UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Mojca Berce

Informacijska zasebnost na internetu in v E-upravi

Diplomsko delo

Ljubljana, 2009

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Mojca Berce

Mentor: doc. dr. Jaroslav Berce
Somentor: asist.dr. Matej Kovačič

Informacijska zasebnost na internetu in v E-upravi

Diplomsko delo

Ljubljana, 2009

Iz srca se zahvaljujem za pomoč in solidarnost pri izvedbi in oblikovanju dokončnega sadeža mojega študija mentorju doc.dr. Jaroslavu Berce in somentorju asist.dr. Mateju Kovačiču. Brez njiju mi ne bi uspelo, tako da hvala vama.

Zahvaljujem se tudi svojemu fantu Jožku, ki mi je skoraj od začetka študija stal ob strani in mi je stal ob strani tudi sedaj, ko sem najbolj rabila podporo.

Zahvala gre tudi mojim prijateljem, ki so verjeli vame in se niso vdali.

Zahvala gre tudi moji mami, ki me je celo pot študija bodrila in se veselila z menoj vsakega uspeha.

INFORMACIJSKA ZASEBNOST NA INTERNETU IN V E-UPRAVI

Informacijsko zasebnost varuje zakon o varovanju osebnih podatkov in je ena izmed najbolj pomembnih človekovih pravic. Informacijske zasebnosti pa ne moremo pravilno definirati, če ne poznamo definicije osebnega podatka. Torej, informacijska zasebnost temelji na naših osebnih podatkih. Živimo v času, ko se tehnologija spreminja, nas nadzoruje in s tem postaja varovanje informacijske zasebnosti čedalje bolj pomembno za posameznike, organizacije ter za nove generacije. S pojavom interneta in razvojem spletnih strani se obseg informacijske zasebnosti zmanjšuje. Na internetu dobimo veliko podatkov na različnih spletnih straneh. Imamo več vrst spletnih strani in mene je predvsem zanimala spletna stran javne uprave z imenom E-uprava. Vendar se informacijska zasebnost ne odraža samo v E-upravi, vendar tudi v zdravstvu, prometu. V empiričnem delu naloge so predstavljeni rezultati samostojne raziskave med uporabniki glede varovanja informacijske zasebnosti in uporabe E-uprave, povzet pa je tudi intervju z informacijsko pooblaščenko. Na podlagi analiz rezultatov so bile potrjene hipoteze in teza. Iz tega sledi zaključek, da je informacijska zasebnost pomembna človekova pravica.

Ključne besede: Informacijska zasebnost, E-uprava, uporabniki, varovanje osebnih podatkov, informacijska tehnologija

INFORMATION ON THE INTERNET AND PRIVACY IN E-GOVERNMENT

Information privacy is protected by law and is one of the most important human rights. We live in a time when technology is changing our world rapidly. Information privacy and can not be properly defined, if we do not know definitions of personal data. Thus, information privacy is based on our personal data. The protection of information privacy is becoming increasingly important for individuals, organizations and the new generation. With the emergence of the Internet and the development of websites, reduction in privacy emerged. On the Internet we can get a lot of information on various sites. I was particularly interested in the public administration web sites, called E-government. However, information privacy is not reflected only in the E-government, but also in health, transport. In the empirical part of the paper I present the results of the survey of how well Internet users are familiar with information security and privacy of e-government sites. I also included an interview with the Information Commissioner. Based on the analysis results were confirmed hypothesis and thesis. It is followed by the conclusion that information privacy is an important human right.

Keywords: Information privacy, E-government users, protect personal data, information technology

Kazalo

Kazalo slik:

Kazalo tabel:

Kazalo grafov:

UVOD

Tehnološki razvoj, s tem mislim predvsem na razvoj informacijske tehnologije, omogoča čedalje lažje shranjevanje, obdelovanje (velikokrat povsem avtomatizirano) in distribucijo oziroma izmenjavo osebnih podatkov. S problemi, povezanimi z varovanjem osebnih podatkov oziroma z informacijsko zasebnostjo posameznikov, se države oziroma zveze držav, kot je Evropska Unija (EU), spopadajo s sprejemanjem ustrezne zakonodaje, ustanavljanjem posebnih samostojnih delovnih teles, vendar je področje varstva informacijske zasebnosti in zasebnosti nasploh ob čedalje več zahtevanih podatkih za vodenje države, vedno težje nadzorovati. Številne zbirke osebnih podatkov, ki jih hranijo podjetja, razne organizacije, društva, ipd. je verjetno sploh nemogoče v celoti ustrezno nadzorovati, oziroma, nadzorovati njihove upravljavce, da s podatki, ki so jim zaupani, ravnajo v skladu z veljavno zakonodajo. Pri tem je človeška, in ne toliko tehnološka razsežnost tisti odgovor, ki omogoča uspešno vladanje in s tem nadzor nad ustreznim varovanjem zbranih podatkov (Berce v Stare in Bučar 2005, 168). Posebno poglavje problematike pridobivanja, hranjenja in obdelave osebnih podatkov (pa tudi prestrezanja komunikacij) pa predstavlja internet, kjer so kraje raznih sicer tajnih osebnih podatkov, kot so kraja identitete, kraje številk kreditnih kartic, maskiranje spletnih strani z namenom pridobivanja osebnih podatkov, vdori v zbirke osebnih podatkov, praktično vsakdanja praksa. Lahko rečemo, da ne obstaja nobena »on-line« aktivnost, ki bi omogočala popolno zasebnost (Kovačič 2003, 40).

David Flaherty, eden prvih pooblaščencev za varstvo zasebnosti v Kanadi, pravi, da se pravica do zasebnosti tesno povezuje z naslednjimi pojmi: pravica do osebne avtonomije, pravica do biti puščen pri miru, pravica do zasebnega življenja, **pravica do nadzora informacij o sebi**, pravica do omejitve dostopnosti do sebe, pravica do ekskluzivnega nadzora dostopa do zasebnega področja, pravica do zmanjšanja nadlegovanja na najmanjšo možno mero, pravica do pričakovanja zaupnosti, pravica do uživanja osamljenosti, pravica do uživanja intimnosti, pravica do uživanja anonimnosti, pravica do uživanja zadržanosti in pravica do tajnosti (Flaherty v Kovačič 2006, 39).

Ko smo dobili internet, smo s tem tudi dobili precejšen dostop do podatkov, ki so lahko osebni, javni, zaupni. Država se trudi posameznikom omogočiti enostavno iskanje podatkov ter še posebno želi omogočiti, da lahko do večine storitev dostopaš od doma, preko

interneta. S tem, ko smo dobili internet, smo dobili tudi različne spletne strani, ki nam ponujajo veliko podatkov, obrazcev in seveda storitev. Sem seveda spadajo tud strani E-uprave, ki so namenjene vsem, ki želijo preko interneta opravljati poslovanje z državo oziroma z javno upravo.

V empiričnem delu smo predstavili odnos uporabnikov do varovanja osebnih podatkov in kako so seznanjeni z spletno stranjo E-uprava ter ali jo uporabljajo. Pridobiti smo tudi želeli podatke od ministrstev glede varovanja osebnih podatkov in njihove hrambe, da bi lahko naredili ustrezno primerjavo. Vendar zaradi nesodelovanja s strani ministrstev, s katerimi smo komunicirali preko elektronske pošte, raziskave nismo mogli narediti točno takšne, kot je bila zamišljena. Od 27 naslovov, na katere smo poslali elektronsko pošto, smo dobili pravi odziv samo od enega ministrstva, ostali so samo pregledali oziroma „preklikali“ spletno anketo. Poleg spletnih anket smo naredili tudi intervju z informacijsko pooblaščenko Natašo Pirc-Musar, ki mi je povedala veliko zanimivih podatkov in dejstev in iz njenih odgovorov smo tudi dobili delno pojasnilo za nesodelovanje ministrstev.

Hipoteze in teza so bile oblikovane glede na zanimanje ter samo temo. V veliko pomoč pri oblikovanju dela sta bila mentor in somentor, ki sta vsak s svojim znanjem pomagala obogatiti naše delo.

1 POGLAVJE: ZGODOVINA INFORMACIJSKE TEHNOLOGIJE IN ZASEBNOSTI

Informacijska tehnologija se deli na štiri obdobja, ki so zaznamovana z glavnimi tehnologijami, uporabljenimi za reševanje vnosa, obdelave, proizvodnje in komunikacijskih časovnih problemov (Butler 1997):

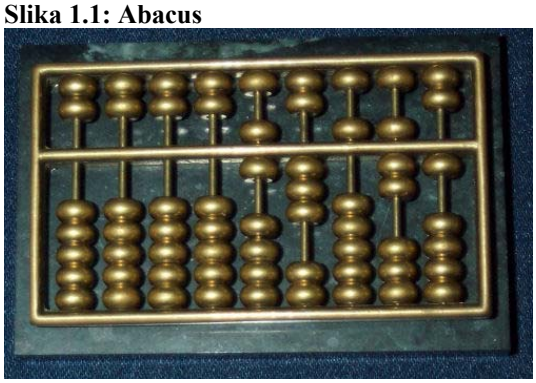
1. Predmehanska doba
2. Mehanska doba
3. Elektronsko-mehanska doba
4. Elektronska doba

Glavni značilnosti predmehanske dobe, ki se je začela 3000 pred našim štetjem in končala 1450 našega štetja (Butler 1997) sta pisanje in abeceda. Prvi začetniki so se sporazumevali preko risb oziroma slikarij ter skozi svojo obliko jezika. Okoli 3000 let pred

našim štetjem so v Mezopotaniji, torej v današnjem južnem Iraku, izumili napravo cuniform[1]. Okoli leta 2000 pred našim štetjem so Feničani odkrili simbole, s katerimi so se začeli sporazumevati med seboj. Nato so sledili Grki z abecedo in Rimljani, ki so kasneje dali črkam latinska imena ter ustvarili abecedo, ki jo uporabljamo še danes. Vhodna tehnologija[2] je bila največje odkritje poleg abecede, simbolov ter splošnega jezika. Sem sodijo papir in pisala. Tehnologija zapisovanja je temeljila na tankem, ozkem peresu, s katerim si praskal na mokro glino. Okoli leta 2600 pred našim štetjem so Egipčani začeli pisati na papirus, narejen iz rastlinskih listov. Okoli leta 100 po našem štetju so Kitajci naredili papir iz krp, na katerih temelji sedanji papir.

Knjige in knjižnice so bila tretja pridobitev v tej dobi in so imele vlogo hrambe podatkov oziroma informacij. Začetniki teh hramb so bili verski pripadniki in so edini imeli shranjene knjige. Četrta pridobitev so bili številski sistemi oziroma prva oštevilčenja. Prvi številski sistem, podoben današnjemu, so izumili med leti 100 in 200 po našem štetju, ko so Hindujci v Indiji ustvarili devet-mestni sistem številčenja. Peta pridobitev je bila pridobitev prvega ročnega računala oziroma kalkulatorja. Imenoval se je Abacus (Butler 1997).

Slika 1.1: Abacus



Vir: Jo Edkins (2007).

Predmehanski dobi sledi mehanska doba, ki se začne leta 1450 in konča 1840. Tu pride do prve informacijske eksplozije. Johann Gutenberg je izumil premična kovinska tipala v procesu tiskanja leta 1450. Razvije se tudi indeksiranje knjig z razširjeno uporabo številskih strani. Pojavi se tudi prvo namensko računalo. Leibniz in Pascaline sta izumila logaritmično

1 Cuniform je pisava s podobami, ki so jo uporabljali v Mezopotamiji pred Kristusovim rojstvom .
2 input technologies

ravnilo.[3] Blaise Pascal je izumil tudi Pascaline[4]. To je prvi mehanski računalniški stroj, ki je nastal okoli leta 1642 (Butler 1997).

V elektronsko-mehanski dobi, ki se je začela leta 1840 in končala 1940, je informacijska tehnologija dosegla ključni dosežek v tem obdobju in sicer odkritje načina za izkoriščanje električne energije. Znanje in informacije so zdaj lahko pretvorili v električne impulze. Tako so se začeli prvi telekomunikacijski procesi. Prvi shranjevalec napetosti je bil narejen pozno v 18. stoletju in se je imenoval voltažna baterija. V začetku 19. stoletja je Samuel Morse odkril telegraf. Kasneje sta sledila še telefon, ki ga je izumil Alexander Bell v letu 1876 in preko tega je prišlo do novega odkritja, da električni valovi potujejo skozi prostor in lahko proizvajajo tudi učinek daleč od točke, na kateri so nastali. Tako je leta 1894 Guglielmo Marconi izumil radio. V letu 1880 je sledil s svojim odkritjem še Herman Hollerith (1860-1929), ki je ustanovil IBM. Leta 1890 je IBM (**International Business Machines Corporation**) dobil tudi svoj prvi logotip (Butler 1997).

Slika 1.2: Prvi IBM logo

vir : Zlok (2009).

Zadnja doba je elektronska doba, ki se je začela leta 1940 in traja še danes. Prva iznajdba so bile elektronske vakuumske cevi – elektronke. John Mauchly - fizik in J.Prosper Eckert, inženir za elektriko sta bila prva, ki sta naredila hiter, večnamenski računalnik, ki je uporabljal elektronke: Electronic Numerical Intergrator and Computer (ENIAC)[5]. Za izračune je uporabljal elektronske vakuumske cevi ter ni imel sposobnost shranjevanja programov (nabora ukazov) (Butler 1997).

3 Logarítemsko računálo (po domače imenovano »reh'nšiber«, iz nemške besede Rechenschieber) je preprost analogni računalnik, podoben ravnilu, po navadi sestavljen iz treh vpetih umerjenih tračnih letev in drsečega okvirja (Slovenska wikipedia).

4 Pascaline je računalo, ki je bil narejen za izračun 8 številk ter tudi za računovodstvo.

5 Razvoj je financirala ameriška vojska. ENIAC ekipo so sestavljali: J. Presper Eckert, Jr.; John Grist Brainerd; Sam Feltman; Herman H. Goldstine; John W. Mauchly; Harold Pender; Major General G. L. Barnes; Colonel Paul N. Gillon.

Maurice Wilkes, britanski znanstvenik na univerzi v Cambridgu je dokončal EDSAC (Electronic Delay Storage Automatic Calculator) leta 1949 - dve leti pred dokončanjem dela na EDVAC-u. Tako je EDSAC postal prvi računalnik s shranjenim programom v splošni uporabi (ni bil zgolj prototip).

V poznih 1940-ih sta Eckart in Mauchly pričela z razvojem računalnika, poimenovanega UNIVAC (Universal Automatic Computer). Prvi splošnonamenski računalnik za komercialno rabo: Universal Automatic Computer (UNIVAC) so dostavili statističnemu uradu ZDA leta 1951, s katerim so izvedli popis prebivalstva (Butler 1997).

Slika 1.3: UNIVAC

vir:KKU Web hosting (2009).

Digitalno računalništvo je pridobilo elektronke od leta 1951 do leta 1958. Za vnos in zunanje shranjevanje podatkov so uporabljali luknjane kartice, za notranje shranjevanje podatkov in programov pa vrteče magnetne bobne. Programi so bili spisani v strojnem jeziku, zbirnem jeziku ter so zahtevali prevajalnik (Butler 1997). Od leta 1959 do leta 1963 elektronke zamenjajo tranzistorji. Prve tranzistorje so razvili v laboratorijih Bell AT&T v 40-ih letih 20.stoletja. Materiale, ki se imenujejo polprevodniki, so uporabljali za izdelavo naprav, ki se imenujejo tranzistorji. Magnetni trakovi in diski začenjajo zamenjevati luknjane kartice kot naprave za zunanje shranjevanje podatkov. Pojavijo se višjenivojski programski jeziki (Butler 1997). Od leta 1964 in vse do današnjega časa se je razvilo še veliko programov kot so: BASIC ter operacijski sistemi, Visicalc, Lotus 1-2-3, dBase, Microsoft Word in ostali programi. Pojavijo se mikroprocesorji, ki vsebujejo pomnilnik, logiko in nadzorna vezja (celotna CPE - centralna procesna enota, CPU v ang.) na enem čipu. To omogoči razvoj osebnih računalnikov (PC-jev), kot sta Apple (II in Mac) ter IBM PC.

1.2 Kratek pregled informacijske zasebnosti skozi zgodovino

V Angliji so leta 1361 sprejeli zakon Justices of Peace Act[6], ki je predvidel kazen za posameznike, ki bi drugim prisluškovali ali jih skrivaj opazovali. To je možno šteti kot začetek zakonodaje, ki ščiti pred posegi v zasebnost. V letu 1466 ali 1467 se je pojavil eden najstarejših na zahodu znanih esejev o kriptoanalizi, torej je bila komunikacijska zasebnost resno dojeta že vsaj od 15. stoletja naprej (Kahn v Kovačič 2006,49). Prva pravna regulacija preiskovanja zasebnih prostorov s strani oblasti se pojavi v letih med 1765 in 1781 najprej v Angliji, kasneje pa tudi v ZDA. Na Švedskem se v letu 1776 pojavi prvi zakon, ki je namenjen zaščiti informacijske zasebnosti – predpiše namreč, da lahko država zbira podatke le za uporabo v zakonite namene. Leta 1858 Francija sprejme kazni za sankcioniranje primerov nepooblaščene objave osebnih podatkov. V ZDA se je začel razvoj sodobne pravice do zasebnosti in sicer je leta 1880 Thomas M. Cooley kot eden prvih objavil definicijo zasebnosti v okviru odškodninskega prava, ki je bila nato uporabljena na sodišču v letu 1881. Eden izmed pomembnih mejnikov pri razvoju pravice do zasebnosti predstavlja tudi članek The Right to Privacy avtorjev Samuela D. Warrena in Louisa D. Brandeisa, ki je posebej izpostavil uporabo takrat novih tehnologij (fotoaparat, naprave za glasovno snemanje), ki so povečale vdor v zasebnost, obenem pa sta se obregnila tudi ob nadležen tisk (Warren D. S.in Brandeis D. L., 1890 v Kovačič 2006, 48).

V sodobnejšem času pa je pomembna predvsem pravna praksa ZDA, v kateri je iz leta 1967 pomemben pojem pričakovane zasebnosti (Kovačič 2006, 52). Takrat je namreč Vrhovno sodišče ZDA v primeru Katz proti ZDA razsodilo, da pravo ščiti zasebnost posameznikov v vseh prostorih, v katerih lahko posameznik upravičeno pričakuje zasebnost (Kovačič 2006, 53). S tem so presegli do takrat veljaven koncept zasebnosti kot lastninske pravice. Seveda pa je prav tako pomembno mednarodnopravno varovanje zasebnosti, oziroma temelji zasebnosti v mednarodnih dokumentih – le te sta postavili Splošna deklaracija človekovih pravic iz leta 1948, ki v 12. členu pravi [7]:

6 Zakon Justices of Peace Act je zakon ko, sodni uradnik imenuje s pomočjo komisije za ohranitev miru.
7 Splošna deklaracija o človekovih pravicah iz leta 1948 kot skupen ideal vseh ljudstev in vseh narodov z namenom, da bi vsi organi družbe in vsi posamezniki (Varuh 2007).

12. člen

Nikogar se ne sme nadlegovati s samovoljnim vmešavanjem v njegovo zasebno življenje, v njegovo družino, v njegovo stanovanje ali njegovo dopisovanje in tudi ne z napadi na njegovo čast in ugled. Vsakdo ima pravico do zakonskega varstva pred takšnim vmešavanjem ali takšnimi napadi.

Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin (v nadaljevanju EKČP) iz leta 1950, ki v 8. členu pravi:

8. člen

Pravica do spoštovanja zasebnega in družinskega življenja

> *Vsakdo ima pravico do spoštovanja svojega zasebnega in družinskega življenja, svojega doma in dopisovanja. Javna oblast se ne sme vmešavati v izvrševanje te pravice, razen če je to določeno z zakonom in nujno v demokratični družbi zaradi državne varnosti, javne varnosti ali ekonomske blaginje države, zato, da se prepreči nered ali zločin, da se zavaruje zdravje ali morala ali da se zavarujejo pravice in svoboščine drugih ljudi.*

V slednjem členu je tudi jasno razvidna omejitev pravice do zasebnosti v primerih, ko se gre za državno/javno varnost, ekonomsko blaginjo, vzdrževanje reda in miru, zavarovanje zdravja ali morale in varovanje pravic ter svoboščin ostalih ljudi. EKČP je pri razvoju razumevanja pravice do zasebnosti v Evropski Uniji (EU) še posebej pomembna, saj pomeni pravno podlago za delovanje Evropskega sodišča za človekove pravice, ki s svojimi razsodbami ustvarja sodno prakso, ki ima vpliv na poenotenje obravnavanja človekovih pravic na področju EU.

1.3. Razvoj pravice do informacijske zasebnosti

V bistvu je tehnološki razvoj tisti, ki je pripeljal do prvega zakona, ki je obravnaval pravico do informacijske zasebnosti. Prvi tovrstni zakon je namreč sprejela nemška dežela Hesse leta 1970 kot odgovor na reakcije ob vzpostavljanju informacijskega sistema, ki bi omogočil centralizacijo, povezovanje in nastanek velikih zbirk podatkov. Razlogi za javni odpor proti takim načrtom so v negativni izkušnji druge svetovne vojne, kjer so nacisti uporabljali Hollerithove stroje za popis prebivalstva, kar jim je omogočalo identifikacijo

judovskega prebivalstva. Te stroje so glede na navedbe v knjigi *IBM and the Holocaust*[8] nacisti uporabljali tudi za vodenje vojske, ekonomije, koncentracijskih taborišč itd (Kovačič 2006, 72). Pri tem se je tudi jasno pokazala povezava med tehnologijo, informacijsko zasebnostjo in totalitarizmom. Potrebno pa je opozoriti na to, da se je v začetku zakonodaja ukvarjala predvsem z računalniško obdelavo podatkov in ne s posameznikom in njegovimi pravicami. Dokler ni prišlo v razvoju tehnologije do korenite spremembe smeri.

Z razvojem je namreč prišlo do prvih poceni in širše dostopnih računalniških sistemov, ki so sčasoma izrinili velike računalniške sisteme. S tem pa se je pojavila nova težava – razpršene sisteme je namreč precej težje nadzorovati kot centralizirane. Tako je bilo potrebno zakonodajo razširiti tudi na zasebni sektor – kot to počne prvi tovrstni zakon, ki je postavil enotna merila za javni in zasebni sektor.

Razvoj pa je v osemdesetih letih 20. stoletja prinesel še eno problematično področje – sprva se je informacijska zasebnost namreč obravnavala kot notranja težava nacionalnih držav, potem pa je razvoj prinesel internacionalizacijo problema v obliki pretoka osebnih podatkov preko meja držav. Kot reakcijo na to je OECD[9] leta 1980 (Kovačič 2006, 76) sprejela **Smernice za zaščito zasebnosti in čezmejni pretok zasebnih podatkov**, ki postavljajo enotna merila za javni in zasebni sektor, so pa prvotno namenjene neoviranemu pretoku zasebnih podatkov med državami in je torej varovanje podatkov v funkciji izmenjave le-teh med državami. Leto dni kasneje je nato Svet Evrope sprejel[10] (Kovačič 2006, 76) **Konvencijo o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov**, ki je eden najpomembnejših dokumentov s področja varovanja informacijske zasebnosti. Nadalje se je razvoj zaščite nadaljeval leta 1983, ko je razsodba nemškega ustavnega sodišča izpostavila načelo informacijskega samoodločanja, kar v praksi pomeni, da se lahko posamezniki odločajo, ali bodo podatke dali ali ne, naloga države pa je pojasnitev, zakaj podatke rabi in kakšne so posledice zavrnitve oddaje podatkov (Mayer- Schonberger, 2001,199 v Kovačič 2006,77). Ker pa je v praksi še vedno prihajalo do zlorab, se je razvoj usmeril v absolutno zaščito nekaterih področij informacijske zasebnosti. To v praksi pomeni, da se posameznik ne more v pogodbi odreči nekaterim pravicam, prepovedano ali močno omejeno pa je obdelovanje nekaterih vrst osebnih podatkov (Kovačič 2006, 77).

8 IBM and the Holocaust je knjiga, ki opisuje odnos med IBm in tretjih rajhom. Napisal jo je Edwin Black (English wikipedia 2009).

9 OECD. 1980. Smernice za zaščito zasebnosti in čezmejni pretok osebnih podatkov(The OECD on the Protection of Privacy and Transborder Flows of Personal Data), sprejete 23.septembra 1980.

10 Svet Evrope.1981. Konvencija Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov(Convention for the Protection of Individuals with Automatic Processing of Personal Data), sprejel jo je Svet evrope 28.1.1981. Uradni list RS, Mednarodne pogodbe, št.3/1994. Konvencijo je državni zbor Republike Slovenije ratificiral dne 25.1.1994. Veljati je začela dne 1.3.1994

2 POGLAVJE: OPREDELITEV POJMOV INFORMACIJSKA ZASEBNOST IN E-UPRAVA

2.1 Informacijska zasebnost

»Informacijska zasebnost je možnost posameznika, da obdrži podatke in informacije o sebi«(Pestotnik 2007, 15). Posameznik mora biti vedno z zbiranjem in namenom seznanjen oziroma mora biti določen čas zbiranja, inšpektorski nadzor, transparentnost uporabe (Kovačič 2000,27). Mellors ugotavlja, »da najboljša zaščita ni ta, da oni(država) vedo manj o nas, pač pa da mi vemo več o njih, da vemo kaj vedo o nas in kako te informacije o nas uporabljalo« (Mellors v Kovačič v Pestotnik 2007, 15).

Lahko jo pa definiramo tudi na način, kot jo definira Wagner DeCewova[11]: varovanje osebnih podatkov posameznika, skupaj s komunikacijami posameznika. Ogrožena pa je (informacijska zasebnost), kadar se osebni podatki zbirajo in objavljajo brez privoljenja ali vednosti posameznika, ali pa samo s poskušanjem zbiranja podatkov (Kovačič 2006, 46). Pri nas se glede na spletne strani informacijskega pooblaščenca, ki obenem opravlja tudi naloge ugotavljanja kršitev Zakona o varstvu osebnih podatkov (ZVOP-1, 2004), informacijska zasebnost enači z varstvom osebnih podatkov. Pri nadaljnjem raziskovanju pravice do informacijske zasebnosti se bomo osredotočili predvsem na razvoj in zakonsko utemeljitev te pravice na področju sedanje EU.

Informacijska zasebnost se je kot posebna dimenzija pojavila v 60. in 70. letih 20. stoletja (Bennett v Kovačič v Pestotnik 2007,16). Vendar se je v tem času pojavljala kot problem in bila razumljena tudi kot problem, ki je obstajal znotraj nacionalnih držav. Kasneje, v 80. letih in naprej, pa je zaradi razvoja in povečanja dostopnosti tehnologije informacijska zasebnost postala izrazito globalen izziv (Bennett v Kovačič 2007, 247).

V Sloveniji imamo z zakonom določeno informacijsko zasebnost. Sicer je v kazenskem zakoniku to 154. člen, ki pravi naslednje :

> *Kdor v nasprotju z zakonom uporabi osebne podatke, ki se smejo voditi samo na podlagi zakona ali na podlagi osebne privolitve posameznika, na katerega se osebni*

11 Wagner DeCew, Judith.1997.In pursuit of Privacy.Ithaca, London: Cornell University Press (Kovačič, 2006,238)

podatki nanašajo, se kaznuje z denarno kaznijo ali z zaporom do enega leta. Enako se kaznuje, kdor vdre v računalniško vodeno zbirko podatkov z namenom, da bi sebi ali komu drugemu pridobil kakšen osebni podatek. Če stori dejanje iz prvega ali drugega odstavka tega člena uradna oseba z zlorabo uradnega položaja ali uradnih pravic, se kaznuje z zaporom do dveh let. (Kazenski zakonik 2004).

2.1.1 Smernice EU glede varovanja informacijske zasebnosti

EU poskuša s svojimi direktivami poenotiti področje varovanja informacijske zasebnosti v državah članicah, kar je povsem v skladu z načrti o nadaljnji integraciji Unije. Tako je leta 1995 sprejela Direktivo o zaščiti osebnih podatkov 95/46/EC, katere prvi osnutek so pripravili že leta 1990. Prvi osnutek je imel to pomanjkljivost, da je varstvo osebnih podatkov obravnaval drugače v javnem in zasebnem sektorju, kar je direktiva kasneje poenotila. Direktiva pa poleg tega, da zagotavlja zaščito osebnih podatkov posameznika, obenem jasno omogoča tudi izmenjavo osebnih podatkov med državami članicami – v 2. točki 1. člena:

Člen 1

Namen direktive

1. V skladu s to direktivo države članice varujejo temeljne pravice in svoboščine fizičnih oseb in predvsem njihovo pravico do zasebnosti pri obdelavi osebnih podatkov.
2. Države članice ne omejujejo niti ne prepovedujejo prostega prenosa osebnih podatkov med državami članicami zaradi razlogov, povezanih z varstvom, ki je zagotovljeno na podlagi odstavka 1.

Poseben vpliv ima na varstvo osebnih podatkov tudi zaradi 28. člena, ki zahteva ustanovitev nadzornega organa, ki skrbi za izvajanje predpisov, ki so jih države sprejele s to direktivo. Člen tudi natančno opredeli naloge takega organa. Pri nas te naloge opravlja informacijski pooblaščenec.

Direktiva ravno tako prepoveduje iznos osebnih podatkov v države, ki nimajo urejene zaščite informacijske zasebnosti in s tem močno vpliva na razvoj te pravice v ostalih državah. Tako so recimo tudi ZDA morale (vsaj delno) sprejeti pogoje, ki jih postavlja direktiva in so tako z EU sprejele dogovor Safe Harbor Agreement, ki je omogočil pretok osebnih podatkov med EU in ZDA (Kovačič 2006, 79).

2.1.2 Informacijska zasebnost v Sloveniji – pravna podlaga in varovanje

Varstvo pravice do informacijske zasebnosti oziroma varovanje osebnih podatkov pri nas izvaja informacijski pooblaščenec, na podlagi ZVOP-1. Takšna ureditev je v veljavi od 31. decembra 2005, ko se je na podlagi Zakona o informacijskem pooblaščencu ustanovil neodvisen in samostojen državni organ informacijski pooblaščenec (Informacijski pooblaščenec, 2007). Pred tem je v Sloveniji področje nadzora nad varstvom osebnih podatkov opravljal Inšpektorat za varstvo osebnih podatkov. Prva različica ZVOP je bila v Sloveniji sprejeta leta 1990.

Poleg ZVOP-1 v Sloveniji področje varstva osebnih podatkov ureja Ustava RS in sicer v 38. členu:

38. člen

(varstvo osebnih podatkov)

Zagotovljeno je varstvo osebnih podatkov. Prepovedana je uporaba osebnih podatkov v nasprotju z namenom njihovega zbiranja.

Zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa zakon.

Vsakdo ima pravico seznaniti se z zbranimi osebnimi podatki, ki se nanašajo nanj, in pravico do sodnega varstva ob njihovi zlorabi.

Morebitne kršitve informacijske zasebnosti sankcionira Kazenski zakonik Republike Slovenije (KZ-1, 2008) z na novo prikrojenim zakonom, in sicer:

Zloraba osebnih podatkov

143. člen

(1) Kdor uporabi osebne podatke, ki se obdelujejo na podlagi zakona, v neskladju z namenom njihovega zbiranja ali brez osebne privolitve osebe, na katero se osebni podatki nanašajo, se kaznuje z denarno kaznijo ali zaporom do enega leta. (2) Enako se kaznuje, kdor vdre ali nepooblaščeno vstopi v računalniško vodeno zbirko podatkov z namenom, da bi sebi ali komu drugemu pridobil kakšen osebni podatek. (3) Kdor na svetovnem medmrežju objavi ali omogoči drugemu objavo osebnih podatkov žrtev kaznivih dejanj, žrtev kršitev pravic ali svoboščin, zaščitenih prič, ki se

nahajajo v sodnih spisih sodnih postopkov, kjer po zakonu ali po odločitvi sodišča ni dovoljena prisotnost javnosti ali identifikacija žrtev ali zaščitenih prič ter osebnih zapisov o njih v zvezi s sodnim postopkom, na podlagi katerih se te osebe lahko določi ali so določljive, se kaznuje z zaporom do treh let.

(4) Kdor prevzame identiteto druge osebe in pod njenim imenom izkorišča njene pravice, si na njen račun pridobiva premoženjsko korist ali prizadene njeno osebno dostojanstvo, se kaznuje z zaporom od treh mesecev do treh let.

(5) Če stori dejanje iz prejšnjih odstavkov tega člena uradna oseba z zlorabo uradnega položaja ali uradnih pravic, se kaznuje z zaporom do petih let.
(6) Pregon iz tretjega odstavka tega člena se začne na predlog.

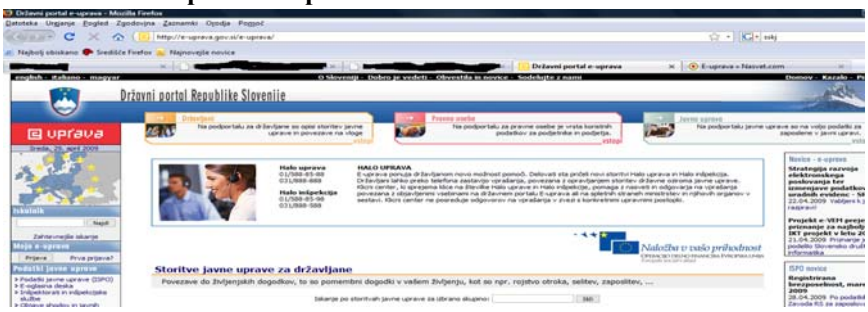
Neposredno se uporabljajo tudi določbe Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov, ki je bila ratificirana leta 1994 (Kovačič, 2003, 84).

2.2 E-uprava

»E-uprava je izraz do katerega pridemo, če združimo pojma javno upravo ter elektronsko poslovanje«(Ministrstvo za javno upravo).

Lahko trdimo, da gre za intenzivno uvajanje spletnih storitev in elektronskega poslovanja v upravo, med upravnimi organi v upravi, navzven z občinami, podjetji in drugimi organizacijami. »V ožjem smislu je torej E-uprava nabor upravnih storitev za civilne in pravne osebe, vezanih na informacijsko tehnologijo«(Cimolini 2003,17). Če pa vzamemo širši pojem E-uprave, je javna uprava kot neko podjetje, ki v svoje poslovanje vključuje načela E-poslovanja za izboljšanje učinkovitosti storitev preko informacijsko podprte javne uprave, informacijske infrastrukture, elektronskega poslovanja, sodelovanja z delavci z znanjem in sodobno tehnično industrijo ter višanja življenjskega standarda (Silič in drugi v Cimolini 2003,17).

Slika 2.1: Državni portal E-uprava



Vir: E-uprava (2006).

»Država bo lahko torej s prehodom na e-poslovanje in izvajanjem transakcij preko interneta, znatno zmanjšala stroške«(Skrt 2003). Država bo stroške zmanjševala tako, da se bodo transakcije deloma izvajale preko interneta, s tem se bo razbremenilo zaposlene na okencih in dosegli se bodo veliki časovni prihranki, kar bi se naj odražalo predvsem v večji učinkovitosti in preglednosti poslovanja ter kvalitetnejšem zadovoljevanju potreb državljanov (Skrt 2003). Glede na uvedbo elektronskega poslovanja ter same elektronske uprave bi se dalo pričakovati tudi večjo točnost opravljenih storitev in manjše število napak ter samo večje število obravnavanih in rešenih zahtevkov. Pri tem se tudi pričakuje, da se bodo hitreje lotevali reševanja postopkov ter večjo personalizacijo storitev in nenazadnje tudi boljši imidž uprave (Skrt 2003).

2.2.1 Nastanek spletnega portala E-uprava skozi leta 2001-2008

Začetek E-uprave se postavlja v leto 2000, ko je bil sprejet zakon o elektronskem poslovanju in elektronskem podpisu.[12] Ker je država želela pospešiti razvoj in slediti trendom Evropske Unije, je morala po hitrem postopku sprejeti določene strategije. Meseca februarja leta 2001, ko je Vlada Republike Slovenije sprejela strategijo e-poslovanja v javni upravi za obdobje od leta 2001 do leta 2004, nekaj mesecev kasneje pa je imenovala Strateški svet za informacijsko družbo (SID) (Skrt 2003), ki usmerja in vodi informatizacijo družbe in iz tega je nastala spletna stran E-uprava. Istega leta je Center vlade za informatiko (CVI) odprl spletni portal E-uprava (http://euprava.gov.si) in s tem začel uresničevati projekt e-poslovanja v državni upravi. Enotni državni portal zagotavlja informacije in storitve tako državljanom, gospodarskim subjektom, zaposlenim v javni upravi, kot tudi ustanovam javne uprave (Skrt 2003).

V tabeli je viden razvoj skozi leta in pridobitve na spletni strani.

12 Zakon o elektronskem poslovanju in elektronskem podpisu, prečiščena verzija 1.člen ter 2.člen (Uradni list 2004)

Table 2.1: Pregled dopolnitev E-uprave po letih

Leto	dopolnitev na strani
2001	• prvi državni portal E-uprava • uporabniki začeli uporabljati prve prave elektronske storitve za državljane • pridobivanje izpiskov iz matičnih knjig (rojstne matične knjige, poročne matične knjige in knjige umrlih)
2002	• prvi pravi projekt G2G[13](omogočal izmenjavo podatkov med centralnim registrom prebivalstva in Zavodom za pokojninsko in invalidsko zavarovanje Slovenije.) • začetek projekta e-notar
2003	• prenovitev portala • začeli delovati portali upravnih enot • pridobitev možnosti vpogleda v svoje osebne podatke (VLOP) • pridobitev možnosti vpogleda v centralni register prebivalstva (CRP).
2004	• generični sistem dostopa za sprejem E-vlog, E-podpis[14], usmerjanje E-vlog na upravno enoto in izvedbo E-plačil. • odprt sodni register za državljane • E-davki • obogatitev s podatki iz naslednjih področij: statistični urad, AJPES, carina • odprli tudi zemljiški kataster ter zemljiško knjigo
2005	• prva oddaja elektronske napovedi dohodnine • tesno sodelovanje med E-upravo ter informatiki • prenovljen register stalnega prebivalstva • informatizacija matični knjig ter zaključitev prenove registra vozil • izvajanje projekta E-vem (vse na enem mestu) priročen za samostojne podjetnike posameznike
2006	• ustanovi se urad za informatiko in E-upravo • prenovitev spletnega portala E-uprava • administrativno orodje: E-podpis, E-plačila, E-vročanje • projekt uradnih evidenc, tako je tudi država dobila svoj prvi metaregister, v katerem so popisane uradne evidence, viri in podatki • dostop državljanom do aplikacije podaljševanja registracije motornih vozil • integracijo z zavarovalnicami • Ministrstvo za javno upravo: vzpostavili tako imenovan izdajatelj časovnih žigov ter ustanovili so agencijo za podporo biometričnem potnim listom
2007	• dokončali generično orodje za izdelovanje poljubnih E-vlog, ki omogoča vnašanje podatkov iz uradnih evidenc in registrov • E-vem, ki je bil tudi tehnološko izveden za vse gospodarske družbe
2008	• portal namenjen otrokom in mladini

Vir:Batagelj in etc.: E-uprava, zavezništvo z uporabniki (2008).

13 G2G je online nekomercialna interakcija med državnimi organizacijami, avtoritetami in drugimi državnimi organizacijami (Wikipedia 2009).

14 Elektronski podpis je niz podatkov v elektronski obliki, ki je vsebovan, dodan ali logično povezan z drugimi podatki, in je namenjen preverjanju pristnosti teh podatkov in identifikaciji podpisnika (Ministrstvo za javno upravo 2009).

3 POGLAVJE: UREDITEV ZASEBNOSTI V NEELEKTRONSKI (JAVNI) IN V ELEKTRONSKI UPRAVI

3.1 Urejenost informacijske zasebnosti v javnem sektorju

Varovanje osebnih podatkov se glede na javno (neelektronsko) in elektronsko upravo razlikuje v načinu zbiranja podatkov. V neelektronski upravi lahko pride do sledeče situacije. Stranka pride na mestno upravo, vzame listek in čaka, kdaj bo na vrsti. Pri elektronski upravi oz. E-upravi pa vse to urediš preko interneta. Če se vprašamo, kateri način je najbolj varen in kateri način prinese večje varovanje zasebnosti, moramo narediti krajšo primerjavo med njima. Torej, javni sektor lahko osebne podatke obdeluje samo, če je obdelava osebnih podatkov določena v zakonu, na podlagi osebne privolitve pa znova, če je takšna obdelava določena v zakonu (Musar 2008, 6).

Temeljno načelo poslovanja v javni upravi določa:

> *Vsako delo organov javne uprave, ko opravljajo upravne naloge, je treba dokumentirati z ustreznim pisnim zapisom: dokumentom, zaznamkom ali pisarniško odredbo tako, da je mogoče delo kasneje pregledovati, preverjati njegovo pravilnost, pravočasnost in kakovost izvajanja, dokazovati dejstva in ohraniti zapise za znanost ter kulturo ali pravno varnost pravnih in fizičnih oseb (Žumer 2008, 130).*

Torej, obstajajo določene zahteve glede delovanja javne in državne uprave in te zahteve se čedalje bolj zaostrujejo, saj so v navezavi z sledljivostjo transakcij (Žurga v Dujić v Svete in Pintarič 2007,208).

Pri tem moramo vedeti, da se pričakovanja državljanov in gospodarskih subjektov večajo, kar pa se odraža predvsem v njihovih zahtevah glede obsega sredstev za delovanja uprave (Žurga v Dujić v Svete in Pintarič 2007,208).

Slovenska državna uprava se je za doseganje učinkovitosti odločila za zapisan enostaven cilj, ki si ga je zadala - prijazna in učinkovita ustava. S tem je Ministrstvo za javno upravo prikazalo, da je uprava prijazna, usmerjena k svojim uporabnikom ter hkrati prijazno delovno okolje za uslužbence, kar je vsekakor pomembno (Dujič v Svete in Pintarič 2007,207). Vendar sledi še , da tako prijazna uprava ne bi pomenila ničesar, če bi presegla svoje finančne zmožnosti države ali delovala sicer prijazno, vendar nekoristno (Dujič v Svete in Pintarič 2007,208). Ministrstvo za javno upravo izpostavlja svojo učinkovitost na sledeči

način, da je pomembno kakovostno in pravočasno odločanje državne uprave ter učinkovito upravljanje s kadrovskimi, finančnimi in materialnimi viri v državni upravi (Dujič v Svete in Pintarič 2007,208).

Zasebnost ter splošni pogoji upravljanja dokumentarnega gradiva v javni upravi so v Republiki Sloveniji urejeni s sodnimi predpisi, usklajenimi z mednarodnimi ISO standardi, priporočili Evropske komisije, resolucijami Sveta Evrope ter sodobnimi zahtevami informacijske znanosti (Žumer 2008, 129).

Upravljanje z dokumentarnim gradivom v javni/državni upravi vodijo z informacijskim sistemom in informacijsko tehnologijo, ki jo sestavljajo računalniško strojna in programska oprema ter storitve.

Uporaba interneta v javni upravi služi le v službene namene in je določena v skladu z določili informacijske varnostne politike organa. Sicer to določilo vsebuje sledeči zapis:

> *Ne smejo ga uporabljati za dostop ali prednost gradiva in podatkov, ki so žaljivi, nezakoniti, nevarni, škodljivi za ugled organa ali kako drugače neprimerni ali če bi povzročili odškodninsko odgovornost organa. Izjemoma ga lahko uporabljajo v zasebne namene, vendar to ne sme povzročati informacijskega tveganja in je dopustno le v obsegu, ki ne ovira ali ogroža normalnega delovnega procesa* (Žumer 2008, 133).

3.2 Urejenost informacijske zasebnosti v E-upravi

Informacijska zasebnost je v E-upravi ter na različnih spletnih straneh urejena z izjavo o varovanju osebnih podatkov[15]. Sicer spletna stran E-uprava ima to izjavo navedeno na sledeči način:

> *Zagotavljamo vam, da bomo vse podatke o vas, ki nam jih boste na kakršenkoli način posredovali, brezpogojno varovali ter ravnali z njimi v skladu z Zakonom o varstvu osebnih podatkov (ZVOP-1, Ur.l.RS št. 86/2004, 113/2005).Vaših podatkov ne bomo pod nobenim pogojem uporabili brez vašega privoljenja, jih kakorkoli posredovali ali dali v uporabo tretjim osebam ali institucijam, razen v primerih, ki jih določa zakon.*

15 E-uprava in varovanje osebnih podatkov : varstvo osebnih podatkov na Državnem portalu republike Slovenije

Kadar nam boste posredovali vaše podatke, bomo le te uporabili izključno za potrebe pošiljanja informacij, ki jih boste zahtevali. Zagotavljamo, da vaših osebnih podatkov ne bomo nikoli zlorabili, vam pošiljali nezaželene komercialne elektronske pošte ali kako drugače kršili vaše zasebnosti.
Vaši podatki ne bodo nikoli uporabljeni v namene, ki niso v skladu z zakonom, ali v namene, ki bi vam lahko kakorkoli škodovali. Vaši osebni podatki se bodo shranjevali in uporabljali le toliko časa, dokler bo to potrebno za dosego namena, zaradi katerega so bili obdelovani. Zagotavljamo vam, da bo dostop do vaših podatkov po izpolnitvi namena blokiran. (E-uprava 2009)

Kar se tiče same informacijske zasebnosti na E-upravi je, kot pravi Žumer (2008, 348), določeno, da mora vsaka organizacija določiti odgovorno osebo za spremljanje zakonodaje in redno izvajanje varnostnih pregledov. Sicer mora imeti tudi odgovorno osebo za varovanje informacij, neposredno odgovorno najvišjemu vodstvu ter naloge s področja varovanja informacij in opredelitve odgovornosti zaposlenih morajo biti opredeljene v opisu nalog in del.

Pri E-upravi je njihova informacijska zasebnost urejena z certifikati.Tu gre za elektronsko identifikacijo in overovitev uporabnikov in kontrolo dostopa. Če želite uporabljati E-upravo oziroma storitve, ki jih nudi sama E-uprava potrebujete certifikat ter digitalno potrdilo oziroma podpis. Identifikacija s potrdilom SIGENCA[16] deluje tako, da mora biti uporabnik preverjen oziroma identificiran s strani CA. Postopek poteka:

Kvalificirana digitalna potrdila se pridobijo na podlagi zahtevka, ki ga mora podpisati bodoči imetnik. Izpolnjen zahtevek se odda osebno na prijavno službo (seznam je objavljen na spletni strani http://www.sigen-ca.si/prijavne-slu.htm) ali pa se zahtevek digitalno podpiše z veljavnim kvalificiranim digitalnim potrdilom za fizične osebe, ki ga je imetniku izdal izdajatelj SIGEN-CA. Digitalno podpisan zahtevek se po elektronski poti posreduje izdajatelju SIGEN-CA (Sigen-ca 2009)

16 SIGENCA – digitalno potrdilo (Ministrstvo za javno upravo 2008).

SIGENCA je digitalno potrdilo, ki omogoča dostop do spletnih storitev. Spodaj je prikazan krog kako deluje digitalno potrdilo oziroma SIGENCA.

Slika 3.1 : Prikaz delovanja SIGENCE

vir:SIGOV-CA (2008).

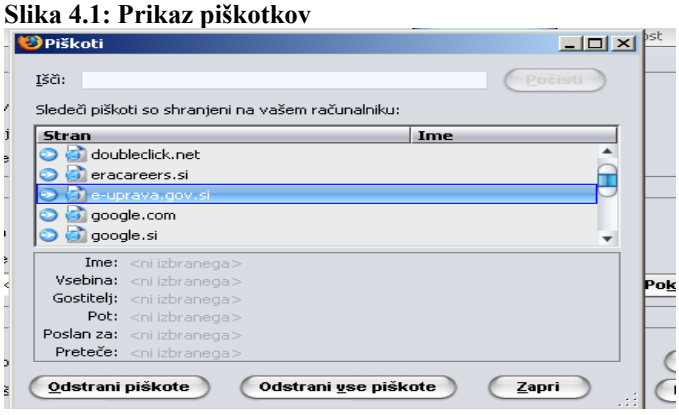
4 POGLAVJE : INFORMACIJSKA ZASEBNOST NA INTERNETU IN V E-UPRAVI

»Internet je kot del informacijskih tehnologij prišel v tisto dobo zrelosti, ko nas nova odkritja sama po sebi ne fascinirajo več tako kot nekoč, hkrati pa čutimo tako pozitivne kot negativne posledice njegove vseprisotnosti ter se o njih seveda vedno bolj sprašujemo in jih vrednotimo mimo začetnega navdušenja ali strahu nad novim.« (Ocvirk 2003)

Informacijska zasebnost na internetu se iz dneva v dan zmanjšuje, saj nas velika večina spletnih strani, katere obiskujemo, locira in se nam spletni naslovi shranjujejo v piškotke (ang. cookies). Piškotki se najpogosteje uporabljajo za ugotavljanje števila obiskov na spletni strani. So majhni paketi podatkov, ki jih spletni strežnik pošlje spletnemu brskalniku, ta pa jih shrani v uporabnikov računalnik in jih vrne strežniku, ko ta to zahteva od njega (Kovačič 2006, 148). Strežnik lahko nastavi čas veljavnosti piškotka in na podlagi tega se lahko tudi določa kateri del spletnega strežnika bo imel dostop do uporabnikovega računalnika oziroma piškotka na njegovem računalniku.

Ločimo več vrst piškotkov in sicer po času trajanja imamo sejne piškotke (ang. Session cookies) in trajne piškotke (ang. Persistent cookies). Torej, piškotek je dostopen strežniku toliko časa, dokler ga uporabnik ne izbriše. Pri tem pa moramo paziti, saj ločimo piškotke glede na obiskanost spletne strani (ang. First-party cookies) in piškotke, ki jih pošiljajo tretje spletne strani, ki so sicer vključene v obiskano spletno stran (ang. third-party cookies). Zadnji so namenjeni sledenju uporabnikov (Data Protection Working Party v Kovačič 2006, 148).

Slika 4.1: Prikaz piškotkov



vir: Firefox Mozilla 3.0.1 (2009).

In če dobro pogledamo sliko, ki je prikaz piškotkov, ugotovimo, da tudi spletna stran E-uprave zapisuje piškotke v naš računalnik.

Kako zagotoviti informacijsko zasebnost na internetu ter na E-upravi? Če pogledamo konstrukcijo spletne strani E-uprave in ponujenih storitev. In da za uporabo storitev potrebujem digitalni podpis ali pa digitalno potrdilo. Digitalna potrdila so lahko potencialno nevarna. Velika večina jih ima shranjene na računalniku brez kakršnekoli zaščite kot je šifriranje. Lahko rečemo tudi, da gre v bistvu za vprašanje varnosti terminalnih naprav[17]. In tudi marsikdo ima napisano svoje geslo na vidnem mestu. Za uporabo certifikatov moraš poskrbeti za svojo varnost ter varnost drugih.

»Evropska komisija je izrekla ultimat vsem medmrežnim podjetjem: če ta ne bodo v kratkem času izboljšala varovanja zasebnosti svojih uporabnikov, jim grozi zakonodaja, ki jih bo v to prisilila«(Kavs 2009).

Poleg certifikatov obstaja tudi časovni žig[18] in je uporaben, ko želimo v neki aplikaciji časovno žigosati nek elektronski dokument oziroma podatke, pošljemo strežniku z zgostitveno funkcijo narejen "povzetek" (hash) dokumenta oziroma podatkov (Si-tsa).

Način, kako izvajajo vse funkcije nadzora varovanja zasebnosti so sledeče. Torej, največjo skrb evropski komisiji povzročajo eksperimenti operaterjev s tehnologijami za vpogled v vsebino komunikacije (DPI – Deep Packet Inspection[19]), ki jih izkoriščajo za zbiranje podatkov o uporabniških navadah pri brskanju po svetovnem (Kavs 2009).

Glede na letno poročilo informacijskega pooblaščenca za leto 2005[20], Slovenija na področju varstva osebnih podatkov ne zaostaja za Zahodno Evropo, ZVOP-1 pa ureja nekatera področja varovanja osebnih podatkov celo bolje, kot v primerljivih državah. To velja predvsem za iznos osebnih podatkov v tretje države, za področje neposrednega trženja, videonadzora, evidentiranja vstopanja in izstopanja iz prostorov, povezovanja zbirk osebnih podatkov iz uradnih evidenc in javnih knjig ter strokovnega nadzora (Informacijski pooblaščenec 2006, 31). Kršitve po navedbah večinoma niso namerne, ampak so posledica slabega poznavanja zakonodaje. Poročilo kot najbolj kritična področja kršitev ZVOP-1 navaja v zvezi z vodenjem zbirk osebnih podatkov, kar opredeljuje 26. člen ZVOP-1 in v zvezi s

17 Varnost terminalnih naprav je odvisno od zaščite, ki jo imamo (Schneier 2006).

18 Časovni žig je strežnik za časovno žigosanje in je del infrastrukture javnih ključev (PKI) (Ministrstvo za javno upravo 2008).

19 DPI se zgodi, ko paket potuje skozi točko nadzora, ki išče odstopanja od protokola, viruse, spam, vdore ali prednastavljene kriterije s poočjo katerih se odloči, kaj naj naredi z nekim paketom. To vključuje tudi zbiranje statističnih podatkov. Takšno delovanje je v nasprotju s t.i. plitkim preverjanjem paketov (ki se običajno imenuje stateful packet inspection- SPI). Ta namreč samo preglejuje glave paketov (Wikipedia 2009).

20 Informacijski pooblaščenec: Letno poročilo o delu inšpektorata za varstvo osebnih podatkov v letu 2005. Ljubljana, 2006.

posredovanjem teh podatkov nadzornemu organu – 27. člen ZVOP-1. Med kršitelji je tudi veliko število državnih organov, kot so sodišča, organi lokalne samouprave in zdravstveni zavodi. Kot problematična področja poročilo izpostavlja področje videonadzora, kjer so pomanjkljivosti predvsem pri prijavi kataloga zbirke osebnih podatkov nadzornemu organu[21], manjkajoča opozorila o izvajanju videonadzora, ali pa predstojniki pred začetkom izvajanja videonadzora o tem niso izdali odločbe (Informacijski pooblaščenec 2006, 33).

Nadalje se pogoste kršitve pojavljajo v zvezi s prekomernim zbiranjem podatkov za namene neposrednega trženja, oziroma uporabe prevelikega števila osebnih podatkov, kar natančneje opredeljuje 72. člen ZVOP-1, v drugem odstavku. Problematični so tudi notranji akti, s katerimi bi naj upravljavci osebnih podatkov urejali ravnanje z zbirkami le-teh. Precej velik problem predstavlja tudi področje varovanja zbirk osebnih podatkov, na primer:

- neustrezno hranjenje dokumentacije
- neustrezno varovani prostori, v katerih se nahajajo nosilci osebnih podatkov
- neustrezno varovanje osebnih podatkov pri zbiranju s pomočjo interneta
- pošiljanje dokumentacije v neustrezno zavarovanih kuvertah
- računalniško vodene zbirke niso ustrezno varovane (gesla, avtorizacija)
- ni zagotovljena sledljivost obdelave osebnih podatkov
- neustrezno varovanje osebnih podatkov pri uničevanju dokumentacije, ki te podatke vsebuje oziroma malomarno uničevanje nosilcev z zapisi o osebnih podatkih.
- ugotovljen je bil tudi primer predaje računalnika z zbirko osebnih podatkov, pri kateri ni bilo poskrbljeno za uničenje teh podatkov pred predajo.

Med ostalimi kršitvami je še tudi posebej izpostavljeno prekomerno zbiranje osebnih podatkov, kar krši načelo sorazmernosti (Informacijski pooblaščenec 2006, 34-35).

Informacijska zasebnost predstavlja velik izziv zakonodajalcem in izvajalcem zakonodaje, predvsem pri zagotavljanju pravnih okvirov, ki bi lahko sledili hitremu razvoju tehnologije in v smislu primernega nadzora nad upoštevanjem zakonodaje s tega področja. Internet pomeni namreč še posebej težavno področje, saj ga je zaradi porazdeljene infrastrukture zelo težko nadzorovati in se kot tak ponuja kot idealna priložnost za vse, ki hočejo na protipravni način (in večinoma za protipravne namene) pridobivati osebne podatke

21 V kolikor so osebe na posnetku prepoznavne, se tak posnetek šteje za zbirko osebnih podatkov (ZVOP-1, 6.člen)

uporabnikov. Kot lahko vidimo iz poročila informacijskega pooblaščenca, se internet pri nas (še) ne izpostavlja kot posebej problematično področje, očitno je dosti dela z ostalimi, tudi tehnološko manj sofisticiranimi oblikami nepravilnosti glede na zbiranje in obdelavo osebnih podatkov. Vsekakor pa informacijska zasebnost v luči novih tehnologij in načinov zbiranja in obdelave podatkov pomeni tudi vedno bolj pomembno področje varovanja zasebnosti, saj se prostor zasebnega v zadnjem času vedno bolj krči in se vzpostavlja prostor nadzora – kot primer lahko navedemo primer v zadnjem času zelo popularnih in vseprisotnih video kamer, ki so si očitno izborile svoj prostor pod soncem, tudi na Fakulteti za družbene vede in ostalih fakultetah. Drug tak primer možnega vdora v informacijsko zasebnost pa je hramba prometnih podatkov o komunikacijah posameznika, ki se vzpostavlja na osnovi direktive EU o hrambi prometnih podatkov,[22] ki obsegajo:

- obvezno hrambo prometnih podatkov telefonskih in internetnih komunikacij (vključno z naslovi elektronske pošte) ter podatkov o lokacijah mobilnih telefonov;
- čas hrambe ne bo enak po celotni EU, znašal pa bo od 6 do 24 mesecev, poleg tega pa je dovoljen tudi daljši čas hrambe (Poljska je npr. predlagala 15 let);
- povračilo stroškov operaterjem nastalih zaradi obvezne hrambe prometnih podatkov ureja vsaka država po lastni presoji;
- omejitve za katera kazniva dejanja je mogoče shranjene podatke uporabiti niso določene (torej jih bo mogoče uporabiti tudi za boj proti kršitvam avtorske pravice);
- obvezna bo tudi hramba podatkov o neuspešnih poizkusih klicanja;
- neodvisna evalvacija ni predvidena;
- dodatni ukrepi za zaščito zasebnosti niso predvideni;
- nadzorni organ, ki bo bdel nad izvajanjem direktive ne bo vključeval predstavnikov organizacij za zaščito državljanskih pravic. (Slo-Tech 2005)

V nadaljevanju bomo z lastno raziskavo prikazali, koliko uporabniki vedo o svojih pravicah varovanja osebnih podatkov ter koliko ljudi zaupa in uporablja spletno stran E-uprava.

22 Direktiva Eu o hrambi prometnih podatkov - Direktiva 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES (EURLex 2006).

5 POGLAVJE: EMPIRIČNI DEL

»Porabljajte denar za nakup zasebnosti, saj vam v življenju večino časa ni dovoljeno, da bi bili normalni.« Johnny Depp

5.1 Opredelitev problema in ciljev raziskave

Za cilj v diplomskem delu smo si zastavili raziskati prednosti in nevarnosti uporabe internetnih podatkov za zasebnost posameznika v javni upravi oziroma v E-upravi.

Zastavili smo naslednjo tezo ter iz nje izpeljali hipoteze, ki jih bomo zavrnili ali potrdili. Teza diplomskega dela je sledeča:

Informacijska zasebnost na internetu in v E-upravi temelji na zasebnosti podatkov in njihovemu nadzoru.

To tezo lahko utemeljimo na primeru nadzora, ki ga je lepo opisal Kovačič v svoji knjigi Nadzor in zasebnost v informacijski družbi[23], saj pravi, da je Evropska unija najprej omogočila le hrambo prometnih podatkov, kasneje pa so dokazali, da so hranili še mnoge druge podatke, ki jih ne bi smeli.

Hipoteze izpeljane iz teze so sledeče:

1. Informacijska zasebnost na internetu je lahko ogrožena, če je zakonska regulacija tega področja pomanjkljiva in če ni neposrednega nadzora nad tem, kako se obstoječa pravila upoštevajo.
2. Uporabniki interneta vedo za zakon o varovanju osebnih podatkov, a vendar ga ne poznajo dovolj, zato je njihova informacijska zasebnost na internetu bolj ogrožena.

5.2 Metodologija

Na raziskovalne hipoteze smo poizkušali odgovoriti s pomočjo kvalitativne metodologije ter kvantitativne metodologije, ki se uporablja v družboslovnem raziskovanju.

Mesec kvalitativne podatke definira kot podatke, ki imajo vrednosti opisne narave, atributivne narave (Mesec 1998, 20). Izraz kvalitativne metode se uporablja kot krovni izraz

23 Kovačič, Matej. 2006, Nadzor in zasebnost v informacijski družbi.Ljubljana: Fakulteta za družbene vede

za različne pristope k raziskovanju družbe. Uporabljajo pa se naslednje metode: odprti intervju, opazovanje z udeležbo, skupinska razprava ipd. (Mesec 1998, 21).

Ragin, ki se v svojem delu Družboslovna raziskovanja ukvarja z naslovom: Enotnost in raznolikost metode, poglavje Kaj je družboslovno raziskovanje sprašuje, v čem se kvalitativno raziskovanje razlikuje od novinarstva in ostalih neznanstvenih dejavnosti. Sami smo poizkušali biti pri naših opazovanjih čimbolj temeljiti in se tudi poskušali oddaljiti od objekta opazovanja ter tako postati objektivni opazovalci.

Raziskovalno delo smo opravili z dvema metodama. Sicer z eno kvalitativno metodo polstrukturiranih kvalitativnih intervjujev ter s kvantitativno metodo kvantitativna anketa. Metode smo izbrali zaradi lažjega načina preučevanja odnosa ter obnašanja ljudi do informacijske zasebnosti in E-uprave. Nekatere informacije lahko namreč pridobimo zgolj skozi pogovor z javno pooblaščenko Natašo Pirc-Musar ter uporabniki, ki so se že kdaj srečali z E-upravo. Iz strani ministrstev zaradi nesodelovanja nismo pridobili nobenih podatkov oziroma smo pridobili en podatek, ki ne more pripomoči k izvedbi dokončne analize. Zato se nam je zdela triangulacija metod edini zares smiseln pristop k proučevanju.

5.2.1. Polstrukturirani oziroma kvalitativni intervju

Nestrukturirani ali polstrukturirani, neformalni intervjuji so bliže običajnemu pogovoru kot npr. anketni intervju.

Izpraševanec je aktivni udeleženec. Gre za vzajemno deljenje izkušenj. Izpraševanec se izraža kar se da "naravno", kot običajno. Vendar daje poudarek na perspektivo izpraševanca. Usmerja se ga le na teme, na katere se lahko že vnaprej pripravi ali pa v tiste teme, ki ga zanimajo.

Da izpraševalec pridobi vsa potrebna sredstva in intervjuvance, si mora na začetku zgraditi zaupanje ter dobiti osnovne informacije. Pri tem mora paziti, da gre postopno bolj v globino ali pa v dodatno preverjanje že povedanega.

Kvalitativni intervju je bliže »*prijateljskemu pogovoru*« kot pa anketni intervju. Saj tu ni jasnega konca in tudi intervju se lahko dokonča naslednjič (Kogovšek 2009).

Vprašanja v vprašalniku, ki je bil namenjen polstrukturiranemu intervjuju, so bila po priporočilih Alasuutarija postavljena tako, da z odgovori nismo mogli neposredno odgovoriti na hipoteze. Alasuutari (1995, 169) namreč trdi, da ne moremo preveriti zgolj s

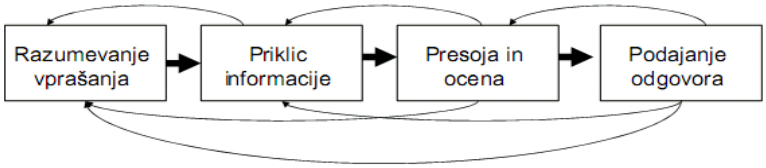
tem, da intervjuvance vprašamo, ali je naša interpretacija pravilna. Kar ne pomeni, da tega ne smemo vprašati.

Na podlagi intervjuja smo tako prišli do subjektivnih pogledov posameznikov. To predstavlja problem pri pridobivanju objektivnih dejstev, vendar omogoča boljši pogled v preučevani predmet.

5.2.2 Kvantitativna anketa

Anketa je sistematična metoda zbiranja podatkov s strani nekih oseb (vnaprej pripravljen standardiziran anketni vprašalnik). Za izbrane enote (običajno vzorec) zbiramo podatke o njihovih značilnostih (spremenljivkah). Enote niso nujno osebe. Na ta način konstruiramo kvantitativne (numerične) opise značilnosti večje skupine enot (populacije) (Lozar 2008). Proces odgovarjanja na anketno vprašanje:

Slika 5.1: Proces odgovarjanja



Vir: Groves (2004).

Na koncu bomo poizkusili združiti dognanja obeh metod in jih razložiti. Gola opažanja namreč še niso rezultat raziskave. Na podlagi zbranega gradiva, vodil, indicev, ki so zbrani, bomo podali še interpretativno razlago preučevanega fenomena. Pri tem bomo morali biti sposobni priti do odgovora, ki ni v nasprotju z nobenim opažanjem o raziskovanem predmetu (Alasuutari 1995, 16).

5.3 Opis raziskave

Izvedba ankete je potekala od 1.avgust 2009 do 25.avgust 2009 na spletu. Vzorec, ki smo ga izbrali je bil "snowball sample". Na podlagi efekta snežne kepe se ne more posplošiti na celotno populacijo. Z vprašalnikom smo preverjali, koliko so uporabniki interneta soočeni z varovanjem podatkov ter E-upravo. Anketo smo poslali po elektronski pošti prijateljem in ti so jo pošiljali naprej ostalim znancem in prijateljem, bila je tudi objavljena na Facebooku. Geografsko se je anketa izvajala po celi Sloveniji. Bila je zasnovana kot dva sklopa: zasebnost, varovanje podatkov ter E-uprava. Tretji sklop pa je bila demografija.

V prvem sklopu smo želeli izvedeti ali nam je zasebnost pomembna, ali poznamo zakonodajo v zvezi zakonom o varovanju osebnih podatkov ter ali vemo, da ne smejo drugi brez naše privolitve predajati osebnih podatkov naprej.

V drugem sklopu smo želeli izvedeti ali so uporabniki seznanjeni z spletno stranjo E-uprava in seveda, koliko jo uporabljalo ter ali imajo digitalno potrdilo oziroma podpis.

V tretjem sklopu smo zajeli demografijo. Anketirance smo spraševali po njihovi starosti, izobrazbi ter spolu.

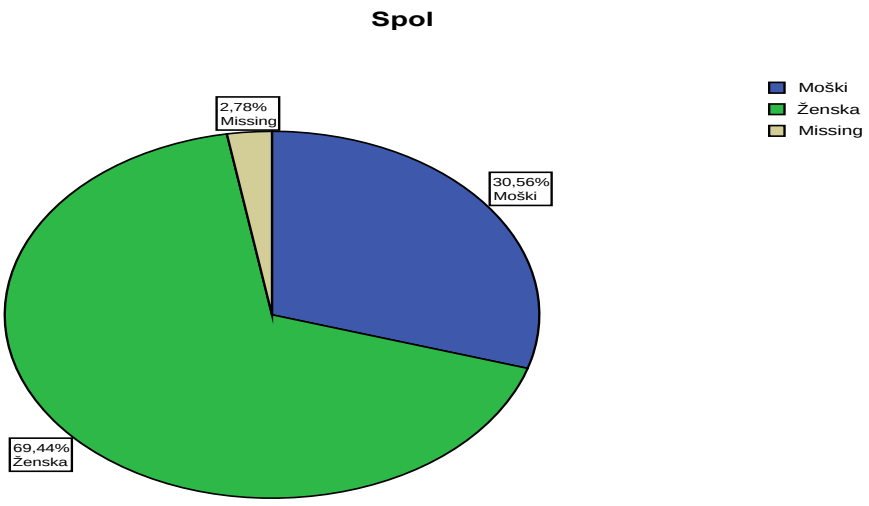
5.4 Interpretacija pridobljenih rezultatov

Na anketo je odgovarjalo 111 anketirancev, različnih starosti ter različne izobrazbe in različnega spola. Na tem pridobljenem številu odgovorov na anketo lahko naredimo posplošitev na vzorec populacije. Za pravo analizo bi potrebovali veliko večji vzorec ki bi moral biti drugače strukturiran.

5.4.1 Sodelujoči v anketi oziroma demografija

V anketi je sodelovalo 33 (29,7%) moških ter 75 (67,6%) žensk, 3 (2,7%) anketirancev ni podalo, katerega spola so.

Graf 5. 1: Delitev po spolu



vir: Priloga C, demografija

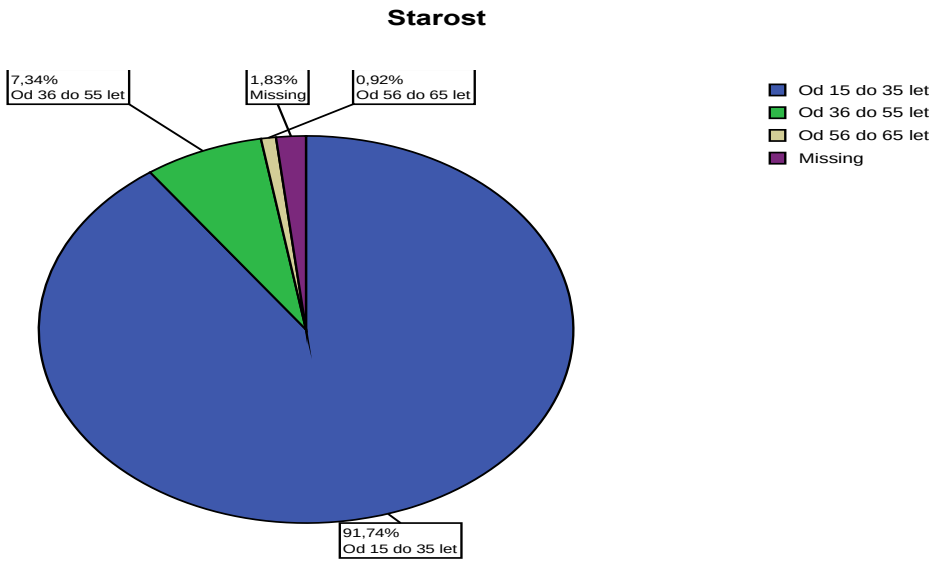
Sodelovali so uporabniki stari nad 15 let, ki pa smo jih razdelili v 4 skupine, vendar nekateri niso podali svoje starosti, tako da so bili prestavljeni v manjkajoče vrednosti. Vendar nad starostjo 66 let ni bilo nobenega uporabnika, zato odgovora ni podanega.

Table 5.1: Starostna struktura anketirancev

Starost(leta)	Frekvenca	Odstotek
Od 15 do 35	100	90,1
Od 36 do 55	8	7,2
Od 56 do 65	1	,9
Ni odgovora	2	1,8
skupaj	111	100,0

Vir: Priloga C, demografija

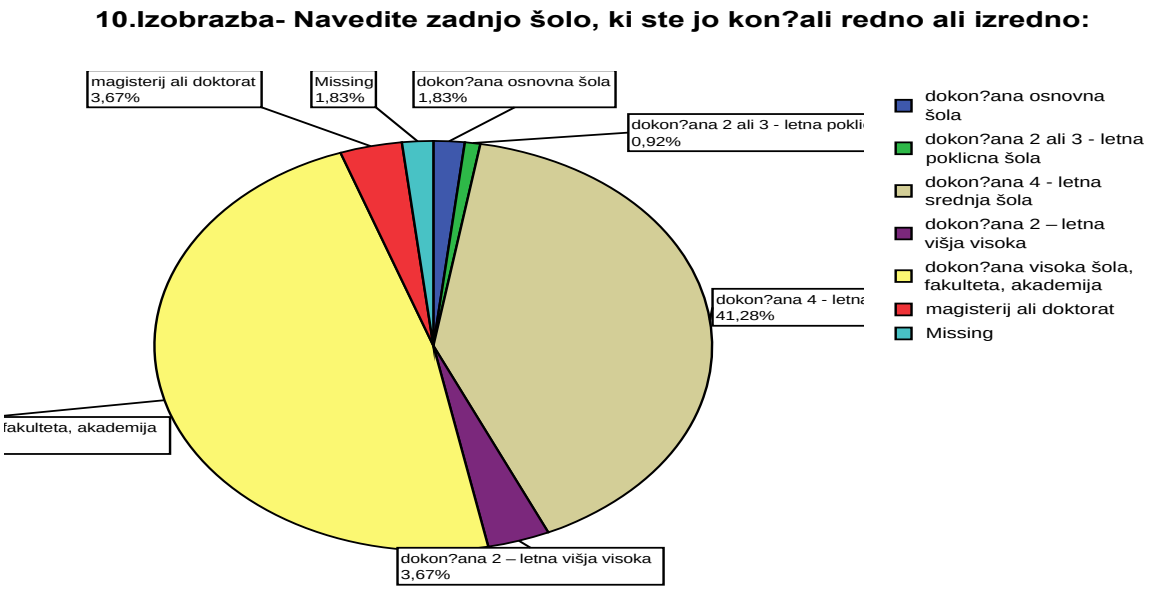
Graf 5.2: starostna struktura anketirancev



Vir: Priloga C, demografija

Po izobrazbeni strukturi smo anketirance razdelili v 6 skupin in sicer: dokončana osnovna šola (1,8%), dokončana 2 ali 3 - letna poklicna šola (0,9%), dokončana 4 - letna srednja šola (40,5%), dokončana 2 – letna višja visoka (3,6%), dokončana visoka šola, fakulteta (47,7%), akademija ter magisterij ali doktorat (3,6%). 2 anketiranca nista podala svoje dokončane izobrazbe.

Graf 5.3: Izobrazbena struktura anketirancev



Vir: Priloga C, demografija

5.4.2 Zasebnost in osebni podatki

V prvem delu ankete so bila vprašanja glede zaskrbljenosti o varovanju osebnih podatkov ter o zakonu o varovanju osebnih podatkov ter o hrambi namembnosti podatkov samih uporabnikov.

Na vprašanje o tem ali so zaskrbljeni, da njihovi podatki niso dovolj zavarovani pri različnih javnih in zasebnih organizacijah, ki zbirajo njihove podatke, je odgovorilo 111 anketirancev. Največ jih ji odgovorilo (47,7%), da »*jih do neke mere skrbi*« za varovanje osebnih podatkov glede organizacij. Na odgovora, »*da jih zelo skrbi*« in jih »*skrbi*« je skupno odgovorilo 36,9 % anketiranca ter da jih »*ne skrbi*« 15,3 % anketirancev.

Table 5.2: Zaskrbljenost glede varovanja podatkov

zaskrbljenost	Frekvenca	Odstotek	Kumulativni odstotek
da zelo skrbi	11	9,9	9,9
me skrbi	30	27,0	36,9
do neke mere skrbi	53	47,7	84,7
ne skrbi	17	15,3	100,0
skupaj	111	100,0	

Vir: Priloga C, vprašanje 1

Graf 5.4: Zaskrbljenost uporabnikov glede varovanje zasebnosti

Vir: Priloga C, vprašanje 1

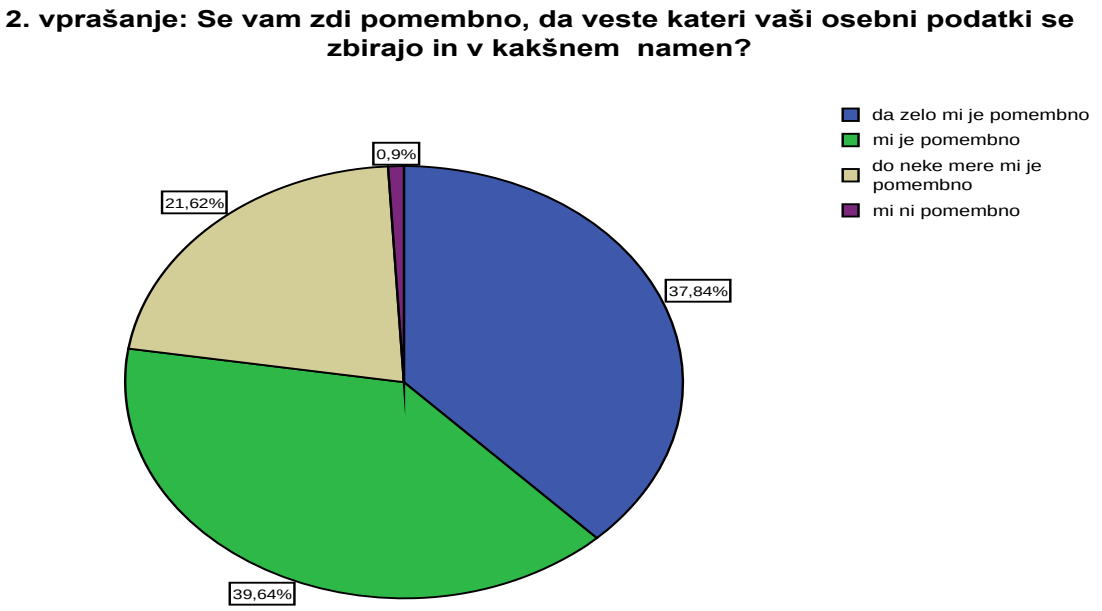
Iz pridobljenih podatkov vidimo, da uporabnike do neke mere skrbi zasebnost njihovih osebnih podatkov. Zato smo v naslednjem vprašanju spraševali o tem, ali jim je pomembno, da vedo, kateri osebni podatki se zbirajo in kakšen je njihov namen zbiranja. Na vprašanje »*Se vam zdi pomembno, da veste kateri vaši osebni podatki se zbirajo in v kakšnem namen*?« je kar 39,65% anketirancev odgovorilo, da jim je to pomembno, 37,8% je to zelo pomembno, le 0,9% anketirancem pa ni pomembno, v kakšen namen se zbirajo njihovi podatki in kateri podatki se zbirajo o njih.

Table 5. 3: Obveščenost uporabnikov o hrambi osebnih podatkov

pomembnost	frekvenca	Odstotek	Kumulativni odstotek
Zelo pomembno	42	37,8	37,8
pomembno	44	39,6	77,5
Do neke mere pomembno	24	21,6	99,1
Mi ni pomembno	1	,9	100,0
skupaj	111	100,0	

vir: Priloga C, vprašanje 2

Graf 5.5:Obveščenost uporabnikov o hrambi osebnih podatkov



vir: Priloga C, vprašanje 2

V naslednjem vprašanju nas je zanimalo ali uporabniki vedo, da se kakršnikoli osebni podatki ne smejo zbirati brez njihovega privoljenja. Dostikrat se zgodi, da se za razne javne marketinške namene izdajajo podatki, ki bi morali biti varovani. Tu predvsem namigujemo na podatke, ki so javno dostopni in se marketing okorišča z osebnimi podatki (telefonski imenik). Dobili smo odgovor »da« vedo za to, da s njihovi podatki ne smejo zbirati brez njihovega privoljenja v kar 92,8%, le 4,5 % anketirancev ni vedelo zato ter 2,7% anketirancev je odgovorilo, da zakonodaje o tem področju ne pozna.

Table 5.4: Vednost o zbiranju podatkov brez privoljenja

	Frekvenca	Odstotek	Kumulativni odstotek
da	103	92,8	92,8
ne	5	4,5	97,3
Ne vem	3	2,7	100,0
Skupaj	111	100,0	

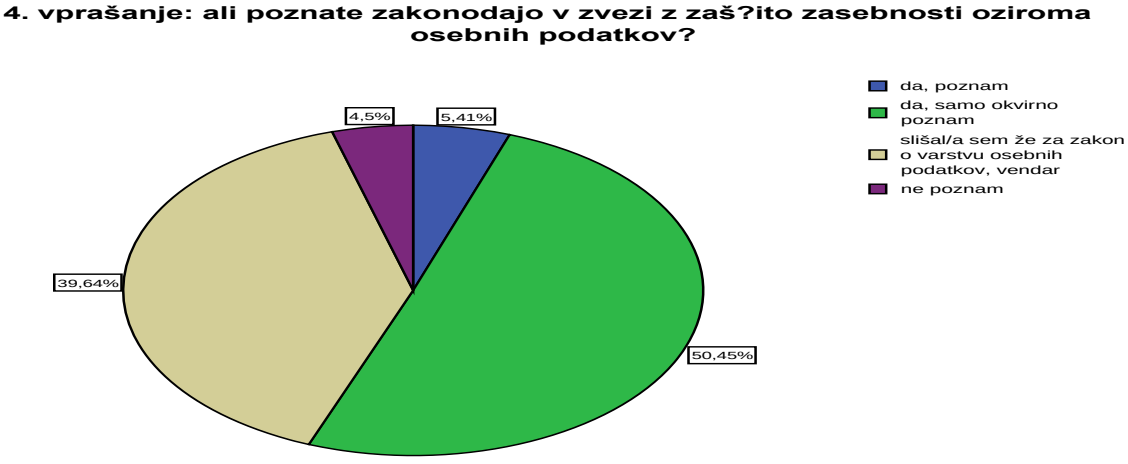
vir: Priloga C, vprašanje 3

Graf 5.6: Vednost o zbiranju podatkov brez privoljenja

vir: Priloga C, vprašanje 3

Glede na to, da smo anketirance v prejšnjem vprašanju spraševali o tem ali so seznanjeni z vednostjo zbiranja podatkov, smo bili pri naslednjem vprašanju prepričani, da velika večina pozna zakon, a vendar le v tem smislu, da so ga že videli in se ne podrobno spuščali vanj. To trditev smo tudi preverili in jo potrdili v tem smislu, da 50,5% anketirancev pozna zakon samo okvirno ter da je 39,6% anketirancev že slišalo za zakon, a se ni poglabljalo vanj. Presenetilo nas je to, da zakon pozna le 5,4% anketirancev in 4,5% anketirancev ne pozna zakona.

Graf 5.7: Poznavanje zakonodaje



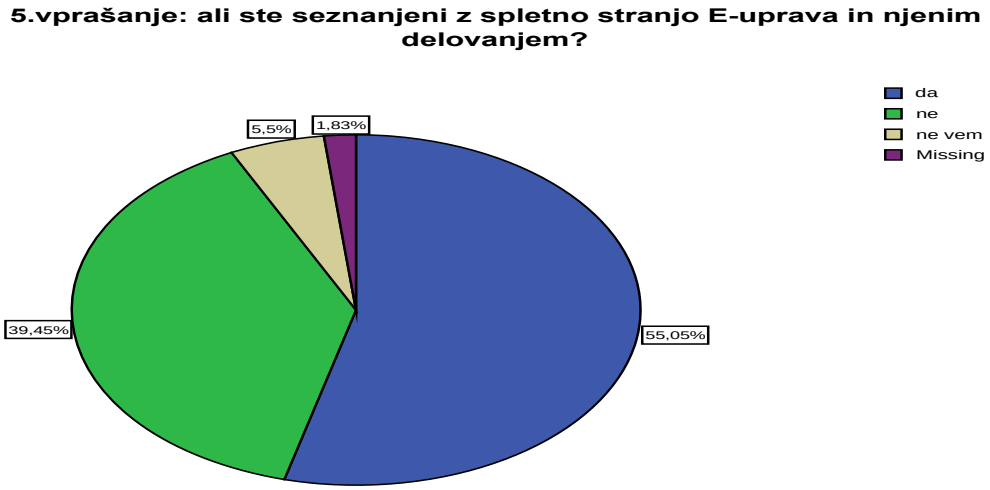
vir: Priloga C, vprašanje 4

5.4.3 E-uprava

V tem sklopu nas ja zanimalo ali uporabniki uporabljajo E-upravo ter ali so soočeni z njenim delovanjem. Zanimalo nas je tudi ali imajo digitalno potrdilo oziroma podpis s katerim lahko dostopajo do raznih aplikacij na spletni strani E-uprave.

Tu nas je najprej zanimalo ali so uporabniki soočeni z spletno stranjo E-uprava. In dobili smo naslednje odgovore. Kar 54,1% anketirancev pozna spletno stran E-uprava. To pomeni, da so že iskali razne podatke ter pregledovali spletno stran in jo morda tudi uporabljali v javne ali zasebne namene. Presenetil je odgovor, da se 38,7 % anketirancev še nikoli ni soočilo s spletno stranjo E-uprava in da 5,4% anketirancev ne ve, da spletna stran E-uprave obstaja. 1,8% anketirancev ni odgovorilo.

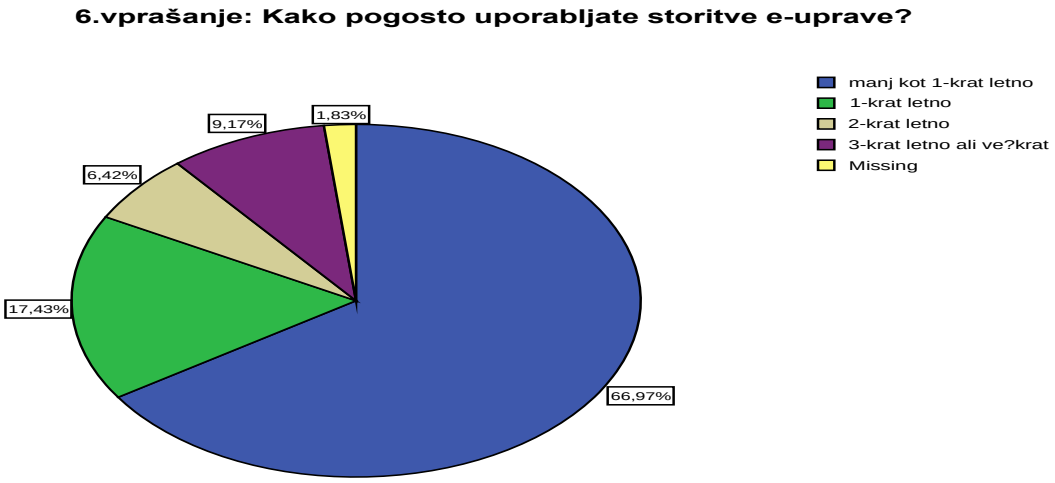
Graf 5.8: Seznanjenost z spletno stranjo E-uprava in njenim delovanjem



vir: Priloga C, vprašanje 5

V navezavi s tem vprašanjem smo tvorili vprašanje vsem, ki so seznanjeni s spletno stranjo E-uprava, in sicer, kako pogosto jo uporabljajo. Iz odgovorov razberemo, da manj kot enkrat letno uporablja spletno stran E-uprava kar 65,8 %, iz česar bi lahko sledilo, da so na njej iskali samo določene podatke in potem nikoli več. 1-krat letno uporablja spletno stran 17,1% anketirancev, 2-krat letno 6,3% anketirancev ter 3-krat letno ali več 9,0% anketirancev. 1,8% anketirancev ni podalo svojega odgovora.

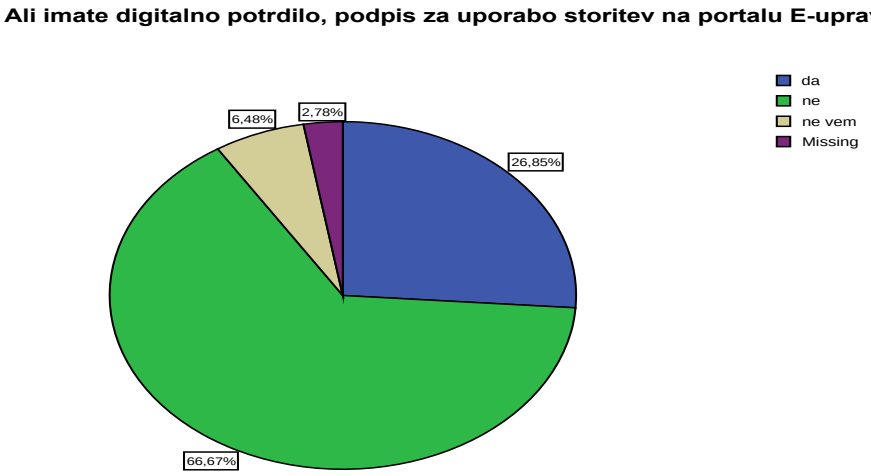
Graf 5.9: Uporaba spletne strani E-uprava



Vir: Priloga C, vprašanje 6

In če smo že povpraševali po tem ali poznajo in uporabljajo spletno stran E-uprava, smo se odločili še povprašati ali imajo digitalno potrdilo oziroma elektronski podpis. Kolikor vemo, so razni certifikati pomembni za dostop do podatkov kot so e-bančništvo (pri nas je to npr Klik), e-dohodnina, itd. Odgovori uporabnikov so bili sledeči: digitalno potrdilo ali podpis ima le 26,1% anketirancev, največji odstotek, in sicer 64,9% anketirancev, pa ga nima. Le 6,3% anketirancev ne ve ali ima digitalno potrdilo oziroma podpis. Pri tem pa moram opozoriti, da 2,7% anketirancev ni podalo nobenega odgovora.

Graf 5.10: Digitalno potrdilo da ali ne



vir: Priloga C, vprašanje 7

5.5 Sklepna ugotovitev

Iz raziskave lahko povzamemo, da je slovenskim uporabnikom interneta informacijska zasebnost pomembna. Glede varovanja zasebnosti ne izražajo prevelike zaskrbljenosti, saj jih je več kot polovica odgovorila, da jih do neke mere skrbi glede varovanja osebnih podatkov ter same informacijske zasebnosti. 15,7% je odgovorilo, da jih za varovanje osebnih podatkov in zasebnosti ne skrbi. Le manjši delež, 9,7% pa jih je odgovorilo, da jih skrbi glede varovanja zasebnosti in varovanja osebnih podatkov. Velika večina anketirancev ve, da podatkov brez njihovega privoljenja ne smejo posredovati naprej, še posebej če to delajo razne organizacije in seveda, tu gre tudi za to, da je treba spoštovati zakon o varovanju osebnih podatkov.

Raziskava torej potrjuje hipotezo, da »**uporabniki interneta vedo za zakon o varovanju osebnih podatkov, a vendar ga ne poznajo dovolj, zato je njihova informacijska zasebnost na internetu bolj ogrožena**.« Pri tem lahko izpostavim še, da s prihodom nove tehnologije in vseh groženj, ki pretijo, moramo sami poskrbeti, da se osebni podatki ne znajdejo v napačnih rokah. To pomeni, da se moramo zavedati komu posredujemo podatke ter katere pravice jim dopuščamo na podlagi osebnih podatkov.

5.6 Povzetek intervjuja z informacijsko pooblaščenko Natašo Pirc-Musar

Intervju je bil izveden preko elektronske pošte v mesecu avgustu. Razdelili smo ga na dva sklopa. Prvi se je nanašal na mesto kandidature ter o definiciji informacijske zasebnosti, drugi pa je temeljil na vprašanjih o nadzoru zakona in prihajajočih novosti glede tehnologije.

Na prvo vprašanje, zakaj se je odločila za kandidaturo informacijske pooblaščenke je bil njen odgovor zelo presenetljiv.

> *Predvsem zaradi neizmerno velikega izziva. Orati ledino na povsem novem pravnem področju je izziv za vsakega pravnika. Pravica dostopa do informacij javnega značaja je v slovenski pravni red »zakorakala« prvič šele leta 2003 in jaz sem imela priložnost popeljati jo do spoštovane temeljne človekove pravice. Varstvo osebnih podatkov, ki smo ga pod isto streho dobili leta 2006, pa je bil tudi poseben izziv, saj do takrat ta temeljna človekova pravica ni zaživela v praksi, ker enostavno ni bilo dovolj ljudi, ki bi zakon o varstvu osebnih podatkov lahko nadzirali. Danes po zaslugi vseh nas, ki delamo*

na uradu informacijskega pooblaščenca, obe pravici živita polno življenje pravi Pirc-Musarjeva(Glej priloga B).

Glede definicije informacijske zasebnosti, je Pirc-Musarjeva povedala, da „*varstvo osebnih podatkov definirano kot pravica posameznika, da se preprečijo nezakoniti in neupravičeni posegi v njegovo zasebnost in dostojanstvo pri obdelavi njegovih osebnih podatkov je za opredelitev, kaj sodi v pojem varstvo osebnih podatkov ključna* ***definicija osebnega podatka***." Vse to je dejansko na podlagi zakona ZVOP-1, ki opredeljuje kaj je osebni podatek in kako je opredeljen.

Število kršitev varovanja osebnih podatkov iz leta v leto narašča. Nataša Pirc-Musar pravi, da je bilo leta 2008 prijavljenih 635 zadev zaradi suma kršitev določb ZVOP-1 in sicer na javnem jih je bilo 256 ter v zasebnem sektorju 379 pritožb(Glej priloga B).

Na vprašanje, kako sankcionirajo kršitelje, pravi, da za ugotovljeni prekršek najprej izrečejo opozorilo, če je seveda storjeni prekršek neznatnega pomena in če pooblaščena uradna oseba oceni, da je glede na pomen dejanja opozorilo zadosten ukrep(vir: intervju). Za storjen težji prekršek pa sta sankciji globa, ki se lahko izreče tudi v obliki plačilnega naloga in opomin (Glej priloga B).

Na vprašanje o tem, da je zakon spisan tako, da si ga nekatere organizacije razlagajo po svoje, kot primer je bil naveden Univerzitetni Klinični Center Ljubljana, pravi, da varstvo osebnih podatkov ni privilegij zdravnika, temveč pravica posameznika. Pravi, tudi da se razmere v zdravstvenem sektorju izboljšujejo tudi zaradi zakona o pacientovih pravicah, ki je jasno določil, kdaj sme zdravnik posredovati podatke pacienta še komu drugemu (Glej priloga B).

Če je kršena informacijska zasebnost posameznika je posameznik lahko upravičen do opravičila ter tudi do odškodnine. Odškodnino dobi posameznik nazaj v primeru, če je bilo ugotovljeno, da

> *Je s protipravnim dejanjem (lahko je to prekršek ali kaznivo dejanje) posega v njegove osebnostne pravice (tudi pravico do varstva osebnih podatkov), skladno z določbami 134. člena Obligacijskega zakonika (Uradni list RS, št. 83/01 s spremembami, v nadaljevanju OZ) od sodišča zahteva, da prepreči takšno dejanje ali da odstrani njegove posledice. V primeru, da je posamezniku povzročena škoda (kar mora posameznik izkazati), pa lahko od povzročitelja skladno z določbami 179. in 181. člena OZ (Glej priloga B).*

Tu pa lahko tudi dodamo naslednje vprašanje tega sklopa, ki se nanaša na to vprašanje, saj prijave kršitev lahko prijavimo na strani informacijskega pooblaščenca ali pa tudi na inšpekcijski nadzor nad izvajanjem zakona.

Drugi sklop smo začeli z vprašanjem, kako lahko nadzorujejo ustanove, da ne kršijo zakona o varovanju zasebnosti podatkov se izvaja tudi neposredni inšpekcijski nadzor na izvajanjem predpisov s področja varstva osebnih podatkov(Glej priloga B).

O tem ali se bo zakon o varovanju osebnih podatkov začel spreminjati je povedala Nataša Pirc-Musar, da je »*zakon živa stvar in da se zaradi razvoja modernih informacijskih tehnologij bo osvežil. Pravi tudi, da bodo moderne tehnologije vse bolj posegale v zasebnost posameznika« (Glej priloga B).*

Glede biometrije pravi Nataša Pirc-Musar, da :

> *Se je potrebno zavedati, da biometrija ni le metoda ugotavljanja oz. preverjanja identitete, temveč je tehnologija, ki za svoj cilj uporablja človeško telo oziroma tiste telesne in vedenjske značilnosti vseh nas, ki so nespremenljive in samo nam lastne. Predvsem pri proizvajalcih in prodajalcih biometričnih sistemov obstaja zelo močna tendenca po trivializaciji zbiranja podatkov o človeških telesnih in vedenjskih značilnosti. Če pustimo ob strani vprašanja, ki so povezana s temeljno človekovo pravico do telesne celovitosti in dostojanstva, ima nekritična in nekontrolirana uporaba biometrije lahko zelo realne in resne posledice za vsakega posameznika (Glej priloga B).*

In tudi kar se tiče elektronskega cestninjenja pravi, da „*vključuje zbiranje in obdelavo velike količine osebnih podatkov posameznikov – predvsem informacije o njihovi lokaciji in času potovanja. Obdelava take količine podatkov pa glede na namen obdelave (ki je cestninjenje in ne sledenje posamezniku!) pomeni velik in pretiran poseg v zasebnost posameznika«* (Glej priloga B).

5.7 Sklepna ugotovitev

Na podlagi intervjuja z informacijsko pooblaščenko lahko potrdimo hipotezo ki pravi, da je **informacijska zasebnost na internetu je lahko ogrožena, če je zakonska regulacija tega področja pomanjkljiva in če ni neposrednega nadzora nad tem, kako se obstoječa pravila upoštevajo.** Na podlagi odgovora koliko pritožb so imela ministrstva v letu 2008 glede varovanja osebnih podatkov, smo sklepali, da zaradi tega niso želela sodelovati v raziskavi. Odgovor, ki ga je podala informacijska pooblaščenka je sledeči: »državne organe, ministrstva in organe v njihovi sestavi (102)*« (*Glej priloga B*).*

Informacijska zasebnost na internetu in v E-upravi temelji na zasebnosti podatkov in njihovemu nadzoru je glavna teza, ki je skupaj z hipotezami potrjena na podlagi ankete ter intervjuja z informacijsko pooblaščenko.

6 ZAKLJUČEK

Z modernizacijo tehnologij je potreba po dostopu do interneta iz dneva v dan večja. Brez interneta dejansko ne moremo več živeti. To pravimo zato, ker vse kar počnemo vsak dan, je del „matrice“, ki jo sestavlja milijon majhnih delcev in polno skrivnosti. Kot primer bi tu izpostavili Facebook. Spletna stran Facebook je socialno omrežje, kjer se zbirajo podatki, ki jih želiš objaviti in jih razkriti vsem svojim prijateljem ali neznancem. Sicer skrbijo za varovanje osebnih podatkov, vendar se z vsakim klikom, ki ga uporabnik izvede na spletni strani, nekomu nekje napiše nov podatek o njih. Zato je treba na straneh, ki zahtevajo vnos osebnih podatkov, biti zelo pazljiv in vedeti, da je vsaka informacija, ki je bila podana s strani uporabnika, lahko postane last ene ali več organizacij. Nikoli ne ve točno, kaj se skriva v ozadju.

V mislih so nam ostale besede informacijske pooblaščenke, da se vsaka zloraba lahko prijavi in da ima vsaka prijava svoje posledice.

Če pomislimo koliko prekrškov se zgodi letno in koliko se jih bo še dogajalo tekom razvoja moderne tehnologije, ki še ni dosegla svojega vrha. In kolikokrat postanemo tarče zlorab varovanja osebnih podatkov od organizacij, katerim naj bi zaupali.

Na podlagi vseh teh pomislekov, ki se nas lotevajo smo izvedli spletno anketo, ki nam je potrdila hipotezo, da uporabniki interneta vedo za zakon o varovanju osebnih podatkov, a vendar ga ne poznajo dovolj, zato je njihova informacijska zasebnost na internetu bolj

ogrožena. So to raziskavo smo hoteli prikazati, koliko vedo uporabniki o svojih pravicah in o zakonu varovanja osebnih podatkov. Ter ali vedo za vse morebitne podrobnosti, da se osebni podatki brez njihovega privoljenja ne smejo posredovati naprej drugim organizacijam ter ustanovam, ki bi mogoče njihove osebne podatke zlorabili v marketinške namene. V raziskavi smo tudi povpraševali o spletni strani E-uprava. Predvsem nas je zanimalo koliko anketirancev redno obiskuje spletno stran E-uprava in koristi spletne storitve na prej imenovani spletni strani. In vključno s tem smo tudi pridobili odgovore, koliko anketirancev ima digitalno potrdilo oziroma podpis, da lahko uporablja storitve E-.uprave.

Poleg ankete smo izvedli tudi intervju z informacijsko pooblaščenko Natašo Pirc-Musar, ki nam je z odgovori na vprašanja potrdila še drugo zastavljeno hipotezo, ki se nanaša na informacijsko zasebnost. In sicer informacijska zasebnost na internetu je lahko ogrožena, če je zakonska regulacija tega področja pomanjkljiva in če ni neposrednega nadzora nad tem, kako se obstoječa pravila upoštevajo. To se nanaša na zakon o varovanju osebnih podatkov. Informacijska pooblaščenka je lepo potrdila, da je v Sloveniji zakonska regulacija urejena in da imamo tudi nadzor nad zakonom in njegovem upoštevanju. Čeprav se zgodi, da tudi nimamo neposrednega nadzora nad izvajanjem zakona, se morajo obstoječa pravila še vedno upoštevati.

Iz raziskovanja smo lahko potrdili tudi tezo, ki smo si jo zastavili tako, da informacijska zasebnost na internetu in v E-upravi temelji na zasebnosti podatkov in njihovemu nadzoru. To se je razločno pokazalo v spletni anketi ter tudi v intervjuju z informacijsko pooblaščenko.

Na podlagi celotne analize besedil in izvedene ankete ter intervjuja smo ugotovili, da so uporabniki tisti, ki morajo skrbeti, da bodo osebni podatki v pravih rokah. Da morajo vedeti, kaj pomeni zakon o varovanju osebnih podatkov in kakšne so lahko morebitne sankcije in postopki prijave, če se zgodi kršitev zakona o varovanju osebnih podatkov.

In kot smo omenili že na začetku, so številne zbirke osebnih podatkov, ki jih hranijo podjetja, razne organizacije, društva, ipd., verjetno sploh nemogoče v celoti ustrezno nadzorovati oziroma nadzorovati njihove upravljavce, da s podatki, ki so jim zaupani, ravnajo v skladu z veljavno zakonodajo. In dokler se bo zakon spreminjal ne bomo mogli do potankosti nadzorovati organizacij, se bomo morali sami soočati s problemi in na najboljši način zavarovati osebne podatke.

LITERATURA

- Alasuutari, Pertti. 1995. *Researching Culture. Qualitative Metod and Cultural Studies*. London, Thousand Oaks, New Delhi: Sage Publications.
- Batagelj, Teja, Tadej Gabrijel, Helena Gregorc, Dušan Kričej, Roman Rep, Davorka Šel, Renata Zatler, Tatjana Mizori Zupan in Maja Zupančič. 2008. *E-uprava: zavezništvo z uporabnik*i. Ljubljana: Založba Pasadena.
- Berce, Jaro. 2005. Značilnosti in vplivi uvajanja modernih tehnologij in organizacijskih pristopov v državni upravi. V *Učinki informacijsko komunikacijskih tehnologij*, ur. Metka Stare in Maja Bučar, 153-170. Ljubljana: Fakulteta za družbene vede.
- Butler, Jeremy G. 1997. *A History of Information Technology and Systems*. The university of Alabama. Dostopno prek: http://www.tcf.ua.edu/AZ/ITHistoryOutline.htm (2. maj 2009).
- Cimolini, Črt. 2003. *Elektronska uprava v Sloveniji*. Diplomsko delo. Ljubljana: Fakulteta za družbene vede. Dostopno prek: http://dk.fdv.uni-lj.si/dela/Cimolini-Crt.PDF (1. maj 2009).
- *Direktiva Evropskega parlamenta in Sveta 95/46/ES o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov, z dne 24. oktobra 1995.* Dostopno prek:
- Državni portal republike Slovenije. 2009.*E-uprava in varovanje osebnih podatkov*. Dostopno prek: http://e-uprava.gov.si/e-uprava/portalStran.euprava?pageid=42 (25.avgust 2009).
- Dujić, Sladjan. 2007. Zagotavljanje večje ekonomičnosti poslovanja javne uprave s pomočjo odprtokodnih in prostih programskih rešitev. V *Elektronsko upravljanje in poslovanje v službi uporabnika = E-governance and E-business at the service of customer*, ur. Uroš Pinterič in Uroš Svete, 207-228. Ljubljana: Fakulteta za družbene vede.
- Edkins , Jo. 2007. *Abacus*. Dostopno prek: http://gwydir.demon.co.uk/jo/numbers/machine/abacus.jpg (30. maj 2009).
- Egan, Mark. 2005. *Varnost informacij: grožnje izzivi in rešitve: vodnik za podjetja.* Ljubljana: Založba Pasadena.

- E-Uprava. 2009. *Varstvo osebnih podatkov na Državnem portalu Republike Slovenije*. Dostopno prek: http://e-uprava.gov.si/e-uprava/portalStran.euprava?pageid=42 (1. maj 2009).
- EURLex. 2006.*Direktiva Eu o hrambi prometnih podatkov*. Dostopno prek: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:SL:HTML (28.avgust 2009)
- Gantar, Pavel. 2004. Informacijska družba- izzivi in realnost za Slovenijo. *Teorija in praksa* 41 (1-2): 212-219.
- Generalna skupščina OZN. 1948. *Splošna deklaracija o človekovih pravicah.* Sprejeta dne 10. december. Dostopno prek: http://www.ip-rs.si/index.php?id=221 (25. avgust 2009).
- Groves. 2004. *Survey Methodology. Wiley series in survey methodology.* New Yersy: Hoboken http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:006:SL:HTML (25. maj 2009).
- Informacijski pooblaščenec. 2005. Dostopno prek: http://www.ip-rs.si/varstvo-osebnih-podatkov/informacijske-tehnologije-in-osebni-podatki/varstvo-osebnih-podatkov-na-internetu/ (27. maj 2009) .

  --- 2006. *Letno poročilo o delu inšpektorata za varstvo osebnih podatkov v letu 2005.* Dostopno prek: http://www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/letna_porocila_2006.pdf (27.maj 2009)

  --- 2008. *Smernice za zavarovanje osebnih podatkov v informacijskih sistemih bolnišnic.* Dostopno prek: http://www.ris.org/uploadi/editor/1234435464Smernice_za_zavarovanje_OP_v_IS_bolnisnic_15022008.pdf (26. julij 2009).
- Jalušič, Vlasta.1996. *Hannah Arendt: Politika kot možnost*. Ljubljana: Krtina.
- Jerman-Blažič, Borka. 2001. *Elektronsko poslovanje na internetu*. Ljubljana: Gospodarski vestnik.
- Kavs, Barbara.2009**.** *Evropska komisija odločno tudi za varovanje zasebnosti na spletu***.** Dostopno prek: http://www.e-demokracija.si/2009/04/06/evropska-komisija-odlocno-tudi-za-varovanje-zasebnosti-na-spletu/ (06. april 2009).

- *Kazenski zakonik Republike Slovenije* (KZ). Ur. l. RS 63/1994 (70/1994), 60/1999, 40/2004, 37/2005, 16/2006. Dostopno prek: http://zakonodaja.gov.si/rpsi/r05/predpis_ZAKO905.html (25. maj 2009).
- *Kazenski zakonik Republike Slovenije* (KZ-1). Ur. l. RS 55/2008. Dostopno prek: http://www.uradni-list.si/1/objava.jsp?urlurid=20082296 (25. maj 2009).
- KKU Web hosting. 2009. *1951 univac* . Dostopno prek: http://std.kku.ac.th/4830503256/New%20Folder/1951_univac_large.jpg (20. avgust 2009).
- Kogovšek, Tina. 2009. *Predavanje 4*. Dostopno prek: http://kogovsek.fdvinfo.net/uploadi/editor/1224774430OKM_4.ppt (25.junij 2009).
- *Konvencija o varstvu človekovih pravic in temeljnih svoboščin.* Uradni list RS(13.6.1994) MP, št.7-41/1994 (RS 33/1994). Dostopno prek: http://www.varuh-rs.si/index.php?id=108 (25. maj 2009).
- Kovačič Matej. 2000. Zasebnost v informacijski družbi. *Teorija in praksa* 37 (6): 1019-1034. Dostopno prek: http://dk.fdv.uni-lj.si/tip/tip20006kovacic.PDF (25. maj 2009).

  --- 2003. *Nadzor in zasebnost v informacijski družbi*. Diplomsko delo. Ljubljana: Univerza v Ljubljani, Fakulteta za družbene vede (25. maj 2009).

  --- 2003. *Zasebnost na internetu*. Ljubljana: Mirovni inštitut. Dostopno prek: http://www2.mirovni-institut.si/slo_html/publikacije/pdf/MI_politike_zasebnost_na_internetu.pdf (25. maj 2009).

  --- 2006. *Nadzor in zasebnost v informacijski družbi: filozofski, sociološki, pravni in tehnični vidiki.* Ljubljana: Fakulteta za družbene vede. Dostopno prek: http://dk.fdv.uni-lj.si/eknjige/EK_Kovacic_2006_Nadzor.pdf (25. maj 2009).
- Kričej, Dušan. 2002. *E-uprava na dlani*. Ljubljana: Založba Pasadena.
- Leben, Marija. 2007. *Trendi razvoja E-uprave v Sloveniji*. Dostopno prek: http://www.ris.org/uploadi/editor/1233562098UpravaDec04-LebenKunstelj.pdf (25. maj 2009).
- Lenarčič, Blaž. 2003. *Matej Kovačič*: *Zasebnost na internetu.* Ljubljana: Mirovni inštitut Dostopno tudi na: http://dk.fdv.uni-lj.si/dr/dr45Lenarcic.PDF (30. junij 2009).
- Lozar, Manfreda. 2008. *Predavanja 1*. Dostopno prek: anket.fdvinfo.net (25.junij 2009).

- Mali, Judita. 2007. *E-uprava*. Diplomsko delo. Ljubljana: Ekonomska fakulteta. Dostopno prek: http://www.cek.ef.uni-lj.si/u_diplome/mali2713.pdf (30. junij 2009).
- Mesec, Blaž. 1998. *Uvod v kvalitativno raziskovanje v socialnem delu*. Ljubljana: Visoka šola za socialno delo.
- Ministrstvo za javno upravo. 2008. *Časovni žig.* Dostopno prek: http://www.si-tsa.gov.si/navodila.php (30. avgust 2009)

  ---2008. *Elektronski podpis*. Dostopno prek: http://www.mju.gov.si/si/pogosta_vprasanja/?type=98 (23.avgust 2009).

  --- 2009. *SIGENCA – Digitalno potrdilo*. Dostopno prek: http://www.sigen-ca.si/ (30.avgust 2009).

  --- 2009. *Pogosta vprašanja.* Dostopno prek : http://www.mju.gov.si/si/pogosta_vprasanja/?type=98 (23. avgust 2009).

- Musar-Pirc, Nataša in Klemen Mišič. 2008. *Vodič pri varstvu osebnih podatkov za starše in učitelje.* Dostopno prek: http://www.ris.org/uploadi/editor/1234436078Brosura_ucitelji_koncna_CMYK.pdf (27. julij 2009).
- Ocvirk, Vasja. 2003. *Zasebnost na internetu ni zgolj tehnološko vprašanje.* Dostopno prek http://www.nasvet.com/zasebnost-internet/ (23. avgust 2009).
- Pestotnik, Andreja. 2007. *Zasebnosti in mobilni telefoni*.Diplomsko delo. Ljubljana: Fakulteta za družbene vede. Dostopno prek: http://dk.fdv.uni-lj.si/diplomska/pdfs/Pestotnik-Andreja.PDF (30. maj 2009).
- Pinterič, Uroš in Uroš Svete. 2007. *Elektronsko uporabljanje in poslovanje v službi uporabnika= e-governance and e-bussiness at the service of customer*. Ljubljana: Fakulteta za družbene vede.
- Pirc-Musar, Nataša. 2009. Intervju z avtorico. Ljubljana, 20.avgust.
- Pivec, Franci. 2004. *Informacijska druž*ba. Ljubljana: Frontier. Dostopno prek:http://www.ris.org/uploadi/editor/pivec_id.pdf (26. julij 2009).
- Praprotnik, Darja. 2006. *Varovanje podatkov in zasebnosti na internetu.* Magistrsko delo. Ljubljana: Ekonomska fakulteta. Dostopno prek: http://www.cek.ef.uni-lj.si/magister/praprotnik2867.pdf (26. julij 2009).
- Pravna fakulteta v Mariboru. 2008. *Pravna informatika*. Dostopno prek: http://www.pf.uni-mb.si/pravna_informatika/kazalo_predgovor.html (24. april 2009).

- Ragin, Charles. 2007. *Družboslovno raziskovanje: Enotnost in raznolikost metode*. Ljubljana: Fakulteta za družbene vede.
- Scheiner, Bruce. 2006. *Varnost terminalnih naprav*. Dostopno prek: http://www.schneier.com/blog/archives/2006/08/updating_the_tr.html (30.avgust 2009)
- SI- TSA.2009. *Navodila za uporabo storitev SI-STA.* Dostopno prek: http://www.si-tsa.gov.si/navodila.php (30. avgust 2009).
- SIGEN-CA. 2009. *Potek postopka sigenca.* Dostopno prek: http://www.sigen-ca.si/politika-sigen-ca-fizicne-osebe.php *(*30. avgust 2009 *).*
- SIGOV-CA. 2008. *Vloga prijavnih služb za javno upravo*. Dostopno prek: http://www.sigov-ca.gov.si/images/vloga-prijavnihSluzb-zaJU.gif (30. julij 2009).
- Skrt, Rados. 2003. *E-uprava.* Gospodarski vestnik, članek. Dostopno prek: http://www.nasvet.com/doc/e-uprava.php (29.april 2009).
- Slovenska Wikipedia. 2009 .*Logaritemsko računalo.* Dostopno prek: http://sl.wikipedia.org/wiki/Logaritemsko_ra%C4%8Dunalo (30. julij 2009).

  --- 2009. *Informacijska tehnologija.* Dostopno prek: http://sl.wikipedia.org/wiki/Informacijska_tehnologija (24. april 2009).
- Stare, Metka in Maja Bučar. 2005. *Učinki informacijsko-komunikacijskih tehnologij*. Ljubljana: Fakulteta za družbene vede.
- Svete, Uroš in Uroš Pinterič. 2008. *E- država: upravno- varnostni vidik*i. Nova Gorica: Fakulteta za družbene študije.
- The Krysstal Web site. 2000. *Cuniform*. Dostopno prek: http://www.krysstal.com/writing_cuniform.html (15.avgust 2009).
- Tocp. 2007. *Pascaline.* Dostopno prek: http://www.thocp.net/hardware/pascaline.htm (30.julij 2009).
- Toplišek, Janez. 1998. *Elektronsko poslovanje*. Ljubljana: Atlantis.
- Uradni list. 2004. *Zakon o elektronskem poslovanju in elektronskem podpisu* . Dostopno prek: http://zakonodaja.gov.si/rpsi/r01/predpis_ZAKO4161.html (30.avgust 2009).

  --- 2004. *Kazenski zakonik (KZ-UPB1). Ur. l. RS 95/2004.* Dostopno prek: http://www.uradni-list.si/1/objava.jsp?urlid=200495&stevilka=4208 (2. junij 2009).

  --- 2009. Dostopno prek: http://www.uradni-list.si/uploads/VSEBINAe-demokracija.pdf (1. avgust 2009).

- Ustava Republike Slovenije /URS/. (Ur.l. URS) 42/1997, 66/2000, 24/2003, 69/2004, 69/2004, 69/2004, 68/2006. Dostopno preko: http://zakonodaja.gov.si/rpsi/r01/predpis_USTA1.html (26. maj 2009).
- Varuh človekovih pravic. 2007. *Splošna deklaracija o človekovih pravicah iz leta 1948*. Dostopno prek: http://www.varuh-rs.si/index.php?id=102 (25.avgust 2009).
- Vidic, Matjaž. 2006. *Uporaba e-uprave na Ministrstvu za notranje zadeve.* Seminarska naloga. Dostopno prek: http://www.ris.org/uploadi/editor/1235311354e-uprava_na_mnz_vidic.pdf (27. julij 2009).
- Vlada Republike Slovenije. 2007. *Strategija razvoja informacijske družbe v Sloveniji – si2010.* Ljubljana. Dostopno prek: http://www.mvzt.gov.si/fileadmin/mvzt.gov.si/pageuploads/pdf/informacijska_druzba/si2010.pdf (25. maj 2009).
- Wikipedia. 2009. *G2G.* Dostopno prek: http://en.wikipedia.org/wiki/Government_to_Government (23.avgust 2009).

  --- 2009. *IBM and the Holocaust.* Dostopno prek : http://en.wikipedia.org/wiki/IBM_and_the_Holocaust (30.avgust 2009).

  --- 2009. *Zakon Justices of Peace Act.* Dostopno prek: http://en.wikipedia.org/wiki/Justice_of_the_peace(25.avgust 2009).

  --- 2009.*DPI.* Dostopno prek: http://en.wikipedia.org/wiki/Deep_packet_inspection (30.avgust .2009)
- *Zakon o varstvu osebnih podatkov* (ZVOP-1). Ur.l. RS, 86/2004, 113/2005. Dostopno prek: http://zakonodaja.gov.si/rpsi/r06/predpis_ZAKO3906.html (5. maj 2009).
- Zlok. 2009. *IBM logo design history.* Dostopno prek: http://www.zlok.net/blog/wp-content/uploads/ibm4.jpg (27. julij 2009).
- Žumer, Vladimir. 2008. *Poslovanje z zapisi: upravljanje in hramba dokumentarnega gradiva, klasifikacijski načrt za razvrščanje gradiva z roki hrambe in elektronska hramba gradiva v digitalni obliki.* Ljubljana: Planet,GV.

PRILOGE

Priloga A: Intervju z pooblaščenko
I.sklop: O mestu kandidature ter o definiciji informacijske zasebnosti

1. Kako to, da ste se odločili za kandidaturo za mesto informacijske pooblaščenke?
2. Kako definirate informacijsko zasebnost (kaj vse po vašem sodi zraven in kaj ne sodi zraven)?
3. Koliko prijav glede kršitve varovanja osebnih podatkov prejmete po vaši oceni? Majhno, veliko?
4. Kako sankcionirate kršitelje?
5. Zakon o varovanju osebnih podatkov je napisan na tak način, da si ga nekatere organizacije razlagajo po svoje, npr. klinični center. Kaj menite o tej situaciji?
6. Če je kršena posameznikova informacijska zasebnost, ali je oškodovanec upravičen do opravičila, odškodnine?
7. V primeru, da se zgodi kršitev varovanja osebnih podatkov, na koga se torej naprej obrnemo - na vas, na koga drugega in na kakšen način lahko to storimo?

II.sklop: Nadzor zakona in prihajajoče novosti glede tehnologij

8. Kako lahko nadzorujete ustanove, da ne kršijo zakona o varovanju zasebnosti podatkov?
9. Ali se bo zakon o varovanju osebnih podatkov začel kaj spreminjati in če se bo, v katerih točkah se bo spremenil?
10. Kakšno morebitno grožnjo predstavljata biometrija ter satelitsko cestninjenje varnosti osebnih podatkov? S katerimi ukrepi se bodo preprečevale zlorabe osebnih podatkov?

Priloga B: ODGOVORI NA VPRAŠANJA

1. Kako to, da ste se odločili za kandidaturo za mesto informacijske pooblaščenke?

Predvsem zaradi neizmerno velikega izziva. Orati ledino no povsem novem pravnem področju je izziv za vsakega pravnika. Pravica dostopa do informacij javnega značaja je v slovenski pravni red »zakorakala« prvič šele leta 2003 in jaz sem imela to priložnost popeljati jo do spoštovane temeljne človekove pravice. Varstvo osebnih podatkov, ki smo ga pod isto streho dobili leta 2006, pa je bil tudi poseben izziv, saj do takrat ta temeljna človekova pravica ni zaživela v praksi, ker enostavno ni bilo dovolj ljudi, ki bi zakon o varstvu osebnih podatkov lahko nadzirali. Danes po zaslugi vseh nas, ki delamo na Informacijskem pooblaščencu, obe pravici živita polno življenje.

2. Kako definirate informacijsko zasebnost (kaj vse po vašem sodi zraven in kaj ne sodi zraven)?

Informacijska zasebnost oziroma *varstvo osebnih podatkov* je pravica posameznika, da se preprečijo nezakoniti in neupravičeni posegi v njegovo zasebnost in dostojanstvo pri obdelavi njegovih osebnih podatkov. Je pravica posameznika, da ima nadzor nad zbiranjem, obdelavo in posredovanjem njegovih osebnih podatkov, je pravica posameznika, da ve, kje vse se njegovi podatki nahajajo in s kakšnim namenom se jih obdeluje.

Informacijska zasebnost je del širše pravice do zasebnosti, ki vključuje tudi zasebnost v prostoru (vsak posameznik ima pravico do svobodnega nenadzorovanega gibanja in pravico do zasebnosti bivališča/stanovanja) in komunikacijsko zasebnost (pravica posameznika, da se nezakonito in neupravičeno nihče ne seznani z vsebino sporočila, ki ga posreduje ali prejme prek kateregakoli komunikacijskega sredstva; da svobodno odloča o tem, komu, v kakšnem obsegu, na kakšen način in pod katerimi pogoji bo posredoval določeno sporočilo).

Informacijska zasebnost je torej načeloma vezana le na osebne podatke, ki se nanašajo na posameznika, in ne tudi na ostale vidike zasebnosti. Moramo pa se zavedati, da se v sodobnem svetu, kjer stalno puščamo elektronske sledi, ti vidiki zasebnosti prepletajo: podatki o lokaciji posameznika, ki jih lahko razberemo iz sledenja lokaciji njegovega mobilnega telefona, sicer spadajo med osebne podatke, pa vendar pri nezakoniti obdelavi teh

podatkov ni storjen le poseg v informacijsko zasebnost posameznika, pač pa tudi v njegovo širšo pravico do zasebnosti v prostoru in gibanju.

Ker je varstvo osebnih podatkov definirano kot pravica posameznika, da se preprečijo nezakoniti in neupravičeni posegi v njegovo zasebnost in dostojanstvo pri obdelavi njegovih osebnih podatkov je za opredelitev, kaj sodi v pojem varstvo osebnih podatkov ključna ***definicija osebnega podatka***.

Glede na določbo prve točke 6. člena ZVOP-1 je osebni podatek **katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen**; druga točka 6. člena ZVOP-1 določa, da **je posameznik določena ali določljiva fizična oseba, na katero se nanaša osebni podatek**, pri čemer je fizična oseba določljiva, če **se jo lahko neposredno ali posredno identificira**, predvsem s sklicevanjem na identifikacijsko številko, enega ali več dejavnikov, ki so značilni za njeno fizično, fiziološko, duševno, ekonomsko, kulturno ali družbeno identiteto, pri čemer način identifikacije ne povzroča velikih stroškov, nesorazmerno velikega napora ali ne zahteva veliko časa.

Definicija osebnega podatka je torej zelo široka, ključna sestavina pri določanju, ali je nek podatek osebni podatek, pa je določljivost posameznika. Če je na podlagi nekega podatka osebo mogoče določiti/identificirati, potem je to osebni podatek. Identifikacija je lahko neposredna, torej, da je iz podatka že takoj razvidno za katero osebo gre (npr. ime, priimek zaposlitev in delovno mesto skupaj jasno pokažejo na določeno osebo) ali pa posredna, kar pomeni, da se posameznika lahko identificira s pomočjo nekoga drugega (npr. samo IP-naslov uporabnika policiji ne pove veliko, lahko pa lastnika IP-naslova poišče s pomočjo operaterja, ki ima podatke o tem, komu naslov pripada). Pri posrednem določanju je pomembno tudi to, da identifikacija ne sme povzročiti velikih stroškov, nesorazmerno velikega napora ali ne zahteva veliko časa. V primeru, da je posredna identifikacija praktično nemogoča brez veliko vloženega napora, pa težko govorimo o osebnem podatku. Tako tudi zgolj ime in priimek osebe nista vedno osebna podatka: če je osebi ime Janez Novak, v Sloveniji ni določljiva, če pa je to Janez Novak, Vošnjakova 2, Ljubljana, je posameznik seveda določljiv.

Več o definiciji osebnega podatka si lahko preberete v Mnenju 4/2007 Delovne skupine za varstvo podatkov iz člena 29 o pojmu osebnih podatkov (dostopno preko: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_sl.pdf).

Pri tem pa je potrebno opozoriti, da vsi osebni podatki sami po sebi ne uživajo zaščite po ZVOP-1, temveč so te zaščite deležni šele, če so del zbirke osebnih podatkov ali so namenjeni vključitvi v zbirko osebnih podatkov, kot to določa peta točka 6. člena ZVOP-1. Zbirka pa je glede na določilo šeste točke 6. člena ZVOP-1 vsak strukturiran niz podatkov, ki vsebuje vsaj en osebni podatek, ki je dostopen na podlagi meril, ki omogočajo uporabo ali združevanje podatkov, ne glede na to, ali je niz centraliziran, decentraliziran ali razpršen na funkcionalni ali geografski podlagi; strukturiran niz podatkov je niz podatkov, ki je organiziran na takšen način, da določi ali omogoči določljivost posameznika.

Kar pomeni, da zloraba osebnega podatka, ki ni del zbirke, ne sodi v pristojnost Pooblaščenca.

O pojmu osebnih podatkov je Pooblaščenec izdal že veliko število neobvezujočih mnenj, ki so objavljena na spletni strani http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/.

Med drugimi pojem osebnega podatka pojasnjujejo tudi naslednja mnenja:

- storitvi podobni Google Street View: http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/odlocbe-in-mnenja-varstvo-osebnih-podatkov/?tx_jzvopdecisions_pi1[showUid]=1715&cHash=5948aeda63;
- zlorabi osebnih podatkov na socialnih omrežjih: http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/odlocbe-in-mnenja-varstvo-osebnih-podatkov/?tx_jzvopdecisions_pi1[showUid]=1656&cHash=1dbfecbb25;
- fotografiji kot osebnemu podatku: http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/odlocbe-in-mnenja-varstvo-osebnih-podatkov/?tx_jzvopdecisions_pi1[showUid]=888&cHash=a90c4e4688;
- elektronski pošti na delovnem mestu: http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/odlocbe-in-mnenja-varstvo-osebnih-podatkov/?tx_jzvopdecisions_pi1[showUid]=1516&cHash=61528a5333 in http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/odlocbe-in-mnenja-varstvo-osebnih-podatkov/?tx_jzvopdecisions_pi1[showUid]=245&cHash=c889e5ba84;

- podatkih o avtomobilu: http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/odlocbe-in-mnenja-varstvo-osebnih-podatkov/?tx_jzvopdecisions_pi1[showUid]=986&cHash=0bfe82c9fa;

3. Koliko prijav glede kršitve varovanja osebnih podatkov prejmete po vaši oceni? Majhno, veliko?

Število prijav zaradi suma kršitev določb ZVOP-1 **iz leta v leto narašča**: leta 2008 je Pooblaščenec vodil 635 zadev zaradi suma kršitev določb ZVOP-1, 256 v javnem in 379 v zasebnem sektorju.

Zoper pravne osebe javnega sektorja je prejel 192 prijav, 64 postopkov je uvedel po uradni dolžnosti. V prijavah zoper **pravne osebe javnega sektorja** se je največ sumov kršitev določb ZVOP-1 nanašalo na:

- nezakonito zbiranje oziroma zahtevanje osebnih podatkov (62);
- posredovanje osebnih podatkov nepooblaščenim uporabnikom s strani upravljavca zbirke osebnih podatkov (58),
- neustrezno zavarovanje osebnih podatkov (22),
- nezakonito objavo osebnih podatkov, npr. na oglasnih deskah, na internetu (20),
- nezakonito izvajanje videonadzora (14).

Prijave so bile vložene in postopki po uradni dolžnosti uvedeni zoper naslednje institucije:

- državne organe, ministrstva in organe v njihovi sestavi (102),
- javne sklade, zavode, agencije in druge osebe javnega prava (38),
- zdravstvene ustanove (34),
- izobraževalne ustanove (30),
- sodišča in vrhovno državno tožilstvo (19),
- občine (18),
- upravne enote (15).

Zoper zasebni sektor je Pooblaščenec prejel 310 prijav, 69 postopkov pa je uvedel po uradni dolžnosti. Največ sumov kršitev določb ZVOP-1 pri **pravnih osebah zasebnega sektorja** je bilo zaradi:

- nezakonitega zbiranja oziroma zahtevanja osebnih podatkov (121),
- posredovanja osebnih podatkov nepooblaščenim uporabnikom (59),

- nezakonite objave osebnih podatkov, npr. na oglasnih deskah večstanovanjskih stavb, v medijih (43),
- nezakonitega izvajanja videonadzora (32),
- zlorabe osebnih podatkov za namene neposrednega trženja (29),
- neustreznega zavarovanja osebnih podatkov (9).

Več si lahko preberete v **Letnem poročilu Pooblaščenca 2008** (str. 24 do 28), objavljenem na spletni strani Pooblaščenca (http://www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/Letno-porocilo-2008.pdf) oziroma v preteklih letnih poročilih, ki so prav tako dostopna na spletni strani Pooblaščenca: http://www.ip-rs.si/publikacije/prirocniki-in-smernice/.

4. Kako sankcionirate kršitelje?

Zaradi kršitev določb ZVOP-1 je bilo leta 2008 uvedenih 279 postopkov o prekršku, 49 postopkov zoper pravne osebe javnega sektorja, 78 postopkov zoper pravne osebe zasebnega sektorja in 155 postopkov zoper fizične osebe oziroma posameznike.

Postopek o prekršku Pooblaščenec vodi v skladu z Zakonom o prekrških (ZP-1). Za ugotovljeni prekršek lahko Pooblaščenec v skladu s 53. členom ZP-1 izreče **opozorilo**, če je storjeni prekršek neznatnega pomena in če pooblaščena uradna oseba oceni, da je glede na pomen dejanja opozorilo zadosten ukrep.

Če je storjen težji prekršek, Pooblaščenec izda **odločbo o prekršku**, s katero lahko kršitelju **izreče sankcijo**. V skladu s 4. členom ZP-1 sta sankciji za prekršek **globa** in **opomin**, glede na 57. člen ZP-1 pa se lahko globa izreče tudi v obliki **plačilnega naloga**.

Zaradi ugotovljenih prekrškov je Informacijski pooblaščenec v letu 2008 izdal:
- 40 opozoril (tri v postopkih, uvedenih leta 2007),
- 131 odločb o prekršku (103 opomine, od tega osem v postopkih, uvedenih leta 2007 in 28 glob, od tega tri v postopkih, uvedenih leta 2007),
- tri plačilne naloge.

(Vir: Letno poročilo Pooblaščenca 2008)

5. Zakon o varovanju osebnih podatkov je napisan na tak način, da si ga nekatere organizacije razlagajo po svoje, npr. klinični center. Kaj menite o tej situaciji?

Ravno za zdravstvo je potrebno poudariti, da varstvo osebnih podatkov (zdravstvenih podatkov) ni privilegij zdravnika, temveč pravica posameznika. Zdravstvo se mora zavedati, da poleg zakonov s področja zdravstva pravico do vpogleda v osebne podatke lahko določa tudi kakšen drug zakon (recimo zakon o inšpekcijskem nadzorstvu, zakon o davčnem postopku…). Razumevanja je v zdravstvenem sektorju vsako leto več, razmere se izboljšujejo tudi zaradi zakona o pacientovih pravicah, ki je jasno določil, kdaj mora zdravnik posredovati podatke pacienta še komu drugemu. Do uveljavitve tega zakona pa je bilo največ težav takrat, ko so sorodniki hoteli videti zdravstveni karton umrlega pacienta, da bi se lahko odločili, ali bodo zaradi morebitne zdravniške napake sprožili sodne postopke.

6. Če je kršena posameznikova informacijska zasebnost, ali je oškodovanec upravičen do opravičila, odškodnine?

Ustava RS v 35. členu zagotavlja posamezniku nedotakljivost človekove telesne in duševne celovitosti, njegove zasebnosti ter osebnostnih pravic. V 38. členu pa kot temeljno pravico posameznika izpostavlja tudi varstvo osebnih podatkov.

> *38. člen*
> *(varstvo osebnih podatkov)*
>
> *Zagotovljeno je varstvo osebnih podatkov. Prepovedana je uporaba osebnih podatkov v nasprotju z namenom njihovega zbiranja.*
> *Zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa zakon.*
> *Vsakdo ima pravico seznaniti se z zbranimi osebnimi podatki, ki se nanašajo nanj, in pravico do sodnega varstva ob njihovi zlorabi.*

Zloraba osebnega podatka lahko pomeni tudi storitev kaznivega dejanja po 143. členu Kazenskega zakonika (Uradni list RS, št. 55/2008):

> *Zloraba osebnih podatkov*

143. člen

(1) ***Kdor uporabi osebne podatke, ki se obdelujejo na podlagi zakona, v neskladju z namenom njihovega zbiranja ali brez osebne privolitve osebe, na katero se osebni podatki nanašajo, se kaznuje z denarno kaznijo ali zaporom do enega leta.***
(2) Enako se kaznuje, kdor vdre ali nepooblaščeno vstopi v računalniško vodeno zbirko podatkov z namenom, da bi sebi ali komu drugemu pridobil kakšen osebni podatek.
(3) Kdor na svetovnem medmrežju objavi ali omogoči drugemu objavo osebnih podatkov žrtev kaznivih dejanj, žrtev kršitev pravic ali svoboščin, zaščitenih prič, ki se nahajajo v sodnih spisih sodnih postopkov, kjer po zakonu ali po odločitvi sodišča ni dovoljena prisotnost javnosti ali identifikacija žrtev ali zaščitenih prič ter osebnih zapisov o njih v zvezi s sodnim postopkom, na podlagi katerih se te osebe lahko določi ali so določljive, se kaznuje z zaporom do treh let.
(4) Kdor prevzame identiteto druge osebe in pod njenim imenom izkorišča njene pravice, si na njen račun pridobiva premoženjsko korist ali prizadene njeno osebno dostojanstvo, se kaznuje z zaporom od treh mesecev do treh let.
(5) Če stori dejanje iz prejšnjih odstavkov tega člena uradna oseba z zlorabo uradnega položaja ali uradnih pravic, se kaznuje z zaporom do petih let.
(6) Pregon iz tretjega odstavka tega člena se začne na predlog.

Posameznik, ki je prepričan, da se s protipravnim dejanjem (lahko je to prekršek ali kaznivo dejanje) posega v njegove osebnostne pravice (tudi pravico do varstva osebnih podatkov), skladno z določbami 134. člena Obligacijskega zakonika (Uradni list RS, št. 83/01 s spremembami, v nadaljevanju OZ) od sodišča zahteva, da prepreči takšno dejanje ali da odstrani njegove posledice. *V primeru, da je posamezniku povzročena škoda* (kar mora posameznik izkazati)*, pa lahko od povzročitelja skladno z določbami 179. in 181. člena OZ zahteva* ***tudi odškodnino****.*

7. V primeru, da se zgodi kršitev varovanja osebnih podatkov, na koga se torej naprej obrnemo - na vas, na koga drugega in na kakšen način lahko to storimo?

Informacijski pooblaščenec sme v skladu z načelom zakonitosti ravnati samo v okviru svojih pooblastil, za katera ima neposredno podlago v 2. členu Zakona o Informacijskem pooblaščencu (Uradni list RS, št. 113/05 in 51/07 – ZUstS-A; ZInfP), na podlagi katerega je med drugim pristojen za:

- *inšpekcijski nadzor nad izvajanjem zakona in drugih predpisov, ki urejajo varstvo ali obdelavo osebnih podatko*v oziroma iznos osebnih podatkov iz Republike Slovenije, ter opravljanje drugih nalog, ki jih določajo ti predpisi;
- *odločanje o pritožbi posameznika, kadar upravljavec osebnih podatkov ne ugodi zahtevi posameznika glede pravice posameznika do seznanitve z zahtevanimi podatki*, do izpisov, seznamov, vpogledov, potrdil, informacij, pojasnil, prepisovanja ali kopiranja po določbah zakona, ki ureja varstvo osebnih podatkov.

Če posameznik meni, da je v zvezi z njegovim primerom prišlo do kršitve ZVOP-1, lahko na Pooblaščenca naslovit prijavo. Prijavo lahko vloži osebno, pisno ali preko spletnega obrazca, ki je na voljo na spletni strani: http://www.ip-rs.si/kazalo-kontakt-iskalnik/kontakt/.

8. Kako lahko nadzorujete ustanove, da ne kršijo zakona o varovanju zasebnosti podatkov?

Med pristojnosti Pooblaščenca spada tudi neposredni inšpekcijski nadzor nad izvajanjem predpisov s področja varstva osebnih podatkov:

- nadzor zakonitosti obdelave osebnih podatkov;
- nadzor ustreznosti ukrepov za zavarovanje osebnih podatkov ter izvajanja postopkov in ukrepov za zavarovanje osebnih podatkov po 24. in 25. členu ZVOP-1;
- nadzor nad izvajanjem določb zakona, ki urejajo katalog zbirke osebnih podatkov, register zbirk osebnih podatkov in evidentiranje posredovanja osebnih podatkov posameznim uporabnikom osebnih podatkov;
- nadzor nad izvajanjem določb zakona v zvezi z iznosom osebnih podatkov v tretjo državo in njihovim posredovanjem tujim uporabnikom osebnih podatkov.

Inšpekcijski nadzor nad izvajanjem določb ZVOP-1 s strani ustanov v javnem in zasebnem sektorju **izvajajo državni nadzorniki za varstvo osebnih podatkov** (ki delujejo v okviru Informacijskega Pooblaščenca), ki svoje delo opravljajo v okviru in na podlagi ustave in zakonov, ter so pri opravljanju svojih nalog v skladu s svojimi pooblastili samostojni.

Splošna načela inšpekcijskega nadzora, splošne pravice, dolžnosti, pooblastila državnih nadzornikov, postopek inšpekcijskega nadzora, inšpekcijski ukrepi in druga vprašanja, povezana z inšpekcijskim nadzorom, so določeni v Zakonu o inšpekcijskem nadzoru, specifične pristojnosti državnega nadzornika pa so določene v 53. členu ZVOP-1.

Državni nadzorniki torej izvajajo inšpekcijske nadzore v ustanovah javnega in zasebnega sektorja, lahko na podlagi prijave posameznika ali pa po uradni dolžnosti. Ob inšpekcijskem nadzoru državni nadzornik preveri skladnost delovanja ustanove z določbami ZVOP-1 (zakonitost obdelave osebnih podatkov, zavarovanje, prijava v register zbirk, iznos podatkov, idr.). V primeru kršitev Pooblaščenec izda opozorilo oziroma odločbo o prekršku (kot pri vprašanju št. 4.). Pooblaščenec lahko inšpekcijski nadzor na mestu izvede tudi brez vnaprejšnjega opozorila institucije (česar npr. Informacijski Pooblaščenec iz Velike Britanije ne sme).

Pomembna je tudi pristojnost Pooblaščenca, da v zvezi z varstvom osebnih podatkov daje pojasnila zainteresiranim posameznikom in ustanovam ter izdaja neobvezna mnenja. V praksi to pomeni, da pogosto ustanove že pred uvedbo ukrepov, ki bi lahko pomenili poseg v varstvo osebnih podatkov posameznikov, zaprosijo za pisno mnenje Pooblaščenca glede skladnosti ukrepov z ZVOP-1.

9. Ali se bo zakon o varovanju osebnih podatkov začel kaj spreminjati in če se bo, v katerih točkah se bo spremenil?

ZVOP-1 se bo spreminjal, saj je vsak zakon živa stvar. Ta zakon bo potrebno predvsem osvežiti z vidiki razvoja modernih informacijskih tehnologij, ki vse bolj posegajo v zasebnost posameznika.

10. Kakšno morebitno grožnjo predstavljata biometrija ter satelitsko cestninjenje varnosti osebnih podatkov? S katerimi ukrepi se bodo preprečevale zlorabe osebnih podatkov?

Biometrija

Zavedati se je potrebno, da biometrija ni le metoda ugotavljanja oz. preverjanja identitete, temveč je tehnologija, ki za svoj cilj uporablja človeško telo oziroma tiste telesne in vedenjske značilnosti vseh nas, ki so nespremenljive in samo nam lastne. Predvsem pri proizvajalcih in prodajalcih biometričnih sistemov obstaja zelo močna tendenca po trivializaciji zbiranja podatkov o človeških telesnih in vedenjskih značilnosti. Če pustimo ob strani vprašanja, ki so povezana s temeljno človekovo pravico do telesne celovitosti in

dostojanstva, ima nekritična in nekontrolirana uporaba biometrije lahko zelo realne in resne posledice za vsakega posameznika.

Naša zasebnost je lahko resno ogrožena zaradi nepotrebnega ali neavtoriziranega zbiranja, uporabe, neprimernega shranjevanja, povezovanja ali posredovanja naših osebnih podatkov. Četudi proizvajalci zatrjujejo, da do zlorab praktično ne more priti, pa nas zgodovina vedno znova opominja, da noben sitem ni nezlomljiv. Zakaj bi bili biometrijski sistemi izjema?

Proizvajalci biometričnih sistemov zatrjujejo, *da njihovi sistemi shranjujejo predloge (template), t.j. reducirane, digitalizirane oblike biometričnih značilnosti, na takšen način, da rekonstrukcija izvirnih podatkov ni več mogoča*. Trdijo, da unikatne značilnosti o npr. prstnem odtisu sistem zajame, jih obdela in pretovori v predlogo, na podlagi katere ni več mogoče ugotoviti, kateri osebi pripada. *To utemeljujejo s tem, da so izvirni biometrični podatki zaščiteni z njihovim lastnim algoritmom*, ki onemogoča rekonstrukcijo biometričnih značilnosti. Takšna trditev pa je s stališča informacijske varnosti vprašljiva vsaj iz dveh vidikov.

Prvi vidik je povezan z vprašanjem *ali je rekonstrukcija biometričnih značilnosti iz predloge mogoča oziroma ali je mogoče razvozlati (razbiti) algoritem, ki je biometrične podatke »zakodiral«*. Če poiščemo vzporednice v kriptografskih algoritmih, so praviloma najbolj varni algoritmi tisti, ki so izpostavljeni javni presoji in so na voljo vsakomur, ki jih poskuša razbiti z vsemi sredstvi, ki so mu na voljo. Za algoritem ali metodo lahko rečemo, da je varna le, če so strokovnjaki lahko preizkusili njeno nezlomljivost in ugotovili, da se brez izjemno velikih sredstev ali časa tega ne da narediti z obstoječo tehnologijo. Algoritmi in postopki lastniške ali skrite narave takšni presoji niso podvrženi in je zato težko soditi, kako varni in nezlomljivi dejansko so. Varstvo osebnih podatkov ne more temeljiti na tajnosti algoritmov ali nedostopnosti strojne opreme. Varnostni mehanizmi v tem primeru predpostavljajo nevednost napadalcev, kar je pa na današnji stopnji razvoja iluzorno pričakovati.

Drug vidik pa je povezan z vprašanjem, *ali je preprečitev rekonstrukcije izvirnih biometričnih podatkov res odločilna pri zagotavljanju zasebnosti posameznikov.* Namreč, proizvajalci biometrijskih naprav se pogosto sklicujejo na trditve, da je zasebnost uporabnikov zagotovljena že s tem, ko iz predloge ni možna restavracija npr. prstnega odtisa. Predpostavimo za trenutek, da to drži. Predpostavimo, da rekonstrukcija izvirnih podatkov

resnično ni možna. Četudi je to res, pa zasebnost uporabnika vseeno še ni zagotovljena, saj sta tako vzorec prstnega odtisa kot njegov vzorec v digitalni obliki enolična identifikatorja in tako surogata identitete posameznika. Predstavljajmo si scenarij, ko bi namesto predložitve našega biometrijskega podatka sistem zahteval npr. dvakratnik naše EMŠO. Vprašanje razbitja algoritma in rekonstrukcije izvirnih podatkov je irelevantno, ne glede na to ali se uporablja zelo enostaven algoritem (dvakratnik nekega števila) ali sofisticirano matematično metodo. Ključna vprašanja s stališča zasebnosti posameznika so povezana z uporabo, povezljivostjo in varnostjo tovrstnega identifikatorja. Napadalec bi isti namen lažje dosegel s pridobitvijo latentnega prstnega odtisa (npr. na kozarcu), kot z vlaganjem velikega napora, sredstev, znanja in časa v razbitje algoritma in s tem pridobitve izvirnih podatkov.

V izogib zlorabam osebnih podatkov zaradi uporabe biometrijskih ukrepov je v Sloveniji pred uvajanjem biometrije pridobiti dovoljenje Informacijskega Pooblaščenca. Pooblaščenec mora pred izdajo odločbe celovito presoditi, ali je uvajanje biometrijskih ukrepov v skladu z načeli in pravili varstva osebnih podatkov. Pri presoji uporabe posamezne tehnologije Pooblaščenec tehta poleg namena, ki ga zasleduje upravljavec osebnih podatkov, tudi določene tehnične lastnosti nameravanih biometrijskih ukrepov, predvsem tiste, ki nakazujejo stopnjo tveganja uporabe določene biometrijske tehnologije, kot so odkritost/prikritost, puščanje sledov, možnosti povezovanja, možnost nadzora nad svojimi osebnimi podatki, (de)centralizirano hrambo in drugo.

Več o biometriji si lahko preberete na spletni strani Pooblaščenca: http://www.ip-rs.si/varstvo-osebnih-podatkov/informacijske-tehnologije-in-osebni-podatki/biometrija/.

Pooblaščenec je na temo biometrije izdal tudi smernice, ki so dostopne na: http://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Biometrija_-_smernice.pdf

Več o praktičnih primerih biometrijskih ukrepov pa si lahko preberete v številnih mnenjih Pooblaščenca, ki so dostopna preko iskalnika po odločbah in mnenjih http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/ (za prikaz mnenj in odločb o biometriji odkljukajte kategorijo »biometrija«).

Elektronsko cestninjenje

Elektronsko cestninjenje vključuje zbiranje in obdelavo velike količine osebnih podatkov posameznikov – predvsem informacije o njihovi lokaciji in času potovanja. Obdelava take količine podatkov pa glede na namen obdelave (ki je cestninjenje in ne sledenje posamezniku!) pomeni velik in pretiran poseg v zasebnost posameznika.

Gotovo je do zasebnosti posameznika najbolj prijazen pristop, ko so podatki, ki so potrebni za izvedbo samega cestninjenja, pod izključnim nadzorom uporabnika. V tem primeru se obračun cestnine izvrši v napravi sami (t.i. inteligentna naprava ali Smart Client), nadzornemu centru pa se posreduje samo seštevek potrošene vsote. Vse štiri faze obračunskega postopka pri elektronskem cestninjenju se torej v tem primeru izvedejo v sami napravi:

1. določitev lokacije,
2. določitev cestninskega segmenta in ustrezne tarife,
3. izračun porabljene vsote za ta segment,
4. seštevek porabljenih vsot.

Za redno elektronsko pobiranje cestnine bi torej morali zadoščati podatki o identifikacijski številki posamezne *naprave za cestninjenje* in *podatki o višini cestnine*, ***niso pa pri tem potrebni podatki o lokaciji vozila in lastniku naprave***. Več podatkov je lahko potrebnih le v primerih, ko gre za izogibanje plačila cestnine, napačno delovanje naprave ipd.
Zadovoljiv način varovanja zasebnosti bi bil, da bi nadzorni center v kontrolnih točkah nadziral pravilnost delovanja naprave v vozilu na način, da se, vse dokler naprava v vozilu pravilno deluje, *nadzornemu centru identiteta naprave ne bi razkrila*. Identiteta posameznika bi se lahko razkrila le v zakonsko določenih primerih, med drugim v primeru predrugačenja ali drugih zlorab elektronske naprave za cestninjenje; v primeru nedelovanja elektronske naprave za cestninjenje na vozilu med vožnjo po cestninskih cestah; v primeru, ko je bilo vozilo ukradeno.
Pooblaščenec poudarja, da za samo redno in pravilno delovanje sistema upravljavcem cestninskih cest ni potrebno stalno razkrivanje identitete in lokacije vsakega voznika, v kolikor ne nastopijo vnaprej zakonsko opredeljeni primeri, ko je identifikacija in določitev lokacije vozila potrebna.

Povzeto po:

- mnenju Pooblaščenca glede elektronskega cestninjenja (dostopno preko: http://www.ip-rs.si/fileadmin/user_upload/Pdf/razno/Opinion_on_electronic_toll_collection_Information_Commissioner_Slovenia.pdf;

- Tomšič, A., Jerše A. (2007): Elektronsko cestninjenje - na račun zasebnosti? Pravna praksa 26(46), str. 13-15.

Priloga C: ANKETA UPORABNIKI:

Spoštovana obiskovalka, spoštovani obiskovalec spletne ankete,
pred vami je krajša anonimna anketa o informacijski zasebnosti na internetu in E-upravi. Moje ime je Mojca Berce in sem študentka 4. Letnika družboslovne informatike na Fakulteti za družbene vede (FDV) ter Informacijska zasebnost na internetu in E-upravi, je naslov mojega diplomskega dela.
Vprašanja se bodo nanašala na hrambo podatkov ter varovanjem njih in uporabo ter poznavanjem E-uprave.
Za odgovore se vam vnaprej zahvaljujemo in zagotavljamo varovanje zasebnosti in tajnost vaših odgovorov.

I. Zasebnost, osebni podatki

1.vprašanje: Različne javne in zasebne organizacije zbirajo osebne podatke o nas. Ali ste zaradi tega zaskrbljeni, na primer zaradi morebitnega nezadostnega varovanja vaše zasebnosti?

a.) da zelo me skrbi
b) da me skrbi
c) do neke mere me skrbi
d) me sploh nič ne skrbi
e) ne vem

2. vprašanje: Se vam zdi pomembno, da veste kateri vaši osebni podatki se zbirajo in v kakšnem namen?

a) da zelo mi je pomembno
b) da mi je pomembno

c) do neke mere pomembno

d) mi ni pomembno

e) ne vem

3.vprašanje: Ali veste, da se vaši osebni podatki ne smejo zbirati brez vašega osebnega soglasja?

A)da

b) ne

c) ne vem

4. vprašanje: Ali poznate zakonodajo v zvezi z zaščito zasebnosti oziroma osebnih podatkov?

a) da, poznam

b) poznam samo okvirno

c) slišal/a sem že za zakon o varstvu osebnih podatkov, vendar ga ne poznam podrobneje

d) ne poznam

II. E-uprava

5.vprašanje: Ali ste seznanjeni z spletno stranjo E-uprava in njenim delovanjem?
a) da
b) ne
c.) ne vem

6.vprašanje: Kako pogosto uporabljate storitve v E-upravi?
a) manj kot 1-krat letno
b)1-krat letno
c) 2-krat letno
d) 3-kratno letno

7.vprašanje: Ali imate digitalno potrdilo, podpis za upravljanje storitev na portalu E-uprava?
a) da
b) ne
c.) ne vem

III. Demografija

8.Spol

1. moški
2. ženski

9.Starost

1. Od 15 do 35 let
2. Od 36 let do 55 let
3. Od 56 do 65 let
4. Nad 65 let

10.Izobrazba- Navedite zadnjo šolo, ki ste jo končali redno ali izredno:

1. dokončana osnovna šola
2. dokončana 2 ali 3 - letna poklicna šola
3. dokončana 4 - letna srednja šola
4. dokončana 2 – letna višja visoka
5. dokončana visoka šola, fakulteta, akademija
6. magisterij ali doktorat

Hvala za sodelovanje!

Priloga D: IZPISI IZ SPSS-A:

```
FREQUENCIES
  VARIABLES=V8
  /STATISTICS=MINIMUM MAXIMUM MEAN
  /PIECHART  PERCENT
  /ORDER=  ANALYSIS .
FREQUENCIES
  VARIABLES=V9
  /STATISTICS=MINIMUM MAXIMUM MEAN
  /PIECHART  PERCENT
  /ORDER=  ANALYSIS .
FREQUENCIES
  VARIABLES=V10
  /STATISTICS=MINIMUM MAXIMUM MEAN
  /PIECHART  PERCENT
  /ORDER=  ANALYSIS .
FREQUENCIES
  VARIABLES=V1
  /STATISTICS=MINIMUM MAXIMUM MEAN
  /PIECHART  PERCENT
  /ORDER=  ANALYSIS .
FREQUENCIES
  VARIABLES=V2
  /STATISTICS=MINIMUM MAXIMUM MEAN
  /PIECHART  PERCENT
  /ORDER=  ANALYSIS .
FREQUENCIES
  VARIABLES=V3
  /STATISTICS=MINIMUM MAXIMUM MEAN
  /PIECHART  PERCENT
```

```
  /ORDER=  ANALYSIS .
FREQUENCIES
  VARIABLES=V4
  /STATISTICS=MINIMUM MAXIMUM MEAN
  /PIECHART  PERCENT
  /ORDER=  ANALYSIS .
FREQUENCIES
  VARIABLES=V5
  /STATISTICS=MINIMUM MAXIMUM MEAN
  /PIECHART  PERCENT
  /ORDER=  ANALYSIS .
FREQUENCIES
  VARIABLES=V6
  /STATISTICS=MINIMUM MAXIMUM MEAN
  /PIECHART  PERCENT
  /ORDER=  ANALYSIS .
FREQUENCIES
  VARIABLES=V7
  /STATISTICS=MINIMUM MAXIMUM MEAN
  /PIECHART  PERCENT
  /ORDER=  ANALYSIS .
```

Priloga E: Tabele frekvenčnih porazdelitev anketnih vprašanj

Vprašanje 4

zakonodaja	frekvenca	Odstotek	Kumulativni odstotek
Da poznam	6	5,4	5,4
Samo okvirno poznam	56	50,5	55,9
Slišala sem že,…	44	39,6	95,5
Ne poznam	5	4,5	100,0
skupaj	111	100,0	

vprašanje 5

		frekvenca	odstotek	kumulativni odstotek
	da	60	54,1	55,0
	ne	43	38,7	94,5
	ne vem	6	5,4	100,0
	skupaj	109	98,2	
manjk	-3	2	1,8	
skupaj		111	100,0	

vprašanje 6

		frekvenca	odstotek	kumulativni odstotek
	manj kot 1-letno	73	65,8	67,0
	1-krat letno	19	17,1	84,4
	2-krat letno	7	6,3	90,8
	3-krat ali veckrat letno	10	9,0	100,0
	skupaj	109	98,2	
Mi	-3	2	1,8	
skupaj		111	100,0	

V8

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	33	29,7	30,6	30,6
	2	75	67,6	69,4	100,0
	Total	108	97,3	100,0	
Missing	-3	2	1,8		
	-1	1	,9		
	Total	3	2,7		
Total		111	100,0		

V9

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	100	90,1	91,7	91,7
	2	8	7,2	7,3	99,1
	3	1	,9	,9	100,0
	Total	109	98,2	100,0	
Missing	-3	2	1,8		
Total		111	100,0		

V10

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	2	1,8	1,8	1,8
	2	1	,9	,9	2,8
	3	45	40,5	41,3	44,0
	4	4	3,6	3,7	47,7
	5	53	47,7	48,6	96,3
	6	4	3,6	3,7	100,0
	Total	109	98,2	100,0	
Missing	-3	2	1,8		
Total		111	100,0		

V1

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	11	9,9	9,9	9,9
	2	30	27,0	27,0	36,9
	3	53	47,7	47,7	84,7
	4	17	15,3	15,3	100,0
	Total	111	100,0	100,0	

V2

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	42	37,8	37,8	37,8
	2	44	39,6	39,6	77,5
	3	24	21,6	21,6	99,1
	4	1	,9	,9	100,0
	Total	111	100,0	100,0	

V3

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	103	92,8	92,8	92,8
	2	5	4,5	4,5	97,3
	3	3	2,7	2,7	100,0
	Total	111	100,0	100,0	