UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Mitja Slana

Varnost informacijske zasebnosti Evropske unije v primerjavi s Slovenijo

Diplomsko delo

Ljubljana, 2011

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Mitja Slana

Mentor: izr. prof. dr. Marjan Brezovšek

Varnost informacijske zasebnosti Evropske unije v primerjavi s Slovenijo

Diplomsko delo

Ljubljana, 2011

Varnost informacijske zasebnosti Evropske unije v primerjavi s Slovenijo

Pred iznajdbo, današnjih sodobnih naprav, je posameznik bil lahko skorajda prepričan, da mu v zasebnost nihče ne more vdreti oziroma jo ogroziti, prav tako je bil vdor v zasebnost večje skupine ljudi še pred kratkim, pred iznajdbo računalnikov skorajda nemogoč, saj so takrat bile informacije pogosto raztresene in težko dostopne, medtem ko je danes vdor v bazo podatkov lahka naloga ljubiteljev računalnikov. Zato je danes potreba po varstvu zasebnosti še kako pomembna, saj danes nove kršitve zasebnosti omogočajo nove, moderne, informacijske tehnologije. Da ne bi prišlo do ogrožanja varnosti informacijske zasebnosti Evropska unija, kot tudi ostale države članice na tem področju poskuša s svojimi pravnimi akti, doseči ravnotežje med pravico do zasebnosti in med legitimnimi razlogi za uporabo osebnih podatkov, kot tudi poenotiti področje varovanja informacijske zasebnosti v skupnosti.

Ključne besede: zasebnost, varnost, varnost informacijske zasebnosti, informacijski pooblaščenec.

Information privacy protection in the European Union in comparison with Slovenia

Prior to invention of today's modern devices, the individual was almost completely convinced that no one could invade his privacy. Prior to invention of computers, invading privacy of a larger group of people was almost impossible, since information was often scattered and usually almost inaccessible then. Therefore the need for privacy protection is very important today, since new, modern information technologies make new violations of privacy possible. In order to avoid threat to information privacy protection, the European Union as well as other Member States try to pursue equilibrium between the right to privacy and legit reasons for usage of personal data and to unify the field of information privacy protection in the community.

Key words: privacy, protection, information privacy protection, information commissioner.

KAZALO

1 UVOD 7
1.1 IZHODIŠČE DIPLOMSKEGA DELA 7
1.2 NAMEN, CILJI IN TEZE DIPLOMSKEGA DELA 7
1.3 METODE DELA 8
1.4 STRUKTURA DIPLOMSKEGA DELA 9

2 VARNOST INFORMACIJSKE ZASEBNOSTI 10
2.1 NASTANEK SODOBNE ZASEBNOSTI 10
2.1.1 Zasebnost 10
2.1.2 Razvoj pojma informacijske zasebnosti 12
2.2 NASTANEK SODOBNE VARNOSTI 13
2.2.1 Varnost 14
2.2.2 Razvoj pojma informacijska varnost 14
2.2.2.1 Sistem 15
2.2.2.2 Informacijski sistem 15
2.2.2.3 Informacijska varnost, računalniška varnost in varnost informacijskih sistemov 16

3 VARNOST INFROMACIJSKE ZASEBNOSTI V EVROPSKI UNIJI 17
3.1 NASTANEK IN REGULATIVNI PRISTOP EVROPSKE UNIJE 17
3.1.1 Nastanek Evropske unije 17
3.1.2 Regulativni pristop Evropske unije na področje varnosti informacijske zasebnosti 18
3.1.2.1 Pravna praksa: Vpliv ameriške izkušnje »koncept razumnega pričakovanja zasebnosti« na evropska tla 22
3.2 VARSTVO INFORMACIJSKE ZASEBNOSTI 23
3.3 IZNOS PODATKOV IZ EVROPSKE UNIJE V DRŽAVE TRETJEGA SVETA 24
3.3.1 Iznos osebnih podatkov iz Evropske unije v ZDA 25

4 VARNOST INFORMACIJSKE ZASEBNOSTI V REPUBLIKI SLOVENIJI.. 26
4.1 REGULATIVNI PRISTOP SLOVENIJE NA PODROČJU VARNOSTI INFORMACISJKE ZASEBNOSTI 26
4.1.1 Pravna praksa: primer dileme, ki ga prinaša kolizija dveh pravic in kakšne dileme prinaša uporaba nove tehnologije, internet 28
4.2 VARSTVO INFORMACIJSKE ZASEBNOSTI 28
4.2.1 Statistika kršitve informacijske zasebnosti 29
4.2.2 Najodmevnejši primeri kršitev varstva osebnih podatkov v zadnjih letih, ki jih je ugotovil in rešil informacijski pooblaščenec 32
4.2.2.1 Obdelava osebnih podatkov zavarovancev brez podlage v zakonu ali v osebni privolitvi posameznika s strani zavarovalnic 32
4.2.2.2 Primer nezakonite pridobitve osebnih podatkov potencialnih volivcev s strani političnih strank 32
4.2.2.3 Nezakoniti vpogled v osebne podatkov komitentov pri bankah 33
4.2.2.4 Obdelava osebnih podatkov uporabnikov kartice Urbana 33
4.2.2.5 Zbiranje osebnih podatkov pri nakupu z vrednostnimi boni 34
4.3 IZNOS PODATKOV IZ SLOVENIJE V TRETJE DRŽAVE SVETA 34
4.3.1 Primer za iznos podatkov v Republiko Hrvaško 35
4.3.2 Primer iznosa podatkov v ZDA 36
4.4 PROBLEM INFORMACIJSKE ZASEBNOSTI NA INTERNETU 36
4.4.1 Tehnične možnosti varstva zasebnosti na internetu 37

5 ZAKLJUČEK 38

6 LITERATURA 40

KAZALO GRAFOV:

Graf 4.1: Število zadev, ki jih je zaradi suma kršitev določb ZVOP-1 vodil informacijski pooblaščenec med letoma 1996 in 2010 30
Graf 4.2:Število zadev zaradi suma kršitev določb ZVOP-1 med letoma 2006 in 2010…….30
Graf 4.3: Število uvedenih postopkov o prekrških med letoma 2006 in 2010 31
Graf 4.4: Število izdanih odločb za iznos osebnih podatkov med letom 2006 in 2010 . 35

1 UVOD

1.1 IZHODIŠČE DIPLOMSKEGA DELA

Pravica do zasebnosti oziroma angleška inačica »*right to privacy*«, v francoskem pravu največkrat imenovana »*droit au respect de la vie privée*« oziroma »pravica do spoštovanja zasebnega življenja«, ter v nemškem pravni terminologiji poimenovana kot »recht auf privatheit« je elementarna oziroma osnovna človekova pravica, ki je tako mednarodna kot tudi ustavna pravica javnopravnega značaja ter osebna pravica civilnopravnega značaja, kot eden izmed nepogrešljivih elementov človekove eksistence, ki varuje človeka pred prekomernimi posegi državne oblasti, javnosti in drugih posameznikov v posameznikovo odločitveno, društveno, prostorsko in informacijsko zasebnost (Lampe 2003, 121).

1.2 NAMEN, CILJI IN TEZE DIPLOMSKEGA DELA

Namen moje diplomske naloge je podrobneje predstaviti varnost informacijske zasebnosti v Evropski uniji, ter v Republiki Sloveniji.

Cilji moje diplomske naloge so:

- opredeliti nastanek sodobne zasebnosti,
- opredeliti nastanek sodobne varnosti,
- predstaviti nastanek in regulativni pristop Evropske unije na področju varnosti informacijske zasebnosti,
- predstaviti varstvo informacijske zasebnosti v Evropski uniji,
- predstaviti iznos podatkov iz Evropske unije v države tretjega sveta
- predstaviti regulativni pristop Slovenije na področju varnosti informacijske zasebnosti,
- predstaviti varstvo informacijske zasebnosti v Sloveniji,
- predstaviti iznos podatkov iz Slovenije v države tretjega sveta,
- predstaviti problem informacijske zasebnosti na internetu.

Hipoteze moje diplomske naloge:

- Hipoteza 1: Evropska unija, kot tudi Slovenija imata dobro pravno podlago na področju varnosti informacijske zasebnosti.
- Hipoteza 2: Informacijski pooblaščenec je v letu 2010 in 2009 vodil 200 zadev, zaradi suma kršitev določil ZVOP-1.
- Hipoteza 3: Največ vdorov v posameznikovo zasebnost prihaja v zasebnem sektorju.
- Hipoteza 4: V Sloveniji je v zadnjih letih prišlo do 50 vdorov v posameznikovo informacijsko zasebnost.
- Hipoteza 5: Ljudje se ne zavedamo, da internet je le eno od orodij s katerimi lahko ljudje posežejo v našo zasebnost.

1.3 METODE DELA

Moja diplomska naloga je sestavljena le iz teoretičnega dela, ki zajema naslednje metode:

- metodo opisovanja oziroma metodo deskripcije,
- metodo primerjave oziroma metodo komparacije,
- metodo kompilacije oziroma metodo povzemanja različnih domačih in tujih virov,
- metodo dedukcije oziroma metodo sklepanja o posebnih ali posameznih dejstvi na osnovi splošnih spoznanj in
- metodo indukcije oziroma metodo utemeljevanja splošnih spoznanj na podlagi posameznih ali posebnih dejstev.

1.4 STRUKTURA DIPLOMSKEGA DELA

Svojo diplomsko nalogo sem razdelil na pet poglavij. V prvem, uvodnem, poglavju sem opredelil izhodišče diplomske naloge, predstavil svoj namen, cilje, ter metodo dela.

Drugo poglavje zajema opredelitev nastanka sodobne varnosti in zasebnosti. V tem poglavju je podrobneje opisan pojem zasebnost in varnost, kot tudi razvoj pojma informacijska zasebnost in informacijska varnost.
V naslednjem, tretjem poglavju, je opredeljen nastanek in pravni pristop Evropske unije na področju varnosti informacijske zasebnosti, čemur sledi varstvo informacijske zasebnosti, ter predstavitev in opredelitev iznosa podatkov iz Evropske unije v države tretjega sveta, Hrvaške in Združenih držav Amerike.

Četrto poglavje predstavlja regulativni pristop Slovenije na področju varnosti informacijske zasebnosti, opredelitev varstva informacijske zasebnosti v Sloveniji, ki je podkrepljeno z najodmevnejšimi medijskimi primeri, sledi opredelitev iznosa podatkov iz Slovenije v države tretjega sveta, ter sodobni problem informacijske zasebnosti na internetu.

Sledi peto poglavje, sklep, kjer sem povzel svoje ugotovitve, na katere sem naletel ob pisanju diplomskega dela.

V šestem poglavju se nahaja seznam literature in virov uporabljenih v moji diplomski nalogi.

2 VARNOST INFORMACIJSKE ZASEBNOSTI

2.1 NASTANEK SODOBNE ZASEBNOSTI

Zasebnost oziroma potreba po zasebnosti se je pojavila sočasno z nastankom in razvojem živega bitja. Torej je potrebo po zasebnosti človek čutil že v praskupnosti. Vendar pa je zasebnost v različnih zgodovinskih obdobjih imela in predstavljala različen pomen, saj je sprva imela le pomen fizičnega umika na varno lokacijo pred drugimi subjekti, medtem ko danes velja za eno od temeljnih človekovih pravic. Saj je po mnenju Lampeta (2003, 121) tako mednarodna kot tudi ustavna pravica, prav tako pa je tudi osebna pravica, ki predstavlja element človekove eksistence, ki varuje človeka pred prekomernimi posegi bodisi državne, javne ali druge oblasti v njegovo odločanje, kot tudi v njegovo duševno, prostorsko in informacijsko zasebnost.

2.1.1 Zasebnost

Zametke zasebnosti lahko zasledimo že v biblijskih zapisih,[1] v Koranu, v judovski tradiciji, v antični Grčiji in starodavni Kitajski, kar kaže na to, da zasebnost poznajo različne kulture in družbe. Zato lahko zasebnost definiramo kot nekaj kaj je medkulturno in medvrstno univerzalno, ter ni značilno samo za človeka (Kovačič 2006, 11). Zasebnost torej ni značilna le za ljudi, pač pa je značilna tudi za vsa druga živa bitja, tudi za živali. Te se po mnenju Alana Westinga (v Wagner DeCew 1997, 12) v določenih obdobjih zatečejo v samoto ali v intimen objem manjših skupin, kar prikazuje njihovo zasebnost. Prav tako pa se njihova zasebnost izraža in kaže, ko živali branijo svoj lasten teritorij. Vendar pa se je današnja, sodobna zasebnost po mnenju Kovačiča (2006,11) rodila oziroma izoblikovala nekaj stoletij kasneje, v času razsvetljenstva, kot *pravica do zasebnosti*, ki se nekoliko jasneje začne izražati šele v času kodificiranja univerzalnih človekovih pravic, a kljub temu je že v tistem času, v 18. stoletju, bila kar dobro poznana vsem.

[1] Zasebnost se v biblijskih zapisih kaže kot zavedanje Adama in Eve, da sta gola, prav tako zavedanje Noeta o svoji goloti, ki je povezana s sramjo (Wagner DeCew 1997, 11).

»Čeprav se pravica do zasebnosti, kot vrednota in posledično kot pravica začne uveljavljati šele v 18. stoletju, pri njenem priznanju ne gre za proces, katerega obseg bi se skozi čas širil, temveč ravno nasprotno« (Kovačič 2006, 11). Pomen zasebnost se torej skozi zgodovino oža, prav tako pa pravica do zasebnosti v zadnjih letih postaja čedalje bolj omejena, saj v današnji družbi izgublja svoj osnovni pomen, saj je današnji sovražnik posameznikove zasebnosti družba, ki je kot črv, ki vrta v zasebnost posameznika, katerega v zadnjih letih lahko označimo za zelo dobičkonosen posel. Vendar pa pri tem nikakor ne smem izključiti tudi države, ki po eni strani posega v posameznikovo zasebnost, po drugi strani pa posameznika varuje pred radovedno družbo (Kovačič 2006, 11).

Danes, ko govorimo o zasebnosti, po mnenju Pavčnika (1997, 116–17), govorimo predvsem o pravici do zasebnosti, katere osrednja prvina je možnost, da posameznik na določen način ravna, medtem ko pravo to pravico dodeljuje posamezniku zato, da ta lahko zadovoljuje svoje interese, potrebe.

Prva definicija zasebnosti pa se je pojavila v Združenih državah Amerike, kjer je zasebnost pomenila biti sam oziroma *right to be left alone*. Ta se je prvič pojavila v članku Wareena in Brandeisa, ki je predstavljala odziv na konflikt med vsiljivimi mediji in posameznikom, ko je ta zahteval kontrolo nad svojim imenom in videzom, da ga pustijo pri miru (Bohinc in Gradišar 1999, 240).

Bellottijeva (v Kovačič 2006, 40) kasneje ugotavlja, da je mogoče pravico do zasebnosti definirati na dva načina, normativno in operativno. Normativna definicija po njenem mnenju govori o tem, da so nekateri vidiki posameznikove narave in njegovih dejanj zasebni, kar pomeni, da se jih ne sme razkriti drugim. Ta definicija, pravice do zasebnosti, je izrazito kulturno pogojena, saj lahko nekatera enaka dejanja v nekaterih kulturah pomenijo poseg v zasebnost, medtem ko so v drugih povsem neproblematična. Prav tako je ta definicija tudi kontekstualno pogojena. Različen kontekst je možno videti v primeru identifikacijskih kartic oziroma osebnih izkaznic, ter v videonadzorih. Kot ugotavlja Kovačič (2006, 40) vlada v Združenih državah Amerike in v Veliki Britaniji proti osebnim izkaznicam velik odpor, saj je po njihovem mnenju identifikacija z osebno izkaznico v veliki meri povezana s posegom v zasebnost posameznika, medtem ko so v celinski Evropi osebne izkaznice nekaj vsakdanjega. Operativna

definicija pravice do zasebnosti pa je po mnenju Bellotijeve bolj operacionalna in se nanaša na nadzor nad dostopom, kjer se posameznik sam odloči koliko informacij želi izmenjati z okolico in kdaj. [2]

Torej zasebnost danes ne moremo definirati le z eno samo definicijo, saj jo različni teoretiki in praktiki definirajo različno, a kljub temu je vsem definicijam zasebnosti enako, da je zasebnost danes v sodobnih državah označena in uzakonjena kot temeljna vrednota in pravica vsakega živega bitja. »Prvi začetki zakonodaje, ki ščiti zasebnost, segajo v leto 1361, ko je v Angliji zakon Justices of the Peace Act predvidel kazen za tiste, ki so skrivaj opazovali druge posameznike ali jim prisluškovali. Medtem ko so leta 1400 tudi že na zahodu začeli bolj šifrirati vsebino občutljivih pisem« (Kovačič 2006, 49).

2.1.2 Razvoj pojma informacijske zasebnosti

Že leta 1928 je znameniti sodnik Vrhovnega sodišča v Združenih državah Amerike, Louis Brandeis, v enem izmed svojih primerov, telefonskega prisluškovanja zapisal: »Napredek znanosti, ki državi omogoča nove možnosti vohunjenja, se ne bo ustavil pri elektronskem prisluškovanju, telefona. Nekega dne bo razvoj znanosti državi omogočil reproduciranje papirjev, ne da bi jih dejansko fizično vzela iz obdolženčevega predala, in bo tako lahko sodišču razkrila najbolj intimne informacije iz njegove zasebnosti. Dosežki v fiziki in sorodnih znanostih bodo prinesli sredstva za raziskovanje neizraženih mnenj, misli, čustev« (Klemenčič 2003, 102).

Louis Brandeis se pred manj kot tisoči leti v svojem predvidevanju ni niti malo uštel. Saj je že v takratnem času napovedoval razvoj znanosti in tehnologije, ki je danes v moderni družbi še kako pomembna, predvsem informacijska tehnologija, računalniki in internet oziroma računalniško omrežje, ki omogočajo zasebnost a na nek način predstavljajo tudi sredstvo s katerim lahko posežemo v posameznikovo zasebnost.

[2] Informacija je znanje o predmetih, stvareh, pojmih, torej o stvareh, ki nas obdajajo (Vintar 2006, 53).

Informacijsko tehnološki razvoj, katerega je napovedal že Louis Brandeis, je zaradi nove informacijske tehnologije pripeljal do prvega sprejetega zakona na področju informacijske zasebnosti, ki ga je sprejela nemška dežela Hesse leta 1970, kot odgovor na reakcije ob vzpostavljanju informacijskega sistema, ki bi omogočal centralizacijo, povezovanje in nastanek velikih zbirk podatkov. Razlogi za javen odpor proti takšnim načrtom, so tičali v negativni izkušnji Nemčije, ko so nacisti v času 2. svetovne vojne uporabljali Hollerithove stroje[3] za popis prebivalstva.

Nova tehnologija, osebni računalniki, pa so se začeli intenzivno uporabljati od leta 1980, pri čemer so se prav tako intenzivno začeli združevati s področjem komuniciranja, kar pripelje do povezanosti zasebnosti osebnih podatkov in zasebnosti osebnega komuniciranja,[4] to kombinacijo pa lahko poimenujem kar informacijska zasebnost.

Informacijska zasebnost je po mnenju Pestotnikove (2007, 15) možnost posameznika, da obdrži podatke in informacije o sebi. To pravico je po mnenju Bohinčeve in Gradišarja (1999, 240) potrebno upoštevati pri zbiranju, obdelovanju, prenosu in shranjevanju podatkov in pri njihovi uporabi. Vendar pa včasih pride do zlorabe zasebnosti, na kar je opozoril že Brandeis, ki jih omogoča nova informacijska tehnologija, internet.

2.2 NASTANEK SODOBNE VARNOSTI

Kot zasebnost se je občutek varnosti pojavil sočasno z nastankom človeka, ko je ta ugotovil, da živi v neprijaznem svetu, kjer mu vsaki dan preti sovražnik. Človek je torej zaradi nevarnosti razvil občutek varnosti, ko se je ta zavaroval pred pretečo se mu nevarnostjo. Vendar pa je včasih lahko občutek človeške varnosti nerealen.

[3] Hollerithov stroj ali angleško *Hollerith machine* je predhodnik današnjih osebnih računalnikov, tega je izumil konec 19. Stoletja Herman Hollerith, kot posebno napravo za obdelovanje podatkov. Tega so najprej uporabljali za analizo podatkov v ZDA pri popisu prebivalstva leta 1890. Medtem ko ga je tretjih rajh, leta 1933 začel uporabljal za popis prebivalstva, katerega glavni namen je bila identifikacija judovskega prebivalstva in izdelava načrta za učinkovito deportacijo in zaplembo premoženja (Black 2002, 34; 70; 77).

[4] Osebni podatek je katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen (Pirc Musar in drugi 2006, 15).

2.2.1 Varnost

»Ni varnosti na enem področju, če-le ta ni zagotovljena na vseh drugih« (Markham v Berniku in Prislanu, 2). Zato je varnost kompleksen pojem, katero mora vsaka država, skupnost zagotoviti svojemu narodu.

Varnost je razvojno gledano vgrajena kot biološki organizem, kot težnja organizma po obstoju, kot prilagajanje organizma na ogrožajoče vplive okolja. Torej je varnost pogoj za delovanje osnovnih življenjskih funkcij in je tako vzgib za razvoj, zavestno dejanje, da se stanje varnosti zmeraj znova vzpostavlja (Buzan 1983, 18).

»Varnost se nanaša torej na družbo, na državo, kot tudi na mednarodne skupnosti, zato je varnost družbena in politična vrednota, ki označuje okvir socialne in politične skupnosti. Hkrati pa omogoča obstoj družbene reprodukcije, notranji red in mir, razvoj notranje ureditve ter zagotovitev običajnih procesov diferenciacije in integracije znotraj družbe in države« (Anžič 1997, 35–6). Varnost je torej vrednota posameznika, družbe, države ter skupnosti.

Vendar pa varnost največkrat omenjamo, kot občutek, ki včasih oziroma velikokrat ni realen. Saj se naš subjektivni občutek, kako varno se počutimo v nekem okolju, le redko ujema z realnim stanjem varnosti v okolju v katerem se trenutno nahajamo. Torej lahko rečem, da absolutne varnosti ni (Schneier 2000, 1–2).

Medtem ko je po mnenju Grizolda (1992, 6) varnost stanje, v katerem je zagotovljena uravnoteženost, fizični, duhovni ter gmotni obstoj posameznika in družbene skupine v razmerju do drugih posameznikov, družbenih skupin in narave.

2.2.2 Razvoj pojma informacijska varnost

»Vse kar človek naredi, lahko človek premaga. Vse kar za to potrebuje je zadostna količina znanja, časa in denarja. Če je slednjega dovolj se bo vedno našel nekdo, ki bi storil vse, da bi onesposobil potreben del varnostnega sistema« (Robinson v Bernik in Prislan, 2).

Vendar pa preden definiram informacijsko varnost moram definirati pojem *sistem* in *informacijski sistem*.

2.2.2.1 Sistem

Za pojem sistem obstajajo različne definicije tega pojma. Vendar najpogostejša definicija sistema je, da je sistem skupina medsebojno povezanih elementov, zasnovana za doseganje nekega cilja oziroma za opravljanje neke funkcije. Sistem je skupina objektov, združenih po pravilih medsebojne interakcije.

Medtem ko so posamezni deli sistema po mnenju Vintarja (2006, 40) elementi, ki imajo določene lastnosti in funkcije, katere so povezane z lastnostmi in funkcijami drugih elementov sistema.

2.2.2.2 Informacijski sistem

Človek za opravljanje najpogostejših aktivnosti po mnenju Vintarja (2006, 40) potrebuje znanje. Znanje pridobiva s pomočjo informacij, ki jih sprejema iz svojega okolja, torej iz realnega sveta. Vendar pa pretok in izmenjava informacij ni samo osnovna potreba vsakega človeka, družbe, ampak je temelj funkcioniranja večine tehničnih sistemov, med katere uvrščamo tudi informacijske sisteme.

Informacijski sistem je pojem, ki se danes pogosto pojavlja v sodobni literaturi, vendar pa še vedno ne obstaja enotna definicija tega pojma. Razlogi za to so po mnenju Vintarja (2006, 54) v izredno široki paleti informacijskih sistemov, ki jih lahko vsakodnevno srečamo v praksi. Vendar pa je po njegovem mnenju informacijski sistem del poslovnega sistema, ki obravnava le-tega z informacijskega vidika.

Medtem ko je po mnenju Simčiča (2007, 10–11) informacijski sistem celotna infrastruktura, osebje in komponente, ki so namenjene zbiranju obdelovanju, shranjevanju, oddajanju, prikazovanju, širjenju in dispoziciji informacij.

Informacijski sistem pa je po mnenju Kojca (2010, 20) sestavljen iz treh glavnih delov:

- strojne opreme,
- programske opreme in
- standardov informacijske varnosti.

2.2.2.3 Informacijska varnost, računalniška varnost in varnost informacijskih sistemov

Informacijska varnost je področje, ki se ukvarja z varovanjem podatkov pred nepooblaščenim dostopom, uporabo, razkritjem, uničenjem, spremembo ali nerazpoložljivostjo. V angleškem izvoru, *information assurance*, se beseda uporablja kot sinonim za informacijsko varnost, računalniško varnost ter varnost informacijskih sistemov, vendar si te varnosti v marsičem niso enake (Gaberšček 2007, 13).

Informacijska varnost se ukvarja z varovanjem informacij, ne gleda na njihovo obliko, bodisi elektronsko, papirno ali drugo, medtem ko *varnost informacijskih sistemov* omogoča varovanje sistemov, ki omogočajo hrambo, procesiranje, predstavitev ali prenos informacij. Ta, varnost informacijskih sistemov, pa daje velik poudarek na zasebnost podatkov, informacij, pri čemer upošteva vse predpisane zakonske in druge določbe. *Računalniška varnost* pa se osredotoča le na zagotavljanje varne uporabe računalnikov (Gaberšček 2007, 13).

Kot sem že zapisal, varnost informacijskih sistemov, ki bo v nadaljevanju moje diplomske naloge bolje predstavljena na ravni Evropske unije, kot tudi na ravni Slovenije, po mnenju Haydena (v Kojcu 2010, 16) omogoča zaščito informacijskih sistemov pred nepooblaščenimi dostopi ali modifikacijami informacij, najsi bodo ti v shranjeni obliki, v procesu ali prenosu, ki omogoča zaščito pred zatajitvijo delovanja pooblaščenim uporabnikom ter zagotavlja delovanje nepooblaščenim uporabnikom, vključno z vsemi ukrepi za odkrivanje, dokumentiranje in zavračanje tovrstnih groženj.

3 VARNOST INFROMACIJSKE ZASEBNOSTI V EVROPSKI UNIJI

3.1 NASTANEK IN REGULATIVNI PRISTOP EVROPSKE UNIJE

Evropska unije je nastala na temelju ideje evropske povezanosti, ki je sprava bila imenovana kot Evropska skupnost, medtem ko se je šele leta 1992 preimenovala v Evropsko unijo. Danes je v njo vključenih 27 držav Evrope, držav članic, katere pa so se zavezale s pristopno pogodbo, da bodo upoštevale pravni red Evropske unije.

3.1.1 Nastanek Evropske unije

Evropska unija je posledica ideje evropske povezanosti, ki sega v čas pred našim štetjem, natančneje v leto 355 pred našim štetjem, ko je 81-letni atenski govornik Istokrat zapisal svoj manj znani spis ki govori o miru. Omenjen spis govori o mirovnih pogajanjih Aten s Hiosom, Kosom, Rodosom in Bizancem. Torej spis ne govori o združevanju Evrope, vendar po mojem mnenju spada med začetke evropskega združevanja, saj kot je Accetto (2006, 86) dejal, Istokar sodi v historični prikaz evropskega združevanja oziroma lahko ta tvori njegov začetek, saj spis o miru vsebuje vse poglavitne motive in predpostavke združevanja, ki jih najdemo pri kasnejših pobudah in ki so tudi temelji današnje Evropske unije. Vendar je od tedaj pa do nastanka Skupnosti, preteklo kar nekaj časa, da se je njegova ideja o evropski povezanosti uresničila (Accetto 2006, 84). Medtem ko je ideja o ustanovitvi Evropske skupnosti priletela na plodna tla šele, ko je francoski minister za zunanje zadeve, Robert Schuman razklano in s sovraštvom napolnjeno Evropo opozoril na nevarnost pred tretjo svetovno vojno, [5] prav tako pa je v svoji izjavi predlagal oblikovanje skupnega trga v dveh pomembnih gospodarskih panogah, ki so ju do tedaj uporabljali v vojaške namene, in sicer v industriji premoga in jekla (Moussis 1999, 30-1).

[5]Robert Schuman je 9. maja 1950 dejal, da Evrope ne bo mogoče ustvariti naenkrat ali po enostavnem načrtu, pač pa se bo lahko zgradila le s konkretnimi dosežki, ki bodo najprej ustvarili dejansko solidarnost (Moussis 1999, 30–1).

Torej zaradi Schumanovega znamenitega govora, so Evropejci začeli razmišljati o ustanovitvi Skupnosti, katero so leta 1951 uresničile s podpisom prve evropske pogodbe, Pogodbe o Evropski skupnosti za premog in jeklo. Zaradi velike dinamike integracijskih procesov, je bila leta 1992 v Maastrichtu podpisana Pogodba o Evropski uniji, ter s tem se je Skupnost preimenovala v Evropsko unijo. Države članice, ki so vstopile v to skupnost pa ob podpisu pristopne pogodbe izgubijo del svoje suverenosti, kajti pravo Evropske unije je nad pravom držav članic.

3.1.2 Regulativni pristop Evropske unije na področje varnosti informacijske zasebnosti

Zasebnost je danes v večini evropskih držav ustavna kategorija, kar pomeni, da je zapisana v ustavi držav članic kot pravica vsakega njenega državljana. Omeniti velja, da imajo v Avstriji poseben zakon o varstvu osebnih podatkov, katerega del ima ustavni status, medtem ko je v Franciji in na Norveškem ustavno sodišče presodilo, da je pravica do zasebnosti v ustavi omenjena implicitno (Kovačič 2006, 71).

Z razvojem in nastankom množičnih mikroprocesorskih tehnologij uporaba velikih računalniških sistemov ni bila več ekonomsko upravičena. Saj je nastanek množičnih majhnih, poceni ter zmogljivih računalnikov do tedaj, zaščito informacijske zasebnosti, obrnil v povsem drugo smer, saj je bilo novo, razpršeno tehnologijo veliko težje nadzirati. Zato so se v Evropi odločili, da je potrebno zaradi razvoja nove tehnologije zakonodajo razširiti, ne samo na primarni sektor ampak tudi na zasebni sektor, skupaj z majhnimi podjetji (Kovačič 2006, 75). Saj so ugotovili, da niso podatki tisti, ki potrebujejo zaščito, temveč da zaščito potrebuje posameznik. Zato so postopoma začeli uvajati pravice. Prva takšna pravica je bila, da je zbiranje podatkov bilo mogoče le na podlagi zakona ali s soglasjem posameznika, pri tem so posamezniki morali biti obveščeni o namenu zbiranja, obenem pa so imeli pravico zahtevati spremembo ali celo izbris netočnih podatkov (Mayer-Schonberger v Kovačič 2006, 75). Prišlo je do premika, informacijska zasebnost ni bila več problem nacionalnih držav, pač pa je v 80. letih 20. stoletja postala mednarodni izziv (Bennett v Kovačič 2006, 75).

Zato je Organizacija za ekonomsko sodelovanje in razvoj (*Organisation for Economic Co-operation and Development* – OECD) leta 1980 sprejela *Smernice za zaščito in čezmejni pretok osebnih podatkov.*[6] V teh Smernicah je bilo izrecno navedeno, da velja tako za javni, kot za zasebni sektor, načelo poštenega in zakonitega ravnanja z osebnimi podatki. Prav tako pa je v teh smernicah, v 17. točki, bilo izrecno določeno, da je omejitev čezmejnega pretoka podatkov mogoča, kadar država, v katero so podatki namenjeni, ne spoštuje teh Smernic.

Medtem ko zametki regulativne pristojnosti na področju varstva informacijske zasebnosti v Evropski uniji segajo leto dni kasneje, v leto 1981, ko je Svet Evrope podpisal in tudi sprejel *Konvencijo o varstvu posameznikov glede avtomatske obdelave podatkov*. Ta Konvencija je bila pripravljena na podlagi Smernic, medtem ko je njen pomen bil, da imajo države članice prav poseben zakon o varstvu osebnih podatkov ter imajo vzpostavljen nadzorni organ, ki bdi nad varstvom informacijske zasebnosti. Čeprav se v praksi zakonodaje, ki zadeva varovanje informacijske zasebnosti, ta mnogokrat ne upošteva, imajo potrošniki in državljani v Evropi vsaj možnost pritožbe, popravka napačnih podatkov ali uporabe drugega pravnega sredstva (Kovačič 2006, 71).

Torej je Konvencija določala, da se smejo osebni podatki uporabljati in shranjevati samo za zakonite namene in pošteno. Zbirati se torej smejo samo podatki, ki so ustrezni in v skladu z namenom za katerega se zbirajo, medtem ko njihov upravljalec mora zagotoviti njihovo točnost in posodobljenost ter jih ne sme hraniti dlje, kot je potrebno za dosego njihovega namena, zaradi česar se zbirajo (Čebulj 2002, 411).

Uvedba Konvencije, ki je omogočala zaščito informacijske zasebnosti je v praksi naletela na kar nekaj težav. Ena njenih večjih težav je bila v njeni ne definiciji. Ta problem pa je skušala rešiti Evropska unija v svoji direktivi, *Direktivi o zaščiti osebnih*

[6] Smernice za zaščito in čezmejni pretok osebnih podatkov ali izvorno *Guidelines on the Protection of Privacy and Transborder Plows of Personal Date* vsebujejo osem načel: 1. načelo omejevanja pri izbiri podatkov, 2. načelo kvalitete podatkov, 3. načelo ciljev zbiranja podatkov, 4. načelo omejene uporabe podatkov, 5. načelo varstva hranljivih podatkov, 6. načelo vpogleda v hranjene podatke, 7. načelo aktivnosti posameznika in 8. načelo odgovornosti (Lempe 2003, 138).

podatkov iz leta 1995,[7] čeprav je njen prvi osnutek bil pripravljen že leta 1990. Njen namen je bila uskladitev zakonodajnega varstva v vseh državah članicah. Vendar pa je njen pomen bil tudi v tem, da je jasno izpostavila povezavo med zaščito osebnih podatkov in temeljnimi pravicami in svoboščinami posameznika, prav tako pa je iz njenih točk možno razbrati željo o zagotovitvi neoviranega pretoka osebnih podatkov med državami. Ta želja je jasno razvidna iz 2. točke 1. člena Direktive 95/46/EC, kjer je jasno določeno, da »države članice ne smejo omejevati ali prepovedati prostega pretoka osebnih podatkov med državami članicami zaradi razlogov«. Prav tako pa je v njenem 28. členu določena zahteva po ustanovitvi neodvisnega nadzornega organa, ki skrbi za spoštovanje zakonodaje za zaščito zasebnosti (Kovačič 2006, 78). V Sloveniji to nalogo opravlja informacijski pooblaščenec, medtem ko drugod po Evropi to nalogo opravljajo pooblaščene agencije, pooblaščenci ali posebni 'ombudsmani', ki morajo imeti določeno stopnjo pooblastil (Laurant v Kovačič 2006, 78).

Zaradi vse večjega naraščanja osebnih računalnikov in posledično vse večje uporabe leteh v organizacijah, je leta 2001 bila sprejeta *Uredba (ES) št. 45/2001 evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov.*[8] Ta v svojih določilih določa pravila in standarde ravnanja organov Evropske unije z osebnimi podatki, torej ureja enake pravice in obveznosti, kot Direktiva 95/46/ES, vendar na ravni institucije in organov Skupnosti. Uredba (ES) št. 45/2001 pa določa ustanovitev Evropskega nadzornika za varstvo podatkov. In sicer so naloge Evropskega nadzornika za varstvo podatkov po mnenju Kmetca (2010, 12):

- Nadzor, kot zagotavljanje, da institucije EU spoštujejo temeljno pravico do varstva osebnih podatkov.
- Svetovanje glede predlagane nove zakonodaje, ki vpliva na varstvo osebnih podatkov.
- Sodelovanje z drugimi pomembnimi udeleženci na tem področju.

[7] Direktiva 95/46/EC oziroma *Directiva of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal date on the free movement of such date.*

[8] *Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data*.

Leto kasneje, je bila sprejeta *Direktiva 2002/58/ES o varstvu zasebnosti v elektronski komunikaciji oziroma e-komunikacijska direktiva*, ki je nastala kot odgovor moderni informacijski družbi, ki v današnjem svetu temelji na zmogljivi računalniški tehnologiji, katera s pomočjo elektronske komunikacije krši elektronsko zasebnost. Namen te sprejete direktive je bil v ojačanju dosedanje zakonodaje o varstvu podatkov v telekomunikacijskem sektorju, ki vključuje splošno telefonijo, elektronsko pošto, uporabo svetovnega spleta, kot tudi SMS sporočila. Ta e-komunikacijska direktiva pa vsebuje v svojem 15. členu, ki se navezuje na 23. člen Direktive o varnosti osebnih podatkov iz leta 1995, da morajo države članice zagotoviti, da je vsaka oseba, ki je utrpela škodo kot rezultat protipravne operacije ali kakršnegakoli dejanja v nasprotno z zakonodajo, upravičena uveljaviti odškodnino od odgovorne osebe. Medtem ko je primarno načelo te direktive zagotoviti varnost (Lampe 2003, 147; 149–50).

Naslednja pomembna direktiva je *Direktiva 2006/24/ES o hrambi podatkov pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih storitev ali javnih komunikacijskih omrežij.*[9] Namen te direktive je uskladiti določbe držav članic glede obveznosti ponudnikov javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij glede hrambe določenih podatkov, ki jih pridobivajo ali obdelujejo, da se zagotovi dostopnost podatkov za namen preprečevanja, preiskovanja, odkrivanja in pregona hudih kaznivih dejanj, kakor jih opredeljuje nacionalna zakonodaja vsake od držav članic. Ta direktiva se uporablja za podatke o prometu in lokaciji pravnih subjektov in fizičnih oseb, kakor tudi za povezane podatke, potrebne za določitev naročnika ali registriranega uporabnika. Ne uporablja se za vsebino elektronskih komunikacij, vključno z informacijami, pregledanimi z uporabo elektronskega komunikacijskega omrežja (1. člen Direktive 2006/24/ES).

[9] *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.*

3.1.2.1 Pravna praksa: Vpliv ameriške izkušnje »koncept razumnega pričakovanja zasebnosti« na evropska tla

Koncept razumnega pričakovanja zasebnosti je bil utemeljen v ustavnopravni praksi Vrhovnega sodišča ZDA, katerega je v kasnejših letih sprejelo tudi Evropsko sodišče za človekove pravice (ESČP). Ta koncept temelji na posameznikovem svobodnem izvrševanju pravic do zasebnosti v sferi, kjer lahko ta upravičeno in razumno pričakuje uživanje svoje zasebnosti brez vmešavanja državne oblasti. Ta koncept pa je tesno povezan s prostorsko kot tudi z informacijsko zasebnostjo (Lampe 2003, 131). Četrti amandma ameriške ustave zagotavlja človeku pravico biti varen v svoji hiši, s svojimi papirji in dokumenti, kot tudi pred nerazumnimi preiskavami, »*unreasonable searches and seizures*«. Na temelju tega amandmaja pa ameriška sodna praksa poudarja, da je s tem amandmajem človek zavarovan pred nezakonitimi kršitvami svetosti doma, kar pomeni, da je človekov dom človekov grad. Zato je Vrhovno sodišče ZDA uveljavilo pravico posameznika, da se ta umakne v svoj dom, kjer je prost pred nerazumnimi vdori državnih organov (Lampe 2003, 131).

Leta 1967 se je končal odločilen primer *Katz* v ZDA,[10] v katerem je Vrhovno sodišče preseglo prostorski vidik varstva posameznikove zasebnosti in ustvarilo 'test' razumno pričakovane zasebnosti, katero merilo je prevzelo ESČP v odločbi primera *Halford* proti Združenemu kraljestvu, v katerem je šlo za vprašanje ali je varovana 'razumno pričakovana zasebnost' policistke, ki je telefonirala z uradnega telefona na policijski postaji (Zupančič v Mihelič 2009, 102).

Gospa Halford, ki je bila pomočnica poveljnika policije v Merseyside, je imela svojo pisarno in dva telefona, od katerega je bil en za zasebno uporabo. Telefona sta bila del notranje mreže policije v Merseysidu, telekomunikacijskega sistema zunaj javnega omrežja. Glede uporabe telefonov ji niso bile naložene nikakršne prepovedi niti ji niso bila dana posebna navodila. Halfordova je v tem primeru zatrjevala, da so bili klici,

[10] Primer Katz velja v ZDA za enega temeljnih primerov glede pravice do zasebnosti. Ta primer temelji na pritožbi obtoženega, ki se je pritožil zaradi obsodbe, ki je temeljila na dokaznem materialu, katerega je policija pridobila brez predhodnega sodnega naloga s prisluškovanjem obtoženčeve komunikacije v javni telefonski govorilnici. Zato se je obtožen skliceval na dejstvo, da kdo hoče plačati telefonski pogovor zapre vrata svoje govorilnice in nedvomno pričakuje , da njegove besede ne bodo predvajane svetu. Zato je po tem javni telefon namenjen zasebni komunikaciji, kar določa četrti amandma Ameriške Ustave (Lampe 2003, 131–2).

opravljeni z njenega domačega telefona in telefonov v pisarni, nadzorovani z namenom, da bi bila njihova vsebina uporabljena proti njej v postopku glede diskriminacije (Mihelič 2009, 102–3).[11]

Sodišče je v tem primeru poudarilo, da sodijo klici tako iz poslovnih prostorov kot iz zasebnih pod zasebno življenje, zato je zavzelo stališče, da je Halfordova razumno pričakovala zasebnost. Zato je sodišče odločilo, da obstaja razumna verjetnost, da je njene klice nadzorovala policija iz Merseysida z osrednjim ciljem, da ta zbere gradivo za njeno obravnavo v postopku zaradi diskriminacije. To je pomenilo vmešavanje javne oblasti brez pravne podlage (Mihelič 2009, 103).

3.2 VARSTVO INFORMACIJSKE ZASEBNOSTI

Pred iznajdbo današnjih sodobnih naprav je posameznik bil lahko skorajda prepričan, da mu v zasebnih prostorih nihče ne prisluškuje. Tudi vdor v zasebnost večje skupine ljudi je bil pred iznajdbo računalnikov skorajda nemogoč, saj so takrat bile informacije pogosto raztresene in težko dostopne, medtem ko je danes vdor v bazo podatkov lahka naloga ljubiteljev računalnikov. Zato je danes potreba po varstvu zasebnosti še kako pomembna, saj danes nove kršitve zasebnosti omogoča nova, moderna informacijska tehnologija (Pirc Musar in drugi 2006, 13).[12]

Evropska unija na tem področju poskuša s svojimi direktivami in uredbami, pravnimi akti, doseči ravnotežje med pravico do zasebnosti in med legitimnimi razlogi za uporabo osebnih podatkov, kot tudi poenotiti področje varovanja informacijske zasebnosti v Skupnosti ter v vseh njenih državah članicah. Zato je Evropska unija v svoji Direktivi 95/46/EC določila, da morajo imeti države članice nadzorni organ, ki skrbi za izvajanje njenih predpisov, medtem ko je z kasnejšo direktivo, Direktivo 2002/58/ES določila Evropskega nadzornika za varstvo podatkov, ki nadzoruje, svetuje in sodeluje z ostalimi institucijami Evropske unije.

[11] Halfordova se je kar sedem let potegovala za mesto namestnika poveljnika policije in je zaradi domnevne spolne diskriminacije začela postopek pred delovnim sodiščem (Mihelič 2009, 102).

[12] Nove tehnologije omogočajo vdor v zasebnost predvsem s prisluškovanjem telefonskih pogovorom, uporaba mikrofona in drugih elektronskih naprav, zbiranje, shranjevanje in iskanje informacij z videokamerami, računalniki in podobno (Pirc Musar in drugi 2006, 13)

Torej direktive imajo največji pomen pri varstvu informacijske zasebnosti v Evropski uniji, prav tako pa imajo pomen pri prepovedanemu iznosu zasebnih podatkov, kot tudi pri kazni vdora v informacijsko zasebnost.

3.3 IZNOS PODATKOV IZ EVROPSKE UNIJE V DRŽAVE TRETJEGA SVETA

V Evropski uniji se vsak dan preko podjetij, javnih ustanov, kot tudi s pomočjo posameznikov prenesejo velike količine osebnih podatkov prek meja držav članic kot tudi znotraj Skupnosti. Prenos podatkov med državami je danes še kako pomemben, saj je to orodje s pomočjo katerega se vrši mednarodno sodelovanje. Da pa ta pretok steče so potrebna pravila, da ne bi prišlo do njihove zlorabe. Zato je Evropska unija sprejela Direktivo o varstvu podatkov, Direktiva 95/46/ES, s katero določa posebna pravila za prenos osebnih podatkov zunaj njenih meja. Saj le s pravnim redom vrši in zagotavlja zaščito podatkov svojih državljanov.

Direktiva 95/46/ES določa v svojem 25. členu prenos osebnih podatkov v tretjo državo, ki se lahko izvede le, če je prenos podatkov v tretjo državo dovoljen s strani nacionalne zakonodaje posamezne države članice oziroma, če tretja država nudi ustrezno varnost osebnih podatkov. Države članice in Komisija se medsebojno obveščajo o primerih za katere menijo, da tretja država ne zagotavlja ustreznega varstva osebnih podatkov. V primeru, da Komisija ugotovi, da tretja država ne zagotavlja ustrezne ravni varstva osebnih podatkov, države članice same sprejmejo ukrepe, ki so potrebni za preprečevanje kakršnih koli prenosov podatkov v tretjo državo (25. člen Direktive 95/46/ES).

3.3.1 Iznos osebnih podatkov iz Evropske unije v ZDA

Leta 1998 so ameriške oblasti ugotovile, da omejitve pri pretoku osebnih podatkov iz Evropske unije v ZDA utegnejo škodovati ameriškemu gospodarstvu, zato je bolje da skupnosti med seboj podpišeta sporazum, *Safe Harbor Agreement* oziroma Varnostni sporazum. Ta predvideva, da bodo ameriška podjetja prostovoljno odločila sama o spoštovanju načela o zaščiti zasebnosti, ki sta jih pripravila ameriško trgovinsko ministrstvo in uprava za interni trg Evropske komisije (v Kovačič 2006, 79). Ta sporazum pa je kljub številnim kritikam bil sprejet leta 2000. Vendar kljub poročilu o uspešnosti tega projekta, se je vprašanje o pretoku podatkov izostrilo, ko so ZDA zahtevale od EU, da jim ta naj sporoča podatke o letalskih potnikih, ki letijo iz njihove Skupnosti v ZDA, čeprav pa ne smemo zanemariti tudi zahtevo ZDA da naj EU uvede biometrične potne liste.

EU je zahtevo ZDA, kljub nasprotovanju Evropskemu parlamentu sprejela s posebnim sporazumemo o letalskih potnikih med EU in ZDA. Vendar pa je kasneje Evropsko sodišče presodilo, da je ta sporazum nezakonit, zato je sporazum med EU in ZDA bil razveljaven. Saj so ZDA 15 minut po vzletu letala dobile kar 30 podatkov od vsakega potnika, medtem ko ZDA ne zagotavljajo ustrezne zaščite varnosti teh osebnih podatkov (Kovačič 2006, 80).

4 VARNOST INFORMACIJSKE ZASEBNOSTI V REPUBLIKI SLOVENIJI

4.1 REGULATIVNI PRISTOP SLOVENIJE NA PODROČJU VARNOSTI INFORMACISJKE ZASEBNOSTI

Ustava (Ur.l. RS, št. 33I/1991, 68/2006, v nadaljevanju Ustava RS), kot najvišji pravni akt v Republiki Sloveniji, v svojem okviru zagotavlja pravico do zasebnosti in osebnih pravic, varstvo tajnosti pisem in drugih občil ter varstvo osebnih podatkov skozi določbe.

Ta v svojem 35. členu določa, da je z Ustavo RS zagotovljena nedotakljivost človekove telesne in duševne celovitosti, njegove zasebnosti ter osebnostnih pravic. Kar po mnenju Oreharja (v Miheliču 2009, 32) ta člen poudarja zagotovljeno celotno varstvo vseh pravic osebnosti ne glede na to ali so z Ustavo izrecno urejene ali ne. Omenjene pravice so zagotovljene vsem fizičnim osebam, državljanom kot tudi tujcem, ter državljanom brez statusa ne glede ali so ti poslovno sposobni ali ne. Medtem ko so pravne osebe naslovniki tovrstnih pravic le v primeru, če se lahko varovane pravice po svoji naravi nanašajo tudi naj.

Medtem ko v svojem 37. členu Ustava RS navaja varstvo tajnosti podatkov in drugih občil.[13] Ta določba je danes še kako pomembna, saj s sodobno komunikacijsko tehnologijo človek lahko poseže v zasebnost posameznika. Vendar pa je ta določba nekoliko sporna, saj drugi odstavek tega člena določa, da lahko zakon predpiše, da na podlagi odločbe sodišča za določen čas ne upošteva tajnosti pisem in drugih občil in nedotakljivosti človekove zasebnosti, če je to nujno za uvedbo ali potek kazenskega postopka ali varnosti države. Zato lahko ta odstavek po mnenju Lampea (2003, 134) jemljemo kot eno bolj dvoumnih določb naše slovenske ustave. Vendar pa je takšen poseg države v posameznikovo zasebnost upravičen, če je določen z zakonom. Medtem ko 38. člen Ustave RS določa varstvo osebnih podatkov,[14] po katerem je varstvo

[13] Občila ali medij je vsako komunikacijsko sredstvo, kot so knjige, časopisi, letaki, plakati, kot tudi sodobna komunikacija tehnologija, kamor uvrščamo radio, televizijo, računalnik splet in medmrežja.

[14] »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

osebnih podatkov v državi ena izmed z ustavo zagotovljenih človekovih pravic in temeljnih svoboščin. Ta določba, določba 38. člena Ustave RS zagotavlja varstvo osebnih podatkov, prepoveduje uporabo osebnih podatkov v nasprotju z namenom njihovega zbiranja, vsakomur zagotavlja pravico do seznanitve z zbranimi osebnimi podatki, ki se nanašajo nanj ter pravico do sodnega varstva ob njegovi zlorabi (Pirc Musar 2010, 29).

Ustava RS pa sama ne določa varnost informacijske zasebnosti, zato skrbi informacijski pooblaščenec na podlagi Zakona o varstvu osebnih podatkov (Ur.l. RS, št. 86/2004, 94/2007-UPB1, v nadaljevanju ZVOP-1),[15] področnega zakona. Takšna ureditev je v veljavi od 31. decembra 2005, saj se je Slovenija z vstopom v EU odrekla delu svoje suverenosti, kar pomeni da pravni akti EU vplivajo in spreminjajo pravni red Slovenije. Da je Slovenija dobila informacijskega pooblaščenca,[16] pa je vplivala Direktiva 95/46/EC, ki v svojem 28. členu določa oziroma zahteva ustanovitev neodvisnega nadzornega organa, ki skrbi za spoštovanje zakonodajem, za zaščito zasebnosti. V Sloveniji ima to nalogo informacijski pooblaščenec oziroma državni nadzornik za varstvo osebnih podatkov. Pred njim pa je njegovo nalogo opravljal Inšpektorat za varstvo osebnih podatkov.

Morebitne kršitve informacijske zasebnosti se sankcionirajo po Kazenskem zakoniku Republike Slovenije (Ur.l. RS, št. 63/1994, 95/2004-UPB1, 5/2009 Odl.US: U-I-88/07-17, v nadaljevanju KZ-1), kjer je bil dodan 143. člen, ki govori o zlorabi osebnih podatkov. »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. 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. Kdor na

podatkov določa zakon. 'Vsakdo ima pravico seznaniti se z zbranimi osebnimi podatki, ki se nanašajo nanj, in pravico do sodnega varstva ob njihovi zlorabi.« (38. člen Ustave RS).

[15] Prvi člen ZVOP-1 določa, da so s tem zakonom določajo pravice, obveznosti, načela in ukrepi, s katerimi se preprečujejo neustavni, nezakoniti in neupravičeni posegi v zasebnost in dostojanstvo posameznika oziroma posameznice pri obdelavi osebnih podatkov (1. člen ZVOP-1).

[16] Informacijski pooblaščenec je samostojen in neodvisen državni organ v RS od leta 2005, ko je bil sprejet nov zakon, Zakon o informacijskem pooblaščencu (Ur.l. RS, št. 113/2005, št. 51/2007-ZUstS-A, 14/2010 Odl.US: U-I-303/08-9, v nadaljevanju ZInfP). Ta zakon je združil dva organa, in sicer Pooblaščenca za dostop do informacij javnega značaja in Inšpektorat za varstvo osebnih podatkov. Leta 2006 je ta postal državni nadzorni organ za varstvo osebnih podatkov.

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. 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« (143 .člen KZ-1).

4.1.1 Pravna praksa: primer dileme, ki ga prinaša kolizija dveh pravic in kakšne dileme prinaša uporaba nove tehnologije, internet

Leta 2004 se je zgodil prvi odmevnejši primer, ko je Banka Slovenije na podlagi zakona o plačilnem prometu na svoji spletni strani objavila podatke o vseh imetnikih transakcijskih računov, tako pravnih kot tudi fizičnih oseb. Podatki, ki so vsebovali ime, priimek in naslov oseb, brez hišnih številk ter številko računa ter evidenco o neporavnanih obveznostih, so na njihovi spletni strani bili dostopni brez omejitev. A kljub razburjenju javnosti objava teh podatkov ni bila s stališča zakona o varstvu osebnih podatkov sporna, saj je ta imela pravno podlago v zakonu o plačilnem prometu. Vendar pa je inšpektor za varstvo osebnih podatkov kljub temu izdal odločbo, s katero je prepovedal dostop do teh podatkov, saj z neomejeno objavo na internetu ni mogoče zagotoviti sledljivosti posredovanja osebnih podatkov, kot to določa 11. člen ZVOP (Kovačič 2006, 77).

4.2 VARSTVO INFORMACIJSKE ZASEBNOSTI

Kot je že zapisano je informacijski pooblaščenec v Sloveniji nadzorni organ, ki nadzoruje varstvo osebnih podatkov. Zato je njegova najpomembnejša naloga zagotavljanje enotnega uresničevanja varstva osebnih podatkov, kot tudi sodelovanje z ministrstvi pri pripravi predpisov s področja osebnih podatkov. Torej informacijski pooblaščenec je 'oko', ki skupaj s pravnimi organi gleda in odkriva kršitve zasebnosti.

4.2.1 Statistika kršitve informacijske zasebnosti

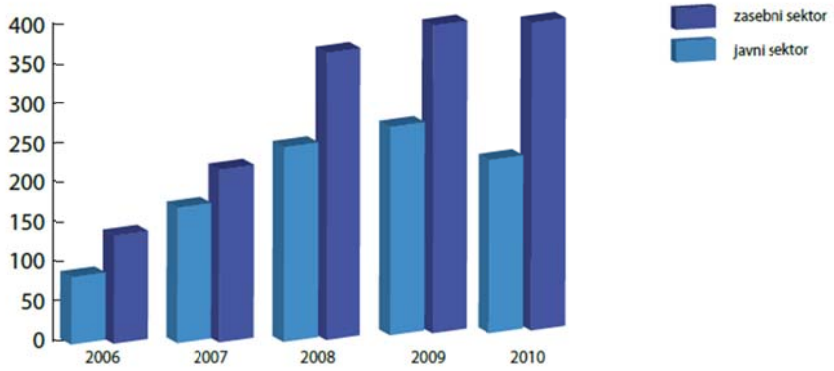
Informacijski pooblaščenec je leta 2010 zaradi suma kršitev določb ZVOP-1 vodil kar 599 zadev, od tega kar 202 v javnem sektorju in 397 v zasebnem sektorju. Leto prej, 2009, pa je informacijski pooblaščenec vodil zaradi suma kršitev določb ZVOP-1 624 zadev, od tega 219 v javnem sektorju in 405 v zasebnem sektorju, kar prikazujeta graf 4.1 in 4.2. Od tega je leta 2010 zoper pravne osebe javnega sektorja prijel 176 prijav, medtem ko je 26 postopkov uvedel sam po uradni dolžnosti. Medtem ko je zoper zasebni sektor prijel, istega leta, 367 prijav, 30 postopkov pa je uvedel sam po uradni dolžnosti. Leta 2009 pa je informacijski pooblaščenec prijel zoper javni sektor 165 prijav, 54 postopkov pa je uvedel po uradni dolžnosti. Medtem ko je zoper zasebni sektor leta 2009 prijel 332 prijav ter kar 73 postopkov je uvedel po uradni dolžnosti. Največ prijav zoper javnih institucij je bilo v letu 2010 vloženih in uvedeni po uradni dolžnosti zoper državne organe, ministrstva in organe v njihovi sestavi. Teh je bilo 57. Sledile so izobraževalne ustanove, kjer je bilo leta 2010 41 prijav, najmanj pa jih je bilo v upravnih enotah, kjer je bilo le 6 prijav. Leto prej, 2009, je bilo največ vloženih in uvedenih po uradni dolžnosti prijav zoper izobraževalne ustanove, kar 53, sledile so jim državni organi, ministrstva in organi v njihovi sestavi, kjer je bilo podanih 42 prijav, prav tako pa je tega leta bilo najmanj prijav uvedenih v upravnih enotah, le 8.[17]

[17] Podatki pridobljeni iz Letnega poročila Informacijskega pooblaščenca 2009 in 2010.

Graf 4.1: Število zadev, ki jih je zaradi suma kršitev določb ZVOP-1 vodil informacijski pooblaščenec med letoma 1996 in 2010

Vir: Pirc Musar in drugi (2011, 31)

Graf 4.2:Število zadev zaradi suma kršitev določb ZVOP-1 med letoma 2006 in 2010



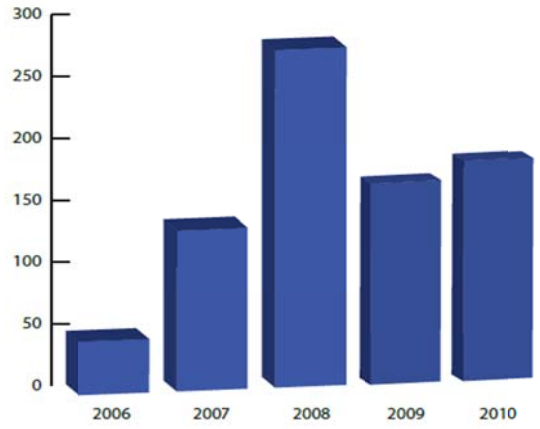
Vir: Pirc Musar in drugi (2011, 32)

V omenjenih prijavah so se leta 2010 pritožbe največkrat nanašale na posredovanje osebnih podatkov nepooblaščenim uporabnikom s strani upravljavca osebnih podatkov, in sicer leta 2010 je teh prijav bilo 52, medtem ko leta 2009 le 41 prijav. Sledijo nezakonite objave osebnih podatkov, na oglasnih deskah ali preko spleta. Zoper te nezakonitosti je leta 2010 bilo prijavljenih 37 prijav, leto prej pa kar 20. Sledi nezakonito zbiranje oziroma nezakonito zahtevanje osebnih podatkov. In sicer leta 2010 je informacijski pooblaščenec prijel kar 31 prijav, leto prej pa kar 55. Sledi neustrezno zavarovanje osebnih podatkov, zoper katerih je leta 2010 bilo podanih 22 prijav, leta

2009 pa ni bila podana nobena prijava. Za nezakonito izvajanje videonadzorov je leta 2010 bilo podanih 8 prijav, leto prej pa 11 prijav.[18]

Leta 2010 je bilo uvedenih 179 postopkov o prekršku, 45 postopkov zoper pravnih oseb javnega sektorja, 82 postopkov zoper pravnih oseb zasebnega sektorja ter 52 postopkov zoper posameznike. Leta 2009 pa je bilo uvedenih 163 postopkov o prekršku, 41 postopkov zoper pravnih oseb javnega sektorja, 70 postopkov zoper pravnih oseb zasebnega sektorja in 52 postopkov zoper posameznika. Število teh postopkov prikazuje graf 4.3, ti postopki pa se vodijo, kot je že zapisano v skladu z ZP-1.[19]

Graf 4.3: Število uvedenih postopkov o prekrških med letoma 2006 in 2010



Vir: Pirc Musar in drugi (2011, 33)

V postopkih o prekrških pa lahko informacijski pooblaščenec v skladu z zakonom izda opozorila, odločbo o prekrških ter plačilni nalog. Ta je leta 2010 izdal 36 opozoril, 116 odločb o prekrških od tega 81 opominov, 35 glob ter 10 plačilnih nalogov. Leta 2009 pa je izdal 59 opozoril, 93 odločb o prekrških od tega 67 opominov in 26 glob ter 12 plačilnih nalogov.[20]

[18] Podatki pridobljeni iz Letnega poročila Informacijskega pooblaščenca 2009 in 2010.
[19] Podatki pridobljeni iz Letnega poročila Informacijskega pooblaščenca 2009 in 2010.
[20] Podatki pridobljeni iz Letnega poročila Informacijskega pooblaščenca 2009 in 2010.

4.2.2 Najodmevnejši primeri kršitev varstva osebnih podatkov v zadnjih letih, ki jih je ugotovil in rešil informacijski pooblaščenec

V šestih letih delovanja informacijskega pooblaščenca se je na njegovem področju že izoblikovala utečena praksa, ki jo nadgrajujejo tudi odločitve sodišč. Na področju varstva osebnih podatkov se v zadnjih letih informacijski pooblaščenec inšpekcijskih zadevah in zahtevah za mnenja srečuje z vse kompleksnejšimi in zahtevnejšimi izzivi varstva informacijske zasebnosti. Kršitve, kot tudi nepravilnosti, ki so bile na področju varstva osebnih podatkov ugotovljena v zadnjih letih, se praktično ne razlikujejo od tistih, ki so bile ugotovljene v preteklosti (Pirc Musar in drugi 2010, 7).

4.2.2.1 Obdelava osebnih podatkov zavarovancev brez podlage v zakonu ali v osebni privolitvi posameznika s strani zavarovalnic

V Letu 2009 je informacijski pooblaščenec obravnaval zelo medijsko odmeven primer nezakonite obdelave osebnih podatkov, in sicer s strani dveh zavarovalnic. V tem primeru je s pomočjo inšpekcijskega postopka bilo ugotovljeno, da je ena zavarovalnica v drugo brez ustrezne pravne podlage posredovala osebne podatke o 2382 nekdanjih zavarovancih, ki so kasneje bili uporabljeni za neposredno trženje. V tem postopku je informacijski pooblaščenec zavarovalnicama in odgovornim osebam v obeh zavarovalnicama izrekel sankcije zaradi nezakonite obdelave osebnih podatkov. Ta sankcija je bila globa, ki je doslej najvišja globa, saj je prvi zavarovalnici informacijski pooblaščenec določil globo 112.590 evrov, odgovorni osebi pa 20.000 evrov, medtem ko je druga zavarovalnica bila oglobljena za 108.420 evrov, odgovorne oseba pa za 20.000 evrov (Pirc Musar in drugi 2010, 46; 50).

4.2.2.2 Primer nezakonite pridobitve osebnih podatkov potencialnih volivcev s strani političnih strank

Informacijski pooblaščenec je leta 2008 uvedel inšpekcijski postopek zaradi suma nezakonite pridobitve osebnih podatkov potencialnih volivcev v tujini za potrebe neposrednega trženja pred parlamentarnimi volitvami. Na kršitev je postal pozoren šele takrat, ko je od več posameznikov, ki živijo v tujini, prejel prijavo, kateri je bil priložen

tudi propagandni material političnih strank. V okviru inšpekcijskega nadzora je informacijski pooblaščenec dokazal, da dve politični stranki nista mogli izkazati pravne podlage za pridobivanje in hrambo naslovov slovenskih volivcev v tujini. A kljub temu se tema dvema političnima strankama ni uspelo uvrstiti v parlament (Pirc Musar in drugi 2010, 45).

4.2.2.3 Nezakoniti vpogled v osebne podatkov komitentov pri bankah

Leta 2009 je informacijski pooblaščenec izvedel sistematičen nadzor nad zavarovanjem osebnih podatkov v bančnem sektorju, v okviru katerega je preverjal zakonitost obdelave osebnih podatkov pri medbančni izmenjavi podatkov o boniteti komitentov v okviru novega sistema, SISBON, ter zakonitost dostopa do podatkov na računih komitentov. Ugotovil je, da pri medbančni izmenjavi podatkov o boniteti komitentov do nezakonitega dostopa do podatkov ne prihaja, medtem ko je ugotovil, da sta dve banki omogočile nezakoniti vpogled v podatke. Zato je zoper uslužbence bank, ki so nezakonito dostopali do podatkov na osebnih računih komitentov izrekel sankcijo v skladu z ZP-1 (Pirc Musar in drugi 2010, 46).

4.2.2.4 Obdelava osebnih podatkov uporabnikov kartice Urbana

Informacijski pooblaščenec je v inšpekcijskem postopku, ki ga je vodil zoper javnega podjetja Ljubljanski potniški promet (LPP) ugotovil, da je podjetje zbiralo in hranilo podatke o času, kraju in liniji vstopa njihovih uporabnikov, neselektivno. Zato je podjetje LPP na podlagi odločbe informacijskega pooblaščenca takoj prenehalo zbirati podatke linijskega prevoza njihovih uporabnikov, prav tako pa so morali izbrisati vse svoje zbirke linijskih podatkov njihovih uporabnikov, ki imajo mesečne vozovnice, zelenih karticah. Te podatke pa je podjetje LPP zbiralo in obdelovalo brez pravne podlage, saj zavezanec lahko beleži le podatke o številu vstopu in izstopu na določeni postaji, ne pa tudi podatke o tem, kateri potniki so bili pripeljani do želenega cilja. Informacijski pooblaščenec je LPP-ju naložil v odločbi tudi izbris statusa, upokojenec, šolska, ki se je pojavil ob predložitvi kartice k terminalu, saj je to oseben podatek, ki se ne razkriva drugim potnikom (Pirc Musar in drugi 2011, 47).

4.2.2.5 Zbiranje osebnih podatkov pri nakupu z vrednostnimi boni

V inšpekcijskem postopku, ki ga je informacijski pooblaščenec uvedel zoper trgovske družbe, je bilo ugotovljeno, da je družba od strank, ki so kupili želeno blago z vrednostnimi boni, zahtevalo oseben dokument, s katerega je trgovka prepisala strankine osebne podatke, ker naj bi prišlo do ponarejanja bonov. Ta družba je že med postopkom sama prenehala zbirati osebne podatke kupcev, vendar pa je informacijski pooblaščenec z odločbi odredil, da mora trgovska družba izbrisati vse osebne podatke strank, ki so svoj nakup plačale z boni, torej datum plačila, ime in priimek, vrsta in številka osebnega dokumenta ter registrske številke bonov (Pirc Musar in drugi. 2011, 50).

4.3 IZNOS PODATKOV IZ SLOVENIJE V TRETJE DRŽAVE SVETA

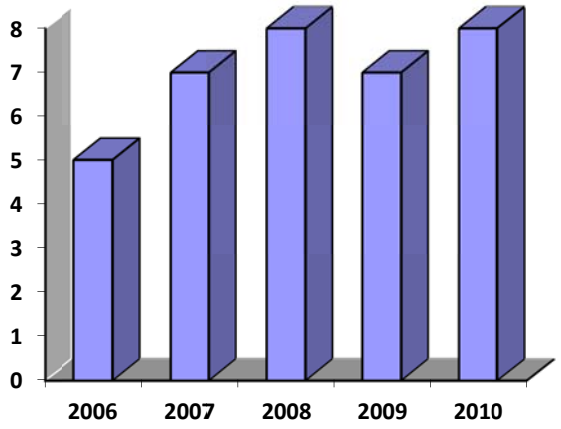
Pravila o iznos podatkov v države tretjega sveta se ne navezujejo na države Evropske unije in za države Evropskega gospodarskega prostora, kar določa 62. člen ZVOP-1.[21] Medtem ko za vse ostale države, razen držav članic EU in za Švico, Republiko Hrvaško in za ZDA[22] ne veljajo pravila o iznosu podatkov, ki so določena v 63. členu ZVOP-1, kar pomeni da v te države informacijski pooblaščenec ne rabi odobriti iznosa osebnih podatkov. Medtem ko pred iznosom v ostale, tretje, države mora tisti, ki želi podatke iznositi dobiti odločbo državnega nadzornega organa, informacijskega pooblaščenca, da država, v katero se podatki iznašajo, zagotavlja ustrezno raven varstva osebnih podatkov. Informacijski pooblaščenec je leta 2009 po mnenju Pirc Musar in drugih (2010, 39) prejel sedem vlog za iznos podatkov, kasneje je en vlagatelj vlogo umaknil ter izdal šest odločb za iznos osebnih podatkov, od katerih je eno vlogo prejel leto prej. Medtem ko je leta 2010 prejel osem vlog za iznos osebnih podatkov ter izdal deset

[21] V 62. členu ZVOP-1 določa, »da kadar se posredujejo osebni podatki upravljavcu osebnih podatkov, pogodbenemu obdelovalcu ali uporabniku osebnih podatkov,ki je ustanovljen, ima sedež ali je registriran v državi članici Evropske unije ali Evropskega gospodarskega prostora ali zanj kako drugače velja njen pravni red, se ne uporabljajo določbe tega zakona o iznosu osebnih podatkov v tretje države« (62 .člen ZVOP-1).

[22] Medtem ko v celoti zagotavljata ustrezno raven varstva osebnih podatkov Švica in Republika Hrvaška, za ZDA to ne velja, saj ZDA zagotavljajo ustrezno raven varstva osebnih podatkov le v delu, ko gre za iznos osebnih podatkov organizacijam, ki delujejo po načelih varnega pristana, uveljavljenih v skladu z najpogosteje zastavljenimi vprašanji (FAQ), ki jih je 21. julija 2000 izdalo Ministrstvo za trgovino ZDA (Informacijski pooblaščenec).

odločb, od tega dve za vlogi prejeti leta 2009 (Pirc Musar 2011, 39). Prejete vloge od leta 2006 do leta 2010 prikazuje spodaj prikazan graf, graf 4.4. Iz njega torej lahko vidimo, da je število prejetih vlog v zadnjih letih naraslo ter se giblje od sedem do osem.

Graf 4.4: Število izdanih odločbza iznos osebnih podatkov med letom 2006 in 2010



Vir: Pirc Musar in drugi (2010, 41).

4.3.1 Primer za iznos podatkov v Republiko Hrvaško

Informacijski pooblaščenec je leta 2009 prejel predlog družbe za grafične in dokumentacijske storitve iz Slovenije, ki ima v lasti tudi družbo v Republiki Hrvaški, za prenos podatkov, saj je ta družba bila mnenja, da je neizogibno in da za svoje delovanje potrebuje prenos osebnih podatkov iz ene države v drugo državo. Informacijski pooblaščenec je po prejetju predloga uvedel postopek ugotavljanja ustreznosti pravnega varstva osebnih podatkov na Hrvaškem, ter ugotovil, da Republika Hrvaška ni na seznamu držav po členu 66. ZVOP-1, prav tako pa se ta ne nahaja na seznamu za katere je ustrezno raven varstva osebnih podatkov ugotavljala Komisija evropskih skupnosti.[23] Zato je moral informacijski pooblaščenec pregledati poročila o delu Agencije za varstvo osebnih podatkov Republike Hrvaške ter pregledal posredovane odločbe Agencije, saj se je s tem moral prepričati, da pravna ureditev v Republiki Hrvaški zajema vsa načela varstva osebnih podatkov v Sloveniji (Pirc Musar in drugi. 2010, 39).

[23] Republika Hrvaška je na podlagi tega primera z Odločba št. 0601-1/2009/8 dne 3.7.2009 prišla na seznam držav, ki izpolnjujejo varstvo osebnih podatkov.

4.3.2 Primer iznosa podatkov v ZDA

Družbi za proizvodnjo, razvoj in prodajo v Sloveniji je informacijski pooblaščenec dovolil, da po prejemu odločbe osebne podatke svojih zaposlenih, pogodbenih delavcev in študentov iznaša v ZDA, saj ZDA zagotavljajo ustrezno raven varstva osebnih podatkov, ko gre za iznos osebnih podatkov organizacijam. Tam, v ZDA, lahko podatke posreduje določenim poslovnim skupinam, pri čemer lahko izvoznik podatkov uvoznikom podatkov posreduje naslednje podatke; osebno ime, davčno številko, EMŠO, naslov, številko bančnega računa, podatke o plači in uspešnosti na delovnem mestu, delovno dobo, dopust, podatke o družinskih članih, vendar le-te če so ti vključeni v zdravstveno zavarovanje prek zaposlenega in če se v Sloveniji uveljavljajo kot davčna olajšava. Ti osebni podatki pa se iznašajo le zaradi kadrovskih namenov, učinkovitosti poslovanja in upoštevanja zakonskih zahtev (Pirc Musar in drugi 2010, 40).

4.4 PROBLEM INFORMACIJSKE ZASEBNOSTI NA INTERNETU

Vprašanje zasebnosti v današnji informacijski družbi predstavlja enega ključnih pravnih, sociooloških, filozofskih in etičnih vprašanj sodobne družbe. Ob vrsti pozitivnih vidikov, in do pred nekaj desetletij naslutenih možnosti, ki jih omogočata razvoj tehnologije v informacijski družbi in predvsem globalno računalniško omrežje, prinaša ta tehnološki razvoj veliko nevarnosti naši zasebnosti.

Znameniti, že zapisan stavek Louisa Brandeisa, se je torej rodil, rodil se je internet. »Internet je odprl javni sistem, ki deluje po tehnično znanih protokolih in katerega tehnična in programska konstrukcija sta primarno usmerjena na izmenjavo informacij in ne na zagotavljanje zaupnosti in tajnosti teh podatkov. To obenem omogoča vsakomur z minimalnim tehničnim znanjem, da najde in uporabi vrsto programskih orodij, namenjenih prestrezanju in razkrivanju podatkov, ki se pretakajo po internetu.« (Klemenčič 2003, 102). Zato res poglaviten razlog za ogrožanje zasebnosti na internetu predstavlja tehnologija, na kateri internet temelji.

Nezamerljivo je, če zapišem, da niso pomembni rezultati raziskav, ki kažejo, da so uporabniki interneta izrazito neosveščeni oziroma podcenjujejo tveganje, ki ga uporaba

interneta po mnenju Klmemnčiča (2003, 102) predstavlja s stališča varnosti osebnih podatkov in zasebnosti. Saj se ti internetne nevarnosti sploh ne zavedajo, ko objavljajo svoje osebne podatke, šele takrat ko njihov elektronski predal začnejo polniti reklamna sporočila oziroma 'junk mail' se ti zavedajo, da svoje podatke ni dobro objavljati na internetu, bodisi preko socialnih omrežij, bodisi preko različnih spletnih strani.

4.4.1 Tehnične možnosti varstva zasebnosti na internetu

Zaradi narave interneta, ki je zaenkrat še vedno v veliki meri pravno neurejen prostor, ki ne priznava državnih meja ter posledično predstavlja veliko oviro državnemu nadzoru, je za varovanje lastnih pravic najprej odgovoren uporabnik sam. Tako kot razvoj tehnologije vedno prinaša nova in učinkovitejša orodja, s katerimi se lahko posega v posameznikovo zasebnost, nova tehnologije ponuja tudi vrsto rešitev, ki služijo varovanju v poseg zasebnosti posameznika.

Uporabnikom interneta, so danes na voljo različne tehnološke rešitve varnosti, med katere spadajo požarne stene, anonimne pošiljatelje e-pošte, programska oprema za filtriranje e-pošte, programska oprema za anonimno deskanje po spletu, ubijalce piškotov, šifriranje elektronske pošte, posameznih datotek ali celotnega računalniškega diska, digitalni podpis ter digitalni certifikat (Makarovič in drugi 2001, 144–5).

5 ZAKLJUČEK

»Zasebnost je kot kladivo, lahko ga uporabiš,
da kaj popraviš, ali pa zato, da nekomu
povzročiš hud glavobol«. (Privacy Revolt)

Zasebnost se je pojavila sočasno z razvojem človeštva, saj je človek potrebo po zasebnosti začutil že v praskupnosti, vendar se je njena definicija razvila šele nekaj tisočletij kasneje, kot pravica do zasebnosti. Pravica do zasebnosti je danes temeljna človekova pravica, ki je v slovenskem pravnem redu urejena že z ustavo.

Sočasno s pojmom zasebnost pa se je pojavila varnost oziroma nevarnost, ki se je najprej razvila, zaradi nje pa je človek razvil občutek za varnost. Danes je varnost vgrajena v naš, biološki organizem, ki se prilagaja na ogrožajoče se vplive okolja tudi na ogrožanje naše zasebnosti.

Skupnost oziroma država v kateri ljudje živimo, se je vedno trudila zbirati osebne podatke o posameznikih, torej zasebne podatke. Vendar ta v preteklosti ni imela na voljo ustrezno tehnologijo za procesiranje, klasificiranje in za povezovanje podatkov, kot tudi ne za avtomatsko zbiranje podatkov kot jo ima danes. To moderno tehnologijo pa jo je omogočil razvoj informacijsko komunikacijske tehnologije, ki danes zaznamuje moderno družbo. Vendar to ne pomeni, da je zasebnost postala ogrožena šele s pojavom nove informacijsko komunikacijske tehnologije in računalniških zbirk podatkov, pač pa je ta dala misliti oziroma je vzpodbudila zavednost, da nova tehnologija omogoča hitrejši vdor v posameznikovo zasebnost.

Vendar, da do vdorov v posameznikovo zasebnost ne bi prišlo, država in Skupnost s pravno podlago urejata področje varnosti informacijske zasebnosti, vendar kljub temu se najde posameznik, ki brska in brska po sodobni tehnologiji s pomočjo katere poišče zasebne podatke posameznika.

V uvodnem delu sem si zastavil pet hipotez, katere sem potrdil ali zavrnil s pomočjo teorije in pravne prakse.

Potrjene hipoteze so naslednje:

- Hipoteza 1: *Evropska unij, kot tudi Slovenija imata dobro pravno podlago na področju varnosti informacijske zasebnosti*.
- Hipoteza *3: Največ vdorov v posameznikovo zasebnost prihaja v zasebnem sektorju*.
- Hipoteza 5: *Ljudje se ne zavedamo, da internet je le eno od orodij s katerimi lahko ljudje posežejo v našo zasebnost*.

Zavrnjeni hipotezi sta naslednji:

- Hipoteza 2: *Informacijski pooblaščenec je v letu 2010 in 2009 vodil 200 zadev, zaradi suma kršitev določil ZVOP-1*. Ta hipoteza ne drži, saj je informacijski pooblaščenec leta 2010 zaradi suma kršitev določb ZVOP-1 vodil kar 599 zadev, od tega kar 202 v javnem sektorju in 397 v zasebnem sektorju. Leto prej, 2009, pa je informacijski pooblaščenec vodil zaradi suma kršitev določb ZVOP-1 624 zadev, od tega 219 v javnem sektorju in 405 v zasebnem sektorju.
- Hipoteza 4:*V Sloveniji je v zadnjih letih prišlo do 50 vdorov v posameznikovo informacijsko zasebnost*.Ta hipoteza ne drži, saj je leta 2010 bilo uvedenih 179 postopkov o prekršku, 45 postopkov zoper pravnih oseb javnega sektorja, 82 postopkov zoper pravnih oseb zasebnega sektorja ter 52 postopkov zoper posameznike. Leta 2009 pa je bilo uvedenih 163 postopkov o prekršku, 41 postopkov zoper pravnih oseb javnega sektorja, 70 postopkov zoper pravnih oseb zasebnega sektorja in 52 postopkov zoper posameznika.

6 LITERATURA IN VIRI

1. Accetto, Matej. 2006. *Izgradnja Evrope: od razvoja ideje Evrope do njene ustavne prihodnosti.* Ljubljana: Uradni list Republike Slovenije.

2. Anžič, Andrej. 1997. *Varnostni sistem Republike Slovenije.* Ljubljana: Uradni list Republike Slovenije.

3. Bernik, Igor in Kaja Prislan. *Proces upravljanja s tveganji v informacijski varnosti.* Univerza v Mariboru. Fakulteta za varnostne vede. Dostopno prek: http://www.fvv.uni-mb.si/DV2010/zbornik/informacijska_varnost/Bernik_Prislan%20proces%20upravljanja.pdf (10. avgust 2011).

4. Black, Edwin. 2002. *IBM and the Holocaust*. London: Time Warner.

5. Bohinc, Marija in Miro Gradišar. 1999. Informacijska zasebnost pacientov v zdravstvu. *Obzornik zdravstvene nege* 33 (5–6): 239–42.

6. Buzan, Barry. 1983. *People, States, and Fear: The National Security Problem in International Relations.* Brighton, Sussex: Wheatsheaf Books.

7. Consumer Federation of California Education Foundation. 2007. *Privacy revolt*. Dostopno prek: http://consumercal.blogspot.com/2007/08/privacy-is-like-hammer-you-can-use-it.html (7. september 2011).

8. Čebulj, Jenez. 2002. 38. člen (varstvo osebnih podatkov). V *Komentar Ustave Republike Slovenije*, ur. Lovro Šturm, 408–16. Ljubljana: Fakulteta za podiplomske državne in evropske študije.

9. *Direktiva Evropskega parlamenta in sveta 2006/24/ES*. Ur. l. EU 24/2006 Dostopno prek: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:SL:PDF (20. avgust 2011).

10. *Direktiva Evropskega parlamenta in sveta 95/46/ES*. Ur. l. EU 281/1995 Dostopno prek: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:SL:HTML (25. avgust 2011).

11. Gaberšček, Samo. 2007. *Ekonomika naložb v informacijsko varnost*. Ljubljana: Ekonomska fakulteta. Dostopno prek: http://www.cek.ef.uni-lj.si/magister/gaberscek3253.pdf (10. avgust 2011).

12. Grizold, Anton. 1992. Oblikovanje slovenske nacionalne varnosti. V *Razpotja nacionalne varnosti: obramboslovne raziskave v Sloveniji*, ur. Anton Grizold , 59–93. Ljubljana: Fakulteta za družbene vede.

13. Informacijski pooblaščenec. 2011. *Varstvo osebnih podatkov*. Dostopno prek: https://www.ip-rs.si/varstvo-osebnih-podatkov/obveznosti-upravljavcev/iznos-osebnih-podatkov-v-tretje-drzave/seznam-tretjih-drzav-66-clen-zvop-1/ (6. september 2011).

14. *Kazenski zakonik Republike Slovenije* (KZ-1-UPB-1). Ur. l. RS 63/1994. Dostopno prek: http://zakonodaja.gov.si/rpsi/r05/predpis_ZAKO905.html (4. september 2011).

15. Klemenčič, Goran. 2003. Internet in pravica do zasebnosti. V *Internet in pravo*, ur. Boštjan Makarovič, Damjan Možina, Špela Mežnar, Domen Bizjak, Maja Bogataj in Goran Klemenčič, 101–41. Ljubljana: Pravna fakulteta univerze v Ljubljani.

16. Kmetec, Tomaž. 2010. *Varstvo osebnih podatkov pri uporabi sodobne informacijske tehnologije.* Ljubljana: Pravna fakulteta.

17. Kojc, Marko. 2010. *Informacisjka varnost v Republiki Sloveniji*. Ljubljana: Fakulteta za družbene vede.

18. Kovačič, Matej. 2006. *Nadzor in zasebnost v informacijski družbi: filozofski, sociološki, pravni in tehnični vidiki nadzora in zasebnosti na internetu*. Ljubljana: Fakulteta za družbene vede.

19. Lampe, Rok. 2003. Pravni in drugi izzivi informacijske družbe. V *Pravna informatika: zapiski predavanj* ur. Dušan Lesjak, Tomaž Klojčnik, Benjamin Lesjak, Rok Lampe in Viktorija Sulčič, 120–73. Maribor: Pravna fakulteta

20. Makarovič, Boštjan, Goran Klememnčič, Tomaž Klobučar, Maja Bogataj in David Pahor. 2001. *Internet in pravo: Izbrane teme s komentarjem Zakona o elektronskem poslovanju in elektronskem podpisu*. Ljubljana: Pasadena.

21. Mihelič, Anže. 2009. *Zagotavljanje pravice do zasebnosti skozi slovensko zakonodajo v primerjavi z domačo in tujo sodno prakso.* Maribor: Fakulteta za varnostne vede. Dostopno prek: http://dkum.uni-mb.si/Dokument.php?id=12211 (2. september 2011).

22. Moussis, Nicolas. 1999. *Evropska unija: pravo, ekonomija, politika.* Ljubljana: Littera pieta.

23. Pavčnik, Marijan. 1997. *Teorija prava: prispevek k razumevanju prava*. Ljubljana: Cankarjeva založba.

24. Pestotnik, Andreja. 2007. *Zasebnost in mobilna telefonija*. Ljubljana: Fakulteta za družbene vede.

25. Pirc Musar, Nataša, Mojca Prelesnik in Sonja Bienet. 2006. *Varstvo osebnih podatkov:vstop v zasebnost prepovedan!* Ljubljana: Informacijski pooblaščenec. Dostopno prek: https://www.ip-rs.si/fileadmin/user_upload/Pdf/brosure/zasebnoNIjavno_slo.pdf (8. september 2011).

26. Pirc Musar, Nataša, Monika Benkovič Krašovec, Jože Bogataj, Alenka Jerše, Kristina Kotnik Šumah, Jasna Rupnik, Andrej Tomšič in Sandra Vesel. 2010. *Letno poročilo Informacijskega pooblaščenca 2009*. Ljubljana: Informacijski pooblaščenec. Dostopno prek: https://www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/Letno_porocilo_2009-net.pdf (7. avgust 2011).

27. Pirc Musar, Nataša, Monika Benkovič Krašovec, Jože Bogataj, Eva Kalan, Nina Komočar, Tina Kraigher, Kristina Kotnik Šumah, Rosana Lemut-Strle in Andrej Tomšič. 2011. *Letno poročilo Informacijskega pooblaščenca 2010*. Ljubljana: Informacijski pooblaščenec. Dostopno prek: https://www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/Letno_porocilo_2010_net.pdf (8. september 2011).

28. Schneier, Bruce. 2000. *Secrets and Lies: digital security in a networked world*. New York: John Wiley and Sons.

29. Simčič, Simon. 2007. *Ogrožanje kritične informacijske infrastrukture v Republiki Sloveniji.* Ljubljana: Fakulteta za družbene vede. Dostopno prek: http://dk.fdv.uni-lj.si/diplomska/pdfs/Simcic-Simon.PDF (10.8.2011).

30. *Ustava Republike Slovenije* (URS). Ur. l. RS 33/1991. Dostopno prek: http://zakonodaja.gov.si/rpsi/r01/predpis_USTA1.html (3. september 2011).

31. Vintar, Mirko. 2006. *Informatika*. Ljubljana: Fakulteta za upravo.

32. Wagner DeCew, Judith. 1997. *In Pursuit of Privacy: law, ethics, and the rice of technology*. Ithaca, London: Cornel university press.

33. *Zakon o informacijskem pooblaščencu* (ZInfP). Ur. l. RS 113/2005. Dostopno prek: http://zakonodaja.gov.si/rpsi/r08/predpis_ZAKO4498.html (3. september 2011).

34. *Zakon o varstvu osebnih podatkov* (ZVOP-1-UPB-1). Ur. l. RS 86/2004. Dostopno prek: http://zakonodaja.gov.si/rpsi/r06/predpis_ZAKO3906.htm l (3. september 2011).