí hodnotu.

Průzkumu se zúčastnilo 154 respondentů, což je dostatečný počet na to, aby průzkum mohl být objektivní a poskytl dostatečně široký náhled na danou problematiku. Dotazník byl šířen pomocí webu vypln.to a Facebooku, tudíž celý dotazník byl zodpovídán anonymně a elektronicky.

4.1.1 Otázka č.1: Pohlaví

První otázka byla zaměřena na zjištění pohlaví. Jedná se o jedno z nejdůležitějších rozdělení respondentů, protože muži a ženy mohou na soukromí nahlížet poměrně odlišně. Ženy jsou mnohem častěji obětmi stalkingu, kyberšikany apod., tudíž bylo zajímavé zjistit, jestli si své soukromí chrání více či nikoliv. Dalším důvodem zařazení otázky pohlaví bylo, aby dotazník obsahoval obě pohlaví a byl co nejvíce objektivní a vyvážený.

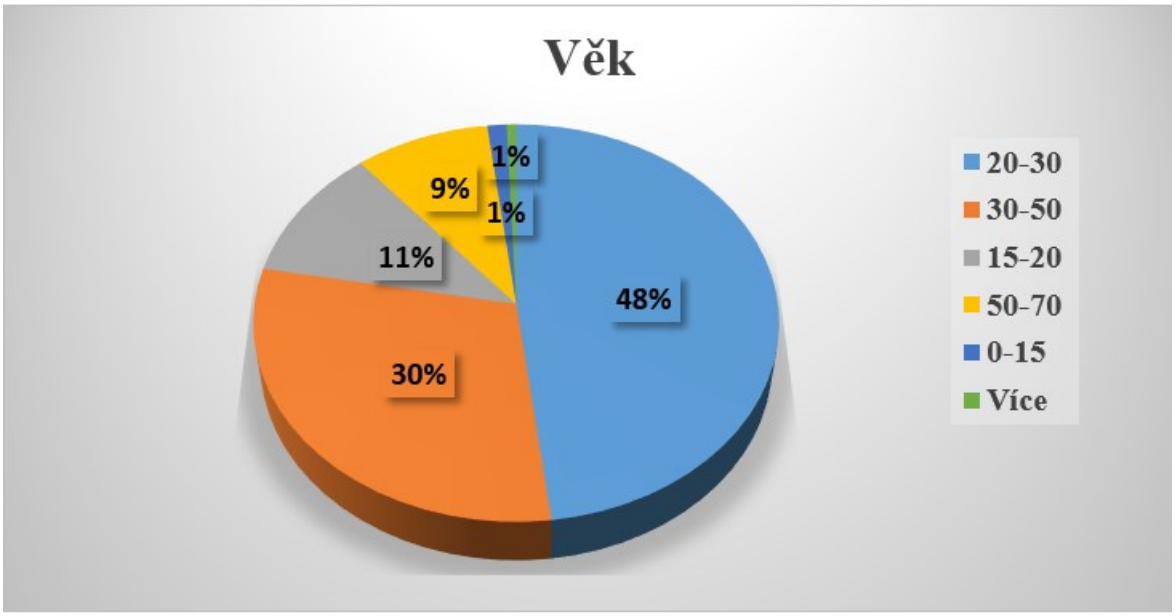


Obr. 1: Pohlaví [vlastní

Z dotazníku můžeme vidět, že poměr mužů a žen byl poměrně vyrovnaný. Na dotazník odpovědělo 56% žen a 44% mužů. Vyrovnanost pohlaví je pro dotazník důležitá, jelikož dotazník bylo více vypovídající a nepřevažuje názor jednoho nebo druhého pohlaví.

4.1.2 Věk:

Další otázka, které slouží k všeobecnému rozdělení respondentů, byl věk. Různé věkové kategorie se mohou setkávat s odlišnými způsoby narušení soukromí. Taky pohled na soukromí se může postupně s věkem výrazně lišit.

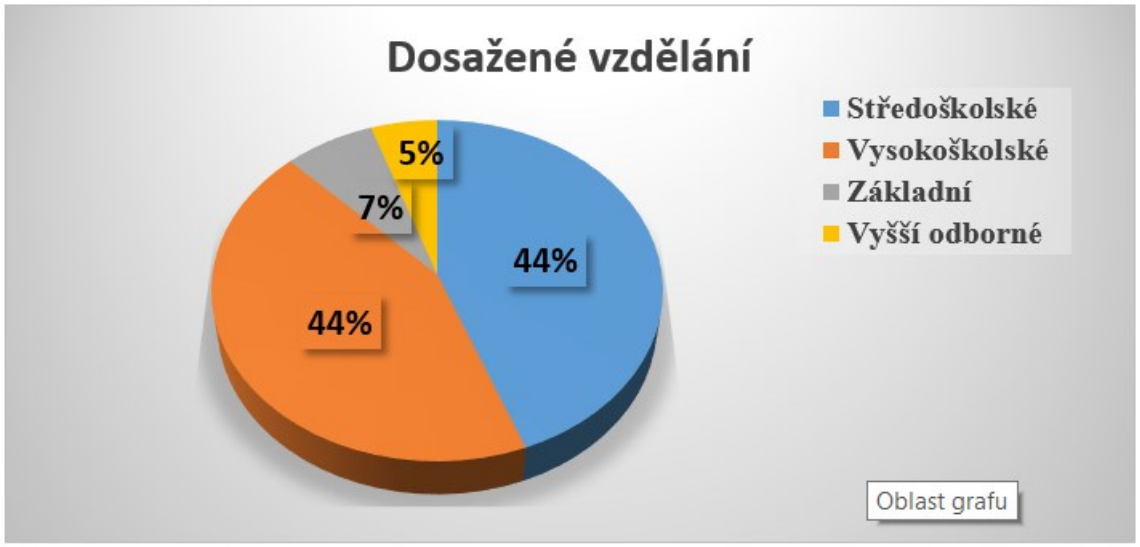


Obr. 2: Věk [vlastní]

Nejobsáhlejší věkovou kategorií, která se zúčastnila průzkumu, byla věková kategorie 20 - 30 let. V rozpětí těchto let bylo celých 48% respondentů, dále následovala věková kategorie 30-50 let. Tyto 2 kategorie jsou v dotazníků nejrozšířenější, protože dotazník byl šířen elektronicky pomocí webových stránek vyplň.to a Facebookových skupin. Tato věková skupina je na internetu nejaktivnější. Následovala věková skupina 50 - 70 let s 11 %. Nejméně respondentů bylo ve věku 1 - 15 let a seniorů, kteří nejsou tak aktivní na sociálních sítích a internetu.

4.1.3 Dosažené vzdělání

Poslední otázkou rozdělující respondenty do skupin bylo vzdělání. Jednalo se pouze o otázku informativního charakteru, která nemá pro průběh dotazníkového šetření velký vliv.



Obr. 3: Dosažené vzdělání [vlastní]

Jak se dalo předpokládat z věkových skupin, nejvíce respondentů je středoškolského a vysokoškolského vzdělání, shodně 44 %. Stejný poměr vysokoškolských a středoškolských respondentů můžeme přisuzovat i tomu, že do styku s dotazníkovými šetřeními přijdou nejvíce právě studenti vysokých a žáci středních škol. Malé množství respondentů bylo základního, nebo vyššího odborného vzdělání.

4.1.4 Považujete narušení soukromí za hrozbu?

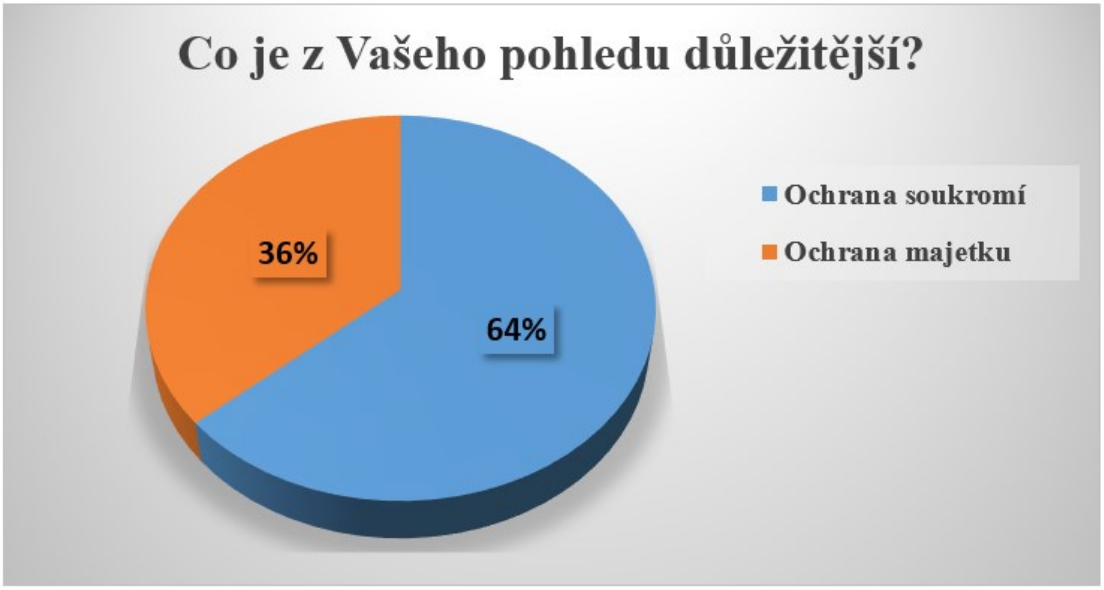
První otázkou, která se týkala již samotné problematiky, bylo, zda respondenti považují narušení soukromí za hrozbu. Tato otázka je položena záměrně na začátku dotazníku, jelikož pro respondenty, kteří odpoví ne, je zbytečné se dále zabývat vyšší ochranou soukromí.

Obr. 4: Narušení soukromí jako hrozba [vlastní]

Narušení soukromí představuje hrozbu pro 95% respondentů. Tento fakt je velmi důležitý pro další šetření. Pouze 5% respondentů narušení soukromí za hrozbu nepovažuje. Poukazuje to i na to, jak je v dnešní době důležité si lépe chránit své soukromí.

4.1.5 Co je z vašeho pohledu důležitější? Ochrana soukromí, nebo majetku?

Další otázkou bylo, co je pro respondenty důležitější, zda ochrana majetku, nebo ochrana soukromí. Otázka se může zdát záludná, protože bychom si měli rovnoměrně chránit svůj majetek i svoje soukromí. Ovšem bylo důležité zjistit, zda lidé pohlížejí na ochranu soukromí, minimálně stejně důležitě jako na ochranu majetku, protože všichni lidé si svůj majetek samozřejmě chrání a považují ochranu majetku za důležitou.



Obr. 5: Ochrana soukromí, nebo majetku [vlastní]

I přesto, že ochrana majetku je velmi důležitá a každý si svůj majetek chrání, odpovědělo 64% respondentů, že je pro ně ochrana soukromí důležitější, než ochrana majetku. Pouze pro 36% je důležitější ochrana majetku důležitější, než ochrana samotného soukromí.
Z toho vyplývá, že respondenti si svého soukromí cení i na úkor majetku a berou ho jako aktivum, které pro ně má vysokou hodnotu.

4.1.6 Myslíte, že si své soukromí dostatečné chráníte?

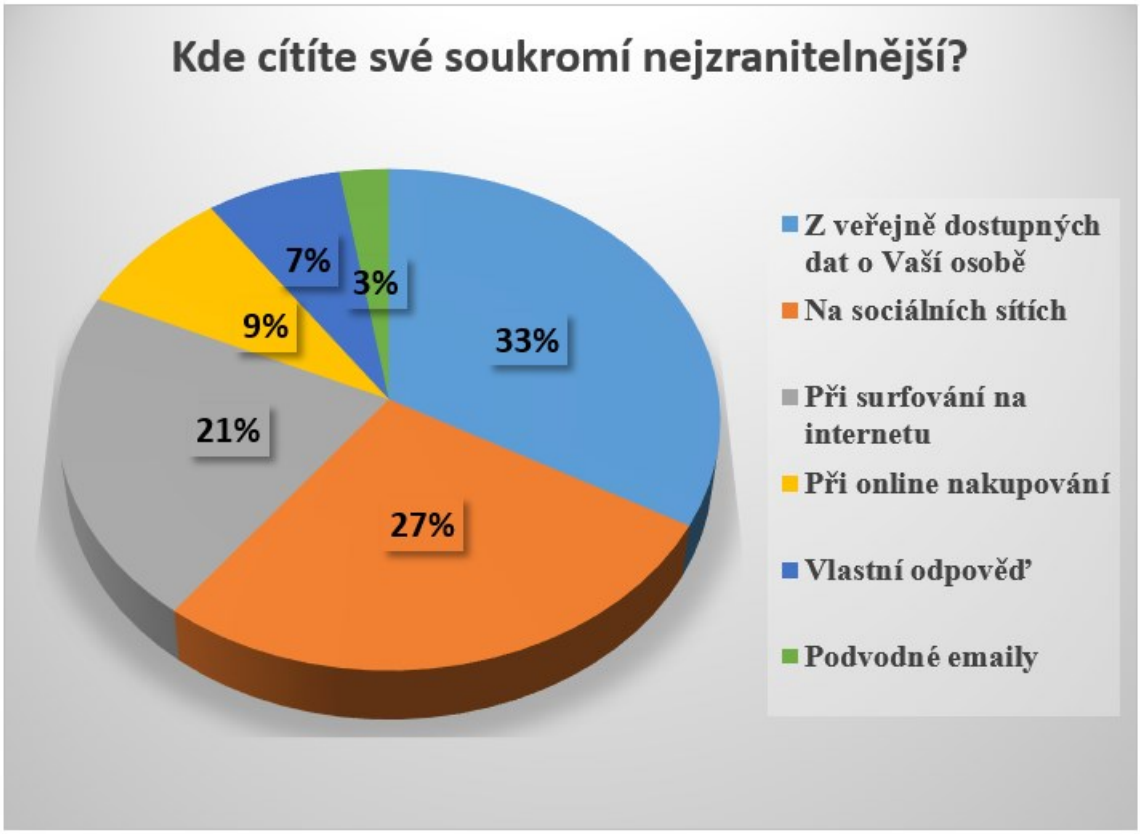
Další otázka už byla více osobní, kde měli respondenti odpovědět, zda své soukromí dostatečné chrání. Tato otázka je pro vyšší ochranu soukromí velmi důležitá, jelikož respondenti, co si nedostatečně chrání své soukromí a jsou si toho vědomi, mohou patřit do ohrožené skupiny, navíc se dá předpokládat, že nebudou dbát ani v budoucnu o lepší zabezpečení svého soukromí.

Obr. 6: Aktuální ochrana soukromí respondentů [vlastní]

Výsledek byl předpovídaný, že 71% respondentů se domnívá, že své soukromí dostatečně chrání. Tento výsledek je pozitivní, protože lidem není soukromí lhostejné a zaměřují se na jeho ochranu. Dále se dá předpokládat, že pokud bude respondentům předložena možnost, jak své soukromí lépe chránit, na tuto možnost přistoupí.

4.1.7 Kde cítí své soukromí nejzranitelnější?

Úkolem této otázky bylo zjistit, kde respondenti spatřují největší hrozbu pro své soukromí. Na tuto otázku bylo možné odpovědět pouze jednou odpovědí, z důvodu zjištění nejrizikovějších sektorů v ochraně soukromí. Respondenti měli na výběr z různých oblastí, kde se s narušením soukromí mohou setkat. Z výběru mohli vybrat sociální sítě, surfování na internetu, online nakupování, podvodné emaily, nebo z volně dostupných dat o svojí osobě. Respondentům při této otázce byla nabídnuta i možnost vlastní odpovědi.



Obr. 7: Zranitelnost soukromí [vlastní]

Nejvíce respondentů a to 33 % cítí své soukromí nejohroženější z veřejně dostupných dat o své osobě. Dalo se to předpokládat, protože se dá o každém při troše štěstí najít opravdu velké spektrum informací. Nezanedbatelné jsou i sociální sítě s 27% a 21% surfování na internetu. Nejohroženější na sociálních sítích jsou lidé, kteří na sociálních sdílí velké množství ze svého soukromého života. Při surfování na internetu můžeme narazit na závadný web, nebo nechtěně stáhnout infikovaný soubor a útočníci tak mohou jednoduše naše soukromí narušit a je mu mnohem složitější se bránit, než na sociálních sítích. Při online nakupování se cítí ohrožených pouze 9 % respondentů, protože se dá předpokládat, že se jedná o lidi znalé problematiky falešných obchodů apod. Podvodných emailů se bojí pouze 3 % respondentů. S falešnými emaily se setkal určitě každý, ale jsou notoricky známé a je poměrně snadné je odhalit.

Z vlastních odpovědí převažovaly odpovědi, že lidé cítí své ohrožení ze strany státu, ovšem množství těchto odpovědí bylo oproti pohybu na internetu a sociálních sítích zanedbatelné. Dále se lidé bojí o své soukromé při zadávání osobních údajů soukromým osobám, například při ubytování, nebo činnostech, kde bez vyplnění osobních údajů provozovatel neposkytne danou službu.

Lidé se bojí o veřejně dostupné údaje o své osobě, tudíž o jakousi digitální stopu, kterou za sebou v průběhu používání internetu zanechali, nebo o nich zanechala třetí strana.

4.1.8 Obáváte se o své soukromí na internetu?

Poté co jsme od respondentů zjistili, kde cítí své soukromí nejvíce ohrožené, bylo důležité zjistit, zda se lidé na internetu opravdu o své soukromí obávají.

Obr. 8: Obava o soukromí na internetu [vlastní]

Většina respondentů 71% se o své soukromí na internetu obává. Je zajímavé, že se jedné o stejné množství respondentů, kteří tvrdí, že si své soukromí dostatečně chrání. Tudíž lze předpokládat, že i přesto, že si své soukromí snaží střežit, není tato ochrana dostatečná a dále se o své soukromí obávají. Otázka dále ukazuje, že přechod do virtuálního prostředí nahrává k tomu, aby soukromí uživatelů internetu bylo více zranitelné.

4.1.9 Jste aktivní na sociálních sítích?

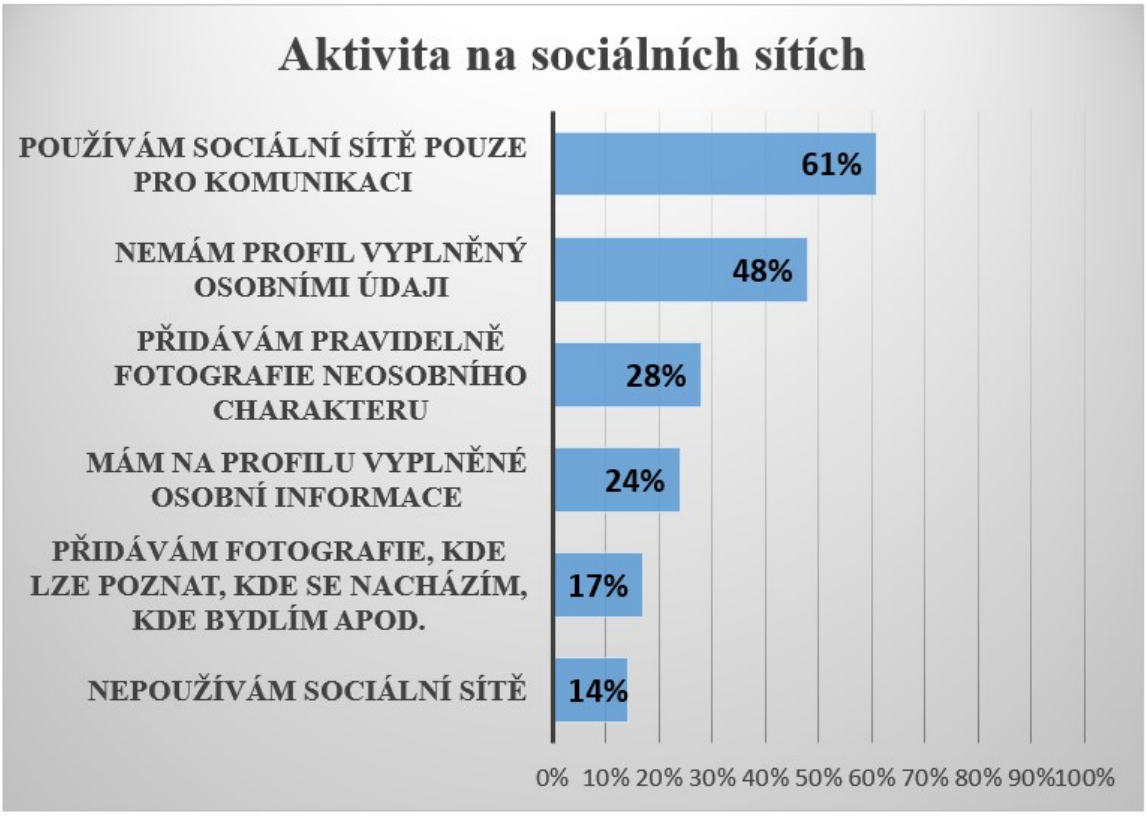
Další otázkou navazující na otázku 8., je, zda respondenti jsou aktivní na sociálních sítích. Právě aktivita na sociálních sítích je nejčastější aktivita, kterou lidé provádějí na internetu. Dalším důvodem zařazení této otázky je, že sociální sítě jsou obrovský rezervoár osobních údajů uživatelů sociálních sítí, které mohou být pro pachatele jednoduše získatelné.

Obr. 9: Používání sociálních sítí [vlastní]

I přesto, že se značná část respondentů na sociálních sítích cítí své soukromí nejohroženější, tak sociální sítě většina a to 74% respondentů používá. Ovšem sociální sítě, se dají používat pouze pro komunikaci a ohrožení soukromá se tak značně snižuje, jak sociální sítě lidi využívají, bude zodpovězeno v následující otázce.

4.1.10 Aktivita na sociálních sítích

Další otázka rozvíjí otázku aktivity na sociálních sítích. Cílem otázky bylo zjistit, jak uživatelé sociální sítě využívají a zda na sociálních sítích dbají o své soukromí, či ho upozaďují. Na tuto otázku mohli respondenti vybrat z více odpovědí, aby dokázali lépe vyobrazit svou aktivitu na sociálních sítích.



Obr. 10: Aktivita na sociálních sítích [vlastní]

Jak se již dalo z předešlých otázek očekávat, lidé si své soukromí chrání, a proto 61 % respondentů používá sociální sítě pouze pro komunikaci a 48 % nemá svůj profil na sociální síti vyplněný osobními údaji. Menší skupina lidí 28 % na svůj profil přidává fotky neosobního charakteru, pouze 17 % respondentů na svůj profil přidává fotografie, které odhalují jejich aktuální lokaci, nebo trvalé bydliště. Pouze 24 % má svůj profil vyplněný osobními údaji. 14 % respondentů uvedlo, že sociální sítě nepoužívá, v přechozí otázce ovšem 26 % respondentů uvedlo, že sociální sítě nepožívají. Z toho usuzuji, že 1 2% respondentů například pouhou komunikaci, přes sociální sítě, nepovažuje za plnohodnotné používání sociálních sítí.

4.1.11 Vyplňování osobních údajů při registraci, online nákupu apod.

Další otázka se již týkala přímo osobních údajů respondentů. Jednalo se o to, jestli si uvědomují, kde všude zadávají své osobní údaje. Cílem otázky bylo zjistit, zda a za jakým účelem lidé poskytují své osobní údaje, které mohou být dále zneužity. Respondenti mohli zvolit více odpovědí zároveň, protože se jednotlivé části otázky na sebe navazovaly.

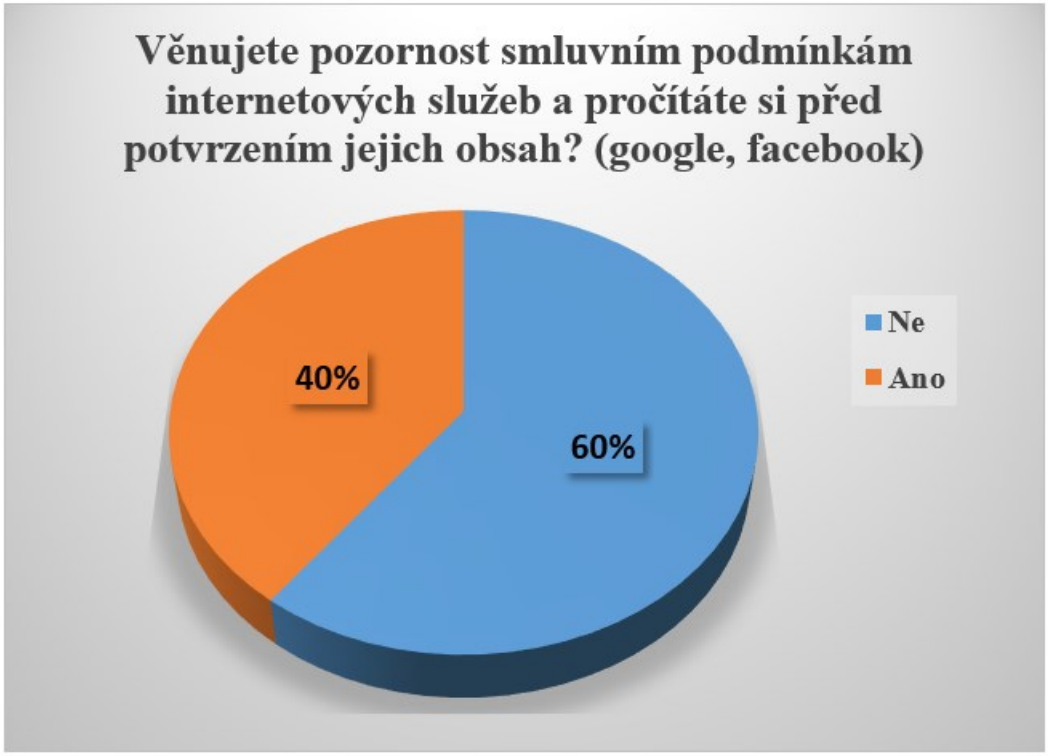
Obr. 11: Vyplňování osobních údajů při registraci, online nákupu apod. [vlastní]

Z průzkumu vyplývá, že respondenti se snaží své soukromí chránit. To potvrzuje i jejich nakládání s osobními údaji. 72 % respondentů při zadávání osobních údajů kontroluje, zda je web, kde zadávají své osobní informace důvěryhodný. 66 % respondentů zadává, své osobní údaje pouze při online nakupování, kde je zadat své osobní informace nezbytné, pokud chceme svou zásilku obdržet. 12% respondentů své osobní údaje nikdy nikde na internetu nevyplňuje a stejné procento respondentů ovšem své osobní údaje zadává i na různé blogy a webové služby, kde není potřeba zadávat své pravé osobní údaje. 17% respondentů na tyto služby zadává falešné údaje. Nejpozitivnější je, že pouze 7% respondentů nekontroluje, zda web, kde zadávají osobní informace, je důvěryhodný.

Zdá se, že 12 % lidí, kteří vyplňují své osobní údaje na blogy apod. a dokonce 7% respondentů co vůbec nekontroluje, zda weby, kde zadávají své osobní informace jsou důvěryhodné, jako zanedbatelné číslo. Ovšem z globálního hlediska je 7 % lidí obrovské množství lidí, kteří nevědí, kdo nakládá s jejich osobními údaji a je tedy důležité nadále upozorňovat všechny uživatele internetu, aby své osobní údaje zadávali jen na důvěryhodné weby a jen pokud je to opravdu nutné.

4.1.12 Věnujete pozornost smluvním podmínkám internetových služeb a pročítáte si před potvrzením jejich obsah? (Google, Facebook)

Další otázka se týká pročítáních smluvních podmínek. Z vlastní zkušenosti vím, že tyto smluvní podmínky spousta lidí pouze potvrdí, ale nepročítá si jejich celý obsah. Ovšem tyto smluvní podmínky nám často oznamují, jak s našimi osobními údaji bude zacházeno.



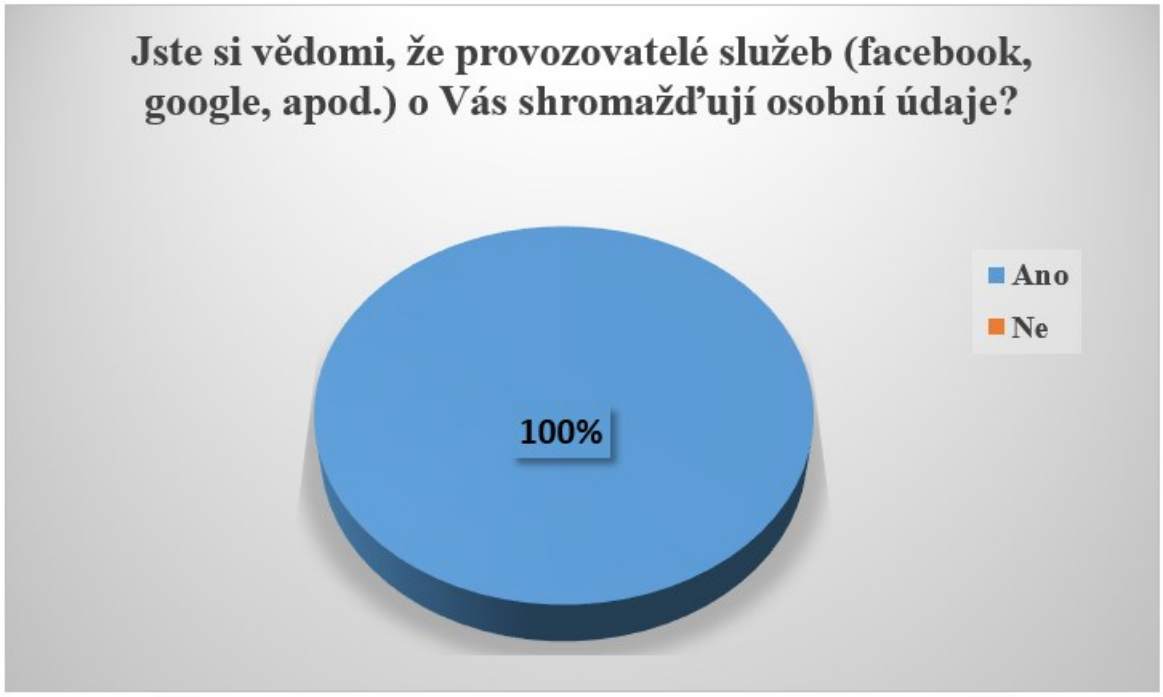
Obr. 12: Smluvní podmínky [vlastní]

60 % respondentů smluvním podmínkám nevěnuje pozornost. Dá se předpokládat, že je to tím, že tyto služby chtějí, nebo potřebují používat a věnování pozornosti, by znamenalo pouze ztrátu času. Menší polovina, 40 % respondentů si smluvní podmínky před potvrzením pročítá, dává jim to alespoň lepší představu o tom, jak je s jejich údaji zacházeno, dále vědí, na co mají při ochraně svého soukromí nárok.

Zde je důležité zmínit, že tyto smluvní podmínky jsou mnohdy zdlouhavé a nesrozumitelné pro normálního uživatele se jeví jako jednodušší pouze tyto podmínky potvrdit. Zde bych dal návrh, aby tyto smluvní podmínky obsahovaly více „lidského slova“ a byly zjednodušeny, abychom byli alespoň částečně všichni lépe informování o tom, jak různé weby využívají cookies a další osobní údaje, jak jsou zabezpečeny a jak je s nimi manipulováno.

4.1.13 Jste si vědomi, že provozovatelé služeb (facebook, google, apod.) o Vás shromažďují osobní údaje?

Rozšiřující otázka k smluvním podmínkám, jejímž cílem je zjistit zda uživatelé internetových služeb, mají podvědomí o tom, že tyto služby o uživatelích shromažďují osobní údaje.



Obr. 13: Shromažďování osobních údajů [vlastní]

Všech 154 respondentů odpovědělo shodně, že si jsou vědomi, že o nich provozovatelé Facebook a Google shromažďuje osobní informace. Jedná se především o informace typu, které webové stránky jsme navštívili, kolik jsme na nich strávili času a další informace, které mohou poskytnout pro reklamní účely.

4.1.14 Slyšeli jste někdy o chytré (behaviorální) reklamě?

Otázka číslo 14, také navazuje na předešlé otázky ke smluvním podmínkám, kdy jeden z důvodů, proč o nás poskytovatelé shromažďují osobní údaje, je právě poskytnutí těchto údajů pro své vlastní zákazníky, za účelem cílené behaviorální reklamy. Díky tomuto jsou tyto služby zdarma, ale platíme za ně svým soukromím.

Obr. 14: Chytré reklamy [vlastní]

83% respondentů někdy slyšelo, o behaviorální reklamě. Myslím si, že se s ní někdy setkali všichni respondenti, ale pouze netušili, o co se jedná, nebo jí nevěnovali vyšší pozornost.

4.1.15 Považujete chytré (behavioroální) reklamy za narušení soukromí?

Poslední otázka, která se týkala smluvních podmínek a užívání osobních údajů poskytovateli služeb byla, zda toto jednání respondenti považují na narušení soukromí, kdy prodejce přímo ví jaký druh produktů a služeb preferujeme k tomu, aby na nás mohl zacílit co nejlepší reklamou.

Obr. 15: Chytré reklamy jako narušení soukromí [vlastní]

Tyto reklamy považuje na narušení soukromí 61% respondentů. Samozřejmě se svým způsobem o narušení soukromí jedná, ale všichni uživatelé s tímto souhlasí při odsouhlasení smluvních podmínek. Dalším řešením, jak se dá těmto reklamám zabránit, je mazat své cookies, nebo používat prohlížeče, které blokují přístup cookies třetích stran.

4.1.16 Který případ narušení soukromí považujete za nejhorší?

Otázka, která se zabývá přímo narušením soukromí, jejímž cílem bylo zjistit, kterého narušení soukromí se respondenti nejvíce obávají a považují jej za nejhorší. Díky této otázce bude možnost se zaměřit na ochranu soukromí tam, kde se o své soukromí respondenti nejvíce obávají. Respondenti měli na výběr z konkrétních případů narušení soukromí, nebo mohli přidat vlastní odpověď.

Obr. 16: Nejhorší případy narušení soukromí [vlastní]

Podle respondentů je nejhorším narušením soukromí krádež identity spojená s bankovními podvody a shodlo se na tom 40% respondentů, toto narušení soukromí je nejhorší právě proto, že má přímý finanční dopad, po kterém mnohdy následuje zadlužení obětí, exekuce a zhoršení životních podmínek oběti.

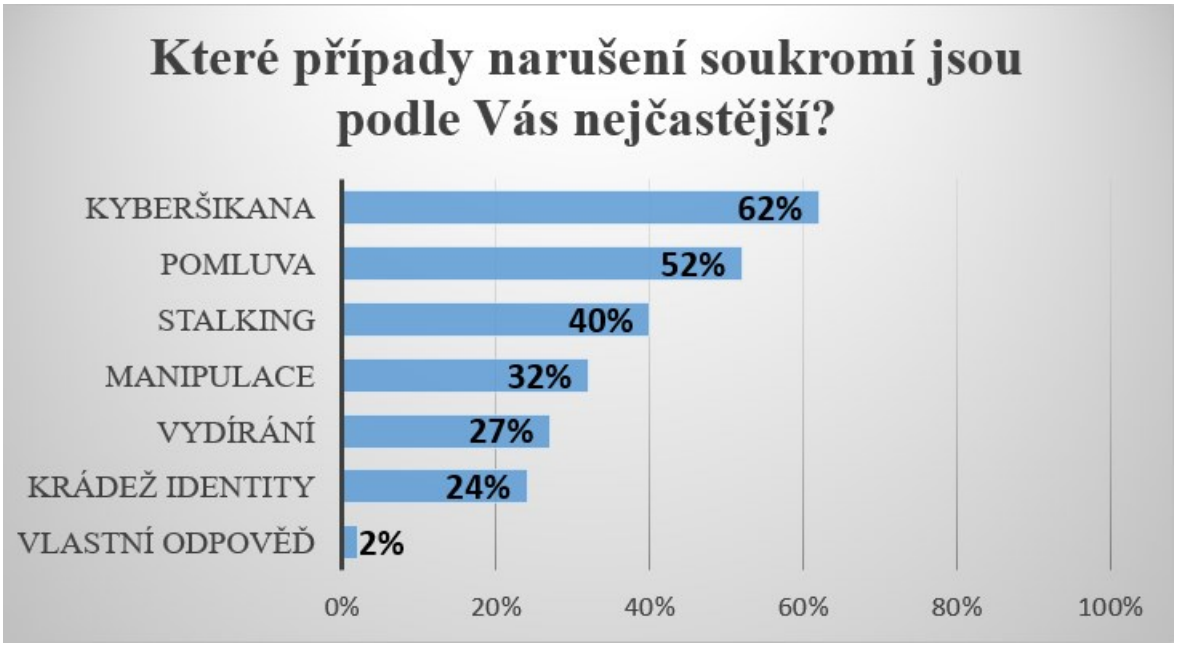
Dalších 18 % připadá na krádež identity, kdy se za nás někdo s nějakým účelem vydává a není spojená přímo s bankovními podvody. Následuje s 11 % kyberšikana, vydírání 10 %, 7 % stalking a manipulace 7 % Tato narušení soukromí jsou sice závažná, ale respondenti je nepovažují za nejhorší, nejspíše z důvodu, že nemají přímý finanční dopad, i když můžou mít na jedince fatální dopad na psychickou i fyzickou stránku poškozeného. Pouze 1 % respondentů považuje za nejhorší pomluvu, přitom cílené pomluvy mohou vést k rozpadu rodiny, vyhození z práce, nebo rozpadu přátelství.

Z vlastních odpovědí byly téměř všechny odpovědi, že každé narušení soukromí se dá považovat za nejhorší, nebo stejně závažné.

Zneužití identity pro bankovní podvody je určitě velký problém, který by mohl vyřešit nástroj pro spolehlivé ověření identity, kdy by zneužít identitu pro peněžní podvody bylo mnohem složitější.

4.1.17 Které případy narušení soukromí jsou podle Vás nejčastější?

Podotázka k narušení soukromí, kde respondenti podle vlastního uvážení odpovídají, které způsoby narušení soukromí jsou nejčastější. Podle četnosti těchto případů narušení soukromí, bude možno dále lépe navrhnout lepší ochranu soukromí, tam kde je to nejvíce potřebné. Na tuto otázku mohli respondenti odpovědět více možností a i přidat vlastní odpověď.



Obr. 17: Nejčastější případy narušení soukromí [vlastní]

Podle respondentů je nejčastější případ narušení soukromí kyberšikana. Kyberšikana je čím dál častější, převážně u mladistvých lidí, kdy útočníkům dává pocit anonymity. Právě díky tomu je tento případ narušení soukromí tak častý, útočníci si často nejsou vědomi toho, že se dopouští trestného činu, nebo jak velké následky to může nést na oběť.

Druhým nejčastějším narušením soukromí je podle respondentů pomluva. S pomluvou se již setkal každý z nás, ovšem záleží na druhu pomluvy. Každá pomluva může mít odlišný dopad na soukromí. Ovšem každý pomluva se dá považovat za narušení soukromí jedince a může mít své následky. Následuje manipulace 32 % a vydírání 27 %. Za manipulaci se dá považovat, kterékoliv jednání, kdy jedna strana do něčeho nutí druhou, může se jednat o snahu politických stran získat voliče, snahu prodejce oklamat zákazníky ke koupi produktu, nebo asi nejhorší druh manipulace, kdy pachatel manipuluje oběť, aby jednala proti své vůli, které přechází až právě k vydírání. Vydírání má mnoho podob, ovšem dá se říci, že pachatel má o oběti určité informace a nutí oběť k něčemu, z čeho bude mít pachatel prospěch. Jedná se o velice časté a závažné narušení soukromí. Méně častá je podle respondentů krádež

identity 24 %, jedná se ovšem o velmi závažný problém, se kterým musíme v budoucnu čím dál častěji počítat. Zejména díky virtualizaci téměř každé činnosti, kdy není zapotřebí přímá přítomnost jedince.

4.1.18 Setkali jste se někdy s pojmem GDPR? (obecné nařízení o ochraně osobních údajů)

Následuje poslední blok otázek, zabývající se přímo ochranou soukromí. První otázka směřovala k ověření skutečnosti, zda jsou respondenti seznámeni s pojmem GDPR, které je v České republice uplatňováno jako Obecné nařízení o ochraně osobních údajů (GDPR) a nahradilo zastaralé zákony o ochraně osobních údajů.

Obr. 18: Obeznámenost s GDPR [vlastní]

Téměř všichni respondenti 99%, se setkali s pojmem GDPR a dá se předpokládat, že ví, jak se smí nakládat s jejich osobními údaji.

4.1.19 Považujete nařízení GDPR za dostatečnou ochranu osobních údajů?

Otázka navazující na předchozí otázku o GDPR, která zjišťuje, zda respondenti považují ochranu osobní za dostatečnou. Tato otázka může dále sloužit k vylepšení ochrany osobních údajů.

Obr. 19: GDPR jako dostatečná ochrana osobních údajů [vlastní]

Přesto, že GDPR doplnilo Zákon č.110/2015 SB. o zpracování osobních údajů a dává lidem větší ochranu osobních údajů a jsou mnohem lépe informovaní, jak je s jejich osobními údaji manipulováno, tak 62 % respondentů nepovažuje GDPR za dostatečnou ochranu osobních údajů. Jak GDPR funguje, je rozebráno v teoretické části práce. GDPR sice nařizuje informovat, jak je s našimi osobními nakládáno a jak mají být uchovávány, ale přímo neřeší problematiku zacházení s osobními údaji. Výsledkem je, že jsme seznámení, že s našimi údaji je manipulováno, ale stejně pokud chceme využívat nejrůznější služby, toto nakládání s osobními informacemi odsouhlasíme. Lidé by spíše uvítali přímou regulaci toho, jaké informace o nás mohou být shromažďovány, když už tyto služby používáme.

4.1.20 Považujete své soukromí za aktivum, které je za zapotřebí více chránit?

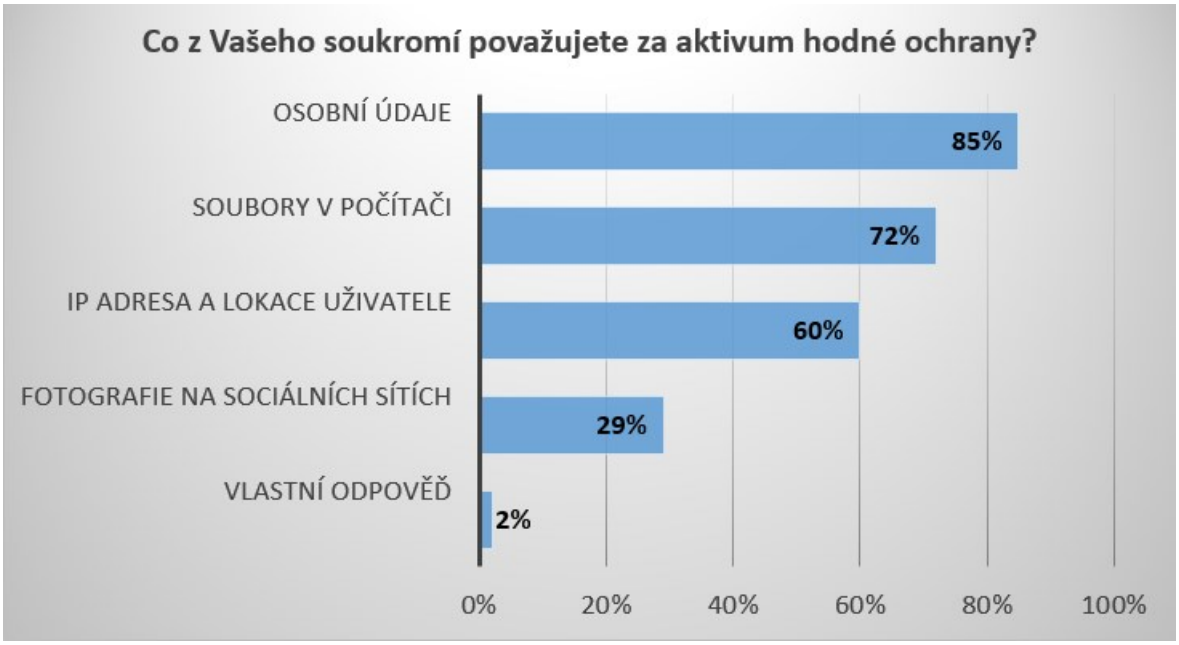
Otázka číslo 20 je pro tento výzkum klíčová. A to zda respondenti považují své soukromí za aktivum, které je zapotřebí více chránit. Respondenti na tuto otázku mohli odpovědět i vlastní odpovědí.

Obr. 20: Soukromí jako aktivum [vlastní]

Z průzkumu vyplývá, že většina respondentů považuje soukromí za aktivum, které je zapotřebí více chránit a to 84% respondentů. Tato skutečnost jen potvrzuje, jak je ochrana soukromí v dnešní době čím dál důležitější a dává nové podměty k vytvoření nových programů pro kvalitnější ochranu soukromí. Z vlastních odpovědí respondentů vyplývá, že prozatím je soukromí dostatečně chráněno, bude ho ovšem nutno tuto ochranu zlepšit.

4.1.21 Co z Vašeho soukromí považujete za aktivum hodné ochrany?

Podotázka k soukromí jako novému druhu aktiva, kdy se dotazují respondentů, co ze svého soukromí považují za aktivum. Díky této otázce lze dobře určit sektory soukromí, které kde je zapotřebí zlepšit jejich ochranu. Na tuto otázku mohli respondenti přidat více odpovědí, nebo přidat vlastní odpověď.



Obr. 21: Aktiva soukromí [vlastní]

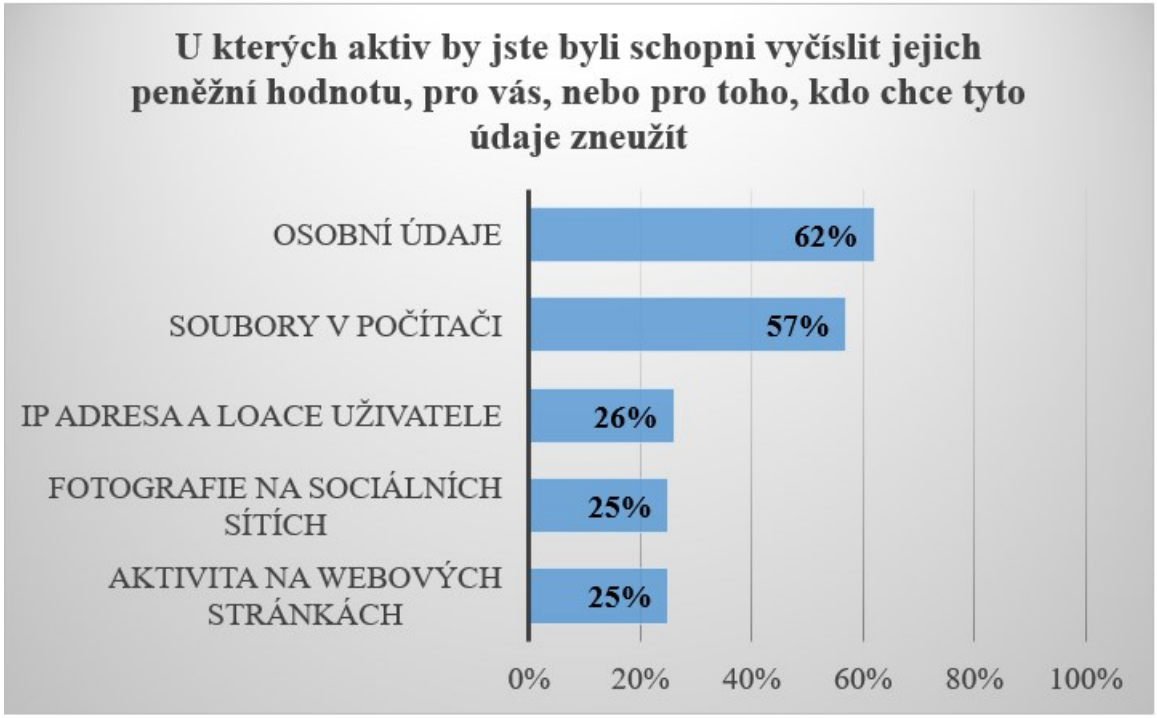
Nejvíce respondentů a to 85 % považuje za aktivum hodné ochrany své osobní údaje. Je to pochopitelné, jelikož zneužití osobních údajů může mít obrovské následky, jako krádež identity apod. Jak již z dotazníku vyplynulo, v České republice je platné GDPR. Toto nařízení je zaměřeno přímo na ochranu osobních údajů, ale existuje zde dále prostor pro vylepšení ochrany osobních údajů, protože většina respondentů se necítila tímto nařízením dostatečně chráněna. Dalším důležitým blokem jsou soubory v počítači 7 2%. V počítači máme mnohdy uložená hesla, pracovní soubory, důležité dokumenty apod. Jejich ochrana spadá spíše pod kybernetickou bezpečnost, ale samozřejmě souvisí i s ochranou soukromí.

Dalším důležitým bodem, který je dle respondentů hodný ochrany, je IP adresa a lokace uživatele 60 %. Jelikož lze v dnešní době poměrně snadno zjistit IP adresu, je tím soukromí uživatelů značně narušováno. Z IP adresy lze zjistit spoustu informací o uživateli. Například poskytovatele internetu uživatele, jeho přibližnou lokaci, dále lze podle ní zjistit, jaké weby navštěvujeme.

Méně lidí považuje za hodné ochrany fotografie, například na sociálních sítích. Tento problém je spíše pro známé osobnosti, kdy je jejich osobní fotografie využita pro nejrůznější reklamy účely s kterými nesouhlasí. Jedná se samozřejmě o trestný čin, ale děje se to poměrně často. Z vlastních odpovědí respondentů je považována za aktivum aktivita uživatelů na webových stránkách.

4.1.22 U kterých aktiv by jste byli schopni vyčíslit jejich peněžní hodnotu, pro vás, nebo pro toho, kdo chce tyto údaje zneužít

Tato otázka přímo navazuje na to, co respondenti považují ze svého soukromí za aktivum. Pro jeho ochranu je ovšem důležité zjistit co má pro respondenty, ale i pachatele, kteří se snaží narušit naše soukromí, nejvyšší hodnotu. Dá se předpokládat, že pachatelé budou chtít z narušení soukromí finančně profitovat.



Obr. 22: Aktiva s peněžní hodnotou [vlastní]

Nejvíce respondentů by dokázalo vyčíslit hodnotu u osobních údajů 62 %. Lze to přikládat tomu, že osobní údaje jsou klíčem k elektronickému bankovnictví jejich prostřednictvím se přihlašujeme do nejrůznějších služeb. Pomocí osobních údajů si můžeme vypůjčit peníze, je tudíž jasné, že mají obrovskou hodnotu. Dalších 57 % považuje za aktivum s určitou peněžní hodnotou soubory v počítači. Tento údaj se spíše odvíjí od lidí, kteří na dotazník odpovídali. Je samozřejmé, že nějaký IT specialista, nebo někdo kdo používá počítač pracovně a ukládá v něm důležité dokumenty, bude považovat soubory v počítači za mnohem důležitější, než lidé, kteří v počítači téměř nic nemají. Následuje s 26 % IP adresa a lokace uživatele, tyto údaje jsou samozřejmě zneužitelné, ale mnohem méně než přímo osobní údaje. Fotografie na sociálních sítích považuje za aktivum pouze 25 % respondentů, zde bylo zjištěni, že je malá škála lidí, u kterých tyto fotografie mají opravdu hodnotu. Se stejným % hlasů skončila aktivita na webových stránkách. Tyto informace mají sice vysokou hodnotu pro reklamní

účely a jsou hodně využívány pro behaviorální reklamu, ale běžný pachatel ji nedokáže nijak zpeněžit.

4.1.23 Dokážete peněžně vyčíslit hodnotu svého soukromí?

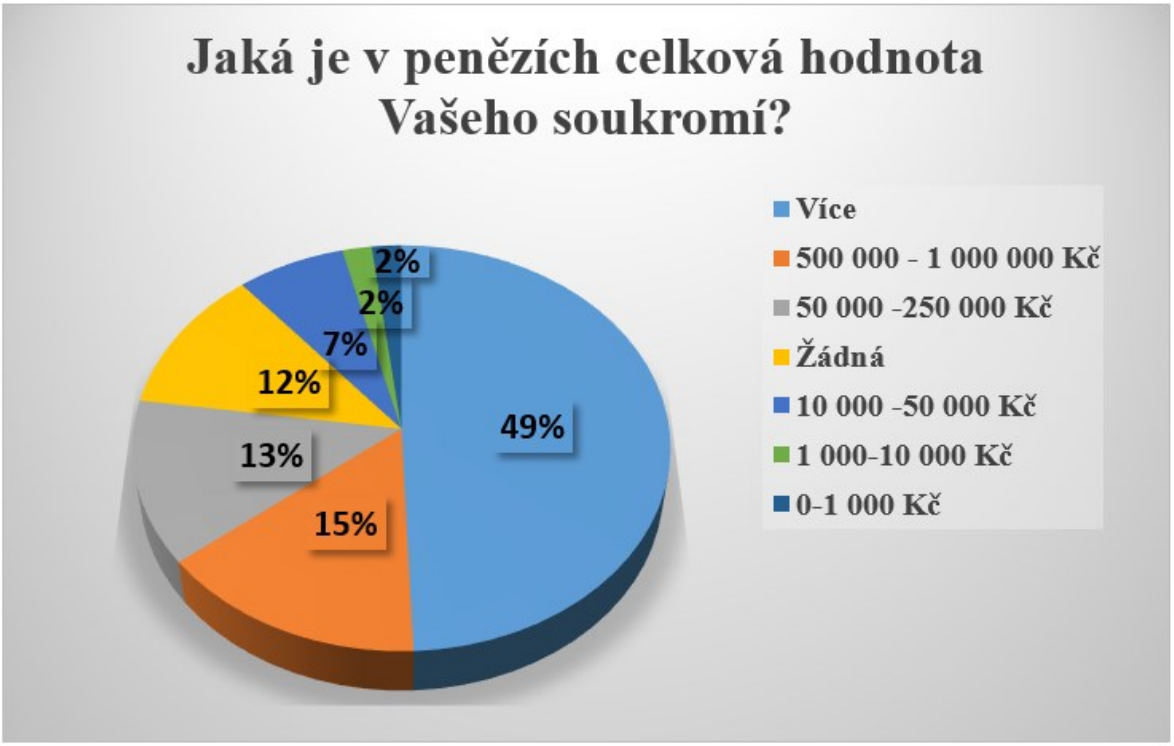
Poté co v přechozí otázka zněla, u jakých aktiv by respondenti dokázali určit jejich hodnotu, následuje otázka, zda by respondenti dokázali vyčíslit hodnotu svého soukromí v peněžním měřítku.

Obr. 23: Vyčíslení hodnoty soukromí [vlastní]

Přesto, že lidé dokáží určit, jaké aktiva mají peněžní hodnotu, tak 79% respondentů nedokáže vyčíslit hodnotu svého soukromí. Nejspíše je i tím, že považují soukromí za abstraktní pojem a neberou ho dostatečně jako nové aktivum. Nebo také to, že vyčíslit hodnotu je poměrně složité, protože soukromí je velmi obsáhlé a k tomu, abychom určili, co vše do něj patří a jakou má hodnotu zabere hodně času a uvažování. Pouze 21 % respondentů uvedlo, že dokáží peněžně vyčíslit hodnotu svého soukromí.

4.1.24 Jaká je v penězích celková hodnota Vašeho soukromí?

Následuje otázka, jejímž cílem bylo, aby se respondenti zamysleli, co vše spadá do jejich soukromí a jakou to má celkovou peněžní hodnotu.



Obr. 24: Celková hodnota soukromí [vlastní]

I když většina lidí, nebyla schopná vyčíslit hodnotu svého soukromí, tak 49% respondentů tvrdí, že hodnota jejich soukromí je více než 1 000 000 Kč. Dá se přikládat tomu, že si svého soukromí a jsou si vědomi, že třeba osobní údaje můžou mít obrovskou hodnotu. Dále 15 % odpovědělo, že hodnota jejich soukromí je 500 000 – 1 000 000 Kč. Nejspíše zhodnotili, kolik mají například peněz na účtu, jaké mají soubory v počítači a pokusili se tuto hodnotu vyčíslit. Následuje skupina respondentů s 13 % hlasů, podle kterých je hodnota jejich soukromí 50 000 – 250 000 Kč. Pouze 12 % respondentů se domnívá, že jejich soukromí nemá žádnou peněžní hodnotu. Následuje hodnota 10 – 50 000 Kč, na kterou vyčíslilo své soukromí 7 % Respondentů. Pouze 4 % respondentů se shoduje na tom, že hodnota jejich soukromí je menší než 10 000 Kč.

4.1.25 Kdyby existovala možnost pojistit si své soukromí u pojišťovny, využili byste této pojistky?

V dnešní době existují pojistky, téměř na vše, proto bylo cílem této otázka, zda by si respondenti své soukromí pojistili, kdyby tato možnost existovala.

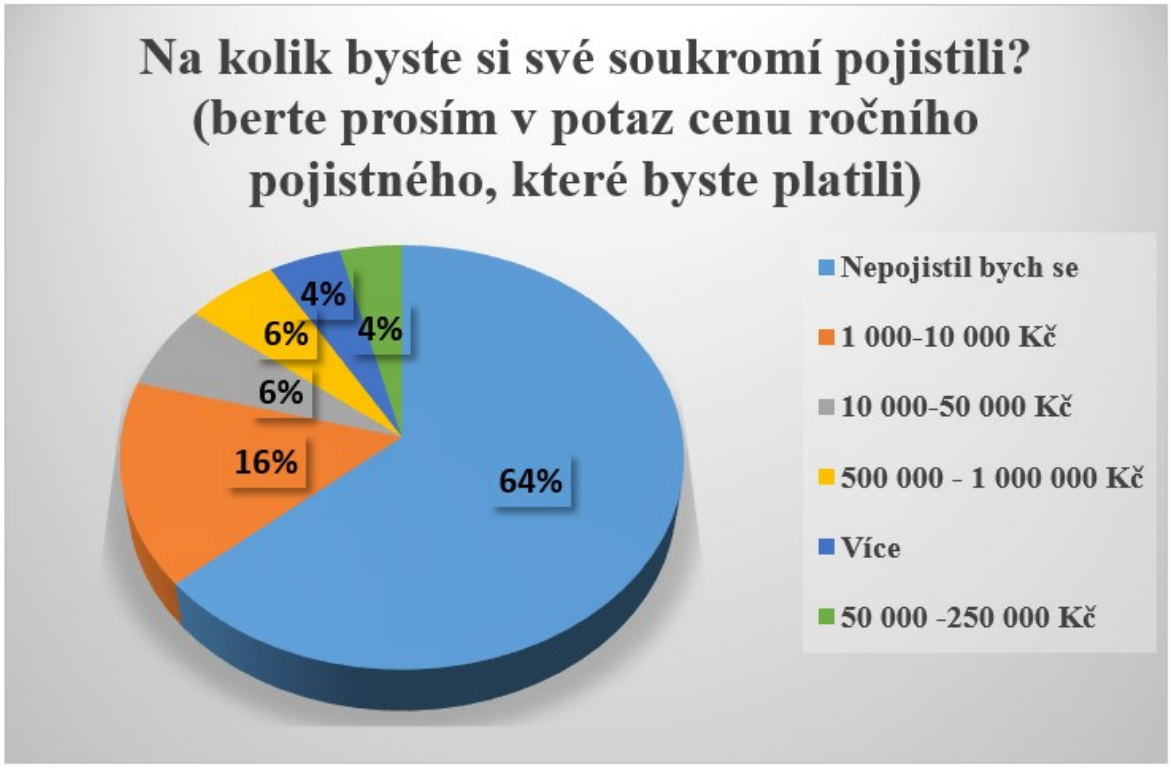
Obr. 25: Využití pojištění soukromí [vlastní]

Velká část respondentů vyčíslila své soukromí na více než 1 000 000 Kč, přesto by si 68% respondentů své soukromí nepojistilo. Dá se to předpokládat, že nejspíše by jim vadili další výdaje za pojistku, nebo dostatečně neuvažují nad svým soukromím jako aktivem, které opravdu má určitou finanční hodnotu.

Pojištění soukromí se tedy pro větší část lidí nejeví jako vhodná ochrana soukromí.

4.1.26 Na kolik byste si své soukromí pojistili? (berte prosím v potaz cenu ročního pojistného, které byste platili)

Poslední otázka dotazníku zní, na kolik by si respondenti své soukromí pojistili. Tato otázka cílila na to, zda si respondenti cenní svého soukromí natolik aby byli ochotní platit si na něj určitou pojistnou částku za jeho lepší ochranu.



Obr. 26: Částka pojistky [vlastní]

Jak již z průzkumu vyplynulo větší polovina respondentů, by své soukromí nepojistilo 64%. Pouze 16% respondentů by své soukromí pojistilo na 1 000 – 10 000 Kč. Shodně 6% respondentů by své soukromí pojistilo na 10 100 – 50 000 Kč a 500 000 – 1 00 000 Kč, 4% respondentů by své soukromí pojistilo na 50 000 – 250 000 Kč. Pouze 4% respondentů by uzavřela pojistku vyšší než 1 000 000 Kč. Celkově z průzkumu vyplývá, že pojištění se respondentům nejeví jako vhodná ochrana jejich soukromí.

4.2 Shrnutí dotazníku a specifikace problémů

Z dotazníku vyplývá, že lidé se nejvíce obávají o své osobní údaje a zejména z pohledu toho, že jsou snadno dohledatelné na internetu. Jedná se o jakousi digitální stopu, kterou zanechali vědomě, nebo ji o nich zanechala třetí strana. Zanechávání digitální stopy je problém, který je určitě aktuální a pokusíme se jej co nejlépe vyřešit v další části práce.

Se zanecháváním digitální stopy souvisí i snadný přístup k osobním údajům z veřejně dostupných zdrojů. Lidé mají své osobní informace vyplněny na svých profilech, nejrůznějších webech a registrech, kde je pro pachatele jednoduché je dohledat. Z mého pohledu by téměř nikdo, neměl mít důvod k tomu, aby jeho osobní údaje byly veřejně viditelné, pokud si to výslovně nepřeje a neumístí je na jakýkoliv web, nebo sociální síť s tím účelem, že chce, aby byl dohledatelný.

S volně dostupnými osobními údaji následuje další problém, který lidé z dotazníkového šetření považují za nejhorší a to zneužití identity, nebo některých osobních údajů k nejrůznějším bankovním podvodům. S tímto problémem nejvíce souvisí i to, že některé půjčky lze vyřídit například po telefonu, nebo přes internet a není zde nutná ani osobní schůzka. Je to velmi dobře viditelné na konkrétním případu zneužití identity, který byl popsán v teoretické části práce. Navazuje to na problém toho, že když jsou tyto osobní údaje již dohledatelné a identifikační prostředky jako občanské průkazy zfalšovatelné, nedisponujeme žádným nástrojem, který by identitu důvěryhodně ověřoval.

Nikoliv za nejhorší, ale za nejčastější narušení soukromí lidé považují kyberšikanu. Kyberšikana je zajisté problém, se kterým jsme se dříve nepříliš setkávali, ale v dnešní době je čím dál více častější. Souvisí to zajisté s přechodem do virtuálního prostředí a jakousi anonymizací pachatelů, kdy útočníci jsou ukryti za falešnými profily na sociálních sítích. Anonymita pachatelů je obrovský problém virtuálního prostředí a napomáhá k omezování soukromí obětí kyberšikany, pomluv, kyberstalkingu a nejrůznějších forem diskreditace a pomluv.

Dalším identifikovaným problémem je zajisté to, že lidé nepovažují GDPR za dostatečnou ochranu osobních údajů a to navzdory tomu, že GDPR by mělo napomáhat k řešení správy osobních údajů a jejich používání. Identifikovanými problémy z hlediska ochrany soukromí jsou:

- Zanechávání digitální stopy
- Snadný přístup k osobním údajům
- Kyberšikana
- Absence důvěryhodného nástroje pro ověření identity
- Nedostatečná ochrana osobních údajů nařízením GDPR

4.3 Analýza ochrany soukromí pomocí interview

Pro lepší pochopení problému a potvrzení toho, že problémy které byly identifikovány z dotazníkového šetření, jsou opravdu problémy, které se dějí a můj výzkum, neměl pouze kvantitativní, ale i kvalitativní hodnotu, jsem provedl interview s policistou a právníkem. S policistou byly řešeny otázky související s narušením soukromí. S právníkem byly řešeny otázky ohledně právního ukotvení soukromí. Zda považuje právní ochranu soukromí za dostatečnou. Další část rozhovoru se týkala GDPR a toho jaké změny z hlediska právní ochrany soukromí, můžeme v budoucnu očekávat.

4.3.1 Interview s příslušníkem Policie ČR

První interview mi poskytl příslušník Policie ČR policista, jménem Tomáš, který si nepřál, aby bylo zveřejněno jeho celé jméno. Otázky se týkaly převážně trestné činnosti spojené s narušením soukromí, jako je stalking, nebo kyberšikana, ale i nejrůznější pomluvy a četnosti těchto trestných činů.

Mou první otázkou bylo, zda řeší nějaké případy narušení soukromí (stalking, kyberšikana, sledování).

Odpověď: Nejčastěji se jedná nejrůznější pomluvy. Nejzajímavějším případem, kdy se snažili zdiskreditovat poměrně známou osobu v legislativě, která proti nim šla, na základě shody jmen ze starých složek STB, kdy se snažili dokázat, že byl členem STB na základě shody jmen. Dalším případem pomluvy, byl případ, kdy se před volbami snažili o zdiskreditování starosty. Ovšem tyto případy pomluv, řešíme jen tehdy, když mají velký společenský dopad.

Řešíte i jiné případy narušení soukromí, například stalking, nebo kyberšikanu?

Případy stalkingu řešíme. Legislativní název je nebezpečné pronásledování. Teď si vzpomínám na jeden konkrétní případ. Ti pachatelé jsou většinou bývalý partneři, nebo milenci. Ten konkrétní případ, chlap čekal od 23:00 do 3:00 do rána před barákem, zvonil na zvonek a psal jí zprávy. Zde je problém i to, že mnohdy oběť s pachatelem komunikuje a občas mu napíše jako první, takže je těžké dokázat, že se opravdu jedná o nebezpečné pronásledování.

Kyberšikanu jste někdy řešil?

Tyto případy většinou řeší oddělení kyberkriminality, ale dá se říct, že tyto případy jsou častější. Ale nemám náhled do spisů, abych Vám řekl kolik těch případů opravdu je, protože

je otázka kolik se toho nahlásí. Ale já jsem zaznamenal případ, kdy kluci opili holku, natáčeli ji při intimních věcech. Potom toto video nahráli na internet a různě si ho posílali.

Ještě jsem zaznamenal případ, kdy se rozešel kluk s holkou a ten kluk zřídil na erotických stránkách profil té holky. Dal tam nahé fotky pornoherečky, co se jí podobá, její jméno a její telefonní číslo, že nabízí erotický služby.

Řešíte i případy zneužití osobních údajů?

Případy, kdy si někdo vezme třeba půjčku na občanku, nebo tak? S tímto jsem se moc nesetkal, ale většinou to přebírá rovnou kriminálka. Spíše řeším krádeže kreditek a platebních prostředků. Vím, že cizinecká policie dost řeší, že někteří cestují na podobnost, že si koupí od někoho platný pas a jede přes hranice na cizí pas, jen na podobnost.

Jak často tyto případy narušení soukromí řešíte?

Moc je neřešíme. Spíš řešíme případy s majetkovou podstatou, než duševního a nehmotného vlastnictví, jako je identita a ochrana osobních údajů, ale třeba případy kyberšikany se rozmohly víc než dřív, ale je otázka kolik se jich opravdu nahlásí.

Když už nějaké případy řešíte, o jaké případy se nejčastěji jedná?

Nejčastější je určitě pomluva, ale aby to naplnilo trestní rovinu, musí to mít fakt vážnější společenský dopad. Jinak je to řešeno jako soužití, nebo přestupek. Většinou řešíme, až když se jedná o nějaké zdiskreditování někoho jiného. Potom jsou to ty případy stalkingu, nebo kyberšikany. Se zneužíváním osobních údajů, nebo krádeže identity jsem se já osobně nesetkal, ale netvrdím, že se jinde nedějí, nebo tyto případy neřeší.

O jaké skupiny lidí se nejčastěji jedná?

Ta kyberšikana je nejčastěji problém mladých lidí. Co se týká stalkingu tak, se jedná většinou o bývalého partnera, nebo milence. Ale zažil sem i případ, že si vyhlídl holku, co se mu líbila, namontoval jí do auta GPSku a sledoval ji tímto způsobem. U těch pomluv je to různé, ale většinou řešíme, až to má opravdu nějaký dopad. Až když se jedná o společensky důležitější lidi.

Jak by si podle Vás měli lidé soukromí lépe chránit, myslíte si, že by mělo smysl třeba pojištění soukromí?

Určitě nedávat na Facebook a Instagram o sobě všechny informace, aby lidi hned nevěděli o člověku všechno. Další bych řekl hlídat si líp své osobní doklady, protože denně řešíme případy ztrátu dokladů. Další bych řekl, dávat si pozor co kde lidé o sobě píšou na internetu.

Myslíte, si že soukromí má vyšší hodnotu než dříve?

Jsem mladší generace, takže sem nezažil, že jsem nemusel řešit, jak to bylo dřív, když ten náhled do soukromí nebyl tak jednoduchý. Ale myslím si, že vzhledem k tomu jak je všechno provázané, má soukromí určitě vyšší hodnotu než dřív. Zejména, že už třeba i internetové prohlížeče o nás shromažďují informace a monitorují nás. Dále jsou volně přístupné registry, jako katastrální registr, nebo pojistitelský registr. I ta hranice soukromí se určitě posunula a soukromí neznamená to soukromí, co bylo dřív.

Domníváte se, že v budoucnu se bude policie specializovat na narušení soukromí (jako např. na vraždy, hospodářské delikty atd.).

Myslím si, že ne. Máme oddělení obecné kriminality, hospodářské kriminality a kyberkriminality, takže se to podle kvalifikace někam přihodí. Navíc o soukromí není žádný paragraf, vždy se to pod něco hodí.

4.3.2 Interview s právníkem

Druhým člověkem, který mi poskytl interview, byl olomoucký právník. Otázky směřovali na právní ukotvení soukromí v české legislativě a měli za úkol ověřit, zda je v České republice soukromí dostatečně právně chráněno.

První otázkou bylo, které zákony a vyhlášky se zabývají ochranou soukromí

Takto z hlavy to bude občanský zákoník, trestní zákoník a dále GDPR.

Domníváte se, že v České republice je soukromí, dostatečně právně ukotveno?

Domnívám se, že nedostatečně.

A dochází v dnešní době ke zvýšení právní ochrany soukromí?

No jediné co mě napadá, jsou nové směrnice o ochraně osobních údajů GDPR. Dochází zde k mírném zvýšení právní ochrany soukromí.

Myslíte si, že GDPR pomohlo v ochraně osobních údajů?

Z mého pohledu si nemyslím, že by zásadně pomohlo, protože minulá právní úprava, ač nebyla dobře vymahatelná, nebyla o tolik rozdílná oproti dnešnímu GDPR. GDPR tudíž

nebylo zásadním přelomem. Jedině v tom, že si spousta lidí začala uvědomovat, že se o údaje musí starat, i když to museli dělat i předtím. Ale právní stav, před GDPR a po GDPR se úplně nezměnil. Ale u lidí k změnu došlo, převážně v jejich informovanosti, že se musí o osobní údaje starat.

Z mého pohledu, se změnilo pouze to, že jsou lidé informovaní lépe, ale jen s tím rozdílem, že musí souhlasit s více smluvními podmínkami. Ale k žádné zvýšené ochraně osobních údajů přesto nedošlo. Vnímáte to podobně?

Ano, toto vnímám úplně stejně, ale tím, že se o tom hodně mluvilo, si dost lidí uvědomilo, že si musí osobní údaje hlídat. Když jim řeknu, že to museli dělat i 10 roků dozadu, tak nechápali. Alespoň to posloužilo jako osvěta.

Jde brát z právního hlediska soukromí, jako aktivum, které má určitou peněžní hodnotu?

Z faktického hlediska ano, z praktického si to úplně nemyslím. Samozřejmě škoda, pokud Vám zasáhnou do soukromí, by měla být ocenitelná. Prakticky svoje soukromí prodáváme všichni, ale právně by to takto býti nemělo.

Dochází z Vašeho pohledu k nárůstu narušení soukromí? Mění se formy narušení soukromí?

V jakém horizontu? V horizontu třeba 20 let určitě ano a formy se mění. Ale i třeba v horizontu 5 let bych také řekl, že dochází k nárůstu.

Myslíte, že se časem dočkáme právní specializace na ochranu soukromí? (jako např. v rozvodovém právu)

Myslíte, že vznikne nová právní disciplína, nebo že budou lidé, kteří se budou specializovat na ochranu soukromí? Že vznikne nová právní disciplína, si nemyslím. Ale druhý případ, že budou lidé, kteří se budou specializovat na ochranu soukromí, to máme už teď. V budoucnu určitě, budou existovat kolegové, kteří se budou zabývat výhradně tady tím, ale aby to vzniklo jako samostatná disciplína v rámci práva, to si nemyslím.

4.3.3 Dílčí závěr

Interview daly podklad k tomu, že k narušení soukromí opravdu dochází. Policista potvrdil, že případy narušení soukromí, zejména kyberšikany jsou častější. Pro praktickou část práce, návrhu řešení problému interview přispěl skrze to, že problémy, které byly identifikované

v dotazníkovém šetření, nejsou jen problémy, o kterých se domnívá veřejnost, ale že se opravdu dějí.

Další interview, který byl veden s právníkem, se týkal především právního ukotvení soukromí. Interview potvrdil, že soukromí není dostatečně právně chráněno. Zejména skrze vyhlášku GDPR, která sice zvýšila obeznámenost lidí, ale nijak nezvýšila ochranu osobních údajů. Právník i respondenti z dotazníkového šetření se shodli na tom, že GDPR není dostatečnou ochranu osobních údajů a soukromí.

5 NÁVRH ŘEŠENÍ IDENTIFIKOVANÝCH PROBLÉMŮ

Většina nových problémů, související s narušením soukromí, je spjata s přechodem do kybernetického prostředí. Lidé se nejvíce bojí o své osobní údaje, které jsou dostupné právě na internetu, v nejrůznějších rejstřících, ale i na sociálních sítích, diskuzních fórech a dalších stránkách kde buďto uživatelé, nebo třetí strana o nich ukládá osobní údaje.

Dalším problémem, souvisejícím se soukromím, je sběr údajů, které nezanecháváme vědomě. Jedná se o různé soubory cookies, polohy a nejrůznější identifikační znaky nějakého uživatele internetu, které jsou dále uchovávány webovými stránkami a mnohdy i dále šířeny.

Přechod do kybernetického prostředí velmi napomohl i narušení soukromí skrze šíření nejrůznějších pomluv, nebo jiné snahy o to člověka zdiskreditovat. Nyní můžeme na internetu vystupovat anonymně i anonymně komunikovat s dalšími lidmi. S anonymitou pachatelů nepochybně souvisí i nárůst kyberšikany, kdy pachatelé se díky tomu, že vystupují pod falešnými profily, méně bojí o to, že budou odhaleni a chovají se o to brutálněji.

S tímto přechodem do kybernetického prostředí mnohdy i doplácíme na to, že metody ověřování identity, které byly dříve dostačující, dnes už dostačující nejsou. Je mnohem jednodušší o někom vyhledat osobní informace a ty následně přetvořit v doklad totožnosti, který pachatelé budou moci nadále použít pro různé bankovní půjčky a platby.

Samotný přechod do online prostředí neznamená nutně přímo riziko pro soukromí, ale je díky němu soukromí mnohem zranitelnější a přicházejí s ním nové problémy, které vyplynuly již z dotazníkového šetření. Jako nejvýznamnější problémy spojené se soukromím a jeho ochranou tedy shledávám:

- Zanechávání digitální stopy
- Snadný přístup k osobním údajům
- Anonymita pachatelů (kyberšikany, kyberstalking, pomluvy, vydírání)
- Absence důvěryhodného nástroje pro ověření identity
- Nedostatečná ochrana osobních údajů nařízením GDPR

5.1 Zanechávání digitální stopy

Digitální stopa je využívána v mnoha odvětvích. Nejčastěji se jedná o marketing prostřednictvím chytrých behaviorálních reklam. Kdy společnosti jako Google, Facebook o

uživatelích shromažďují údaje, které jsou využívány pro reklamní účely. Tyto reklamy využívají údaje z aktivity uživatelů na internetu a podle toho co navštěvuje nejvíce, nabízí uživatelům reklamy. Behaviorální reklamy jsou podle respondentů narušením soukromí. Dalším využitím digitální stopy je například personalistika, kdy zaměstnavatelé vyhledávají informace o svých budoucích zaměstnancích.

Nejhorší využitím digitální stopy je samozřejmě trestná činnost, kdy pachatelé cíleně vyhledávají informace o svých obětech, které se následně snaží využít. Může se jednat o nejrůznější bankovní podvody, vylákání peněz od lidí, nebo vydávání se za cizí osobu.

Stejně jako digitální stopa napomáhá k trestné činnosti, lze ji stejně dobře využít proti pachatelům, kteří trestnou činnost konají. Může i sloužit jako prevence při sledování například teroristických skupin, podezřelých osob z trestné činnosti, nebo k dohledávání pachatelů.

5.1.1 Zanechávání digitální stopy

I přesto, že digitální stopu lze využít k dohledávání pachatelů trestné činnosti, je pro většinu uživatelů internetu i pro ochranu soukromí důležité digitální stopu nezanechávat, nebo její zanechávání minimalizovat.

Jak již bylo řečeno v teoretické části, úplnému nezanechávání digitální stopy, pokud chceme používat internet plnohodnotně, nelze. Jediné řešení, jak nezanechávat žádnou digitální stopu by bylo nepoužívat internet vůbec. To ovšem není přijatelné, protože žijeme v digitálním světě, kde se téměř všechny úkony dají řešit online a je to mnohdy jednodušší a šetří nám to čas.

5.1.2 Současná řešení minimalizace digitální stopy

Minimalizovat svou digitální stopu není pro běžného uživatele nic jednoduchého a zabere to navíc čas a používání internetu, nebude tak rychlé a praktické.

Zanechávání digitální stopy lze minimalizovat například používáním nejrůznějších anonymních režimů. Anonymní režimy nám částečně umožní nezanechávat digitální stopu. Anonymní režim nedovolí o nás sbírat informace, co a kde jsme vyhledávali, tudíž můžeme používat internet více anonymně, ale jedná se spíše o aktivitu na webových stránkách, soubory cookies a údaje například o IP adrese apod. se budou nadále ukládat. Používání anonymních režimů nám sice část soukromí ochrání, ale nejedná se o úplné řešení. [11]

Prohlížeče už nyní nabízí i možnost blokovat cookies třetích stran. Jedná se nejčastěji o cookies majitelů reklam na webu, které jsme navštívili. Ti tyto cookies se využívají nejčastěji pro reklamní účely. Dnešní prohlížeče už nabízí blokování cookies třetích stran, můžeme ho nálezt například v prohlížeči Mozzila Firefox, nebo Safari. [30]

Ovšem některé weby nefungují plnohodnotně bez těchto cookies třetích stran a neřeší to problém uložení cookies první strany (majitele webu), který o nás může dále shromažďovat nejrůznější informace.

Dalším řešením jsou nejrůznější šifrovací programy a zařízení. Pomocí šifrovacích programů a zařízení lze svou digitální stopu šifrovat. Ovšem tyto programy jsou mnohdy nákladné a nemůžeme si být jisti, zda fungují, tak jak si přejeme.

Řešením může být i zakoupení si nejrůznějších šifrovacích zařízení, jako je například šifrovací mobilní telefon, který šifruje veškerou komunikaci, vyhledávání apod. Ovšem tato zařízení představují finanční náklady při koupi zařízení a jejich provoz nebude tak komfortní jako při běžných zařízeních.

5.1.3 Právo být zapomenut

Z internetu lze vymazat údaje o naší osobě. Jak již vyplynulo z dotazníkového šetření, nejvíce se lidé obávají o své soukromí z důvodů, že jejich osobní údaje jsou jednoduše dohledatelné. Řešením může být využití práva „být zapomenut“.

Například společnost Google umožňuje vymazat URL odkazy, které odkazují na údaje o naší osobě. Pro vymazání těchto údajů stačí vyplnit formulář společnosti Google.

Postup podání formuláře:

- Vyplnit jméno uživatele
- Odkaz na adresu URL odkazu s osobními údaji, které chce uživatel odstranit
- Důvody, které vedou k vymazání těchto odkazů
- Zaslání fotokopie průkazu žadatele [31]

Ovšem využití tohoto práva je poměrně složité, jelikož je těžké ho uplatnit, zejména pokud jsou naše osobní údaje využívány státními institucemi. Proto, aby mohly být osobní údaje vymazány, musí splňovat následující podmínky:

- *„osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány,*

- *subjekt údajů odvolá souhlas a neexistuje žádný další právní důvod pro zpracování,*
- *subjekt údajů vznese námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování,*
- *osobní údaje byly zpracovány protiprávně,*
- *osobní údaje musí být vymazány ke splnění právní povinnosti,*
- *osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti podle článku 8 odst. 1 Obecného nařízení.“* [7]

5.1.4 Návrh řešení

Všechny tyto nástroje, které jsou momentálně dostupné ke spravování naší digitální stopy, jsou neúplné a mnohdy nezajišťují ochranu soukromí. Používání anonymních režimů, skryje pouze část digitální stopy, šifrovací zařízení jsou nákladná a nemusí plnit účel ochrany soukromí. Navíc pro běžného uživatele jsou tyto metody značně nepraktické z důvodů časových i finančních nároků.

Možným řešením je, aby se digitální stopa ukládala pouze do chráněného registru, který by byl zabezpečován například Googlem. Tento registr by byl přístupný pouze Googlu a například oddělením Policie ČR pro boj s kyberkriminalitou. Byl by uložen v anonymizované formě tak, aby mohl sloužit pouze pro jednodušší a příjemnější relaci webových stránek (pamatoval si oblíbené videa apod.). Důležité by bylo, aby nebyl přístupný žádné třetí straně, o které už nevíme, jak s osobními údaji nakládá. Úřady pro boj s kyberkriminalitou, by měly přístup do registru bez šifrování. Ideální by bylo, kdyby se domluvili všichni majitelé velkých společností a tento problém s uchováváním dat o uživatelích vyřešili společně, nebo všechny tyto informace o uživatelích byly shromážděny pouze na jedno místo, odkud by se mohli brát jen anonymizované indicie od uživatelů k funkčnosti webu.

Vymazat celou digitální stopu určitě není možné. Už skrze dohledávání pachatelů kyberkriminality, nebo skrze to, že by internet už nebyl místem jako dřív, hlavně kvůli tomu, že by weby, které nic neprodávají a jsou pouze informační, nemohly dále nijak žít z reklam a jejich provoz by byl značně omezen a to ovšem nikdo nechce. Ideálním řešením by bylo těmto majitelům reklam poskytovat opravdu jen nějaké anonymizované indicie, které by

napomohly k tomu, aby si mohli vytvořit svou chytrou reklamu, a nadále platili majitelům webu za reklamu, aby i informační weby mohly nadále stále fungovat.

Toto řešení se nabízí pouze pro digitální stopu zanechanou jako vedlejší činnost na internetu. Řešením digitální stopy, kterou zanecháváme vědomě při nejrůznějších registrování, vyplňování profilů, nebo to co o nás umístí někdo jiný žádným krytým registrem na osobní údaje a fotografie nelze. Zde lze využit jen již zmiňované právo „být zapomenut“, aby poskytovatelé služeb smazali údaje o osobě uživatele. Využití práva „být zapomenut“ je ovšem zdlouhavé a poměrně komplikované. Jediným řešením smazání obsahu na nejrůznějších místech o osobě uživatele by bylo zjednodušit proces práva „být zapomenut“.

5.2 Snadný přístup k osobním údajům

Hlavním problémem spojeným s krádeží identit a nejrůznějšími bankovními podvody, jsou lehce dohledatelné osobní údaje. Pachatelům stačí znát jméno své vytipované oběti a z nejrůznějších zdrojů dostupných na internetu jsou schopni poskládat celou identitu. Ke všemu jim stačí pouze zadat jméno do internetového vyhledávače.

Většina těchto osobních údajů je dostupná díky neopatrnosti uživatelů internetu. Z pohledu ochrany se jedná především o neobeznámenost lidí, kteří údaje o své osobě vyplňuji i přesto, že to není nutné k úkonu, který se chystají provést. Jedná se zejména o vyplňování osobních údajů na profily sociálních sítí a vyplňování osobních údajů na nejrůznější weby.

Dalším problémem osobních údajů je i to, že je mnohdy zveřejňuje i další strana. Může se jednat o nejrůznější smlouvy na internetu, obchodní rejstříky a další rejstříky, kde jsou mnohé osobní údaje o osobách.

Tyto údaje je pak velice snadné zneužít. Dají se zneužít například k již zmíněným bankovním podvodům, kdy pachatelé vytvoří falešné dokumenty (občanské průkazy, řidičské průkazy), na které si budou brát půjčky. Konkrétní případ, krádeže identity k bankovním podvodům byl podrobněji popsán v kapitole 3.2.1 Krádež identity a bankovní podvody.

Dalším častým případem zneužití osobních údajů je formou emailu. Pachatelé vytvoří emailové adresy, které se podobají pravým emailům. Tyto emaily následně posílají například sekretářkám, nebo účetním svých obětí, kdy požadují platbu na určitý účet. Nejčastěji své platby vydávají za běžné transakce, které vypadají důvěryhodně a v účetních obětí nebudí žádné podezření na podvodnou platbu.

Dále si jen pachatel může zjišťovat údaje o oběti, jako je bydliště, místa, kde se často nachází, zaměstnaní apod., k tomu, aby jej mohl sledovat. Většina případů stalkingu je sice od osoby, která má s pachatelem nějaký vztah, ale jsou i případy, kdy si pachatel svou oběť vybere náhodně na internetu a poté si o ní zjišťuje nejrůznější údaje k tomu, aby ji mohl sledovat. Z počátku se jedná o stalking ve virtuálním prostředí, který může přerůst až ve stalking fyzický, kdy oběť sleduje.

5.2.1 Opatrnost při vyplňování osobních údajů

Nejlepším řešením problému snadného přístupu k osobním údajům je osobní údaje nepoužívat. Mnohdy to samozřejmě nejde, ale uživatelé by si měli být vědomi, kam zadávají své osobní údaje. Pokud je to možné, zadávat osobní údaje pouze při online nákupech, online platbách a při službách, kde je to nutné. Například při ubytování v hotelech, na úřadech apod.

Pokud poskytovatel webu vyžaduje vyplnit osobní údaje za nějakou službu, (shlédnutí videa, stažení souboru) a nemáme zájem o to, aby měl naše osobní údaje, používat pro tyto registrace speciální email (ne osobní, pracovní) a zadat smyšlené jméno i údaje.

5.2.2 Doporučení k nakládání s osobními údaji

- Při registracích na webové služby, zadávat jen nejnutnější množství osobních údajů
- Kontrolovat důvěryhodnost webové stránky (SSL)
- Pokud se nejedná o závaznou objednávku, ale jen využívání online služeb, použít falešné osobní údaje
- Nezadávat na tyto služby svůj osobní email, ale email, který používáme jen pro tyto účely
- Nepřidávat na sociální sítě žádné osobní údaje (zejména místo bydliště, datum narození, mobilní číslo, osobní email (použít email, který není určený pro osobní komunikaci, práci) informace o osobním životě apod.)
- Na sociálních sítích kontrolovat, zda všechny kontakty známe, respektive potřebujeme je mít v přátelích
- Kontrolovat, co kde píšeme a zda by nám to nemohlo v budoucnu ublížit, údaje a informace vložené na internet je téměř nemožné odstranit

- Pokud své osobní údaje již zadáváme, kontrolovat k jakému účelu budou osobní informace použity, zda budou dále šířeny a po jakou dobu budou archivovány
- Seznámit se se smluvními podmínkami služeb, které používáme

5.2.3 Zvýšit obeznámenost uživatelů

Pokud si uživatelé nebudou vědomi toho, jak je s jejich osobními údaji nakládáno a jak se dají osobní údaje zneužít, budou dále přibývat případy bankovních podvodů, krádeže identit a narušení soukromí. Proto by bylo vhodné, aby se o této problematice více vědělo. V dnešní době už je naštěstí obeznámenost mnohem lepší, na internetu je plno článků, jak zacházet se svými osobními údaji, kdo o nás shromažďuje osobní údaje. Zkrátka je zde snaha o to, aby soukromí člověka zůstalo zachováno. Ovšem otázkou je, jak se lidé z těchto článků poučí. Proto je nutné obeznamovat lidi už v nižším věku o této problematice, například při výuce informatiky na základních a středních školách.

5.2.4 Návrh řešení

Návrh řešení uvedeného problému je skrýt osobní údaje před jejich vyhledáním pomocí speciálního nástroje. Jednalo by se o nástroj, mající stejnou funkčnost, jako používá Facebook, nebo Youtube na obsah s rasismem, extremismem, nebo sexuální tématikou, nebo dává varování, že obsah je nevhodný pro mladistvé a zda ho skutečně chceme vidět. Tento nástroj by fungoval na zakrývání obsahu části textu s osobními údaji, aby nebyl přístupný lidem, kteří ho chtějí zneužít. Viditelný by byl pouze se souhlasem uživatele, který opravdu chce, aby tento obsah byl vidět.

Myslím si, že návrh je realizovatelný, když už podobné nástroje existují, ale za jiným účelem fungují. Tento nástroj by fungoval na základě vyhledávání jména, data narození, rodného čísla, bydliště, telefonního čísla, ale například i IP adresy. Největší jeho nevýhodou by bylo, že algoritmus na vyhledávání osobních údajů, by nejspíše zakrýval i nezávadný obsah, který by byl osobním údajům podobný, ovšem tyto chyby by se daly s postupem eliminovat až k tomu, kdy by nástroj fungoval správně.

Dalším pomocníkem by bylo, posílaní varování uživatelům. Pokud by někdo často vyhledával něčí jméno s kombinací výrazů jako bydliště, datum narození apod. Dostal by tento člověk varování.

5.3 Anonymita pachatelů

V dnešní době máme možnost anonymně vystupovat na internetu (anonymně před ostatními lidmi). Můžeme mít profily na sociálních sítích s falešným jménem, falešnou emailovou adresou a jiné prostředky, díky kterým se budeme moci anonymně s někým spojit. Mnohdy to bereme jako velké pozitivum, ale má to i své stinné stránky, zejména pro oběti nejrůznějších forem pomluv, vydírání a kyberšikany.

Anonymita je hlavním důvodem toho, proč se sociální sítě a jiné komunikační prostředky stávají prostředky k realizaci nejrůznějších pomluv, vydírání, ale i kyberšikany. Kyberšikany se mnohdy dopouštějí i jedinci, kteří by při fyzickém kontaktu mnohdy svou oběť fyzicky, nebo psychicky nenapadali.

5.3.1 Kyberšikana

Kybešikana je podle dotazníkového šetření častým narušením soukromí, 62 % respondentů ji považuje za nejčastější narušení soukromí vůbec. Kyberšikana je problém převážně mladistvých na základních a středních školách. Může se stát, že obětí nějakého druhu kyberšikany se stávají i dospělí jedinci (například kyberstalking, sexting, vydírání), ale drtivá většina případů jsou oběti školního věku. Proto by žáci zejména na základních školách měli být více obeznamování s kyberšikanou, jak se jí můžou bránit, jaké postihy hrozí pachatelům a zejména, kde ji můžou anonymně nahlásit. Kyberšikana souvisí s narušením soukromí, protože oběti často zasahují do osobního života oběti. Sbírají o ní osobní údaje, nebo ji vydírají skrze osobní fotografie. Proto by součástí přednášek o kyberšikaně, měly být i přednášky, kde budou žáci seznámeni, jak nakládat s osobními údaji a fotografiemi.

Kyberšikana je velmi častá i z důvodů anonymity pachatelů. Pocit anonymity dává útočníkům více prostoru a možnost chovat se mnohem více zákeřně a agresivně. Kdyby se podařilo vyřešit problém anonymity pachatelů, problém kyberšikany by se značně omezil.

5.3.2 Doporučení obětem kyberšikany

Před samotným návrhem řešení problémů kyberšikany je potřeba, dobře obeznámit oběti s tím, jaké možnosti mají, když už kyberšikanu prožívají. Nejdůležitějším krokem je, si uvědomit, že být obětí kyberšikany není nic ponižujícího a je potřeba se tomu postavit. Nejdůležitější na celém procesu kyberšikany je sběr důkazů a samotné ohlášení kyberšikany.

5.3.2.1 Sběr důkazů

Důležitým krokem k odhalení pachatelů kyberšikany je sběr důkazů. Pokud se někdo dostane do problémů kyberšikany, je důležité sbírat důkazy, jako jsou uložené fotografie, kopie zpráv a další důkazy. Díky těmto důkazům je jednodušší pachatele odhalit a následně jej i usvědčit. [32]

5.3.2.2 Ohlášení

Oběti kyberšikany se mnohdy stydí za to, že jsou obětí kyberšikany. Je proto důležité, když se oběti nechtějí svěřit například své rodině, nebo učitelům, aby měly možnost ohlašovat kyberšikanu anonymně. Kyberšikanu lze například anonymně nahlásit na linku Národního centra bezpečnějšího internetu. [32]

Ovšem, aby k těmto krokům mohlo docházet, musí být oběti dobře seznámeny s tím, že tyto možnosti, jako je anonymní nahlášení, existují. Dalším důležitým krokem je i prevence proti kyberšikaně. Všichni by si měli uvědomovat, jaké může mít kyberšikana následky pro oběť, ale i pachatele jelikož se jedná o trestný čin.

5.3.3 Návrh řešení problému

Navrhovaným řešením problému kyberšikany, ale i jiných deliktů kdy se pachatel skrývá za svou anonymitu a narušuje tak soukromí a osobní život jiného je důkladnější verifikace profilů na sociálních sítích. Většina případů kyberšikany probíhá právě na sociálních sítích. Pachatelé mnohdy používají falešné profily proto, aby se dostali do kontaktu se svou obětí, nebo svůj profil vydávají za někoho jiného. Mnohdy si založí i falešný profil oběti, z kterého se za oběť vydávají a snaží se ji tím poškodit. Pokud by se profil musel vázat na oficiální doklad totožnosti (např. e-identita), nebyla by možnost zakládat falešné profily, popřípadě by bylo jednodušší zjistit, kdo za tímto falešným profilem je a kdo se za něj vydává.

Tento návrh řešení je poněkud radikální, ale dokud se budou moci útočníci schovávat za anonymitu profilu, budou i nadále přibývat nejrůznější případy kyberšikany a dalších případech poškozování druhého přes tyto profily i přes doporučení a opatření, které jsou popsány v doporučení obětem kyberšikany.

5.3.3.1 Ztráta soukromí

Argumentací je, že by mnozí lidé přicházeli o své soukromí tím, že by nemohli anonymně používat tyto sociální sítě a jiné prostředky pro komunikaci. Dalším důvodem nezavést toto

opatření je to, že by majitelé sociálních sítí měli například číslo našeho občanského průkazu, které by odtud mohlo uniknout. Ovšem číslo občanského průkazu a naše pravé jméno, musíme uvést například při ubytování a jiných službách, kde je mnohem větší šance úniku těchto dat, než od majitelů nejrůznějších gigantů, kteří vlastní tyto sociální sítě a mohou si dovolit tyto údaje uchovávat v anonymizované formě a na mnohem bezpečnějších uložištích, než některé orgány, které naše osobní údaje uchovávají s mnohem menším zabezpečením.

5.3.3.2 Mladiství

Sociální sítě, jsou většinou dovoleny k užití od 13 let. Ovšem v České republice máme občanské průkazy sloužící k identifikaci od 15 let. Můj návrh je ten, aby si mladiství ověřovali své profily pomocí občanských průkazů, nebo e-identity jednoho z rodičů, nebo jiného zákonného zástupce, protože osoby mladší 15 let mohou používat sociální sítě a jiné internetové služby, kde je zapotřebí registrace pouze se souhlasem rodičů.

5.4 Absence důvěryhodného nástroje k ověření identity

Přechod k virtuálnímu prostředí vede k tomu, že můžeme provádět online platby, online nákupy apod. a přesto nikde není vyžadována naše identita. K verifikaci stačí většinou číslo kreditní karty, heslo, email apod., které pachatel dokáže získat, třeba díky podvodným emailům, hackerským útokem, nebo metodami sociálního inženýrství.

Přitom kdybychom chtěli tyto úkony provést osobně, byl by zapotřebí minimálně platný občanský průkaz s fotografií a podpis, kterými bychom měli prokázat, že se jedná skutečně o nás. Ale jak jsme již viděli v případě bankovních podvodů mužů z Ostravska, které jsou rozebírány v teoretické části práce, si stačilo pouze vyhledat osobní údaje na internetu a díky nim tyto občanské průkazy zfalšovat. Tudíž tyto nástroje k ověření identity jsou v dnešní době poměrně zastaralé a navíc se téměř nikdo nekontroluje, zda občanský průkaz není nijak zfalšovaný.

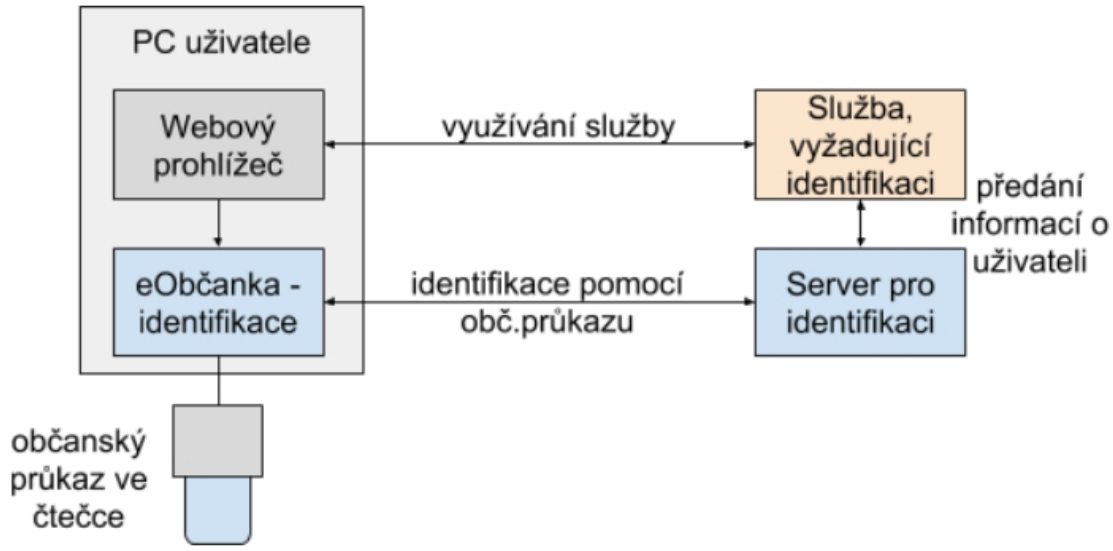
5.4.1 Občanské průkazy

Občanský průkaz slouží k ověření naší identity. Jsou na něm naše osobní údaje jako: rodné číslo, místo bydliště, fotografie a podpis. Ovšem tyto průkazy totožnosti jsou v dnešní době poměrně zastaralé, protože existuje spousta úkonů, ke kterým se sice občanský průkaz potřebuje, ale už se neověřuje jeho pravost. Jedná se zejména o podvodné půjčky, které byly popsány v teoretické části práce.

5.4.2 Elektronická identita

V České republice jsou od 1. července. 2018 vydávány občanské průkazy s elektronickým chipem. Ovšem většina lidí má občanské průkazy staršího data, nebo i přesto, že mají nové občanské průkazy, tento chip nijak nevyžívají. Aktivace tohoto chipu je dobrovolná.

Pomocí těchto elektronických identit lze vytvářet i digitální podpisy a provádět některé úkony online, slouží k identifikaci online službám pro veřejnou správu. Ovšem, abychom mohli využívat tuto elektronickou identitu online, je zapotřebí mít aktivovaný chip v občanském průkazu vydaném po 1. července. 2018, zakoupenou čtečku čipových karet a nainstalovanou podpůrnou aplikaci. Postup ověření elektronické identity je vysvětlen na obrázku číslo 27. [33]



Obr. 27: Schéma identifikace e-identity [33]

5.4.3 Návrh řešení problému

Problémem zde již není, že nedisponujeme vhodným nástrojem k ověření identity, ale to, že tento nástroj není nikde vyžadován. Jediné místo kde ho můžeme, ale nemusíme využít, je pro služby veřejné správy. To je z mého pohledu obrovská škoda, protože tento nástroj se mi jeví jako spolehlivé ověření identity a jeho zfalšování je velmi komplikované.

Mým návrhem je zavedení používání tohoto chipu při více úkonech, zejména při převodech peněz a zřizování půjček. Zejména při zřizování půjček by se téměř zamezilo zneužití cizí identity, kdy by nestačilo tento občanský průkaz ukázat, ale bylo by nutné při těchto úkonech použít jeho chip + běžná verifikace, která funguje dnes.

Dále by se pomocí čtečky a chipu dalo implementovat na všechny platební úkony a půjčky, které se vyřizují online. Nevýhodou by bylo, že na každý by si byl ochotný zakoupit tuto čtečku a aktivovat chip. Aktivaci chipu bych ovšem zavedl jako povinnou a pro osoby, které by neuměly s tímto zařízením, nebo by nebyly ochotny si tuto čtečku zakoupit, by existovaly nejrůznější pobočky, které by zajišťovaly podporu tohoto druhu ověření identity a pomohly by těmto lidem s ověřením identity při půjčkách, platbách apod.

5.5 Nedostatečná ochrana osobních údajů nařízením GDPR

GDPR má sloužit k ochraně osobních údajů a mělo by určovat, jak s nimi bude zacházeno a jak manipulováno. Podrobněji je GDPR popsáno v teoretické části práce. V praxi ovšem jsou o uživatelích nadále ukládány osobní údaje majiteli nejrůznějších webů. Jediné co se změnilo je, že s tím souhlasíme ve smluvních podmínkách, které si majitelé webů vyžadují potvrdit, proto, abychom je mohli používat. Tudíž se zdá, že jediné co běžnému uživateli internetu přineslo GDPR je to, že se musí proklikat více smluvními podmínkami, které nám sice oznamují, že jsou tyto osobní údaje o nás shromažďovány a pro co jsou používány, ale nijak už nereguluje to, že osobní údaje jsou o nás shromažďovány. Nejedná se jen o webové stránky, ale i nejrůznější mobilní aplikace, které když chceme použít, musíme odsouhlasit jejich smluvní podmínky, které zahrnují používání našich osobních údajů, jinak tyto aplikace nebudeme moci používat.

5.5.1 Návrh řešení

Řešením se nabízí to, aby GDPR neregulovalo převážně to, že musíme být obeznámeni s tím, že o nás jsou shromažďovány osobní údaje, ale aby přímo nařizovala provozovatelům webových a mobilních aplikací, které údaje o nás mohou uchovávat. Je více než jasné, že ne všechny informace, které o nás jsou ukládány (s našim souhlasem) jsou potřeba pro chod těchto aplikací a stránek. Tudíž toto nařízení by se nadále mělo zaměřovat na to, aby o nás byly opravdu ukládané jen ty informace, které jsou pro chod stránek nezbytné, zbytek informací nebyl vůbec přístupný, nebo byl okamžitě mazán.

Dalším vhodným nařízení by bylo, zjednodušení těchto smluvních podmínek, aby bylo pro každého na první pohled jasné, že o nás jsou ty a ty informace shromažďovány, protože mnohdy si ani nejsme jistí, co jsme odsouhlasili, skrze komplikovanost těchto smluvních podmínek.

ZÁVĚR

Práce se zabývala problematikou ochrany soukromí. V teoretické části bylo vyspecifikováno, co je to soukromí a jak je právně vymezeno. Bylo popsáno, jaká práva na soukromí člověku poskytuje Listina základních práv a svobod a občanský zákoník, kde je právo na soukromí specifikováno v několika dílčích právech a zákonech. Ochranou soukromí se zabývá i trestní zákoník a napomáhá k tomu, aby bylo právo lépe právně vymahatelné. Důležitým právním faktorem v ochraně soukromí bylo i nařízení GDPR, které je zaměřeno na ochranu osobních údajů.

V druhé kapitole teoretické části bylo analyzováno proč, by mělo být soukromí bráno jako nový druh aktiva. Byly zde rozebrány příčiny k zvýšené ochraně soukromí, zejména zanechávání digitálních stop a snadnému přístupu k osobním údajům. Byly zde popsány i dopady, které sebou nesou tyto příčiny. Pro lepší pochopení toho, proč je soukromí zapotřebí chránit, byly v práci vypsány i jednotlivé části soukromí, jako jsou osobní údaje, dokumenty uložené v osobním počítači apod. Narušení soukromí sebou tudíž nenese jen psychický dopad, ale může vést i k finanční újmě.

Posledním blokem teoretické části byla specifikace jednotlivých hrozeb ohrožujících soukromí. Jedná se o hrozby, které můžou mít psychický, fyzický, nebo peněžní dopad na oběť. Většina hrozeb je poměrně nových, o kterých se v minulosti příliš nemluvilo, jako je kyberšikana a krádež identity za pomocí osobních údajů. Moderní technologie a přechod do kybernetického světa napomohly i k tomu, že narušení soukromí dostalo nové formy. Pomluvy, manipulace, nebo snaha zdiskreditovat člověka jsou mnohem jednodušší než dříve. Z pohledu ochrany soukromí, jsou zde i nadále hrozby, které nesouvisející s používáním nových technologií. Jedná se o stalking, nebo padělání, či krádež dokladů sloužícím k ověření identity. V závěru kapitoly jsou popsány konkrétní případy narušení soukromí.

Praktická část se zabývá analýzou toho, zda respondenti opravdu cítí, že je zapotřebí si své soukromí více chránit. Otázky měly potvrdit, nebo vyvrátit, že hrozby pro soukromí jsou skutečné a opravdu se dějí. Z dotazníkového šetření vyplynulo, že se lidé o své soukromí obávají a nepovažují ho za dostatečně chráněné, protože se o něj obávají i přes snahu si ho lépe chránit. Pomocí tohoto dotazníku, byly identifikované problémy související s narušením soukromí. Veřejný průzkum doplnily i interview s odborníky, kteří se setkávají s případy narušení soukromí, konkrétně se zástupcem z řad Policie ČR, který byl tázán, jestli

k narušení soukromí opravdu dochází. Dalším kdo poskytl do diplomové práce interview, byl právník, který potvrdil, že soukromí a zejména osobní údaje nejsou v české právní legislativě dostatečně chráněny.

Poslední část práce se zabývala návrhem řešení identifikovaných problémů, které vyplynuly z dotazníkového šetření. Bylo zde vyspecifikováno 5 hlavních problémů souvisejících s narušením soukromí. Tyto problémy byly popsány, včetně doporučení jak je možné je za současné situace minimalizovat. Každý jednotlivý problém dále obsahoval vlastní návrh řešení, který z pohledu zpracovatele diplomové práci, by tyto problémy mohl vyřešit.

SEZNAM POUŽITÉ LITERATURY

[1] MATES, Pavel. Ochrana soukromí ve správním právu. Praha: Linde, 2004. 307 s. ISBN 80-7201-458-7.

[2] VALOUŠEK, Martin, Pavel MATES, Eva FIALOVÁ, et al. Ochrana osobnosti, soukromí a osobních údajů. Praha: Leges, 2019. Praktik. ISBN 978-80-7502-346-9.

[3] LISTINA ZÁKLADNÍCH PRÁV A SVOBOD. Poslanecká sněmovna České republiky [online]. [cit. 2020-08-08]. Dostupné z: https://www.psp.cz/docs/laws/listina.html

[4] Zákon č. 89/2012 Sb.: Zákon občanský zákoník. Zákony pro lidi [online]. Praha: AION CS, 2010 [cit. 2020-08-08]. Dostupné z: https://www.zakonyprolidi.cz/cs/2012-89

[5] Zákon č. 40/2009 Sb.: Zákon trestní zákoník. Zákony pro lidi [online]. © AION CS, 2010 [cit. 2020-08-08]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

[6] GDPR: Obecné nařízení o ochraně osobních údajů. GDPR [online]. [cit. 2020-08-08]. Dostupné z: https://www.gdpr.cz/gdpr/co-je-gdpr/

[7] Základní příručka k ochraně údajů. Úřad pro ochranu osobních údajů [online]. [cit. 2020-08-08]. Dostupné z: https://www.uoou.cz/zakladni-prirucka-k-ochrane-udaju/ds-4744/archiv=0&p1=3938

[8] Co považuje GDPR za osobní údaje. *GDPR* [online]. [cit. 2020-08-08]. Dostupné z: https://www.gdpr.cz/gdpr/osobni-udaje/

[9] Jaké zásadní změny GDPR přinese. GDPR [online]. [cit. 2020-08-08]. Dostupné z: https://www.gdpr.cz/gdpr/zmeny/

[10] Jaké povinnosti ukládá GDPR institucím a firmám. GDPR [online]. [cit. 2020-08-08]. Dostupné z: https://www.gdpr.cz/gdpr/povinnosti/

[11] DIGITÁLNÍ STOPA. Internetem bezpečně [online]. 2018 [cit. 2020-08-08]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/dobre-vedet/digitalni-stopa/

[12] Proč a jak chránit na internetu své osobní údaje. Vím, kam klikám [online]. 2017 [cit. 2020-08-08]. Dostupné z: https://www.vimkamklikam.cz/soukromi/proc-a-jak-chranit-na-internetu-sve-osobni-udaje

[13] SILBERBERG, Adam. Všichni máme právo na soukromí: konspirativní techniky. V prvním vydání. [Praha]: Restart project, 2018. Samizdat. ISBN 978-80-270-4239-5.

[14] MICHL, Petr. Jak funguje Cambridge Analytica: příběh zneužívání dat uživatelů a jejich strachu. Focus agency [online]. 2018 [cit. 2020-08-09]. Dostupné z: https://www.focus-age.cz/m-journal/internet/jak-funguje-cambridge-analytica--pribeh-zneuzivani-dat-uzivatelu-a-jejich-strachu__s281x13594.html

[15] SKOČEK, Jakub. Politika společnosti Google v oblasti sběru a uchovávání dat uživatelů. *Knihovna AV ČR* [online]. 2015 [cit. 2020-08-08]. Dostupné z: https://www.lib.cas.cz/casopis_informace/politika-google-sber-uchovavani-dat/

[16] Zásady ochrany soukromí google. *Google* [online]. 2020 [cit. 2020-08-08]. Dostupné z: https://policies.google.com/privacy?hl=cs

[17] Proč a jak chránit na internetu své osobní údaje. Vím, kam klikám [online]. 2017 [cit. 2020-08-08]. Dostupné z: https://www.vimkamklikam.cz/soukromi/proc-a-jak-chranit-na-internetu-sve-osobni-udaje

[18] POKORNÝ, Jiří. Vybrané typy kyberšikany a její preventivní opatření. Medium [online]. 2019 [cit. 2020-08-08]. Dostupné z: https://medium.com/edtech-kisk/vybran%C3%A9-typy-kyber%C5%A1ikany-a-jej%C3%AD-preventivn%C3%AD-opat%C5%99en%C3%AD-bbd1254eb227

[19] Zneužitím osobních údajů přišli o peníze. Policie České republiky [online]. 2013 [cit. 2020-08-08]. Dostupné z: https://www.policie.cz/clanek/zneuzitim-osobnich-udaju-prisli-o-penize.aspx

[20] Stalking a navazující trestná činnost v souvislosti se sociálními sítěmi. Šance dětem [online]. 2018 [cit. 2020-08-08]. Dostupné z: https://www.sancedetem.cz/cs/hledam-pomoc/rodina-v-problemove-situaci/rizikove-chovani-ditete/stalking-a-navazujici-trestna-cinnost-v-souvislosti-se-socialnimi-sitemi.shtml

[21] Co už je nebezpečným pronásledováním - stalking. Právní linka [online]. 2015 [cit. 2020-08-08]. Dostupné z: https://www.pravnilinka.cz/bezplatna-pravni-poradna-zdarma/stalking.html

[22] Krádež identity. Internetem bezpečně [online]. 2018 [cit. 2020-08-08]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/kradez-identity/

[23] Zneužití identity při bankovních podvodech roste epidemicky. Spotrebitele.dtest.cz [online]. 2017 [cit. 2020-08-08]. Dostupné z: https://spotrebitele.dtest.cz/clanek-6239/zneuziti-identity-pri-bankovnich-podvodech-roste-epidemicky

[24] CHLUP, Marek. Viry a Antiviry. ANZDOC [online]. 2013 [cit. 2020-08-09]. Dostupné z: https://adoc.tips/viry-a-antiviry-marek-chlup.html

[25] Sociální inženýrství. AVAST [online]. [cit. 2020-08-09]. Dostupné z: https://www.avast.com/cs-cz/c-social-engineering

[26] Na kradené občanské průkazy si zloději berou půjčky i jezdí načerno. Novinky.cz [online]. 2013 [cit. 2020-08-08]. Dostupné z: https://www.novinky.cz/finance/clanek/na-kradene-obcanske-prukazy-si-zlodeji-berou-pujcky-i-jezdi-nacerno-198762

[27] Soud vynesl tresty za krádeže identity a podvody. Moravskoslezsky.denik.cz [online]. 2019 [cit. 2020-08-08]. Dostupné z: https://moravskoslezsky.denik.cz/zlociny-a-soudy/soud-vynesl-tresty-za-kradeze-identity-a-podvody-20190831.html

[28] Soud s podvodníky v Ostravě: Čtení obžaloby zabralo několik hodin. Moravskoslezsky.denik.cz [online]. 2018 [cit. 2020-08-08]. Dostupné z: https://moravskoslezsky.denik.cz/zlociny-a-soudy/soud-s-podvodniky-v-ostrave-cteni-obzaloby-zabralo-nekolik-hodin-20180723.html

[29] Zverejňovanie súdnych rozhodnutí a ďalších informácií (InfoSúd). In: Europan justice [online]. 2016 [cit. 2020-08-08]. Dostupné z: https://obcan.justice.sk/infosud/-/infosud/i-detail/rozhodnutie/3142dd66-070c-4db6-9b53-3593ddae35c6%3A65a136f8-e256-42a1-999f-5f770fffd9f9

[30] Jak zablokovat reklamní sledování. Jak zablokovat cookies [online]. [cit. 2020-08-09]. Dostupné z: https://jakzablokovatcookies.cz/gdpr-v-prohlizeci/opera-zablokovani-cookies-a-reklamnich-skriptu-pomoci-ublock-origin

[31] Jak se daří právu být zapomenut? EPRAVO.CZ – Sbírka zákonů, judikatura, právo [online]. 2017 [cit. 2020-08-09]. Dostupné z: https://www.epravo.cz/top/clanky/jak-se-dari-pravu-byt-zapomenut-104710.html

[32] PREVENCE - Kyberšikana. Policie České republiky [online]. [cit. 2020-08-09]. Dostupné z: https://www.policie.cz/clanek/prevence-kybersikana.aspx

[33] Elektronická identifikace pomocí občanského průkazu. Eidentita.cz [online]. [cit. 2020-08-09]. Dostupné z: https://info.eidentita.cz/eop/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

OZ Občanský zákoník

PC Personal Computer

GDPR General data regulation protection

GPS Global positioning system

SIM Subscriber identity module

SSL Secure socket layer

SMS Short message service

IP Internet protocol

SEZNAM OBRÁZKŮ