UNIVERZA V LJUBLJANI

FAKULTETA ZA UPRAVO

Diplomsko delo

PROBLEMATIKA VARSTVA OSEBNIH PODATKOV V SPLETNIH DRUŽBENIH OMREŽJIH

Sabina Medvešek

Ljubljana, junij 2016

UNIVERZA V LJUBLJANI

FAKULTETA ZA UPRAVO

DIPLOMSKO DELO

PROBLEMATIKA VARSTVA OSEBNIH PODATKOV V SPLETNIH DRUŽBENIH OMREŽJIH

Kandidatka:	Sabina Medvešek
Vpisna številka:	04042705
Študijski program:	univerzitetni študijski program Upravljanje javnega sektorja, prva stopnja
Mentor:	doc. dr. Mitja Dečman

Ljubljana, junij 2016

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Podpisana Sabina Medvešek, študentka prve stopnje univerzitetnega študijskega programa Upravljanje javnega sektorja z vpisno številko 04042705, sem avtorica diplomskega dela z naslovom: Problematika varstva osebnih podatkov v spletnih družbenih omrežjih.

S svojim podpisom zagotavljam, da:

- je predloženo delo izključno rezultat mojega lastnega raziskovalnega dela,
- sem poskrbel/-a, da so dela in mnenja drugih avtorjev oz. avtoric, ki jih uporabljam v predloženem delu, navedena oz. citirana v skladu s fakultetnimi navodili,
- sem poskrbel/-a, da so vsa dela in mnenja drugih avtorjev oz. avtoric navedena v seznamu virov, ki je sestavni element predloženega dela in je zapisan v skladu s fakultetnimi navodili,
- sem pridobil/-a vsa dovoljenja za uporabo avtorskih del, ki so v celoti prenesena v predloženo delo, in sem to tudi jasno zapisal/-a v predloženem delu,
- se zavedam, da je plagiatorstvo – predstavljanje tujih del, bodisi v obliki citata bodisi v obliki skoraj dobesednega parafraziranja bodisi v grafični obliki, s katerim so tuje misli oz. ideje predstavljene kot moje lastne – kaznivo po zakonu (Zakon o avtorskih in sorodnih pravicah, Ur. list RS, št. 21/95), kršitev pa se sankcionira tudi z ukrepi po pravilih Univerze v Ljubljani in Fakultete za upravo,
- se zavedam posledic, ki jih dokazano plagiatorstvo lahko predstavlja za predloženo delo in za moj status na Fakulteti za upravo,
- je elektronska oblika identična s tiskano obliko diplomskega dela ter soglašam z objavo dela v zbirki »Dela FU«.

Diplomsko delo je lektorirala: Aleksandra Jurman, prof. slov.

Ljubljana, 16. 06. 2016

Podpis avtorice: Sabina Medvešek

POVZETEK

Naše življenje je v današnjem času že skoraj odvisno od uporabe informacijske tehnologije. Ključni razlog za pisanje diplomskega dela s tem naslovom je čedalje večja uporaba spletnih družbenih omrežij, kar pa vključno z vsemi prednostmi prinese tudi negativne stvari, kot so zlorabe osebnih podatkov in vdori v naše zasebnosti.

V diplomskem delu želimo raziskati raven zavedanja uporabnikov spletnih družbenih omrežij na področju varstva osebnih podatkov, kar bomo dosegli z empirično raziskavo, ki bo temeljila na teoretičnih temeljih na tem področju in bo izvedena med naključno izbranimi uporabniki spletnih družbenih omrežij.

V okviru analize dobljeni rezultati nas niso kaj dosti presenetili, ampak le potrdili našo osnovno trditev, da posameznik ne ravna dovolj previdno s svojimi osebnimi podatki in da je raven poznavanja varstva osebnih podatkov zelo šibka, in lahko rečemo, da je, kljub temu da smo to pričakovali, skrb vzbujajoče.

Dobljeni rezultati nakazujejo, da je potrebno še veliko informiranja glede pomembnosti in nevarnosti ter zaščite naših osebnih podatkov tako v spletnih družbenih omrežjih kot v drugih spletnih okoljih. Zaradi konstantnega razvoja informacijske tehnologije pa lahko o osveščanju na tem področju govorimo kot o trajnostni nalogi države in družbe.

Naše diplomsko delo prav tako želi spodbuditi oziroma prepričati posameznika, da so njegovi osebni podatki dandanes izredno pomembna dobrina, ki jo je potrebno varovati. Želeli bi dvigniti ozaveščenost vsakega posameznika o pomembnosti zlorabe osebnih podatkov na spletnih družbenih omrežjih ter jih usmeriti k razmisleku o tem.

Ključne besede: osebni podatki, informacijska tehnologija, spletna družbena omrežja, zasebnost, zloraba osebnih podatkov.

SUMMARY

THE ISSUE OF PERSONAL DATA PROTECTION WITHIN WEB SOCIAL NETWORKS

Nowadays our life almost depends on the use of information technology. The main reason for writing diploma with this title is growing multiplicity of use of web social networks which bring us a lot of advantages but their use is also bringing us some negative things, such as abuse of personal data and intrusions into our privacy.

In diploma, we want to investigate the level of awareness of users of web social networks in the field of personal data protection which will be achieved through empirical research, based on the theoretical foundations of the field and will take place between randomly selected users of web social networks.

In the context of the analysis and the results didn't surprise us and we only confirmed our basic argument that individual does not act sufficiently careful with their personal data and that the level of awareness of personal data protection is very weak. Despite though we have expected this, we can for sure say that this is alarming.

The results indicate that there is still a lot of information regarding to the importance of dangers and protecting our personal data in web social networks and also other online environments. Due to the continuous development of information technology, we are able to say that providing information in this area must be sustainable task of state and society.

Our diploma also seeks to encourage or persuade every individual that his personal data are nowadays extremely important commodity that must be protected. We would like to raise awareness among everyone about the importance of abuses of personal data in web social networks and direct them to a reflection about it.

Keywords: personal data, information technology, web social networks, privacy, abuse of personal data.

KAZALO

KAZALO PONAZORITEV

KAZALO SLIK

KAZALO TABEL

1 UVOD

Osebni podatki so z razvojem tehničnih sredstev, ki nam omogočajo zelo hitro in avtomatizirano obdelavo podatkov, postali zelo občutljiva in dragocena človekova dobrina, zato jih ne smemo prepustiti dejstvu, da postanejo predmet svobodne uporabe, posredovanja in zbiranja. Takšni podatki vključujejo številne intimne in tudi druge lastnosti, stanja ter razmerja vsakega posameznika, zaradi česar lahko njihova zloraba nasploh pomeni kršitev človekove duševne in telesne integritete.

Varstvo osebnih podatkov je ena izmed temeljnih človekovih pravic in osebnih svoboščin, ki je v demokratičnih državah zajamčena z ustreznimi pravnimi akti. To lahko vidimo na podlagi tega, da izhaja iz Splošne deklaracije o človekovih pravicah ter nekaterih drugih mednarodnih dokumentov. Je tudi ena izmed pravic, ki je močno povezana s pravico do zasebnosti. Varstvo osebnih podatkov predstavlja del pojma zasebnosti in samo besedo lahko razumemo kot sopomenko besedne zveze informacijska zasebnost. Informacijska zasebnost je torej sopomenka za varstvo osebnih podatkov in ena od treh sestavin zasebnosti, katerim se bomo posvetili v drugem poglavju.

V Sloveniji poleg Ustave RS samo varstvo osebnih podatkov ureja tudi poseben zakon, Zakon o varstvu osebnih podatkov, ki je stopil v veljavo 1. 1. 2005. Zakon določa pravice, obveznosti, načela ter ukrepe, s katerimi se pravno preprečujejo nezakoniti, neustavni ter neupravičeni posegi v posameznikovo zasebnost in dostojanstvo, medtem ko se njegovi podatki obdelujejo. V diplomskem delu se posvečamo tudi opredelitvi pravic posameznika in varstvu le-teh.

Ker je pojem informacijska tehnologija širok, se v diplomi ukvarjamo s tematiko spletnih družbenih omrežij. Družbena omrežja izhajajo iz besedne zveze social network, ki jo nekateri prevajajo tudi kot spletna socialna omrežja ali družabna omrežja. Mi bomo v diplomski nalogi uporabljali prevod spletna družbena omrežja, ker je še najbolj sprejemljiv prevod, saj če pogledamo že sami besedi družaben in družben, se da ugotoviti precejšne razlike. Tudi beseda socialen ni primerna, saj je pridevnik socialen zaradi svoje večpomenskosti problematičen za uporabo. Sam pojem spletna družbena omrežja pa predstavlja platforme, spletne storitve in aplikacije, ki vsakemu posamezniku pomagajo ustvariti osebni profil, preko katerega dostopa do profilov drugih uporabnikov. Dandanes že presegajo enosmerno komunikacijo in uporabniki so postavljeni v aktivnejšo vlogo, v kateri jim je na voljo možnost soustvarjanja.

Zavedati se moramo dejstva, da objava kakršnegakoli podatka na internetu pomeni posredovanje naše informacije ali podatka v prostor, v katerem se nekontrolirano širi. Dostop do naše objave ima po navadi veliko število ljudi, lahko pa naša objava pride tudi do tretje osebe. Ta jo lahko zlorabi in pri tem je težko zaščititi svoj podatek. Po navadi zlorabo prepoznamo šele po tem, ko je škoda že storjena.

Cilji diplomskega dela so sledeči:

- opisati pravico do varstva osebnih podatkov in pravico do zasebnosti ter predstaviti njun zgodovinski pregled ter mednarodnopravno ureditev,
- predstaviti Zakon o varstvu osebnih podatkov, ki je bistvenega pomena za obravnavano področje,
- predstaviti spletna družbena omrežja – kaj sploh so, kakšne so njihove prednosti ter slabosti, kako poteka komunikacija znotraj njih in katera so najbolj priljubljena,
- predstaviti nevarnosti, ki nam grozijo pri njihovi uporabi, ali na kakšen način so lahko naši osebni podatki zlorabljeni,
- predstaviti smernice varne uporabe spletnih družbenih omrežij ter
- raziskati raven zavedanja na področju varstva osebnih podatkov pri uporabi spletnih družbenih omrežij.

V empirični raziskavi, s katero bomo dosegli naš zadnji cilj, pa smo si zastavili tudi naslednje hipoteze:

- Večina anketirancev uporablja več kot eno spletno družbeno omrežje ter je na njih tudi zelo aktivna.
- Uporabniki spletnih družbenih omrežij svoje osebne podatke delijo z mnogimi drugimi uporabniki ter v različnih družbenih omrežjih v različni meri posvečajo svojo pozornost varnostnim nastavitvam.
- Večina uporabnikov še ni bila soočena z zlorabo osebnih podatkov in misli, da njihovi podatki niso dovolj zanimivi, da bi lahko postali predmet zlorabe.
- Uporabniki ne vedo, kako je varstvo osebnih podatkov v slovenski zakonodaji urejeno, ne poznajo Zakona o varstvu osebnih podatkov in v primeru zlorabe njihovih osebnih podatkov ne vedo, kaj bi storili.

Skozi naše diplomsko delo pa bi radi preverili še osnovno trditev diplomskega dela, ki pravi, da posameznik ne ravna dovolj previdno s svojimi osebnimi podatki in da je raven poznavanja varstva osebnih podatkov zelo šibka.

2 VARSTVO OSEBNIH PODATKOV

2.1 SPLOŠNO O ČLOVEKOVIH PRAVICAH

Človekove pravice je težko opredeliti, ker sta njihova definicija in pravzaprav tudi njihov obstoj odvisna od čustev prav toliko kot od razuma. Prepričanje o njihovi samoumevnosti se opira na čustven naboj: prepričljive so, če v posamezniku predramijo nek občutek. Da gre za vprašanje človekovih pravic, z največjo gotovostjo vemo takrat, kadar smo zgroženi zaradi njihove kršitve (Hunt, 2015, str. 33).

Pojem, kot so človekove pravice, je nedvomno vrednota, ki jo velja tako ohranjati kot razvijati v njenem vrednostno pozitivnem smislu. To pa je oziroma bo mogoče le, če vsak posameznik v zadostni meri spozna, da je treba človekove pravice nujno in neprestano komplementirati s tistimi moralnimi vrednotenji, ki upoštevajo, da je vrednota vsak človek in ne le jaz sam ter da je to vrednoto možno ustrezno razvijati in varovati le ob dejstvu, če vsak sam prispeva k vrednostno pozitivnemu razvoju družbe ter obratno (Türk, Accetto, Cerar, Jamnikar & Smrkolj, 2002).

2.2 PRAVICA DO VARSTVA OSEBNIH PODATKOV IN PRAVICA DO ZASEBNOSTI

Kot smo že omenili, sta pravica do varstva osebnih podatkov in pravica do zasebnosti dva pojma, ki se med seboj močno povezujeta. Varstvo osebnih podatkov lahko razumemo kot del zasebnosti, in sicer tisti del, ki se navezuje na informacijski del zasebnosti, se pravi, da je varstvo osebnih podatkov sopomenka za informacijsko zasebnost. Sam pojem bi lahko na podlagi dveh ustavnih določb, 37. člena slovenske Ustave (varnost tajnosti pisem in drugih občil) in 38. člena (varstvo osebnih podatkov) razdelili na dve temeljni skupini. V prvo skupino lahko uvrstimo komunikacijsko oziroma korespondenčno informacijsko zasebnost, v drugo pa zasebnost varstva osebnih podatkov. Prva se navezuje na njihovo posredovanje, druga pa na njihovo zasebnost.

Pravica do zasebnosti, oziroma angloameriška inačica Right to privacy, je elementarna človekova pravica – tako mednarodna kot ustavna, javnopravnega značaja ter osebnostna pravica civilnopravnega značaja kot ena izmed nepogrešljivih elementov človekove eksistence, ki varuje človeka pred državno oblastjo, javnostjo in drugimi posamezniki, je pravica biti sam z minimumom posegov v odločitveno, duševno, prostorsko in informacijsko zasebnost (Lampe, 2004, str. 42).

Torej, kje je meja med javnostjo in zasebnostjo? John Thompson je v svojem delu Media and modernity dihotomijo javno/zasebno soočil z dihotomijo vidno/nevidno. Javno je torej tisto, kar je vidno ali opazovano, kar je izvedeno pred gledalci, kar lahko vsi ali mnogi vidijo in slišijo. Zasebno pa je tisto, kar je skrito pred pogledi, kar je izgovorjeno ali storjeno v zasebnosti ali v krogu manjšega števila ljudi (Thompson, 1995, str. 123).

Da je zasebnost postala pravica, je določil že eden izmed prvih pooblaščencev za varstvo zasebnosti v Kanadi. Pravico je povezal s sledečimi pojmi: pravica biti puščen na miru, pravica do zasebnega življenja, pravica do osebne avtonomije, pravica nadzorovati informacije o sebi, pravica pričakovati zaupnost, pravica uživati osamljenost, pravica omejiti dostop do sebe, pravica zmanjšati nadlegovanje na najmanjšo možno mero, pravica uživati anonimnost, pravica do tajnosti ter pravica uživati zadržanost (Kovačič, 2006).

Čebulj (1992, str. 7) navaja tri sestavine zasebnosti, katere del oziroma ena izmed sestavin je tudi varstvo osebnih podatkov oziroma informacijska zasebnost. Te sestavine so naslednje:
zasebnost v prostoru, zasebnost osebnosti in informacijska zasebnost.

Večina ljudi si pod sestavino zasebnost v prostoru predstavlja predvsem čas, ko nas nihče ne moti. To so ti določeni trenutki, ki jih kot posamezniki ne želimo deliti z nobeno drugo osebo. To pomeni, da ima vsakdo možnost biti sam oziroma biti fizično ločen od drugih ljudi. Določen del te zasebnosti se navezuje na osnovne oziroma biološke potrebe, ki jih imamo vsi, a so tako osebne, da jih želimo izvajati sami. Čeprav smo ljudje družbena bitja, ima vsakdo pravico, da se izolira od ostalih.

Zasebnost osebnosti se nanaša na svobodo posameznikovih misli, izražanja, opredelitev, se pravi pravice do izražanja. Ta v družbeni praksi čedalje pogosteje prihaja v konflikt s pravico do zasebnosti. Če pogledamo vidik svobode medijev, je vdor v pravico do zasebnosti največkrat storjen s strani zasebnih subjektov, kot so na primer televizija, radio in tisk, manj pa neposredno s strani države. Država je prisiljena storiti vse potrebno, da zavaruje pravico do zasebnosti vsakega posameznika, četudi se ta nanaša na razmerje posameznika in subjekte zasebnega prava (Teršek, 2005).

Že definicija izraza osebni podatek nam pove, da so to informacije, ki nimajo javnega značaja. Osebni podatki, kot so na primer ime in priimek, spol, starost, zdravstveno stanje, zaposlitev, morajo biti varovani že iz razloga, ker je iz njih mogoče razbrati osebne in druge značilnosti določene osebe, ki lahko tej osebi neupravičeno škodujejo v njenem zasebnem ali javnem življenju. Vendar pa ob razvoju informacijske družbe ni mogoče, da bi bili vsi podatki, ki se nanašajo na posameznika, izvzeti iz širše ali javne uporabe. Dostop do osebnih podatkov in upravljanje z njimi sta dopustna le ob privolitvi posameznika (Cerar, 2004, str. 58).

2.3 MEDNARODNOPRAVNA UREDITEV IN RAZVOJ

2.3.1 GLOBALNI PRAVNI AKTI

Boj za človekove pravice sega še v čase kraljevin, o katerih pričajo mnogi dokumenti, kot so: Magna Charta Libertatum, Petition of Rigths, Deklaracija pravic delovnega in izkoriščenega ljudstva Kongresa sovjetov, Mednarodni pakt o državljanskih in političnih pravicah, Splošna deklaracija človekovih pravic, Mednarodni pakt o ekonomskih, socialnih in kulturnih pravicah in drugi. Prostost in življenje sta kot dve najpomembnejši dobrini

človeka postali izhodišče za deklaracijo človekovih pravic. Pri tem naj bi država prevzela glavno nalogo, da je dolžna skrbeti za blagor svojih državljanov, da varuje vsakega posameznika, da ta lahko uživa svoje absolutne pravice, ki imajo podlago v nespremenljivih naravnih zakonih (pravica do osebne svobode, pravica do lastnine, pravica do osebne varnosti). V ustave posameznih modernih držav so bile sprejete iz deklaracij o človekovih pravicah samo svoboščine in pravice, pri katerih so bili državni organi omejeni pri njihovem delovanju, ki bi poseglo v zasebno sfero vsakega posameznika. Po drugi svetovni vojni in po številnih drugih teptanjih človekovih pravic se je tako oblikovala vera v temeljne človekove pravice. V tem času so bili omenjeni dokumenti, kot sta Splošna deklaracija človekovih pravic iz leta 1948 in Mednarodni pakt o državljanskih pravicah. Mednarodni akti so tako pomembno vplivali na ustave številnih držav, med njimi tudi na slovensko ustavo, saj neposredno vplivajo na notranjo pravno ureditev države. Med najpomembnejše akte, ki urejajo pravico do zasebnosti, spadata Splošna deklaracija o človekovih pravicah in Mednarodni pakt o državljanskih in političnih pravicah (Finžgar, 1985).

2.3.2 EVROPSKI PRAVNI AKTI

Leta 1949 je bil ustanovljen Svet Evrope in predstavlja najstarejšo evropsko mednarodno organizacijo. Zavzema se za varstvo, razvoj in kodifikacijo človekovih pravic in temeljnih svoboščin. Njeno članstvo je Sloveniji priznalo 14. 5. 1993 in s tem je Slovenija prevzela izpolnjevanje smernic, načel in priporočil, ki jih daje Svet Evrope za zavezujoče. Glede področja varstva osebnih podatkov bi lahko izpostavili dva pomembna dokumenta: Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin ter Konvencija o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov.

Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin je bila podpisana 4. 11. 1950 in je bila pripravljena s strani Evrope. V veljavo je stopila tri leta pozneje. Slovenija je omenjeno konvencijo ratificirala leta 1994, do sedaj pa je bila dopolnjena z večimi protokoli. Najpomembnejši člen, ki se navezuje na področje varstva osebnih podatkov, je 8. člen, ki pravi, da je pravica do spoštovanja zasebnega in družinskega življenja, doma in dopisovanja zagotovljena čisto vsakemu. V svojem drugem odstavku še navaja, da se javna oblast ne sme vmešavati v izvrševanje te pravice, razen v izrecnih primerih, ko to dopušča zakon in je le-to nujno v demokratični družbi v imenu javne varnosti, državne varnosti ali ekonomske blaginje države, ali zato, da se prepreči zločin ali nered, da se zavaruje moralo ali zdravje, ali pa da se zavarujejo svoboščine in pravice drugih ljudi.

Zaradi vse večjega pomena osebnih podatkov, njihovega zbiranja, shranjevanja, dostopa do njih ter razpolaganja z njimi v današnjem času je bila na predlog Sveta Evrope leta 1981 sprejeta Konvencija o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov. Je eden najpomembnejših dokumentov s področja varovanja informacijske zasebnosti. Njegov temeljni namen je zagotoviti vsakemu posamezniku spoštovanje njegovih pravic in temeljnih svoboščin, predvsem pa spoštovanje pravice do zasebnosti glede na avtomatsko obdelavo osebnih podatkov, ki se nanašajo nanj. Neposredno ureja

le področje avtomatske obdelave osebnih podatkov, vendar pa državam članicam dopušča tudi izjeme. Konvencija določa pravila o zbiranju in obdelavi osebnih podatkov in izenačuje zbirke podatkov v javnem in zasebnem sektorju. Poleg tega določa osnovne pravice posameznika in načine ravnanja z osebnimi podatki z zagotovili, ki jih mora zakonodajalec predvideti pri posamezniku za obdelavo njegovih osebnih podatkov (Kovačič, 2006, str. 76).

Konvencija vsebuje številna temeljna načela, kot so načelo kakovosti podatkov, načelo omejitve obdelave določenih kategorij osebnih podatkov, načelo zavarovanja podatkov ter načelo odprtosti in sodelovanja ljudi. Zaradi poenotenja pravil varstva morajo države podpisnice zagotoviti spoštovanje določil v okviru svojega nacionalnega prava (Čebulj, 1992, str. 13, 21).

Konvencija med drugim nalaga podpisnicam nalogo, da določijo ustrezne sankcije in pravna sredstva za kršitve določil nacionalne zakonodaje, s katero se udejanja in zagotavlja uresničevanje temeljnih načel za zaščito podatkov iz konvencije.

2.3.3 UREDITEV V EVROPSKI UNIJI

Evropska unija je izdala številne dokumente, ki se nanašajo na področje varstva osebnih podatkov, z namenom, da bi zakonodajno uskladila varstvo zasebnosti v vseh državah članicah Evropske unije. Evropska unija si je prizadevala za temeljni akt, ki bi Evropsko unijo in njene članice zavezal k spoštovanju človekovih pravic pod njenimi pravnimi akti ter da bi hkrati omogočal tudi sodni nadzor Sodišča Evropskih skupnosti. V letu 2000 je bila sprejeta Listina Evropske unije o temeljnih pravicah, ki zaradi svoje neusklajenosti formalnopravno ni zavezovala niti članic EU niti njenih institucij. Po koncu številnih pogajanj so jo leta 2007 razglasili za pravno zavezujoč dokument kot sestavni del Lizbonske pogodbe, ki na žalost ne velja na Poljskem in v Veliki Britaniji. Njena naloga je, da enotno ureja vse temeljne pravice na ravni Unije. Te pravice so politične, gospodarske, socialne, državljanske in kulturne pravice. Vsebina listine je večinoma povzetek iz Evropske konvencije o varstvu človekovih pravic in temeljnih svoboščin, povzema pravice tudi iz pogodb EU, mednarodnih konvencij, sodne prakse Sodišča Evropskih skupnosti, skupnih ustavnih tradicij držav članic in stališča evropskega parlamenta. Za področje varstva osebnih podatkov je pomemben 8. člen te listine, ki pravi, da ima vsak posameznik pravico do varstva osebnih podatkov, ki se nanj nanašajo, obdelava osebnih podatkov mora biti poštena, določen mora biti tudi namen in navsezadnje mora obstajati tudi privolitev posameznika oziroma kakšna druga legitimna podlaga, ki je določena z zakonom ter vsakemu posamezniku zagotavlja dostop do podatkov, ki se nanj navezujejo. Ta pa lahko zahteva tudi, da se njegovi osebni podatki popravijo (Lampe, 2010).

Direktiva 95/46/ES Sveta o zaščiti posameznikov pri obdelavi osebnih podatkov in prostem gibanju teh podatkov ter Evropskega parlamenta je bistveno izhodišče za zaščito podatkov pri njihovem obdelovanju ter izpostavlja povezavo med zaščito osebnih podatkov na eni strani ter na drugi strani povezavo med temeljnimi pravicami in svoboščinami

posameznika. V letu 1995 sta to direktivo sprejela Svet Evropske unije in Evropski parlament. Določa, da morajo biti vsi osebni podatki obdelani pošteno in zakonito, zbrani morajo biti za vnaprej točno določen in zakonit namen ter ne smejo biti obdelani za kakšne druge namene, če to ni določeno. Podatki morajo biti aktualni, ustrezni in ne prekomerni. Ti so lahko shranjeni v obliki, ki dopušča identifikacijo posameznika le toliko časa, dokler ni dosežen namen njihove obdelave. Za vse osebne podatke, ki se obdelujejo, mora nujno obstajati neko soglasje osebe, katere last so ti podatki, prav tako mora biti tudi ta posameznik seznanjen s tem, kateri njegovi podatki se zbirajo in za kakšen namen. Posameznik mora biti obvezno seznanjen z možnostjo dostopa do svojih osebnih podatkov ter s pravico do popravka le-teh. Direktiva svojo posebno pozornost namenja obdelavi občutljivih osebnih podatkov, poleg tega pa je njena zahteva ustanovitev neodvisnega nadzornega organa, ki bi skrbel za zaščito zasebnosti in zakonodajo (Kovačič, 2006).

Uredba ES 45/2001 o varstvu posameznikov pri obdelavi osebnih podatkov pa določa ustanovitev posebnega nadzornega organa, ki se imenuje Evropski nadzornik za varstvo podatkov. Ta ima pristojnost za nadzor spoštovanja predpisov o varstvu podatkov v evropskih institucijah. V osnovi naj bi urejal enake obveznosti in pravice kot Direktiva 95/46/ES, razlika je le v tem, da jih ta ureja na ravni institucij in organov Evropske skupnosti. V letu 2000 je bila sprejeta s strani Evropskega sveta in parlamenta, njena obveznost pa je, da določa standarde in pravila ravnanja organov Evropske unije s samimi osebnimi podatki.

2.3.4 RAZVOJ VARSTVA OSEBNIH PODATKOV V REPUBLIKI SLOVENIJI

Potreba po varstvu osebnih podatkov kot človekove pravice se je v Sloveniji pričela kazati že v ustavni ureditvi še v času takratnega komunističnega oziroma socialističnega sistema, dejansko pa so jo vključili v ustavo leta 1989 v takratnem začetnem obdobju demokratizacije Slovenije. S tem se je umestila v ozek krog držav, katere že na ustavni ravni zagotavljajo takšno varstvo. Ko je leta 1991 sprejela novo ustavo, je v njej obdržala določbo o varstvu osebnih podatkov (Kramar, 2013).

Prvi začetki oziroma ideje o varstvu osebnih podatkov kot eni od človekovih pravic, zajamčenih z ustavo, segajo v leto 1989, ko so bili sprejeti amandmaji k republiški ustavi iz leta 1974. Na podlagi teh amandmajev je Slovenija v marcu leta 1990 dobila svoj prvi zakon s področja varstva osebnih podatkov, katerega glavni cilj je bil urediti to področje in opredeliti ter določiti pravice, ukrepe ter načela zoper zlorabo omenjenih pravic in poseganja v človekovo osebnost. Pomembno vlogo pa je imela tudi ratifikacija Konvencije o varstvu posameznika glede na avtomatsko obdelavo podatkov. Le-ta je postala merilo zakonskega procesiranja, zbiranja in uporabe osebnih podatkov. V letu 1999 je bil Državni zbor Republike Slovenije zaradi pritiska prisiljen sprejeti nov Zakon o varstvu osebnih podatkov zaradi približevanja Evropski uniji in potrebno je bilo zadovoljiti zahteve Direktive 95/46/ES. Novi zakon je bil tako že usklajen z omenjeno direktivo, ni pa določal institucije, ki bi bila neodvisna in namenjena nadzoru nad varstvom osebnih podatkov. Tako sta bila zaradi nadaljnje uskladitve z Direktivo 95/46/ES, ki se nanaša na neodvisni nadzorni organ za varstvo osebnih podatkov, leta 2001 z Zakonom o spremembah in dopolnitvah zakona

o varstvu osebnih podatkov ustanovljena varuh človekovih pravic kot neodvisni nadzorni organ za varstvo osebnih podatkov (bolj s svetovalnimi pristojnostmi in pristojnostmi za dajanje predlogov za ukrepanje Inšpektoratu za varstvo osebnih podatkov) ter Inšpektorat za varstvo osebnih podatkov kot organ v sestavi Ministrstva za pravosodje (Kramar, 2013).

Zaradi 38. člena Ustave Republike Slovenije in Zakona o varstvu osebnih podatkov bi lahko rekli, da je v Sloveniji varstvo osebnih podatkov na zakonodajni ravni doživelo ustaljenost, saj so bili s tem določeni nameni, načini zbiranja in tudi vrste osebnih podatkov, ki se obdelujejo na posameznih področjih. Tudi v javnosti se čuti občutljivost glede varstva osebnih podatkov zaradi povečanega inšpekcijskega nadzora in svetovalnih zadev.

Slovenija je 1. 5. 2004 vstopila v Evropsko unijo in s tem se je bila primorana prilagoditi pravnemu redu Evropske unije. Tako je sprejela novi Zakon o varstvu osebnih podatkov, ki je bil uradno sprejet 15. 7. 2004, v veljavo pa je stopil 1. 1. 2005. Pomen novega zakona je v osnovi ostal enak prejšnjemu, vendar obstaja razlika med njima. In sicer novi, sedanji zakon je tudi področni zakon, ne samo sistemski zakon. Dotika se tudi različnih področij, kot so trženje, videonadzor, biometrija, strokovni nadzor ter evidentiranje vstopov in izstopov iz prostorov. Zaradi te svoje preciznosti je tudi veliko obsežnejši. Zakon je bil 27. 7. 2007 nazadnje spremenjen v ZVOP-1-UPB1, Zakon o varstvu osebnih podatkov – ZVOP-1-UPB1 (Uradni list RS, št. 94/07 z dne 16. 10. 2007).

2.4 ZAKON O VARSTVU OSEBNIH PODATKOV

Zakon o varstvu osebnih podatkov (v nadaljevanju ZVOP-1) je temeljni zakon področja varstva osebnih podatkov, ki tudi v celoti vsebuje in upošteva vsa načela, ki jih narekujejo mednarodne konvencije. Je precej težko razumljiv zakon, vendar je v pravni red Slovenije prinesel veliko pomembnih novosti, ki so pripomogle k zavedanju o pomenu ter teži varstva osebnih podatkov.

2.4.1 TEMELJNI POJMI

V tem poglavju bomo predstavili osnovne izraze Zakona o varstvu osebnih podatkov. V 2. členu določa zakonsko uporabljene izraze, ki se nanašajo na področje, in ti so sledeči:

- Osebni podatek predstavlja katerikoli podatek, ki se navezuje oziroma nanaša na posameznika in pri katerem ni obvezna oblika, v kateri je le-ta izražen.

- Občutljivi osebni podatki so tisti, ki vsebujejo podatke o posameznikovem verskem, političnem, filozofskem prepričanju, članstvu v sindikatu, o rasnem, narodnem ali narodnostnem poreklu, zdravstvenem stanju, vpisu ali izbrisu v ali iz kazenske ali prekrškovne evidence, spolnem življenju ter biometričnih značilnostih.

- Posameznik je določena ali določljiva fizična oseba, katere osebni podatek je last oziroma na katero se le-ta nanaša. Ta oseba je določljiva, če se le lahko identificira na način, ki ne zahteva veliko časa in ne napravi veliko stroškov.

- Zbirko osebnih podatkov predstavlja vsak strukturiran niz podatkov, v katerem je vsebovan vsaj en osebni podatek in ni važno, če je ta centraliziran ali organiziran in strukturiran na podlagi meril, ki omogočajo združevanje ali uporabo podatkov, in ne glede na to, ali so ti obdelani s pomočjo informacijske tehnologije ali ne.

- Obdelava osebnih podatkov pomeni shranjevanje, zbiranje ali združevanje osebnih podatkov v zbirkah, spreminjanje, sporočanje ali uporabo, vključno z iskanjem, brisanjem, prenosom in blokiranjem. Obdelava lahko poteka s pomočjo sredstev informacijske tehnologije ali ročno.

- Nosilci podatkov so čisto vse vrste sredstev, na katerih so podatki posneti ali zapisani: gradiva, listine, spisi, mikrofilmi, naprave za prenos podatkov ipd.

- Uporabnik osebnih podatkov je pravna ali fizična oseba zasebnega ali javnega sektorja, ki se ji osebni podatki razkrijejo ali posredujejo.

- Upravljavec osebnih podatkov je pravna ali fizična oseba, ki skupaj z drugimi ali pa sama določa sredstva ter namene obdelave osebnih podatkov, oziroma je to oseba, ki je določena z zakonom in določa tudi sredstva in namene obdelave.

- Skupni katalog osebnih podatkov je katalog vseh zbirk osebnih podatkov, ki ga vodi in upravlja pristojni organ.

- Blokiranje pomeni takšno spremembo oblike osebnih podatkov, da se ne morejo več povezovati s posameznikom ali pa je to mogoče z nesorazmerno velikimi stroški in napori ali porabo časa.

2.4.2 TEMELJNA NAČELA

Za ZVOP-1 smo ugotovili, da deluje po principu treh pomembnih elementov ali, drugače rečeno, načel. In ta so:

- Načelo zakonitosti in poštenosti – to načelo vsebuje 2. člen ZVOP-1 in je primarno ter najpomembnejše načelo, ki pravi, da se morajo vsi osebni podatki obdelovati pošteno ter zakonito.

- Načelo sorazmernosti – določa 3. člen in pravi, da morajo biti vsi osebni podatki ustrezni in primerni po obsegu glede na namene, za katere se zbirajo in kasneje tudi obdelujejo.

- Načelo prepovedi diskriminacije je opisano v 4. členu zakona ter zagotavlja vsakemu posamezniku varstvo njegovih osebnih podatkov ne glede na raso, barvo, narodnost, jezik, spol, veroizpoved, etično pripadnost, politično ali kakšno drugo prepričanje, izobrazbo, rojstvo, spolno usmerjenost, državljanstvo, družbeni položaj, premoženjsko stanje, vrsto oziroma kraj prebivališča ali katerokoli drugo osebno okoliščino.

2.4.3 OBDELAVA OSEBNIH PODATKOV

Obdelavo osebnih podatkov zakon določa od svojega 8. člena in vse do 28. člena. Zaradi različnih pristojnosti in položaja se je zakonodajalec odločil, da se regulacija obdelave osebnih podatkov v javnem in zasebnem sektorju obravnava različno. V javnem sektorju so pravne podlage precej ožje kot v zasebnem sektorju. Le če zakon določa obdelavo tako med zasebnim in javnim sektorjem, ne obstajajo razlike, saj je tako dopustna že ex lege, ampak še vseeno je treba paziti na sorazmernost obdelave in njen namen, ki mora biti zapisan v vsakem zakonu. V zasebnem sektorju se posameznikovo osebno privolitev enači z določenostjo v zakonu. To pomeni, da se v zasebnem sektorju osebni podatki lahko obdelujejo, če konkretizacijo in obdelavo podatkov določa zakon ali če je za obdelavo podana osebna privolitev posameznika. Vsak posameznik, čigar podatki se obdelujejo na podlagi njegove privolitve, mora biti vedno prehodno seznanjen z namenom obdelave. 12. člen uvaja tudi poseben režim za obdelovanje, ki pravi, da je obdelava nujna, kadar gre za potrebe po varovanju posameznikovega telesa ali življenja. Tu ZVOP-1 daje pravno podlago brez druge zakonite pravne podlage. Posebej zaščitena in zavarovana kategorija je zaradi svoje subtilnosti kategorija občutljivih osebnih podatkov, ki se lahko obdelujejo le v osmih, posebej določenih namenih (Pirc Musar, Prelesnik & Bien Karlovšek, 2006).

2.4.4 KATALOG ZBIRKE OSEBNIH PODATKOV IN REGISTER ZBIRK

Vsak posameznik ima pravico vedeti, na kakšen način, zakaj in kdo obdeluje njegove osebne podatke, zato je v ta namen ZVOP-1 zavezal upravljavce osebnih podatkov k vzpostavitvi kataloga za vsako zbirko osebnih podatkov. To lahko interpretiramo tako, da je zagotovljeno vsakemu posamezniku, da ve, na kakšen način, zakaj in kdo obdeluje njegove osebne podatke, zakon pa tudi določa, da se obvezno naredi katalog zbirke osebnih podatkov, ki ima kot večina uradnih dokumentov tudi obvezne sestavine. Informacijski pooblaščenec hkrati vodi, vzpostavi in vzdržuje register zbirk osebnih podatkov. Register mora biti obvezno objavljen na njegovi spletni strani.

2.4.5 PRAVICE POSAMEZNIKA

Tej kategoriji se bomo posebej posvetili v naslednjem poglavju, tukaj pa smo jo vseeno omenili, ker predstavlja pomembno področje zakona.

2.4.6 IZNOS OSEBNIH PODATKOV

Glede iznosa osebnih podatkov iz Slovenije je ZVOP-1 izenačil vse države Evropske unije in Evropskega gospodarskega prostora (Evropski gospodarski prostor predstavlja prosto trgovinsko področje, ki poleg držav članic Evropske unije zajema še Islandijo, Norveško in Lichtenstein) s Slovenijo. Poudarek je na iznosu osebnih podatkov v tretje države, torej tiste, ki niso del Evropske unije ali Evropskega gospodarskega prostora. Iznos v tretjo državo je dovoljen le, če informacijski pooblaščenec izda odločbo, da ta država zagotavlja ustrezen nivo varstva osebnih podatkov. Odločba ni potrebna v primeru, če je ta država na seznamu držav, ki ga ima informacijski pooblaščenec, in za katero je potrjeno, da v celoti ali pa vsaj delno zagotavlja ustrezen in kakovosten nivo varstva osebnih podatkov, če tako določata zakon in mednarodna pogodba ali če vsak posameznik v to pisno privoli.

Možen je tudi iznos zaradi zavarovanja življenja ali telesa posameznika, izvršitve in sklenitve pogodbe, ki je v korist posameznika, in še zaradi nekaterih drugih določenih razlogov, ki jih taksativno našteva zakon (Pirc Musar, Prelesnik & Bien Karlovšek, 2006).

2.4.7 POSEBNA PODROČJA

ZVOP-1 zaradi razlogov, kot so moderna tehnologija, specifična materija in sodobni način življenja, ureja pet posebnih področij varstva osebnih podatkov. Ti so urejeni od 72. do 90. člena. Posebna področja so sledeča: neposredno trženje, videonadzor, biometrija, evidenca vstopov in izstopov iz prostorov ter javne knjige in povezovanje zbirk osebnih podatkov.

3 PRAVICE POSAMEZNIKA IN NJIHOVO VARSTVO

3.1 PRAVICE POSAMEZNIKA

V zvezi z obdelovanjem osebnih podatkov ima vsak posameznik vrsto pravic, ki mu omogočajo seznanjanje, zagotavljanje točnosti in ažurnosti podatkov ter ustrezno institucionalno varstvo v primeru kršitve predpisov varstva osebnih podatkov.

3.1.1 VPOGLED V REGISTER

Informacijski pooblaščenec je vsakomur dolžan omogočiti vpogled v register zbirk osebnih podatkov in tudi prepis le-teh; tako lahko iz tega sklepamo, da se mora vsakemu posamezniku omogočiti vpogled v njegove zbrane osebne podatke, ima pa tudi pravico do prepisa. Prepis in vpogled se morata dovoliti in omogočiti praviloma še v istem dnevu, najkasneje pa v osmih dneh, sicer se šteje, da je bila zahteva posameznika zavrnjena (Pirc Musar, Prelesnik & Bien Karlovšek, 2006).

3.1.2 PRAVICA DO SEZNANITVE

Upravljavec osebnih podatkov mora posamezniku na njegovo zahtevo:

- omogočiti vpogled v katalog zbirke osebnih podatkov;
- potrditi, ali se podatki v zvezi z njim obdelujejo ali ne, in mu omogočiti vpogled v osebne podatke, ki so vsebovani v zbirki osebnih podatkov in se nanašajo nanj, ter njihovo prepisovanje ali kopiranje;
- posredovati izpis osebnih podatkov, ki so vsebovani v zbirki osebnih podatkov in se nanašajo nanj;
- posredovati seznam uporabnikov, katerim so bili posredovani osebni podatki, kdaj, na kakšni podlagi in za kakšen namen;
- dati informacijo o virih, na katerih temeljijo zapisi, ki jih o posamezniku vsebuje zbirka osebnih podatkov, in o metodi obdelave;
- dati informacije o namenu obdelave in vrsti osebnih podatkov, ki se obdelujejo, ter vsa potrebna pojasnila v zvezi s tem;
- pojasniti tehnične oziroma logično-tehnične postopke odločanja, če izvaja avtomatizirano odločanje z obdelavo osebnih podatkov posameznika.

Izpis iz 3. točke prejšnjega odstavka ne more nadomestiti listine ali potrdila po predpisih o upravnem ali drugem postopku, kar se označi na izpisu (ZVOP-1, 30. člen).

To pravico pa lahko posameznik uresniči le, ko vloži ustrezno pisno ali ustno zahtevo na zapisnik pri upravljavcu njegovih osebnih podatkov, se pravi, da mora to na ustrezen in predpisan način zahtevati, drugače pravice sploh ne more uveljaviti. Upravljavec mu je dolžan omogočiti vpogled ali prepis najpozneje v roku petnajstih dni, ko posameznik ustrezno zahteva uveljavitev pravice, v primeru, če mu upravljavec tega ne dovoli, mu mora v istem roku pisno sporočiti razloge, zakaj to ne bo mogoče. Če upravljavec posameznika v predpisanem roku ne obvesti o tem, kakšna je njegova odločitev, se šteje,

da je bila zahteva posameznika za uveljavitev pravice zavrnjena. Če posamezniku ni omogočena seznanitev z njegovimi osebnimi podatki in misli, da mu je bila storjena krivica, ima le-ta pravico do pritožbe pri informacijskem pooblaščencu.

3.1.3 PRAVICA DO DOPOLNITVE, POPRAVKA, BLOKIRANJA, IZBRISA IN UGOVORA

Po določilu 18. člena morajo biti vsi osebni podatki, ki so v obdelavi, točni in ažurni, tako mora tudi upravljavec zbirke osebnih podatkov na zahtevo posameznika osebne podatke izbrisati, blokirati, popraviti ali dopolniti, če je posameznik ugotovil, da so netočni, nepopolni, neažurni ali da so bili obdelani ali zbrani v nasprotju z zakonom. Če se posameznik odloči, da to zahteva, mora upravljavec obvestiti vse morebitne uporabnike in pogodbene obdelovalce, ki jim je posredoval te posameznikove osebne podatke. Tega pa mu ni potrebno storiti le v primeru, če bi to zahtevalo veliko dela in časa ter bi napravilo veliko stroškov. Sama zahteva se vloži ustno ali pisno na zapisnik pri upravljavcu. Navedene spremembe mora opraviti v roku petnajstih dni od prejema zahteve in o tem tudi obvestiti vlagatelja zahteve ali pa ga v istem roku obvestiti o konkretnih razlogih, zakaj tega ne bo opravil. Če se upravljavec odloči za molk, se v tem primeru šteje, da je zahteva zavrnjena. Stroške sprememb in vseh ostalih dejanj upravljavca krije on sam. V primeru, če upravljavec sam ugotovi, da so osebni podatki posameznika nepopolni, netočni ali neažurni, jih mora po uradni dolžnosti popraviti ali dopolniti in hkrati o tem svojem dejanju tudi obvestiti posameznika, če le v zakonu ni določeno kako drugače (Pirc Musar, Prelesnik & Bien Karlovšek, 2006).

3.2 SODNO VARSTVO PRAVIC POSAMEZNIKA

Vsakemu posamezniku pravico do sodnega varstva jamči že Ustava RS, podrobneje pa je urejena v ZVOP-1. Posameznik lahko svojo pravico do varstva osebnih podatkov zahteva s tožbo ali s pomočjo Zakona o pravdnem postopku ali pa z Obligacijskim zakonikom. Posameznik lahko zahteva sodno varstvo s tožbo za ves čas trajanja krivice in za ugotovljeno krivico, ki ne obstaja več, če ni zagotovljeno drugo sodno varstvo. Postopek s tožbo je na sodišču prednosten in nujen, zato ga je sodišče prisiljeno izvesti v najkrajšem možnem času. V postopku ugotovljene krivice odloča pristojno sodišče po določbah zakona, ki jih ureja upravni spor. Med postopkom mora biti javnost izključena, če na predlog posameznika sodišče iz utemeljenih in tehtnih razlogov ne odloči kako drugače. V tožbi, ki je bila vložena zaradi kršitev pravic iz 32. člena ZVOP-1, lahko posameznik zahteva od sodišča, da do pravnomočne odločitve sodišča v upravnem sporu le-ta naloži upravljavcu osebnih podatkov, da mora preprečiti vsakršno obdelavo spornih osebnih podatkov, sploh če bi močno prizadela posameznika, ki je vložil tožbo, težko popravljiva škoda, odložitev obdelave pa ni v nasprotju z javno koristjo in tudi ne obstajajo nevarnosti, da bi pri nasprotni stranki nastala večja škoda. V kazenskem zakoniku so tako vsebovane vse človekove pravice in temeljne svoboščine, ki jih jamčijo Ustava RS in mednarodni pravi akti. 38. člen Ustave RS zagotavlja pravico do varstva osebnih podatkov in v primeru kršitev tudi določene sankcije. S kazenskimi določbami, ki urejajo in določajo kazni za primere kršitev določb zakona, so posamezniki na posreden način zavarovani pred zlorabami njihovih osebnih podatkov. Kršitev določil Zakona o varstvu osebnih podatkov

oziroma zlorabo osebnih podatkov Kazenski zakonik označuje in jo pojmuje kot kaznivo dejanje, saj je to poseg v pravico do zasebnosti vsakega posameznika. V prekršku je vsak, ki osebne podatke uporabi neskladno z namenom njihovega zbiranja, neskladno z zakonom oziroma brez osebne privolitve posameznika, vsakdo, ki vstopi v računalniško vodeno zbirko podatkov, ki nepooblaščeno vdre z namenom pridobitve določenih osebnih podatkov, vsakdo, ki z namenom izkoriščanja pravic in premoženjske koristi druge osebe prevzame identiteto druge osebe. Kazen, ki se predpiše, je lahko zaporna ali denarna (Kramar, 2013).

Tudi ZVOP-1 v svoji vsebini vsebuje kazenske določbe, in sicer vse od svojega 91. člena in do vključno 103. člena. Narekuje nam denarne kazni in tako smo iz njegovih določil videli, da najvišja možna denarna kazen oziroma globa znaša 12.510 evrov, najmanjša možna kazen pa 200 evrov.

3.3 INSTITUCIONALNO VARSTVO – INFORMACIJSKI POOBLAŠČENEC KOT NADZORNI ORGAN

V letu 2005, natančneje 31. decembra tega leta, ko je stopil v veljavo Zakon o informacijskem pooblaščencu, smo v Sloveniji dobili samostojen in neodvisen državni organ, ki bdi nad varstvom osebnih podatkov. Informacijski pooblaščenec ima poleg svojih pristojnosti na področju dostopa do informacij javnega značaja tudi mnoge pristojnosti na področju varstva osebnih podatkov. Ena od njegovih pristojnosti je izvajanje inšpekcijskega nadzora nad izvajanjem ZVOP-1 in drugih predpisov s področja varstva osebnih podatkov, zagotavlja nam enotno uresničevanje ukrepov, sodeluje tudi s pristojnimi ministrstvi, ko gre za priprave predpisov s področja varstva osebnih podatkov (Pirc Musar, Prelesnik & Bien Karlovšek, 2006).

Informacijski pooblaščenec v okviru inšpekcijskega nadzora nadzoruje zakonitost obdelave osebnih podatkov, ustreznost ukrepov in izvajanje postopkov za zavarovanje le-teh, izvajanje zakonskih določb, ki urejajo katalog zbirk osebnih podatkov ter register zbirk in evidentiranje posredovanja osebnih podatkov posameznim uporabnikom, iznos osebnih podatkov v druge, tretje države ter posredovanje tujim uporabnikom (Pirc Musar, Prelesnik & Bien Karlovšek, 2006).

Informacijski pooblaščenec sodeluje tudi z drugimi državnimi organi, organi Evropske unije, ki so zadolženi za varstvo osebnih podatkov, mednarodnimi organizacijami, združenji, zavodi, nevladnimi organizacijami s področja varstva osebnih podatkov ali zasebnosti, tujimi nadzornimi organi za varstvo osebnih podatkov ter tudi z drugimi organizacijami, ki so aktivne in pomembne na področju varstva osebnih podatkov (Pirc Musar, Prelesnik & Bien Karlovšek, 2006).

3.4 OMEJITEV PRAVIC

Nekatere posameznikove pravice pa je mogoče tudi omejiti. To je mogoče le z izvedbo testa sorazmernosti, ki je zelo strogo izveden predvsem iz razloga, ker je pravica do varstva osebnih podatkov ena izmed ustavnih pravic. Omejiti je mogoče le sledeče pravice:

- pravico do dopolnitve, popravka, blokiranja, izbrisa in ugovora,
- pravico posameznika do seznanitve z lastnimi osebnimi podatki ter
- pravico do obveščanja posameznika o obdelavi njegovih osebnih podatkov.

Takšen poseg v pravico oziroma njeno omejitev izvrševanja je mogoče določiti le z zakonom ter zaradi tega, da se pravno varuje pomembne dobrine oziroma objekte varstva, ki jih sam zakon eksplicitno narekuje.

4 VARSTVO OSEBNIH PODATKOV PRI UPORABI INFORMACIJSKE TEHNOLOGIJE – UPORABA SPLETNIH DRUŽBENIH OMREŽIJ

4.1 INFORMACIJSKA TEHNOLOGIJA IN INFORMACIJSKO KOMUNIKACIJSKA TEHNOLOGIJA

Pod pojem informacijska tehnologija, skrajšano IT, vključujemo vse tehnologije, ki se uporabljajo za obdelovanje, zbiranje, zaščito in shranjevanje podatkov. Ta se nanaša na strojno opremo ali hardware, software ali računalniško programsko opremo ter na računalniško omrežje. Programska oprema je za razliko od strojne opreme nematerialni del računalnika in obsega vse računalniške programe. Te programe pišejo programerji ali razvijalci v različnih programskih jezikih in so sestavljeni iz zaporedja ukazov, napisanih v skladu s strogimi pravili. Računalniško omrežje je sestavljeno iz dveh ali več med seboj povezanih računalnikov, z ali brez žic, ki lahko med seboj komunicirajo ali si izmenjujejo informacije. Najbolj znano in razširjeno omrežje je internet. Obstaja približno 2 milijardi njegovih uporabnikov, število še vedno dnevno narašča (Čelebić & Rendulić, 2012).

Pod pojmom informacijsko komunikacijska tehnologija ali skrajšano IKT mislimo na prenos in uporabo vseh vrst informacij. Je temelj gospodarstva in pobudnik družbenih sprememb 21. stoletja ter ima vpliv na vse vidike našega življenja. Lahko rečemo, da bi brez te tehnologije naše življenje bilo nepredstavljivo. Oddaljenost ne predstavlja več ovire do dostopa informacij. Kot primer lahko izpostavimo npr. delo in učenje na daljavo, e–bančništvo, e–uprava itd. Izraz zajema vsa tehnična sredstva, ki so namenjena za ravnanje z informacijami in omogočanje komunikacije, ki vključuje tako računalnike kot tudi omrežne strojne opreme, komunikacijske linije ter ves potreben software. Z drugimi besedami povedano, IKT sestavljajo vse informacijske tehnologije, elektronski mediji, telefonija, vse vrste obdelave in prenosa video in avdio signalov ter vse funkcije spremljanja in nadzora, ki temeljijo na tehnologiji omrežja (Čelebić & Rendulić, 2012).

4.2 OPREDELITEV IN OSNOVNE ZNAČILNOSTI DRUŽBENIH OMREŽIJ

Ker se internet nezadržno širi po vsem svetu in ga vsak dan uporablja več ljudi, bodo varnostna vprašanja postala še pomembnejša. Posamezne države bodo imele različne zakone, ki bodo določali, kaj je lahko oziroma kaj ne sme biti šifrirano in katera metoda sme biti uporabljena. Razrast interneta bo močno vplival na naš odnos do komunikacij in način sodelovanja med državami (Hoffman, 1996, str. 180).

Spletna družabna omrežja predstavljajo spletne storitve, aplikacije, strani ali platforme, ki odražajo in gradijo socialne mreže ali socialne odnose med posamezniki, ki imajo na primer skupne interese ali aktivnosti. Posameznikom omogočajo:

- ustvarjanje delno javnega ali popolnoma javnega profila znotraj omenjenega sistema,

- ustvarjanje seznama uporabnikov, s katerimi so povezani ter
- pretok in prikazovanje njihovih seznamov povezav in povezav drugih znotraj sistema.

Glavni atribut omrežij je ponujanje posamezniku možnost ohranjanja stikov z ljudmi, ki jih morda ne bo videl nikoli več. Potem lahko po drugi strani z njihovo pomočjo vsak posameznik zgradi novo obsežnejšo mrežo poznanstev in tako pridobiva nove prijatelje. Vsi odnosi, ki so zgrajeni na spletu oz. omrežju, zajemajo veliko število uporabnikov interneta, katerih članstvo pa ni trdno - je izredno tekoče z nizkimi socialnimi stroški, ki so povezani z vstopom ali izstopom.

Za spletno mreženje so značilne konvencionalne funkcije. V največ primerih morajo uporabniki narediti svoj profil, le-ta pa vsebuje različne informacije o njih. Obstaja tudi možnost, da na svoj profil naložijo svoje slike ali objavijo blog. Dodatek k profilom je mesto, kjer se zbirajo komentarji vseh naših prijateljev in drugih uporabnikov. Za varstvo zasebnosti vsakega uporabnika imajo omrežja po navadi ukaze, ki omogočajo uporabniku, da sam uredi, kdo lahko vidi njegov profil, ga kontaktira itd.

Nekatera spletna družbena omrežja imajo še dodatne funkcije. Te so recimo možnost nalaganja in predvajanja video datotek, možnost razpravljanja v forumih ter možnost ustvarjanja skupin, ki imajo skupne pripadnosti in interese. Navsezadnje pa je postalo popularno tudi mobilno socialno mreženje. To nam dodatno poenostavi nenehno povezovanje samih uporabnikov, saj računalnik ni več potreben, hkrati pa si lahko v stiku s svojimi prijatelji kjer koli in kadar koli, se pravi na vsakem koraku.

4.3 VRSTE IN PREDSTAVITEV NAJBOLJ PRULJUBLJENIH

Katere vrste spletnih družbenih omrežij bomo zasledili, je odvisno od tega, kakšne interaktivne storitve nam ponujajo in kako se dostopa do njih. Dandanes so mobilna omrežja že skoraj vsa družbena omrežja in omogočajo tudi dostop preko mobilnega telefona (primer: Facebook, Twitter, Myspace). Ena vrsta, bi lahko rekli, so spletna omrežja, ki so usmerjena v profile. Na spletni strani oziroma profilu posameznika se tako hranijo informacije o njegovih aktivnostih, interesih, željah, slike itd. (primer: Facebook, Myspace). Potem imamo vsebinska omrežja, ki so specializirana za eno vsebino, dober primer je Flickr, ki omogoča deljenje slik, deljenje videa pa omogočata npr. najbolj znani YouTube in Vimeo, obe našteti storitvi pa ponuja na primer Instagram. Kot vrsto lahko omenimo še omrežja, ki imajo večuporabniško virtualno okolje (primer: Second Life in World of Warcraft) ter spletna družbena omrežja, ki nam nudijo pisanje mikrobloga, katerega najbolj znani predstavnik je Twitter z omejitvijo 140 znakov na sporočilo.

4.3.1 FACEBOOK

Facebook je spletno družbeno omrežje, ki je bilo ustanovljeno v letu 2004, natančno 4. februarja v mestu Cambridge. To pripada zasebnemu podjetju Facebook Inc. Omogoča nam brezplačen dostop in možnost, da se povežemo na eno ali več omrežij, kot so na primer šola, zemljepisno območje ali delovno mesto, in tako na lažji način komuniciramo

z ljudmi iz istega omrežja. Določene univerze v ZDA takšne profile razdelijo svojim bodočim študentom in svojemu osebju, da se le-ti hitreje in uspešneje spoznajo z ljudmi na ozemlju univerze.
Zaradi njegove odprtosti je dokaj veliko držav preprečilo dostop do njega, med njimi so države, kot so Sirija, Burma, Iran, Združeni arabski emirati ter Butan. Sirska vlada je recimo njegovo uporabo prepovedala zato, ker naj bi se na njem promoviralo napade na oblast, prav tako se so zbali izraelskega prepletanja družbenih omrežij na strani. Državljani so Facebook uporabljali tudi kot sredstvo za kritiziranje vlade, v Siriji pa so zaradi tega uvedli celo zaporno kazen. Združeni arabski emirati so Facebook prepovedali zaradi dejstva, da naj bi spodbujal internetne zmenke, v Iranu pa so se zbali oblastniki, da se bo preko njega začelo delovanje različnih opozicijskih gibanj.

4.3.2 TWITTER

Twitter je tudi eden izmed najbolj znanih brezplačnih spletnih družbenih omrežij današnjega časa, ki je pričelo z delovanjem leta 2006. Po svojem namenu in bistvu Twitter spominja na nekakšno mešanico klepetalnice in bloga, razlika med objavami na Twitterju in na blogu je v tem, da lahko objava na Twitterju vsebuje maksimalno 140 znakov, čemur pravimo tudi microblogging.

Velik plus pri njegovi uporabi je v tem, da pri registraciji ni potrebno posredovati nobenih osebnih podatkov razen priimka ter imena in e-mail naslova, na Facebooku pa že prosijo za spol, datum rojstva, telefonsko številko itd. Ker dejansko nimamo možnosti objavljati velike količine osebnih podatkov, smo manj izpostavljeni različnim zlorabam ter vdorom v zasebnost.

4.3.3 LINKEDIN

Tukaj se lahko vsak posameznik povezuje s strokovnjaki s svojega delovnega področja, širi svojo mrežo poznanstev znotraj svoje stroke ali izven nje, pride v stik z določenimi kadri v izbranem podjetju in si ustvarja svoj profesionalni ugled tudi v virtualnem svetu. Namenjen je tudi iskanju zaposlitve, saj nam predstavlja brezčasen zaposlitveni sejem, kjer lahko delodajalec na enostaven način dobi vpogled in pregled nad delom, izobrazbo, spretnostnimi posameznika ipd.

Če želite priti v stik z neko določeno osebo, zaposleno v podjetju, kjer bi si želeli zaposlitev, obiščete profil tega podjetja, si ogledate seznam vseh zaposlenih in pošljete tej osebi sporočilo z namenom poizvedovanja o delu.

Tudi tu sta potrebni premišljenost in previdnost pri uporabi ter objavah. Previdni moramo biti predvsem zato, ker svoj profil ustvarjamo tudi za popolnoma neznane osebe, naše potencialne sodelavce in delodajalce, s katerimi še nismo vzpostavili stikov. Mnogo jih tukaj dela veliko napak in le-te jim včasih otežijo iskanje službe.

4.3.4 YOUTUBE

Youtube je javna spletna komunikacijska stran, ki svojim uporabnikom omogoča nalaganje video posnetkov in gledanje posnetkov drugih registriranih uporabnikov. Videe lahko nalagajo vsi, tako začetniki kot profesionalci. Video vsebine si lahko ogledaš, tudi če nisi registriran uporabnik. Stran vsebuje ogromno količino video posnetkov, od glasbe do posnetih hišnih ljubljenčkov, nasvetov, kako si napraviti frizuro in se naličiti, najdemo res prav vse, tudi najbolj čudne stvari. Youtube pride prav tudi mnogim podjetjem, saj lahko za nizko ceno predstavljajo svoje produkte širši okolici. Predstavlja tudi možnost za nadobudneže, ki si želijo uspeti v glasbenih vodah in tu najdejo eno izmed možnosti, da se predstavijo širši množici. Youtube vseeno ni čisto nefiltriran, pri njegovi uporabi najdemo in zasledimo veliko videov, ki niso primerni za mlajše občinstvo.

4.3.5 MYSPACE

To spletno družbeno omrežje je priljubljeno med ustvarjalci glasbene industrije, ker ga uporabljajo za brezplačno predstavitev širši javnosti. Financiranje strani omogočajo oglasi na njihovi strani, članstvo in ustvarjanje profila pa sta brezplačna. V slovenskem jeziku ime pomeni moj prostor, uporabniki pa objavljajo svoje slike, ustvarijo blog in dodajo svoj opis ipd.

4.4 MEDSEBOJNA KOMUNIKACIJA

Ljudje smo po naravi izrazito prosocialno naravnani. Vsak posameznik ima željo po druženju in pripadnosti. To dejstvo pripomore k temu, da vzpostavljamo odnose tudi v kibernetskem prostoru. Spletna družbena omrežja lahko uvrščamo v tako imenovane komunikacijske modele, in sicer v model »eden-z-enim« oziroma one to one. Zanj je značilno medosebno in neposredno komuniciranje ali komuniciranje iz oči v oči, ki poteka med dvema posameznikoma v istem prostoru.

Za vsa spletna družbena omrežja je značilno, da je komunikacija v precejšnji meri odvisna od obligacije, da se komunicira. Ta pa ni samo verbalna, ampak tudi neverbalna ter vizualna. Nekje lahko za komunikacijo uporabljamo slike ter videoposnetke, nekje pa tudi zelo razširjene aplikacije, kot jih ima Facebook, ki jih naredijo uporabniki sami in služijo kot virtualna darila. Pogosto pride do kombinacije tako neverbalnih kot verbalnih sredstev komunikacije, v veliko primerih pa so besedila integrirana v digitalni videoposnetek ali sliko. Druga pomembna značilnost komunikacije v spletnih družbenih omrežjih je tudi možnost sinhrone v realnem svetu in asinhrone, odložene komunikacije.

4.5 SLABOSTI SPLETNIH DRUŽBENIH OMREŽIJ

Poleg vseh pozitivnih lastnosti je potrebno omeniti nekatere slabe lastnosti. Kot pri vsaki spletni aplikaciji ali storitvi tudi tukaj naletimo na morebitne neprijetnosti in zlorabe. Najbolj problematično vprašanje je vprašanje zasebnosti in varstva osebnih podatkov, ki ga obravnavamo v diplomskem delu. Uporabniki v svojih profilih objavljajo preveč svojih osebnih podatkov, ki so lahko tarča nepridipravov. Lahko pride do kraje identitete, pojavijo se številni vprašljivo pristni profili, lažni profili in informacije ter dvojni profili. Kraja

identitete se lahko pojavi v obliki prevzema le-te v dobesednem pomenu: da se nekdo registrira v spletno družbeno omrežje z identiteto nekoga drugega. Uporabniki lahko zaradi objav različnih osebnih podatkov na svojem profilu postanejo žrtve tako prevzema identitete izven virtualnega sveta kot tudi tako imenovane finančne kraje identitete. Kaznivo dejanje kraje identitete bom podrobneje opisala v naslednjem poglavju. Problem je v tem, da ko se enkrat določena stvar objavi, jo je skoraj nemogoče izbrisati. Poleg zlorabe osebnih podatkov in posega v posameznikovo zasebnost zasledimo tudi dva druga tipa zlorab, to sta spletno teroriziranje ter trolling oz. emocionalna zloraba, se pravi norčevanje in žaljenje.

Širša uporaba spletnih družbenih omrežij pa glede na neko raziskavo iz leta 2009 otežuje ohranjanje popolne anonimnosti uporabnikov. Raziskovalca Arvind Narayanan in Vitalij Šmatikov sta z analizo povezav med uporabniki spletnih družbenih omrežij tako identificirala mnoge posameznike, ki naj bi objavili domnevno anonimne podatke. Te podatke namreč lastniki spletnih strani prodajajo oglaševalskim podjetjem, ki jim predstavljajo pomemben vir dohodka. Rezultati raziskave so pokazali, da bi morala spletna podjetja narediti dokaj več za zaščito zasebnosti njihovih uporabnikov.

Razvila sta računalniški algoritem, ki zna domnevno anonimnim podatkom pripisati imena in naslove uporabnikov, na katere se navezujejo. Ta algoritem dejansko analizira povezave med vsemi uporabniki družbenih omrežij in ne samo med neposrednimi prijatelji. Oba opozarjata, da bo z množično uporabo spletnih družbenih omrežij ohranjanje anonimnosti uporabnikov postalo zahtevnejše . Uporabnike bi bilo potrebno obvestiti, menita, da se nameravajo njihovi podatki razkriti tretjim osebam ali podjetjem, čeprav so jim ponudili možnost, da onemogočijo razkritje njihovih osebnih podatkov (Narayanan & Šmatikov, 2009).

5 NEVARNOSTI ZA ZLORABE OSEBNIH PODATKOV PRI UPORABI SPLETNIH DRUŽBENIH OMREŽIJ

5.1 KIBERNETSKA KRIMINALITETA

Danes si zelo težko predstavljamo, da je bila prva spletna stran postavljena samo dve desetletji nazaj, sploh ker se razvoj informacijsko komunikacijskih tehnologij odvija z eksponentno hitrostjo. Pojem informacijsko komunikacijske tehnologije (ali skrajšano IKT) vsebuje predvsem informacijsko komunikacijske tehnologije, ki so se razvile iz računalniške in telekomunikacijske industrije. Ko se je oblikovalo globalno interaktivno virtualno okolje, se je začel kibernetski prostor neizogibno prepletati s fizičnim prostorom. Zaradi hitrega razvoja pa niso prilagodili niti etičnih niti moralnih, kaj šele kazenskopravnih vidikov delovanja kibernetskega prostora. S prenosom v virtualno okolje so se tako izboljšale obstoječe oblike kaznivih dejanj, hkrati pa so se razvile nove oblike, ki obstajajo samo v virtualnem okolju. Ta kazniva dejanja povzročajo najrazličnejše psihološke, fizične, finančne ali čustvene posledice. Kot sem že prej omenila, se zloraba osebnih podatkov šteje kot kaznivo dejanje (Dimc & Dobovšek, 2012).

Kibernetska kriminaliteta se zaradi značilnosti kibernetskega prostora, kot so občutek anonimnosti, mednarodni vidik, lokacijska in časovna neodvisnost, širi z neverjetno hitrostjo in zajema iz dneva v dan nove prostore in niše, le malo od teh pa je odkritih in procesiranih. Prav zaradi problema pojavnosti novih oblik in težjega odkrivanja bi lahko računalniško kriminaliteto uvrstili med najnevarnejše in družbi najbolj škodljive pojavne oblike sodobnega kriminala (Dobovšek, 2012, str. 11).

Z vidika kazensko procesnega prava morajo tako biti vsa kazniva dejanja obravnavana enako, ne glede na dejstvo, kje je bilo to kaznivo dejanje storjeno – v resničnem ali v virtualnem svetu.

5.2 KAZNIVA DEJANJA

V nadaljevanju oziroma v obeh podpoglavjih tega poglavja bomo na kratko našteli in predstavili vsa kibernetska kazniva dejanja in jih razdelili v dve skupini, katerih avtorja sta oziroma ju navajata Dobovšek in Dimc. V vsaki skupini kaznivih dejanj se bomo posebej posvetili enemu izmed njih, za obe kaznivi dejanji pa menimo, da lahko najbolj prizadeneta uporabnike spletnih družbenih omrežij, ko gre za varstvo njihovih osebnih podatkov.

5.2.1 KAZNIVA DEJANJA ZOPER ZAUPNOST, CELOVITOST IN DOSTOPNOST RAČUNALNIŠKIH PODATKOV IN SISTEMOV

Ta kazniva dejanja spadajo v novo obliko kriminalitet, ki so se razvile skupaj z informacijsko komunikacijskimi tehnologijami. Primarno se izvajajo v kibernetskem prostoru. V takšnih primerih je potrebna določena stopnja tehničnega znanja, sama raven pa je odvisna od zahtevnosti izvedenega napada. Gre za kazniva dejanja, katerih posledice so predvsem tehnične narave, čedalje pogosteje pa tudi finančne narave (Dimc & Dobovšek, 2012).

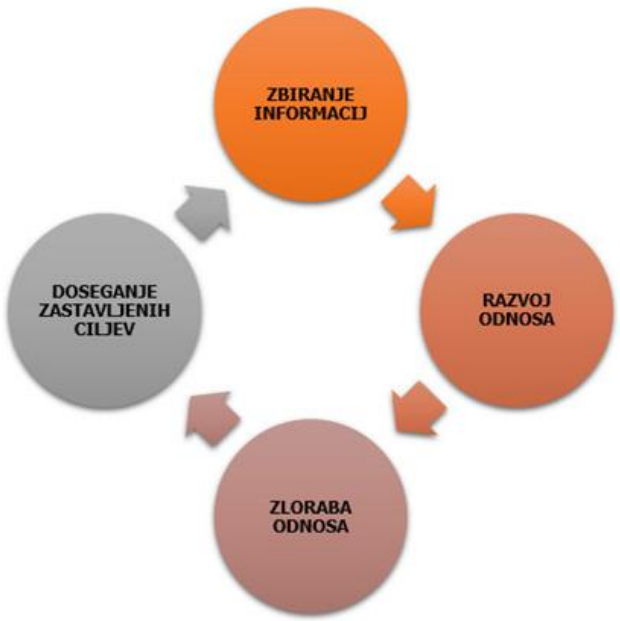
Ta kazniva dejanja lahko razdelimo v štiri skupine, in sicer so to:

- vdori v sisteme (programi za vohunjenje …),
- onemogočanje ali motenje storitev (DOS ali DDOS napadi),
- škodljiva programska koda (trojanski konji, računalniški črvi, virusi, kombinirane grožnje) ter
- ugrabitev, kraja ali uničenje informacij.

Pozornost bomo posebej namenili socialnemu inženiringu, ki spada v to kategorijo kaznivih dejanj, in sicer sta ga Dobovšek in Dimc podrobneje umestila v kategorijo vdorov v sistem. Socialni inženiring je pojem, ki ga srečujemo že od rojstva, in sicer gre tu za dejanje oziroma za nekakšno zvijačo, da nekoga pripravimo do nekega dejanja, katerega sam po sebi verjetno ne bi storil. Je ena izmed pomembnejših tehnik, ki jo danes uporabljajo najboljši hekerji, pri čemer gre za primarno pridobivanje določenih koristi, hkrati pa zmanipuliramo določenega posameznika. Osnovno vodilo vseh nas je namreč zaupanje in prav na to se osredotoči storilec, ki z uporabo socialnih in psiholoških tehnik zlorabi zaupanje posameznika oziroma svoje žrtve z namenom, da pridobi želene informacije. Poudarek je tukaj predvsem na uporabi socialnih veščin v nasprotju s tehničnim znanjem, ki je predvsem značilen za to skupino kaznivih dejanj (Dimc & Dobovšek, 2012).

Uporablja se za izvrševanje številčnih in najrazličnejših kaznivih dejanj, vendar se lahko določi nek vzorec, ki se pojavlja v vseh primerih. Gre za njegov življenjski cikel, ki je sestavljen iz zbiranja informacij, razvoja odnosa, zlorabe odnosa ter izvajanja postavljenega cilja (Dimc & Dobovšek, 2012) .

Slika 1: Življenjski cikel socialnega inženiringa



Vir: Gartner v: Dimc & Dobovšek (2012, str. 40)

Do neke mere bi socialni inženiring oziroma njegove tehnike lahko razdelili na tiste, ki zahtevajo večje tehnično znanje, in tiste, ki ga ne zahtevajo.

Med tehnike, ki ga zahtevajo, bi tako uvrstili:

- ribarjenje – gre za vzpostavitev stika po elektronski poti (kot primer lahko rečemo, da dobimo privatno sporočilo na spletnem družbenem omrežju Facebook), kjer je sporočilo prirejeno tako, kot da prihaja iz nekega verodostojnega vira, na primer iz banke. Vzpostavljeno je zaupanje na podlagi legitimnega izgleda sporočila in tako je žrtev pripravljena dati svoje podatke;
- zvabljanje – gre za preusmerjanje na ponarejene spletne strani, ki v celoti delujejo enako kot legitimne različice, zato žrtev nevede izda svoje osebne podatke ob prijavi;
- vishing – je pol tehnični pristop in uporablja oziroma izkorišča internetno telefonijo. Žrtev mora recimo poklicati nek klicni center, ker mu je bilo puščeno lažno sporočilo, in tako operater od njih izvabi osebne podatke in številko kreditne kartice.

Med tehnike, ki ne zahtevajo tehničnega znanja, sodijo:

- gledanje čez ramo – storilec pridobi informacije preprosto z opazovanjem žrtve pri prijavi;
- brskanje po smeteh – gre za dejansko brskanje po smeteh, saj posamezniki in organizacije pogosto vržejo v smeti stvari, ki bi storilcu lahko veliko pomagale;
- neposredni pristop – pri tem lahko navedemo primer, da se nekdo izdaja za nekoga, ki izvaja anketo ali je član nekega tehničnega osebja in tako od nas izvabi določene osebne podatke.

Ena izmed tehnik socialnega inženiringa je tudi povratni ali obrnjeni inženiring. Ta zahteva sicer malo več načrtovanja, vendar se ga ne sme zanemariti. Igro storilec prične s sabotažo sistema, kjer napravi dejansko ali samo navidezno napako. Žrtvi jo pojasni in ji zagotovi, da jo bo popravil. Tako žrtev prepriča, da bo lahko to popravil s pomočjo neke informacije, ki po navadi vključuje vsaj uporabniško ime in geslo žrtve (Dimc & Dobovšek, 2012).

5.2.2 TRADICIONALNA KAZNIVA DEJANJA

Tradicionalna kazniva dejanja, v katere uvrščamo poneverbe, prevare, kraje identitet, nadlegovanja in zalezovanja, so se tako v ogromni meri in količini prenesla v okolje virtualnega sveta, v katerem se izkoristijo prednosti, ki jih ponuja informacijsko komunikacijska tehnologija za pripravo ter izvedbo kaznivih dejanj (Dimc & Dobovšek, 2012).

Tradicionalna kazniva dejanja sta Dobovšek in Dimc razdelila na pet pomembnih skupin, in to so:

- intelektualna lastnina in kršenje avtorskih pravic,

- kibernetsko nadlegovanje, zalezovanje in ustrahovanje,
- širjenje materialov s sporno in žaljivo vsebino (sovražni govor, otroška pornografija),
- prevare, poneverbe in kraja identitete,
- kibernetski terorizem.

Podrobneje bomo opisali kaznivo dejanje kraje identitete. Pojem identiteta lahko definiramo in predstavimo kot način, po katerem se vsak posameznik ali skupina razlikuje od ostalih posameznikov ali skupin. Bistveno vlogo igra priznanje identitete vsakega posameznika v okolju s strani drugih, ker brez tega obstoj identitete posameznika ne obstaja.

Informacijski pooblaščenec opisuje krajo identitete kot uporabo osebnih podatkov ali identitete nekoga drugega za inkriminacijo druge osebe ali za pridobitev neke koristi. Kazenski zakonik razloži v svojem 143. členu krajo identitete kot prevzem identitete neke druge osebe z namenom, da bi izkoristila njene pravice, pridobitve premoženjske koristi ali pa samo zaradi prizadetja njenega osebnega dostojanstva.

Kraja identitete se glede na podatke oziroma področje, na katerega je usmerjena, deli še na naslednje podskupine:

- kloniranje identitete – celovit prevzem identitete žrtve, in sicer jo storilec prevzame za svoje vsakodnevno življenje;
- kraja finančne identitete – zloraba podatkov žrtve z namenom, da storilec pridobi premoženjsko korist;
- kraja poslovne identitete – zloraba poslovnega subjekta storilca kaznivega dejanja z namenom, da si ta pridobi premoženjsko korist;
- kraja zdravstvene identitete – zloraba podatkov žrtve za pridobitev medicinskih storitev ali zdravil;
- kraja kriminalne identitete – storilec uporabi podatke žrtve z namenom, da bo lahko storil kaznivo dejanje.

Pri kraji lahko storilci praviloma uporabljajo različne tehnike, ki zlorabljajo funkcionalnosti IKT-ja, ali pa se osredotočijo na uporabo psihološko socialnih prijemov. Pri slednjem lahko omenimo že predstavljeni socialni inženiring. Ta predstavlja pomemben člen kraje identitete (Dimc & Dobovšek, 2012).

Ključnega pomena za krajo pa so podatki o posamezniku, ki jih storilci kaznivih dejanj najlažje pridobijo na način, ko jim uporabnik nevede in neposredno zaupa podatke. Za to pa uporabljajo naslednje metode:

- skimming ali presnemavanje podatkov s kartic;
- ribarjenje oziroma fishing - storilci želijo s pomočjo lažnih spletnih strani in elektronskih sporočil od žrtve na takšen ali drugačen način izvabiti osebne podatke, kot so: številke kreditnih kartic, uporabniška imena in gesla, digitalna potrdila itd.;

- zvabljanje oziroma pharming kot v primeru ribarjenja pridobivanje zaupnih podatkov žrtev, razlika je zgolj v izvedbi;
- vishing - gre za zlorabljanje telefonskih sistemov za izvedbo socialnega inženiringa in pridobivanja občutljivih podatkov z namenom pridobitve premoženjske koristi. Lahko bi rekli, da gre za ribarjenje z uporabo glasu;
- programi za vohunjenje oziroma spyware – to so vse vrste programov, ki so namenjeni za sledenje uporabnika, za zbiranje informacij o njem, za ogled njegovega delovanja, navadno brez njegove vednosti, in tudi krajo občutljivih osebnih podatkov, kot so gesla.

5.3 VARNOSTNI NASVETI PRI UPORABI SPLETNIH DRUŽBENIH OMREŽIJ – PRIMER FACEBOOKA

Za primer smo izbrali Facebook, ker se nam zdi, da ima izmed vseh spletnih družbenih omrežij največ uporabnikov in ker ga uporabljamo sami. Zato se nam je zdelo primerno, da predstavimo v nadaljevanju nekaj varnostih nasvetov, ki bi jih moral poznati prav vsak uporabnik Facebooka. Žal pa se nam zdi, da ni tako. Res je, da je Facebook še vedno brezplačen, ampak vseeno na njem trgujemo z valuto, ki je v današnjem času izredno dragocena, in to so naši osebni podatki. Če svojega profila ne zavaruješ z ustreznimi ukrepi, boš omogočil dostop do svojega življenja tudi popolnim neznancem. Preveč odprt profil lahko negativno vpliva na našo poklicno kariero in, kar je najpomembnejše, izpostavil boš svoje osebne podatke morebitnim spletnim storilcem kaznivih dejanj. Sodobnim zaposlovalcem je v navado prešlo preverjanje spletne dejavnosti potencialnih kandidatov za zaposlitev. Zelo pogosto se zgodi, da za določeno delovno mesto sicer zelo primernega in ustreznega kandidata zavrnejo na podlagi neprimerne dejavnosti na Facebooku in nasploh na vseh družbenih omrežjih. Tako v nadaljevanju dajemo nekaj nasvetov, ki so po našem mnenju pomembni za vsakega uporabnika. Ti pa so:

1. Prikažite minimalno količino svojih osebnih podatkov, kot so ime, priimek, datum rojstva. Tiste rubrike, katere ni potrebno izpolniti, pustite prazne ter nujno, če jih že navedete, obdržite vse svoje kontaktne podatke v zasebnosti.
2. Preglejte objave, v katerih ste označeni, še preden se pojavijo na vaši časovnici. To nastavitev si lahko uredite v kategoriji časovnica in oznake in obkljukate možnost, da pregledate vse objave, v katerih ste označeni, preden se pojavijo na vašem profilu.
3. Skrbno izberite, katero osebo boste sprejeli med svoje prijatelje.
4. Kako vaš profil vidijo vaši prijatelji ter kako ga vidi javnost? Preverite s to možnostjo, kako je vaš profil viden vsem ostalim, ki niso med vašimi prijatelji. V sliki je prikazano, kje najdemo to možnost.
5. Izberite raven zasebnosti vseh bodočih objav in omogočite, da so videne le vašim prijateljem.
6. Moja časovnica je moja, zato uredite nastavitve tako, da na vašo časovnico lahko pišete le vi in vaši prijatelji. Tu pa se lahko stopi še korak dlje in v primeru, če želite popoln nadzor, objavljanje onemogočite tudi vašim prijateljem.

Slika 2: Prikaz varnostnih nastavitev na Facebooku, ki jih priporočamo

Nastavitve za časovnico in označevanje

Kdo lahko dodaja stvari na mojo časovnico?	Kdo lahko objavlja na tvojo časovnico?	Samo jaz	Uredi
	Preglej objave, v katerih so te prijatelji označili, preden se pojavijo na tvoji časovnici	Vključeno	Uredi
Kdo lahko vidi stvari na moji časovnici?	Preveri, kaj lahko drugi ljudje vidijo na tvoji časovnici		Poglej kot
	Kdo lahko vidi objave, v katerih si bil označen, na tvoji časovnici?	Prijatelji	Uredi
	Kdo lahko vidi objave tvojih prijateljev na tvoji časovnici?	Prijatelji	Uredi
Kako lahko upravljam z oznakami, ki jih dodajo drugi ljudje, in predlogi za oznake?	Želiš pregledati oznake, ki jih drugi ljudje dodajo tvojim objavam, preden se oznake pojavijo na Facebooku?	Vključeno	Uredi
	Koga želiš dodati med občinstvo, ki še predhodno ni bil vključen, če te nekdo označi v objavi?	Prijatelji	Uredi
	Komu so vidne predlagane oznake, ko nekdo naloži sliko, na kateri kaže, da si ti? (zate to ni na voljo)	Ni na voljo	

Vir: lasten

7. Onemogočite možnost, da se drugi iskalniki povežejo z vašo časovnico.
8. Vklopite varnostno kodo - Obvestila o neznanih prijavah v račun.
9. Zaščitite svoje albume in s tem tudi svoje fotografije. Vse omogočite le tako, da bodo vidne le vam in vašim prijateljem.
10. Zadnja stvar, ki jo priporočamo, je, da sami pri sebi ocenite, kaj sploh je za v javnost in kaj spada v vašo zasebnost. Vse stvari le niso za na Facebook.

Spoštujmo zasebnost drugih ter premislimo, kakšen vpliv imajo naše objave na druge, pa če so označeni v njih ali ne.

6 EMPIRIČNA RAZISKAVA

6.1 SPLOŠNE ZNAČILNOSTI RAZISKAVE

Cilj empirične raziskave je bil, da raziščemo raven zavedanja na področju varstva osebnih podatkov pri uporabi spletnih družbenih omrežij. Izdelali smo anketni vprašalnik, ki je sestavljen iz dvajsetih vprašanj, vključno z demografskimi podatki, odprtega in zaprtega tipa. Anketni vprašalnik je razdeljen na pet sklopov, in sicer: demografski podatki, uporaba spletnih družbenih omrežij, odnos do osebnih podatkov in varnostne nastavitve, zloraba osebnih podatkov ter poznavanje zakonodaje. Ta nam je pomagal zavrniti oz. potrditi štiri zastavljene hipoteze, ki so sledeče:

- Večina anketirancev uporablja več kot eno spletno družbeno omrežje ter je na njih tudi zelo aktivna.
- Uporabniki spletnih družbenih omrežij svoje osebne podatke delijo z mnogimi drugimi uporabniki ter v različnih družbenih omrežjih v različni meri posvečajo svojo pozornost varnostnim nastavitvam.
- Večina uporabnikov še ni bila soočena z zlorabo osebnih podatkov in misli, da njihovi podatki niso dovolj zanimivi, da bi lahko postali predmet zlorabe.
- Uporabniki ne vedo, kako je varstvo osebnih podatkov v slovenski zakonodaji urejeno, ne poznajo Zakona o varstvu osebnih podatkov in v primeru zlorabe njihovih osebnih podatkov ne vedo, kaj bi storili.

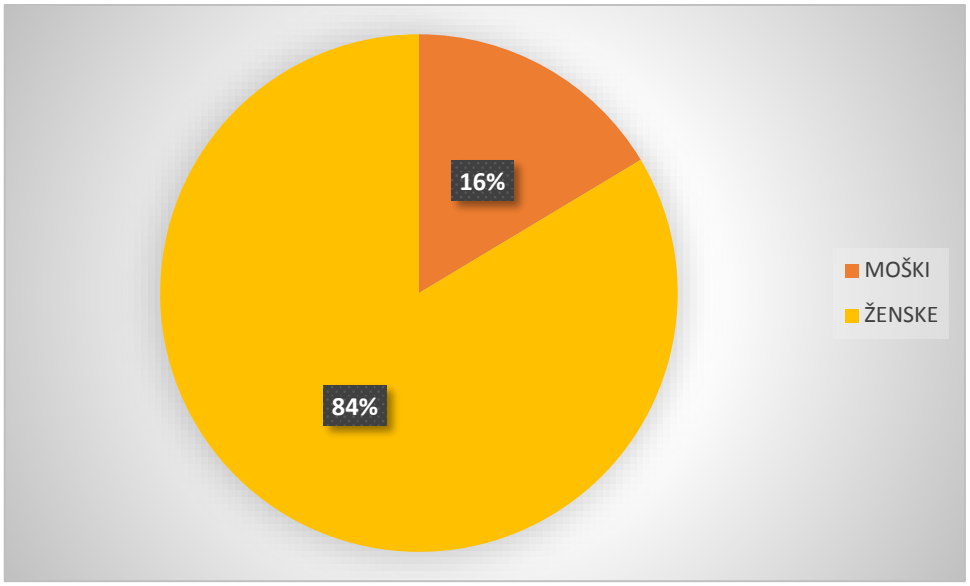
Anketni vprašalnik (Priloga 1) smo pretvorili v elektronsko obliko in s pomočjo spletne strani 1KA prišli do izpolnjenih anket, ki so jih izpolnili naključni uporabniki med našimi prijatelji na Facebooku. Anketo je izpolnilo 141 uporabnikov, vendar je bilo 19 anket le delno rešenih, zato bomo v svojo analizo vključili 122 ustrezno in v celoti izpolnjenih anket. Anketiranje smo izvajali od 10. maja 2016 do vključno 13. maja 2016.

6.2 DEMOGRAFSKI PODATKI

V anketnem vprašalniku smo zastavili 3 vprašanja, ki so se navezovala na demografske podatke, in sicer smo anketirance vprašali po spolu, starosti in doseženi izobrazbi.

K izpolnjevanju ankete smo povabili tako ženske kot moške. V večini so se na našo anketo odzvale ženske. Na anketo je tako odgovarjalo 20 moških (16 %) ter 102 ženski (84 %).

Slika 3: Spol anketirancev



Vir: lasten

Drugo vprašanje demografskega tipa se je navezovalo na starost anketirancev. Iz tabele 1 lahko razberemo, da je bil najmlajši, ki je izpolnil anketo, star 12 let, najstarejši pa je imel 70 let.

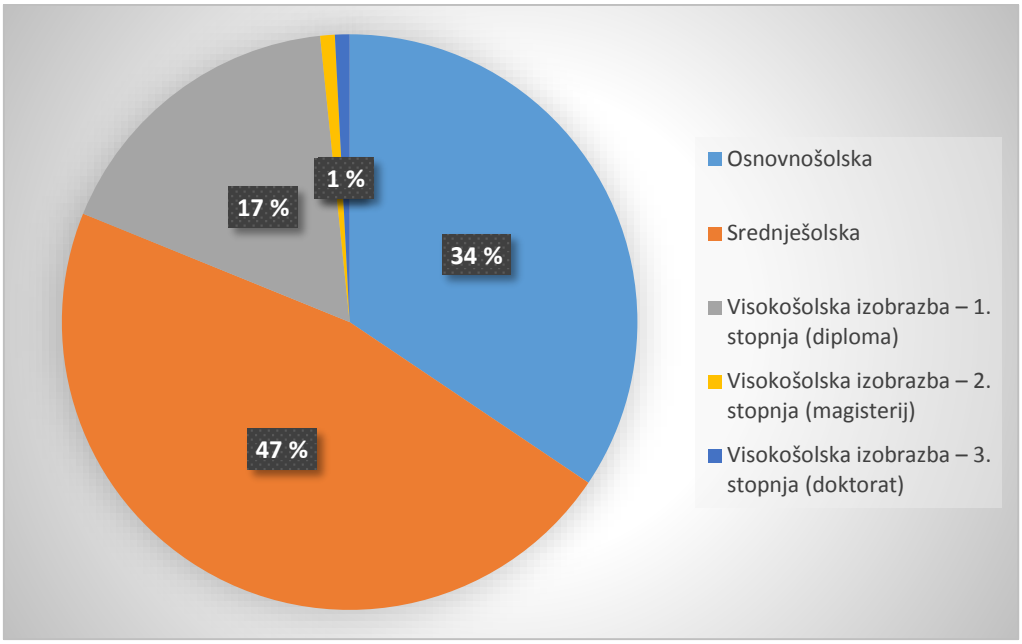
Tabela 1: Tabela anketirancev po starostnih skupinah

STAROSTNA SKUPINA	ŠTEVILO ANKETIRANCEV
12-22	70
23-32	38
33-42	7
43-52	3
53-62	3
63-70	1
SKUPAJ:	**122**

Vir: lasten

Za tretje vprašanje pa smo anketirance spraševali še po njihovi doseženi izobrazbi. To kategorijo smo razdelili v 5 skupin, in sicer: osnovnošolska, srednješolska, visokošolska izobrazba – 1. stopnja (diploma), visokošolska izobrazba – 2. stopnja (magisterij) in visokošolska izobrazba – 3. stopnja (doktorat).

Slika 4: Izobrazbena struktura anketirancev



Vir: lasten

6.3 ANALIZA IN INTERPRETACIJA REZULTATOV ANKETNEGA VPRAŠALNIKA

Pri analizi in interpretaciji rezultatov se bomo lotili obdelave po vsakemu vprašanju posebej.

1. **Napišite imena spletnih družbenih omrežij, ki jih poznate, tudi če nimate na njih svojega profila (npr. Facebook, Instagram, Snapchat itd.).**

Pri prvem vprašanju smo pričeli z odprtim tipom, ker nas je zanimalo, kaj vse anketiranci pojmujejo kot spletna družbena omrežja. Za najpogostejša spletna družbena omrežja, ki jih anketirani poznajo, lahko izpostavimo Facebook, Instagram, Twitter, Snapchat, Viber ter Youtube. Nekateri anketiranci smatrajo za družbena omrežja tudi Gmail, Google + in Endomondo, med odgovori se je enkrat pojavil 24ur. Izjeme, ki bi jih tudi želeli izpostaviti, pa so sledeča spletna družbena omrežja, ki so večini, predvidevamo, nepoznana, ker so se pojavila samo po enkrat: Hi5, Pinterest, We heart it, Tinder, Tumblr, Whatsapp, Ask.fm, Musical.ly, Flickr, Yohoo ter 9gag.

2. **Na kolikih imate profil oziroma aktiven račun? (vpišite število)**

Maksimalno število aktivnih računov oziroma profilov je 10 profilov oz. aktivnih računov, večina pa nam je odgovorila, da jih ima na treh omrežjih. Takoj za tremi pa se je zvrstilo še število 4 in 5. Manj kot tri profile oziroma aktivne račune pa ima 38 anketiranih, kar znaša 31 % od vseh.

3. **Kako pogosto uporabljate spodaj našteta omrežja.**

Anketirance smo vprašali, kako pogosto uporabljajo pet omenjenih spletnih družbenih omrežij, katera smo opisali v teoretičnem delu diplomskega dela. Iz tabel 2, 3, 4, 5 in 6

lahko torej vidimo, koliko anketirancev jih uporablja ter kako pogosto. Ponudili pa smo jim tudi možnost drugo, če bi sami želeli vpisati še katero drugo omrežje, ki ni bilo navedeno med odgovori.

Tabela 2: Uporaba Facebooka

	FREKVENCA	ODSTOTEK	KUMULATIVA FREKVENC
Vsakodnevno	118	97 %	118
Nekajkrat na teden	3	2 %	121
Nekajkrat na mesec	0	0 %	121
Zelo redko	0	0 %	121
Ne uporabljam	1	1 %	122
SKUPAJ:	**N = 122**	**100 %**	

Vir: lasten

Tabela 3: Uporaba Twitterja

	FREKVENCA	ODSTOTEK	KUMULATIVA FREKVENC
Vsakodnevno	9	7 %	9
Nekajkrat na teden	6	5 %	15
Nekajkrat na mesec	3	2 %	18
Zelo redko	12	10 %	30
Ne uporabljam	92	76 %	122
SKUPAJ:	**N = 122**	**100%**	

Vir: lasten

Tabela 4: Uporaba LinkedIna

	FREKVENCA	ODSTOTEK	KUMULATIVA FREKVENC
Vsakodnevno	0	0 %	0
Nekajkrat na teden	0	0 %	0
Nekajkrat na mesec	0	0 %	0
Zelo redko	6	5 %	6
Ne uporabljam	116	95 %	122
SKUPAJ:	**N = 122**	**100 %**	

Vir: lasten

Tabela 5: Uporaba Youtuba

	FREKVENCA	ODSTOTEK	KUMULATIVA FREKVENC
Vsakodnevno	70	57 %	70
Nekajkrat na teden	32	26 %	102
Nekajkrat na mesec	8	7 %	110
Zelo redko	3	2 %	113
Ne uporabljam	9	8 %	122
SKUPAJ:	**N = 122**	**100 %**	

Vir: lasten

Tabela 6: Uporaba Myspacea

	FREKVENCA	ODSTOTEK	KUMULATIVA FREKVENC
Vsakodnevno	0	0 %	0
Nekajkrat na teden	1	1 %	1
Nekajkrat na mesec	0	0 %	1
Zelo redko	2	2 %	3
Ne uporabljam	119	97 %	122
SKUPAJ:	**N = 122**	**100 %**	

Vir: lasten

DRUGO:

Pod drugo je 84 anketirancev navedlo še nekaj drugih, ki jih uporabljajo, in sicer so navedli: Instagram, Snapchat, Tumblr, Endomondo ter Viber. Kar 57 izmed njih je odgovorilo, da jih uporabljajo vsakodnevno.

4. Prosim, če v spodnji tabeli označite, kako pogosto izvajate določene aktivnosti na spletnih družbenih omrežjih.

Zanimalo nas je, kako zelo aktivni so anketiranci na svojih profilih oziroma aktivnih računih. Odgovorili (glej tabelo 7) pa so v sledečih številkah.

Tabela 7: Izvajanje določenih aktivnosti na spletnih družbenih omrežjih

	Vsakodnevno	Nekajkrat na teden	Nekajkrat na mesec	Zelo redko	Nikoli	SKUPAJ
Všečkam	86 (71 %)	27 (22 %)	6 (5 %)	3 (2 %)	0 (0 %)	122 (100 %)
Objavljam svoje fotografije/ video = posnetke	4 (3 %)	16 (13 %)	44 (37 %)	55 (45 %)	3 (2 %)	122 (100 %)
Komentiram objave drugih	20 (16 %)	37 (30 %)	28 (23 %)	31 (26 %)	6 (5 %)	122 (100 %)
Izražam svoje mnenje glede aktualnega dogajanja	6 (5 %)	9 (7 %)	19 (16 %)	55 (45 %)	33 (27 %)	122 (100 %)
Objavljam povezave	4 (3 %)	19 (16 %)	27 (22 %)	51 (42 %)	21 (17 %)	122 (100 %)
Objavljam podatke na svojem statusu: kaj delam, kje sem, kam grem itd.	1 (1 %)	6 (5 %)	8 (7 %)	53 (43 %)	54 (44 %)	122 (100 %)

Vir: lasten

5. Preden ste si ustvarili profil na kateremkoli spletnem družbenem omrežju, ste si prebrali splošne pogoje uporabe?

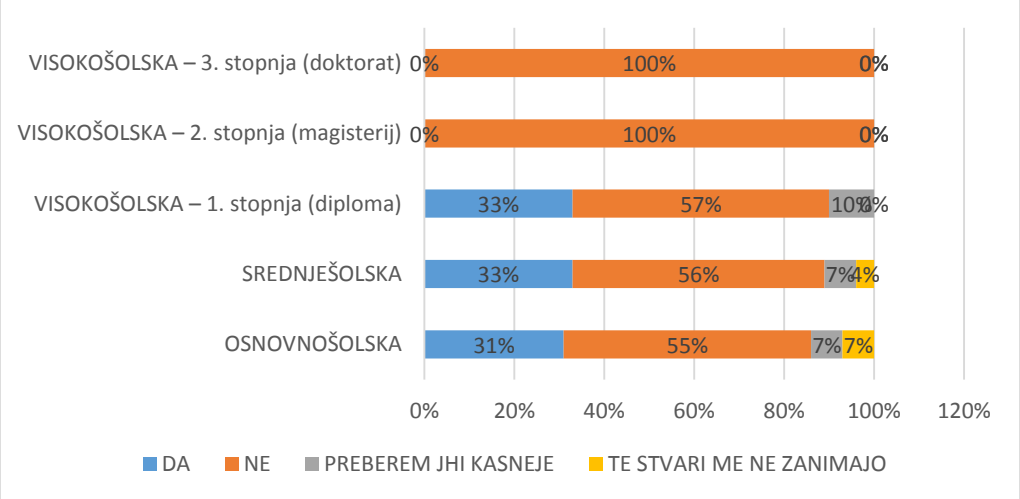
Rezultate bomo primerjali po izobrazbeni strukturi. V tabeli 8 lahko vidimo, kako si je določena izobrazbena struktura prebrala splošne pogoje uporabe, preden si je ustvarila profil na kateremkoli omrežju.

Tabela 8: Preden ste si ustvarili profil na kateremkoli spletnem družbenem omrežju, ste si prebrali splošne pogoje uporabe?

	DA	NE	PREBEREM JIH KASNEJE	TE STVARI ME NE ZANIMAJO	SKUPAJ:
OSNOVNOŠOLSKA	13 (31 %)	23 (55 %)	3 (7 %)	3 (7 %)	42 (100 %)
SREDNJEŠOLSKA	19 (33 %)	32 (56 %)	4 (7 %)	2 (4 %)	57 (100 %)
VISOKOŠOLSKA – 1. stopnja (diploma)	7 (33 %)	12 (57 %)	2 (10 %)	0 (0 %)	21 (100 %)
VISOKOŠOLSKA – 2. stopnja (magisterij)	0 (0 %)	1 (100 %)	0 (0 %)	0 (0 %)	1 (100 %)
VISOKOŠOLSKA – 3. stopnja (doktorat)	0 (0 %)	1 (100 %)	0 (0 %)	0 (0 %)	1 (100 %)

Vir: lasten

Slika 5: Preden ste si ustvarili profil na kateremkoli spletnem družbenem omrežju, ste si prebrali splošne pogoje uporabe?



Vir: lasten, tabela 8

6. **Osredotočimo se samo na Facebook (lahko tudi na drugo spletno družbeno omrežje, če slučajno niste tukaj registrirani) in mi, prosim, v spodnji tabeli označite, kako so vaši osebni podatki vidni ostalim uporabnikom.**

Anketirancem smo ponudili nekaj možnih odgovorov oziroma tipov osebnih podatkov in za vsakega posebej so morali označiti, kako je viden ostalim uporabnikom spletnih družbenih omrežij. Glede resničnosti podatkov, vsaj glede imena in priimka in še nekaj drugih, lahko tukaj smatramo, da imajo objavljene (če jih imajo) resnične osebne podatke, saj so bili anketiranci izbrani med našimi prijatelji na Facebooku, med katerimi imamo tudi mi samo tiste, ki jih poznamo. V tabeli 9 lahko tako vidimo rezultate tega vprašanja.

Tabela 9: Prikaz osebnih podatkov drugim uporabnikom

	Nastavljeno kot skrito (vidim samo jaz)	Vidno vsem	Vidno mojim prijateljem	Ne vem	Tega podatka nimam objavljenega	SKUPAJ
Ime in priimek	11 (9 %)	81 (66 %)	28 (23 %)	0 (0 %)	2 (2 %)	122 (100 %)
Naslov prebivališča	18 (15 %)	3 (2 %)	17 (14 %)	8 (7 %)	76 (62 %)	122 (100 %)
Elektronski naslov	30 (25 %)	28 (23 %)	42 (34 %)	12 (9 %)	10 (9 %)	122 (100 %)
Telefonska številka	33 (27 %)	3 (3 %)	8 (6 %)	5 (4 %)	73 (60 %)	122 (100 %)
Delovno mesto	13 (11 %)	64 (52 %)	18 (15 %)	2 (2 %)	25 (20 %)	122 (100 %)
Izobraževanje	6 (5 %)	62 (51 %)	36 (29 %)	3 (3 %)	15 (12 %)	122 (100 %)
Datum rojstva	11 (9 %)	66 (54 %)	31 (25 %)	6 (5 %)	8 (7 %)	122 (100 %)
Kraj bivanja	13 (11 %)	75 (61 %)	10 (9 %)	4 (3 %)	20 (16 %)	122 (100 %)

Vir: lasten

Pod drugo pa je še 8 anketirancev dodalo svoje odgovore, kot so profilna slika, status ter svoje razmerje oziroma partner, katere imajo v večini prikazane samo svojim prijateljem.

7. **Označite, koliko pozornosti posvečate varnostnim vidikom pri uporabi naštetih družbenih omrežjih.**

Zanimalo nas je, koliko pozornosti usmerjajo uporabniki v spodaj naštetih (istih, kot že pri prejšnjih vprašanjih) spletnih družbenih omrežjih v varnostne nastavitve. Rezultati, ki jih prikazuje tabela 10, so naslednji:

Tabela 10: Posvečanje pozornosti varnostnim vidikom

	Nič	Srednje	Veliko	Ne uporabljam	**SKUPAJ**
FACEBOOK	8 (6 %)	60 (49 %)	53 (44 %)	1 (1 %)	122 (100 %)
TWITTER	18 (15 %)	10 (8 %)	2 (2 %)	92 (75 %)	122 (100 %)
LINKEDIN	4 (3 %)	2 (2 %)	0 (0 %)	116 (95 %)	122 (100 %)
YOUTUBE	33 (27 %)	59 (48 %)	21 (18 %)	9 (7 %)	122 (100 %)
MYSPACE	2 (2 %)	0 (0 %)	1 (1 %)	119 (97 %)	122 (100 %)

Vir: lasten

Tudi tu smo ponudili možnost drugo in od 24 anketirancev dobili še tri spletna družbena omrežja Instagram, Snapchat ter Tumblr. Njihovi odgovori so se v večini uvrstili v kategorijo srednje.

8. Kako pomembna vam je zasebnost vaših osebnih podatkov, ki jih imate na spletnih družbenih omrežjih?

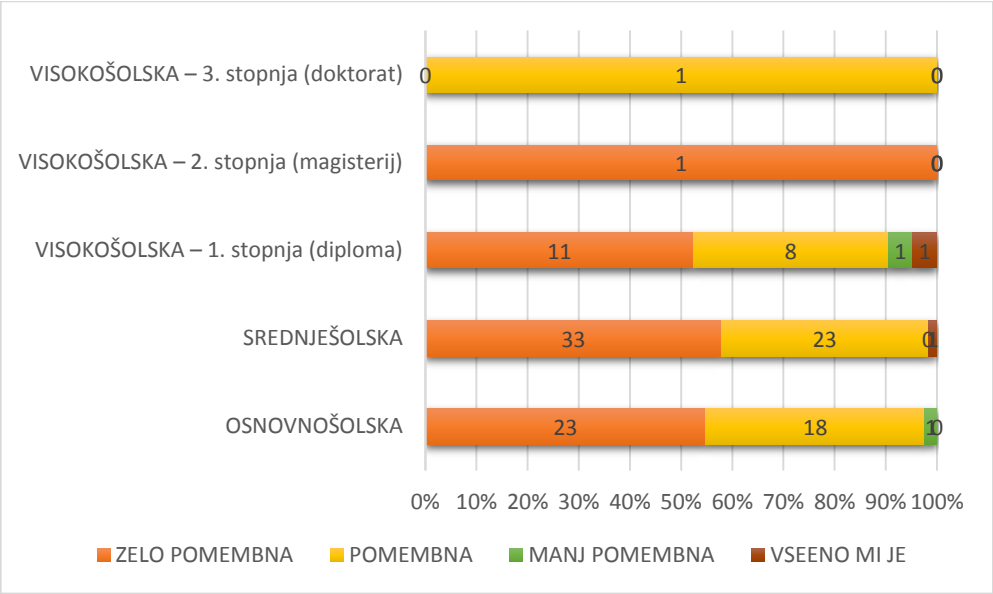
Vprašanje smo spet analizirali po izobrazbeni strukturi. Zanimalo nas je, koliko jim je pomembna zasebnost njihovih osebnih podatkov, ki jih imajo razkrite v spletnih družbenih omrežjih. Tabela 11 tako prikazuje naslednje rezultate.

Tabela 11: Kako pomembna vam je zasebnost vaših osebnih podatkov, ki jih imate na spletnih družbenih omrežjih?

	ZELO POMEMBNA	POMEMBNA	MANJ POMEMBNA	VSEENO MI JE	SKUPAJ
OSNOVNOŠOLSKA	23 (55 %)	18 (43 %)	1 (2 %)	0 (0 %)	42 (100 %)
SREDNJEŠOLSKA	33 (58 %)	23 (40 %)	0 (0 %)	1 (2 %)	57 (100 %)
VISOKOŠOLSKA – 1. stopnja (diploma)	11 (52 %)	8 (38 %)	1 (5 %)	1 (5 %)	21 (100 %)
VISOKOŠOLSKA – 2. stopnja (magisterij)	1 (100 %)	0 (0 %)	0 (0 %)	0 (0 %)	1 (100 %)
VISOKOŠOLSKA – 3. stopnja (doktorat)	0 (0 %)	1 (100 %)	0 (0 %)	0 (0 %)	1 (100 %)

Vir: lasten

Slika 6: Kako pomembna vam je zasebnost vaših osebnih podatkov, ki jih imate na spletnih družbenih omrežjih?



Vir: lasten, tabela 11

9. Ali ste bili že kdaj soočeni z zlorabo vaših osebnih podatkov (za primer, se vam je že kdaj zgodilo, da so vam ukradli vašo identiteto)?

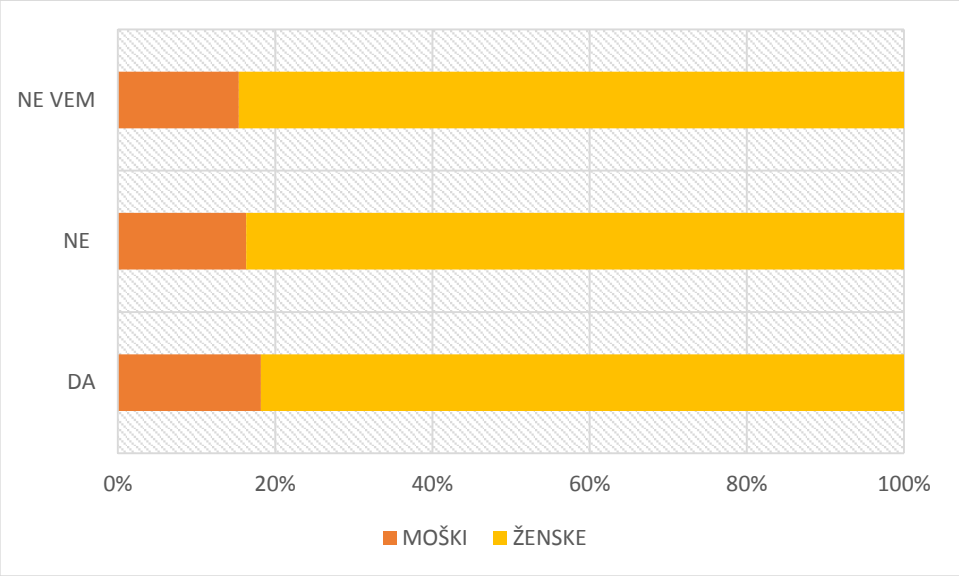
Iz tabele 12 lahko vidimo, da jih večina izmed žensk in moških še ni bila soočena z zlorabo osebnih podatkov.

Tabela 12: Ali ste bili že kdaj soočeni z zlorabo vaših osebnih podatkov?

	DA	NE	NE VEM	SKUPAJ:
MOŠKI	2 (10 %)	16 (80 %)	2 (10 %)	20 (100 %)
ŽENSKE	9 (9 %)	82 (80 %)	11 (11 %)	102 (100 %)

Vir: lasten

Slika 7: Ali ste bili že kdaj soočeni z zlorabo vaših osebnih podatkov?



Vir: lasten, tabela 12

10. Kako verjetno se vam zdi, da vaši osebni podatki v prihodnosti postanejo predmet zlorabe? (označite na lestvici od 1 do 5)

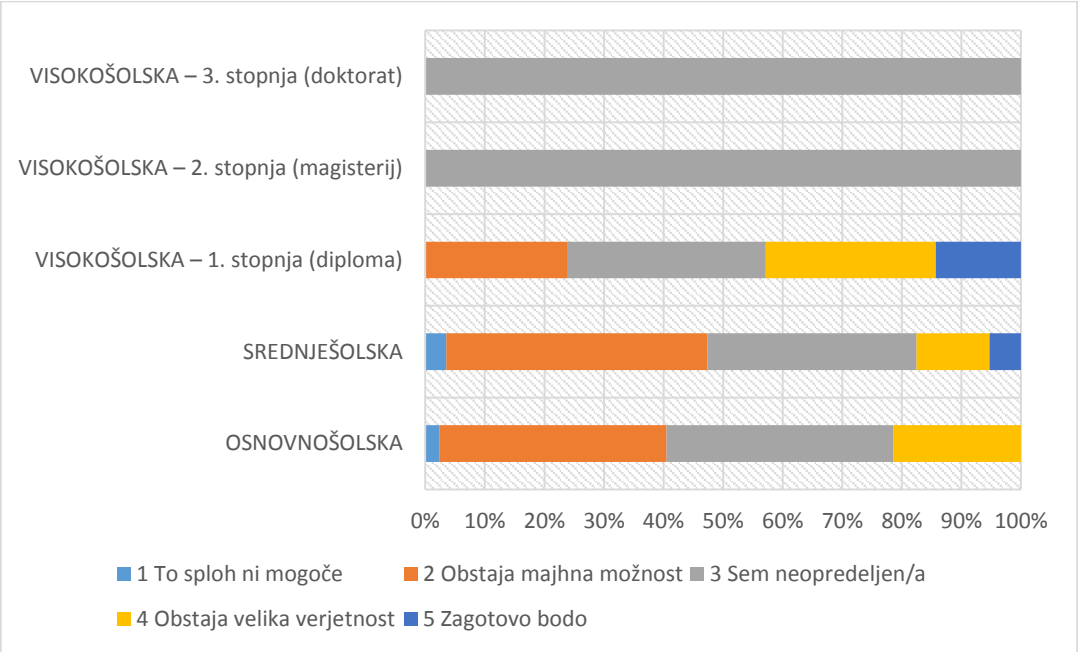
Anketirance, ki smo jih spet razdelili po izobrazbeni strukturi, smo spraševali po verjetnosti, koliko mislijo, da je možnosti, da njihovi osebni podatki v prihodnosti postanejo predmet zlorabe. Rezultati so prikazani v tabeli 13.

Tabela 13: Kako verjetno se vam zdi, da vaši osebni podatki v prihodnosti postanejo predmet zlorabe?

	1 To sploh ni mogoče	2 Obstaja majhna možnost	3 Sem neopre = deljen/a	4 Obstaja velika verjetnost	5 Zagotovo bodo	SKUPAJ:
Osnovnošolska	1 (2 %)	16 (38 %)	16 (38 %)	9 (22 %)	0 (0 %)	42 (100 %)
Srednješolska	2 (3 %)	25 (44 %)	20 (35 %)	7 (13 %)	3 (5 %)	57 (100 %)
Visokošolska – 1. Stopnja (diploma)	0 (0 %)	5 (24 %)	7 (33 %)	6 (29 %)	3 (14 %)	21 (100 %)
Visokošolska – 2. Stopnja (magisterij)	0 (0 %)	0 (0 %)	1 (100 %)	0 (0 %)	0 (0 %)	1 (100 %)
Visokošolska – 3. Stopnja (doktorat)	0 (0 %)	0 (0 %)	1 (100 %)	0 (0 %)	0 (0 %)	1 (100 %)

Vir: lasten

Slika 8: Kako verjetno se vam zdi, da vaši osebni podatki v prihodnosti postanejo predmet zlorabe?



Vir: lasten, tabela 13

11. Ne glede na to, kako ste pri prejšnjem vprašanju izbrali verjetnost, me zanima razlog, zakaj tako mislite.

Najprej bomo pogledali razloge verjetnosti od 1 do 3, kjer se odgovori gibljejo od ni mogoče do sem neopredeljen/a, za kar se je opredelilo kar 77 % vseh anketirancev. Izpostavili bomo nekaj razlogov, ki so se nam zdeli zanimivi: nisem zanimiva za širšo javnost, nisem zvezda, ker nobeden ne bi hotel tega narediti, ker dvomim, da bom kdaj tarča kakšne hujše zlorabe, ker so podatki dobro zaščiteni z različnimi varnostmi programi, ki so na določeni spletni strani. Nekaj jih je odgovorilo v tem smislu, da nikoli ne veš, kaj se lahko zgodi. Potem pa imamo na drugi strani verjetnost 4 in 5, na katere so anketiranci odgovorili v primeru, če so skoraj prepričani, da bodo postali žrtev zlorabe osebnih podatkov. Teh je 23 % in njihovi razlogi so sledeči: oseba, ki bi mi močno hotela zagreniti življenje, bi naredila vse, da bi to dosegla, ker smo tako napredni s tehnologijo, da bo v prihodnosti lahko kdorkoli prevzel naše podatke, najbolj zanimiv pa je bil odgovor: ker so podatki lahko dostopni in omrežja nezavarovana pred vsemi in sami posredujemo podatke na omrežje, tako da ljudem sploh ni potrebno vdirati, ampak samo pogledajo profil.

12. Ali mislite, da imamo varstvo osebnih podatkov v Sloveniji urejeno s pravnimi akti?

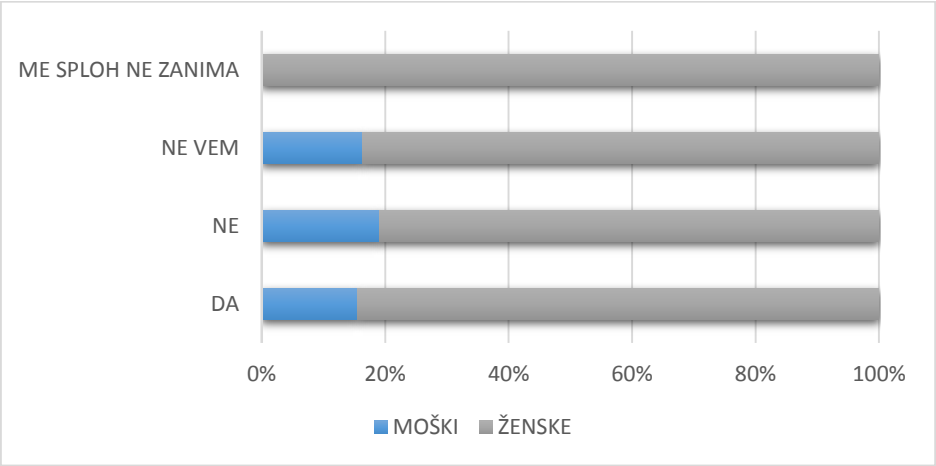
Naše vprašanje se je navezalo na poznavanje pravne urejenosti področja varstva osebnih podatkov v Sloveniji. Iz tabele 14 lahko vidimo, da so tako moški kot tudi ženske v največjem odzivu odgovorili z ne vem.

Tabela 14: Ali mislite, da imamo varstvo osebnih podatkov v Sloveniji urejeno s pravnimi akti?

	DA	NE	NE VEM	ME SPLOH NE ZANIMA	SKUPAJ:
MOŠKI	7 (35 %)	4 (20 %)	9 (45 %)	0 (0 %)	20 (100 %)
ŽENSKE	38 (37 %)	17 (17 %)	46 (45 %)	1 (1 %)	102 (100 %)

Vir: lasten

Slika 9: Ali mislite, da imamo varstvo osebnih podatkov v Sloveniji urejeno s pravnimi akti?



Vir: lasten, tabela 14

13. Za kateri zakon mogoče mislite ali ste že slišali, da ureja področje varstva osebnih podatkov?

Od vseh anketiranih jih je samo 11 napisalo Zakon o varstvu osebnih podatkov, 9 jih je napisalo ZVOP, kar pomeni, da jih od 122 anketiranih samo 20 pozna Zakon o varstvu osebnih podatkov. Večina je napisala, da še ni slišala zanj in da ga ne pozna.

14. Na koga bi se obrnili, če bi bili vaši osebni podatki zlorabljeni?

Pri tem vprašanju jih je večina napisala, da bi se obrnila na policijo, nekaj tudi na informacijskega pooblaščenca ter varuha človekovih pravic, nekaj pa na administratorje spletnih strani ter na starše. Bilo pa je tudi nekaj primerov, da bi poiskali pomoč pri psihologu ali odvetniku.

15. Prosim, če mi na lestvici od 1 do 5 označite, kako pogosto prebirate priročnike in smernice varne uporabe spleta (npr. od informacijskega pooblaščenca, varuha človekovih pravic ...).

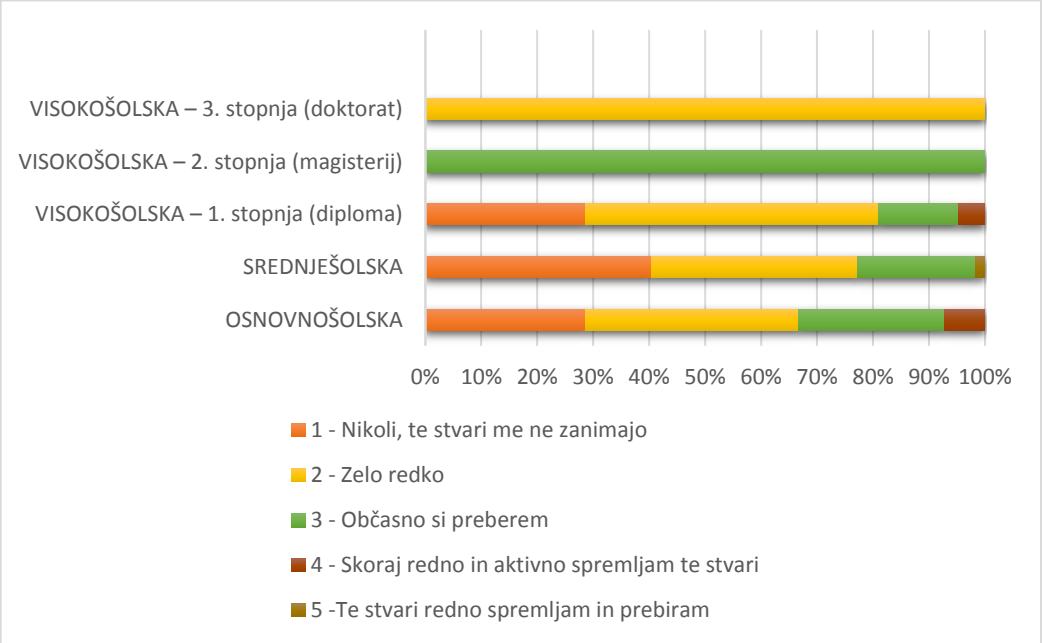
Iz tabele 15 lahko vidimo, da jih zelo malo redno spremlja in prebira priročnike ter smernice varne uporabe spleta. 90 izmed vseh anketirancev jih je na to vprašanje odgovorilo z 1 in 2, kar pomeni, da jih več kot polovica te stvari spremlja ali zelo redko ali pa jih to ne zanima.

Tabela 15: Branje in spremljanje priročnikov in smernic varne uporabe spleta

	1 - Nikoli, te stvari me ne zanimajo	2 - Zelo redko	3 - Občasno si preberem	4 - Skoraj redno in aktivno spremljam te stvari	5 -Te stvari redno spremljam in prebiram	SKUPAJ:
Osnovnošolska	12 (29 %)	16 (38 %)	11 (26 %)	3 (7 %)	0 (0 %)	42 (100 %)
Srednješolska	23 (40 %)	21 (37 %)	12 (21 %)	0 (0 %)	1 (2 %)	57 (100 %)
Visokošolska – 1. Stopnja (diploma)	6 (29 %)	11 (52 %)	3 (14 %)	1 (5 %)	0 (0 %)	21 (100 %)
Visokošolska – 2. Stopnja (magisterij)	0 (0 %)	0 (0 %)	1 (100 %)	0 (0 %)	0 (0 %)	1 (100 %)
Visokošolska – 3. Stopnja (doktorat)	0 (0 %)	1 (100 %)	0 (0 %)	0 (0 %)	0 (0 %)	1 (100 %)

Vir: lasten

Slika 10: Branje in spremljanje priročnikov in smernic varne uporabe spleta po izobrazbeni strukturi



Vir: lasten, tabela 15

16. Bi si želeli vedeti več o nevarnostih, ki vam jih prinašajo spletna družbena omrežja, in kako se zaščiti pred njimi ter kaj bi morali storiti v primeru, ko so vaši osebni podatki že zlorabljeni?

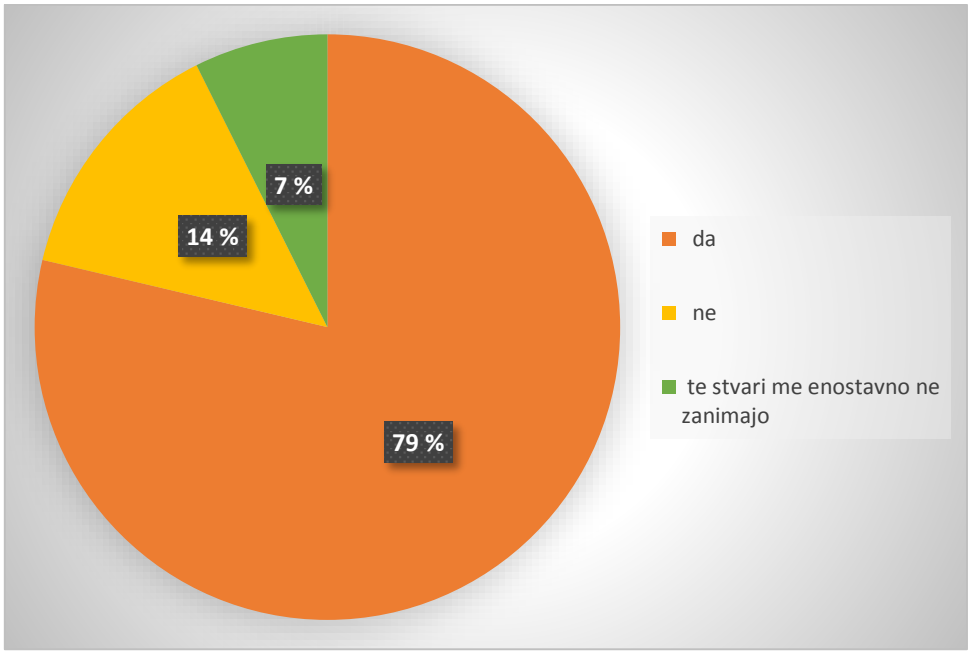
96 anketirancev je odgovorilo, da bi si želeli več vedeti o samih nevarnostih, ki jih prinašajo spletna družbena omrežja, in kako se zaščiti pred njimi ter kaj bi morali storiti v primeru, ko so njihovi osebni podatki že zlorabljeni.

Tabela 16: Bi si želeli vedeti več o nevarnostih, ki vam jih prinašajo spletna družbena omrežja, in kako se zaščiti pred njimi ter kaj bi morali storiti v primeru, ko so vaši osebni podatki že zlorabljeni?

ODGOVORI	FREKVENCA	ODSTOTEK	KUMULATIVA FREKVENC
DA	96	79 %	96
NE	17	14 %	113
TE STVARI ME ENOSTAVNO NE ZANIMAJO	9	7 %	122
SKUPAJ	122	100 %	

Vir: lasten

Slika 11: Bi si želeli vedeti več o nevarnostih, ki vam jih prinašajo spletna družbena omrežja, in kako se zaščiti pred njimi ter kaj bi morali storiti v primeru, ko so vaši osebni podatki že zlorabljeni?



Vir: lasten, tabela 16

17. Podajte mi predlog, kako bi vam to najbolj ustrezalo, da se izvede.

Večina anketiranih je podala svoje predloge, nekaj jih tudi ni, ker to vprašanje ni bilo nastavljeno kot obvezno. Izpostavili pa so predloge, kot so recimo preko interneta ali predavanj po osnovnih in srednjih šolah, oglaševanja (reklame na televiziji), na samih družbenih omrežjih, tečajih, v brošurah, preko člankov ter elektronske pošte.

IZVEDBA T-TESTA

Kot dodatno nalogo pri analizi anketnega vprašalnika smo si zadali še izvedbo t-testa. Primerjali bomo povprečji dveh skupin enot, se pravi dveh neodvisnih vzorcev. Za spremenljivko smo izbrali kraj bivanja pri vprašanju številka 6, ki je anketirance spraševal po tem, kako določene osebne podatke razkrivajo drugim uporabnikom. Kot dva neodvisna vzorca bomo vzeli skupini osnovnošolska izobrazba ter srednješolska izobrazba, ker imata obe skupini zadostno velikost vzorca (vsaj 30), da se izvede med njima t-test. Naši hipotezi se tako glasita:

Ničelna hipoteza: Pravi povprečji spremenljivke kraj bivanja za osnovnošolsko ter srednješolsko izobrazbo sta enaki.

Alternativna hipoteza: Pravi povprečji spremenljivke kraj bivanja za osnovnošolsko ter srednješolsko izobrazbo se razlikujeta.

Naša p-vrednost je bila večja od 0,05, zato ostanemo v prvi vrstici, pri ničelni hipotezi, ki jo potrdimo. Iz dobljene vrednosti tako vidimo, da je razlika med povprečjema premajhna, da bi jo bilo smiselno razglašati, in tako lahko rečemo, da pri običajnem 5 % tveganju anketiranci s srednješolsko ter osnovnošolsko izobrazbo v poprečju enako razkrivajo svoj kraj bivanja drugim.

6.4 PREVERJANJE HIPOTEZ

Hipoteza 1: Večina anketirancev uporablja več kot eno spletno družbeno omrežje ter je na njih tudi zelo aktivna.

Glede uporabe spletnih družbenih omrežij lahko prvi del hipoteze potrdimo, saj smo videli pri drugem vprašanju ankete, da večina uporablja tri spletna družbena omrežja. Kar se tiče uporabe le-teh, smo videli, da Facebook uporablja večina vsakodnevno, kar pa se tiče določenih aktivnosti, pa je odziv malce drugačen. Uporabniki všečkajo recimo vsak dan. Ko pa pogledamo objavljanje kakšnih fotografij in videoposnetkov, se večina uvrsti v zelo redko, zato lahko ta del hipoteze le delno potrdimo.

Hipoteza 2: Uporabniki spletnih družbenih omrežij svoje osebne podatke delijo z mnogimi drugimi uporabniki ter v različnih družbenih omrežjih v različni meri posvečajo svojo pozornost varnostnim nastavitvam.

Uporabnikom smo v anketi ponudili več osebnih podatkov, za katere pa se je izkazalo, da jih delijo v različni meri, glede na tip osebnega podatka. Recimo, če pogledamo naslov prebivališča in telefonska številka, sta to dva podatka, ki ju uporabniki skrivajo ali nimajo objavljenih. Kar se pa tiče imena in priimka, delovnega mesta, izobraževanja, datuma rojstva ter kraja bivanja, pa jih večina razkriva vsem. Ker je to več kot polovica osebnih

podatkov, lahko ta del potrdimo. Tudi drugi del hipoteze lahko potrdimo, ker lahko vidimo iz rezultatov, da na Facebooku večina posveča srednje ali veliko pozornosti, ko pa pogledamo Youtube, pa jih večina posveča pozornost pod nič ali pa srednje. Tudi za LinekdIn jih je večina dala nič.

Hipoteza 3: Večina uporabnikov še ni bila soočena z zlorabo osebnih podatkov in misli, da njihovi podatki niso dovolj zanimivi, da bi lahko postali predmet zlorabe.

Prvi del hipoteze lahko potrdimo, saj je večina oziroma kar 80 % odgovorila, da še niso bili soočeni z zlorabo osebnih podatkov. Kar se tiče drugega dela hipoteze, pa ga lahko po našem mnenju samo delno potrdimo, saj večina meni, da obstaja možnost, da se zlorabijo njihovi podatki ali pa so glede tega neopredeljeni.

Hipoteza 4: Uporabniki ne vedo, kako je varstvo osebnih podatkov v slovenski zakonodaji urejeno, ne poznajo Zakona o varstvu osebnih podatkov in v primeru zlorabe njihovih osebnih podatkov ne vedo, kaj bi storili.

Prvi del hipoteze lahko potrdimo, saj jih je kar 77 odgovorilo z ne, ne vem ali pa sploh, da ga ne zanima. Kar se tiče Zakona o varstvu osebnih podatkov, lahko tudi ta del potrdimo, saj smo iz rezultatov videli, da dejansko samo 20 anketiranih od 122 pozna zakon. Zadnji del hipoteze pa bi lahko zavrnili, saj bi v primeru zlorabe vsaj nekaj naredili, in sicer bi se obrnili na policijo, kar vseeno pomeni, da bi ukrepali.

7 ZAKLJUČEK

Varstvo osebnih podatkov je področje, ki vse bolj pridobiva na svojem pomenu, tako v svetovnem smislu kot tudi pri nas. Posameznik je vse bolj ogrožen, ker dandanes živimo v svetu, ki je prepleten z informacijsko tehnologijo. Zaradi njenega konstantnega napredka je tako posledično vse težje zagotavljati varstvo osebnih podatkov in preprečevati vdore v našo zasebnost. Na eni strani nam avtomatska obdelava podatkov olajša veliko dela, po drugi strani pa nam spet prinaša določene nevarnosti, sploh v primeru, če podatki pridejo v napačne roke, v roke nekoga, ki jih zlorabi.

Skozi diplomsko nalogo smo se spoznali s pojmom zasebnosti, ki ga je že od nekdaj zelo težko opredeliti z neko enotno definicijo. Vemo, da pravica do zasebnosti in pravica do varstva osebnih podatkov spadata med temeljne človekove pravice in osebne svoboščine, zato smo delček diplomske naloge namenili tudi temu. Spoznali smo se tudi s področjem varstva osebnih podatkov, predstavili smo tudi zgodovini obeh pojmov ter mednarodnopravno ureditev.

Z naše strani, se pravi s strani posameznikov, je zelo pomembno, da se zavedamo, da nas v Sloveniji ščiti zakonodaja, Zakon o varstvu osebnih podatkov in 38. člen Ustave RS, na podlagi katerih lahko zahtevamo varstvo naših pravic. Pomembno vlogo pa ima tudi informacijski pooblaščenec, pri katerem lahko vsak posameznik vloži prijavo, če misli, da so njegovi osebni podatki postali predmet zlorabe.

Lahko rečemo, da je zloraba osebnih podatkov na spletnih družbenih omrežjih postala nekakšen fenomen, katerega razsežnost je dosegla vse ljudi po svetu. Spletna družbena omrežja so v zadnjih letih postala zelo priljubljena, kar nam potrjuje čedalje večja številka njihovih uporabnikov. Lahko jih uporabljamo za različne namene, tako za marketinško oglaševanje kot recimo za ohranjanje stikov z drugimi. Seveda pa s povečevanjem števila uporabnikov raste tudi problem varstva osebnih podatkov, saj je potrebno za samo včlanitev v spletno družbeno omrežje navesti kar nekaj osebnih podatkov. V diplomski nalogi smo predstavili nekaj osnovnih značilnosti spletnih družbenih omrežij, vrste le-teh, njihove prednosti ter slabosti, kakšna je komunikacija znotraj njih ter predstavili nekaj najbolj priljubljenih.

Vsaka kršitev varstva osebnih podatkov je obravnavana kot kaznivo dejanje in mora biti z vidika kazensko procesnega prava tako kot vsa kazniva dejanja obravnavana enako, ne glede na dejstvo, kje je bilo to kaznivo dejanje storjeno, ali v resničnem ali virtualnem svetu. V diplomskem delu vidimo, da je nevarnosti za zlorabo osebnih podatkov zelo veliko. Mi smo jih nekaj predstavili in opisali, izpostavili pa smo tudi nekaj naših nasvetov glede same uporabe in delovanja na spletnih družbenih omrežjih.

S pridobljenim znanjem smo se tako lotili empirične raziskave, v kateri smo sestavili anketni vprašalnik, ki smo ga razdelili med naključne uporabnike spletnih omrežij v Sloveniji. Zastavili smo si štiri hipoteze, ki smo jih v večini potrdili. Anketni vprašalnik smo razposlali po Facebooku in nanj so se odzvali kar v precejšnem številu. Anketo smo razdelili

v pet sklopov, izmed katerih nam je vsak posebej pomagal potrditi ali zavrniti naše zastavljene hipoteze. Naš cilj, raziskati raven zavedanja na področju varstva osebnih podatkov pri uporabi spletnih družbenih omrežij, je bil tako dosežen. V večini nas dobljeni rezultati niso preveč presenetili, saj smo takšne rezultate nekako pričakovali. Mogoče nas je presenetilo samo to, da se anketiranci dejansko zavedajo, da v prihodnosti lahko postanejo žrtve zlorabe svojih osebnih podatkov, čeprav tudi ne v takšni meri, ki ne bi bila skrb vzbujajoča.

Za našo osnovno trditev, ki pravi, da posameznik ne ravna dovolj previdno s svojimi osebnimi podatki in da je raven poznavanja varstva osebnih podatkov zelo šibka, lahko na tej točki rečemo, da je v celoti potrjena. Uporabniki premalo cenijo svoje osebne podatke in jih v veliki meri delijo z mnogimi drugimi uporabniki, čeprav smo v anketi pokazali, da dejansko menijo, da obstaja neka mala možnost, da njihovi osebni podatki kdaj v prihodnosti postanejo predmet zlorabe. Velikokrat svoje podatke razkrivamo brez potrebe, kljub temu pa čutimo nek strah pred razkritjem le-teh. Po našem mnenju bo potrebno še veliko informiranja glede pomembnosti in nevarnosti ter zaščite naših osebnih podatkov nasploh, ne samo na spletnih družbenih omrežjih. Pojavilo se bo tudi vse več novosti v informacijski tehnologiji, katere nam bodo prinesle še večja tveganja za zlorabo osebnih podatkov, zato se nam zdi, da je vseeno izredno pomembna zlasti naša preudarnost, da bomo tako znali ločiti mejo med javnim in zasebnim. Potrebno bi bilo tudi osveščanje že med najmlajšimi, še preden pridejo v spletna okolja, in jih tako že pred samo uporabo spleta pričnemo opozarjati, kako določene stvari lahko prinesejo tudi veliko negativnih stvari in resnih posledic, ne samo zabave. Tudi neka določena mera skepticizma bi predstavljala za posameznika izjemno prednost, saj bi bili tako posledično manj naivni in ne bi nasedali prav vsem neumnostim tako na spletnih družbenih omrežjih kot tudi na celotnem spletu.

LITERATURA IN VIRI

Literatura:

- Cerar, M. (2004). *Temelji ustavne ureditve, človekove pravice in temeljne svoboščine, gospodarska in socialna razmerja*. Ljubljana: Ministrstvo za notranje zadeve, Direktorat za javno upravo, Upravna akademija.
- Čebulj, J. (1992). *Varstvo informacijske zasebnosti v Evropi in Sloveniji*. Ljubljana: Inštitut za javno upravo pri Pravni fakulteti.
- Čelebić, G., Ilija Rendulić, D. (2012). *ITdesk.info – načrtovanje računalniškega e-izobraževanja s prostim dostopom - Priročnik za digitalne pismenosti : osnovni pojmi informacijske in komunikacijske tehnologije*. Zagreb: Otvoreno društvo za razmjenu ideja (ODRAZI).
- Dimc, M., Dobovšek, B. (2012). *Kriminaliteta v informacijski družbi*. Ljubljana: Fakulteta za varnostne vede.
- Finžgar, A. (1985). *Osebnostne pravice = Die Persönlichkeitsrechte*. Ljubljana: Slovenska akademija znanosti in umetnosti.
- Hoffman, P. (1996). *Vse o Internetu & World Wide Webu*. Ljubljana: Pasadena.
- Hunt, L. (2015). *Iznajdevanje človekovih pravic*. Ljubljana: Znanstvena založba Filozofske fakultete.
- Kovačič, M. (2006). *Nadzor in zasebnost v informacijski družbi.* Ljubljana: Fakulteta za družbene vede.
- Kramar, B. (2013). *Varstvo osebnih podatkov v Sloveniji.* Diplomsko delo*.* Ljubljana: Ekonomska fakulteta.
- Lampe, R. (2004). *Sistem pravice do zasebnosti*. Ljubljana: Bonex založba.
- Lampe, R. (2010). *Pravo človekovih pravic: sistem človekovih pravic v mednarodnem, evropskem in ustavnem pravu.* Ljubljana: Formatisk.
- Pirc Musar, N., Prelesnik, M., Bien Karlovšek, S. (2006). *Predpisi s področja prava varstva osebnih podatkov in dostopa do informacij javnega značaja*. Ljubljana: GV Založba.
- Teršek, A. (2005). Svoboda izražanja in pravica do zasebnosti. Analiza in komentar sodbe ESČP v primeru Von Hannover proti Nemčiji. *Revus – Revija za evropsko ustavnost,* 4, str. 97–114.
- Thompson, J. B. (1995). *The media and modernity: a social theory of the media*. Stanford: Stanford University Press.
- Türk, D., Accetto, M., Cerar, M., Jamnikar, J., Smrkolj, M. (2002). *Dokumenti človekovih pravic z uvodnimi pojasnili.* Ljubljana: Društvo Amnesty International Slovenije, Mirovni inštitut.

Viri:

- (1989). Ustavni zakon za izvedbo ustavnih amandmajev IX-LXXXIX k Ustavi Socialistične republike Slovenije (ZEG-B). Ur. list SRS, št. 32/89.
- (1991). Ustava Republike Slovenije (URS). Ur. list RS, št. Ur. list RS, št. 33/91-I, 42/97, 66/00, 24/03, 69/04, 69/04, 69/04, 68/06, 47/13, 47/13.

- (1994). Zakon o ratifikaciji Konvencije o varstvu človekovih pravic in temeljnih svoboščin, spremenjene s protokoli št. 3, 5 in 8 ter dopolnjene s protokolom št. 2, ter njenih protokolov št. 1, 4, 6, 7, 9, 10 in 11. Ur. list RS, št. 33/1994.
- (1994). Zakon o ratifikaciji konvencije o varstvu posameznikov glede avtomatske obdelave osebnih podatkov. Ur. list RS, št. 11/1994.
- (1999). Zakon o pravdnem postopku (ZPP). Ur. list RS, št. 26/99, 96/02, 12/03, 58/03, 2/04, 2/04, 36/04, 69/05, 90/05, 43/06, 52/07, 73/07, 45/08 , 45/08, 111/08, 57/09, 12/10, 50/10, 107/10, 75/12, 40/13, 92/13, 10/14, 48/15.
- (2001). Obligacijski zakonik (OZ). Ur. list RS, št. 83/01, 32/04, 28/06, 40/07, 97/07.
- (2004). Zakon o varstvu osebnih podatkov (ZVOP-1). Ur. list RS, št. 86/04, 113/05, 51/07, 67/07, 94/07.
- (2005). Zakon o informacijskem pooblaščencu (ZInfP). Ur. list RS, št. 113/05, 51/07.
- (2008). Kazenski zakonik (KZ-1). Ur. list RS, št. 55/08, 66/08, 39/09, 91/11, 50/12, 6/16, 54/15.
- Center za varnejši internet. (14. 4. 2016). *Zaščita zasebnosti na spletu - 10 naj nasvetov. Pridobljeno iz Center za varnejši internet:* http://safe.si/podrocja/moja-identiteta-in-zasebnost-na-spletu/10-naj-nasvetov-o-zasciti-zasebnosti-na-spletu
- Editor, d. o. o. (13. 4. 2016). *Nastop na družabnih omrežjih. Pridobljeno iz Editor, d. o. o.:* http://www.editor.si/nastop-na-druzabnih-omrezjih
- European Commission. (12. 4. 2016). *EU Charter of Fundamental Rights. Pridobljeno iz European Commission:* http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm
- Evropska komisija. (12. 4. 2016). *Direktiva 95/46/EC. Pridobljeno iz Evropska komisija:* http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf
- Gliha Komac, N. (11. 4. 2016). *Socialna, družbena in družabna omrežja.* Pridobljeno iz: http://isjfr.zrc-sazu.si/sl/svetovalnica/socialna-dru%C5%BEbena-in-dru%C5%BEabna-omre%C5%BEja#v
- Informacijski pooblaščenec. (14. 4. 2016). *Varstvo osebnih podatkov na internetu. Pridobljeno iz Informacijski pooblaščenec:* https://www.ip-rs.si/varstvo-osebnih-podatkov/informacijske-tehnologije-in-osebni-podatki/varstvo-osebnih-podatkov-na-internetu/
- Kvas, B. (11. 4. 2016). `*Varuhi spleta´ razkrivajo: goljufi vedno bolj prebrisani, uporabniki pa naivni*. Pridobljeno iz: http://www.e-demokracija.si/2015/05/11/varuhi-spleta-razkrivajo-goljufi-vedno-bolj-prebrisani-uporabniki-pa-naivni/
- Kvas, B. (11. 4. 2016). *Raziskava: Spletna omrežja so "zlata jama" osebnih podatkov.* Pridobljeno iz: http://www.e-demokracija.si/2009/03/30/raziskava-spletna-omrezja-so-zlata-jama-osebnih-podatkov/
- RIS. (11. 4. 2016). *Spletna socialna omrežja. Pridobljeno iz RIS*: http://www.ris.org/db/26/9805/Novice/Spletna_socialna_omrezja/0/?preid=1208
- Socialbakers. (13. 4. 2016). *Free Social Media Statistics. Pridobljeno iz Socialbakers*: http://www.socialbakers.com/statistics/

- Tim 4. (12. 4. 2016). *Socialna omrežja – Facebook. Pridobljeno iz Tim 4:* https://tim4doba.wordpress.com/
- Varuh človekovih pravic RS. (13. 4. 2016). *Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin. Pridobljeno iz Varuh človekovih pravic RS:* http://www.varuh-rs.si/index.php?id=108
- Vendi, spletni marketing, d. o. o. (12. 4. 2016). *Facebook. Pridobljeno iz Vendi, spletni marketing, d. o. o.:* http://www.vendi.si/kaj-je-facebook/

PRILOGE

Priloga 1: Anketni vprašalnik

ANKETA

Pozdravljeni. Sem Sabina Medvešek, študentka Fakultete za upravo, in trenutno končujem svoje izobraževanje. Prosila bi Vas, da si vzamete 7 minut časa in mi izpolnite sledeči anketni vprašalnik, ki mi bo v veliko pomoč pri sami izdelavi mojega diplomskega dela.

Ta anketa je namenjena vsem uporabnikom spletnih družbenih omrežij, zato že v samem začetku vabim k izpolnjevanju ankete samo tiste, kateri uporabljate vsaj eno spletno družbeno omrežje. Anketni vprašalnik je popolnoma anonimen.

Vnaprej hvala za sodelovanje.

DEMOGRAFSKI PODATKI:

Spol: M Ž

Starost: _____

Izobrazba:

- Osnovnošolska
- Srednješolska
- Visokošolska izobrazba – 1. stopnja (diploma)
- Visokošolska izobrazba – 2. stopnja (magisterij)
- Visokošolska izobrazba – 3. stopnja (doktorat)

UPORABA SPLETNIH DRUŽBENIH OMREŽIJ

1. Napišete imena spletnih družbenih omrežij, ki jih poznate, tudi če nimate na njem svojega profila (npr. Facebook, Instagram, Snapchat, itd.)

   _____

2. Na kolikih imate profil oziroma aktiven račun? (vpišite število)

   _____

3. Kako pogosto uporabljate spodaj našteta:

	Vsakodnevno	Nekajkrat na teden	Nekajkrat na mesec	Zelo redko	Ne uporabljam
a) FACEBOOK					
b) TWITTER					
c) LINKEDIN					
d) YOUTUBE					
e) MYSPACE					
f) DRUGO: (napiši katero) _____					

4. Prosim, če v spodnji tabeli označite, kako pogosto izvajate določene aktivnosti na spletnih družbenih omrežjih.

	Vsakodnevno	Nekajkrat na teden	Nekajkrat na mesec	Zelo redko	Nikoli
všečkam					
objavljam svoje fotografije/ videoposnetke					
komentiram objave drugih					
izražam svoje mnenje glede aktualnega dogajanja					
objavljam povezave					
objavljam podatke na svojem statusu: kaj delam, kje sem, kam grem itd.)					

ODNOS DO OSEBNIH PODATKOV IN VARNOSTNE NASTAVITVE

1. Preden ste si ustvarili profil na kateremkoli spletnem družbenem omrežju, ste si prebrali splošne pogoje uporabe?

a) da
b) ne
c) preberem jih kasneje
d) te stvari me ne zanimajo

2. Osredotočimo se samo na Facebook (lahko tudi na drugo spletno družbeno omrežje, če slučajno niste tukaj registrirani) in mi, prosim, v spodnji tabeli označite, kako so vaši osebni podatki vidni ostalim uporabnikom.

	Nastavljeno kot skrito (vidim samo jaz)	Vidno vsem	Vidno mojim prijateljem	Ne vem	Tega podatka nimam objavljenega
Ime in priimek					
Naslov prebivališča					
Elektronski naslov					
Telefonska številka					
Delovno mesto					
Izobraževanje					
Datum rojstva					
Kraj bivanja					
Drugo: _____					

3. Označite, koliko pozornosti posvečate varnostnim vidikom pri uporabi naštetih družbenih omrežjih.

	Nič	Srednje	Veliko	Ne uporabljam
a) FACEBOOK				
b) TWITTER				
c) LINKEDIN				
d) YOUTUBE				
e) MYSPACE				

f) DRUGO: (napiši katero) _____				

ZLORABA OSEBNIH PODATKOV

1. Kako pomembna vam je zasebnost vaših osebnih podatkov, ki jih imate na spletnih družbenih omrežjih?

a) zelo pomembna
b) pomembna
c) manj pomembna
d) vseeno mi je

2. Ali ste bili že kdaj soočeni z zlorabo vaših osebnih podatkov (za primer, se vam je že kdaj zgodilo, da so vam ukradli vašo identiteto)?

a) da
b) ne
c) ne vem

3. Kako verjetno se vam zdi, da vaši osebni podatki v prihodnosti postanejo predmet zlorabe? (označite na lestvici od 1 do 5)

1 To sploh ni mogoče	2 Obstaja majhna možnost	3 Sem neopredeljen/a	4 Obstaja velika verjetnost	5 Zagotovo bodo

4. Ne glede na to, kako ste pri prejšnjem vprašanju izbrali verjetnost, me zanima razlog, zakaj tako mislite:

_____

POZNAVANJE ZAKONODAJE

1. Ali mislite, da imamo varstvo osebnih podatkov v Sloveniji urejeno s pravnimi akti?

a) Da
b) Ne

c) Ne vem
d) Me sploh ne zanima

2. Za kateri zakon mogoče mislite ali ste že slišali, da ureja področje varstva osebnih podatkov?

   _____

3. Na koga bi se obrnili, če bi bili vaši osebni podatki zlorabljeni?

   _____

4. Prosim, če mi na lestvici od 1 do 5 označite, kako pogosto prebirate priročnike in smernice varne uporabe spleta (npr. od informacijskega pooblaščenca, varuha človekovih pravic …).

1- Nikoli, te stvari me ne zanimajo
2- Zelo redko
3- Občasno si preberem
4- Skoraj redno in aktivno spremljam te stvari
5- Te stvari redno spremljam in prebiram

5. Bi si želeli vedeti več o nevarnostih, ki vam jih prinašajo spletna družbena omrežja, in kako se zaščiti pred njimi ter kaj bi morali storiti v primeru, ko so vaši osebni podatki že zlorabljeni?

   a) da
   b) ne
   c) te stvari me enostavno ne zanimajo

6. Podajte mi predlog, kako bi vam to najbolj ustrezalo, da se izvede:

   _____

Še enkrat hvala za vaš čas in sodelovanje! Sabina Medvešek