

**UNIVERZA V LJUBLJANI
FAKULTETA ZA UPRAVO**

Diplomsko delo

**EVROPSKI IN AMERIŠKI KONCEPT
ZASEBNOSTI**

Marijana Markovc

Ljubljana, februar 2012

**UNIVERZA V LJUBLJANI
FAKULTETA ZA UPRAVO**

DIPLOMSKO DELO

EVROPSKI IN AMERIŠKI KONCEPT ZASEBNOSTI

Kandidat/ka: Marijana Markovc
Vpisna številka: 04038258
Študijski program: visokošolski študijski program uprava prva stopnja

Mentor: doc. dr. Alenka Kuhelj

Ljubljana, februar 2012

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Podpisana Marijana Markovc, študentka visokošolskega študijskega programa uprava prva stopnja, z vpisno številko 04038258, sem avtorica diplomskega dela z naslovom: **Evropski in ameriški koncept zasebnosti**.

S svojim podpisom zagotavljam, da:

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

Diplomsko delo je lektoriral: Primož Markovc.

Ljubljana, 06.02.2012

Podpis avtorice: _____

POVZETEK

Različna razumevanja pojma zasebnosti v ZDA in EU je mogoče razumeti kot posledico temeljnih razlik pojmovanja vloge države in gospodarstva. Na splošno evropski pristop h korporativnemu upravljanju zahteva tesno sodelovanje med gospodarstvom in državo. Država je aktivni partner pri razvoju gospodarstva, poleg tega pa ima širšo vlogo pri reševanju socialnih problemov. V nasprotju z Evropo v ZDA dajejo nosilci odločanja prednost tržnemu gospodarstvu, poudarjajo vlogo zasebne in tržne svobode.

V Evropi je pravica do zasebnosti temeljna človekova pravica, ki jo je država preko svojih vzvodov dolžna zagotavljati. Prav tako je pravica do zasebnosti navedena v številnih ustavah evropskih držav in zapisana v Evropski konvenciji o varstvu človekovih pravic in temeljnih svoboščin.

V nasprotju z Evropo, kjer je pravica do zasebnosti zakonsko urejena, pa je zasebnost v ZDA podvržena pritiskom prostega trga. Zasebnost je v ZDA močno iskano tržno blago. Država ne posega in ne regulira področja razen ko problematike ni mogoče rešiti v okviru zasebnega sektorja. Praktično je vloga države pri reševanju problematike zasebnosti in vdora vanjo bolj izjema kot pravilo oziroma je v primeru neuspešnega reševanja sporov država zadnji razsodnik.

KLJUČNE BESEDE

- človekove pravice
- zasebnost
- pravica do zasebnosti
- osebni podatki
- varstvo osebnih podatkov

SUMMARY

EUROPEAN AND AMERICAN CONCEPT OF PRIVACY

Different understandings of the concept of privacy in the USA and EU are to be understood as a result of basic differences in considering the role of the state and economy. In general the European approach towards corporate governance requires close cooperation between the two. The state is an active partner in economy development, and in addition to it, it has a larger role in solving social problems. Unlike in Europe, in the USA the decision-makers give preference to the market economy, and they emphasize the role of private and market freedom.

In Europe the right to privacy is a basic human right, which the state is obliged to ensure through its levers. The right to privacy is set out in numerous constitutions of European countries and written in the European Convention for the Protection of Human Rights and Fundamental Freedoms.

KEYWORDS

- human rights
- privacy
- right to privacy
- personal data
- personal data protection

KAZALO

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA.....	iii
POVZETEK.....	v
SUMMARY.....	vi
KAZALO.....	vii
KAZALO PONAŽORITEV	ix
1 UVOD.....	1
2 OPREDELITEV TEMELJNIH POJMOV	8
2.1 Pravo človekovih pravic.....	8
2.2 Razvoj ustavnega sodstva ter ustavno sodna presoja.....	10
2.3 Razvoj ustavnega sodstva v Sloveniji.....	12
2.4 Veljavna ureditev ustavnega sodstva v Sloveniji	12
3 ZASEBNOST	14
3.1 Zgodovinski razvoj sodobne zasebnosti	15
3.2 Zasebnost v množični družbi.....	17
3.3 Omejevanje zasebne sfere	20
3.4 Pomen zasebne sfere.....	21
4 PRAVICA DO ZASEBNOSTI	23
4.1 Splošni pogledi na pravico do zasebnosti	23
4.2 Klasifikacija pravice do zasebnosti.....	24
4.3 Razvojni temelji pravice do zasebnosti.....	24
5 PRAVICA DO ZASEBNOSTI V ZDA.....	27
5.1 Ustavni temelji pravice do zasebnosti v ZDA	27
5.2 Pravica do zasebnosti v ZDA na delovnem mestu	29
5.3 Varstvo informacijske zasebnosti v ZDA v zasebnem sektorju	31
5.4 Obdelava in izmenjava osebnih podatkov v ZDA – grožnje zasebnosti	32
6 PRAVICA DO ZASEBNOSTI V EVROPI	35
6.1 Varstvo informacijske zasebnosti v Evropi	36
6.2 Vpliv direktiv EU na varstvo informacijske zasebnosti v Evropi	38
6.3 Pretok osebnih podatkov iz Evropske unije v ZDA.....	39

6.4 Pravica do zasebnosti v EU na delovnem mestu	40
6.5 Komunikacijska zasebnost v Evropi	42
6.6 Boj za pravico do zasebnosti	44
7 ZASEBNOST OSEBNIH PODATKOV	46
7.1 Mednarodnopravni vidiki	46
7.2 Ameriško pravo	48
7.3 Evropsko pravo	49
7.4 Slovenska ureditev	52
7.5 Zdravstveni podatki	57
7.5.1 Pravne osnove za obdelavo pacientovih podatkov v Republiki Sloveniji	58
7.5.2 Upravljalci osebnih podatkov pacientov	58
8 ZAKLJUČEK.....	62
8.1 Anketa in analiza ankete	62
8.2 Sklepna misel.....	72
LITERATURA IN VIRI.....	76
PRILOGA	82
PRILOGA 1: Anketa	82

KAZALO PONAŽORITEV

KAZALO GRAFOV

Graf 1: Pregled anketirancev po spolu	62
Graf 2: Pregled po starostnem obdobju	63
Graf 3: Pregled delovne dobe	63
Graf 4: Pregled anketirancev glede na sektor zaposlitve	64
Graf 5: Kako pomembna se vam zdi pravica do zasebnosti posameznika?	64
Graf 6: Katera pravica se vam zdi pomembnejša?	65
Graf 7: Ali na delovnem mestu uporabljate službeni računalnik za brskanje po internetu? ...	65
Graf 8: Vsebina uporabe interneta med delovnim časom	66
Graf 9: Ali ste pri zasedbi delovnega mesta podpisali dogovor o omejitvi vaše zasebnosti med službenim časom?	66
Graf 10: Ali menite, da vam delodajalec nadzoruje vaše aktivnosti ne vašem računalniku? ..	67
Graf 11: Ali ste kdaj pri uporabi službenega računalnika opazili nepričakovano in nerazumljivo upočasnjeno delovanje le tega?	68
Graf 12: Ali menite, da vam lahko delodajalec pregleduje vsebino službene elektronske pošte?	68
Graf 13: Ali ste pri pogovoru z nadrejenimi mogoče opazili, da oni kakorkoli poznajo vsebino vaših elektronskih sporočil?	69
Graf 14: Ali ste bili kdaj opozorjeni na prekomerno brskanje po internetu?	69
Graf 15: Kdo je po vašem mnenju najbolj odgovoren za varovanje vaše zasebnosti na delovnem mestu?	70
Graf 16: Nadzor delodajalca nad aktivnostmi zaposlenega med delovnim časom od elektronske pošte, brskanja po internetu, telefona, gibanja.. se mi zdi nedopusten.	71
Graf 17: Moja zasebnost na delovnem mestu je s strani delodajalca vedno bolj ogrožena. ..	71

KAZALO SLIK

Slika 1: Javna in zasebna sfera skozi čas	17
Slika 2: Razlike med javnim in zasebnim delovanjem / interesom	19

1 UVOD

Imam pravico do zasebnosti?? Kje je meja moje zasebnosti in do kam lahko posežeta država in družba?

Pravica do zasebnosti (*»Right to privacy«*, »pravica do spoštovanja zasebnega življenja« - *»droit au respect de la vie privée«* ali *»Recht auf Privatheit«*) je osnovna človekova pravica. Zasebnost je z ustavo in mednarodnimi pogodbami osebnostna pravica civilnopravnega značaja, kot eden izmed nepogrešljivih elementov človekovega obstoja, ki varuje človeka pred prekomernimi posegi državne oblasti, javnosti in drugih posameznikov v posameznikovo zasebnost. Pojmovanje zasebnosti, toleranca in družbena upravičenost posegov v zasebnost posameznika je pogojena z družbenim razvojem. Že pred¹ in po drugi svetovni vojni je pomen varovanja zasebnosti spoznalo in priznalo tudi pravo, ki je pravico do zasebnosti kodificiralo v mednarodnih pravnih dokumentih, kasneje pa zaradi grožnje tehnologije še v posameznih nacionalnih zakonodajah. Vendar pogoste spremembe zakonodaje s področja zasebnosti kažejo, da razmerje med posegom v zasebnost in zasebnostjo še zdaleč ni statično oziroma dokončno urejeno, ampak se spreminja. Kljub čedalje večji pravni regulaciji zasebnosti kritiki opozarjajo, da se zasebna sfera dejansko krči. Težko je sicer ugibati kam lahko takšno krčenje zasebnosti privede, toda zgodovinsko dejstvo je, da je bila zasebnost kot vrednota postranskega pomena predvsem v vojnah, v izrednih stanjih in v totalitarnih režimih.

Posegi državne oblasti v zasebnost posameznika niso edini. Obstajajo še posegi v zasebnost posameznika s strani drugega posameznika, ki so postali že prava industrija² in so zelo dobičkonosni.

Prag družbene upravičenosti vdora v posameznikovo zasebnost je odvisen glede na konkretne družbene dogodke in na razpoloženje v družbi³. Poglavitna lastnost posameznikove pravice do zasebnosti je tako njena omejenost. Moderni družbeni tokovi porajajo pojav »deprivatizacije« človekovega življenja. Tukaj gre za družbeni pojav, ki se pojavlja predvsem z moderno tehnologijo in ki ustvarja »*big brother*« efekt nad posamezniki in skupinami družbe. Po drugi strani pa »komercializacija in globalizacija« družbe

¹ Sodnik ameriškega Vrhovnega sodišča Louis Brandeis je leta 1928 v odločbi primera »*Olmstead v. U.S.*« zapisal, da napredek znanosti omogoča državi oblasti nove možnosti nadzora in da se le-ta ne bo ustavil s prisluškovanjem telefona. Predvidel je, »da bo država nekega dne sodišču lahko predložila reproducirane papirje, ne da bi jih vzela iz obtoženčevega predala in poroti razkrivala njegove najbolj intimne podatke«.

² Nepogrešljivi »*reality shows*« tipa »*Big Brother*«.

³ Globalno gledano se je v ZDA po 11. 9. v tipičnem primeru družbene dinamike - prag upravičenosti vdora v posameznikovo zasebnost - jeziček na tehtnici tehtanja interesov radikalno prevesil na stran nasprotujočih si interesov družbe po ohranitvi nedotakljivosti posameznikove zasebnosti zaradi družbenega interesa po državni varnosti.

predstavljata veliko nevarnost moderne družbe nad varnostjo posameznikove osebnosti nasploh. Pri tem gre za zmanjšano spoštovanje zasebnosti v zameno za denar.

Pravica do zasebnosti kot človekova pravica mednarodnopravne narave, kot ustavna pravica ter kot osebnostna pravica, varovana z instrumenti civilnega prava, ima absolutni značaj, kar pomeni, da deluje proti vsem - *erga omnes*, tako proti državnim organom kot tudi nasproti tretjim osebam. Vendar njen absolutni značaj pomeni le, da deluje zoper vsakogar, a ne brez omejitev. Potrebno je vedeti, da mora vsak posameznik za svojo varnost odstopiti del svoje svobode in »suverenosti«. Tukaj pa je tista tanka meja, ko govorimo o omejenosti zasebnosti posameznika. Po drugi strani pa pri pretiranem poseganju lahko kaj hitro pridemo v situacijo, ki se ponavlja skozi celo zgodovino človeške družbe, kolikokrat in na kakšne nečloveške načine lahko pride do kršitev in vdorov v človekove pravice, skratka tudi v pravico do zasebnosti.

Pri vprašanju meje dovoljenega je treba posvetiti pozornost analizi razmerja med nadzorom in zasebnostjo. Takšno razmerje naj bi izražala pravna ureditev zasebnosti, ki je v evropskem (kontinentalnem) in ameriškem (anglosaksonskem) pravnem sistemu različno varovana. Ob primerjavi obeh pravnih sistemov je opazna razlika, da je v ZDA zasebnost varovana predvsem v razmerju do države oziroma javnega sektorja, mnogo manj pa v razmerju do privatnega sektorja. V Evropi je zakonodaja s področja zasebnosti strožja tudi v privatnem sektorju, kar po eni strani izraža drugačno pravno tradicijo, po drugi strani pa še zmeraj prisoten strah, kateri je posledica obdobja od 1933 do 1945⁴. S tem se nemudoma pojavljajo vprašanja kot so: »Kje postaviti mejo, da bosta varovana posameznikov interes in njegova pravica ter na drugi strani interes družbe? Kako regulirati pogoje vdora državnega organa ali tretje osebe v pravico do zasebnosti posameznika?«

Slovenija je del Evropskega pravnega reda in vsa njena zakonodaja je v skladu z Evropskim pravnim redom. V Ustavi je v 3. odst. 15. člena opredeljena pravica do zasebnosti⁵, vendar je to načelo presplošno. Ustavno sodišče je v svojih odločbah dalo smernice za razumevanje omenjenega člena⁶. Potrebno je tudi poudariti, da je se vsaka država s podpisom EKČP odpovedala določeni stopnji svoje suverenosti. Omejitve, ki jih nalaga 2.odst. 8. člena EKČP, so tako nad njeno nacionalno zakonodajo. Celoten člen varuje posameznika, čeprav se zdi, da 2. odst. močno omejuje pravico do zasebnosti. Država je še vedno suverena in lahko s

⁴ Robert Butler; Ilustrirana zgodovina gestapa; Murska Sobota 1998

⁵ Človekove pravice in temeljne svoboščine so omejene samo s pravicami drugih in v primerih, ki jih določa ta ustava.

⁶ V odločbi *OdIUS VI, 58*, s katero je z odložnim rokom razveljavilo 150. do 156. člen ZKP, je US izreklo, daje Ustava z določbo 3. odst. 15. člena postavila mejo temeljnim ustavnim pravicam glede na pravice drugih in zaradi varstva prednostnih pravnih dobrin ter se opredelila zoper morebitne zlorabe temeljnih pravic, s katerimi bi bile lahko ogrožene tako pravice posameznika kot varstvo družbe kot celote. To po stališču US v navedeni odločbi pomeni, da se mora posameznik vendarle podrediti tistim omejitvam svoje svobode ravnanja, ki jih določi [...] zakonodajalec zaradi varstva in razvoja sožitja v družbi [...] ob predpostavki, da ostane zagotovljena samostojnost človeka kot posameznika.

svojimi organi dokaj nenadzirano posega v zasebnost posameznikov. 2. odst. 8. člena⁷ omogoča, da se posameznik sklicuje na vsako besedo dikcije zakona. V nasprotnem primeru, če državna oblast ne bo delovala v skladu s postavljenimi pravili iz 2. odst. 8. člena EKČP, bo neupravičeno kršila posameznikove pravice do zasebnosti. Ob izčrpanju vseh pravnih poti pa se lahko posameznik pritoži oziroma toži državo na Sodišču za človekove pravice.

Zavedati se je potrebno, da je *de iure* EKČP najvišja sodna instances varstva posameznikove pravice do zasebnosti. Pravna praksa tega telesa pa je po logiki »*stare decisis*« precedenčni pravni vir, ki ga posamezna država mora z ustreznimi pravnimi instrumenti implementirati v nacionalno pravo kot t.i. minimalni standard človekovih pravic. Državna oblast je vezana s strasburško sodno prakso, ki ji mora podrediti zakonodajo, če njena dotedanja praksa ne ustreza ustvarjenemu (minimalnemu) standardu zagotovitve človekovih pravic. Zagotavljanje minimuma standardov človekovih pravic je primarna funkcija pravne prakse ESČP, ki mora biti ažuriran v nacionalnem pravu.

Anglosaški sistem pojmovanja zasebnosti je razvil t.i. »Koncept razumnega pričakovanja zasebnosti«, utemeljenega v ustavnopravni praksi Vrhovnega sodišča ZDA. Sam koncept posameznikove pravice do zasebnosti v sferi, kjer lahko »upravičeno in razumno pričakuje« uživanje svoje zasebnosti brez vmešavanja državne oblasti. Koncept razumnega pričakovanja zasebnosti je tesno povezan tako prostorsko kot informacijsko. 4. amandma ameriške ustave zagotavlja človeku pravico biti varen tako glede svoje osebe, hiše, papirjev in dokumentov ter pred nerazumnimi preiskavami (*unreasonable searches and seizures*). Ameriška sodna praksa poudarja pojmovanje, da tekst 4. amandmaja predvsem varuje človeka pred »nezakonitimi kršitvami svetosti doma⁸« (*unlawful invasion of the sanctity of the home*). Bistvo, da je človekov dom človekov grad (*A man's home is a man's castle*), je Vrhovno sodišče ZDA tudi razširilo na »pravico posameznika umakniti se v svoj dom in biti tam prost pred nerazumnim vdorom državnih organov« v primeru *Silverman v. U.S.*⁹ iz leta 1961. *Silverman* je izoblikoval t.i. »ustavno zaščiteno področje« človekovega doma v primerih preiskave kaznivih dejanj, (Lampe, 2003, str. 118 - 132).

Za Ameriško sodno prakso v zvezi z varovanjem zasebnosti in posegov državnih organov je primer *Katz v. U.S.*¹⁰ iz leta 1967 eden izmed najpomembnejših presedanov ameriškega Vrhovnega sodišča glede pravice do zasebnosti. V tem primeru je sodišče izoblikovalo pojmovanje »pričakovane zasebnosti« – »*expectation of privacy*«, kar je spremenilo varstvo zasebnosti doma, pojmovane »kot ustavno zaščiteno področje«. »Četrty amandma varuje

⁷ Evropska konvencija o človekovih pravicah in temeljnih svoboščinah je pri normiranju omejitve pravice do zasebnosti preciznejša. 2. odst. 8. člena namreč določa, »Javna oblast se ne sme vmešavati v izvrševanje te pravice, (I.) - razen če je to določeno z zakonom in (II.) - nujno v demokratični družbi zaradi : (a) državne varnosti, (b) javne varnosti ali (c) ekonomske blaginje države, zato (1.) da se prepreči nered ali zločin, (2.) da se zavaruje zdravje ali morala, ali (3.) da se zavarujejo pravice in svoboščine drugih ljudi«.

⁸ Tako je Vrhovno sodišče zapisalo v primeru *Adams v. New York*, 192 U.S. 585, leta 1904.

⁹ 365 U.S. 505

¹⁰ 389 U.S. 347

ljudi in ne prostorov«, je zapisalo Vrhovno sodišče ter razveljavilo sodbo pritožbenega sodišča, ki je sodbo prvostopenjskega potrdilo. Obtoženi se je v tem primeru namreč pritožil zaradi obsodbe, ki je temeljila na dokaznem materialu, ki ga je policija dobila brez predhodnega sodnega naloga s prisluškovanjem obtoženčeve komunikacije v javni telefonski govorilnici. »Kar oseba zavestno izpostavi javnosti, tudi v svojem domu ali pisarni, ni zavarovano s 4. amandmajem. Vendar, kar hoče oseba ohraniti zasebno, tudi v prostoru, ki je dostopen javnosti, je ustavnopravno zaščiten. Kar je obtoženi želel izključiti ob vstopu v telefonsko govorilnico, ni bilo »moteče« oko – bilo je »nepovabljeno« uho. Kdor uporablja telefonsko govorilnico, zapre vrata za seboj in plača telefonski pogovor, nedvomno upravičeno pričakuje, da njegove besede ne bodo predvajane »svetu«. Preozko branje Ustave pomeni ignorirati življenjsko situacijo, da je javni telefon namenjen »zasebni komunikaciji«, je sodišče obrazložilo svojo odločitev¹¹ (Lampe, 2003, str. 118 - 133).

Bistvo primera Katz pa je bila sprememba pojmovanja nerazumne in neupravičene preiskave in zasegov. Hkrati je pomenila ne samo presedan v Ameriški sodni praksi ampak je tudi vplivala na odločitve EKČP leta 1997 v odločbi primera *Halford v. UK*, kjer je pritožnica zatrjevala, da je bila kršena njena pravica do zasebnosti iz 8. člena EKČP s tem, da je delodajalec prisluškoval (*interception*) njenim privatnim telefonskim pogovorom, saj bi naj bili njeni telefonski privatni pogovori zaščiteni (*to fall within*) področje zasebnega življenja in dopisovanja iz 1. odst. 8. člena EKČP.

Prav ta odločba ESČP je pokazala na nevarne posege nedržavne sfere v posameznikovo zasebnost izražene skozi moč in ukrepe delodajalca pri nadzoru delojemalcev.

Problem in predmet proučevanja v diplomski nalogi sta v nekaterih delih povsem nasprotujoča koncepta dojemanja in urejevanja področja zasebnosti (anglosaški in kontinentalni).

¹¹ S tem je Vrhovno sodišče premaknilo objekt varstva (tudi zasebnosti) z lastninsko pravnega pojmovanja varstva k osebnostno pravnemu pojmovanju. Cilj varstva ni več samo človekova lastnina, temveč njegova oseba. Pojmovanje, da je pred nerazumnimi preiskavami in zasegi (*unreasonable searches and seizures*) varovana »le« človekova lastnina je izhajalo iz dotedanje sodne prakse Vrhovnega sodišča. Le-to je leta 1928 v primeru *Olmstead v. U.S.* 277 U.S. 438 dosodilo, da prisluškovanje telefonskim pogovorom (*wiretaping*) načeloma ne predstavlja kršitev 4. amandmaja Ustave ZDA. Pojem zasega (*seizure*) 4. amandmaja se nanaša le na materialne stvari (osebe, hiše, papirje ali predmete) v kar ni vključen telefonski pogovor. Takratni predsednik Vrhovnega sodišča Taft je v mnenju večine citiral besede Vrhovnega sodnika Fielda v primeru *Jackson* (96 U.S. 727), da 4. amandma varuje zapečateni pisma in poštni pakete in da se tak predmet lahko odpre samo na podlagi sodne odločbe (odredbe), ki ga sodišče izda po zaprisegi in v kateri podrobno opiše stvari, ki naj se zasežejo.

Namen v nadaljevanju predstavljenih tez je teoretične predpostavke eksplicitno in empirično preveriti. Teze so oblikovane na podlagi induktivnega in deduktivnega pristopa. V diplomski nalogi bom preverila tri temeljne teze:

Teza 1: *Pojma zasebnost in pravica do zasebnosti kljub obširnim znanstvenim delom še vedno nista enoznačno predstavljena ampak njuna različna razlaga izhaja iz naslova geografskega in družbenega sveta.*

Teza 2: *V EKČP in Lizbonski pogodbi so zaradi zgodovinskega razvoja človekove pravice zapisane kot pravice, vendar so kljub temu Evropska ustavna sodišča vključno z ESČP polno zaposlena z reševanjem pritožb kršenja pravic, medtem ko se v ZDA to rešuje skozi sodno prakso na vseh nivojih sodišč.*

Teza 3: *Razvoj zasebnosti na področju odnosa delodajalec – delojemalec v ZDA, gre v smeri zaostrovanja in omejevanja ter zmanjševanja pravic delojemalcev, medtem ko se v Evropi nadaljuje trend povečevanja obsega pravic.*

V procesu verifikacije zastavljenih tez in doseganja zastavljenih ciljev naloge sem se oprla na teoretične kot tudi praktične raziskovalne metode.

Namen in cilj raziskovanja je poglobljeno in popolnejše poznavanje vprašanja zasebnosti posameznika v odnosu do družbe. V diplomski nalogi sem si zastavila naslednje cilje:

1. Razložiti temeljni pojem »pravica do zasebnosti«,
2. Opisati razumevanje »pravice do zasebnosti« v anglosaškem in kontinentalnem svetu,
3. Izvesti primerjavo različnih konceptov zasebnosti (anglosaškega in kontinentalnega),
4. Razložiti temeljne značilnosti posameznega koncepta obravnavanja zasebnosti,
5. Zgodovinsko opisati razvoj področja tudi skozi sodno prakso Vrhovnega sodišča in EKČP ter nacionalnih ustavnih sodišč,
6. Opisati novejša trenda razvoja razumevanja »pravice do zasebnosti« in sodne prakse po začetku 21. stoletja.

Če pogledamo **dosedanja raziskovanja** o vprašanju o zasebnosti, o nadzoru, posegih države in družbe, lahko ugotovimo, da omenjeno področje raziskujejo številni raziskovalci in strokovnjaki. S tem problemom se ukvarjajo tudi številni aktivisti za varstvo človekovih pravic. Zaradi soodvisnosti je nujna hkratna obravnava vseh vprašanj, kajti gre za problematiko, ki ima družboslovne, pravne, tehnološke in filozofske razsežnosti in se dotika pravic posameznikov. Zadnja raziskovanja področja zasebnosti gredo v smeri uporabe najnovejših tehnologij (mobilna telefonija in internet) in na področje delovno pravnih odnosov – odnosa delodajalec in delavec ter nadzora nad njim.

Problem s katerim se vsi raziskovalci in aktivisti srečujejo je odsotnost nedvoumne in jasne definicije, kaj sploh je zasebnost. Delno se vzrok najde v nedorečenosti pojma, delno pa v stalnem tehnološkem in družbenem razvoju. Poleg tega je pri prebiranju strokovne literature

in raziskovanju sodne prakse opaziti različne pristope do pojma zasebnost in različno sodno prakso glede na dejstvo ali gre za anglosaški ali gre za kontinentalni svet. V anglosaškem svetu raziskovalci predvsem vidijo državo kot glavno grožnjo, medtem ko se vpliv družbe zanemarja.

Izdelava diplomske naloge temelji na **metodah znanstvenega raziskovanja**. V procesu verifikacije hipotez in doseganja zastavljenih ciljev proučevanja, sem uporabila tako teoretične kot tudi empirične raziskovalne metode.

Med teoretičnimi raziskovalnimi metodami sem uporabila:

- z analizo vsebine pisnih virov sem proučila vsebino, tako primarnih, kot tudi sekundarnih virov. Iz teh bom pridobila informacije, ki jih bom potrebovala za predstavitev in primerjavo koncepta zasebnosti med anglosaškim in kontinentalnim svetom;
 - primarni viri so bili predvsem internet, strokovne publikacije in lastno gradivo;
 - sekundarni viri pa v obliki člankov in drugih publikacij s področja varovanja zasebnosti, zakonodaje in internet;
- metodo zgodovinske analize sem uporabila predvsem pri opisovanju razvoja posameznega koncepta zasebnosti;
- s sistemsko analizo sem analizirala posamezni koncept pojmovanja zasebnosti, ugotavljala povezave med njimi in iz sodb Vrhovnega sodišča ZDA ter Evropskega sodišča za človekove pravice vključno z Ustavnim sodiščem Slovenije poizkušala razumeti razvoj smernic tega področja v prihodnje;
- z metodo primerjalne analize sem primerjala določene odločitve vrhovne sodne oblasti, kje so se obravnavali enaki oziroma zelo podobni primeri.

Med empiričnimi raziskovalnimi metodami sem uporabila:

- metodo analize rezultatov ankete, ki sem jo izvedla med zaposlenimi v večjih podjetjih na nivojsko različnih delovnih mestih, med zaposlenimi v državni upravi ter zaposlenimi pri zasebnikih,
- metodo sekundarne analize rezultatov statistik, ki zadevajo relevantno tematiko, pri pojasnjevanju teoretičnih dejstev in ugotovitev skozi celotno diplomsko nalogo;
- metodo razgovora z nekaterimi predstavniki strokovne javnosti o problematiki varovanja nedotakljivosti zasebnosti na delovnem mestu, ki je služila zgolj kot smernica pri izdelavi diplomske naloge in kot dopolnilna metoda pri oblikovanju zaključkov.

Strukturno je diplomska naloga sestavljena iz treh delov. V **prvem delu** naloge je podrobno predstavljen pojem zasebnosti in pravice do zasebnosti. Opisan je zgodovinski razvoj in razloženi so vzroki kateri so narekovali hiter razvoj obravnavanega področja.

V **drugem delu** sledi opis koncepta pojmovanja zasebnosti v anglosaškem in kontinentalnem svetu, njihov pomen, razlike in morebitne skupne točke. Podrobno je

predstavljena tudi različnost obravnavanja pojma poseganja države v posameznikovo zasebnost.

V **tretjem delu** je opisano občutljivo področje zasebnosti osebnih podatkov v anglosaškem svetu, kontinentalnem svetu in podrobneje v Sloveniji. Posebej so še izpostavljeni zdravstveni podatki, saj so le ti podatki najbolj občutljivi, hkrati pa so izjemno pomembni za razvoj medicinske znanosti in so tudi tržno zanimivi.

PRVO POGLAVJE

V uvodnem delu podajam uvodne misli, opredelila sem predmet proučevanja, zastavila hipoteze, opredelila metodološki pristop in strukturo diplomske naloge.

DRUGO POGLAVJE

V drugem delu opredeljujem najpomembnejše termine kateri so v diplomski nalogi, s čimer se bom izognila problemom terminološke nejasnosti.

TRETJE POGLAVJE

V tretjem poglavju opisujem zgodovinski razvoj pojma zasebnosti, predstavljam pomen množične družbe in začetke omejevanja le te.

ČETRTO POGLAVJE

V četrtem poglavju podrobneje predstavljam pravico do zasebnosti in že nakazujem razlike med ZDA in Evropo.

PETO POGLAVJE

V petem poglavju je predstavljena pravica do zasebnosti v ZDA od ustavne podlage do sodobnih groženj o omejevanju pravice.

ŠESTO POGLAVJE

V tem poglavju je opisana pravica do zasebnosti kot jo pojmuje Evropa, prikazane so konceptualne razlike in zakonske omejitve pred nepooblaščenimi posegi.

SEDMO POGLAVJE

V sedmem poglavju sem predstavila izredno občutljivo področje v poglavju zasebnosti, to je zasebnost osebnih podatkov. Prikazane so mednarodne usmeritve, ameriško in posebej evropsko pojmovanje zaščite osebnih podatkov. Opisana je tudi slovenska ureditev, posebej pa je predstavljeno področje t.i. zdravstvenih podatkov in tanka meja med dovoljeno in nedovoljeno uporabo teh podatkov posameznika.

OSMO POGLAVJE

V osmem poglavju predstavljam izvedeno raziskavo mnenja javnosti, ugotovitve raziskave in podajam sklepne ugotovitve, s pomočjo katerih je bila izvedena verifikacija zastavljenih hipotez.

2 OPREDELITEV TEMELJNIH POJMOV

2.1 Pravo človekovih pravic

Temelji prava človekovih pravic se izražajo v nacionalnih in ustavnih normah in načelih.

Problemi ustavne presoje, metodologije in oblike

Da v nobeni državi ne sme imeti noben državni organ absolutne oblasti (!) je ideja, ki je vzniknila v 18. stol, zaznamo pa jo že pri Aristotelu in Platonu, kot razmišljanja na ravni filozofskih razprav. V pravno doktrino pa jih je prvi zapisal John Locke »oblast mora biti razdeljena« in MontesQue »oblast mora biti razdeljena na tri nosilce oblasti: zakonodajno, izvršilno in sodno«. Sodna oblast je poslednja instanca za presojo kaj je prav in kaj ni, ali je neko ravnanje v skladu z ustavo in ali niso prizadete človekove pravice, MontesQue v knjigi V duhu zakonov (18. stol).

Prvi praktični preizkus te doktrine je bil v Ameriki (II. pol 18. stol). Leta 1776 so federalisti izdajali zbirko »Federalis papers«. V njej Tomas Jefferson navaja, da oblast pripada ljudstvu in ljudstvo postavlja kneza. Citirana Zbirka pomeni uvod v sprejem ameriške ustave, njeno realizacijo in razvoj. Pomembno spoznanje je, da tudi zakonodajalec ne more ravnati neomejeno, čeprav je najvišji organ. Spoštovati namreč mora najvišji zakon (Summa ius) Ustavo, ki jo je sam sprejel. Tem načelom gre pripisati zaslugo za pridobitev vloge ustavnega sodstva (leto 1803). Ameriško vrhovno sodišče je razsodilo, da mora država spoštovati lastne zakone, spoštovati ustavo, in če je zakon v nasprotju z ustavo, ga je treba razveljaviti (primer Adamson – to je bila prva sodba v tej smeri, ki pa je ameriški kongres ni upošteval, zato je ameriško vrhovno sodišče takoj naslednje leto izdalo drugo, po vsebini pa identično sodbo in od takrat dalje kongres spoštuje vse sodne odločbe vrhovnega sodišča. Naloga ameriškega vrhovnega sodišča je torej dvojna presoja: sodbe in presoja skladnosti zakonov z ustavo – od leta 1804 ima torej v tem delu vlogo ustavnega sodišča).

Evropa je na tem področju v vsem 19. stoletju zaostajala za Ameriko, kajti Evropa ne pozna sodnega nadzora nad delom parlamenta. V letih pred I. svetovno vojno je bilo vse pripravljeno za ustavnopravno sodstvo vendar je I. svetovna vojna nekoliko zavrla ta razvoj, saj je do ustanovitve prvih ustavnih sodišč v Evropi prišlo šele, ko Češkoslovaška republika ustanovi prvo Ustavno sodišče, za njimi je bilo ustanovljeno Avstrijsko, ki je tudi najstarejše neprekinjeno delujoče ustavno sodišče na Evropskih tleh. Pravi razcvet pa doživijo ustavna sodišča po II. svetovni vojni. Kršitve človekovih pravic med II. svetovno vojno je v ospredje postavilo zahtevo po spoštovanju človekovih pravic. K temu je pripomoglo tudi sprejetje Deklaracije o človekovih pravicah leta 1948. II. polovica preteklega stoletja pomeni precejšen vzpon pomena ustavnega sodišča, poleg tega pa dobivajo tudi nove pristojnosti in sicer poleg ugotavljanja skladnosti zakona z ustavo tudi primerjavo skladnosti posameznih podzakonskih aktov, z zakoni omogočena pa je tudi ustavna pritožba in sicer če je bila posamezniku kršena

pravica s posamičnim aktom (človekova pravica). Z Ustavno pritožbo se presoja skladnost ravnanja sodne oblasti z ustavo (gre za nadzor nad sodnim delom in delom upravnih organov).

Evropski pravni sistem in Evropsko sodno varstvo v svojem klasičnem vzoru (Franciji) je dedič kartizanskega načina mišljenja (Rene De Scartes) pri katerem prehajaš od teoretične generalne zasnove h konkretnemu. Anglosaški sistem ima drugačen način mišljenja, ki temelji na eksperimentu (F. BACON) – zadeve so reševali na konkretnem primeru in sicer so iz niza konkretnih primerov oblikovali pravila (pravni sistem primerov - case) ali prilogov (Case iz 16. stol. Rooker's case: kdaj je treba neko ravnanje spoznati za samovoljno).

Evropsko sodišče za človekove pravice (ESČP) je bilo ustanovljeno z Evropsko konvencijo, ki je osnova za delo sodišča. Sodišče je začelo nizati kup primerov (case), kar je povzročilo številne posledice, oba pravna sistema sta se začela približevati, pomembno vlogo pa je imelo Kanadsko vrhovno sodišče (Kanada je dežela dveh kultur: angleške in francoske – evropske). Kanada zelo dobro pozna Evropski pravni sistem, skozi Case Low so začele v evropski prostor vstopati odločbe sodišč (vrhovnih, upravnih, ustavnih in ESČP), danes pa je case low normalni sestavni del uporabe prava. Na drugi strani pa je tudi evropski sistem pomembno vplival na anglosaksonski sistem, ki je po »naravi nekoliko zadržan«.

Pri obravnavanju primerov sodišča presojajo zadeve po:

- testu razumnosti;
- testu sorazmernosti.

Test razumnosti

Gre za minimalno sodno presojo ravnanja države in dopušča vsakršno ravnanje države, če je to ravnanje razumno (npr. včasih se za tem ravnanjem skriva prikrita diskriminacija – primer Anglija: nerazumna je pravna ureditev, ki ni dopuščala zaposlovanja učiteljic z rdečimi lasmi - le te so imeli Irci). Test razumnosti je najmilejša presoja. V Evropi pa je tako pravna doktrina kot tudi sodna doktrina razvila bolj tenkočuten pristop, ki daje sodišču večje pristojnosti.

Test sorazmernosti

1. ali je pravna ureditev smiselna – razumna;
2. ali je ta ureditev potrebna za dosego cilja (primerjava med namenom in ciljem); kadar ni na razpolago nobenega drugega sredstva je potrebno uporabiti najmilejše sredstvo, s katerim se prav tako doseže namen zakonodajalca, sicer je napadena ureditev v nasprotju.

Vse do 19. stol. je anglosaksonski sistem presojal zakone le s testom razumnosti, kasneje pa priznajo tudi test prepovedi prekomernih ukrepov (test sorazmernosti). Evropa v 19. stol. pozna prepoved prekomernih ukrepov in jo spoštuje, anglosaksonski sistem pa to od Evrope povzame. (19. stol. San Francisco - odlok o delovanju javnih pralnic je določal pogoje za obratovanje le teh ter je določal, da se sme dejavnost opravljati le v zidanih objektih – v ozadju je bila diskriminacija proti Kitajcem, ki si niso mogli privoščiti zidanih objektov in so

izvajali dejavnost javnih pralnic v brunaricah. Vrhovno sodišče je odlok razveljavilo z navedbo, da postavljanje takih pogojev v svojem bistvu pomeni obliko diskriminacije).

2.2 Razvoj ustavnega sodstva ter ustavno sodna presoja

1. člen zakona o ustavnem sodišču, opredeljuje Ustavno sodišče kot najvišji organ sodne oblasti v državi za varstvo zakonitosti in ustavnosti ter človekovih pravic in temeljnih svoboščin. Na ta način je opredeljena vloga Ustavnega sodišča v nacionalnem pravnem sistemu. Ustavno sojenje zagotavlja varovanje načela ustavnosti, načela prevlade ustave nad zakonom in drugimi akti.

Ustavno sojenje v širšem in pravnem smislu je reševanje v sodni obliki določenih ustavnopravnih vprašanj, in to z namenom varstva ustave: v ožjem smislu to pomeni presojo ustavnosti zakonov s strani sodišča, v širšem pa tudi ustavno sodno presojo drugih predpisov in posamičnih aktov in nekatere druge ustavno in zakonsko določene pristojnosti.

Razvoj ustavnega sodstva za varstvo ustavnosti in zakonitosti sega daleč nazaj v zgodovino. Že v starem atenskem pravu so poznali načelo, da morajo biti akti, ki so bili pod ustavo t. i. Nomos, v skladu z njo. To pomeni, da je ustanovitev najvišjih sodnih organov za varstvo zakonitosti in ustavnosti povezana z razvojem ustavnosti na evropski celini. Elementi ustavnega sodstva se kažejo že v starem nemškem rajhu v letu 1180, tako da se je sodna presoja razvijala skozi zgodovino in bila nenazadnje uvedena v Weimarsko ustavo. Predhodne oblike ustavnega sojenja segajo v sredino 13. stoletja v Franciji, v začetku 17. stoletja pa se je sodna presoja pojavila na Portugalskem v Filipovem zakoniku, v tem obdobju pa se kažejo še v Grčiji in na Norveškem. Leta 1867 se je v Avstriji zvezno sodišče ukvarjalo z ustavno državno pritožbo – varstvo ustavnih pravic pred zveznim sodiščem.

Norveška, Švedska in Danska imajo sodišče za varstvo ustavnih pravic izven rednega sodstva. Pred 1. svetovno vojno najdemo elemente ustavnega sodstva tudi v Romuniji. Leta 1920 je bilo v Avstriji ustanovljeno ustavno sodišče, ki je tudi najstarejše ustavno sodišče v Evropi, ki je vseskozi delovalo neprekinjeno. Sicer je pred njim bilo ustanovljeno ustavno sodišče na Češkoslovaškem, vendar je bilo njegovo delovanje prekinjeno.

Ustavno sodno presojo izvajajo različni organi:

1. Ustavna sodišča
2. Visoko sodišče ali posebni senat visokega sodišča
3. Ustavni svet

Načini s katerim se ustavno sodno odloča so: evropski, ameriški in mešani.

V svetu so poznani modeli ustavnosodne presoje:

1. **Ameriški-judicial review model**, ki temelji na zadevi vrhovnega sodišča ZDA Marbury iz leta 1803, po katerem ustavne zadeve presojuje vsa sodišča splošne pristojnosti (decentralizirana ali difuzna ustavnosodna presoja) v povsem rednem postopku (in venter). V tem sistemu odločitve praviloma učinkujejo le *inter partes*. Odločitev sodišča o neustavnosti zakona je praviloma retroaktivna, t. i. *ex tunc*. Ta sistem so prevzele naslednje države: Danska, Švedska, Norveška, Estonija, Irska, Argentina, Tanzanija, Izrael, Iran, Indija, Japonska, ZDA, Kanada itd.
2. **Novi Commonwealth model** ni mogoče uvrstiti niti v ameriški niti v evropski model. Njegova značilnost je koncentrirana ustavnosodna presoja v pristojnosti vrhovnega sodišča, sestavljenega iz rednih sodnikov brez politične nominacije. Praviloma gre za preventivno presojo in je funkcija vrhovnega sodišča svetovalne narave, čeprav je možna tudi represivna presoja. Odločbe imajo učinek erga omnes. Ta model je povzela država Mavritius.
3. **Avstrijski** (kontinentalni-evropski) model, ki izvira iz Kelsnovega modela iz leta 1920. Ta model sloni na povezavi med načelom prevlade ustave in načelom prevlade parlamenta. V tem modelu ustavne zadeve presojuje ustavna sodišča s posebej kvalificiranimi sodniki ali vrhovna sodišča splošne pristojnosti oziroma njihovi posebni oddelki. Gre za koncentrirano ustavnosodno presojo v posebnem postopku. Odločitve imajo praviloma učinek erga omnes. Organi ustavnosodne presoje imajo lahko različne nazive:
 - *Ustavna sodišča* (Italija, Avstrija, Slovenija, Hrvaška, Madžarska, Nemčija, Poljska, Španija, Turčija itd).
 - *Vrhovna sodišča ali njihovi posebni oddelki* (Belgija, Islandija, Lichtenstein, Zambija, Sudan, Zair,
 - *Ustavni svet* (Libanon, Senegal, Kambodža).
4. **Mešani (ameriško kontinentalni) model** z elementi difuznega in koncentriranega sistema, kljub pristojnosti centralnega ustavnega ali vrhovnega sodišča za ustavnosodno presojo imajo vsa sodišča v konkretni državi pravico, da ne uporabljajo zakonov, ki jih štejejo za protiustavne. Organi ustavnosodne presoje so: *Ustavna sodišča* (Portugalska, Peru, Kolumbija), *Vrhovna sodišča ali njihovi posebni oddelki* (Grčija, Švica, Tajvan, Venezuela itd)
5. **Francoski model (kontinentalni)**, ki temelji na modelu francoskega ustavnega sveta iz leta 1958, kjer ustavnopravne zadeve presojuje posebni organi ustavnosodne presoje, predvsem ustavni svet ali posebni oddelki vrhovnih sodišč splošne pristojnosti, s tem, da je presoja ustavnosti v glavnem preventivne (posvetovalne) narave (Francija, Alžir itd).
6. **Sistem brez ustavnosodne presoje** je v Veliki Britaniji, čeprav ima House of Lords nekatere elemente preventivne presoje ustavnosti, in na Nizozemskem z nekaterimi izjemami, saj je integracija v evropske institucije vplivala na prelom temeljnih načel nizozemskega pravnega sistema o prepovedi ustavnosodne presoje.

Mednarodna združenja institucij, ki izvajajo sodno presojo ustavnosti:

- Komisija za demokracijo skozi pravo (Beneška komisija) – Glavna naloga komisije je promovirati načelo delitve oblasti ter načela pravne in socialne države, podpirati

razvoj sodne presoje ustavnosti, kot tudi promovirati razvoj informacijskih baz organov ustavnosodne presoje v državah članicah;

- Konferenca ustavnih sodišč Skupnosti neodvisnih držav (novih demokracij);
- Južnoameriška skupina organov ustavnosodne presoje;
- Zveza francosko govorečih ustavnih sodišč;
- Evropska konferenca ustavnih sodišč - Ustavna sodišča se od leta 1972 povezujejo v obliki neformalne konference ustavnih sodišč. Gre za razširjeno obliko že tradicionalnih bilateralnih in informativnih stikov med ustavnimi sodišči, ki pomeni razširitev in poglobitev teh stikov. Sodišča so navezala med seboj delovne stike in medsebojno izmenjavo mnenj.

2.3 Razvoj ustavnega sodstva v Sloveniji

Pred letom 1963 je v Sloveniji veljal nadzor nad ustavnostjo in zakonitostjo normativnih aktov po načelu samopresoje znotraj skupščinskega sistema. Nadzor je bil usmerjen predvsem na skladnost politike, izražene v nekaterih normativnih aktih, manj pa na zakonitost v pravem pomenu besede. Glede zakonitosti je bil zelo tolerant in zato malo učinkovit.

Zato so leta 1963 zvezna in republiške ustave bivše jugoslovanske federacije uvedle ustavno sodišče kot samostojni organ po sodobnem evropskem vzorcu s točno opredeljenimi pristojnostmi na področju varovanja ustavnosti in zakonitosti, kot poseben organ poleg organov skupščinskega sistema v ožjem smislu, prav tako pa tudi poleg že obstoječih organov v sistemu rednega sodstva. Pristojnost devetih ustavnih sodišč bivše federacije je bila urejena v skladu s tedanjo delitvijo pristojnosti med federacijo in republikami oz. avtonomnima pokrajinama, tako, da je vsako od teh sodišč delovalo institucionalno samostojno v skladu s pristojnostmi, opredeljenimi v ustavi ustrezne ravni. Pri tem med ustavnimi sodišči ni bilo hierarhičnega odnosa oz. zvezno ustavno sodišče ni bilo instanca nad drugimi ustavnimi sodišči.

V Sloveniji je sodno presojo ustavnosti uvedla ustava tedanje federalne enote republike Slovenije iz leta 1963 in sicer v kombinaciji s tedanjim veljavnim ustavnim načelom enotnosti oblasti. Zakon o ustavnem sodišču je uredil pristojnosti in postopek ter določil dejanski začetek dela sodišča, to je 15. 2. 1964. Pozneje je sodišče sprejelo svoj prvi poslovnik.

2.4 Veljavna ureditev ustavnega sodstva v Sloveniji

Ustava Republike Slovenije iz leta 1991 je ustavnemu sodišču določila pomembnejšo vlogo. Njegove nekdanje »klasične« pristojnosti so razširjene s številnimi novimi (160 člen ustave). Ustava pa dopušča nadaljnje širjenje pristojnosti ustavnega sodišča z zakoni (11. alineja prvega odstavka 106. člena ustave).

Veljavni zakon o ustavnem sodišču (Ur. list RS, št. 15/94) je podrobneje uredil postopek pred ustavnim sodiščem, pravne posledice odločitev, merila in pogoje za obravnavanje ustavnih pritožb ter način izvolitve in razrešitve ustavnih sodnikov.

Na področju varstva ustavnosti in zakonitosti ter človekovih pravic in temeljnih svoboščin je ustavno sodišče postalo najvišji organ v državi. Institut ustavne pritožbe je na ta način ustavno sodišče nadgradil v najvišjo nacionalno sodno instanco za varstvo človekovih pravic in temeljnih svoboščin.

3 ZASEBNOST

Stikanje po zasebnosti drugih je staro toliko kot človeštvo, opravljanje in prenašanje govoric pa pojav, od katerega danes živi dobršen del medijev. Koliko odpreti vrata v območje zasebnosti, kje je meja med zasebnim in javnim, oziroma kje se začne tisti del zasebnosti, do katerega javnost vendarle nima pravice?

Enoznačne opredelitve pojma zasebnosti ni. Težko bi jo našli tudi v pravni teoriji in praksi, ter v odločbah ustavnih sodišč. Zasebnost je nekaj, kar je medkulturno in medvrstno univerzalno in ni značilno samo za človeka.¹²

Z zasebno sfero se povezujejo vprašanja bistva in vrednosti človeka in rangiranje zasebne sfere na sedanji stopnji civilizacije. Upoštevati jo je treba kot posebno pravno dobro, ki ji mora pravni red zagotoviti potrebno varstvo. Na tem področju se vzpostavlja znano razmerje med etiko in pravom. V ustavi ni izrecne opredelitve zasebne ali intimne sfere, vsekakor pa je pojem vsebovan v več ustavnih pravicah in svoboščinah: pravica do osebnega dostojanstva in varnosti (34. člen), varstvo pravic zasebnosti in osebnostnih pravic (35. člen), nedotakljivost stanovanja (36. člen), varstvo tajnosti pisem in drugih občil (37. člen) in varstvo osebnih podatkov (38. člen). Naštete pravice preprečujejo državi poseganje v zasebno področje človeka. Izjemoma je poseganje dovoljeno na podlagi posebnih ustavnih določb ali splošnega pravila iz 15. člena ustave, (Šinkovec, 1997, str. 175).

Tradicionalno so šteli za zasebno sfero domače zasebno življenje, družinski krog, krog sorodnikov, prijateljev in ožjih znancev. Stanovanje je bilo sprva varovano pred radovednimi sosedi, s pojavom senzacionalističnih časopisov ali takih člankov je bilo treba dogajanje v stanovanju (domu) obravnavati širše. Širše obravnavanje je narekoval tudi pojav tehničnih sredstev, s katerimi se zlahka vdira v zasebnost ljudi v stanovanju, (Šinkovec, 1997, str. 176).

Zasebnost ščiti svobodo posameznika, zato za tradicionalnega nasprotnika zasebnosti večinoma velja država, vendar se svoboda ne nanaša zgolj na odnos posameznika do politične oblasti, temveč tudi do družbe.

Poglavitni akter, ki v današnjem času ogroža zasebnost posameznikov je pravzaprav družba, država pa ima ambivalentno vlogo – po eni strani posega v zasebnost posameznikov, po drugi strani pa posameznika varuje pred vplivi družbe. Vloga družbe pri omejevanju posameznikove zasebnosti postane očitna predvsem po zgodovinskem pregledu odnosa med zasebno in javno sfero ter pri analizi sodobnega nadzorovanja, ki kaže, kako se je

¹² Alan Westin je npr. ugotovil, da se tudi živali v določenih obdobjih zatečejo v samoto ali v intimen objem manjših skupin, poleg tega na obstoj zasebnosti kaže tudi branjenje lastnega teritorija (Wagner DeCew, 1997: 12).

izoblikovalo tisto, čemur danes pravimo družba nadzora. Da so vplivi na zasebno sfero s strani družbe bistveno bolj problematični kot posegi s strani države, pa kaže primerjava med pravnim varstvom zasebnosti v Evropi in ZDA, (Kovačič, 2006, str. 11).

V sodobni družbi postaja zasebnost tržno blago, s katerim je mogoče trgovati in ne več pravica, ki jo je treba varovati. Tudi zato se varovanju zasebnosti posveča vedno večja pravna varnost, priznanju pravice do osebnega življenja je namenjena pozornost v mednarodnih listinah, konvencijah, deklaracijah, pa tudi v pravu posameznih držav.

3.1 Zgodovinski razvoj sodobne zasebnosti

Temeljne oziroma klasične človekove svoboščine in pravice so pridobitev tisočletnega spopadanja med nosilci družbene moči in sloji, ki so takšni oblasti podrejeni. Poleg večnostnega argumenta v prid človekovim pravicam ni drugega bolj prepričljivega kriterija za presojo aktualne podobe in razvejanosti pravic, kot je zgodovinsko prehojena pot pri njihovem utemeljevanju, oblikovanju ter uveljavljanju. Samo spremljanje zgodovinskega razvoja človekovih pravic je obenem možnost za preverjanje stanja zgodovinske zavesti o pravicah v posamezni družbeni skupnosti, še posebej njene kontinuitete ter tudi resničnega ali zgolj navideznega vnašanja prelomnic v to kontinuiteto. Prav zgodovinski razvoj kliče v zavest dejstvo, da vprašanje človekovih pravic ni le eno od vprašanj posamezne družbe ter njene politične ureditve, temveč njeno osrednje vprašanje od čigar razrešitve je odvisna celotna politična zgradba družbe. Torej brez jasne zgodovinske zavesti o razvoju človekovih pravic ni možno teoretično razpravljanje o pravicah, saj se ne bi bilo mogoče izogniti oviram ki jih nenehno postavlja močna ideologizacija ter poskusi nezgodovinske absolutizacije stanja pravic v posamezni družbi, (Jambrek in drugi, 1988, str. 17).

Vsa človekova zgodovina je zgodovina njegovega boja za svobodo, saj je svoboda bistvena človekova lastnost, ki jo je prav zaradi tega mogoče antropološko utemeljiti. Zaradi tega je človekova misel, odkar se le-ta zaveda svojega obstoja, pretkana z idejami o svobodi in z njo nerazdružljivo povezanim načelom enakosti, pri čemer so konkretne zgodovinske razmere določale stopnjo abstraktnosti in utopičnosti teh idej. Vsem pa je bilo skupno iskanje odgovora na vprašanje, kakšen je odnos med posameznikovo svobodo in politično skupnostjo, (Jambrek in drugi, 1988, str. 18 - 19).

V Grčiji so grški misleci trdili, da lahko človek svobodno živi le v skupnosti in sicer v politično organizirani skupnosti (polisu), ki je edina sposobna razvijati posameznikovo moralno popolnost in zadostiti njegovemu iskanju sreče. Ker za uresničevanje svobode ni druge možnosti, ni prihajalo do nasprotja med interesi posameznika in skupnosti in zato ni bilo prostora za utemeljevanje takih človekovih pravic, ki bi ga zavarovale pred oblastjo in določale meje njegove svobode. Pravice so torej bile le funkcionalne in ne prednostne. Kot del tako pojmovane demokracije se je v Atenah razvila zamisel o enakosti posameznikov pred zakonom in o pomenu prava kot zaščiti posameznikov pred dejanji drugih. Vendar pa se

je načelo enakosti nanašalo le na svobodne Grke. V nadaljevanju razvoja so zamisel o pomenu prava za enakost državljanov precej bolje razvili Rimljani. Vrh kodifikacije rimskega prava je bil dosežen v Justinijanovem Monumentalnem zakoniku iz leta 529, ki je služil kot temelj zahodnega evropskega prava. Bistvo zakonika je zaščita pravic vsakega posameznika, vendar pa ima vsakdo dolžnost izpolnjevati naloge, ki so mu zaradi njegovega položaja naložene, (Jambrek in drugi, 1988, str. 20).

Že nekatere navedbe v bibliji, v koranu, judovski tradiciji, antični Grčiji in starodavni Kitajski kažejo na to, da zasebno sfero poznajo različne kulture in družbe.

Prve začetke moderne zasnove človekovih pravic moremo iskati šele v 17. in 18. stoletju. Kontinuiteto pa kvečjemu v rastoči zavesti, da je temeljni problem človekovih pravic v vzpostavitvi ustreznih omejitev tistim ki izvršujejo oblast v posamezni prisilno organizirani družbi. Moderna doba je postopoma preoblikovala človekov odnos do politično organizirane skupnosti. Človek se rodi svoboden, država kot prisilna organizacija pa njegovo svobodo na najrazličnejše načine omejuje. Bistvo boja za človekove pravice je tako v prizadevanjih po utesnitvi oblasti in določitvi mej, ki jih le-ta ne sme prestopiti. Meščanski koncept človekovih pravic se razlikuje od vseh prejšnjih predvsem v oblikovanju jasnega spoznanja, da ni mogoče govoriti o človekovih pravicah vse dotlej, dokler niso le-te priznane na pravno oblikovan način, se pravi dokler oblast javno ne prizna svojih omejitev ter sredstev, ki so na voljo posamezniku ko se sooča z oblastjo, (Jambrek in drugi, 1988, str. 20 - 22).

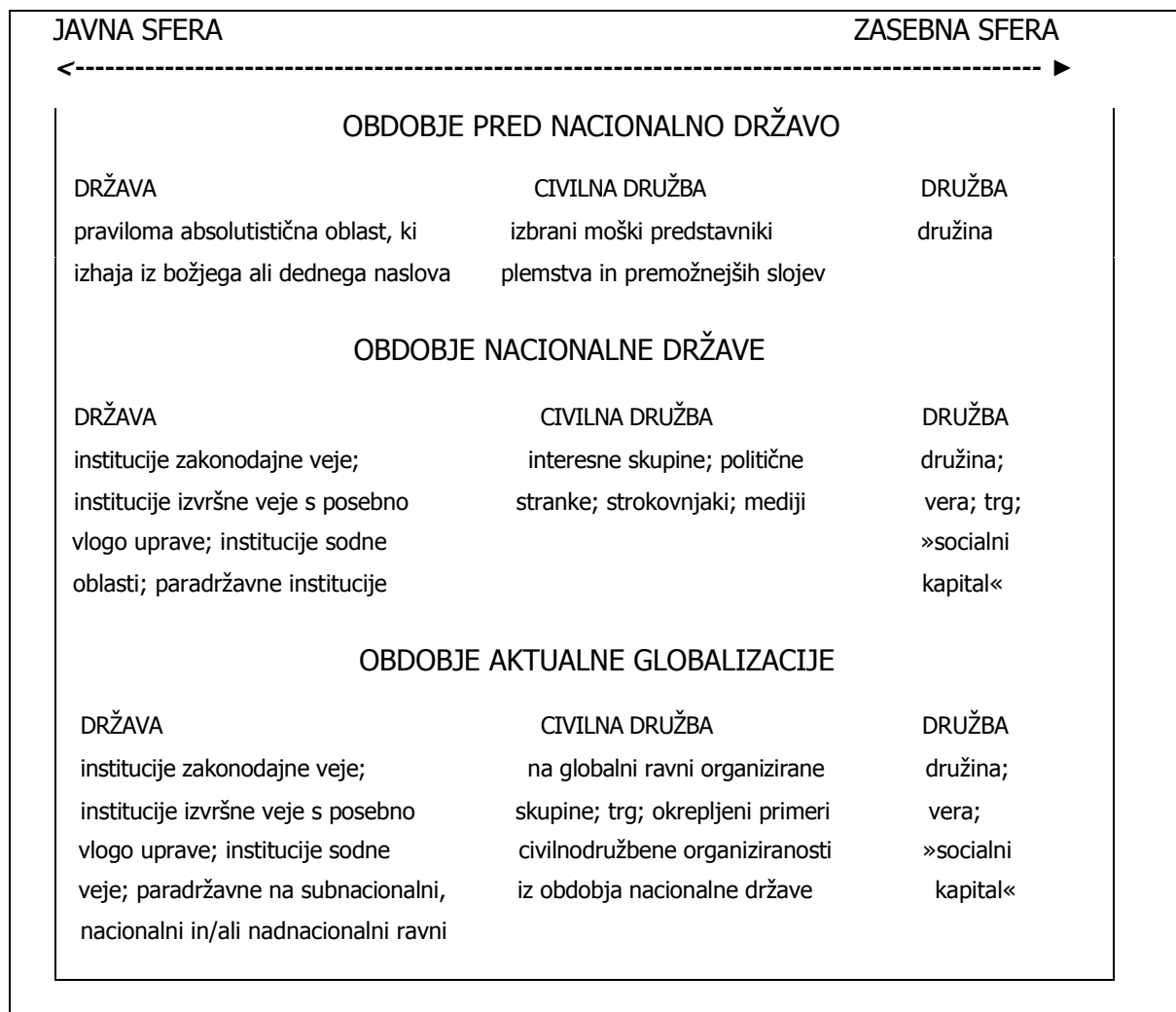
Koncept zasebnosti kot ga pojmuje danes, se razvije šele v 19. stoletju. Zasebnost kot moderna kategorija nastaja istočasno s procesom formalne institucionalizacije javnosti, z ustanavljanjem prvih mnenjskih časopisov, kar pomeni da je legitimnost javnega izražanja mnenj konstitutivno povezana z možnostjo javnega publiciranja. Novi načini komuniciranja so vplivali na pojmovanje javnega in zasebnega. Novoveška zasebnost se razcepi na tisti del, ki je pod neposredno regulacijo države (lastninske pravice in nedotakljivost zasebnih prostorov).

Razkroj javne sfere se je torej začel že pred stoletjem in posledice razkrajanja so vplivale na večje premike med javno in zasebno sfero. Javnost se je privatizirala (in intimizirala), zasebnost pa podružbljala, družbena sfera pa je istočasno začela prevzemati večino vlog, ki jih je v tradicionalnem pojmovanju imela javnost, (Thompson, 1990, str. 112).

V pozno kapitalističnem sistemu prihaja do tekmovalnosti med identitetami. Pride do trčenja med identiteto potrošnika in identiteto državljana prav zaradi tega, ker visoko razvite družbe ponujajo zasebne rešitve za javne probleme. Meščanska država je nadaljevala »tridelni« model, v katerem se med javno in zasebno sfero vmešča sfera družbenega, pozni kapitalizem pa je popolnoma izločil družino iz ekonomske sfere in javnost iz sfere države. Sfera javnosti in države sta javni v tem pomenu da se obe nanašata na celoto, v nasprotju z ekonomijo in družino, ki sta zasebni v tem, da sta vodeni z zasebnimi partikularnimi interesi (Peters, 1993, str. 558). Vendar pa je tisto, kar danes poznamo pod imenom zasebnost oziroma pravica do zasebnosti, pravzaprav iznajdba razsvetljenstva, torej nekaj, kar nastane na zahodu šele v

času nastanka kapitalizma, nekoliko jasneje pa se začne izražati šele ob "nastanku" oziroma kodificiranju univerzalnih človekovih pravic.

Slika 1: Javna in zasebna sfera skozi čas



Vir: Kustec Lipicer (2006, 180).

3.2 Zasebnost v množični družbi

Družba, v kateri so posamezniki informacijsko povezani z množičnimi občili, a razpršeni v prostoru in nepovezani v skupnost v tradicionalnem pomenu besede, imenujemo množična družba. Odras tega je množična kultura, ki obravnava javnost kot statističen pojem in ne kot seštevček posameznikov.

Večina teorij o nastanku množične družbe in kulture je nastala ob začetku procesa industrializacije in z vse hitrejšim preseljevanjem ljudi v mesta in kopičenjem v njih.

Industrijska revolucija je ustvarila nove pogoje za življenje ljudi, ljudje so se na te pogoje odzvali z upanjem na »boljše« življenje in so se začeli množično naseljevati na območja z ustrezno infrastrukturo, ki so bila v mestih.

Ključne značilnosti, ki opredeljujejo pojem množične družbe, lahko opišemo z naslednjimi ugotovitvami (Ilič, 1978, str. 82):

- povečanje prebivalstva v sodobnem svetu (»demografska eksplozija« v industrijsko razvitem delu sveta);
- intenzivni procesi urbanizacije in posledično »ustrezno« spreminjanje življenja;
- mehanizacija in avtomatizacija proizvodnje;
- spremembe v socialni in politični strukturi v mnogih državah;
- v povprečju se je zvišal življenjski standard;
- povečanje količine t. i. prostega časa ter sprememba v načinu njegovega preživljanja.

Za sodobno urbanizirano in industrializirano družbo se je razširil in tudi že uveljavil izraz množična družba. Medtem ko je pojem »družba« jasno opredeljen, pa pojem množična družba nima dovolj trdne strukture. Morda je še najbolj ustrezna opredelitev množičnosti, ki jo uporablja Cazeneuve, ko pravi, da pojem množica pomeni eno od oblik družbenosti, za katero je značilna nehomogenost, (Cazeneuve, 1963, str. 720 – 731).

Koncept množične družbe, kakršnega so razvili predvsem ameriški sociologi, pa temelji na dveh postavkah: prvič, človek je svoboden in drugič, hkrati kontroliran z institucionaliziranimi strukturami. Po mnenju nekaterih teoretikov pomeni množična družba popolno izgubo individualnosti, popoln konformizem in morda celo averzijo posameznih članov družbe, da bi imeli kako posebno identiteto. Na drugi strani pa nekatere teorije trdijo, da porast osrednjih institucij v družbi ne odvzema »svoboščin« posamezniku, temveč jih krepi s tem, da prispeva k odklanjanju tradicije in oboževanja avtoritet.

V sodobnem življenju je človek neredko javno izpostavljen v zelo intimnih občutkih, v javnem življenju so močno presežene nekdanje tabu teme iz področja spolnosti; ljudje so izpostavljeni številnim psihološkim in drugim testom. Nekateri ljudje imajo osebni interes, da sami objavljajo sporočila o svojih intimnostih. Vsi ti pojavi povzročajo, da se pri nekaterih javno delujočih osebah splošen občutek za intimnost zmanjšuje, kar pa ne more opravičevati države, da bi posegala na to področje, spremeniti pa tudi ni mogoče veljavnih pogledov prava o varstvu zasebnosti. Pri večini prebivalstva se pojavlja strah in vznemirjenje zaradi nepreglednih in nekontroliranih možnosti za poseganje v zasebnost. Nekateri celo govorijo o »steklenem človeku«, ker obstajajo tolikšne možnosti za vpogled v zasebno sfero, (Šinkovec, 1997, str. 176).

Vendar pa se ožetje zasebne sfere ne ustavi pri zoženju na intimno. Država (če je demokratična) sicer na intimna področja posameznikov ne prodira, zato pa tja prodira družba. To postane očitno predvsem ob nastanku množičnih medijev in sodobnega potrošništva. Po eni strani zasebne zgodbe posameznikov postanejo tržno blago, javnost pa postane sfera

objavljanja zasebnih življenjskih zgodb (Habermas, 1962/1989, str. 190)¹³, po drugi strani pa zasebnost postane ovira pri uresničevanju ekonomskih in političnih interesov, saj nadzor čedalje bolj postaja orodje množičnega marketinga in upravljanja družbe. (Kovačič, 2006, str. 16)

Slika 2: Razlike med javnim in zasebnim delovanjem / interesom

Lastnosti	Javno	Zasebno
Problematika	Kompleksna, pogosto nejasna, zapletena, ni enoznačnih rešitev	Ozka, problem neke skupine, ki je pogosto vezan na ekonomske razloge
Način reševanja problema in sankcioniranja	Javno, po načelu večinske volje; sankcioniranje izvajajo državni javnopolitični igralci (državno/kazensko pravo)	Ožje, znotraj neke civilnodružbene skupnosti, ki tudi izvaja sankcije (avtonomno/civilno pravo)
Institucionalizacija	Visoka in kompleksna, veliko število različno motiviranega in izobraženega kadra, ki je odgovoren za svoje delo	Navezanost na zasebno organizacijo v kateri praviloma delujejo strokovnjaki
Vrednote	Poštenost, pravičnost, pomen javnega interesa	Tržne, pomen kolektivnosti skupine in zaupanja vanjo
Javna podpora	Vsaj minimalna splošna podpora	Potrebna je le podpora članov neke skupine, ki ni nujno tudi splošna javna podpora

Vir: Kustec Lipicer (2006, 51).

Z vdorom dotlej nepripuščenih množic v meščansko javno sfero - z razširitvijo volilne pravice - se javno mnenje vzpostavi kot "najmočnejša sila", hkrati pa nastanek množičnih medijev odpre nove možnosti za širjenje idej in oglaševanja. Pride do oženja javnega prostora, hkrati pa družba (mediji, oglaševalci) čedalje bolj prodira v intimno sfero. Bistvo množičnih medijev tako postaja potrošniška vzgoja ter nadzor (Habermas, 1962/1989, str. 212 in Splichal, 2002, str. 181), javno mnenje postane sredstvo gospodovanja družbe nad posameznikom (Splichal, 2002, str. 74), kritične državljane nadomestijo potrošniki, delovanje pa je nadomeščeno z obnašanjem. S tem se pokaže tudi, da *"odmiranje javnega ... spremlja radikalno ogrožanje zasebnega"* (Arendt, 1958/1995, str. 62). Brisanje javnega prostora se z razvojem marketinških tehnik, predvsem odnosov z javnostmi (ang. *public relations*), le še nadaljuje, saj te z načrtnim poseganjem v proces javnega mnenja zasebne interese omejene skupine posameznikov - ali podjetij - z manipulacijo spreminjajo v 'javni interes'. Če se je v 18.

¹³ Značilno je, da s tem v zvezi Habermas pravi: *"Nasploh se množični mediji priporočajo kot naslovniki za osebne stike in težave, kot avtoritete življenjske pomoči,.."*, ter *"problematico zasebne eksistence javnost delno vsrka, če je že ne razrešujejo pod vrhovnim nadzorom publicistične javnosti, jo pred njo vsaj prikazujejo"* (Habermas, 1962/1989, str. 191). Zanimivo je, da se je leta 2004 na Internetu zelo razmahnilo pisanje t. i. spletnih dnevnikov - blogov (izraz *blog* izhaja iz angleških besed *web* in *log*), v katerih posamezniki javno pišejo (oziroma objavljajo na spletni strani) svoj dnevnik. Posamezniki torej "na očeh javnosti" javno razgrinjajo svoja najbolj skrita razmišljanja, osebne probleme itd.

stoletju javnost razvijala iz jedra same zasebne sfere, danes oglaševalci javnost vzpostavljajo z 'napadom' na zasebni, intimni prostor posameznika. Oglaševanje (ki postaja čedalje bolj usmerjeno) in ustvarjanje javnosti ter medijsko poseganje v zasebno sfero pod krinko t. i. "interesa javnosti," pa kaže, da se zasebna sfera še naprej oži; v končni fazi celo intimno postaja čedalje bolj javno. Zasebnost postaja moteča ovira, ki onemogoča učinkovitost. Agre in Rotenberg pravita, da postaja *"izdelek, ki ogroža učinkovitost in skriva kriminalce.... naravni sovražnik svobode informacij ... koncept brez definicije in oblike ... [katerega] uveljavljanje je nadležno in drago"*, (Davies, 2001, str. 153 v Kovačič, 2006, str. 17 - 18).

3.3 Omejevanje zasebne sfere

Na ožjenje zasebne sfere ne vplivajo samo zunanji (družbeni) vplivi; včasih postane ožjenje zasebne sfere oziroma njeno izpostavljanje javnosti zavestna taktika podrejenih skupin. Kot je pokazal Habermas, je mogoče s prevajanjem konfliktov iz zasebne sfere na javno, politično področje (Habermas, 1962/1989, str. 160) zasebne konflikte spremeniti v politične konflikte in s tem lažje doseči njihovo rešitev.

Omenili smo že, da je za varstvo zasebnosti pomemben kriterij »izolacija«. Varuje »notranji prostor«, kot področje človekovega umikanja in je zato treba preprečiti ravnanja, kot je katalogiziranje in registriranje celotne osebnosti, ne glede na to v kakšni obliki poteka, pa naj bo tako ravnanje podano z državnimi prisilnimi ukrepi ali anonimno. Taka ravnanja se ne glede na dejanska ravnanja (vdor, prisluškovanje in podobno) štejejo kot psihični pritisk na človeka. Poudarek je na vprašanjih upravno - tehničnih ravnanj, ki vodijo v depersonalizacijo. V taka ravnanja štejemo tudi snemanja pogovorov na trakove, kajti vsak lahko le sam dovoli snemanje in njegovo reprodukcijo. Varovana je človekova svoboda komuniciranja, zaupnost osebnih pogovorov, njihovo zapiranje navzven. Podobno velja za tajnost zdravstvenih kartotek, ki ne smejo biti dostopne javnim organom in tretjim, ter spolno življenje, (Šinkovec, 1997, str. 178).

Pri varovanju zasebnosti ločujemo dve stopnji: nedotakljivo bistvo osebnosti in širšo zasebno sfero. Tu prihaja do izraza teorija o sferah. Ožja sfera se nanaša na bistvo, ko je poudarjeno dostojanstvo človeka, ki mu omogoča ohranjanje, razvijanje in regeneracijo njegovih posebnosti, brez neželjenih zunanjih vplivov. Obstaja »notranji prostor«, ki ga poseduje posameznik, v katerega se lahko umakne in v katerega okolica ne more imeti dostopa, posameznik ima pravico, da ga drugi pustijo v miru in da tako uživa samoto. Absolutno nedotakljivo področje predstavlja najbolj intimna sfera osebnosti, ki nima nobenega razmerja z javnostjo ali pa ima z njim le malenkostno relacijo. Ni mogoče vpeljati orwelske vizije o totalnem nadzoru nad človekom. Nemško ustavno sodišče je poudarilo, da zasebna sfera ni avtomatično opuščena, če človekovo ravnanje posega v drugega človeka, kot je na primer družinsko življenje. Dopustnost posega v zasebno sfero je odvisna od tega, ali je socialno razmerje nekega ravnanja dovolj intenzivno. Kdaj je neko ravnanje dovolj intenzivno, je možno presojati le v konkretnem primeru ob upoštevanju vseh posebnosti, (Šinkovec, 1997, str. 178).

Širša zasebna sfera ne vključuje nedotakljivo področje človeka, v teh primerih so možni nekateri posegi državne oblasti. V bistvu se človek približuje socialni sferi. Zopet ponavljamo, da je poseg dopusten, če temelji na zakonu, ki je skladen z ustavo; za sprejem takega zakona mora biti izrecno ugotovljen javen interes in ukrep mora biti sorazmeren namenu zakona (ni dopusten ostrejši ukrep, če se da namen zakona doseči z blažjim). Vse bolj je poseg nedovoljen, kolikor bolj je prizadeta intimna sfera človeka, (Šinkovec, 1997, str. 178).

3.4 Pomen zasebne sfere

Človekovo dostojanstvo je bistveno. Človek ni »proizvod države«, pri človeku tudi ne moremo razpravljati kot o idealu, pač pa kot o bitju, k živi po lastnih zakonitostih in kot tak pripada posebni vrsti. Iz tega izhaja postulat svobode vsakega posameznika: biti povsem drugačen, zlasti v (duševnem) razvoju; imeti možnost samostojne odgovornosti in samostojnega mišljenja za ravnanje po lastni presoji in za vodenje življenja po lastni odločitvi. Ta svoboda ni neomejena, vsakemu človeku so dane omejitve v ravnanju in odločanju: spoštovati mora ustavni red in svojih pravic ne sme izkoriščati na škodo drugega. Uveljavijo se temeljna pravila možnih omejitev: javni interes skladen z ustavo; določenost v zakonu; sorazmernost ukrepa in sodno varstvo, (Šinkovec, 1997, str. 177).

Zasebna sfera se je v zgodovini iz sfere življenjske nujnosti premaknila na polje svobode. S tem zasebnost ni več nujno zlo, temveč je postala vrednota, predpogoj posameznikove svobode in emancipacije. Arendtova v zasebni sferi vidi območje, na katerem je posameznik varen in skrit pred svetom, in sicer na dva načina: pred vplivi iz sveta in pred tem, da posameznik postane viden v svetu. Arendtova namreč pravi, da so »...lastne štiri stene edini kraj, v katerega se lahko umaknemo pred svetom, ne samo pred tistim, kar se v njem stalno dogaja, temveč pred njegovo javnostjo, pred tem, da smo videni in slišani« (Arendt v Kovačič, 2006, str. 19). Zasebnost je torej meja med posameznikom in drugimi, meja, katere naloga je filtriranje pretoka informacij z obeh strani.

V čem je torej pomen te meje? Hannah Arendt v družini, torej v zasebni sferi, vidi prostor, ki omogoča nastanek in razvoj političnih oseb, od družbenih pritiskov neodvisnih posameznikov (Jalušič v Kovačič, 2006, str. 19). Tako Arendtova kot Habermas izpostavita dva vidika zasebnega: osebni prostor, torej prostor intime, in prostor, ki omogoča interesno združevanje, torej delovanje. Za delovanje, neodvisno od družbenih prisil, sta pomembna oba. Ta delitev pa je opazna tudi v pravni kodifikaciji pravice do zasebnosti, na primer v 8. Členu Evropske konvencije o človekovih pravicah, kjer je pravica do zasebnosti klasificirana na podlagi štirih vidikov pravice do zasebnosti: zasebnega življenja, družinskega življenja, doma in dopisovanja.

Zasebna sfera je torej pomembna zato, ker pravzaprav omogoča delovanje in kritično mišljenje: »da bi ljudje sploh lahko bili politična bitja in da bi se lahko zavedali pomena politike in obstoja javnega prostora, vsak posameznik... potrebuje... prostor, kamor se lahko

umakne. V tem prostoru, ki je svojevrstno varstvo pred družbenimi prisilami, se lahko razvije identiteta političnega patriarha« (v tem je element »varstva« pred totalitarizmom). To je prostor, ki lahko ... pomeni pogoj političnega... vsak lahko postane političen ravno zato, ker ni družben in ker ni izpostavljen nobeni družbeni prisili..." (Jalušič v Kovačič, 2006, str. 19).

Če se je torej zasebna sfera zožila na intimno in če je tudi intimno, ki ga Arendtova dojema kot »nekakšen beg pred družbo, ki se je polastila celotnega zunanjega sveta« (Arendt v Kovačič, 2006, str 20), čedalje bolj na udaru sodobne družbe, potem se lahko zgodi, da je edini zasebni prostor, ki ostane posamezniku, njegova subjektivnost. To pa, po Arendtovi, vodi v nekakšno razčlovečenje, deindividualizacijo posameznikov: »Čisto mogoče je, da se novi vek, ki se je začel z neverjetno obetavnim aktiviranjem človeških sposobnosti, konča z najbolj usodno, sterilno pasivnostjo, kar jih je kdaj poznala zgodovina« (Arendt v Kovačič, 2006, str. 20). Procesi čedalje obsežnejšega nadzorovanja in posledično povprečenja (konstrukcije povprečnega in ne več individualnega posameznika), pa zasebni prostor le še bolj ožijo. »Osiromašenje javnega prostora spremlja rast družbe nadzora in voajerizma«, pravi Seyla Benhabib, (Benhabib v Kovačič, 2006, str. 20 - 21).

4 PRAVICA DO ZASEBNOSTI

Pravica do zasebnosti ima svoj izvor v naravnem pravu in v človekovem dostojanstvu. Gre za pravico, ki je človeku prirojena in jo instinktivno čuti. Povprečen posameznik ne potrebuje nobenega pravnega znanja o tej pravici, da ve, da bo prizadet, če mu tajno sledijo, ga snemajo, razširjajo informacijo iz njegovega zasebnega življenja in podobno.

Posameznik kot družbeno bitje v vsakdanjem življenju vstopa v odnose z drugimi posamezniki, javnostjo in tudi državno oblastjo (Lampe, 2004, str. 40). Iz tega izhaja, da je njegova zasebnost omejena, še več, njegov interes po ohranitvi in nedotakljivosti njegove zasebnosti je omejen z interesi drugih posameznikov, javnosti in državne oblasti. Vedno, ko se sprašujemo, kdaj je interes drugih, da vdrejo v posameznikovo zasebnost, močnejši od interesa tistega v katerega zasebnost posegamo, si lahko predstavljamo tehtnico, ravnovesje na njej pa išče pravo.

Pravica do zasebnosti je opredeljena v različnih pravnih virih, tako slovenskih kot mednarodnih. Obravnavati jo moramo v t.i. dualističnem konceptu. Ne eni strani gre za osebnostno pravico, ki je varovana z instrumenti civilnega prava, na drugi strani pa za človekovo pravico javnopravnega značaja, ki je varovana z ustavo in mednarodnopravnimi dokumenti. Kako pa jo opredeljujejo ti viri pa več v nadaljevanju.

4.1 Splošni pogledi na pravico do zasebnosti

Pravica do zasebnosti je osebnostna pravica, ki pripada vsakemu človeku že s samim njegovim obstojem. Kot osebnostne pravice se štejejo tudi pravice, ki pripadajo človeku v socialnem odnosu z drugimi in kot take varujejo človekovo osebnost. Z razvojem človeštva se je razvijalo tudi varstvo njegovih pravic, kar dokazuje, da se krog pravic ne sme zapirati.

Pravico do zasebnosti pridobi vsakdo že ob rojstvu in jo čuti že po lastnem instinktu, kar pomeni, da posamezniku ni potrebno pravno znanje, da bi vedel, kdaj mu je ta pravica kršena. Te pravice ni mogoče uvrstiti v eno pravno področje, ampak jo je potrebno obravnavati multidisciplinarno, z vidika javnega in socialnega prava, pri čemer je sama pravica centralni pravni fenomen.

Človek je socialno bitje, zato je pomembno njegovo konstruktivno sodelovanje z drugimi, predvsem pa njegovo vključevanje v družbo. Dosego tega mu omogoča avtonomnost, katero doseže z zasebnostjo v kateri najde samega sebe. Zato ne gre samo za vrednoto posameznika, temveč za vrednoto, ki je pomembna za celotno družbo.

4.2 Klasifikacija pravice do zasebnosti

Pravica do zasebnosti varuje področje človekovega življenja, nad katerim bi imel posameznik izključno oblast odločitve, ali naj bo to področje izpostavljeno zunanjemu svetu ali ne. Seveda pa ima tudi ta »zunanji svet« pravico »minimalno« (!) poseči v njegovo zasebnost v določenih pogojih. Samo zasebnost, torej področje človekovega življenja, ki naj bi uživalo pravno varstvo, je moč razdeliti na štiri dokaj fleksibilna področja:

- duševno;
- prostorsko;
- odločitveno;
- informacijsko.

V okvir vsake od teh pa je z določenimi prepletanji moč uvrstiti štiri temeljne dobrine, ki posamezniku omogočajo svoboden razvoj njegove osebnosti z minimalnim vmešavanjem »zunanjega sveta«, ter zato uživajo pravno varstvo – zasebno življenje, družinsko življenje, dom in dopisovanje. Grobo pa je vseeno moč trditi, da (s kar precejšnjim odstopanjem, prepletanjem in dopolnjevanjem) posamezne dobrine, torej tisti temeljni aspekti pravice do zasebnosti sovpadajo z osnovnimi področji zasebnosti z osnovnimi področji zasebnosti - zasebno življenje v odločitveno zasebnost, družinsko življenje v duševno zasebnost, dom v prostorsko, ter dopisovanje v informacijsko zasebnost (torej dajanje in prejemanje informacij). Obratno bi lahko trdili, da omogoča prav pravno zagotovljeno spoštovanje nedotakljivosti zasebnega življenja posamezniku uživati odločitveno zasebnost, spoštovanje družinskega življenja omogoča uživanje duševne (emocionalne) zasebnosti, doma – nedotakljivost tistega makroprostora – torej širše prostorske zasebnosti, pravno zagotovljeno spoštovanje dopisovanja pa informacijske zasebnosti.

4.3 Razvojni temelji pravice do zasebnosti

Prva določba, ki naj bi bila povezana s človekovimi pravicami, je v literaturi omenjena Magna Charta Libertatum iz leta 1215 in naj bi ljudem dajala nove pravice.

Začetki zakonodaje, ki ščiti zasebnost, segajo že v leto 1361, ko je v Angliji zakon Justices of the Peace Act predvidel kazni za tiste, ki so skrivaj opazovali druge posameznike ali jim prisluškovali. Nekje okrog leta 1400 pa so tudi na Zahodu začeli bolj šifrirati vsebino občutljivih pisem. Leta 1466 ali 1467 je Leon Basista Alberti napisal enega najstarejših znanih zahodnih esejev o kriptanalizi (Kahn v Kovačič, 2006, str. 49), kar kaže na to, da je bilo varovanje komunikacijske zasebnosti problem, s katerim so se resno ukvarjali že vsaj od petnajstega stoletja naprej.

K razvoju osebnostnih pravic sta pripomogli dve določbi, Habeas Corpus Act, sprejeta v angleškem parlamentu leta 1679 in Bill of Rights, prav tako sprejeta v angleškem parlamentu leta 1689. Prva je neposredno razširila osebno svobodo, druga pa je z določenimi omejitvami

uveljavila svobodo govora. Ameriška Virginijska deklaracija o pravicah, ki je bila sprejeta leta 1776, je prvič določila osebnostne pravice na ravni ustave. V deklaraciji so zagotovljene pravice do življenja, svobode, lastnine ter osebnostne sreče in varnosti. Kot novost pa je bila določena tudi svoboda tiska, ki je ni moč omejiti. Od sprejetja leta 1789 dalje, je najbolj splošna francoska Deklaracija o pravicah človeka in državljana opredelila enakost in neodvisnost vseh ljudi, priznavala pa je tudi prirojene pravice. K razvoju osebnostnih pravic so prispevale revolucije v letu 1884, ki so v Nemčiji, Avstriji in Italiji z določbami na ustavni ravni prinesle tudi nekatere državljanske svoboščine. Čeprav so določbe po zatrtju revolucij razveljavili, pa pravic ljudem ni bilo moč odvzeti in tako so našle prostor tudi v novih ustavnih aktih (Bašić, 1996, str. 20 - 21).

Po 2. svetovni vojni je bila pozornost namenjena dokumentom za varovanje osnovnih človekovih pravic na mednarodnih nivojih. Najpomembnejši listini sta: Ustanovna listina združenih narodov (sprejeta 1945) in Mednarodni pakt o državljanskih in političnih pravicah iz leta 1966. Z Evropsko konvencijo o varstvu človekovih pravic in temeljnih svoboščin sprejeto 1950. leta, pa so bili prvič določeni ustrezni organi in postopki za varovanje človekovih pravic.

Prvi zakon za zaščito informacijske zasebnosti pa je bil sprejet leta 1970 v Nemčiji v zvezni državi Hesse. Razvoj sodobne pravice do zasebnosti se je začel predvsem v ZDA (tako glede regulacije zasebnosti komunikacij kot tudi zasebne avtonomije in testa upravičenega pričakovanja zasebnosti). Mednarodnopravne temelje varovanja zasebnosti v sodobnem času pa je postavila predvsem Splošna deklaracija človekovih pravic iz leta 1948 v 12. členu¹⁴ ter Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin v 8. členu¹⁵.

Ena izmed prvih omemb pravice do zasebnosti v ameriškem pravu je sicer Cooleyjeva definicija zasebnosti (v okviru odškodninskega prava - tort law) kot pravice biti sam iz leta 1880; prvič pa je bila zasebnost omenjena v razsodbi sodišča že leto za tem, leta 1881, v primeru DeMay proti Roberts¹⁶. Za Thomasa M. Cooleyja je bila to pravica do lastne osebnosti in

¹⁴ 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.

¹⁵ 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.

¹⁶ DeMay v. Roberts, 46 Mich. 160, 9 N. W. 146 (1881). Šlo je za tožbo ga. Roberts, ki je rojevala, proti zdravniku Dr. DeMayu, ki je prišel pomagat pri porodu. S seboj je vzel kot pomočnika mladega neporočenega moškega, ki je bil popolnoma nevešč v medicini in za ga. Roberts popoln neznanec. Dovolil mu je, da je ostal v hiši, čeprav je bilo očitno, da bo lahko slišal in videl vse, kar se bo dogajalo. Sodišče je razsodilo, da *"je imela tožnica v teh trenutkih zakonito pravico do zasebnosti v svojem stanovanju, in da ji pravo to pravico zagotavlja..... Dogodek je bil za tožnico svet in nihče ni imel pravice bili*

osebne imunitete (Wagner DeCew v Kovačič, 2006, str. 50), v njegovem razumevanju zasebnosti pa je podobno kot v ameriškem odškodninskem pravu močno opazno lastninsko koncipiranje zasebnosti. Tudi pravno varstvo posameznikove osebne sfere je imelo v prvotnem ameriškem odškodninskem pravu naravo premoženjskih oziroma lastninskih tožb (Lampe, 2004, str. 54 - 63), na kar kaže tudi ime najstarejšega delikta (ang. tort) ameriškega občega prava (ang. common law) - trespass; gre za protipravno vmešavanje v osebnost, lastnino ali pravico nekoga (Lampe, 2004, str. 55), izraz pa se povezuje predvsem z nezakonitim prečkanjem ali vstopom na tujo lastnino.

zraven, razen če je bil povabljen ali če je za to bila resnična in nujna potreba," je bilo zapisano v razsodbi (Turkington in Allen, 1999, str. 670).

5 PRAVICA DO ZASEBNOSTI V ZDA

5.1 Ustavni temelji pravice do zasebnosti v ZDA

Pravica do zasebnosti v ameriški ustavi ni nikjer izrecno navedena¹⁷, vendar pa je Vrhovno sodišče ZDA leta 1965 v primeru *Griswold proti Conencticut*¹⁸ priznalo obstoj ustavne pravice do zasebnosti. Pri tem se je izkazalo, da ameriška pravna praksa zasebnosti ne dojema zgolj pravico biti sam in kot pravice do komunikacijske zasebnosti, temveč jo povezuje tudi z avtonomijo posameznika, (Kovačič, 2006, str. 55).

Priznanje obstoja pravice do zasebnosti v ameriški ustavi je izzvalo številne kritike in polemike, med drugim tudi zato, ker je sodišče (iz)našlo pravico do zasebnosti v obliki »sence« (ang. penumbra), ki ni izrecno definirana, ampak je zagotovljena le v konceptu. Številne kritike pa so opozarjale, da ustavno priznanje pravice do zasebnosti pomeni vsiljevanje skrajne individualistične filozofije in moralnega relativizma (Sykes, 1999, str. 86).

Vrhovno sodišče je v posameznih odločitvah¹⁹ že pred primerom *Griswold proti Conencticut* posredno priznalo pravico do zasebnosti. Primer *Griswold proti Conencticut*²⁰ ki je bil podlaga za priznanje pravice do zasebnosti v ameriški ustavi, sta namreč sprožila izvršni in strokovni direktor združenja *Planet Parenthood League of Connecticut*, Estelle Griswold in Dr. C. Lee Buxton, ki sta bila zaradi nasveta o uporabi kontracepcije vsak posebej kaznovana z denarno kaznijo 100 dolarjev. Sodišče je ugotovilo, da gre v tem primeru za zakon, ki vpliva na intimno razmerje med možem in ženo, torej posega v njuno "zakonsko (poročno) zasebnost", in zato je zakon o prepovedi kontracepcije razveljavilo. V razsodbi so izrecno zapisali, da se "ukvarjamo s pravico do zasebnosti, ki je starejša kot Listina svoboščin,²¹ starejša kot naše politične stranke in starejša kot naš šolski sistem" (Turkington in Allen v Kovačič, 2006 str. 56).

Ustavnost pravice do zasebnosti je dodatno utemeljil še sodnik Goldberg v ločenem pritrdilnem mnenju. Po njegovem mnenju so sestavljavci ustave priznavali še obstoj drugih

¹⁷ V ustavah vsaj osmih zveznih držav je v nasprotju z zvezno ustavo pravica do zasebnosti izrecno navedena (Cate, 1997, str. 66).

¹⁸ *Griswold v. Conencticut*, 381 U.S. 479 (1965).

¹⁹ Leta 1958 je npr. zavrnilo poizkus države Alabama, da bi prisilila NAACP66 (združenje *National Association for the Advancement of Colored People*), naj razkrije seznam svojih članov. V odločitvi so izrecno poudarili, da prek "zasebnosti združevanja" (ang. *privacy in one's associations*) ščitijo svobodo združevanja (Sykes, 1999: 85). Leta 1960 so v primeru *Talley proti Kaliforniji* odpravili prepoved objave anonimnih pamfletov. Že pred tem so v nekaterih primerih (leta 1923 *Pierce proti Society of Sisters* v kateri so zavrnil zakone, ki so od otrok zahtevali obiskovanje javnih šol, ter leta 1925 *Meyer proti State v. Hunt*, 91 N.J. 338, 450 A.2d 952 (1982).

²⁰ *Griswold v. Conencticut*, 381 U.S. 479 (1965).

²¹ Listina svoboščin (*Bill of Rights*) je prvih deset amandmajev k ameriški ustavi. Sprejeti so bili v paketu leta 1791.

pravic, ki obstajajo ob pravicah, ki so zapisane v ustavi in ustavnih amandmajih. Dokaz za to je videl predvsem v devetem amandmaju²², ki določa, da naštevane pravic v ustavi ne sme biti tolmačeno tako, kot da drugih pravic ni, in pri tem izpostavi svoje strinjanje z ugotovitvijo sodišča, da je pravica do zasebnosti temeljna osebna pravica, (Turkington in Allen v Kovačič 2006, str. 56).

Fred H. Cate ameriško ustavno pravico do zasebnosti deli na štiri področja. Ta področja predstavljajo temelj za priznavanje obsega pravnega varstva zasebnosti v ZDA, hkrati pa tudi omejitve varovanja zasebnosti (predvsem v zvezi z informacijsko zasebnostjo). Prvo področje predstavljajo odločitve Vrhovnega sodišča ZDA, ki se navezujejo na svobodo izražanja, združevanja in religije. Drugo skupino odločitve Vrhovnega sodišča ZDA, ki se nanašajo na preiskavo in zaplenbo s strani državnih organov. Tretjo skupino pa predstavljajo odločitve Vrhovnega sodišča ZDA, ki zadevajo temeljne odločitve posameznika. V četrto skupino spadajo odločitve Vrhovnega sodišča ZDA v zvezi z nerazkritjem, (Cate, 1997, str. 52 – 65).

Ameriška ustava je zasnovana na predpostavki ščitenja posameznika pred državo, torej podeljuje t. i. negativne pravice, s katerimi določa, česa država ne sme storiti in s tem ustvarja prostor posameznikove svobode, je razumljiv razvoj varstva zasebnosti, ki ima za posledico širjenje avtonomije posameznika. Vendar pa ravno od tu in iz pravice do zasebnosti, ki je na nekaterih področjih še vedno lastninsko koncipirana, izvira tudi poglobljena pomanjkljivost varstva zasebnosti v ZDA, ki preprečuje učinkovito varovanje informacijske zasebnosti. Zakon o zasebnosti (ang. *Privacy Act*)²³ vsebuje omejitve pri razkrivanju osebnih podatkov, a te omejitve ne veljajo za Kongres in preiskovalne organe, pa tudi za druge vladne agencije ne, ko gre za njihovo t. i. rutinsko uporabo, ki v praksi lahko pomeni praktično katerokoli rabo, (Cate, 1997, str. 78).

Pravni okvir njenega varovanja informacijske zasebnosti predstavljata zakon o svobodi informacij (ang. *Freedom of Information Act* oziroma FOIA²⁴) ter zakon o zasebnosti²⁵, ki pa veljata samo za javni sektor. Zakon o zasebnosti prepoveduje razkritje posameznikovih osebnih podatkov, hkrati pa določa, da smejo vladne agencije zbirati samo nujne in relevantne osebne podatke, osebne podatke v največji možni meri zbirati neposredno od posameznika, skrbeti za točnost in popolnost ter zagotoviti administrativne in tehnične postopke za zaščito osebnih podatkov. Glavni problem varovanja informacijske zasebnosti

²² Amandma, Listina svoboščin (Bill of Rights), 1791.

²³ Privacy Act of 1974, 5 U.S.C. (1974).

²⁴ Poglavitni namen FOIA je zagotavljati nadzor javnosti nad delovanjem vlade. Zakon določa, da ima vsakdo pravico dostopa do kateregakoli zveznega dokumenta, razen v nekaterih primerih, med drugim je omejen dostop do "osebnih in medicinskih ali podobnih dosjejev, katerih razkritje bi pomenilo očiten nepooblaščen poseg v zasebnost posameznika" ter v primeru kazensko-preiskovalnih zadev, ko je "upravičeno pričakovati, da bi objava dokumentov povzročila nepooblaščen vdor v posameznikovo zasebnost" (US Department of Justice, 1996).

²⁵ Zakon o zasebnosti (Privacy Act of 1974, 5 U.S.C. (1974))

posameznikov v ZDA ne predstavlja javni ampak zasebni sektor, ki ni podvržen državni regulaciji ampak trgu, (Kovačič, 2006, str. 57).

Zato je v ZDA prostorska, komunikacijska in informacijska zasebnost zunaj doma in zunaj konteksta vladnega preiskovanja in zaplembe slabo varovana (Cate, 1997, str. 65), pravna ureditev teh področij pa nesistematična in včasih že kar dvolična. To je očitno predvsem pri problemu zasebnosti na delovnem mestu, pri regulaciji informacijske zasebnosti v zasebnem sektorju, pri regulaciji nezaželene elektronske pošte in pri spoštovanju zasebnosti s strani množičnih medijev. Poseben problem predstavlja vloga ameriške vlade in ameriških korporacij pri razvoju in upravljanju interneta, kajti na njem se močno pozna tudi ameriški pristop do varovanja zasebnosti, (Kovačič, 2006, str. 58).

5.2 Pravica do zasebnosti v ZDA na delovnem mestu

Delodajalci v ZDA večinoma nasprotujejo državni regulaciji zaščite zasebnosti na delovnem mestu in menijo, da zadostuje samoregulacija s strani podjetij. Podobno menijo podjetja tudi glede zaščite zasebnosti potrošnikov, čeprav je v 70. letih prejšnjega stoletja ameriški Kongres ustanovil *Federal Privacy Commission*, ta pa je v svoji raziskavi ugotovila, da je samoregulacija v zasebnem sektorju popolna napaka (Sykes, 1999, str. 142). Kljub temu tako zasebni sektor kot tudi Bela hiša še naprej vztrajata, da je samoregulacija povsem zadostna in da sprejem novih zakonov ni potreben (Laurant, 2003, str. 529).

Raziskava, ki jo je vodil David Linowes, je ugotovila, da delodajalci o zaposlenih zbirajo podatke v prevelikem obsegu ter ne zagotavljajo točnosti in zaupnosti podatkov. Pav tako zaposlenim niso niti omogočili, da bi napačne podatke lahko popravili. Raziskava je razkrila primere, ko so bili zaposleni odpuščeni ali pa jim je bilo onemogočeno napredovanje zaradi nepreverjenih govoric, (Sykes, 1999, str. 141 – 142).

V ZDA na delovnem mestu delodajalec od zaposlenih lahko zahteva oddajo telesnih tekočin (za preverjanje drog ali test nosečnosti). Do leta 1988, ko je bil sprejet *Employee Polygraph Protection Act*²⁶ ki tako početje prepoveduje, razen če delodajalec t. i. "upravičeno sumi", so lahko izvajali tudi poligrafsko testiranje zaposlenih (Sykes, 1999, str. 144). Hkrati zakon ne preprečuje delodajalcem, da bi zaposlene smeli spraševati tudi najbolj osebna vprašanja, (Kovačič, 2006, str. 59).

Če za državne organe velja, da ne smejo preiskovati in prisluškovati brez sodnega naloga, pa v ZDA to ne velja za delodajalca. V primeru *O'Connor proti Ortega*²⁷ je Vrhovno sodišče ZDA

²⁶ Employee Polygraph Protection Act of 1988, 29 U.S.C. (1988).

²⁷ O'Connor v. Ortega, 480 U.S. 709 (1987). V tem primeru je šlo za zdravnika, ki je bil na delovnem mestu že 17 let in je imel na svoji delovni mizi tudi osebne stvari, zaradi česar je sodišče sicer menilo, da uslužbenec v tem primeru upravičeno pričakuje zasebnost na delovnem mestu, vendar tudi v konkretnem primeru niso ugotovili, da bi bila preiskava neupravičena.

leta 1987 presodilo, da je preiskava vladnega uslužbenca upravičena, če je opravljena v povezavi z njegovim delom in ni pretirano vsiljiva (Turkington in Allen v Kovačič 2006, str. 59).

Po raziskavi American Management Association iz leta 2005 se je za podjetja v ZDA pokazalo:

- 76% podjetij nadzoruje uporabo spleta;
- 65% podjetij blokira dostop do določenih spletnih mest;
- 55% shranjuje in pregleduje elektronsko pošto;
- 50% pregleduje računalniške datoteke;
- 36% beleži tipkanje;
- 51% podjetij izvaja videonadzor;
- 51% podjetij beleži klicane telefonske številke in dolžino telefonskih pogovorov;
- 3% beleži vse telefonske pogovore (v izbranih poklicih 19%);
- 8% uporablja GPS sledenje službenih vozil;
- 8% podjetij uporablja GPS sledenje identifikacijskih kartic;
- 5% podjetij uporablja GPS sledenje mobilnim telefonom zaposlenih.

Podjetja iz ZDA pri tem kot razloge za izvajanje nadzora navajajo:

- potreba po podatkih za zdravstveno zavarovanje;
- preverjanje zaposlenih (background checks);
- večanje produktivnosti;
- preprečevanje zlorab;
- varnost;
- odnosi s strankami (npr. nadzor komuniciranja s strankami), itd..

Vendar je študija organizacije *The Privacy Foundation* z naslovom "The Extent of Systematic Monitoring of Employee E-mail and Internet Use" iz leta 2001 pokazala, da je glavni razlog za razmah nadzorovanja zaposlenih nizka cena nadzornih tehnologij.

Med »izgovori« podjetij pa lahko naštejemo:

- "Podjetje je lastnik delovne opreme, sam sebe lahko 'nadzoruješ'."
- "Če zaposleni opremo podjetja uporablja v zasebne namene, s tem oškoduje podjetje, saj mu krade delovni čas in sredstva."
- "Zaposleni je v službi zato, da dela."
- "Naše podjetje je zaskrbljeno zaradi 'internih groženj', potencialni osumljenci so vsi zaposleni."
- "Želimo se zaščititi pred krajo poslovnih skrivnosti."
- "Želimo se zaščititi pred odškodninskimi tožbami zaradi neprimerne ravnanja zaposlenih."

Organizacija ACLU ugotavlja, da se elektronsko nadzorovanje zaposlenih pogosto sprevrže v vohunjenje za zaposlenimi. V podkrepitev svojih ugotovitev navajajo različne primere nadzorovanja, npr. videonadzor v prostorih, ki so jih zaposleni uporabljali za preoblačenje. Po

njihovi oceni delodajalci na leto prisluškujejo 400 milijonom klicev zaposlenih itd, (ACLU, 2003).

Dejstvo je, da podjetja v ZDA svoje zaposlene čedalje bolj obravnavajo kot kos opreme (inventar) in ne kot samostojne posameznike. Prav tako so pogosti posegi v telesno zasebnost (urinski, krvni in genski testi) s strani delodajalca, ki ima nad zaposlenimi ekonomsko moč. S tem se odpirajo vprašanja človekovega dostojanstva in avtonomije na delovnem mestu. Medtem pa odločitve ameriških sodišč kažejo, da država početje delodajalcev legitimira in legalizira.

5.3 Varstvo informacijske zasebnosti v ZDA v zasebnem sektorju

Podobno stanje, kot velja na področju zasebnosti na delovnem mestu, v ZDA velja tudi na področju informacijske zasebnosti (in zasebnosti nasploh) v zasebnem sektorju, v katerem je še vedno zelo razširjen lastninski koncept pravice do zasebnosti. Ravno tako kot za delodajalca velja, da lahko posega v zasebnost svojih zaposlenih bistveno bolj, kot vlada lahko posega v zasebnost svojih državljanov (Sykes, 1999, str. 147), velja za upravljavce osebnih podatkov, da lahko osebne podatke posameznikov zbirajo skoraj brez vsakršnih omejitev. Načeloma namreč v ZDA na zvezni ravni za zasebni sektor ne veljajo skoraj nikakršne omejitve pri zbiranju in obdelavi osebnih podatkov, saj *Privacy Act* velja samo za javni sektor, (Kovačič, 2006, str. 63).

Problem je, ker v ameriški ustavi zasebnost ni omenjena kot pozitivna pravica, hkrati pa prvi amandma²⁸ govori o svobodi govora. Previsoka stopnja zaščite informacijske zasebnosti v zasebnem sektorju na ravni posamezne zvezne države bi namreč lahko bila v nasprotju s prvim amandmajem. To pomeni, da ameriški sistem že v samem temelju onemogoča izenačitev varstva informacijske zasebnosti v javnem in zasebnem sektorju, ki sicer velja v Evropi. Tudi odškodninsko pravo ne nudi zadostne zaščite informacijski zasebnosti. Restatement of The Law of Torts sicer priznava štiri škodljiva dejanja proti zasebnosti, vendar je njihova aplikacija na informacijsko zasebnost mogoča le v delnem obsegu, pa še v teh primerih posamezniki s tožbo redko uspejo, (Cate, 1997, str. 89 - 90).

Ko nekdo zbere osebne podatke, so ti njegova last in lahko z njimi počne praktično karkoli. To pomeni, da ni nikakršnih omejitev za njihovo nadaljnjo prodajo. Nekaj omejitev velja le za nekatere vrste osebnih podatkov, in sicer za finančne zapise, zdravstvene informacije, kreditna poročila, podatke o izposoji video kaset, kabelski TV, internetnih dejavnostih otrok, mlajših od 13 let, podatke o šolanju in izobrazbi, podatke o lastnikih motornih vozil ter podatke, ki jih uporablja telemarketing (Laurant, 2003, str. 526 – 527). Regulacija obdelave osebnih podatkov je v ZDA v najboljšem primeru podobna gašenju požara (razen podatkov o šolanju in izobrazbi in v zadnjem času tudi zdravstvenih podatkov), oziroma se ameriška

²⁸ 1. amandma, Listina svoboščin (Bill of Rights), 1791.

zakonodaja regulacije tega področja loteva izrazito kampanjsko, navadno kot reakcija na kak razvpit primer zlorabe, (Kovačič, 2006, str. 63).

Podobno je tudi na področju prisluškovanja elektronskim komunikacijam ter tajnem snemanju pogovorov. Prisluškovanje brez soglasja ali brez sodnega naloga je prepovedano, vendar le, če ga izvaja tretja oseba. ECPA101 iz leta 1986 namreč določa izjemo, da je razkritje vsebine komunikacij dovoljeno že, če se z razkritjem strinja ena stran (Cate, 1997, str. 84). Podobno je Vrhovno sodišče ZDA razsodilo, da je dovoljeno tajno snemanje pogovora, ki ga ima nekdo z drugo osebo, tudi brez sodnega naloga²⁹, (Kovačič, 2006, str. 64).

Podobno nekonsistentno stanje vlada tudi na področju zaščite osebnih podatkov. Ker se *Privacy Act* ne nanaša na transakcijske podatke, so ponudniki telekomunikacijskih storitev do leta 1996 lahko zbirali in obdelovali te osebne podatke brez omejitev. Leta 1996 pa je Kongres sprejel *Telecommunications Act*, ki je zaščito zasebnosti razširil tudi na transakcijske podatke vendar pa zakon v členu 551f ponudnikom storitev dovoljuje zbiranje teh podatkov, če je to potrebno, da zaščitijo svoj poslovni interes, (Kovačič, 2006, str. 64).

Vprašanje obdelave osebnih podatkov v zasebnem sektorju v ZDA torej ni predvsem vprašanje (informacijske) zasebnosti, temveč svobode trgovanja in svobode komercialnega govora. Namesto poseganja v pravice se postavlja zgolj vprašanje trgovanja med posameznikom in organizacijo, ki zbira osebne podatke. Posameznik ima načeloma sicer možnost, da svojih podatkov ne proda, toda v praksi te možnosti največkrat dejansko nima, če se ne želi izključiti iz družbe. Sistemska neregulacija tega področja v zasebnem sektorju s strani ZDA tako posameznike glede informacijske zasebnosti sili v položaj, ko se svoji informacijski zasebnosti odrekajo na videz prostovoljno, (Kovačič, 2006, str. 64).

5.4 Obdelava in izmenjava osebnih podatkov v ZDA – grožnje zasebnosti

Dodatno grožnjo informacijski zasebnosti predstavlja obdelava in nadaljnja uporaba zbranih osebnih podatkov, ki v ZDA za zasebni sektor ni regulirana. Razlogi za neregulacijo so gotovo ekonomski interesi t. i. trgovcev z zasebnostjo (ang. *privacy merchant*). Po nekaterih ocenah imajo tri podjetja, ki se ukvarjajo s kreditnimi poročili, Equifax, TRW in Trans Union Corporation, osebne podatke o 90 % odraslih Američanov (Etzioni, 1999, str. 128). Podjetje Abacus Alliance iz ZDA je leta 1997 združevalo podatke o nakupih potrošnikov, ki so tisto leto opravili več kot dve milijardi transakcij (Batagelj, 1997). Istega leta je podjetje Axiom posedovalo podatke o 196 milijonih Američanov, (Whitaker, 1999, str. 132).

²⁹ Odmeven primer se je zgodil leta 1998, ko je imel ameriški predsednik Bill Clinton razmerje s svojo pomočnico Monico Lewinsky, podatki o tem razmerju pa so prišli na dan tako, da je prijateljica Monice Lewinsky Linda Tripp snemala pogovor, v katerem se ji je Lewinskyjeva zaupala.

Po drugi strani pa neregulaciji tega področja precej botruje tudi miselnost, ki jo zelo dobro povzema liberalna kritika zasebnosti. Virginia Postrel tako pravi, da sta zbiranje in izmenjava informacij bistvena za svobodno družbo (Sykes, 1999, str. 229). Omejitev obdelave in izmenjave osebnih podatkov naj bi bila tako napad na svobodno novinarstvo, svobodno podjetništvo in svobodo komuniciranja, pri čemer ni mišljeno samo tržno komuniciranje, temveč tudi pravica, da se posamezniki učimo drug o drugem in širimo informacije. Vendar pa liberalci pozabljajo na razliko med medsosedskim opazovanjem ter zbiranjem podatkov v velikih brezosebnih zbirkah. Zakonska neregulacija tega področja v ZDA je privedla do tega, da je edino jamstvo za nerazkritje osebnih podatkov iz zbirk samo dobra volja in etika različnih nadzornih sistemov, pravna zaščita večinoma ni možna, mogoči so le neformalni pritiski javnosti, (Kovačič, 2006, str. 67).

Pri obdelavi osebnih podatkov so mogoče zlorabe iz več razlogov. Enega večjih problemov v zadnjem času povzroča t. i. *outsourcing* – oddaja del zunanjim podizvajalcem. Ameriška podjetja čedalje več del – predvsem razna manj zahtevna programerska dela, vnašanje podatkov ali prepisovanje po posnetem nareku (npr. ugotovitve zdravnika med pregledom pacienta) – 'izvažajo' v Indijo, Pakistan in podobne države, kjer je delovna sila dovolj izobražena, a bistveno cenejša kot v ZDA³⁰. Pri tem podjetja pogosto posredujejo v tujino občutljive podatke in pri tem se lahko zaplete, (Kovačič, 2006, str. 68).

Najnevarnejšo nevarnost pri prodaji osebnih podatkov pa predstavlja možnost, da te podatke od komercialnih posrednikov kupijo preiskovalni organi in tajne službe. Ker so bili predlogi, da bi FBI smel imeti neomejen dostop do vseh nacionalnih zbirk podatkov, oziroma predlogi o vzpostavitvi ene velike zbirke podatkov o vseh državljanih neuspešni (Whitaker, 1999, str. 131), se zastavlja vprašanje, ali neobstoj omejitev pri prodaji osebnih podatkov ne predstavlja možnosti, da se FBI omenjeni prepovedi izogne. Vprašanje so si številni strokovnjaki in aktivisti gibanja za zasebnost že večkrat zastavili (glej npr. Etzioni, 1999, str. 128, Whitaker, 1999, str. 132 ter Sykes, 1999, str. 60). David Banisar pa trdi, da se to že dogaja – FBI, DEA in IRS po njegovih trditvah skrivaj kupujejo komercialne zbirke podatkov in jih povezujejo s svojimi preiskovalnimi zbirkami, (Banisar v Sykes, 1999, str. 60).

Če velja, da zaradi obsega in narave zbranih podatkov ločnica med marketingom in vohunjenjem čedalje bolj izginja, povezovanje trgovcev z zbirkami podatkov s tajnimi službami in državnimi organi to ločnico še dodatno briše, (Kovačič 2006, 70). Pri tem je posebej zaskrbljujoča ugotovitev Davida Flahertyja, ki je zapisal, "*moj vtis je, da si javni sektor ni mogel privoščiti takšne programske opreme in sredstev za povezovanje osebnih*

³⁰ Leta 2003 je tako Lubna Baloch, prepisovalka iz Indije, zagrozila, da bo na internetu objavila medicinske kartoteke, če ji ameriško podjetje, ki ji je delo posredovalo, ne bo plačalo obljubljenih 3 cente na vrstico (pozneje se je izkazalo, da si je delo posredovalo več zunanjih izvajalcev, prvi zunanji izvajalec pa naj bi dobil 18 centov na vrstico). Ker so v medicinskih kartotekah pogosto tudi drugi občutljivi podatki, npr. številke bančnih računov, številke kreditnih kartic, številka zdravstvenega zavarovanja (SSN) itd., in ker ob morebitni zlorabi zunaj ZDA posamezniki nimajo na voljo pravnih sredstev za ukrepanje, je to vsekakor resen problem, (Zetter, 2004a).

podatkov, kakršne upravljajo v neposrednem trženju (posebej vZDA)”, (Flaherty, 2001, str. 187).

Najpomembnejše ali bolj zanimivo vprašanje je zakaj je pri zaščiti informacijske zasebnosti v ZDA prišlo do takšnih pomanjkljivosti? Odgovor leži v ostankih lastninskega koncipiranja pravice do zasebnosti ter v liberalni ideologiji, ki zbiranje in obdelavo osebnih podatkov vidi zgolj kot izmenjavo informacij, kot problem svobode trgovanja, ne pa kot problem poseganja v zasebnost posameznika. Problem je tudi ameriška ustava, ki posameznikom podeljuje negativne pravice, zaradi česar informacijska zasebnost v zasebnem sektorju ostaja večinoma neregulirana. Nekateri vidijo pri vprašanju informacijske zasebnosti celo poskus ameriške države, da bi ustregla korporacijam, pa četudi so pri tem omejene pravice posameznikov³¹, (Kovačič, 2006, str. 70).

³¹ Ustanovitelj organizacije Junkbusters Jason Cattler se sprašuje: “*Zakaj za distribucijo korporacijske programske opreme brez dovoljenja uporabljamo izraz 'piratstvo', za distribucijo osebnih podatkov posameznikov brez dovoljenja pa izraz 'razdeljevanje' (ang. sharing)?*”, (The Pew Internet & American Life Project, 2000, str. 11).

6 PRAVICA DO ZASEBNOSTI V EVROPI

Za razliko od ZDA je v večini evropskih držav zasebnost ustavna kategorija. Države, ki zasebnosti nimajo omenjene v ustavi, so Avstrija, Francija, Norveška in San Marino. Vendar pa imajo v Avstriji poseben zakon o varstvu osebnih podatkov, katerega del ima ustavni status, v Franciji in na Norveškem pa je ustavno sodišče presodilo, da je pravica do zasebnosti v ustavi omenjena implicitno. Velika Britanija, ki nima pisne ustave, je leta 1998 zaradi skladnosti z *Evropsko konvencijo o človekovih pravicah*³², ki so jo sprejele praktično vse evropske države, sprejela *Human Rights Act*³³, v katerem je omenjena tudi pravica do zasebnosti. Evropske države, članice Sveta Evrope, razen San Marina, so sprejele tudi *Konvencijo o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov*³⁴. To pomeni, da imajo večinoma tudi poseben zakon o varstvu osebnih podatkov in vzpostavljen nadzorni organ, ki bdi nad varstvom informacijske zasebnosti. Prav tako je pomembna razlika med Evropo in ZDA v tem da se v Evropi vzpostavljajo tudi enotna merila tako za javni kot za zasebni sektor, (Kovačič, 2006, str. 71).

V Evropi je večina držav podpisala in ratificirala mednarodne akte, ki urejajo varstvo zasebnosti. Najpomembnejši med njimi so *Splošna deklaracija človekovih pravic*³⁵, *Mednarodni pakt o državljanskih in političnih pravicah*³⁶ ter *Evropska konvencija o varstvu človekovih pravic in mednarodnih svoboščin*³⁷. *Splošna deklaracija človekovih pravic* v 12.

³² Svet Evrope (1950), Evropska konvencija o varstvu človekovih pravic in mednarodnih svoboščin, spremenjena s protokoli št. 3, 5 in 8 ter dopolnjena s protokolom št. 2, ter njeni protokoli št. 1, 4, 6, 7, 9, 10 in 11 (Convention on Human Rights and Fundamental Freedoms as amended by Protocols Nos. 3, 5 and 8 and amended by Protocol No. 2 and its Protocols Nos. 1, 4, 6, 7, 9, 10 and 11), sprejel jo je Svet Evrope leta 1950. Uradni list RS, št. 33/1994, "Mednarodne pogodbe", št. 7/1994, 13.6.1994. Konvencijo je državni zbor Republike Slovenije ratificiral 13. 6. 1994. Veljati je začela dne 28. 6. 1994.

³³ Human Rights Act, 1998, Velika Britanija.

³⁴ 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.

³⁵ Generalna skupščina Združenih narodov (1948), Splošna deklaracija o človekovih pravicah (Universal Declaration of Human rights), 10.12.1948.

³⁶ OZN (1966), Mednarodni pakt o državljanskih in političnih pravicah (International Covenant on Civil and Political Rights), sprejeta v OZN leta 1966. Uradni list SFRJ, št. 7/1971. Pakt je ratificiral Zvezni zbor skupščine SFRJ 30. 1. 1971. Veljati je začel 12. 2. 1971.

³⁷ Svet Evrope (1950), Evropska konvencija o varstvu človekovih pravic in mednarodnih svoboščin, spremenjena s protokoli št. 3, 5 in 8 ter dopolnjena s protokolom št. 2, ter njeni protokoli št. 1, 4, 6, 7, 9, 10 in 11 (Convention on Human Rights and Fundamental Freedoms as amended by Protocols Nos. 3, 5 and 8 and amended by Protocol No. 2 and its Protocols Nos. 1, 4, 6, 7, 9, 10 and 11), sprejel jo je Svet Evrope leta 1950. Uradni list RS, št. 33/1994, "Mednarodne pogodbe", št. 7/1994,

členu določa, da se *"nikogar 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 takim vmešavanjem ali takimi napadi."* Enako se glasi tudi dikcija 17. člena *Mednarodnega pakta o državljanskih in političnih pravicah. Evropska konvencija o varstvu človekovih pravic in mednarodnih svoboščin* (EKČP), ki velja za najpomembnejši dokument s področja varovanja človekovih pravic in temeljnih svoboščin v Evropi, v 8. členu pravi, da ima vsakdo pravico do spoštovanja svojega zasebnega in družinskega življenja, doma in dopisovanja; posegi v to pravico so možni samo, če je tako določeno z zakonom in nujno v demokratični družbi zaradi državne ali javne varnosti ali ekonomske blaginje države, da se prepreči nered ali zločin, zavaruje zdravje ali morala ali da se zavarujejo pravice in svoboščine drugih ljudi, (Kovačič 2006, str. 72 - 74).

6.1 Varstvo informacijske zasebnosti v Evropi

V ZDA se je pravica do zasebnosti sprva oblikovala ob sodni praksi, pozneje pa so sprejeli zakone, ki so v posameznih sektorjih urejali varstvo zasebnosti (t. i. sektorski pristop). Sicer je bil zakon, ki ureja varstvo osebnih podatkov, v ZDA sprejet že leta 1977, vendar velja le za javni sektor. V Evropi pa so ubrali povsem drugačen pristop, saj je prvi zakon za zaščito informacijske zasebnosti na svetu, ki je bil sprejet leta 1970 v Nemčiji (v zvezni državi Hesse), postavil enotna merila za javni in zasebni sektor, (Kovačič, 2006, str. 74).

Razlogi za sprejem take zakonodaje so bile obsežne družbene reforme, do katerih je v Evropi prišlo po drugi svetovni vojni. Evropske države so začele čedalje bolj postajati države blaginje in to je prineslo s seboj potrebo po pregledu in načrtovanju, vse skupaj pa veliko potrebo po zbiranju in analizi čedalje več podatkov. Zato so v sedemdesetih letih 20. stoletja v Evropi nastali načrti za centralizacijo, povezovanje in nastanek velikih zbirk podatkov. Take načrte so imeli že leta 1960 na Švedskem in leta 1970 v nemški zvezni državi Hesse. Zaradi negativnih izkušenj iz obdobja druge svetovne vojne je bil odpor proti tem načrtom razumljiv, a se je zakonodaja v začetku ukvarjala predvsem z računalniško obdelavo podatkov. Problem ni bil posameznik in njegove pravice, temveč podatki in uporaba računalniške tehnologije, (Kovačič, 2006, str. 74). Toda razvoj tehnologije se je obrnil v drugo smer. Leta 1963 je DEC je razvil prvi miniračunalnik PDP-1 (Digital Equipment Corporation, 1963), ki je bil precej razširjen po univerzah, leta 1975 pa je nastal prvi poceni (stal je 397 dolarjev) miniračunalnik Altair, ki so ga v ZDA prodajali v trgovinah na drobno, zaradi česar je postal široko dostopen, (Delaney v Kovačič, 2006, str. 74).

Z razvojem mikroprocesorskih tehnologij uporaba velikih računalniških sistemov ni bila več ekonomsko upravičena. Nastanek množice majhnih, poceni, a zmogljivih računalnikov je

13. 6. 1994. Konvencijo je državni zbor Republike Slovenije ratificiral 13. 6. 1994. Veljati je začela dne 28.6.1994.

razpravo o zaščiti informacijske zasebnosti obrnil v povsem drugo smer, saj je bilo novo, razpršeno tehnologijo veliko težje nadzirati kot omejeno število kompleksnih in dragih sistemov. Zaradi nove tehnologije so se v Evropi odločili, da je treba zaščitno zakonodajo razširiti tudi na zasebni sektor, z majhnimi podjetji vred, (Mayer-Schönberger, 2001, str. 225).

Poleg tega so v drugi fazi razvoja informacijske zasebnosti v ospredje stopile pravice posameznika ali, kot pravi Mayer-Schönberger, "*zaščita podatkov kot poskus regulacije tehnologije se je spremenila v individualno svoboščino posameznikov*", (Mayer-Schönberger, 2001, str. 227). Počasi je postajalo jasno, da niso podatki tisti, ki potrebujejo zaščito, temveč da zaščito potrebuje posameznik. Zato so uvedli nekatere nove pravice. Zbiranje podatkov je bilo mogoče le na podlagi zakona ali soglasja posameznika vendar je posameznik moral biti obveščen o namenu zbiranja, imeli so pravico zahtevati spremembo ali celo izbris netočnih podatkov. Hkrati so se pojavili tudi posebni pooblaščenca, katerih naloga je bila skrbeti za izvajanje te zakonodaje, informacijska zasebnost pa je postala ustavna kategorija v Avstriji, Španiji in na Portugalskem, (Mayer-Schönberger, 2001, str. 226 – 227).

Obenem je prišlo še do enega premika. V 60. in 70. letih 20. stoletja je bila informacijska zasebnost problem večinoma znotraj nacionalnih držav. V 80. letih in pozneje pa je zaradi razvoja in povečane dostopnosti tehnologije informacijska zasebnost postala izrazito mednarodni izziv, (Bennett, 2001, str. 103). Zato je *Organizacija za ekonomsko sodelovanje in razvoj* (OECD) 23. septembra 1980 sprejela *Smernice za zaščito zasebnosti in čezmejni pretok osebnih podatkov*³⁸. V *Smernicah* je izrecno navedeno, da veljajo tako za javni kot za zasebni sektor, uveljavljajo pa načela za pošteno in zakonito ravnanje z osebnimi podatki. Ta so bila pozneje povzeta tudi v drugih mednarodnih dokumentih.

Leto dni pozneje je Svet Evrope sprejel enega najpomembnejših dokumentov s področja varovanja informacijske zasebnosti – *konvencijo o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov*. Konvencija, ki je bila pripravljena na podlagi *Smernic OECD*, je jasno izpostavila povezavo med varstvom osebnih podatkov in zaščito zasebnosti posameznika ter problematičnost tehnologije (avtomatska obdelava osebnih podatkov), hkrati pa je določila pravila za zbiranje in obdelavo osebnih podatkov ter izenačila zbirke osebnih podatkov v javnem in zasebnem sektorju. Konvencija določa, da se smejo osebni podatki uporabljati in shranjevati samo za zakonite namene in pošteno; zbirati se smejo samo podatki, ki so ustrezni in skladni z dosegom namena, za katerega se zbirajo; prepovedano je čezmerno zbiranje osebnih podatkov; upravljavec zbirke osebnih podatkov pa mora zagotoviti njihovo točnost in posodobljenost in jih ne sme hraniti dlje, kot je nujno potrebno za doseg namena, zaradi katerega se zbirajo. Konvencija zahteva tudi obstoj ukrepov, ki bodo zagotovili, da bodo osebni podatki shranjeni za določene in zakonite namene in da se bodo obdelovali le podatki, ki so primerni, ustrezni in niso pretirani glede na namen zbiranja, (Čebulj, 2002, str. 411). Poleg tega konvencija daje posameznikom pravico

³⁸ OECD (1980), Smernice za zaščito zasebnosti in čezmejni pretok osebnih podatkov (The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data), sprejete 23. septembra 1980.

do seznaitve z obstojem in vsebino osebnih podatkov, ki jih zadevajo, ob morebitnih napakah pa pravico zahtevati popravek ali izbris osebnih podatkov, (Kovačič, 2006, str. 76).

Toda razvoj zaščite informacijske zasebnosti v Evropi se še ni ustavil. Naslednji pomemben mejnik je rzsodba nemškega ustavnega sodišča iz leta 1983, ki je izpostavila načelo informacijskega samo odločanja, sodišče pa je tudi poudarilo, da mora država pojasniti, zakaj potrebuje podatke in kakšne so posledice zavrnitve oddaje osebnih podatkov, (Mayer-Schönberger, 2001, str. 229).

Kljub ustavni zaščiti posameznikove zasebnosti, pa v poslovnem svetu prihaja do pojavov, ko podjetja posameznikom vsiljujejo podpis soglasja za nadaljnjo obdelavo in uporabo osebnih podatkov. Izoblikovala se je poslovna politika, ko že v pogodbah najdemo soglasja za omenjeno prakso katera se pa veže na pridobitev storitev s strani podjetja. Delna rešitev se kaže v absolutno zaščiteni informacijski zasebnosti, kateri se kljub podpisom pogodbe ni mogoče odreči. Na podlagi direktiv EU se hkrati tudi širijo pristojnosti in pooblastila neodvisnosti pooblaščenecv za varstvo osebnih podatkov. V prihodnosti pa bo verjetno najbolj občutljivo področje, s katerim se bodo ukvarjale evropske države, tehtanje med pravico do zasebnosti in pravico do dostopa do informacij javnega značaja.

6.2 Vpliv direktiv EU na varstvo informacijske zasebnosti v Evropi

Konvencija Sveta Evrope je prvi resnejši poskus poenotenja nacionalnih standardov za zaščito informacijske zasebnosti, v praksi pa je naletela na nekaj težav. Ena večjih odsotnosti definicije je, kaj je ustrezna stopnja zaščite osebnih podatkov, (Cate, 1997, str. 35). Ta problem je skušala rešiti Evropska unija s svojimi direktivami. Namen direktiv EU o zasebnosti je harmonizacija oziroma uskladitev zakonodajnega varstva zasebnosti v vseh državah članicah. Leta 1995 je EU sprejela *Direktivo o zaščiti osebnih podatkov* 95/46/EC³⁹. Prvi osnutek direktive je bil pripravljen že leta 1990, vendar je predvideval drugačno obravnavo osebnih podatkov v javnem in zasebnem sektorju. Leta 1992 pa je evropski parlament sprejel dopolnilo, s katerim je osebne podatke v javnem in zasebnem sektorju izenačil, direktiva pa je bila dokončno sprejeta leta 1995, (Kovačič, 2006, str. 78).

Pomen direktive je sicer tudi v tem, da je jasno izpostavila povezavo med zaščito osebnih podatkov in temeljnimi pravicami in svoboščinami posameznika. Vendar je po drugi strani iz direktive jasno razvidna želja zagotoviti neoviran pretok osebnih podatkov med državami, saj druga točka prvega člena jasno določa, da "*države članice ne smejo omejevati ali*

³⁹ Direktiva 95/46/EC o varstvu posameznikov pri obdelovanju osebnih podatkov in svobodnem pretoku teh podatkov (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data), sprejeta 24. oktobra 1995. Official Journal L 281, 23.11.1995 str. 31 - 50.

prepovedati prostega pretoka osebnih podatkov med državami članicami zaradi razlogov'' zaščite zasebnosti (2. točka 1. člena direktive 95/46/EC). Ta direktiva ima nekaj pomembnih določil, med drugim se ne nanaša samo na živeče posameznike, dovolj široko definira obdelavo osebnih podatkov, posebno pozornost namenja obdelavi občutljivih osebnih podatkov, predvsem pa v 28. členu zahteva ustanovitev neodvisnega nadzornega organa, ki skrbi za spoštovanje zakonodaje za zaščito zasebnosti. V Sloveniji ima to nalogo *Informacijski pooblaščenec* oziroma državni nadzorniki za varstvo osebnih podatkov v okviru tega organa, drugod po Evropi to delo opravljajo specializirane agencije, pooblaščenci ali posebni ombusmani, ki morajo imeti določeno stopnjo pooblastil. Ta obsegajo predvsem dolžnost vlade, da se s tem organom posvetuje v vseh primerih, ki zadevajo spremembo zakonodaje s področja zasebnosti. Nadzorni organ pa ima pravico do vseh informacij, ki so relevantne za njegove preiskave, lahko prepove obdelavo osebnih podatkov ali uniči nezakonito vzpostavljeno zbirko osebnih podatkov, sprejema in obravnava pritožbe ter pripravlja redna poročila. S tem je EU vzpostavila celovit pravni okvir varovanja informacijske zasebnosti, posledica pa je tudi vzpostavitev opazovanja področja, (Kovačič, 2006, str. 79 - 80).

6.3 Pretok osebnih podatkov iz Evropske unije v ZDA

Iz bojazni, da bi omejitve pretoka osebnih podatkov utegnile škodovati ameriškemu gospodarstvu, so ZDA Evropski uniji predlagale poseben sporazum *Safe Harbor Agreement*. Ta predvideva, da se bodo ameriška podjetja prostovoljno odločila spoštovati načela o zaščiti zasebnosti, ki sta jih pripravila ameriško trgovinsko ministrstvo ter uprava za interni trg Evropske komisije. Tako overjena podjetja bi lahko prejemale osebne podatke iz Evropske unije, (Laurant, 2003, str. 17).

Uporaba Safe Harbor načel v praksi pomeni, da je organizacija, ki želi prenesti osebne podatke v tretjo državo, najprej zavezana nacionalni zakonodaji, da zagotovi, da se podatki obdelujejo pravično in zakonito; organizacija iz Slovenije, ki želi prenesti osebne podatke v tretje države je tako najprej zavezana načelom ZVOP-1, v katerem so implementirane zahteve Direktive 95/46/EC, in pred prenosom podatkov v tretje države potrebuje odločbo o ustrezni ravni varstva osebnih podatkov s strani tretje države, ki jo izda državni nadzorni organ (v tem primeru Informacijski pooblaščenec). V primeru iznosa podatkov v ZDA se po odločbi Evropske Komisije 2000/520/ES zavezanost organizacije načelom Safe Harbor šteje kot zagotovilo, da organizacija ustrezno varuje osebne podatke. Organizacija iz ZDA se za pridobitev ugodnosti varnega pristana samocertificira pri Ministrstvu za trgovino ZDA, kar pomeni, da se zaveže k spoštovanju načel varnega pristana in to tudi javno razglasi v svojih politikah varnosti podatkov.

Načela varnega pristana določajo, da mora organizacija posameznike obvestiti o namenu zbiranja in uporabe njihovih podatkov. Prav tako mora posameznikom ponuditi možnost izbire o tem, ali se bodo njihovi osebni podatki razkrili tretji stranki ali se bodo uporabili za namen, ki je različen od tistega, s katerim so bili zbrani. Prenos podatkov tretjim osebam je tako

možen samo ob upoštevanju zgornjih dveh načel. Zavezanost načelom varnega pristana tako načeloma ščiti osebne podatke, prenesene v ZDA pred nepooblaščno uporabo in določa pod kakšnimi pogoji sme organizacija iz ZDA posredovati osebne podatke tretji osebi.

Da organizacija pokaže, da spoštuje načela varnega pristana, mora izvajanje načel preverjati ali s samoocenjevanjem ali zunanjim pregledom. Pri samoocenjevanju mora tako preverjanje pokazati, da je objavljena politika organizacije glede zasebnosti osebnih podatkov, prejetih iz EU, točna, celovita, prikazana na vidnem mestu, v celoti izvedena in dostopna. Pokazati mora tudi, da je njena politika zasebnosti v skladu z načeli varnega pristana. Organizacije morajo voditi evidenco o svojem izvajanju prakse zasebnosti varnega pristana in jo v primeru preiskave ali pritožbe zaradi neskladnosti izročiti neodvisnemu organu, ki je pristojen za preiskavo pritožb, ali agenciji, ki je pristojna za obravnavo nepoštenih in goljufivih praks. Organizacija je ob nespoštovanju načel, h katerim se zaveže, podvržena zakonskim pooblastilom pristojnih organov v ZDA, ki so pooblaščen za preiskave pritožb v primeru nepoštenih praks (Federal Trade Commission ali Ministrstvo za promet ZDA). Nacionalnim nadzornim telesom v državah članicah (torej tudi Informacijskemu pooblaščenču v Sloveniji) pa daje 3. člen Odločbe Komisije 2000/520/ES pooblastilo, da ob ugotovitvi pristojnega organa iz ZDA ali pri utemeljeni podlagi, ki kaže na to, da se kršijo določila varnega pristana, prekinijo prenos podatkov v organizacijo iz ZDA, tako da naslovijo zahtevo po prenehanju prenosa podatkov na organizacijo, ki izvaža podatke. Prekinitev preneha takoj, ko je ugotovljeno, da organizacija iz ZDA zopet spoštuje načela varnega pristana.

Sporazum je bil kljub številnim kritikam julija 2000 sprejet, novembra istega leta pa so ameriškim podjetjem že začeli izdajati certifikate (Laurant, 2003, str. 17). Kritiki so izpostavljali predvsem to, da sporazum predvideva samo-certificiranje, saj je t. i. "*status safe harbor*" podeljen že s tem, ko se podjetje obveže, da bo spoštovalo načela o zaščiti zasebnosti. Problematična je torej samoregulacija in odsotnost zagotavljanja izpolnjevanja in sistematičnega pregleda izvajanja sprejetih obveznosti (Laurant, 2003, str. 18). Čeprav je evalvacijsko poročilo o uspešnosti sporazuma pokazalo, da je sporazum uspešen, pa kot kaže vprašanje pretoka osebnih podatkov med EU in ZDA še ni dokončno rešeno. Dodatno se je namreč zaostriло z zahtevo ZDA po sporočanju podatkov o letalskih potnikih v ZDA, delno pa tudi z zahtevo ZDA po uvedbi biometričnih potnih listov, (Kovačič, 2006, str. 79 - 80).

6.4 Pravica do zasebnosti v EU na delovnem mestu

Pri vprašanju zasebnosti na delovnem mestu v praksi pogosto naletimo na argumentacijo delodajalcev, češ, zaposleni uporablja opremo podjetja, v službi je plačan za opravljanje svojega dela, kako torej lahko na delovnem mestu pričakuje zasebnost? Če je delodajalec lastnik komunikacijske opreme (telefona, računalnika) in delovnega časa zaposlenega – ali torej nima pravice preveriti ali zaposleni dela, ali pa morda "zapravlja" čas podjetja oziroma morda celo krade poslovne skrivnosti?

V Evropi se je uveljavil t.i. "evropski" pristop, ki zaposlenega na delovnem mestu ne vidi samo kot delavca, pač pa tudi kot človeško bitje, ki ima kot tak tudi določene pravice. Hkrati se pojavlja še vprašanje pravic tretjih oseb (z nadzorom komunikacij zaposlenega nadzorujemo tudi komunikacije njegovih zunanjih komunikacijskih partnerjev). Pomembno je tudi vprašanje sorazmernosti (se pravi kolikšen obseg nadzora je sprejemljiv in še opravičljiv oziroma ali zaželenega cilja ni mogoče doseči z blažjimi sredstvi), saj je po eni strani jasno, da ima zaposleni tudi na delovnem mestu interes za čim večjo zasebnostjo, po drugi strani pa je nesporen tudi interes delodajalca po racionalni rabi službenih sredstev in delovnega časa.

V zvezi z nadzorom na delovnem mestu sta verjetno najpomembnejši odločitvi *Evropskega sodišča za človekove pravice Halford proti Združenemu kraljestvu* (*Halford v. Velika Britanija*, odločba z dne 25. 6. 1997⁴⁰) iz leta 1997 ter *Copland proti Združenemu kraljestvu* (*Copland v. Velika Britanija*, odločba z dne 3. 4. 2007), iz leta 2007. *Evropsko sodišče za človekove pravice* je v vseh navedenih primerih presodilo, da varstvo zasebnosti velja tako za telefonske komunikacije, kot tudi za elektronsko pošto in uporabo interneta, in da je iz stališča varstva zasebnosti nepomembno ali gre za zasebno ali za službeno komunikacijsko sredstvo. Prav tako so presodili, da kršitev predstavlja že samo zbiranje in obdelava prometnih podatkov in s tem potrdili, da so prometni podatki integralni element komunikacij. Kršitev zasebnosti torej ni "le" vpogled v vsebino komunikacij, pač pa tudi vpogled v prometne podatke.

Evropski pristop k varovanju komunikacijske zasebnosti se kaže tudi v nekaterih drugih primerih. *Evropsko sodišče za človekove pravice* je leta 1998 v primeru *Lambert proti Franciji* (*Lambert v. Francija*, odločba z dne 24. 8. 1998) jasno poudarilo, da glede tajnosti komunikacij ni razlike med lastnim telefonskim priključkom ali telefonskim priključkom tretje osebe, istega leta pa v primeru *Kopp proti Švici* (*Kopp v. Švica*, odločba z dne 25. 3. 1998) tudi, da so zaščiteni tudi klici iz poslovnih prostorov ter v poslovne prostore.

Zanimiva je tudi razsodba (in predvsem njena utemeljitev) *Kasacijskega sodišča Francije* v primeru *Societe Nikon France, SA v. Onof* št. 99–42.942 iz leta 2001 (*Societe Nikon France v. M. Onof, Cass. soc., 2. oktober 2001, Bull Civ. V, No. 291*)⁴¹.

⁴⁰ Ga. *Halford*, uslužbenka policije, je proti svojemu delodajalcu leta 1990 sprožila postopek zaradi diskriminacije na delovnem mestu. V svoji pisarni je imela dva telefona, od katerih je bil eden namenjen za zasebno uporabo, glede uporabe telefonov pa ji niso bile naložene nikakršne omejitve. *Halfordova* je kasneje ugotovila, da je njen delodajalec nadzoroval telefonske klice iz njenega službenega telefona (pa tudi domačega telefona) in sicer z namenom, da bi zbrali gradivo za svojo obrambo v postopku zaradi diskriminacije. Zadeva je prišla na *Evropsko sodišče za človekove pravice*, ki je presodilo, da je v tem primeru šlo za kršitev 8. Člena EKČP. V razsodbi je izrecno zapisalo, da zaposleni na delovnem mestu upravičeno pričakuje zasebnost.

⁴¹ Delodajalec je preiskal računalnik zaposlenega, zaradi suma, da le-ta krši konkurenčno prepoved. V okviru preiskave je delodajalec pregledal in prekopiral dve mapi na računalniku zaposlenega (označeni z imenom "osebno" in "fax"), pri čemer so ugotovili, da je zaposleni uporabljal računalnik za neslužbene namene in kršil konkurenčno prepoved, čeprav je bilo to z notranjimi pravili organizacije

Omenjeni primeri kažejo, da evropska pravna ureditev na delovnem mestu zaposlenemu priznava bistveno širši krog komunikacijske zasebnosti kot ameriška pravna ureditev, hkrati pa tudi prepoveduje pretirano omejevanje komunikacij z drugimi. Glede nadzora komunikacij na delovnem mestu tako velja, da mora biti zaposleni vnaprej seznanjen s pravili delodajalca glede uporabe telefona, elektronske pošte in interneta, hkrati pa si delodajalec ne more privoščiti pretiranega omejevanja pravice do zasebnosti in pravice do komunikacije z zunanjim svetom. Praviloma tudi velja, da se mora zaposleni z nadzorom strinjati oziroma mora biti nadzor objektivno opravičljiv in sorazmeren. Glede strinjanja velja poudariti, da je zaposleni nasproti delodajalcu seveda v podrejenem položaju, zato mora biti strinjanje prostovoljno in brez prisile.

Pomembno je še dejstvo, da nadzor s strani delodajalca lahko predstavlja tudi kršitev interesa t.i. tretjih oseb, torej oseb, ki komunicirajo z zaposlenim in morda niti ne vedo, da gre za službeno komunikacijsko sredstvo ter da delodajalec nadzoruje komunikacije zaposlenega, s katerim so v stiku (Klemenčič, 2001, str. 188 – 189). Ta problem je zelo očiten pri morebitnem nadzorovanju službenih mobilnih telefonov, kjer je možnosti za razlikovanje med službenim in zasebnim komunikacijskim sredstvom še manj.

6.5 Komunikacijska zasebnost v Evropi

Pravico do komunikacijske zasebnosti najdemo na področju mednarodnega prava, zlasti v 8. členu EKČP, katere razlaga je podkrepljena z bogato sodno prakso ESČP in v 17. členu MPDPP, ki ima komunikacijsko zasebnost urejeno skupaj s splošno opredelitvijo varstva zasebnosti. Napredek v smeri varstva zasebnosti komunikacij pa je pokazala tudi Evropska unija (EU), ki je leta 1997 sprejela Direktivo o zasebnosti telekomunikacij (97/66/EC)⁴², leta 2002 pa Direktivo o zasebnosti in elektronskih komunikacijah, 2002/58/EC⁴³, ki sta nekoliko natančneje opredelili varstvo zasebnosti na področju telekomunikacij in elektronskih komunikacij.

prepovedano. Na podlagi tega so ga odpustili. Zaposleni se je pritožil, in *Kasacijsko sodišče Francije* je presodilo, da ima delavec tudi med delovnim časom in na delovnem mestu pravico do zasebnosti in tajnosti komunikacij. Pri tem so izrecno zapisali, da: "*delodajalec, ki bere sporočila, ki jih zaposleni pošilja ali sprejema preko službenega računalnika, krši temeljne pravice delavca, kot jih določa 8. člen Evropske konvencije o človekovih pravicah ... To velja ne glede na to, ali je bil delavec vnaprej seznanjen, da službenega računalnika ne sme uporabljati v neslužbene namene... Podjetje ali druge ustanove ne smejo biti mesta, kjer bi delodajalci arbitrarno in brez omejitev izvajali svoje diskrecijske pravice; ne smejo postati okolja totalnega nadzora, kjer temeljne človekove pravice nimajo veljave ... Menimo, da je splošna popolna prepoved uporabe e-pošte v neslužbene namene nerealna in krši pravno načelo sorazmernosti*" (Klemenčič, 2002, str. 402).

⁴² Direktiva 97/66/EC o obdelavi osebnih podatkov in varstvu zasebnosti v telekomunikacijskem sektorju, sprejeta 15.12.1997.

⁴³ Direktiva 2002/58/EC o obdelovanju osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij, sprejeta 12.7.2002.

8. člen EKČP priznava tajnost pisem in drugih občil, kar pa se lahko razlaga zelo široko, torej kot telefonske komunikacije, elektronska pošte, sporočila sms idr., saj oblika in vsebina sporazumevanja nista pomembna. Kljub temu imajo v nekaterih državah še težave s prilagajanjem zakonodaje razvoju tehnologije. Seveda pa pravica do komunikacijske zasebnosti ni absolutna, saj je Evropsko sodišče za človekove pravice v primeru *Klaas in drugi proti Nemčiji* leta 1978 zapisalo, da je tajni nadzor telekomunikacij nujno potreben element zagotavljanja nacionalne varnosti (Klemenčič, 2002, str. 398). Seveda je za to potrebna sodna odredba oziroma zakonska podlaga, vendar je ta v primeru tajnih služb lahko precej široka. V Nemčiji npr. tajna služba Bundesnachrichtendienst (BND) po razsodbi nemškega ustavnega sodišča iz leta 1999 sme prisluškovati mednarodnim komunikacijam avtomatsko in brez sodnega naloga v primerih preprečevanja terorizma in nezakonite trgovine z orožjem in drogami, (Laurant, 2003, str. 249). Pri vprašanju, ali so zaščiteni samo komunikacijska sredstva, ki so v lasti posameznika, ali tudi druga sredstva, pa je sodišče leta 1998 v primeru *Lambert proti Franciji* jasno poudarilo, da ni razlike med lastnim telefonskim priključkom ali telefonskim priključkom tretje osebe. Istega leta pa v primeru *Kopp proti Švici* poudarilo, da so prav tako zaščiteni klici iz poslovnih prostorov ter v poslovne prostore. Prav tako so pred posegi delodajalca zaščiteni tudi komunikacijska sredstva, ki jih na delovnem mestu uporablja zaposleni, (Kovačič, 2006, str. 81).

Pomembno novost predstavlja tudi razumevanje terminalske opreme uporabnikov kot dela zasebne sfere, s čimer direktiva uporabnikovi terminalski opremi daje status zasebnega prostora, v katerem lahko posameznik upravičeno pričakuje zasebnost. Iz direktive je viden tudi t.i. evropski pristop pri varovanju informacijske zasebnosti. Direktiva namreč določa, da obdelovanje osebnih podatkov, ki jih zbere ponudnik javno dostopne elektronske komunikacijske storitve za namene trženja brez soglasja uporabnika, ni dovoljeno, ponudniki storitev pa morajo uporabnike vedno obvestiti o tem, katere podatke obdelujejo, s kakšnim namenom in kakšen je čas shranjevanja teh informacij, (Kovačič, 2006, str. 82).

Pomemben korak predstavlja tudi odnos do osebnih podatkov, ki se zbirajo in so objavljeni v javno dostopnih imenikih. Direktiva, ki sicer govori o imenikih naročnikov na elektronske komunikacijske storitve, je očitno pisana z mislijo na javne telefonske imenike, kljub temu pa je definicija dovolj široko zastavljena, da je mogoče kot javni imenik razumeti ne samo telefonski imenik, temveč tudi imenik elektronske pošte ali pa morda imenik drugih osebnih podatkov, (Kovačič, 2006, str. 83).

Precej kritik so bila deležna določila o obsegu zbiranja in obveznem shranjevanju prometnih podatkov. Pri tem ne gre za problem varstva in zaupnosti teh podatkov, temveč za načelno vprašanje zapisovanja osebnih podatkov ljudi, ki niso ničesar osumljeni, ob dejstvu, da je mogoče te podatke pozneje uporabiti tudi v morebitnem postopku proti njim. Novembra 1996 je bila v evropskem uradnem listu objavljena Resolucija o zakonitem prestrezanju telekomunikacij. V njej je zapisano, da je »z zakonom podprto prestrezanje telekomunikacij pomembno orodje za zaščito nacionalnega interesa, nacionalne varnosti in preiskovanje resnih kaznivih dejanj«. Podana pa je tudi zbirka podrobnih zahtev, ki jih bodo morala

izpolnjevati telekomunikacijska podjetja. Izstopa predvsem to, da resolucija od telekomunikacijskih podjetij zahteva zbiranje velikega števila podatkov, med drugim tudi podatke o lokaciji uporabnika mobilnega telefona (Council Resolution v Kovačič 2006, str. 83).

Direktiva o zasebnosti in elektronskih komunikacijah iz leta 2002 pa je v 15. členu državam članicam že omogočila shranjevanje prometnih podatkov za določen čas. Na podlagi tega člena so imele države članice EU možnost operaterjem mobilne telefonije predpisati rok obveznega shranjevanja prometnih podatkov. Sprejemanje Direktive o obvezni hrambi prometnih podatkov so spremljali številni protesti in zapleti, saj sta direktivi nasprotovala tako posebna Alvarova komisija, ki je predlog zavrnila (Alvaro v Kovačič 2006, str. 84), kot tudi Evropski parlament. Kljub temu je bila Direktiva o obvezni hrambi prometnih podatkov decembra 2005 sprejeta, aprila 2006 pa tudi objavljena v uradnem listu EU. Če je bilo v prejšnjih direktivah shranjevanje prometnih podatkov prepovedano, oziroma dovoljeno le kot izjema, pa je direktiva 2006/24/ES to pravilo povsem obrnila na glavo. Zahteva namreč obvezno hrambo prometnih podatkov, telefonskih in internetnih komunikacij ter podatkov o lokacijah mobilnih telefonov, čas hrambe pa traja od 6 do 24 mesecev (Kovačič, 2006, str. 84). Že iz direktive 2002/58/EC je bilo moč razbrati tudi poizkus monopolizacije nadzornih sistemov s strani držav in omejevanje predvsem tistega nadzora, ki ga izvajajo zasebna podjetja. Direktiva je namreč vključevala ukrepe za zavarovanje telekomunikacijskih omrežij ter zagotavljanje tajnosti komunikacij. Ti ukrepi večinoma zadevajo zasebni sektor, saj je za izvajanje takega nadzora potrebno soglasje posameznika. Po drugi strani pa je od operaterjev telekomunikacij v primeru zakonitega prestrezanja komunikacij zahtevala zbiranje in shranjevanje podatkov na lastne stroške. To pomeni, da se stroški zakonitega prestrezanja komunikacij prenašajo na zasebne operaterje. Vprašanje stroškov hrambe prometnih podatkov je bilo pomembno vprašanje tudi pri sprejemanju Direktive o obvezni hrambi prometnih podatkov, na koncu pa je obveljalo, da povračilo stroškov operaterjem, nastalih zaradi obvezne hrambe prometnih podatkov, ureja vsaka država po svoji presoji, (Kovačič, 2006, str. 85).

6.6 Boj za pravico do zasebnosti

Zaradi težavnosti definicije zasebnosti in hitrega tehnološkega razvoja je predvsem v ZDA opaziti številne pomanjkljivosti in nedoslednosti pri zakonodajni zaščiti zasebnosti (Agre, 2001, str. 6); še težje pa je z usklajevanjem mednarodnega varstva zasebnosti.

Ker je zasebnost pravica, in to pogosto pravica posameznika nasproti državi, se z zasebnostjo ukvarjajo tudi nevladne in aktivistične organizacije. Vprašanje zasebnosti je bilo resno politično vprašanje v 70. letih 20. stoletja (Davies, 2001, str. 148). Takrat se je v Evropi dvignilo močno gibanje proti popisu prebivalstva, ki je bilo najmočnejše na Nizozemskem. Iz tega gibanja se je v poznih osemdesetih letih oblikovala organizacija *Privacy Alert* (*Stichting Waakzaamheid Persoonregistratie*), ki je za dvajset let postala največja nevladna

organizacija za varstvo zasebnosti v svetovnem merilu. Vendar pa je leta 1994 organizacija nehala delovati, in to ravno v času, ko je Nizozemska začela uvajati schengenski sistem nadzora meja, osebne izkaznice in identifikacijske številke za prebivalstvo (Davies, 2001, str. 154).

V svetu se je pojavilo gibanje, ki je večinoma neinstitucionalizirano (gre bolj za mrežo posameznikov, ki med seboj komunicirajo po internetu) in se aktivira le občasno, ob kriznih dogodkih, ki ogrožajo zasebnost; zato se zdi, da gibanje zamira. Razlogi za to so številni, izpostaviti pa je treba nekaj dejstev:

- zasebnost ni več resno politično vprašanje, saj se praviloma ne pojavlja v volilnih programih političnih strank, poleg tega v razmerju zasebnost proti varnosti po 11. septembru 2001 prevladuje strah pred terorizmom;
- drugi razlog je verjetno tudi institucionalizacija varstva zasebnosti. Evropske države pa tudi nekatere druge, ki sprejemajo evropski model (npr. Kanada), so uvedle posebne pooblaščenke oziroma varuhe pravic zasebnosti, ki se s področjem varstva zasebnosti ukvarjajo profesionalno, prav tako se z varstvom zasebnosti na določenem segmentu ukvarjajo profesionalno tudi strokovnjaki za informacijsko varnost;
- verjetno največji problem pa je odnos posameznikov do zasebnosti.

Danes se aktivisti gibanja za elektronsko zasebnost ukvarjajo predvsem s tistimi vprašanji varstva zasebnosti, ki niso institucionalizirana, torej s področji zlorab, ki jih ne preganjajo državni organi in s problemi informacijske varnosti ter z nevarnostmi, ki jih prinašajo nove tehnologije. Ukvarjajo pa se tako s spremembami zakonodaje kot s spremljanjem nevarnosti, ki jih prinašajo nove tehnologije. Zato se čedalje bolj ukvarjajo tudi s problemi zasebnosti na internetu. Ključna točka boja za zasebnost na internetu oziroma boja za komunikacijsko zasebnost na splošno pa je boj za svobodno uporabo kriptografije. Pravzaprav se je problem zasebnosti na internetu vzpostavil ravno ob vprašanju kriptografije⁴⁴. Dileme, ki so se ob tem zastavile, pa so povzročile nastanek gibanja za elektronsko zasebnost. (Kovačič, 2006, str. 89 - 90)

⁴⁴ Kriptografija (grško *kryptós* - *skrit* in *gráphein* - *pisati*, ali kriptologija (grško *logos* - *vedenje*)) je znanstvena veda o tajnem, nerazumljivem pisanju sporočil in njihovem prebiranju, ko je poznan spremembni postopek ter z odkrivanjem metod za razkrivanje šifiranih sporočil (dekripcija). To sta tudi dve glavni veji kriptografije: kriptozашčita in kriptanaliza.

7 ZASEBNOST OSEBNIH PODATKOV

7.1 Mednarodnopravni vidiki

V razmerju posameznika nasproti državi, kjer lahko prihaja do vdora v pravico do zasebnosti posameznika glede avtomatske obdelave osebnih podatkov, je moč zaslediti tri vrste razmerij:

1. zbiranje podatkov,
2. hranjenje podatkov
3. razpolaganje s podatki (dostop upravičenca do podatkov in razkrinkanje podatkov).

Pravna vprašanja glede zbiranja, hranjenja osebnih podatkov in razpolaganja z njimi so danes med najzahtevnejšimi in občutljivimi področji posameznikovega položaja znotraj državnega aparata. Posameznikova pravica do zasebnosti je v zvezi z avtomatsko obdelavo njegovih osebnih podatkov zelo izpostavljena.

Na pomen posameznikove zasebnosti ter varstva njegovih podatkov pred zlorabami je opozorila že OZN. Generalni tajnik je v poročilih leta 1973 in 1974 opozoril na varstvo osebnih podatkov iz dveh različnih naslovov. Leta 1973 je v poročilu »*Respect fo the Privacy of Individuals*«⁴⁵ svaril med drugim pred elektronskim prisluškovanjem, vohunjenjem, psihološkimi raziskavami. Leta 1974 pa v poročilu »O človekovih pravicah v znanstvenem in tehničnem razvoju«⁴⁶ (*Human Rights and Scientific and Technological Development*) Generalni tajnik OZN opozarja na človekove pravice tudi v informacijski družbi. Priporoča regulacijo varstva podatkov in seveda njihovo spoštovanje s strani državne oblasti v temeljnih treh načelih:

- zbirajo se naj le tisti podatki, ki so potrebni izključno za doseg določenega cilja, za katerega se podatki morajo zbirati;
- posameznik mora biti obveščen o podatkih, ki se zbirajo;
- za zbiranje podatkov je načeloma potrebno soglasje upravičenca.

Eden prvih takšnih mednarodno uveljavljenih instrumentov so bile smernice OECD⁴⁵, ki so jih članice sprejele prav z namenom, da bi bile zakonodaje (vsaj na evropski ravni) med seboj poenotene, hkrati pa tudi v pomoč državam, ki ustrezne zakonodaje še niso sprejele. Smernice, poznane kot OECD principi vsebujejo načela:

- omejitev zbiranja podatkov;
- kvaliteto podatkov;
- natančno določitev namena zbiranja podatkov;
- omejitev uporabe podatkov;

⁴⁵ OECD - Organisation for Economic Co-operation and Development: Organizacija za ekonomsko sodelovanje in razvoj; članice so principe sprejele 23.9.1980. Sprejetje principov je narekovala potreba po zaščiti zasebnosti v zvezi z osebnimi podatki zaradi naglega razvoja avtomatskega procesiranja podatkov ter prenosa podatkov izven meja držav in kontinentov; principi so neodvisni od tehnologije.

- zagotovitev varnosti podatkov;
- odprtost;
- individualno participacijo;
- odgovornost.

V sprejetem dokumentu je zapisano, da mora biti zbiranje podatkov zakonito in pošteno ter z vednostjo in pristankom osebe na katero se podatki nanašajo. Osebni podatki morajo biti relevantni za namen uporabe, natančni, celoviti ter aktualni. Namen oziroma cilj zbiranja podatkov mora biti natančno določen v času zbiranja podatkov, omejiti je potrebno tudi kasnejše spreminjanje namena. Osebni podatki ne smejo biti razkriti ali kako drugače uporabljeni, kot je bilo to določeno z namenom zbiranja. Biti morajo v soglasju z osebo na katero se podatki nanašajo ali pa mora biti namen zbiranja določen z zakonom. Zagotovljena mora biti zaščita pred izgubo podatkov, neavtoriziranim dostopom, uničenjem, nepravilno rabo, predelavo ali razkritjem podatkov. Princip odprtosti zahteva, da morajo biti na razpolago podatki o zbirkah ki se vodijo, naravi osebnih podatkov, namenu uporabe ter upravljavcu (kontrolorju) podatkov. Posameznik mora imeti pravico do informacije ali se o njem zbirajo podatki in kateri. Zadnji princip pa navaja odgovornost upravljavcev (kontrolorjev) podatkov, da upoštevajo prej navedene principe. Kmalu po sprejetju teh smernic, je podobne smernice sprejel leta 1981 tudi Svet Evrope s Konvencijo o zaščiti posameznika s poudarkom na avtomatski obdelavi osebnih podatkov ter leta 1995 še Evropska unija v znani direktivi o zaščiti podatkov (95/46/ES), (Praprotnik, 2006, str. 13 – 14).

Osnovni principi, ki jih najdemo v skoraj vseh smernicah ter zakonodajah so:

- doseči poštenost in zakonitost;
 - informacije uporabljati samo za namen, ki je bil prvotno določen;
 - točnost, pomembnost in ne prekomernost glede na določen namen;
 - natančnost in časovna omejenost;
 - podatke uničiti, ko je namen izpolnjen,
- (Dodig-Crnkovič, Horniak, 2005, str. 4).

Septembra 2005 so na svetovnem kongresu neodvisnih državnih organov s področja varstva osebnih podatkov v mestu Montreux v Švici prišli do podobnih ugotovitev in smernic. V svoji deklaraciji so izrazili ugotovitev, da gre razvoj informacijskih znanosti v smeri globalizacije informacijske izmenjave in uporabe naprednih vsiljivih tehnologij pri obdelavi podatkov ob hkratnem naraščanju groženj glede nadzora posameznikov.

Iz različnih mednarodnih instrumentov kot so principi OECD, principi konvencije Sveta Evrope, direktive Evropske unije 95/46/ES in drugih, so izpeljali naslednje principe:

- princip zakonitega in poštenega zbiranja in obdelovanja podatkov;
- princip točnosti, natančnosti podatkov;
- princip določitve namena in omejitve;
- princip proporcionalnosti;
- princip transparentnosti;
- princip individualne participacije in zagotovitve pravice dostopa do podatkov;

- posamezniku na katerega se podatki nanašajo;
- princip ne-diskriminacije;
- princip tajnosti podatkov;
- princip odgovornosti;
- princip neodvisnega nadzora in zakonitega sankcioniranja;
- princip o primerni stopnji zaščite v primeru preko mejnega prenosa osebnih podatkov.

Združene narode so pozvali, da pripravijo učinkovito zakonsko osnovo, kjer bo jasno definirana pravica do zaščite podatkov ter zasebnosti kot izterljiva človekova pravica. Vse države sveta pa pozivajo, da sprejmejo zakonodaje o zaščiti podatkov in zasebnosti, ki bodo v soglasju z osnovnimi principi.

(Deklaracija o zaščiti osebnih podatkov in zasebnosti v globaliziranem svetu: splošna pravica upoštevanja različnosti, 2005, str. 1 - 3)

7.2 Ameriško pravo

V ZDA ni veljavnega zveznega zakona kateri bi neposredno varoval osebne podatke ampak imajo veliko število statutov. Pomemben je zvezni zakon splošne narave »*Privacy Act*« ki regulira upravljanje podatkov, vsebovanih v državnem sistemu. Temeljno načelo, po katerem naj bodo podatki zbrani, uporabljeni, preneseni ter hranjeni, je načelo »*fair informational practice*«. Načelo »poštenega ravnanja s podatki« zahteva da državni organi, ki razpolagajo s podatki:

- varujejo osebne informacije/podatke pred javnostjo;
- sprejemajo vsa razumne mere preverjanja/ugotavljanja resničnosti (*to verify*) in ažuriranja podatkov;
- pod zakonskimi pogoji dovolijo posameznikom dostop do njihovih osebnih podatkov;
- odgovorni za ravnanje s podatki morajo dobiti ustrezno dovoljenje (posameznika ali sodišča) za pridobitev podatkov, za katere niso upravičeni (*unauthorized*).

Ta načela - »*fair informational practice*« - naj bi predstavljala splošno ravnotežje med potrebami državne oblasti ter posameznika po ohranitvi tajnosti njegovih osebnih podatkov. V ZDA je področje varstva osebnih podatkov moč uvrstiti v upravno-administrativno pravo. V tej luči je ustanovljeno posebno upravno telo, »Komisija«, sam nadzor zakona pred njo pa poteka po pravilih upravnega postopka. V poročilu »*Privacy Protection Commission*« leta 1977 se je Komisija zavzela za tri cilje s svojem delovanju:

- minimalizirati kršitev zasebnosti;
- povečati preglednost pri regulaciji varovanja podatkov;
- vzpostaviti zaupanje javnosti.

Poleg tega je Komisija izpostavila načelo za vzpostavitev razumevanja problematike varstva osebnih podatkov ter vzpostavitve ravnovesja med interesi posameznika po ohranitvi tajnosti

podatkov ter interesi javnosti oziroma državne oblasti do njihovega dostopa, hranjenja, uporabe itd. - »*fair informational practice*«.

Statuti ZDA posegajo na vsa mogoča področja družbenega življenja v zvezi z zbiranjem, hranjenjem in uporabo osebnih podatkov. To dejstvo kaže na tisto kritičnost zasebnosti posameznika v družbi ter na drugi strani interesov javnosti in državne oblasti po kontroli posameznikovih osebnih podatkov. Tipična regulacija, je »*Video Privacy Protection Act*« iz leta 1994. Zakon poleg dostopa določenih filmov v izposojevalnicah regulira tudi razpolaganje s podatki o strankah. Razpolaganje z osebnimi podatki določa tudi pomemben »*Telecommunications Act*« iz leta 1996, ki regulira dostop državne oblasti do podatkov, vodenih s strani zasebni telekomunikacijskih podjetij. Podatke posameznikov, vodenih v izobraževalnih institucijah, regulira »*Family Educational Rights and Privacy Act*«, sprejet leta 1986. Zasebnost podatkov v pravosodju ter kazenskih evidencah pa je podvržen regulaciji večkrat noveliranega »*Crime Control Act*« iz leta 1973. »*Right to Financial Privacy Act*« iz leta 1978 ter starejši, že omenjeni »*Privacy Act*« iz leta 1974, pa regulirata vodenje baz podatkov državne oblasti ter shranjevanje baz podatkov finančnih institucij, (Lampe, n.d., str. 143 - 144).

7.3 Evropsko pravo

24.10.1995 je Evropska unija sprejela osnovno direktivo za zaščito podatkov znano pod imenom DPD 95/46/ES, ki se nanaša na vsakršno obdelovanje osebnih podatkov ne glede na tehnologijo. Tako zapadejo pod to direktivo tudi osebni podatki, ki se pojavljajo na internetu. V svojem sedemnajstem členu direktiva nalaga upravljavcem zbirk podatkov implementacijo primerne tehnične podpore za zagotovitev osebnih podatkov, še posebej v mrežnih transakcijah.

Cilj direktive DPD 95/46/ES je zaščititi pravice in svoboščine posameznikov glede na obdelavo osebnih podatkov z določitvijo vodilnih načel, ki določajo zakonitost obdelave. Ta načela zadevajo:

- **kakovost** podatkov: osebni podatki morajo biti pošteno in zakonito obdelani ter zbrani za določene, izrecne in zakonite namene. Biti morajo točni in po potrebi ažurirani;
- **zakonitost** obdelave podatkov: osebni podatki se lahko obdelujejo samo, če je posameznik, na katerega se podatki nanašajo, nedvoumno dal svojo privolitev ali če je obdelava potrebna:
 - za izvajanje pogodbe, katere stranka je zadevni posameznik ali;
 - za skladnost z zakonsko obveznostjo, ki velja za upravljavca ali;
 - za varstvo življenjskih interesov zadevnega posameznika ali;
 - za izvajanje naloge, ki se opravlja v javnem interesu ali;
 - zaradi zakonitih interesov, za katere si prizadeva upravljavec;

- posebne **vrste** obdelave: prepovedana mora biti obdelava osebnih podatkov, ki kažejo na rasni ali etnični izvor, politično prepričanje, verska ali filozofska prepričanja, pripadnost sindikatu ter obdelava podatkov v zvezi z zdravjem ali spolnim življenjem. Ta določba se ne uporablja, kadar je na primer obdelava podatkov potrebna za varstvo življenjskih interesov posameznika, ali za potrebe preventivne medicine in zdravstvenih diagnoz;
- **informacije** o posameznikih, na katere se nanaša obdelava: upravljavec mora posamezniku, na katerega se osebni podatki nanašajo, zagotoviti določeno število informacij (istovetnost upravljavca, nameni obdelave podatkov, prejemniki podatkov itd.);
- **pravica do dostopa do podatkov** posameznika, na katerega se nanašajo osebni podatki: vsakemu posamezniku, na katerega se nanašajo osebni podatki, je zajamčena pravica, da pridobi od upravljavca:
 - potrditev tega, ali se podatki v zvezi z njim obdelujejo ali ne, ter podatke, ki so predmet obdelave;
 - popravek, izbris ali blokiranje podatkov, katerih obdelava ni v skladu z določbami te direktive, predvsem zaradi nepopolnih ali netočnih podatkov, ter obvestilo tretjim strankam, ki so jim bili posredovani podatki, o teh popravkih;
- **izjeme in omejitve**: načela, ki se nanašajo na kakovost podatkov, informiranje zadevnega posameznika, pravico do dostopa do podatkov in objavo obdelav, se lahko omejijo zaradi zaščite, na primer v zvezi z državno varnostjo, obrambo, javno varnostjo, pregonom kaznivih dejanj, pomembnim gospodarskim ali finančnim interesom države članice ali Evropske unije ali posameznika, na katerega se nanašajo osebni podatki;
- **pravica posameznika, na katerega se nanašajo osebni podatki, do ugovora**: posamezniku, na katerega se nanašajo osebni podatki, se mora na podlagi zakonitih razlogov zagotoviti pravica do ugovora na obdelavo podatkov, ki se nanašajo nanj. Zagotoviti se mu mora tudi, da na zahtevo in brezplačno ugovarja obdelavi osebnih podatkov, ki se nanašajo nanj, in so namenjeni trženju. Biti mora obveščen, preden se osebni podatki prvič posredujejo tretjim stranem zaradi neposrednega trženja, in izrecno opozorjen na pravico, da ugovarja takemu posredovanju;
- **zaupnost in varnost obdelave podatkov**: nobena oseba, ki odgovarja upravljavcu ali obdelovalcu, vključno s samim obdelovalcem, ki ima dostop do osebnih podatkov, ne sme obdelovati teh podatkov brez navodil upravljavca. Upravljavec mora poleg tega izvajati ustrezne ukrepe za zavarovanje osebnih podatkov pred slučajnim ali nezakonitim uničenjem, pred slučajno izgubo, predelavo, nepooblaščenim posredovanjem ali dostopom;
- **uradno obveščanje** nadzornega organa o obdelavi podatkov: upravljavec mora uradno obvestiti državni nadzorni organ pred začetkom izvajanja postopka obdelave podatkov. Po prejemu uradnega obvestila nadzorni organ izvede predhodno preverjanje posebnih nevarnosti za pravice in svoboščine posameznikov, na katere se osebni podatki nanašajo. Zagotovljena mora biti objava postopkov obdelave, nadzorni organi pa morajo voditi register postopkov obdelave, ki so uradno sporočeni.

Zbiratelj podatkov mora seznaniti osebo na katero se podatki nanašajo, kateri podatki se zbirajo in za kakšen namen. Seznaniti jih mora tudi z možnostjo dostopa do podatkov ter

pravico do poprave podatkov. Prenos osebnih podatkov izven držav Evropske unije je mogoč le, če država, kamor so bili podatki posredovani, zagotovi ustrezno raven varstva.

Evropski parlament je decembra 1997 sprejel še direktivo 97/66/ES, ki je prinesla načela osnovne direktive 95/46/ES v posebna pravila glede zaščite zasebnosti in osebnih podatkov na področju telekomunikacij. Ta direktiva se je nanašala predvsem na obdelavo osebnih podatkov v zvezi z javno dostopnimi telekomunikacijskimi servisi. Direktiva je zagotavljala zaupnost elektronske pošte, ponudnikom storitev pa je naložila obveznost, da s pomočjo tehnične in organizacijske podpore zagotovijo varno zaščito prenosa in seznanjajo uporabnike z morebitnim tveganjem. Zaradi potrebe po prilagoditvi razvoju trgov in tehnologij za elektronske komunikacijske storitve, je bila ta direktiva razveljavljena in nadomeščena z julija 2002 sprejeto direktivo 2002/58/ES.

Kot je zapisano v sami direktivi 2002/58/ES, je le ta bila sprejeta zaradi razvoja digitalne tehnologije komunikacijskih omrežij, ki imajo velike zmogljivosti in zmožnosti za obdelavo osebnih podatkov. Direktivo 97/66/ES je bilo potrebno posodobiti in prilagoditi razvoju trgov in tehnologij za elektronske komunikacijske storitve, da se ne glede na uporabljen tehnologijo zagotovi enaka raven varstva osebnih podatkov in zasebnosti uporabnikov javno razpoložljivih elektronskih komunikacijskih storitev. Internet ponuja uporabnikom nove možnosti, pa tudi nova tveganja glede njihovih osebnih podatkov in zasebnosti. Cilj direktive je čim bolj zmanjšati obdelavo osebnih podatkov in kadar je le mogoče uporabljati anonimne in psevdonimne podatke. Osnovna načela direktive 2002/58/ES:

- **Zaupnost sporočil:** Države morajo zagotoviti zaupnost sporočil in podatkov o prometu, ki se pošiljajo preko javnih komunikacijskih sredstev. Vsem osebam razen uporabnikom je prepovedano poslušanje, prisluškovanje, nadziranje komunikacij (sporočil) in z njimi povezane podatke o prometu brez privolitve uporabnikov, na katerega se nadzor nanaša.
- **Podatki o prometu:** Podatki o prometu lahko dajo dobro sliko o navadah posameznika, njegovih stikih, zanimanjih, aktivnostih in zaradi tega predstavljajo občutljive podatke. Direktiva zato zahteva, da morajo biti podatki, ki jih je ponudnik storitve obdelal in shranil, zbrisani ali predelani v anonimne, potem ko niso več potrebni za namen prenosa sporočila.
Države članice lahko sprejmejo zakonske ukrepe, s katerimi omejijo obseg pravic in obveznosti, če je to v interesu državne varnosti.
- **Podatki o lokaciji:** Podatki o lokaciji se lahko obdelujejo šele potem, ko postanejo anonimni ali s privolitvijo posameznika na katerega se podatki nanašajo.
- **Nepovabljeni sporočila:** Uporabnikom mora biti dana možnost, da na brezplačen in enostaven način ugovarjajo uporabi elektronskega naslova za namene oglaševanja. Prepovedano je pošiljati elektronsko pošto za namene neposrednega trženja na ta način, da se skrije identiteta pošiljatelja ali brez možnosti dati zahtevo, da se taka sporočila v prihodnje ne pošiljajo več.

Za namen zaščite državne varnosti, javne varnosti in obrambe, pa direktiva 2002/58/ES dovoljuje državam članicam sprejetje zakonskih ukrepov, ki lahko nekoliko omejujejo pravice

in obveznosti glede zaupnosti sporočil, podatkov o prometu in podatkov o lokaciji (ne pa tudi podatkov o vsebini!). Eden takšnih ukrepov je bil udejanjen leta 2006 z EU direktivo 2006/24/ES, ki določa zakonsko obvezno hrambo podatkov o prometu in lokaciji, ki se pridobivajo ali obdelujejo med zagotavljanjem komunikacijskih storitev s strani ponudnikov javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežjih (2006/24/ES). Čas obvezne hrambe je določen z intervalom od 6 mesecev pa do 2 let, odvisno od lastne presoje države članice EU.

Po letu 2001 v imenu boja proti terorizmu se je odnos do zasebnosti spremenil v smeri zmanjševanja pravic posameznika. Vse bolj je izražena dilema med zasebnostjo posameznikov in državno varnostjo. Tako direktiva 2002/58/ES dovoljuje državam članicam shranjevanje lokacijskih in prometnih podatkov preko različnih komunikacijskih sredstev: telefonije, mobilne telefonije, interneta, internetne telefonije, medtem ko direktiva 95/46/ES v 6. členu zahteva, da se podatki zbršejo oziroma predelajo v anonimne takoj po končanem namenu za katerega so bili zbrani. Direktive same po sebi niso zakon, predstavljajo le minimum zahtev oziroma smernice, ki jih morajo države EU sprejeti v svojih zakonodajah.

7.4 Slovenska ureditev

Republika Slovenija do sprejetja ustavnih amandmajev oziroma amandmaja XLIV iz leta 1989, ni zagotavljala ustavnopravne garancije varstva osebnih podatkov. Z omenjenim amandmajem je bila v 209. in 210. člen takratne Ustave SRS vnesena dikcija »Zajamčeno je varstvo osebnih podatkov. Zbiranje, obdelovanje in namen uporabe osebnih podatkov določa zakon. Prepovedana je uporaba osebnih podatkov v nasprotju z namenom zbiranja.« S tem je grobo vključila načela o varstvu podatkov, oblikovana v mednarodnih dokumentih. Zaradi zakonske praznine na področju varstva osebnih podatkov je bil leta 1990 sprejet Zakon o varstvu osebnih podatkov⁴⁶. Do tega sprejema zakona, so se z varstvom osebnih podatkov ukvarjali predvsem teoretiki.

Po osamosvojitvi je varstvo človekovih pravic in temeljnih svoboščin zagotovljeno v Ustavi Republike Slovenije (URS, Uradni list RS, št. 33/1991-42/1999), kjer so navedene posamezne pravice in so določena splošna pravila njihovega varstva.

⁴⁶ Uradni list RS, 8/90. S tem zakonom se je največ ukvarjal profesor Čebulj ter tudi spisal komentar tega zakona - Varstvo osebnih podatkov z zakonom in pojasnili, Inštitut za javno upravo PF, Ljubljana 1990.

Med mednarodnimi pravnimi akti, ki jih je ratificirala Republika Slovenija in ki se na podlagi 8. člena Ustave RS uporabljajo neposredno, so zlasti pomembni:

- pravni akti OZN, in sicer: Splošna deklaracija človekovih pravic, Mednarodni pakt o državljanskih in političnih pravicah in Mednarodni pakt o ekonomskih, socialnih in kulturnih pravicah (oba Uradni list SFRJ, št. 7/1971-MP in Uradni list RS, št. 35/1992-MP, št. 9), na področju varstva osebnih podatkov pa zlasti Smernice OZN glede računalniško vodenih baz vsebin podatkov, ki jih je leta 1990 sprejela Generalna skupščina;
- med pravnimi akti ES zlasti Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin (EKČP, Uradni list RS, št. 33/1994-MP, št. 7), Konvencija o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Kon-VOP, Uradni list RS, št. 11/1994-MP 3/94) in različna priporočila, ter
- med pravnimi akti EU zlasti Listina o temeljnih pravicah Evropske skupnosti in posamezne Direktive, ki so bile podlaga za izdajo slovenskega zakona o varstvu osebnih podatkov, in druge.

V navedenih pravnih dokumentih so posamezne pravice in svoboščine opisane splošno. Zaradi njihove široke in nejasne opredelitve prihaja do dvomov, kako jih je treba interpretirati, saj določila pogosto dajejo le smernice za uporabo pravnih standardov. Ker pa je po 15. členu URS mogoče predpisati način uresničevanja ter varstvo in odpravo posledic v ustavi zajamčenih pravic tudi z zakonom, je Parlament sprejel natančnejša pravila v različnih zakonih, zlasti v:

- Kazenskem zakoniku (KZ, Uradni list RS, št. 55/2008-66/2008), kjer so opredeljena posamezna kazniva dejanja in kazni;
 - Obligacijskem zakoniku (Uradni list RS, št. 86/2004-47/2007), kjer so predvidena splošna pravila o povzročitvi škode in o neupravičeni pridobitvi;
 - Zakonu o varstvu osebnih podatkov (ZVOP, Uradni list RS, št. 86/2004-67/2007), ki določa, kaj so osebni podatki, kdo lahko upravlja z njimi in preprečuje neupravičene posege v zasebnost in dostojanstvo posameznika pri obdelavi osebnih podatkov;
 - Zakonu o dostopu do informacij javnega značaja (ZDIJZ, Uradni list RS, št. 51/2006 - uradno prečiščeno besedilo), ki zagotavlja javnost in odprtost delovanja javnega sektorja ter vsakomur omogoča dostop do informacij;
 - Zakonu o medijih (ZMed, Uradni list RS, št. 54/2002-36/2008) ki določa pravice, obveznosti in odgovornosti pravnih in fizičnih oseb ter javni interes na področju medijev. Kritični položaj, ki bi ga lahko povzročila preširoka uporaba pravice do svobode izražanja omejuje s podrobnejšo opredelitvijo pravice do popravka objavljenega obvestila in do odgovora na objavljeno informacijo, ki je zajamčena prizadetemu v 40. členu URS. V 45. členu določa tudi posebne pravice, ki predstavnikom medijev omogočajo pridobivanje informacij, ki so širše od tistih po ZDIJZ;
 - v drugih zakonih;
- (Koman-Perenič, 2009, str. 5).

Uporabo predpisov pogosto dopolnjuje praksa sodišč pri odločanju v posameznih primerih. Pri tem je posebej pomembna sodna praksa Evropskega sodišča za človekove pravice (ESČP), ki razlaga EKČP. Po njej se zgledujejo tudi slovenska nacionalna sodišča, in sicer: Ustavno sodišče Republike Slovenije, kadar odloča o pritožbah v zvezi s kršitvami človekovih pravic in temeljnih svoboščin, in sodišča splošne pristojnosti, med katerimi Vrhovno sodišče Republike Slovenije, ki je najvišje sodišče v državi, odloča o različnih oblikah varstva v vseh razmerjih med državo in fizičnimi in pravnimi osebami ter med posameznimi fizičnimi in pravnimi osebami med seboj.

Če izhajamo iz varovanja osebnih podatkov je bila ustavna podlaga za sprejem Zakona o varstvu osebnih podatkov 38. člen Ustave Republike Slovenije⁴⁷ z dne 23.12.1991 (zadnjič spremenjena 07.03.2003), ki določa: "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." Prav tako je ustavna podlaga za sprejem Zakona o varstvu osebnih podatkov določba tretjega odstavka 3.a člena⁴⁸ Ustave Republike Slovenije, ki določa: "Pravni akti in odločitve, sprejeti v okviru mednarodnih organizacij, na katere Slovenija prenese izvrševanje dela suverenih pravic, se v Sloveniji uporabljajo v skladu s pravno ureditvijo teh organizacij."

Določba 38. člena Ustave Republike Slovenije na splošni ravni pomeni, da je ustavodajalec izbral t.i. "obdelovalni model" v zvezi z varstvom osebnih podatkov ("processing model") in ne t.i. "modela zlorabe" ("misuse model"), saj določa predvsem pravila za urejanje dopustne obdelave osebnih podatkov na zakonski ravni in ne načelne svobode obdelave in pretoka osebnih podatkov, ki je lahko le izjemoma izrecno omejena z zakonom. V pri razlagi ustave (Komentar Ustave RS 2002, 409) je navedeno, da je glede povezave varstva osebnih podatkov z drugimi ustavnimi pravicami s področja zasebnostne sfere: "Varstvo osebnih podatkov se navezuje na ostale človekove pravice, ki jih lahko uvrstimo v okvir zgoraj opredeljene človekove zasebnosti. To so nedotakljivost stanovanja (36. člen), varstvo tajnosti pisem in drugih občil (37. člen), svoboda vesti (41. člen)."

Prav tako je razčlenjena določba 38. člena Ustave Republike Slovenije na naslednji način: "Iz besedila člena ustave, ki določa varstvo osebnih podatkov kot človekovo pravico izhajajo štiri načela: načelo zakonitosti, načelo predhodne določitve namena zbiranja in uporabe osebnih podatkov, načelo seznanjenosti z zbiranjem osebnih podatkov in načelo sodnega varstva." (Čebulj 1998, 2)

Drugi odstavek 38. člena Ustave Republike Slovenije določa obveznost, da se zbiranje, obdelovanje, namen uporabe, nadzor ter varstvo tajnosti osebnih podatkov uredi z zakonom. Po Zakonu o varovanju osebni podatkov pa niso zavarovane naslednje skupine osebnih

⁴⁷ Uradni list RS, št. 33/91-I, 42/97, 66/2000 in 24/2003.

⁴⁸ Uradni list RS, št. 24/2003.

podatkov - osebni podatki, v zbirki osebnih podatkov, za katere je posameznik pisno privolil, da so v njej in je po naravi ali namenu lahko vsakomur dostopna; osebni podatke, ki jih zbirajo stranke, društva ali druge podobne organizacije o svojih članih, če se ti strinjajo; osebni podatki, ki so sestavni del firme ali imena družbe ali poslovalnice ali druge organizacije oziroma ustanove; osebni podatki, vsebovani v knjigah, publikacijah in drugih gradivih, ki se shranjujejo v muzejih, knjižnicah, arhivih in podobnih javnih ustanovah, ter so javno in splošno dostopni.

Pravice⁴⁹, ki gredo posamezniku po zakonu, so:

- pravica do vpogleda v bazo podatkov, ki se nanašajo nanj, zahtevati izpis teh podatkov, zahtevati seznam podatkov, ki so bili posredovani in se nanašajo nanj, pravica do vpogleda v vire, na katerih temeljijo zapisi, ki jih o posamezniku vsebuje zbirka podatkov;
- pravica zahtevati dopolnitev ali ažuriranje podatkov ter pravico do izbrisa osebnih podatkov. Za uresničitev vseh naštetih pravic je po ZVOP predviden poseben postopek.

Sistem pravnega varstva po Zakonu o varovanju osebnih podatkov zapoveduje postopek. Posameznik, ki ugotovi, da so kršene njegove pravice, določene z zakonom, lahko s tožbo (o tožbi odloča upravno sodišče po določbah zakona, ki ureja postopek v upravnem sporu, kolikor ZVOP ne določa drugače) zahteva sodno varstvo ves čas, dokler kršitev traja. Če je kršitev pravic prenehala, lahko posameznik vloži tožbo za ugotovitev, da je kršitev obstajala. Posameznik lahko v primeru uporabe osebnih podatkov, ki se nanašajo nanj in ki so bili zbrani na način ali za namen, ki ni v skladu z določbami tega zakona, povzročena škoda, od povzročitelja zahteva odškodnino v skladu z zakonom (22. člen Zakona o varovanju osebnih podatkov). Prav tako lahko pomeni takšna uporaba osebnih podatkov tudi kaznivo dejanje »zlorabe osebnih podatkov« (iz 154. člena KZ RS – »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 podatki nanašajo[...]«). Za nadzor zakona je zakonodajalec uvedel inšpekcijski nadzor, ki ga natančneje določa ZVOP (členi od 26 do 28). Stanje na področju varstva osebnih podatkov in izvrševanje določb samega ZVOP pa spremlja pristojno delovno telo Državnega zbora, neformalni nadzor varstva osebnih podatkov pa opravlja varuh človekovih pravic, (Lampe, n.d., str. 144 - 148).

⁴⁹ Pravice, zagotovljene z ZVOP, pa so seveda lahko tudi omejene, tako s splošnimi določili omejitve pravice do zasebnosti iz 2. odst. 8. člena EKČP in sam 23. člen ZVOP. In sicer je možno »pravice posameznika v zvezi z varstvom osebnih podatkov omejiti samo izjemoma v primerih, ki jih določa zakon za potrebe nacionalne varnosti, obrambe, javne varnosti, preprečevanja, razkrivanja, odkrivanja in preganjanja kaznivih dejanj ali kršitve etičnih norm za določene poklice, monetarne, proračunske in davčne zadeve, nadzora javne varnosti, in varstva subjekta podatkov ali pravic in svoboščin drugih, v obsegu, ki je nujen za doseg namena, zaradi katerega se določa omejitve, razen v zvezi z varstvom osebnih podatkov, ki so povezani z narodnim, rasnim in drugim poreklom, političnimi, verskimi in drugimi prepričanji, izobrazbo, zdravstvenim stanjem, razen nalezljivih bolezni ali spolnega vedenja«. Nikakor pa ni mogoče omejiti pravice do vpogleda v katalog zbirk osebnih podatkov in pravice zahteve po sodnem varstvu (2. odst. 23. člen ZVOP).

Med najpomembnejše odločitve Ustavnega sodišča štejemo:

- *OdIUS VII, 163, U-I-174/94, Ur. 1. 73/98*: »23. Eden izmed pobudnikov izpodbija tisti del določbe 4. člena Pravilnika-97, po katerem je v prijavi sprejemnika med podatki o naročniku, ki je fizična oseba, potrebno navesti tudi enotno matično številko občana. Po 2. odst. 38. člena zbiranje osebnih podatkov določa zakon, poleg tega pa mora določiti tudi namen njihove uporabe in urediti njihovo obdelovanje. Konvencija o varstvu posameznikov glede na avtomatsko obdelavo podatkov - KonVOP (Ur. 1. MP 3/94) je še natančnejša. Poleg tega, da morajo biti osebni podatki pridobljeni in obdelani pošteno in zakonito, Konvencija terja obstoj ukrepov, ki bodo zagotovili, da bodo osebni podatki shranjeni za določene in zakonite namene in da se bodo obdelovali le podatki, ki so primerni, ustrezni in niso pretirani glede na namen zbiranja (5. člen v zvezi s 4. členom). Po 6. členu Zakona o varstvu osebnih podatkov - ZVOP kot splošnem zakonu o varstvu osebnih podatkov lahko upravljalec zbirke podatkov zbira le tiste osebne podatke, za katere je pooblaščen z zakonom ali s pisno privolitvijo posameznika, na katerega se nanašajo podatki. Zakon o RTV Slovenija - ZRTVS ne določa, da bi RTV Slovenija lahko od posameznika zahtevala, naj v prijavi RTV sprejemnika navede enotno matično številko občana. Določba je zato v nasprotju z 2. odst. 38. člena in jo je treba razveljaviti.
- *OdIUS IX, 257, U-I-238/99, Ur. 1. 113/2000*: »15. posebno mesto med človekovimi pravicami in temeljnimi svoboščinami imajo določbe, ki varujejo človekovo osebno dostojanstvo, osebnostne pravice, njegovo zasebnost in varnost (34. do 38. člen) in ki prepovedujejo vsem — na prvem mestu državi, pa tudi posameznikom - poseganje v našete pravice. V skladu z načelom, da je na tem področju prepovedano vse, kar ni izrecno dovoljeno, je po Ustavi prepovedan vsak poseg v našete pravice, razen tistih, ki so izrecno dovoljeni. Pravica do zasebnosti se za posameznika lahko konča samo takrat in tam, kjer kolidira z zakonsko izkazanim močnejšim interesom drugih (*OdIUS VI, 158, U-I-25/95, Ur. 1. 5/98*).
- *OdIUS X, 76, U-I-18/98, Ur. 1. 37/2001*: »12. Ker so podatki za odmero dohodnine predvsem podatki o dohodkih in torej glede na opredelitev osebnih podatkov kot podatkov, ki kažejo na lastnosti, stanja ali razmerja posameznika, ne glede na obliko, v kateri so izraženi (1. točka 5. člena Zakona o varstvu osebnih podatkov - ZVOP90, Ur. 1. 8/90 in nasl., oziroma od razveljavitve ZVOP90 z dne 7. 8. 1999 točka 1 člena 2 Zakona o varstvu osebnih podatkov - ZVOP, Ur. 1. 59/99), osebni podatki, so podlago za presojo ustavnosti 2. odst. 34. člena ZDavP predstavljala zgoraj navedena zavzeta stališča. US je tako presojo začelo pri vprašanju, ali je v zakonih določno opredeljeno, kateri podatki se smejo zbirati in obdelovati. Pri iskanju odgovora je ugotovilo, da posamezne določbe ZDavP, kot npr. 1. odst. 25. člena ZDavP, ki določa, da fizična oseba predloži svojo davčno številko v vseh primerih, ko prejema dohodke ali prejemke, le izjemoma določno opredeljujejo dolžnost navajanja posameznih podatkov, ki bi kot taka lahko na drugi strani napotovala na dolžnost zbiranja in obdelave podatkov.

7.5 Zdravstveni podatki

Vprašanje zasebnosti osebnih oziroma zdravstvenih podatkov je aktualno tako za pravnike kot tudi za zdravnike in paciente. Ker so zdravstveni podatki glavni vir raziskav, napredka brez njihove uporabe tudi na področju medicine seveda ni mogoče pričakovati. Razvoj tako stroke kot znanosti je vsaj deloma pogojen tudi z dostopom do podatkov o zdravstvenem stanju pacientov.

V Evropi je zasebnost, tudi informacijska zasebnost (kamor sodi varstvo osebnih podatkov) opredeljena kot pravica posameznika, ki jo je treba varovati. V izjemno tržno naravnani družbi, kot je ZDA, pa zasebnost nima narave pravice posameznika in se dojema bolj kot ovira za doseganje različnih ciljev, bodisi drugih posameznikov bodisi gospodarskih subjektov ali države. Zaradi različnih družbenih okvirov tudi posamezniki dojemajo zasebnost drugače. Kar je z vidika pričakovane zasebnosti sprejemljivo za pacienta v ZDA, morda zaradi različnega kulturnega in tudi pravnega okvira ni sprejemljivo za evropskega pacienta.

Pravica do zasebnosti je v ZDA koncipirana kot lastninska pravica. Škodovanje ugledu posameznika tako ni razumljeno kot poseg v njegovo zasebnost, temveč kot poškodba nečesa, kar poseduje – ugleda – in s tem zmanjšanje njegove vrednosti. Iz lastninskega razumevanja zasebnosti sledi, da lahko lastnik s svojo lastnino naredi kar koli, torej jo tudi proda in tako izgubi nadzor nad njo. V ZDA je takšno lastninsko razumevanje zasebnosti zelo razširjeno predvsem na polju informacijske zasebnosti – pri zbiranju osebnih podatkov. Podjetja, ki zbirajo osebne podatke, imajo namreč te za svojo last in ne last posameznikov, od katerih so bili podatki zbrani, iz tega pa sledi, da jih smejo tudi prodajati naprej ali jih celo javno objaviti. Na drugi strani pa je takšno pojmovanje zasebnosti Evropi tuje.

Po drugi svetovni vojni, ko je bil gospodarski in tehnološki razvoj v največjem razmahu, je postalo evropskim državam jasno, da je treba postaviti temelje za pregledno zbiranje in analiziranje podatkov. Tega so se lotile sprva države same, v začetku 80-ih let pa je najprej Organizacija za ekonomsko sodelovanje in razvoj (OECD) sprejela Smernice za zaščito zasebnosti in čezmejni pretok osebnih podatkov (op. 3), nekaj kasneje pa je na podlagi smernic Svet Evrope sprejel Konvencijo o varstvu posameznika glede na avtomatsko obdelavo osebnih podatkov. Konvencija določa, da se smejo osebni podatki uporabljati in shranjevati samo za zakonite namene in pošteno, zbirati se smejo samo podatki, ki so ustrezni in skladni z dosegom namena, za katerega se zbirajo; prepovedano je čezmerno zbiranje osebnih podatkov, upravljavec zbirke osebnih podatkov pa mora zagotoviti njihovo točnost in jih ne sme hraniti dlje, kot je nujno potrebno za doseg namena, zaradi katerega se zbirajo. Poleg tega daje konvencija posameznikom pravico do seznanitve z obstojem in vsebino osebnih podatkov, ki jih zadevajo, ob morebitnih napakah pa pravico zahtevati popravek ali izbris osebnih podatkov.

7.5.1 Pravne osnove za obdelavo pacientovih podatkov v Republiki Sloveniji

Ustava Republike Slovenije v 35. členu varuje pravico do zasebnosti in osebnostnih pravic, v 38. členu pa Ustava RS še posebej varuje osebne podatke (informacijsko zasebnost posameznika). Citirano določilo tudi prepoveduje uporabo osebnih podatkov v nasprotju z namenom njihovega zbiranja, določa, da zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa zakon, ter da se ima vsakdo pravico seznaniti z zbranimi osebnimi podatki, ki se nanašajo nanj in pravico do sodnega varstva ob njihovi zlorabi. V Republiki Sloveniji je torej varstvo osebnih podatkov ustavno zagotovljena temeljna človekova pravica posameznika. Splošne pravne podlage za obdelavo osebnih podatkov v javnem in zasebnem sektorju so določene z Zakonom o varstvu osebnih podatkov. Tako se osebni podatki lahko obdelujejo (npr. zbirajo, posredujejo, vpisujejo, urejajo, shranjujejo, prilagajajo ali spreminjajo, priključijo, vpogledajo, uporabijo, razkrijejo s prenosom, sporočajo, razvrščajo ali povezujejo, blokirajo, anonimizirajo, izbrišejo) le, če obdelavo osebnih podatkov in osebne podatke, ki se obdelujejo, določa zakon ali če je za obdelavo določenih osebnih podatkov podana osebna privolitev posameznika. Če je upravljavec del javnega sektorja, to so npr. vsi izvajalci zdravstvene dejavnosti v javni zdravstveni mreži, lahko obdeluje osebne podatke, če obdelavo osebnih podatkov in osebne podatke, ki se obdelujejo, določa zakon. Samo zakon lahko določi, da se določeni osebni podatki v javnem sektorju obdelujejo le na podlagi osebne privolitve posameznika. Zasebni zdravstveni delavci, ki niso del javne zdravstvene mreže, lahko osebne podatke obdelujejo tudi na podlagi osebne privolitve posameznika.

Še strožji pogoji po ZVOP veljajo za obdelavo občutljivih osebnih podatkov. Občutljivi osebni podatki so podatki o rasnem, narodnem ali narodnostnem poreklu, političnem, verskem ali filozofskem prepričanju, članstvu v sindikatu, zdravstvenem stanju, spolnem življenju, vpisu ali izbrisu v kazensko evidenco ali evidence, ki se vodijo na podlagi zakona, ki ureja prekrške, ali iz njih. Občutljivi osebni podatki so tudi biometrične značilnosti, če je z njihovo uporabo mogoče določiti posameznika v zvezi s kakšno od prej navedenih okoliščin. Za obdelavo zdravstvenih podatkov tako zasebniki zunaj javne zdravstvene mreže potrebujejo praviloma pisno osebno privolitev pacienta, izvajalci zdravstvenih storitev v javni zdravstveni mreži pa zakonsko pooblastilo za njihovo obdelavo (13. člen ZVOP). Zakon za te podatke zahteva tudi strožje zavarovanje. Med drugim morajo biti občutljivi osebni podatki pri obdelavi posebej označeni in zavarovani tako, da se nepooblaščenim osebam onemogoči dostop do njih.

7.5.2 Upravljalci osebnih podatkov pacientov

Fizična ali pravna oseba, ki v skladu z zakonskimi pogoji obdeluje osebne podatke, je po ZVOP *upravljavec* osebnih podatkov. Po Zakonu o zbirkah podatkov s področja zdravstvenega varstva so upravljalci zbirk podatkov s področja zdravstvenega varstva Inštitut za varovanje zdravja in ostali izvajalci zdravstvene dejavnosti v Republiki Sloveniji. Upošteva se koncept izbranega osebnega zdravnika v javni zdravstveni mreži, kot ga določa Zakon o zdravstvenem

varstvu in zdravstvenem zavarovanju, je upravljavec celotne osnovne zdravstvene dokumentacije pacientov izbrani splošni zdravnik ali pediater, njegov izbrani zobozdravnik oziroma njegov izbrani ginekolog. V skladu z ZZVZZ lahko izbrani osebni zdravnik pooblastila, ki so mu dana z zakonom in se nanašajo na diagnostiko in zdravljenje, vključno s predpisovanjem zdravil na recept, kot tudi napotitev na bolnišnično zdravljenje, prenese na ustreznega specialista, če to narekuje bolnikovo zdravstveno stanje in racionalnost dela. V skladu z obsegom pooblastila je napotenemu zdravniku priznana tudi pravica do obdelave pacientovih osebnih podatkov. Slednji je torej upravljavec pacientovih osebnih podatkov le glede storitev, ki jih nudi po pooblastilu izbranega osebnega zdravnika. Tega je o svojih ukrepih in bolnikovem zdravstvenem stanju dolžen tudi redno obveščati. Enako je določeno tudi z Zakonom o zdravstveni dejavnosti. ZZD⁵⁰ poleg navedenega določa tudi, da so zdravstveni delavci, zdravstveni sodelavci in osebe, ki so jim podatki dosegljivi zaradi narave njihovega dela, dolžni varovati podatke o zdravstvenem stanju posameznika in o vzrokih, okoliščinah in posledicah tega stanja kot poklicno skrivnost. Komu in kdaj je dopustno razkriti pacientove osebne podatke (tudi občutljive), je zelo natančno reguliral sprejeti Zakon o pacientovih pravicah. V krog upravičencev sodi najprej pacient sam (njegov zakoniti zastopnik, če je sam mladoleten, ali skrbnik, če je pod skrbništvom), poleg njega pa še njegov pooblaščenec in ožji družinski člani, kolikor za katerega od njih (ali vse) pacient ni prepovedal, da se seznani z njegovo zdravstveno dokumentacijo. Ne glede na pacientovo voljo pa lahko zdravnik sporoči informacije o njegovem zdravstvenem stanju, če je to nujno potrebno za varovanje življenja ali preprečitev hudega poslabšanja zdravja. Kadar pacient v okviru javne zdravstvene mreže zamenja izbranega osebnega zdravnika, prejšnji izbrani zdravnik vso pomembno zdravstveno dokumentacijo o bolniku preda novemu. Tudi ta določba lepo kaže na različno dožemanje koncepta varstva osebnih podatkov pri nas in v ZDA. Zdravnik namreč zdravstvene dokumentacije, pa čeprav se ta nanaša na pacienta, temu ne izroči (ne preda v posest, kjer bi jo pacient lahko tudi uničil, če bi tako hotel), temveč jo izroči novemu izbranemu zdravniku. Če pacienta napoti na zdravljenje na sekundarno ali terciarno raven, bi moral izbrani osebni zdravnik na enak način posredovati za nadaljnje zdravljenje pomembno zdravstveno dokumentacijo napotenemu zdravniku, ki ga je izbral pacient. Tudi ko pacienta napoti delodajalec na obdobjni preventivni pregled, osebni izbrani zdravnik ob soglasju pacienta zdravstveno dokumentacijo posreduje neposredno zdravniku medicine dela, ki ga za pregled pacienta pooblasti delodajalec. Zdravstvena dokumentacija vedno potuje od upravljavca do upravljavca, torej med izvajalci zdravstvene dejavnosti. Zapisano glede varstva osebnih podatkov in obdelave podatkov v zdravstveni dokumentaciji

⁵⁰ ZZDej v 46. členu določa, da storitve s področja osnovne zdravstvene dejavnosti opravlja osebni zdravnik s svojimi sodelavci. Ta lahko napoti bolnika tudi k drugim zdravnikom in usklajuje njihove nasvete, vodi pa tudi bolnikovo zdravstveno dokumentacijo. V razmerju do osebnega zdravnika so vsi drugi zdravniki, ki sodelujejo pri zdravstveni obravnavi posameznika na sekundarni in terciarni ravni, napotni zdravniki. Izvajanje storitev napotnega zdravnika je praviloma časovno omejeno in vezano na napotitev osebnega zdravnika. Le izjemoma, kadar določena kronična bolezen na podlagi strokovnih kriterijev zahteva trajen nadzor na specialistični ravni, lahko napotni zdravnik prevzame bolnika v stalno zdravstveno oskrbo. O tem se mora dogovoriti z bolnikovim osebnim zdravnikom, ki ga mora tudi redno obveščati o bolnikovem zdravstvenem stanju in svojih ukrepih.

velja tudi za zdravnike zasebnike, ki niso del javne zdravstvene mreže. Na zakonodajni ravni sicer ni rešeno napotovanje pacienta na sekundarno oziroma terciarno raven z njihove strani. Vendar je šteti, da je pravica do zdravstvenih storitev, ki jo ima napotni zdravnik, pravica pacienta s statusom zavarovane osebe v obveznem zdravstvenem zavarovanju, pri čemer bi določila ZZVZZ smiselno uporabili tudi v takšnem primeru. Ker je zdravstveno zavarovanje v Republiki Sloveniji obvezno, bi moral biti položaj, ko zasebni zdravnik zunaj javne zdravstvene mreže obravnava pacienta brez obveznega zdravstvenega zavarovanja, zgolj teoretičen.

Ob porastu števila zasebnih izvajalcev zdravstvene dejavnosti, ki niso del javne zdravstvene mreže, bo treba poleg že izpostavljenega vprašanja pooblastil zakonsko urediti tudi obveznost arhiviranja oziroma hrambe in prevzema dokumentacije, ko pacient izbere drugega zdravnika, ali zasebnega ali zdravnika v javni zdravstveni mreži. Predvsem glede arhiviranja bo treba določiti, kako naj poteka odbiranje in prevzemanje tega gradiva ter kje in kdo naj ga hrani. Sicer pa bi obdelavi osebnih podatkov na področju zdravstvenega varstva v Republiki Sloveniji le težko očitali zanemarjanje na zakonski ravni, saj je zakonov, ki urejajo to tematiko, precej. Razdrobljenost vsebine v posameznih zakonih lahko pripelje do nekonsistentnosti, ko določbe v različnih zakonih med sabo niso več skladne ali si celo nasprotujejo, kar seveda praktično izvajanje posameznih določil oteži. Tako bi bilo v prihodnje dobro, da bi regulacijo obdelave pacientovih osebnih podatkov umestili v en zakon.

Največji izziv za zdravstvo na področju obdelave osebnih podatkov v prihodnjih letih predstavlja informatizacija. Vse bolj glasno je izražena potreba po vzpostavitvi elektronske zdravstvene kartoteke, uporabi telemedicine ipd. Informatizacija bo zahtevala tudi strogo in pregledno določitev dostopnih pravic za branje, popravljanje, spreminjanje, vpisovanje in drugo obdelavo zdravstvenih podatkov. Za zdaj drži, da je bil tehnološki napredek, ki mu je zdravstvo v delu, ki se nanaša na medicinsko stroko, sledilo, na področju obdelave podatkov v preteklosti zanemarjen. Težko je verjeti, da v dobi, ko je laserski poseg običajen, tega še vedno (v glavnem) dokumentiramo na papirju. Tudi to je najbrž posledica evropskega dojemanja varstva osebnih podatkov, ko so osebni podatki za gospodarske subjekte sicer zanimivo blago, ki pa je zaradi strogih pogojev obdelave za tržne namene nedosegljivo. Ker pa brez obdelave podatkov, tudi osebnih in občutljivih, ni mogoče pričakovati napredka stroke, je pod določenimi pogoji tudi podatke o zdravstvenem stanju pacientov dopustno uporabiti za znanstvenoraziskovalne namene. Tako je dopustno za te namene uporabiti zdravstvene podatke že pokojnih pacientov, če niso pacienti sami ali kasneje njihovi zakoniti dediči prvega ali drugega dednega reda prepovedali posredovanja osebnih podatkov. Zdravstvenih podatkov živih pacientov brez njihove osebne privolitve tudi za znanstvene in raziskovalne namene ni dopustno uporabiti. Iz zapisanega izhaja, da je upoštevanje pravice posameznika do informacijske zasebnosti – do varstva osebnih podatkov – za namene raziskav dopustno uporabiti le podatke v anonimizirani⁵¹ obliki. Varstvo traja za časa posameznikovega življenja, ko ta lahko prepove posredovanje osebnih podatkov tudi za čas

⁵¹ Anonimizacija pomeni takšno spremembo oblike osebnih podatkov, da jih ni več mogoče povezati s posameznikom ali je to mogoče le z nesorazmerno velikimi naporji, stroški ali porabo časa.

po njegovi smrti. Prav tako lahko posameznik kot nosilec pravice do varstva osebnih podatkov za časa življenja privoli v posredovanje in obdelavo njegovih zdravstvenih podatkov za znanstvene in raziskovalne namene, pri čemer je pomembno, da svojo osebno privolitev poda prostovoljno in na podlagi informacij o vsebini in ciljih raziskave, ki mu jih je dolžan zagotoviti upravljavec oziroma izvajalec raziskave, če ne gre za isti subjekt.

8 ZAKLJUČEK

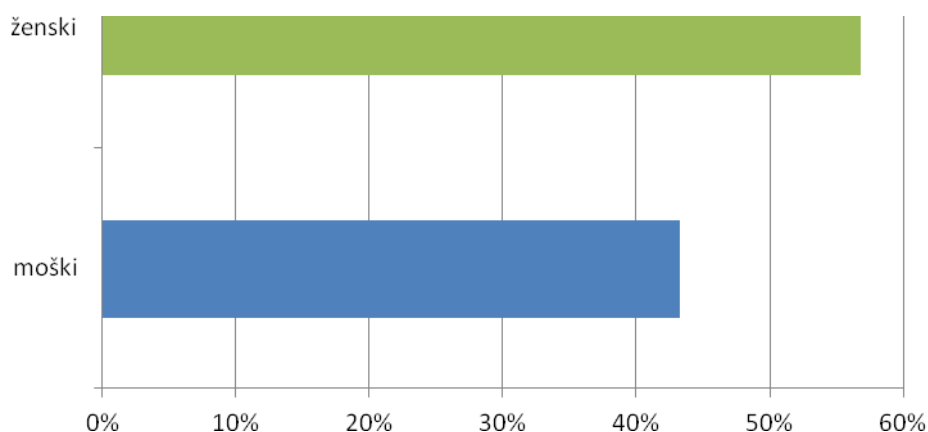
8.1 Anketa in analiza ankete

V empiričnem delu svoje diplomske naloge sem izvedla anketo o pravici do zasebnosti na delovnem mestu. Respondenti so bile osebe starejše od 18 let. Anketa je bila oblikovana kot spletni vprašalnik. Razdeljena je bila med prijatelje in znance preko socialnega omrežja Facebook, kateri so odgovarjali preko spletne forme. Med reševanjem ankete sem bila svojim respondentom na voljo za morebitna dodatna pojasnila. Anketiranje je bilo izvedeno v obdobju med 10.12.2011 in 31.12.2011. V tem času je bilo izpolnjenih 88 vprašalnikov.

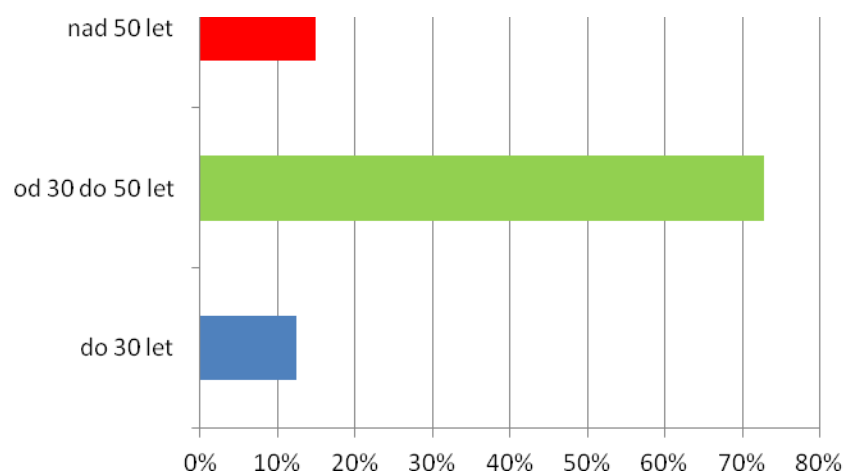
Anketni vprašalnik (v prilogi) je bil sestavljen iz 17 vprašanj in iz treh delov. V prvem me je zanimalo v kolikšni meri se anketirancem zdi pomembna pravica do zasebnosti, ugotoviti s katerimi aktivnostmi na internetu se ukvarjajo med delovnim časom in kaj jih po njihovem mnenju ogroža. V drugem delu se je iskal odgovor glede zasebnosti na delovnem mestu in morebitnih vdorov delodajalcev v zasebnost delojemalca. V tretjem delu pa se je poizkušalo odgovoriti na vprašanje kdo je odgovoren za zasebnost delojemalca in mnenje ob morebitnem poseganju v intimno sfero. Dobljeni rezultati so predstavljeni in obrazloženi skupaj z grafi.

Med značilnosti anketiranih lahko štejemo, da ni močno prevladujoče skupine, kajti razmerje med moškimi 43% in ženskami 57% je uravnoteženo. Prevladujoča starostna skupina, katera je bila pripravljena odgovorjati na vprašanja je med 30 in 50 leti ter z delovno dobo do 15 let.

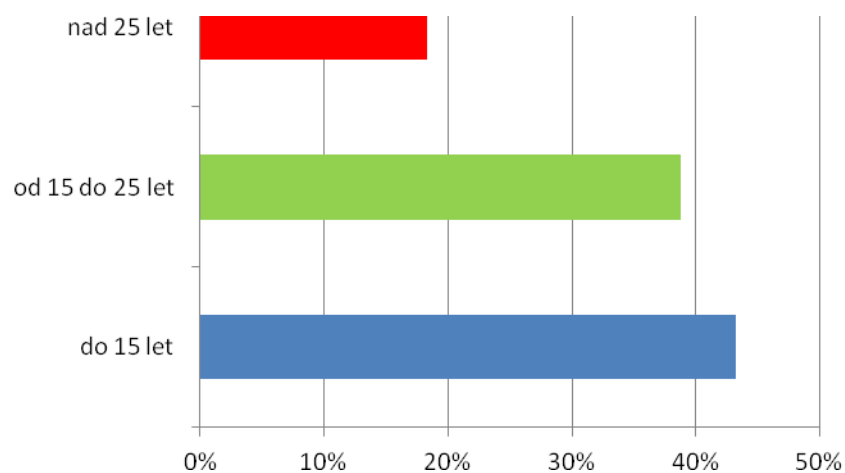
Graf 1: Pregled anketirancev po spolu



Graf 2: Pregled po starostnem obdobju

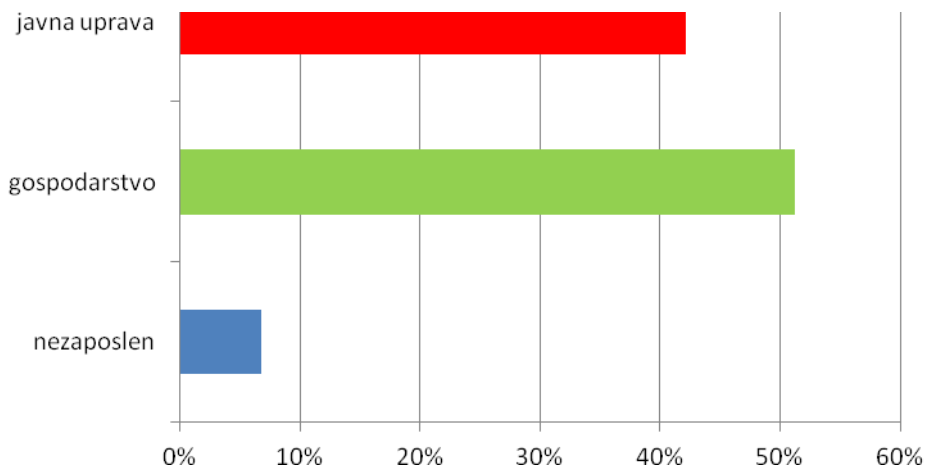


Graf 3: Pregled delovne dobe



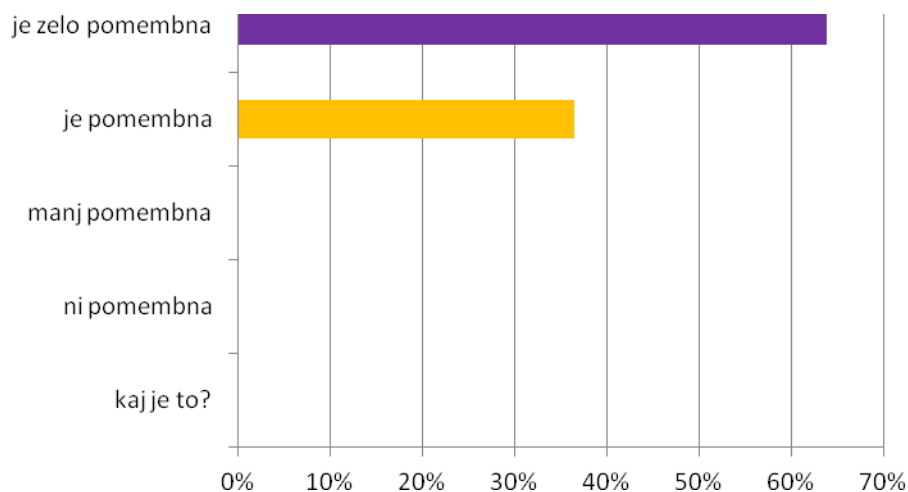
Med anketiranci lahko opazimo, da so sodelovali tako zaposleni v gospodarstvu kakor tudi v javni upravi.

Graf 4: Pregled anketirancev glede na sektor zaposlitve



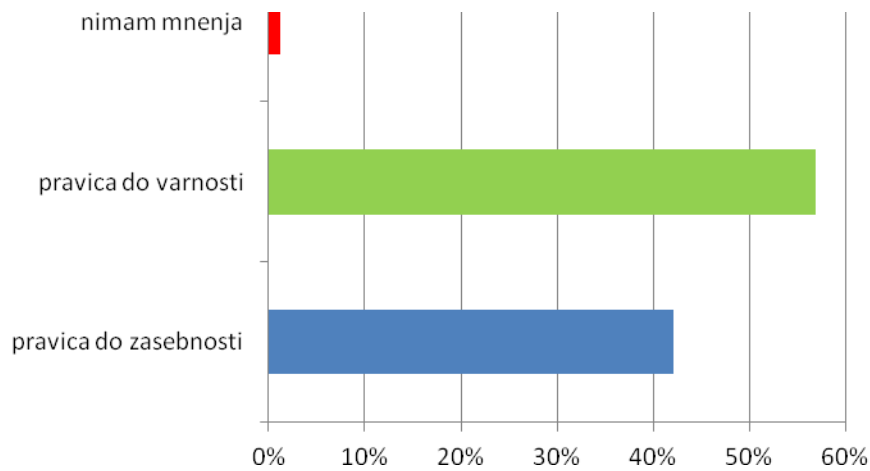
Pri vprašanju kako pomembna je pravica do zasebnosti posameznika, je večina vprašanih odgovorila, da se jim zdi zelo pomembna. Nihče izmed anketiranih ni na to vprašanje odgovoril, da se mu zasebnost ne zdi pomembna ali da mu je vseeno. Kar 64% vprašanih je odgovorilo, da se jim zdi pravica do zasebnosti zelo pomembna, ostalih 36% pa meni, da je pomembna. Iz teh rezultatov lahko sklepamo, da anketirani svoji zasebnosti pripisujejo velik pomen.

Graf 5: Kako pomembna se vam zdi pravica do zasebnosti posameznika?



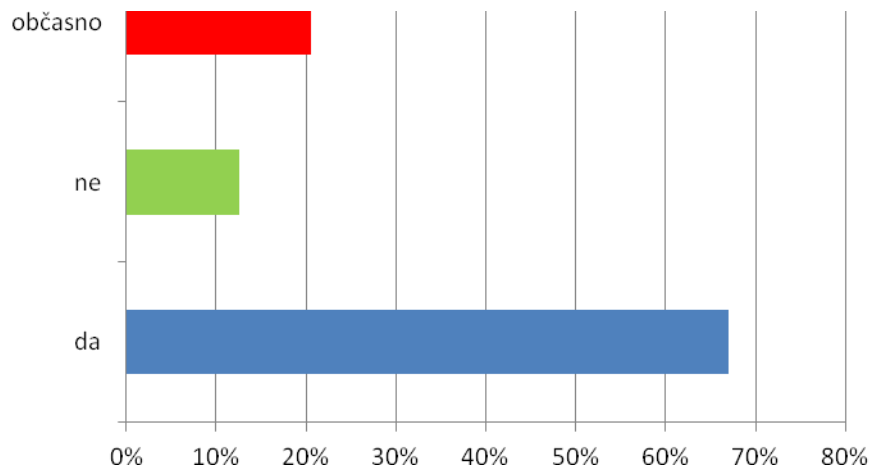
Pri vprašanju katera pravica se posamezniku zdi pomembnejša, pa je 57% vprašanih postavilo na prvo mesto pravico do varnosti, medtem ko 42% meni, da je pravica do zasebnosti primarna. Opaziti pa je tudi 1% prisotnost vprašanih, kateri nimajo izoblikovanega mnenja. To lahko tudi razumemo kot nepoznavanje pojma pravica do zasebnosti in pravica do varnosti.

Graf 6: Katera pravica se vam zdi pomembnejša?

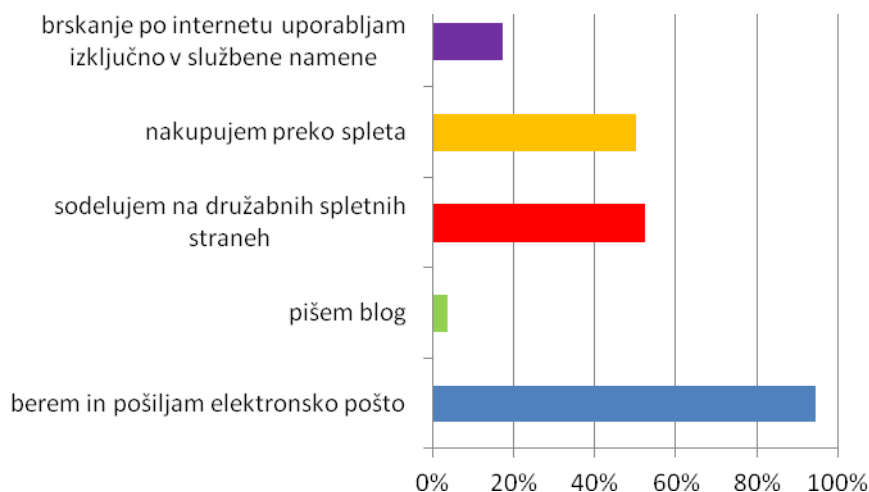


Kar 67% zaposlenih med delovnim časom redno uporablja službeni računalnik za brskanje po spletu. Brskanje po spletu se le v 18% uporablja izključno za službene namene, medtem ko se v 82% uporablja za neslužbene namene (spletno kupovanje 51%, elektronska pošta 94%, socialna omrežja 55%).

Graf 7: Ali na delovnem mestu uporabljate službeni računalnik za brskanje po internetu?



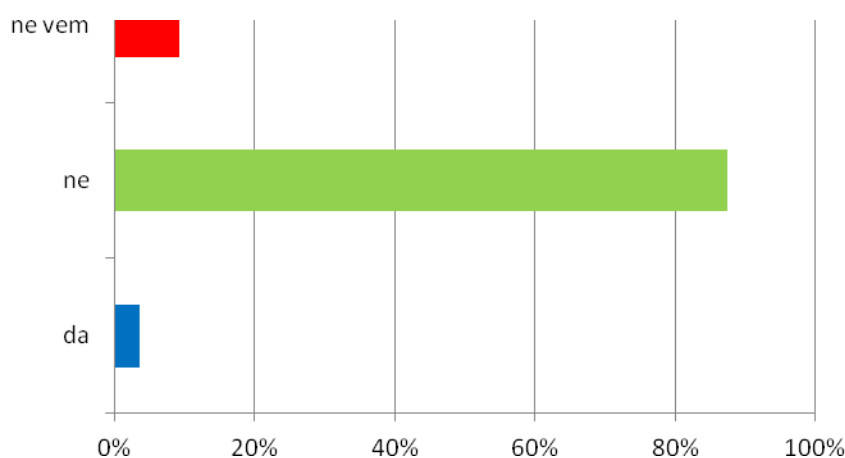
Graf 8: Vsebina uporabe interneta med delovnim časom



V sodobni poslovni praksi se za zahtevnejša delovna mesta vedno bolj zahteva popolna lojalnost do delodajalca. Posledično se nudijo delojemalcu večje bonitete po drugi strani se je za bonitete potrebno odpovedati delu svoje zasebnosti. V zadnjem obdobju se v pogodbah za zaposlitev srednjega in višjega vodstvenega kadra pojavljajo členi, kjer se podpisnik zavestno odpoveduje pravici do popolne zasebnosti.

Pri tem vprašanju vidimo, da kar 88% vprašanih ni podpisalo dogovora o omejevanju zasebnosti, medtem ko 9% sploh ne ve kaj so podpisali. 3% vprašanih je bilo ob podpisu pogodbe seznanjeno z omejitvami njihove zasebnosti.

Graf 9: Ali ste pri zasedbi delovnega mesta podpisali dogovor o omejitvi vaše zasebnosti med službenim časom?



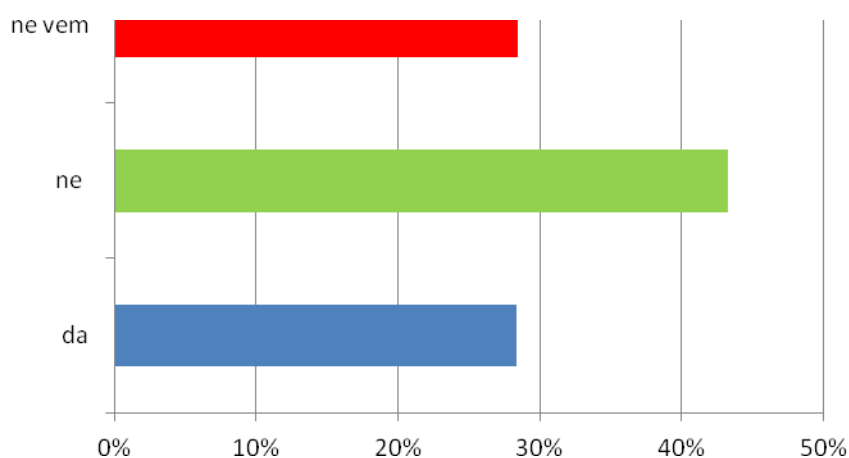
Ne glede na vso zaščitno zakonodajo glede varovanja zasebnosti posameznika in evropske sodne prakse, je v Sloveniji prisoten ilegalen nadzor nad delom zaposlenih. 43% vprašanih

meni, da jim delodajalec ne nadzoruje aktivnosti na službenih računalnikih medtem ko 28% meni, da se ta nadzor izvaja. Zaskrbljujoč je podatek da kar 28% vprašanih ne ve kaj se dogaja. Nekoliko drugačno sliko dobimo, ko pogledamo odgovore na moteno delovanje računalnikov. Pri tem je 7% vprašanih zaznalo redno upočasnjeno delovanje, 48% pa občasno moteno delovanje službenega računalnika, katerega ne morejo povezati z nobenim vzrokom (antivirusni programi, nadgradnja,...). Le 27% vprašanih pa nikoli ne zazna sprememb v delovanju.

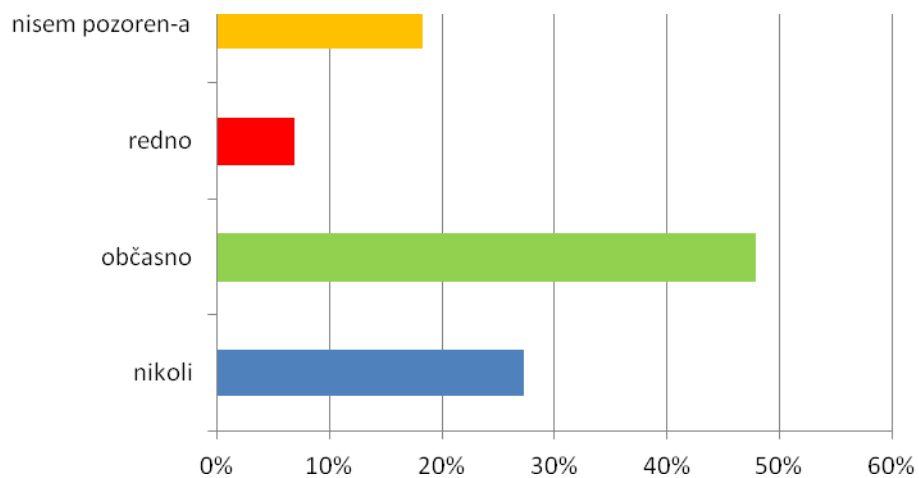
Če pa govorimo o nedotakljivosti vsebine elektronske pošte službene ali zasebne narave, je 48% vprašanih mnenja, da delodajalec pregleduje vsebino elektronske pošte. Drugačno sliko dobimo, ko pogledamo koliko vprašanih je odgovorilo (3%), da so opazili poznavanje vsebine elektronske pošte s strani njihovih nadrejenih.

Potrditev dejanskega nadzora nad zaposlenimi pa dobimo v podatku, da je bilo že 7% vprašanih opozorjenih na prekomerno brskanje po spletu s strani delodajalca. To je več kot 100% kot pri poznavanju vsebine pošte, opozarja pa na trend skrivnega nadzora in profiliranja zaposlenih.

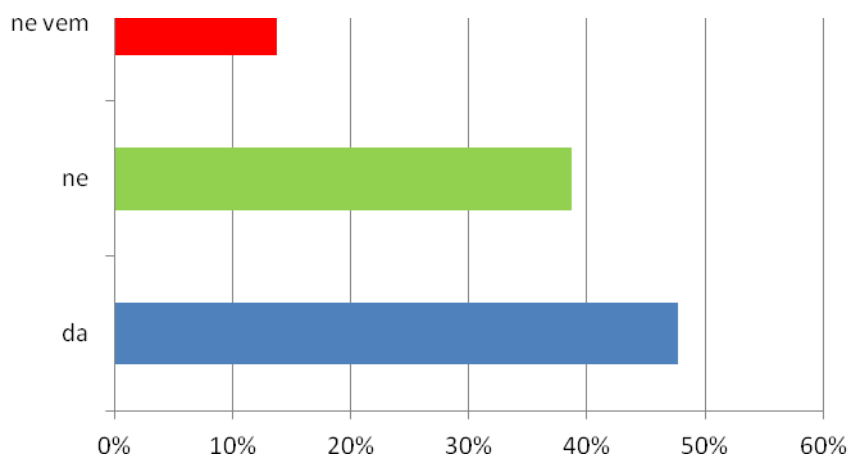
Graf 10: Ali menite, da vam delodajalec nadzoruje vaše aktivnosti na vašem računalniku?



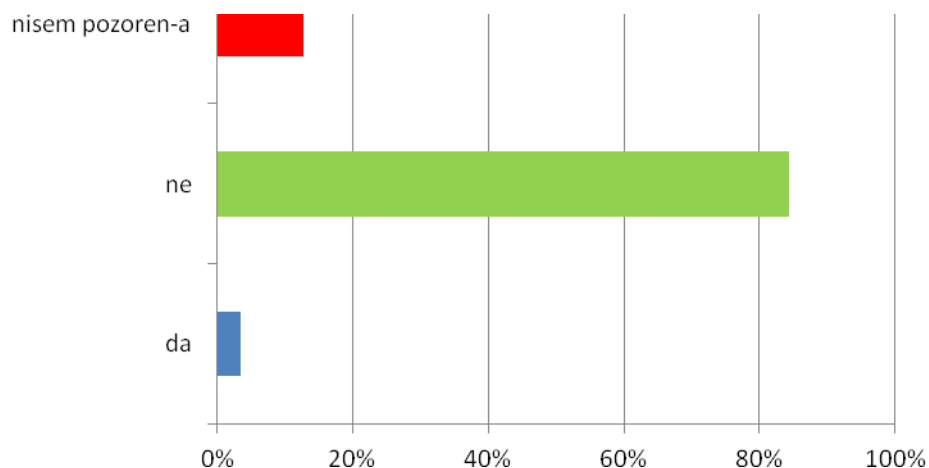
Graf 11: Ali ste kdaj pri uporabi službenega računalnika opazili nepričakovano in nerazumljivo upočasnjeno delovanje le tega?



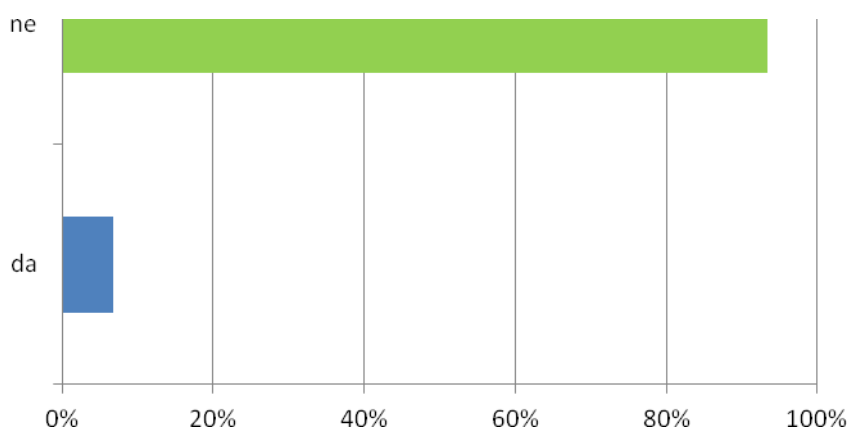
Graf 12: Ali menite, da vam lahko delodajalec pregleduje vsebino službene elektronske pošte?



Graf 13: Ali ste pri pogovoru z nadrejenimi mogoče opazili, da oni kakorkoli poznajo vsebino vaših elektronskih sporočil?

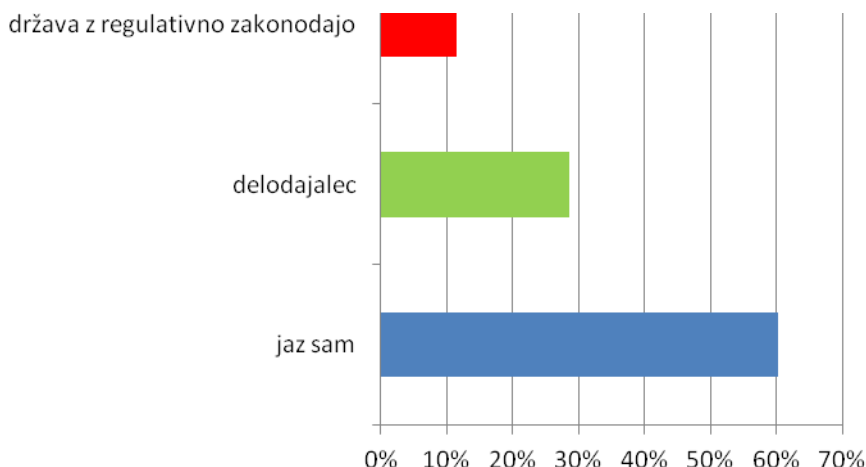


Graf 14: Ali ste bili kdaj opozorjeni na prekomerno brskanje po internetu?



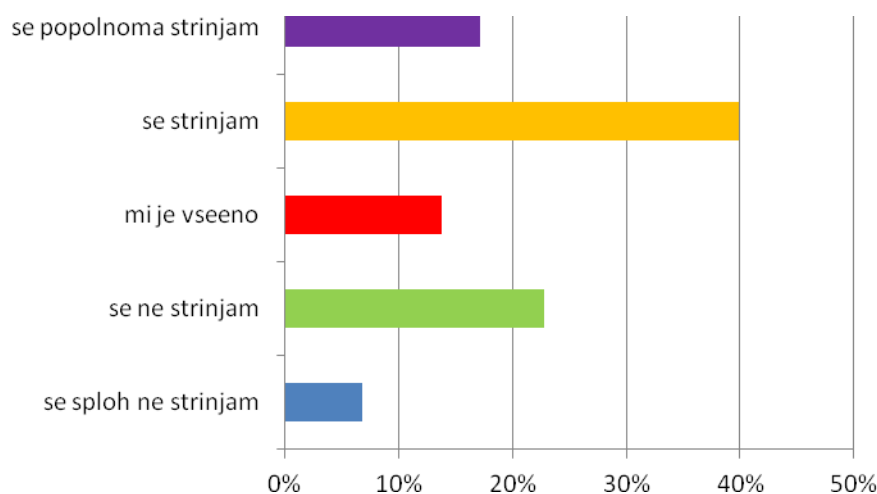
Večina vprašanih (60%) največjo odgovornost za varovanje svoje zasebnosti pripisuje sebi. Takih, ki menijo, da so odgovorni delodajalci je 28%. Preostanek vprašanih (11%) pa meni, da je odgovornost za varovanje svoje zasebnosti na plečih države in regulativne zakonodaje.

Graf 15: Kdo je po vašem mnenju najbolj odgovoren za varovanje vaše zasebnosti na delovnem mestu?



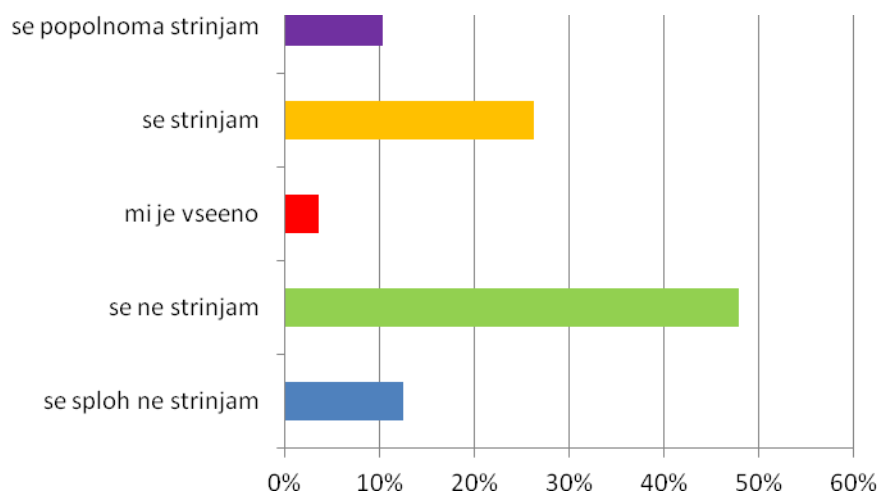
Na delovnem mestu je tanka meja med dopustnim in nedopustnim posegom delodajalca v delojemalca. V težnji po čim bolj izkoriščenem času delojemalca je v težki gospodarski situaciji vedno bolj prisoten globalni nadzor nad zaposlenimi. Po eni strani imamo mobing nad zaposlenimi po drugi strani so osebne informacije posameznika tržno blago in nujno potrebne pri sestavljanju psihološkega profila. Pri iskanju mnenja anketirancev v zvezi z nedopustnostjo nadzora delodajalca, se jih 40% vprašanih ne strinja s posegom, 17% povsem odklanja poseg delodajalca, medtem ko je zaskrbljujoče, da je 14% vprašanim vseeno glede posegov delodajalcev v zasebnost delojemalca. Kar skupno 37% vprašanih se strinja s posegi v zasebnost posameznika med delovnim časom. Za natančnejšo analizo bi bilo potrebno dodatno preveriti nivoje delovnih mest anketirancev. S tem bi dobili odgovore oziroma mnenja posameznikov ali ti izhajajo iz dejanske nezavednosti ali iz službenih potreb (vodstveni kader).

Graf 16: Nadzor delodajalca nad aktivnostmi zaposlenega med delovnim časom od elektronske pošte, brskanja po internetu, telefona, gibanja.. se mi zdi nedopusten.



Na vprašanje ali je moja zasebnost na delovnem mestu s strani delodajalca vedno bolj ogrožena je 26% anketirancev odgovorilo, da se s tem strinjajo. Takih, ki se s tem popolnoma strinjajo pa je 10%. Vzporedno bi lahko omenili, da se ta ugotovitev ujema z odstotkom anketirancev (7%), kateri so bili s strani predstavnikov delodajalcev opozorjeni na prekomerno brskanje po spletu. Kljub temu, da se anketiranci zavedajo pomena zasebnosti na delovnem mestu, pa je izredno velik delež (48%) tistih, kateri menijo, da ni nevarnosti za vdor delodajalca ali pa se s tem sploh ne strinjajo (12%). Te deleže v odstotkih lahko razumemo tudi kot nezavedanje vedno večjega pritiska in nadzora delodajalcev nad delojemalci ali pa tudi kot naivno podcenjevanje nevarnosti, katera nas lahko v bližnji prihodnosti izredno prizadene.

Graf 17: Moja zasebnost na delovnem mestu je s strani delodajalca vedno bolj ogrožena.



8.2 Sklepna misel

V nadaljevanju naloge bom verificirala postavljene hipoteze in podala sklepne misli. S ciljem doseganja večje preglednosti bodo posamezni vsebinski sklopi ločeni.

Teza 1: Pojma zasebnost in pravica do zasebnosti kljub obširnim znanstvenim delom še vedno nista enoznačno predstavljena ampak njuna različna razlaga izhaja iz naslova geografskega in družbenega sveta.

Ena najkompleksnejših nalog v zvezi s pravico do zasebnosti je njena jasna in nedvoumna definicija. Ko razpravljamo o pravici do zasebnosti govorimo o obsegu te pravice in takoj se postavi vprašanje ali je zasebnost sploh pravica ali gre morda le za interes. Če pa govorimo o interesu, se takoj pojavi problem določevanja minimalnega vendar absolutnega standarda zaščite. Pravica do zasebnosti je kljub pogostemu določevanju, da je *"meja, do katere družba lahko vdre v posameznikove zadeve"* problem, ki pa je večdimenzionalen pojem. S to večdimenzionalnostjo ločimo:

- informacijsko zasebnost – navezuje se na obdelavo in uporabo osebnih podatkov in predstavlja možnost posameznika, da obdrži podatke in informacije o sebi, ker ne želi, da bi bili z njimi seznanjeni drugi, znana je tudi kot varstvo osebnih podatkov;
- zasebnost telesa – posameznika ščiti pred invazivnimi posegi v telo posameznika;
- zasebnost osebnosti – nanaša se na svobodo misli, opredelitev in izražanja;
- zasebnost komunikacij – ščiti posameznika pred posegi v njegovo komunikacijsko zasebnost ne glede na obliko komunikacijskih sredstev;
- zasebnost v prostoru – predstavlja možnost, da je posameznik lahko sam, fizično ločen od ostalih ljudi in tako ščiti posameznika v njegovih prostorih, kar zajema npr. preiskovanje in (video) nadzorovanje njegovih domačih in službenih prostorov.

Definiranje pravice do zasebnosti oziroma njenega obsega je torej lahko precej arbitrarno in je odvisno kdo jo razlaga. Gre bolj za regulacijo posegov v zasebnost, kot pa za določitev neke absolutne meje, ki je ni dovoljeno prestopiti. Posledica tega je zaostajanje prava nasproti razvoju tehnologije, ki omogoča nove in nove posege v zasebnost in se tudi hitreje prilagaja potrebam v družbi. Načeloma je meja posameznikove pravice do zasebnosti omejena s pravicami drugih. Pri iskanju meje se tehta med interesom posameznika oziroma družbe. Ker pa se družbena sfera vedno bolj širi v škodo posameznikovega intimnega prostora in velja, da je zasebnost nujen element kakovostnega življenja v družbi, postaja pravica do zasebnosti v Evropi vedno bolj ustavna temeljna pravica. Hkrati pa je varstvo zasebnosti tudi eden izmed pomembnih elementov sodobne demokratične države.

Teza 2: V EKČP in Lizbonski pogodbi so zaradi zgodovinskega razvoja človekove pravice zapisane kot pravice, vendar so kljub temu Evropska ustavna sodišča vključno z ESČP polno zaposlena z reševanjem pritožb kršenja pravic, medtem ko se v ZDA to rešuje skozi sodno prakso na vseh nivojih sodišč.

V večini evropskih držav je zasebnost temeljna človekova pravica zapisana v ustavah. Prav tako je področje zasebnosti dodatno urejeno z vsebinskimi zakoni in vzpostavljena so enotna merila za javni kot tudi zasebni sektor. V ZDA pa pravica do zasebnosti ni nikjer izrecno navedena, Vrhovno sodišče je leta 1965 le priznalo obstoj ustavne pravice. Hkrati pa ameriška praksa zasebnosti ne dojema zgolj pravico biti sam ampak jo povezuje z avtonomijo posameznika.

Zakaj ta razlika? Ameriška ustava je prva pisana ustava v sodobni zgodovini (leta 1787) in je tudi najstarejša veljavna ustava na svetu. Ustava temelji na načelu ljudske suverenosti in zvezne ureditve. Človekove pravice v ameriški ustavi niso izrecno urejene, ampak to področje urejuje deset amandmajev, sodno varstvo ustave pa je poverjeno Vrhovnemu sodišču ZDA. Korenine segajo v leto 1803, za razvoj ustavnega sodstva je bila najpomembnejša zadeva *Marbury v. Madison* (1803), ki je dala ameriškemu vrhovnemu sodišču priložnost za sodno presojo neskladnosti zakona z ustavo. Vrhovno sodišče je sprejelo odločbo (na pobudo) ko je ugotovilo neustavnost zakona, kljub temu da za to ni bilo pristojno - ustava mu tega ni dovoljevala - ker pa je iz svoje prakse ugotovilo, da to mora storiti, je to storilo. Takšna pristojnost se je postopoma vendarle uveljavila, čeprav se je naslednja takšna zadeva pojavila pred tem sodiščem šele leta 1857 (na podoben način je presoјalo čez 50 let).

V ZDA o ustavno pravnem vprašanju lahko odloča vsak sodnik, samo z učinkom za tisto zadevo (ne zoper vse). Ustavne zadeve presoјajo vsa sodišča splošne pristojnosti v povsem rednem postopku. Odločitve praviloma učinkujejo le *inter partes* (samo za konkretno zadevo). Odločitev sodišča o neustavnosti zakona je praviloma retroaktivna. Z učinkom zoper vse, pa lahko odloči le Vrhovno sodišče ZDA. Vrhovno sodišče ZDA letno obravnava približno 100 primerov.

V Evropi velja obdobje po letu 1920 za mejnik nastanka modernih evropski ustav. Po zaslugi avstrijskih pravnih teoretikov Adolfa Merkla in Hansa Kelsna je bilo ustanovljeno Ustavno sodišče, z izključno pristojnostjo za presojo ustavnosti zakonov, izhajalo pa je iz načela kontrole izvršilne in zakonodajne veje oblasti.

Naslednje pomembno obdobje so bila sedemdeseta leta, kot reakcija na prejšnje diktatorske režime. Posebnost je bila uvedba sodne presoje ustavnosti leta 1963 v tedanji Jugoslaviji, po avstrijskem oziroma po nemškem vzoru, saj tedanji socialistični sistemi v načelu niso bili združljivi z institutom sodne presoje ustavnosti. Zadnje največje uvajanje ustavno sodne presoje so bila devetdeseta leta. Bistvo evropskega ustavnega sistema je njegovo načelo prvenstva ustave z načelom prvenstva parlamenta. Ta model uvaja samo eno institucijo (Ustavno sodišče) v državi, ki skrbi za varstvo ustavnosti in zakonitosti in za varstvo pravic in to lahko stori z učinkom za vse. Ustavne zadeve presoјajo posebna ustavna sodišča s

posebej kvalificiranimi sodniki ali vrhovna sodišča splošne pristojnosti oziroma njihovi posebni oddelki. Gre za koncentrirano ustavnosodno presojo v posebnem postopku. Odločitve imajo praviloma učinek *erga omnes* (za vse). Za ustavno presojo na Ustavnem sodišču mora pobudnik ustavne presoje izčrpati vse pravne vire.

Bistvena razlika med obema sodnima sistemoma je v tem, da si ameriški sodniški sistem zadeve izbere; evropski sistem mora obravnavati vse vložene zadeve. Kar je tudi razlog za zasičenost z zadevami.

Teza 3: Razvoj zasebnosti na področju odnosa delodajalec – delojemalec v ZDA, gre v smeri zaostrovanja in omejevanja ter zmanjševanja pravic delojemalcev, medtem ko se v Evropi nadaljuje trend povečevanja obsega pravic.

Pri vprašanju zasebnosti na delovnem mestu prihaja do trka lastninske pravice delodajalca in pravice do zasebnosti zaposlenega. Evropska pravna praksa se je postavila na stališče, da lastninska pravica ne prevlada samodejno nad pravico do zasebnosti, kar pomeni, da je pravico do zasebnosti potrebno (vsaj do določene mere) spoštovati tudi na delovnem mestu. Seveda pa je jasno, da tudi pravica do zasebnosti ni absolutna in tudi ta ne more prevladati nad lastninsko pravico delodajalca. Pomembni pa so tudi družbeni in psihološki vidiki. Pretiran nadzor namreč lahko omejuje kreativnost, motivacijo in lojalnost zaposlenega, zato na določeni točki lahko postane celo kontraproduktiven.

Kljub temu dejstvu zaposlovalci izvajajo nadzor nad zaposlenimi na delovnem mestu, predvsem nadzor njihovih elektronskih komunikacij. Razlogi za nadzor so različni, večinoma podjetja želijo preprečiti odtekanje poslovnih skrivnosti, neprimerno obnašanje zaposlenih - predvsem zlorabo službenega časa in računalnika za neslužbene namene - ter zagotoviti varnost informacijske infrastrukture podjetja (zmanjšati število okužb z virusi in zlonamerno kodo, preprečiti vdore, itd.). Te posege še vzpodbuja agresivno oglaševanje izdelkov za nadzor komunikacijske infrastrukture s strani proizvajalcev in prodajalcev tovrstne opreme, nadzorna tehnologija katera je vedno cenejša in vedno bolj sofisticirana pa je pogosto predstavljena kot magična paličica za rešitev vseh problemov v podjetju.

Pobudniki posegov v Evropi pogosto navajajo "ameriški pristop" k nadzorovanju zaposlenih na delovnem mestu, ki temelji na dejstvu, da zaposleni na delovnem mestu uporabljajo opremo, ki je last delodajalca, v delovnem času pa je plačan s strani delodajalca, zato službenih komunikacijskih sredstev in službenega časa ne sme zlorabljati v zasebne namene. A zakonodaja v Evropi se na tem področju bistveno razlikuje od zakonodaje v ZDA. Evropsko pravo namreč zaposlenega na delovnem mestu ne vidi zgolj kot samo delavca, pač pa predvsem kot človeško bitje oziroma posameznika s človekovimi pravicami. Vsi posegi v zasebnost na področju Evropske unije morajo imeti ustrezno zakonsko podlago, hkrati pa morajo biti tudi nujni v demokratični družbi oziroma sorazmerni. In ravno vprašanja sorazmernosti, ter soglasja zaposlenega oziroma prisile delodajalca so tista, ki bodo v prihodnosti zakoličila obseg pravice do zasebnosti na delovnem mestu.

Po drugi strani pa mora sodobna država zaradi kompleksnosti življenja izvajati nadzor nad državljani ob hkratnem vedenju da liberalne demokratične vrednote visoko cenijo človekovo zasebnost. V demokratični družbi mora biti doseženo pravo razmerje med stopnjo nadzora in zasebnostjo posameznika. Varnost je človekova izjemno visoko uvrščena potreba, človekova svoboda pa temeljna moralna vrednota in osmišljanje pravne države. Vsekakor sta v okvirih vladavine prava v medsebojni soodvisnosti, se dopolnjujeta in dograjujeta, v primeru njune konfliktnosti odloča pravo kot pripomoček pri reševanju spora. Toda to je mogoče le, ko obe stranki v sporu pristajata, da bosta konflikt rešili po pravni poti oziroma takrat, ko so temeljne družbene vrednote sprejete od večine državljanov kot primerne, ustrezne in pravične. Hkrati se je potrebno tudi zavedati, da v demokratičnih državah obstajajo tudi kriminalne združbe, ki pravnega reda ne spoštujejo in ne upoštevajo. Takrat mora država z vsemi svojimi institucijami, da bi zavarovala ljudi in njihovo premoženje ter ohranila človekovo dostojanstvo, delovati represivno in preventivno, tudi tako, da posega v sicer ustavno varovane človekove pravice, med njimi v zasebnost, ki sodi v fizično in duhovno sfero posameznika. Pri tem varnostni interes ni v hierarhičnem odnosu do človekove svobode. Z upoštevanjem zakonskih omejitev je to, zaradi uveljavljanja človekovih pravic, v interesu varnosti in človekove svobode. Neprestano pa je nujen nadzor nad spoštovanjem človekove fizične in duhovne zasebnosti. Nobeno sklicevanje na učinkovitost organov odkrivanja in pregona ne more biti opravičilo za kršitev človekovih pravic. Četudi gre za t.i. boj proti terorizmu. Ravno boj proti terorizmu je s strani države najboljše opravičilo za vedno večja pravna odobranja državnih posegov v zasebnost posameznika. Tej praksi posegov pa v času gospodarske krize sledijo še podjetja. Zasebnost posameznika je vedno kršena in hkrati postaja tržno blago z enormno vrednostjo. Evropa s svojo pravno ureditvijo po eni strani daje vedno večjo težo zaščiti zasebnosti, po drugi strani pa evropske institucije pristajajo na diktate ZDA in pod krinko boja proti terorizmu dajejo prednost varnosti in omejujejo svobodo in zasebnost svojih državljanov.

LITERATURA IN VIRI

SAMOSTOJNE PUBLIKACIJE

1. AGRE, E. Philip (2001). *Technology and Privacy*. The New Landscape, London.
2. ARENDT, Hannah (1958/1995). *Vita Activa*. Krtina, Ljubljana.
3. BAŠIČ, H. Sandra (1996). *Javnost in množični mediji: od dekonstrukcije k rekonstrukciji*. Doktorska disertacija, FDV, Ljubljana.
4. BOGATAJ, Maja (2003). *Internet in pravo*. Pravna fakulteta, Ljubljana.
5. BUTLER, Robert (1998). *Ilustrirana zgodovina gestapa*. Style Maxima, Murska Sobota.
6. CATE, H. Fred (1997). *Privacy in the Information Age*, Brookings Institution Press, Washington.
7. CVETKO, Aleksej (1999), *Varovanje zasebnosti v delovnih razmerjih*. Gospodarski vestnik, Ljubljana.
8. ČEBULJ, Janez (1992). *Varstvo informacijske zasebnosti v Evropi in Sloveniji*. Inštitut za javno upravo pri Pravni fakulteti, Ljubljana.
9. ČEBULJ, Janez (2002). 38. člen (varstvo osebnih podatkov). *Komentar ustave Republike Slovenije*. Str. 408 - 416. FDS, Ljubljana.
10. ČRNČEC, Damir (2009). *Obveščevalna dejavnost v informacijski dobi*. Defensor, Ljubljana.
11. DVORŠAK, Helena (2008), *Kazensko pravno varstvo zasebnosti na delovnem mestu*. Specialistična naloga, FVV, Ljubljana.
12. EPIC in Privacy International, (2002). *Privacy & Human Rights 2002: An International Survey of Privacy Laws and Developments*. EPIC, Washington.
13. ETZIONI, Amitai (1999). *The Limits of Privacy*. Basic Books, ZDA.
14. FIRBAS, Gregor (2009). *Varovanje zasebnosti nekoč in danes*. Diplomsko delo, FDV, Ljubljana.
15. HABERMAS, Jürgen (1962/1989). *Strukturne spremembe javnosti*. Založba ŠKUC in Znanstveni inštitut Filozofske fakultete, Ljubljana.

16. ILIČ, Miloš (1978). *Sociologija kulture i umetnosti*. Naučna knjiga, Beograd.
17. JAMBREK, Peter, PERENIČ, Anton, URŠIČ, Marko (1998). *Varstvo človekovih pravic: razprave, eseji in dokumenti*. Mladinska knjiga, Ljubljana.
18. KLEMENČIČ, Goran (2002). 37. člen (varstvo tajnosti pisem in drugih občil). *Komentar ustave Republike Slovenije*. Str. 391 - 408. FDS, Ljubljana.
19. KOVAČIČ, Matej (2003). *Zasebnost na internetu*. Mirovni inštitut, Inštitut za sodobne družbene in politične študije, Ljubljana.
20. KOVAČIČ, Matej (2006). *Nadzor in zasebnost v informacijski družbi: filozofski, sociološki, pravni in tehnični vidiki nadzora in zasebnosti na internetu*. FDV, Ljubljana.
21. KUHELJ, Alenka (2004). *Varstvo do pravice zasebnosti, veroizpovedi in svobodnega izražanja v pravu Sveta Evrope*. Fakulteta za upravo, Ljubljana.
22. KUSTEC, L. Simona (2006). *Poseganje države v civilno družbo: Javnopolitična perspektiva*. FDV, Ljubljana.
23. LAMPE, Rok (2003). *Pravica do zasebnosti, zagovor njene široke implementacije*. Doktorska disertacija, Pravna fakulteta, Maribor.
24. LAMPE, Rok (2004). *Sistem pravice do zasebnosti*. Bonex založba, Ljubljana.
25. LAURANT, Cedric (2003). *Privacy&HumanRights*. EPIC, Washington.
26. PERENIČ, K. Lidija (2009). *Varstvo osebnih podatkov in mediji*. IP-RS, Ljubljana.
27. PRAPROTNIK, Darja (2006). *Varovanje podatkov in zasebnosti na internetu*. Magistrsko delo, EF, Ljubljana.
28. SOLOVE J. Daniel (2009), *Understanding Privacy*. Harvard University Press, Cambridge.
29. SPLICHAL, Slavko (2002). *Principles of Publicity and Press Freedom*. Rowman & Littlefield Publishers, Oxford.
30. SYKES, J. Charles (1999). *The End of Privacy*. St. Martin's Press, New York.
31. ŠELIH, Alenka (1999). Zasebnost kot človekova pravica v pogojih informacijske družbe. V *Posvet ob 50-letnici Splošne deklaracije OZN o človekovih pravicah*, Slovenska akademija znanosti in umetnosti; str. 41 – 51.

32. ŠTURM, Lovro (2002). *Komentar ustave Republike Slovenije*. FDS, Ljubljana.
33. TERŠEK, Andraž (2006). *Svoboda medijev in varstvo zasebnosti: Kritika dveh precedensov, predlog razvrstitve »javnih oseb« in predlog ustavnopravnih standardov*. Pravna fakulteta, Ljubljana.
34. THOMSON, B. John (1990). *Ideology and Modern Culture: critical social theory in the era of Mass Communications*. Stanford University Press, Stanford.
35. TURKINGTON, C. Richard in ALLEN, L. Anita (1999). *Privacy Law: Cases and Materials*. West Group, ZDA.
36. TURKINGTON, C. Richard in ALLEN, L. Anita (2002) *Privacy Law: Cases and Materials*. West Group, ZDA.
37. WHITAKER, Reg (1999). *The End of Privacy*. The New Press, New York.

ČLANKI

1. BENNET, J. Colin (2001). Convergence Revisited: Toward a Global Policy for the Protection of Personal Data? *Technology and Privacy: The New Landscape*, Cambridge: MIT Press, str. 99-123.
2. BERLIN, Isiah (1992). Dva koncepta svobode. *Sodobni liberalizem*. Krt, str. 69 – 89.
3. CAZENEUVE, George (1963). Sociologija radia i televizije. *Kulturni život*, str. 720—731.
4. DAVIES, G. Simon (2001). Re-engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Comoditv. *Technology and Privacy*. Cambridge: MIT Press , str. 143-165.
5. DODIG, C. Gordana, HORNIAC, Virginia (2005). Good to Have Someone Watching Us from a Distance: *Privacy vs. Security at the Workplace*. Enschede: Sixth International Conference of Computer Ethics CEPE, str. 10.
6. FLAHERTY, H. David (2001). Controlling Surveillance. *Technology and Privacy. The New Landscape*. MIT Press London, str. 167–192.
7. KLEMENČIČ, Goran. 2001. Varstvo elektronske zasebnosti. *Internet in pravo*. Pasadena, str. 129 - 191.

8. KLEMENČIČ, Goran (2004). Internet in pravica do zasebnosti. *Internet in pravo*. Pravna fakulteta, str. 101-141.
9. KUHELJ, Alenka (2010). Izmenjava osebnih podatkov v letalskem prometu med EU in ZDA. *Revija pravnik*. Št.: 5-6/2010, str. 365 – 389.
10. MAYER-SCHONBERGER, Viktor (2001). Generational Development of Data Protection in Europe. *Technology and Privacy: The New Landscape*. Cambridge: MIT Press, str. 219 - 241.
11. PETERS, John (1993). Distrust of Representation: Habermas on the Public Sphere. *Media, Culture and Society*, 15, 4, str. 541 - 571.

PRAVNI VIRI

1. American Convention on Human Rights. Dostopno na:
<http://www.cidh.oas.org/DefaultE.htm>
2. Evropska konvencija o človekovih pravicah. Dostopno na:
http://www.echr.coe.int/NR/rdonlyres/200393FD-EAD3-434F-BD46-41BE147A18E9/0/SVN_CONV.pdf
3. Kazenski zakonik (KZ-1). Ur. 1. RS. 55/2008. Dostopno na:
http://zakonodaja.gov.si/rpsi/r00/predpis_ZAKO5050.html
4. Zakon o Informacijskem pooblaščenju (ZinfP). Ur. 1. RS. 113/2005. Dostopno na:
http://zakonodaja.gov.si/rpsi/r08/predpis_ZAKO4498.html
5. Zakon o kazenskem postopku (ZKP-UPB3). Ur. 1. RS. 8/2006. Dostopno na:
http://zakonodaja.gov.si/rpsi/r07/predpis_ZAKO4787.html
6. Zakon o spremembah in dopolnitvah Zakona o kazenskem postopku (ZKP-J). Ur. 1. RS. 77/2009. Dostopno na:
http://zakonodaja.gov.si/rpsi/r08/predpis_ZAKO5438.html
7. Zakon o varstvu osebnih podatkov (ZVOP- 1-UPBI). Ur. 1. RS. 94/2007. Dostopno na:
http://zakonodaja.gov.si/rpsi/r05/predpis_ZAKO5245.html

SPLETNI VIRI

1. ACLU (2003). *Privacy in America: Electronic Monitoring*. Dostopno na:
<http://www.aclu.org/technology-and-liberty/privacy-america-electronic-monitoring>

2. BACKES, Michael, DURMUTH, Markus, UNRUH, Dominique (2008). *Compromising reflections or how to read LCD monitor s around the corner*. Dostopno na: <http://crypto.m2ci.org/unruh/publications/reflections.pdf>
3. BANISAR, David (1999). *Privacy & Human Rights*. Dostopno na: <http://www.privacyinternational.org/survey/index99.html>
4. BATAGELJ, Zenel (1997). *Direktni marketing, oglaševanje in internet*. Dostopno na: <http://www.cati.si/papers/zbyymm0003.html>
5. EU zakonodaja (2003). *Varstvo osebnih podatkov – povzetek*. Dostopno na: http://europa.eu/legislation_summaries/information_society/data_protection/l14012_sl.htm
6. Informacijski pooblaščenec. Dostopno na: <http://www.ip-rs.si>
7. Informacijski pooblaščenec (2010). *Letno poročilo Informacijskega pooblaščenca za leto 2009*. Dostopno na: <http://www.ip-rs.si/publikacije/porocila>
8. Informacijski pooblaščenec (2010). *Safe Harbor*. Dostopno na: <https://www.ip-rs.si/varstvo-osebnih-podatkov/obveznosti-upravljavcev/iznos-osebnih-podatkov-v-tretje-drzave/safe-harbor/>
9. KOVAČIČ, Matej (2009). *Komentar določb novele Zakona o kazenskem postopku (ZKP-J), ki opredeljujejo nekatere posege v informacijsko zasebnost*. Dostopno na: <http://hr-cjpc.si/pravokator/index.php/2009/10/21/novela-zakona-o-kazenskem-postopku-posegi-v-komunikacijsko-zasebnost/>
10. MARKOVČ, Marijana (2011). *Spletna anketa*. Dostopno na: <http://fluidsurveys.si/s/zasebnost/>
11. Moj Micro (2010). *Legalni hekerji*. Dostopno na: http://www.mojmikro.si/v_srediscu/razkritje/legalni_hekerji
12. Povzetki zakonodaje EU iz področja varovanja zasebnosti. Dostopno na: http://europa.eu/legislation_summaries/information_society/data_protection/l14012_sl.htm
http://europa.eu/legislation_summaries/information_society/data_protection/l14012_sl.htm
13. SCHULMAN, Andrew (2001). *Extent of Systematic Monitoring of Employee E-mail and Internet Use*. Dostopno na: <http://www.diogenesllc.com/internetmonitoring.pdf>

14. Varuh človekovih pravic (2010). *Letno poročilo Varuha človekovih pravic za leto 2009*. Dostopno na: <http://www.varuh-rs.si/publikacije-gradiva-izjave/letna-porocila>
15. ZETTER, Kim (2004a). *Outsourcing: Danger to Privacy*. Wired News. Dostopno na: <http://www.wired.com/techbiz/media/news/2004/02/62356>
16. ZUPANČIČ, Matic (2006). *Zasebnost na delovnem mestu*. Monitor, Ljubljana. Dostopno na: <http://www.monitor.si/clanek/zasebnost-na-delovnem-mestu/>

PRILOGA

PRILOGA 1: Anketa

Spoštovani!

Sem Marijana Markovc, absolventka Fakultete za Upravo in pripravljam diplomsko nalogo z naslovom **Evropski in ameriški koncept zasebnosti**. V ta namen izvajam raziskavo o stališčih do zasebnosti med uporabniki. Prosim, da si vzamete nekaj trenutkov in izpolnite spodnjo anketo.

Zaupnost individualnih podatkov je zagotovljena, saj je anketa anonimna - Vaši odgovori bodo obravnavani z največjo mero zaupnosti in se bodo uporabili samo za namen omenjene diplomske naloge.

Za sodelovanje se Vam najlepše zahvaljujem.

Spol:

- a. Moški
- b. Ženski

Starost:

- a. Do 30 let
- b. 30 – 50 let
- c. Nad 50 let

Delovna doba:

- a. do 15 let
- b. 15 – 25 let
- c. Nad 25 let

V katerem sektorju ste zaposleni (obkrožite ustrezno)?

- a. nezaposlen
- b. gospodarstvo
- c. javna uprava

Kako pomembna se vam zdi pravica do zasebnosti posameznika (obkrožite ustrezno)?

- a. kaj je to?
- b. ni pomembna
- c. manj pomembna
- d. je pomembna
- e. je zelo pomembna

Katera pravica se vam zdi pomembnejša (obkrožite ustrezno)?

- a. pravica do zasebnosti
- b. pravica do varnosti
- c. nimam mnenja

Ali na delovnem mestu uporabljate službeni računalnik za brskanje po internetu? (obkrožite ustrezno)

- a. da
- b. ne
- c. občasno

Ali se na internetu ukvarjate z naslednjimi aktivnostmi (obkrožite ustrezno):

- | | | |
|---|----|----|
| a. Berem in pošiljam elektronsko pošto | DA | NE |
| b. Pišem blog | DA | NE |
| c. Sodelujem na družabnih spletnih straneh: Twitter, Facebook | DA | NE |
| d. Nakupujem preko spleta | DA | NE |
| e. Brskanje po internetu uporabljam izključno v službene namene | DA | NE |

Ali ste pri zasedbi delovnega mesta podpisali dogovor o omejitvi vaše zasebnosti med službenim časom (obkrožite ustrezno)

- a. da
- b. ne
- c. ne vem

Ali menite, da vam delodajalec nadzoruje vaše aktivnosti na vašem računalniku?

- a. da
- b. ne
- c. ne vem

Ali ste kdaj pri uporabi službenega računalnika opazili nepričakovano in nerazumljivo upočasnjeno delovanje le tega?

- a. nikoli
- b. občasno
- c. redno
- d. nisem pozoren-a

Ali menite, da vam lahko delodajalec pregleduje vsebino službene elektronske pošte?

- a. da
- b. ne
- c. ne vem

Ali ste pri pogovoru z nadrejenimi mogoče opazili, da oni kakorkoli poznajo vsebino vaših elektronskih sporočil?

- a. da
- b. ne
- c. nisem pozoren-a

Ali ste bili kdaj opozorjeni na prekomerno brskanje po internetu?

- a. da
- b. ne
- c. ne vem

Kdo je po vašem mnenju najbolj odgovoren za varovanje vaše zasebnosti na delovnem mestu?

- a. jaz sam
- b. delodajalec
- c. država z regulativno zakonodajo

Nadzor delodajalca nad aktivnostmi zaposlenega med delovnim časom od elektronske pošte, brskanja po internetu, telefona, gibanja.. se mi zdi nedopusten poseg v mojo zasebnost:

- a. se sploh ne strinjam
- b. se ne strinjam
- c. mi je vseeno
- d. se strinjam
- e. se popolnoma strinjam

Moja zasebnost na delovnem mestu je s strani delodajalca vedno bolj ogrožena:

- a. se sploh ne strinjam
- b. se ne strinjam
- c. mi je vseeno
- d. se strinjam
- e. se popolnoma strinjam

Zahvaljujem se Vam za sodelovanje in izpolnjeno anketo!