UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

MATJAŽ DREV

MNOŽIČNI NADZOR V SODOBNI DRUŽBI

MAGISTRSKO DELO

Ljubljana, 2010

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

MATJAŽ DREV

MENTOR: izr. prof. dr. Andrej Lukšič

MNOŽIČNI NADZOR V SODOBNI DRUŽBI

MAGISTRSKO DELO

Ljubljana, 2010

Zahvaljujem se mentorju izr. prof. dr. Andreju Lukšiču za idejne spodbude in kritičen pretres magistrskega dela.

Zahvalo dolgujem tudi dr. Mateju Kovačiču za številne strokovne nasvete o nadzoru in še bolj številne nasvete o tem kako se izogibati nadzoru.

MNOŽIČNI NADZOR V SODOBNI DRUŽBI

POVZETEK

Magistrsko delo je sestavljeno iz štirih vsebinskih sklopov, ki obravnavajo različne vidike družbenega nadzora in zasebnosti. V prvem delu sta prikazana razvoj in delovanje družbenega nadzora. Pri tem posebno mesto zavzema panoptikon, ki kljub vse pogostejšim kritikam še vedno predstavlja osnovno matrico za razumevanje nadzora v sodobni družbi. V drugem delu so prikazane nekatere najpomembnejše tehnologije sodobnega družbenega nadzora. Tretji del obsega večrazsežno analizo koncepta zasebnosti, ki vključuje tudi poizkus opredelitve pravice do zasebnosti in kratek oris razvoja te pravice znotraj pravnega reda zahodnega sveta. V četrtem delu pa je predstavljena pravna ureditev pravice do zasebnosti v ZDA, EU in Sloveniji. Magistrsko delo skuša torej sistematično prikazati zgodovinsko pogojeno razmerje med nadzorom in zasebnostjo, ki vključuje družboslovne, pravne in tehnične vidike, ter ob tem nakazati smer razvoja pravice do zasebnosti v postmoderni družbi.

Ključne besede: družbeni nadzor, tehnologija nadzora, zasebnost, pravica do zasebnosti

MASS SURVEILLANCE IN MODERN SOCIETY

ABSTRACT

This Master's thesis consists of four main chapters that cover different aspects of social control and privacy. First chapter describes evolution and functioning of social control. Special attention is given to panopticon, which despite ever increasing criticism still remains fundamental model for interpretation of social control in contemporary society. Second chapter reviews some of the foundamental technologies of contemporary social control. Third chapter represents multidimensional analysis of the concept of privacy. This also includes an attempt to define the right to privacy and to install this right within broader context of western legal order. Fourth chapter is a more thorough attempt to analyse the right to privacy within the legal systems of United States, European Union and Republic of Slovenia. This Master's thesis therefore attempts to systematically represent historicaly conditioned relation between social control and privacy that includes social, legal and technical aspects, and at the same time indicate direction of development of the right to privacy in postmodern society.

Key words: social control, technology of control, privacy, right to privacy

KAZALO

KAZALO SLIK IN TABEL

1 UVOD

Od sedemdesetih let 20. stoletja dalje se v javnosti pogosto izpostavlja problematika razmerja med nadzorom in zasebnostjo. To ne preseneča, saj gre za obdobje izjemnega razcveta informacijske tehnologije, ki je s svojimi učinki zaznamovala domala vse družbene sfere. Človek je postal obkrožen z množico elektronskih naprav, ki po eni strani omogočajo delovanje sodobne družbe, po drugi strani pa zaradi vgrajenega nadzornega potenciala predstavljajo nevarnost posameznikovi zasebnosti in intimi. Na nevarnost krčenja zasebne sfere so najprej opozarjali ozaveščeni posamezniki, kasneje tudi aktivisti. 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 nadzorom 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.

Analiza razmerja med nadzorom in zasebnostjo predstavlja osrednji del magistrske naloge. Prvi del besedila je namenjen nadzoru. Sodeč po številnih zgodovinskih, sociooloških, filozofskih, antropoloških in drugih virih, je družbeni nadzor star toliko kot človeštvo. Družbeni nadzor v svoji osnovni obliki predstavlja sistem regulacije, ki omogoča, da kakršnakoli oblika človeške družbe sploh preživi. Zato nadzor najprej obstaja v neformalni obliki, izvaja pa se s pomočjo nagrajevanja ali kaznovanja (ne)sprejemljivih vedenjskih vzorcev. Šele z razvojem hierarhičnih organizacij in jasno določenih pravil vedenja se vzpostavi formalni nadzor, ki s pomočjo represije ohranja in krepi določen pravni red.

V predmodernih družbah je prevladoval neformalni nadzor. V nacionalnih državah z razvitim birokratskim aparatom, industrijo in velemesti, pa se je bistveno okrepil formalni nadzor. Zanj je bila značilna določena sistematičnost in doslednost. Sprva ga je izvajala država, služil pa je ohranjanju obstoječih družbenih razmer. V drugi polovici dvajsetega stoletja se je zaradi razcveta informacijske tehnologije na področju nadzorovanja zgodila manjša revolucija. Nadzor se je po eni strani avtomatiziral in s pomočjo čedalje večjega števila elektronskih naprav razlil po celotnem

družbenem tkivu. Po drugi strani pa se je prav zaradi tega zanj začel zanimati komercialni sektor, ki je v kopičenju in analizi podatkov o potrošnikih videl sredstvo za večanje profita. Formalni nadzor tako ni izvajala več le država, ampak tudi komercialni sektor.
Ob tem se je zgodil še en pomemben preskok. Če se je nadzor v preteklosti večinoma osredotočal na določeno število posameznikov, je z razvojem računalnika, telefonije, interneta in drugih omrežji postal množičen. Nadzorovani niso bili le »sumljivi« posamezniki, ampak tako rekoč skoraj vsi prebivalci neke države. Nadzor zato ni bil več rezerviran le za določene kategorije ljudi, pač pa je zaobjel celotno populacijo. Tak nadzor je še posebej učinkovit, ker je prikrit, tako rekoč neviden in ker se v javnosti prikazuje kot nekaj koristnega, zato ljudje čedalje pogosteje pristajajo na nadzor prostovoljno. Takšna »prostovoljnost« je značilna predvsem za potrošniški sektor, ki ima mnogo bolj »hinavski obraz« kakor državni »represivni« nadzor. Zato ne preseneča, da je pravna regulacija nadzora v zasebnem sektorju bistveno slabša kot v javnem sektorju.

V drugem delu naloge je pozornost namenjena zasebnosti. Raziskovanje zasebnosti je mogoče začeti iz dveh ločenih pozicij. Zasebnost se lahko razume kot nekaj univerzalnega ali kot nekaj kulturno pogojenega. Je pa seveda prav tako mogoča nekakšna sinteza in sicer pod predpostavko, da izvor zasebnosti korenini v biološki in psihološki predispoziciji ljudi, pojavne oblike pa so odvisne od konkretnih družbenih razmer. V skladu s takšno razlago je zametek zasebnosti sicer univerzalen, vendar pa je vsebina tega kar naj bi zasebnost bila odvisna predvsem od kulturnega konteksta. Vsekakor je zasebnost prisotna v kulturnih in filozofskih temeljih zahodne civilizacije. Delitev na javno in zasebno so poznali že stari Grki, čeprav pri njih zasebno ni imelo posebne vrednosti, ampak je služilo kot predpogoj mnogo bolj dragocene javne sfere, kjer je posameznik, če je imel to srečo, lahko bival med sebi enakimi in je zato bil svoboden. Delitev na javno in zasebno se je s številnimi spremembami vlekla skozi krščanski srednji vek v razsvetljenstvo. Vendar pa se je pravica do zasebnosti pojavila relativno pozno. Prvič je bila eksplicitno omenjena šele ob koncu 19. stoletja, svoje mesto med kodificiranimi človekovimi pravicami pa je dobila šele po drugi svetovni vojni. Kljub splošnemu priznanju pravice do zasebnosti v ustavah in zakonih večine držav in kljub številnim poizkusom definiranja, še danes ni popolnoma jasno kaj naj bi pravica do zasebnosti sploh bila.

V tretjem delu je pozornost namenjena 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. Analiza zakonodaje in sodne prakse ZDA in EU skuša prikazati kakšno je razmerje med nadzorom in zasebnostjo oziroma kako

je pravica do zasebnosti zavarovana. Ob primerjavi obeh pravnih sistemov je nemudoma opazno, da je v ZDA zasebnost varovana predvsem v razmerju do javnega (državnega) 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, ki ga je med prebivalci stare celine zasejala druga svetovna vojna.

V analizo je zajeta tudi pravna ureditev pravice do zasebnosti v Republiki Sloveniji, ki predstavlja značilen izraz »evropskega« pogleda na obravnavanje problematike zasebnosti. Čeprav je imela slovenska zakonodaja v prvih letih po osamosvojitvi določene pomanjkljivosti, je v zadnjih letih z novelami zakonov in s sprejemanjem evropskih direktiv dosegla stopnjo razvoja, ki je primerljiva z ostalimi razvitimi evropskimi državami.

2 DRUŽBENI NADZOR

Družbeni nadzor v svoji najosnovnejši obliki predstavlja temeljno funkcijo in običajno prakso katerekoli človeške skupine. Namenjen je vzpostavljanju in ohranjanju (samo)regulacije človeškega vedenja in delovanja, kar posledično omogoča preživetje družbenih skupin in skupnosti.

Upravičeno je mogoče sklepati, da je družbeni nadzor star toliko kot človeštvo. Seveda pa so se prakse in oblike nadzora skozi zgodovino spreminjale. Zato je v tem poglavju poleg poizkusa opredelitve pojma družbeni nadzor, pozornost namenjena tudi historičnemu pregledu razvoja družbenega nadzora. Če je bil za arhaične družbe značilen predvsem neformalen in relativno enostaven nadzor, velja za moderne družbe ravno nasprotno; prevladuje formalen in kompleksen nadzor.

Velik poudarek je namenjen analizi širših družbenih procesov, ki so na prehodu iz srednjega v novi vek močno zaznamovali razvoj praks družbenega nadzora. Novoveški nadzor je zato predstavljen skozi prizmo Foucaultove analize panoptikona (arhitekturnega osnutka popolnega zapora). Toda zadnja desetletja so predvsem zaradi bliskovitega razvoja in implementacije informacijske tehnologije prinesla bistvene spremembe tudi na področju družbenega nadzora, ki ga ni več mogoče učinkovito pojasnjevati s pomočjo panoptičnega modela. Zato se čedalje pogosteje pojavljajo novi teoretični koncepti in sheme »postpanoptičnega nadzora«, med katerimi je še posebej obetaven t.i. omrežni nadzor, ki deluje s pomočjo razpršenih, vendar medsebojno povezanih nadzornih točk.

V drugem delu poglavja pa je pozornost namenjena predstavitvi različnih tehnik in tehnologij sodobnega informacijskega nadzora, ki poleg »klasičnega« človeškega opazovanja uporablja predvsem video kamere, sisteme za avtomatsko prepoznavo različnih vzorcev, satelite, računalnike, prenosne telefone, internet in druga omrežja, biometrične metode, podatkovno profiliranje in druge s tehnologijo pogojene pristope.

2.1 POJMOVNA OPREDELITEV DRUŽBENEGA NADZORA

Beniger (v Kovačič 2006, 22) nadzor[1] definira kot *»usmerjen vpliv na zastavljen cilj«*. V skladu s

[1] Nadzor je v Slovarju slovenskega knjižnega jezika opredeljen kot *»sistematično pregledovanje, spremljanje poteka ali razvoja česa, zlasti določene dejavnosti; prizadevanje, skrb za pravilno ravnanje, vedenje, delo koga; prevlado in oblast nad nekom ali nečim«*. Ob tem Peruš (2007, 25) poudarja, da etimološki izvor besede nad-zor vsebuje težnjo po obvladovanju objekta ali subjekta. Nadzor tako ni zgolj nekaj pasivnega, kot na primer opazovanje, ampak že vsebuje poizkus nadvlade in manipulacije.

tako široko opredelitvijo nadzor ni značilen zgolj za ljudi, ampak se pojavlja tudi pri številnih drugih organizmih. Peruš (2007, 24) meni, da se enostavne oblike nadzora pojavljajo celo pri enoceličarjih.

Vendar pa se razprave o nadzoru osredotočajo na kompleksen nadzor, ki ga izvajajo ljudje. Pri tem je potrebno ločiti nadzor nad stvarmi, ki se izvaja v interakciji z okolico, ter nadzor nad ljudmi (Kovačič 2006, 22). To drugo vrsto nadzora Pečar (1988) imenuje »družbeni nadzor« in predstavlja enega temeljnih elementov sleherne človeške skupnosti. Lyon (2007, 13) družbeni nadzor (namesto angleškega izraza »social control« uporabi pojem »surveillance«, ki izvira iz francoskega glagola »surveiller«, kar pomeni »opazovati«) opredeljuje kot usmerjeno in načrtno spremljanje človeških ravnanj.

Družbeni nadzor, ki ga kriminološke, sociološke, politološke, pravne, psihološke in filozofske razprave[2] navadno razumejo kot sistem regulacije vedenja posameznikov in skupin s ciljem vzdrževanja nekega družbenega reda, se deli[3] na formalni in neformalni nadzor (Deflem 2007; Pečar 1988).

Formalni nadzor Lyon (2007, 14) definira kot usmerjeno, sistematično in rutinsko pridobivanje informacij o posamezniku, ki zasleduje točno določene cilje: vplivati na posameznika in usmerjati njegovo ravnanje v skladu s pričakovanji tistega, ki nadzor izvaja. Tak nadzor je v veliki meri opredeljen s specifičnimi protokoli in tehnikami, predstavlja pa enega osnovnih elementov vseh birokratskih organizacij (Giddens v Lyon 2007, 14).

Formalni nadzor se izvaja na podlagi prava, usmerjen pa je predvsem v regulacijo deviantnega vedenja s pomočjo formalnih sankcij (globe, zapor), ki jih izvaja država.

Formalni nadzor je mogoče nadalje razčleniti še na državni in institucionalizirani nedržavni nadzor (Pečar 1995). Državni nadzor s ciljem ohranjanja in utrjevanja obstoječega pravnega reda izvajajo državne institucije: policija, tožilstva, sodišča, zapori, bolnišnice, šole, centri za socialno delo, davčni uradi (Pečar 1988). Institucionalizirani nedržavni nadzor pa izvajajo institucije, ki so del privatnega sektorja: nevladne organizacije, družbe za zasebno varovanje, detektivske agencije,

[2] Deflem (2007) poudarja, da se je v sociooloških razpravah v obdobju pred 2. svetovno vojno, družbeni nadzor razlagalo v širšem smislu, ki je obsegal tako neformalni kot formalni nadzor. Po 2. svetovni vojni pa je zlasti v ZDA prišlo do idejnega premika v razumevanju družbenega nadzora, ki se ga je čedalje bolj enačilo s formalnim – državnim nadzorom.

[3] Delitev na formalni in neformalni družbeni nadzor je ustrezna za razumevanja delovanja nadzora v družbah 18. in 19. stoletja. V sodobnih »družbah nadzora« pa prihaja do čedalje pogostejšega brisanja mej med formalnim in neformalnim nadzorom, prav tako se pojavljajo nove vrste nadzora, ki jih ni več mogoče umestiti v eno ali drugo kategorijo. Ob tej delitvi obstajajo še nekatere druge. Mobbs (v Kašnik 2006, 10) deli nadzor na aktivni (primarni) in pasivni (sekundarni) nadzor. Pri aktivnem nadzoru je potrebno podatke šele pridobiti, npr. z uporabo prisluškovalnih naprav, prestrezanjem elektronske pošte ali z videonadzorom. Pri pasivnem nadzoru pa so podatki že na voljo, potrebno jih je le še analizirati, povezati in sestaviti v uporabno informacijo.

redarstva, čedalje pogosteje pa tudi podjetja[4], ki se ukvarjajo z zbiranjem in prodajo podatkov o posameznikih.

Neformalni nadzor je mnogo bolj spontan, poteka brez vpletanja države in ni neposredno utemeljen v pozitivnem pravnem redu. Izvaja se predvsem v okviru primarnih in sekundarnih družbenih skupin: v družini, med sorodniki, prijatelji, znanci, sošolci, sodelavci (Pečar 1991).

Tak nadzor temelji na sistemu vrednot, kulturnih norm, morale in običajev, ki jih posamezniki v procesu vzgoje ponotranjijo. Neformalni nadzor se z različno stopnjo intenzitete vrši v domala vseh družbenih skupinah, se pa seveda glede na posameznika, skupino in družbo razlikuje. Izvaja se s pomočjo nagrajevanja in kaznovanja. Med nagrade običajno sodi odobravanje ali hvaljenje nekega vedenja, med kazni pa neodobravanje, posmeh, kritika, grožnje, diskriminacija, včasih celo izključitev iz skupine.

V arhaičnih družbah prevladuje predvsem neformalni nadzor, kjer poleg družinske socializacije pomembno vlogo opravlja religija. Bolj diferencirane in atomizirane sodobne družbe pa večji poudarek dajejo formalnim mehanizmom nadzora.

Družbeni nadzor torej ni vezan zgolj na institucije. Kanduč pravi, da *»gre za osupljivo širok pojem, saj* (v sodobni kapitalistični družbi, op. M.D.) *zajema tako rekoč vse mehanizme, strukture, institucije, sisteme, dejavnosti in pojave, ki (po)ustvarjajo družbeni red (in urejene, v redu delujoče družbene člane), na primer socializacijo, izobraževanje, medije, rutinsko delovanje državne uprave, kazenskopravni sistem, javno mnenje, običaje, manire, »motivacijske besednjake«, religijo, disciplinske aparate, ideološko indoktrinacijo, manipulacijo, propagando, (dez)informiranje, tehno-prevencijo, »nevidno roko« tržnih zakonitosti, »tiho silo ekonomskih razmerij«, »politiko ustvarjanja potrošniških želja in potreb« po kapitalističnem blagu, in sicer predvsem po njegovih »simbolnih vrednostih«, ki signalizirajo življenjski stil, osebno identiteto in vznemirjenja (hkrati pa posameznika napeljujejo, da si z vsemi močmi prizadeva uresničiti sanje, ki mu jih za drag denar prodaja kapitalistični marketing, na primer sanjsko družinsko hišo, sanjski avtomobil in sanjske počitnice). Po drugi strani pa je mogoče družbeno nadzorstvo razbiti v dva idealna tipa, in sicer na (a) aktivne oziroma pastoralne ali produktivne nadzorstvene prijeme, ki temeljijo na vcepljanju družbeno zaželenih motivacijskih vsebin; (b) reaktivne oblike kontrole, ki se opirajo na de-motiviranje – predvsem z zagroženimi in apliciranimi formalnimi in neformalnimi sankcijami«* (Kanduč 2004, 4).

[4] Takšna podjetja so zelo razširjena predvsem v ZDA (npr. LexisNexis, Choicepoint, Axciom), v zadnjih letih pa se pojavljajo tudi na slovenskem tržišču.

Čeprav je nadzor ponavadi asimetričen, saj ga v največji meri izvaja tisti, ki ima več moči, nad tistim, ki ima manj moči, ni nikoli docela enosmeren. Oblast ali družba lahko nadzor uporabljata proti posameznikom, hkrati pa lahko posameznik nadzor uporabi proti državi. Zato ni naključje, da je za aktiviste, ki se ukvarjajo z zaščito zasebnosti, zakonodaja za dostop do informacij javnega značaja pomembno orodje v boju proti prikritemu državnemu nadzoru. Vendar kljub dejstvu, da je nadzor mogoče uporabiti dvosmerno, v praksi vselej prevladuje asimetričnost in tudi sodobna tehnologija omogoča nadzorovanje predvsem v eno smer: gre bolj za to, da oblast nadzoruje posameznike in manj, da posamezniki nadzorujejo oblast (Kovačič 2006, 22).

Delitev na formalni in neformalni nadzor je prepričljiva predvsem v teoriji, v praksi pa se obe vrsti nadzora pogosto prekrivata. Kljub temu je mogoče trditi, da je v arhaičnih, antičnih in srednjeveških družbah, kjer so bile skupnosti majhne in močno povezane, mobilnost ljudi pa zelo omejena, prevladoval neformalni nadzor. V novem veku pa se je ob razcvetu velemest, nastanku nacionalnih držav in oblikovanju birokratskih organizacij, na račun krčenja neformalnega nadzora okrepil formalni nadzor.

V sodobni potrošniški družbi se je zgodil še en pomemben premik v sferi družbenega nadzora. V 18. in 19. stoletju je sistematičen nadzor izvajala država, danes pa čedalje bolj v ospredje stopa zasebni sektor. Nova vrsta „potrošniškega nadzora“ ne izvira iz represivne moči kazenskega prava, ampak *»temelji na navidez prijaznem zbiranju* (s pomočjo prošenj, reklam, popustov, ugodnosti in daril) *podatkov o potrošnikih«* (Kovačič 2003, 23). Prav tako nadzor potrošnikov ni primarno namenjen uveljavljanju pravnega reda, pač pa (prek ugotavljanja potrošnikovih želja in prilagajanja ponudbe) ustvarjanju profita. Vendar se je ob tem potrebno zavedati, da po podatkih, ki jih zbirajo institucije zasebnega sektorja, pogosto posežejo tudi države in sicer z namenom izvajanja formalnega nadzora, ki pa je od nekdaj namenjen vzdrževanju pravnega in širšega družbenega reda.

Podoba družbenega nadzora se je v zadnjih desetletjih torej precej spremenila. Če se je tradicionalni nadzor razumel kot nekaj negativnega, kot nekaj, kar prisiljuje, pa je nadzorovanje danes dobilo bolj prijazen, pastoralen in celo hinavski obraz. S pomočjo sodobne tehnologije je nadzorovanje postalo skoraj neopazno, vendar povsod navzoče. Prek potrošništva pa je postalo še prijazno in prostovoljno (Kovačič 2006, 22). Ta preskok slikovito opisuje slogan iz Orwellovega romana 1984: *»Veliki brat te opazuje! / Big Brother is watching you!«* se spreminja v *»Veliki brat skrbi zate! / Big Brother is watching out for you!«* (Whitaker 1999, 142).

2.2 ZGODOVINA DRUŽBENEGA NADZORA

Nadzor v svoji najosnovnejši obliki predstavlja pomemben element sleherne medčloveške interakcije. Pojavlja se povsod tam, kjer nastajajo večje ali manjše družbene skupine oziroma skupnosti. Ljudje so drug drugega že od nekdaj opazovali, s tem pa posredno tudi nadzorovali. Zato je družbeni nadzor star toliko kot človeštvo. Seveda je tak najosnovnejši nadzor izrazito neformalen, prikrit, spontan, nezaveden in vgrajen v tkivo socialnih odnosov.

Z razvojem družbenih skupnosti pa se je oblikoval tudi formalni nadzor, ki je utemeljen v pravnem redu in svojo moč v skrajni instanci uveljavlja s pomočjo represivnega aparata. Formalni nadzor je bil vselej povezan z oblastjo in ohranjanjem družbenega reda, zato je bil v zatiranju neposlušnosti in v obvladovanju razmer pogosto zelo militanten in neizprosen (Pečar 1988, 111). To še posebej velja za arhaične, antične in srednjeveške družbe, ki so oblast uveljavljale z izrazito ostro kazensko zakonodajo. Je pa tak nadzor zaradi odsotnosti informacijske in komunikacijske tehnologije temeljil predvsem na neposrednem opazovanju ljudi s pomočjo človeških agentov.

Čeprav je bil »predmoderni nadzor« usmerjen predvsem na posameznika, so se že celo v antiki, seveda v precej omejenem obsegu, pojavljali poizkusi nadzorovanja celotne populacije. Vladarji številnih kraljestev so izvajali popise prebivalstva z namenom pridobivanja podatkov o (ne)plačanih davkih, opravljeni vojaški službi, migracijah, idr. Izraelski nomadi so imeli t.i. Knjigo števil (ang. The Book of number), ki je vsebovala različne podatke o pripadnikih tam živečih plemen. S tovrstnimi popisi so vladarji skušali že zelo zgodaj klasificirati posameznike v skupine, kar se je izkazalo kot posebej uporabno predvsem pri vzdrževanju vojaškega reda. Praktična vrednost popisov je prišla do izraza tudi pri razdeljevanju ozemlja (Lyon 1994, 22) in bolj učinkovitem pobiranju davkov. V tem kontekstu velja posebej izpostaviti Domesday Book[5] iz leta 1086, ki predstavlja enega najbolj znamenitih zgodnjih poizkusov nadzora populacije. Domesday Book je obsežen dokument s podatki o prebivalstvu in zemljiščih na območju današnje Velike Britanije. S pomočjo teh informacij so normanski vladarji bolj učinkovito pobirali davke in izvajali oblast (Lyon 1994, 22), kar kaže, da so že prvi poizkusi množičnega nadzora služili predvsem kot orodje za krepitev vladarjeve moči.

Toda sistematični nadzor, ki se izvaja tako rekoč neprekinjeno in predstavlja vsakdanjo dejavnost državnega aparata, se je pojavil šele v moderni. Lyon (1994, 24) pojasnjuje, da je nastanek

[5] »Domesday Book« ima dva etimološka izvora. Zapiski so bili shranjeni v Domus Dei (Božji hiši) v Winchestru. Leta 1179 je angleški blagajnik zapisal, da se ime Domesday Book metaforično nanaša na sodni dan (»doom`s day«) iz Svetega pisma (Lyon 1994, 23).

sodobnega nadzora sovpadal s formiranjem nacionalnih držav, rastjo vojaških organizacij, razcvetom kapitalizma, industrializacije in urbanizacije, ter širjenjem birokracije. Sistematični[6] družbeni nadzor je postal sestavni del državnega aparata (Lyon 1994, 24), saj je omogočal bolj učinkovito (glede na prejšnja zgodovinska obdobja in sisteme vladavin) izvajanje civilne in vojaške oblasti, bistveno pa je povečal tudi produktivnost proizvodnje in trgovine.

Na razvoj sodobnega nadzora so po mnenju Lyona (2007, 26) močno vplivali trije družbeni procesi: racionalizacija, klasifikacija in tehnologija.
Racionalizacijo Lyon (2007, 26) opredeljuje kot dosleden proces uporabe standardiziranih postopkov, ki so utemeljeni v idealu razuma in ne v tradiciji, čustvih ali zdravorazumski vednosti, predstavljajo pa osnovno shemo družbenega, političnega ter ekonomskega delovanja sodobnih družb.
Klasifikacija je prav tako povezana z idealom razuma. Močno je prisotna v delovanju birokratskih organizacij, kaže se kot težnja po razporejanju posameznikov ali skupin na podlagi določenih parametrov, to pa je eden od pogojev bolj učinkovitega in racionalnega nadzora.
Vznik racionalizacije in klasifikacije je v veliki meri omogočila šele tehnologija, ki v kontekstu nadzora predstavlja predvsem osnovno sredstvo za učinkovito in obsežno zbiranje ter obdelavo podatkov o posameznikih oziroma skupinah.

Lyon (2007, 27) je vznik in razvoj sistematičnega nadzora, ki je značilen za moderno dobo, pojasnil s pomočjo petih družbenih strukturnih elementov; vojske, administracije, industrije, policije in potrošništva.

Vojska in disciplina

Stroga disciplina je že od nekdaj predstavljala sestavni del učinkovite vojske in vojaškega delovanja. Vsekakor je bila disciplina poudarjena že v rimskih legijah, kjer se je najmanjše prestopke in odstopanja od predpisanega vojaškega reda neizprosno kaznovalo. Vendar pa se je šele v 16. stoletju vojaški disciplini pridružilo še natančno opazovanje vojaških praks in manevrov. Takšno opazovanje oziroma nadzorovanje je služilo točno določenemu namenu; določitvi in analizi osnovnih gradnikov vsakega vojaškega procesa. Takšne gradnike je bilo nato mogoče sestaviti v nove, bolj optimalne nize, ki so povečali učinkovitost vojske (Lyon 2007, 27). Analiza osnovnih

[6] Za sodobni družbeni nadzor je značilno predvsem sistematično ustvarjanje in zbiranje dosjejev o posameznikih. Tak proces je v širšem smislu značilen za vse birokratske organizacije in predstavlja temelj sodobnega managementa. Dosjeji o posameznikih namreč služijo – vsaj z organizacijskega vidika – zagotavljanju tehnične učinkovitosti in predvidljivosti (Lyon 2007, 29).

gradnikov pa se ni nanašala le na vojakove gibe ali premike enot, pač pa tudi na arhitekturo[7] vojaškega tabora in organizacijo cele vojske. Vojaški tabori so bili postavljeni na premišljen način, ki je poveljnikom omogočal čim bolj učinkovit nadzor nad vojaki, hkrati pa je zagotavljal čim hitrejše formiranje enot.

Poleg arhitekturne optimizacije je bila za stratege in voditelje zelo pomembna tudi čimbolj smotrna ureditev celotne vojaške organizacije. Vendar pa rigidna hierarhična struktura z natančno določenimi položaji in odgovornostmi ni ostala omejena le na vojsko, pač pa se je kmalu razširila še na civilni sektor in se uveljavila kot osnovna matrica[8] vsakršne birokratske organizacije.

Razen tega je vojaško vodstvo potrebovalo podatke o celotni populaciji, saj je bilo na ta način zagotovljeno učinkovitejše novačenje vojaških nabornikov. S tem, ko se je začelo (čeprav zgolj v specifično vojaške namene) sistematično nadzorovati splošno populacijo, je bil začrtan pomemben mejnik na področju razvoja množičnega nadzora. Z razvojem informacijske in komunikacijske tehnologije se je težnja po množičnem nadzoru le še okrepila. V 20. stoletju pa je razcvet informacijskega nadzora in kibernetskih sistemov prvikrat omogočil uresničevanje sanj o virtualnem bojevanju (Lyon 2007, 29).

Državna administracija in cenzus

Že vladarji antičnih kraljestev so skušali svoje podanike nadzorovati z najrazličnejšimi metodami. Ena najstarejših je cenzus oziroma popis prebivalstva, uporablja pa se za zbiranje podatkov o populaciji, kar je koristno predvsem pri pobiranju davkov, novačenju vojaških nabornikov, nenazadnje pa tudi pri zagotavljanju pravic in dolžnosti posameznikov (Lyon 2007, 30).

V 17. in 18. stoletju so postale tehnike zbiranja podatkov bolj dovršene in racionalne. Z razvojem birokratskih organizacij pa je formalno sistematično nadzorovanje postalo običajna in vsakdanja praksa. Ob tem ni odveč poudariti, da nadzorovanje, ki ga je izvajala moderna država, ni bilo zgolj »maligno«[9] (instrument s katerim elite izkoriščajo množice), pač pa tudi benigno, saj je navadnim državljanom omogočalo bolj učinkovito uveljavljanje pravic in dolžnosti. Razen tega nacionalne države, ki so se pričele oblikovati v obdobju westfalskega miru, ne bi mogle nastati brez birokratskih organizacij in z njimi povezanega sistematičnega nadzora (Lyon 2007, 32-33).

---

[7] Več kot očiten simptom obsedenosti z arhitekturo nadzora predstavlja Benthamov panoptikon, načrt »idealnega« zapora, šole, tovarne, bolnišnice ali kakšne druge zaprte institucije, ki nadzorniku iz osrednjega stolpa omogoča popoln pregled nad drugimi ljudmi.

[8] Klasična dela Tolstoja, Puškina in Dostojevskega jasno kažejo nekatere vzporednice med vojaško in civilno birokratsko organizacijo. Sekretar na ministrstvu v Rusiji 19. stoletja se je na primer imenoval general.

[9] Lep primer malignega državnega nadzora je prikazan v znamenitem Orwellovem romanu 1984 in v Kafkinem Procesu. 1984 prikazuje totalitarno družbo, kjer elita uporablja nadzor za (popolno) obvladovanje državljanov. V Procesu je stvar nekoliko bolj zapletena, saj gre za psihološki izraz izrojenosti in nesmiselnosti birokratske organizacije, ki posameznika dobesedno pogoltne.

Industrija in delovno mesto

Lyon (2007, 33) pravi, da je razvoj sistematičnega nadzora mogoče pojasniti tudi skozi prizmo dela. Cilj, ki ga zasleduje takšen nadzor, je povečevanje delovne učinkovitosti, produktivnosti, dobička, pa tudi zmanjševanje stroškov, ki so povezani s produkcijskimi procesi.

V tem okviru so znane Taylorjeve raziskave s področja managementa in organizacijskih ved. Frederick Taylor (v Lyon 2007, 33) je namreč preučeval proizvodne procese in – podobno kakor analitiki v vojski – skušal določiti osnovne gradnike, ki bi jih lahko sestavil v nove, bolj učinkovite nize.

Sodobne informacijske tehnologije, med katerimi velja omeniti predvsem GPS sisteme za določanje položaja, RFID »pametne« kartice, programe za beleženje udarcev na tipkovnici (t.i. key loggers), prestrezanje elektronske pošte in video sisteme, pa so nadzor na delovnem mestu le še okrepile (Lyon 2007, 34-36).

Policija in kriminaliteta

Lyon (2007, 36) pojasnjuje, da je bil policijski nadzor prvotno povezan z vojaškim nadzorom. Šele kasneje, ko se je policija docela osamosvojila in ločila od vojske, se je policijski nadzor usmeril izključno k vzdrževanju notranjega reda in miru.

Najprej so ga izvajali ljudje z neposrednim opazovanjem, prisluškovanjem in zasliševanjem. Tem elementarnim praksam se je pridružilo oblikovanje bolj ali manj sistematičnih dosjejev o »sumljivih« posameznikih. Kasneje pa je sodobna tehnologija tak nadzor okrepila in razširila. Danes je v širši javnosti znan predvsem video nadzor mestnih središč. Vendar se je pravi preskok zgodil na ravni zbiranja in obdelave podatkov. Računalnik je omogočil združevanje podatkov prek razpršenih podatkovnih baz, tehnike izkopavanja podatkov in analize omrežji pa omogočajo izvajanje nadzora nad t.i. rizičnimi skupinami. Takšne skupine sestavljajo posamezniki, ki sicer še niso izvršili kaznivega dejanja (in ga morda nikdar ne bodo), vendar zaradi različnih parametrov kažejo visoko stopnjo tveganja, da bodo neko dejanje storili nekoč v prihodnosti (Lyon 2007, 36-40).

Potrošništvo

V zadnjih desetletjih se je začel nadzor čedalje bolj pomikati iz javnega v privatni sektor. Razvoj informacijske tehnologije, ki je dostopna širokim množicam, je omogočil sistematično oblikovanje, zbiranje in obdelovanje najrazličnejših informacij o potrošnikih. Nadzor potrošnikov je sicer

predvsem v interesu zasebnih podjetij, vendar tako zbrane podatke nemalokrat uporabijo tudi državne institucije (Lyon 2007, 41-42).

Pomemben mejnik v oblikovanju nadzora potrošnikov predstavlja delo Alfreda Sloana iz začetka tridesetih let prejšnjega stoletja. Sloan je za General Motors zbiral podatke o strankah. S pomočjo računalniške tehnologije podjetja IBM je izdeloval profile posameznikov, ki jih je nato združeval v obsežne skupine s specifičnimi značilnostmi. Prav razvrščanje posameznikov v določene skupine predstavlja osnovo t.i. usmerjenega potrošništva, ki se prilagaja posamezniku glede na njegov okus, želje in zahteve. Največjo revolucijo pa so z razvojem poceni računalnikov in interneta[10] prinesla osemdeseta leta. Obseg podatkov se je bliskovito povečal, tehnike informacijske obdelave pa tudi, zato so na trgu začela nastajati podjetja, ki so se ukvarjala zgolj z zbiranjem, posredovanjem, izmenjavo in prodajo podatkov o potrošnikih.

Lyon (2007, 45) pravi, da je pri nadzoru potrošnikov mogoče ločiti tri (kronološke) faze. V prvi fazi se je potrošnike profiliralo, nato pa se je na podlagi teh profilov oblikovalo usmerjeno oglaševanje, ki je bilo prilagojeno okusu, potrebam in željam posameznika oziroma potrošniške skupine, ki ji je pripadal. V drugi fazi, ki prevladuje v trenutnem »sodobnem« nadzoru potrošnikov, je pozornost namenjena nadzorovanju spletnih dejavnosti (»brskanja po internetu«) potrošnikov. Tretja faza, ki je še v povojih, pa bo po besedah Lyona (2007, 45) združila prvo in drugo fazo s pomočjo lokacijskih tehnologij, ki bodo podatkovne profile povezale s točno določenimi in določljivimi posamezniki.

Lyon (1994) se pri razlagi razvoja družbenega nadzora v modernih družbah opira na idejna izhodišča treh temeljnih družboslovnih mislecev: Karla Marxa, Maxa Webra in Michela Foucaulta. Po besedah Lyona (1994, 25) naj bi Marx družbeni nadzor interpretiral v kontekstu kapitalističnega ekonomskega sistema. V tem pogledu je nadzor predvsem sredstvo, ki ga kapitalisti uporabljajo za krotenje proletariata, kar naj bi omogočalo rast profita na eni in ohranjanje družbene stabilnosti na drugi strani. Lyon (1994, 25) dodaja, da naj bi se s takšno razlago funkcije nadzora delno strinjal tudi nemški sociolog Max Weber. Vendar naj bi Weber za razliko od Marxa dajal poudarek predvsem povezavi med nadzorom in birokracijo. V skladu s tem pogledom nadzor ni značilen le za kapitalizem, pač pa za sleherno obliko vladavine, ki za svoje ohranjanje uporablja bolj ali manj razvit birokratski aparat.

Največ pozornosti pa je po mnenju Lyona (1994, 26) analizi družbenega nadzora namenil francoski filozof in zgodovinar Michel Foucault. V svojem precej odmevnem delu *Nadzorovanje in*

[10] Razvoj interneta je omogočil nenehno nadzorovanje spletnih aktivnosti posameznikov. Takšen nadzor, ki poteka s pomočjo beleženja IP naslovov, piškotkov, key loggerjev, idr., je mogoče do neke mere omiliti z uporabo anonimizacijskih (tor) omrežji, rednim brisanjem piškotkov, onemogočanjem nekaterih programskih skript (predvsem jave). Vendar pa takšni ukrepi zmanjšajo »uporabniško izkušnjo« interneta.

kaznovanje: nastanek zapora je Foucault skušal prikazati razvoj kazenskega pravosodja skozi prizmo družbenega nadzora. Foucault razume nadzor bolj široko kot Marx in Weber. Zanj nadzor ni le značilnost določenega tipa organizacij ali ekonomskega sistema, ampak predstavlja sestavni del sleherne družbe. V skladu s tem pogledom ni družbe brez nadzorovanja. Se pa zato oblika in intenziteta nadzora od družbe do družbe razlikujeta. Foucault poudarja, da je nadzor dobil največjo težo prav v moderni »disciplinski« družbi, ki je na drobno in v celoti prežeta z »mikrofiziko« državne oblasti. Če je bil v 17. in 18. stoletju sistematični nadzor omejen na zaprte institucije, se je kasneje razširil na celotno družbeno strukturo. Zato so v sodobni družbi ljudje čedalje pogosteje in čedalje bolj intenzivno podvrženi nadzoru, njihove dejavnosti pa skrbno dokumentirane. Ob tem pa sistematični nadzor posameznika umešča v ožje ali širše družbene skupine in s tem vzpostavlja posebno vrsto »biopolitičnega« nadzora, ki se ob pomoči statistike ukvarja z upravljanjem celotnih populacij (Lyon 1994, 26).

2.3 PANOPTIKON: ARHETIP DRUŽBENEGA NADZORA

Pred dobrima dvema stoletjema je Jeremy Bentham postavil koncept zgradbe, ki prek premišljene razporeditve arhitekturnih elementov omogoča samodejno vzpostavitev in delovanje nadzora nad zaprto populacijo. Panoptikon je bil prvotno predviden kot zapor, vendar ga je Bentham kmalu razširil še na tovarno, šolo, bolnišnico in norišnico.

V dvajsetem stoletju je idejo panoptikona ponovno obudil Foucault, ki jo je s perspektive zgodovinarja interpretiral kot koncept, ki presega arhitekturno razsežnost. Po razlagi Foucaulta panoptikon ni le zgradba ali rešitev tehničnega problema, pač pa poseben dogodek v zgodovini človeškega duha, ki zarisuje nov tip družbe. Če je bila antika civilizacija spektakla, ki je omogočala množici ogled majhnega števila posameznikov, potem je moderna družba prav nasprotna, saj skuša majhnemu številu ljudi omogočiti vpogled v množico.

Zato je nacionalna država kot temeljna organizacijska oblika moderne družbe za zagotavljanje svojega obstoja morala poseči v vse podrobnosti in razmerja družbenega življenja. To je dosegla s čedalje obsežnejšim in čedalje intenzivnejšim nadzorom, ki se je najprej usmerjal na posameznike, kasneje pa še na cele populacije.

2.3.1 ARHITEKTURNA ZAMISEL

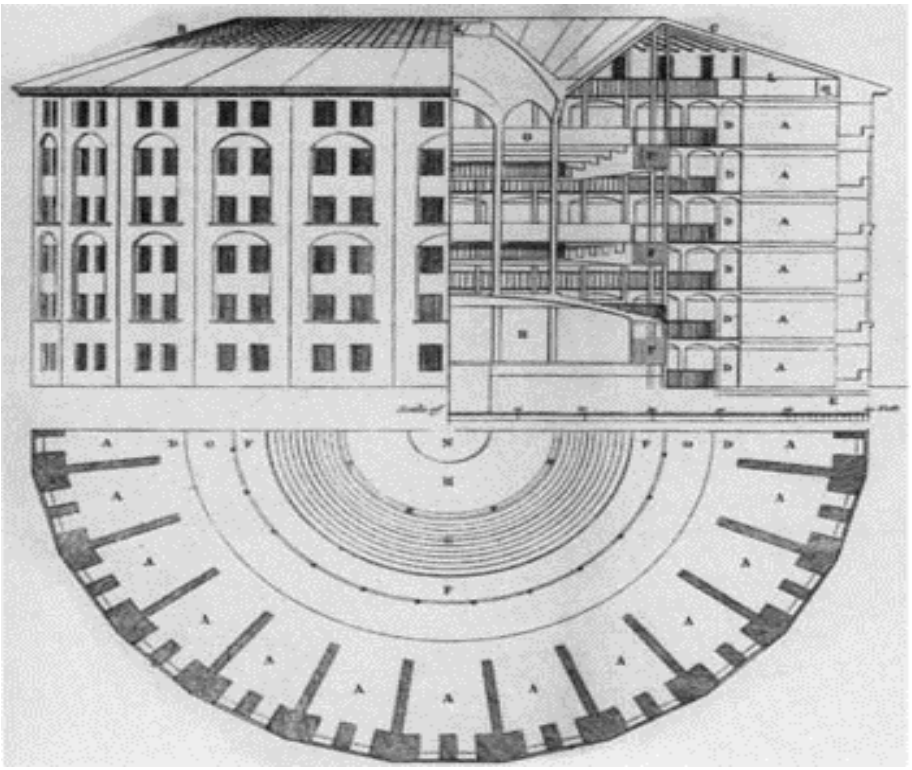
Leta 1787 je angleški filozof Jeremy Bentham napisal niz pisem, ki so bila kasneje objavljena v zvezku z naslovom *The Panopticon Writings*. V pismih je predstavljen arhitekturni načrt zgradbe, imenovane panoptikon (glej sliko 2.1). Ta vsaj v teoriji omogoča izvajanje skoraj popolnega nadzora nad večjim številom ljudi. Prvotni zasnutek panoptikona se je nanašal na zapor, vendar je Bentham kmalu ugotovil široko uporabnost koncepta in ga razširil še na tovarno, šolo, bolnišnico in norišnico, skratka, na sleherno zaprto institucijo.

Zgradba je krožna, ob zunanjem obodu so razvrščene celice z zaporniki. Celice so med seboj ločene s posebnimi razdelki, ki onemogočajo kakršnokoli komunikacijo med zaporniki. Na sredini zgradbe je stolp oziroma nadzornikova loža. Med celicami in osrednjim stolpom je prazen prostor, ta omogoča nadzorniku vizualni pregled nad razvrstitvijo in početjem zapornikov. Na zunanji steni vsake celice je okno, ki prepušča svetlobo v notranjost zgradbe. Notranji del celic zapira kovinska mreža, ki omogoča nadzorniku popoln vpogled. Mreža hkrati služi kot vhod v celico. Okna v nadzornem stolpu imajo žaluzije, te preprečujejo, da bi zaporniki lahko opazovali nadzornika. Prav tako je arhitektura stolpa zamišljena na način, ki preprečuje prehajanje svetlobe iz enega okna skozi drugo. Na ta način se doseže konstantna zatemnitev, zaradi katere je nadzornik zakrit pred radovednimi pogledi zapornikov, hkrati pa mu omogoča, da nemoteno izvaja svoj nadzor.

Prav tako so pri oknih nadzornikove lože nameščene posebne svetilke z zaslonkami, ki se ponoči uporabljajo kot reflektorji za osvetljevanje celic. Med stolpom in celicami so speljane tanke kovinske cevi, ki služijo dvema namenoma. Prvič, nadzorniku omogočajo nemoteno sporočanje ukazov slehernemu zaporniku. Drugič, omogočajo tudi, da nadzornik prisluškuje vsem zapornikom.

Zvonec, uporablja se kot alarm, je nameščen v zvoniku oziroma kupoli in prek vrvi povezan z nadzornikovo ložo. Izbočeni središčni del strehe, ki pokriva zgradbo, ima velika okna z zastori, s pomočjo katerih je mogoče uravnavati prehajanje sončne svetlobe v zgradbo, prav tako pa služi tudi kot sistem prezračevanja. Ogrevanje poslopja se izvaja s pomočjo cevi, prek katerih se pretaka vroča voda ali para. Peči, ki ogrevajo cevi, so nameščene v zgradbi, saj se na ta način izgubi manj toplote (Bentham 1995, 40).

Slika 2.1: Shema panoptičnega zapora



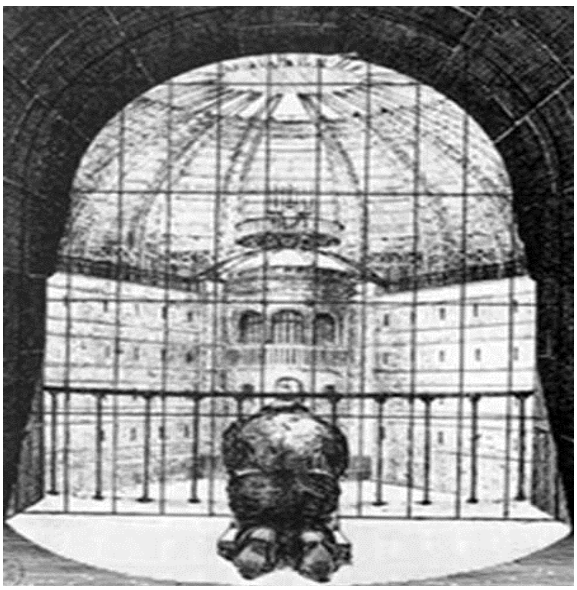
2.3.2 DINAMIKA IN UČINKI PANOPTIČNE DISPOZICIJE

Arhitektura panoptikona omogoča nadzorniku, ki je postavljen v osrednji stolp (glej sliko 2.2), popoln pregled nad jetniki, delavci, šolarji, bolniki in norci. Vsakdo je na svojem mestu in dobro zaprt v celico (glej sliko 2.3), kjer ga od spredaj vidi nadzornik, stranski zidovi pa mu preprečujejo, da bi stopil v stik s tovariši. Zapornik je v vsakem trenutku viden. Je predmet informacije, ne pa subjekt v komunikaciji. S tem je vzpostavljeno zagotovilo za red. Ker obsojenci ne morejo komunicirati drug z drugim, ni nevarnosti zarot, skupinskih pobegov in (slabih) medsebojnih vplivov. Če gre za bolnike, ni nevarnosti za okužbo, če za delavce, ni pretepov, tatvin, razvedril, ki bi upočasnjevala delo. Skratka, premišljena arhitekturna kompozicija onemogoča kakršnokoli medsebojno komunikacijo zapornikov, s tem pa se v kali zatrejo kvarni vplivi, ki bi utegnili

zmanjšati nadzorstveno in disciplinsko učinkovitost panoptičnega stroja (Foucault 2004, 220).

Slika 2.2: Osrednji nadzorni stolp.

Slika 2.3: Jetnik v celici, v ozadju nadzorni stolp



S tem, ko panoptikon pri zaporniku povzroči zavestno in nenehno stanje vidnosti, zagotovi samodejno delovanje oblasti. To pomeni, da se v arhitekturnem stroju ustvarja in vzdržuje oblastno razmerje, ki ni odvisno od tistega, ki izvršuje oblast. Ali drugače: panoptikon povzroči, da so jetniki zajeti v oblastne razmere[11], katerih nosilci so oni sami. To pomeni, da so učinki nadzora stalni, čeprav je njegova dejavnost diskontinuirana. Pomembno je, da se zapornik čuti nadzorovanega, ni pa potrebno, da bi zares bil. Ravno zato je Bentham postavil načelo, da mora biti oblast vidna in nepreverljiva. Jetnik mora nenehno imeti pred očmi visoki obris središčnega stolp, od koder oprezajo za njim. Toda hkrati ne sme nikdar vedeti ali je opazovan prav v tistem trenutku.

Miller pravi, da je največja zvijača Panoptikona v Očesu, ki vidi, ne da bi bilo videno: *»Če lahko razločim pogled, ki me zalezuje, lahko obvladam nadziranje, lahko ga tudi sam zalezujem, ugotovim*

[11] Dejanska podvrženost mehanično nastane iz fiktivnega razmerja. Tako ni treba uporabljati sile, da bi obsojenca prisilili k dobremu obnašanju, norca k miru, delavca k delu, šolarja k marljivosti, bolnika pa k temu, da uboga ukaze. Bentham se je navduševal nad tem, da so panoptične institucije lahko tako lahkotne: ni več rešetk, ni verig, ni težkih ključavnic, dovolj je, da so ločitve jasne, odprtine pa dobro razvrščene. Težke stare »varnostne domove« z arhitekturo trdnjav lahko nadomesti preprosta in varčna geometrija »domov gotovosti«. Učinkovitost oblasti, njena prisiljevalna sila sta nekako prešli na drugo stran – na stran površine, na katero se aplicira. Kdor je podrejen polju vidnosti in to ve, sam prevzame prisile oblasti; spontano jih uporablja na samem sebi; vase vtisne oblastno razmerje, v katerem igra hkrati obe vlogi; postane načelo svoje lastne podvrženosti. Zato pa se lahko zunanja oblast otrese fizičnih bremen; teži k netelesnosti; čim bolj pa se približuje tej meji, tem bolj so njeni učinki stalni, globoki, doseženi enkrat za vselej, nenehno obnavljani: to je nenehna zmaga, ki preprečuje sleherno fizično soočanje in je vselej vnaprej dobljena (Foucault 2004, 222).

njegove premore in slabosti, preučim njegovo regularnost, ga izsledim. Če pa je Oko skrito, potem me gleda tudi takrat, kadar ne vidi. Oko, ki je potuhnjeno v senci, pomnoži vse svoje moči« (Miller v Kovačič 2005, 23). Panoptikon je utemeljen na iluziji vseprisotnega in nenehnega nadzora. Prav s tem pa doseže ponotranjeno delovanje oblasti na mikroravni: *»Kdor je podrejen polju vidnosti in to ve, sam prevzame prisile oblasti; spontano jih uporablja na samem sebi; vase vtisne oblastno razmerje, v katerem igra hkrati obe vlogi: postane načelo svoje lastne podvrženosti*[12]*«* (Foucault 2004, 202).

Revolucionarnost Benthamove ideje je v tem, da je načelo grajskih celic obrnil na glavo. Če je zaporniški sistem grajskih celic zapornika vrgel v temo, je v panoptikonu zapornik izpostavljen svetlobi. Miller (v Kovačič 2005, 23) pravi, da *»svetloba dela iz nas ujetnike«*. In ker je svetlobi oziroma nadzornemu očesu nemogoče uiti, Miller meni, da je *»Panoptikon stroj za proizvodnjo dozdevka Boga«* (Miller v Kovačič 2005, 23). Zaradi tega miselnega preskoka v kaznovanju, preskoka od modela, ki je zapornika izvrgel, v model, v katerem je zapornik izpostavljen oblasti, ki gleda, Foucault Benthama označi za *»enega najpomembnejših inovatorjev na področju tehnologije oblasti«* (Foucault 2008, 48).

Posebna vrednost panoptikona je tudi v tem, da z elementom nevidnosti nadzornika vzpostavlja avtomatizirano in homogenizirano oblast. Ker so ljudje v panoptikonu vselej vidni, sami pa nikoli ne vidijo, je pravzaprav vseeno kdo izvršuje oblast.

Katerikoli malone naključen individuum lahko upravlja[13] *stroj: če ni ravnatelja, lahko to opravlja njegova družina*[14]*, njegovi sodelavci, prijatelji, obiskovalci, celo njegovi služabniki. Prav tako nepomemben je motiv, ki ga poganja: nediskretneževa radovednost, otroška porednost, vedoželjnost kakšnega filozofa, ki si hoče ogledati ta muzej človeške narave, ali hudobija tistih, ki uživajo v zalezovanju in kaznovanju. Čim več je teh anonimnih in začasnih opazovalcev, tem večja je za jetnika možnost, da ga bodo presenetili, in tem bolj se vznemirjeno zaveda, da ga opazujejo. Panoptikon je čudovit stroj, ki iz najrazličnejših želja izdeluje homogene oblastne učinke* (Foucault

---

[12] Podvrženost panoptičnemu nadzoru (v teoriji) ne doseže zgolj tega, da se posameznik obnaša tako, kot se od njega pričakuje, pač pa mu odvzame svobodno voljo in s tem tudi možnost, da bi sploh kaj storil narobe. Foucault pravi: *»Bentham je v svojem besedilu zelo jasno zapisal, kako pomembno je odvračanje. Zelo važno je, da ima Inšpektor zapornika neprestano na očeh; tako mu skorajda ne bo prišlo na misel, da bi storil kaj narobe. S tem smo se znašli v srcu revolucionarnih prizadevanj: kako preprečiti ljudem, da bi storili kaj narobe, kako izničiti njihovo željo, da bi grešili. Skratka, kako jim odvzeti zmožnost in voljo«* (Foucault 2008, 47).
Vendar se je ob tem potrebno zavedati, da se ljudje na zahteve nadzora in oblasti ne odzivamo vselej pasivno. Oblikujemo namreč lahko različne strategije upora in izmikanja, zato popoln nadzor, ki bi človeku v celoti odvzel »svobodno voljo« (kolikor pristanemo na filozofsko pozicijo, da svobodna volja sploh obstaja), zaenkrat ne obstaja, kar nenazadnje potrjuje tudi dejstvo, da panoptikon nikdar ni zaživel v praksi.

[13] Upravljanje »stroja« je Bentham (1995, 67) zaupal upravniku-zasebniku, ki od države pridobi koncesijo za izgradnjo in obratovanje panoptikona. Zlorabe položaja se preprečijo tako, da upravnik za vsakega umrlega ali pobeglega zapornika državi izplača določen znesek oziroma denarno kazen.

[14] Bentham je svetoval, naj v nadzorni loži oziroma osrednjem stolpu živi vsa nadzornikova družina. Na ta način se poveča število ljudi, ki opazujejo celice, posledično pa se pomnoži nadzor.

2004, 220-222).

2.3.3 DIAGRAM OBLASTI

Čeprav je panoptikon izvorno utemeljen kot arhitekturna zamisel, je mogoče njegovo shemo razširiti na celotno družbeno strukturo. Bentham ga sicer prikazuje kot posebno ustanovo, ki je trdno zaprta vase in so jo pogosto imeli za utopijo popolnega zapiranja. Vendar panoptikon ne smemo razumeti zgolj kot sanjsko stavbo: je diagram[15] oblastnega mehanizma, prignan do idealne oblike. Njegovo delovanje, iz katerega je abstrahirana sleherna ovira, odpor ali trenje, bi prav lahko predstavili kot čisti arhitekturni ali optični sistem. Dejansko gre za figuro politične tehnologije, ki jo lahko ločimo in ki jo moramo ločiti od sleherne posebne rabe (Foucault 2004, 225).
V vsakem primeru panoptikon omogoča izpopolnjeno izvrševanje oblasti. To doseže na več načinov. Prvič, skrči število tistih, ki izvršujejo oblast, hkrati pa poveča število onih, nad katerimi se oblast izvršuje. Drugič, moč panoptične oblasti je v tem, da se izvršuje spontano in potiho, njeni učinki se pripenjajo drug na drugega kakor členi verige, ki oklepa ujeta telesa. Tretjič, vzpostavlja se s pomočjo arhitekture in geometrije, ne pa fizične prisile, zato daje *duhu oblast nad duhom*.
Panoptični dispozitiv okrepi katerikoli oblastni aparat. S svojo preprečevalno naravo, s kontinuiranim delovanjem in s samodejnimi mehanizmi zagotavlja gospodarnost in učinkovitost. Je način pridobivanja oblasti *v »količini, ki je bila dotlej* (do moderne, op. M.D.) *brez primere*. Je *velik in nov instrument vladanja, sijajen zaradi velike moči, ki jo lahko da sleherni ustanovi, kjer ga uporabijo«* (Foucault 2004, 227).

Panoptizem je mogoče integrirati v katerokoli funkcijo (vzgojno, terapevtsko, produkcijsko, kazensko) in jo izboljšati. Vzpostavi se mešan mehanizem, v katerem se oblastna in vrednostna razmerja natančno prilagodijo procesom, ki jih je potrebno kontrolirati (Foucault 2004, 227).
Panoptični dispozitiv[16] ni zgolj pregib ali posrednik med oblastnim mehanizmom ali funkcijo. Je način, ki omogoča, da oblastna razmerja delujejo v funkciji, funkcija pa s pomočjo teh oblastnih

[15] Kaj je torej diagram oblasti? Deleuze (2006, 30) ga prek povzemanja Foucaulta opredeli kot delovanje, ki je rešeno sleherne ovire. Diagram je abstraktni stroj, ki je skorajda nem in slep, čeprav naredi, da vidimo in govorimo. Je neka prostorsko-časovna mnogoterost, globoko nestabilna in tekoča, tako rekoč v nastajanju. Gre torej za splošno shemo, prek katere se vzpostavi in vzdržuje specifična mreža oblasti oziroma nadzora, ki povezuje in upravlja posameznike, skupine, institucije, ideje, vrednote, vedenje, skratka, vse elemente družbene realnosti.

[16] Potrebno je opozoriti, da za označevanje te sheme Foucault včasih namesto diagrama uporablja izraz dispozitiv. Zastavi se vprašanje, kakšna je (če sploh) razlika med enim in drugim konceptom? Klepec (2007, 54) pravi, da je diagram po svojih potezah zelo blizu dispozitivu in da prav dispozitivu kasneje skupaj z osrednjim mestom, ki naj bi ga imel pri Foucaultu, Deleuze tudi dodeli poteze in določitve diagrama.

razmerij. Panoptizem je zmožen *»reformirati moralo, zavarovati zdravje, okrepiti industrijo, razširjati izobrazbo, olajšati javne dolžnosti, postaviti gospodarstvo na trden temelj, razvozlati gordijski vozel zakonov o revežih, vse to pa s preprosto arhitekturno zamislijo«* (Bentham 1995).

Na eni strani imamo panoptikon kot arhitekturni koncept zaprte ustanove, postavljene na obrobje in usmerjene k negativnim funkcijam: zaustaviti zlo, pretrgati komunikacije, suspendirati čas. Na drugi strani pa imamo panoptizem. Ta označuje disciplino-mehanizem oziroma funkcionalni dispozitiv, ki izboljša izvrševanje oblasti. Učinkovitost panoptizma je predvsem v tem, da vzpostavi samonadzor[17] oziroma prostovoljno podrejanje posameznikov s pomočjo produkcije negotovosti. Lyon (1994) in Beck (2001) ugotavljata, da je nesimetrično in hierarhično opazovanje postalo del sodobnega projekta uničevanja[18] gotovosti. Zavest, da smo nenehno vidni, zagotavlja samodejno delovanje in obnavljanje oblasti na mikroravni. Vidnost je zato neke vrste past. Panoptizem je politična tehnologija, ki deluje na podlagi subtilnih prisil in omogoča vzdrževanje oblasti.
Ali kakor pravi Servan: *»Bedast despot lahko prisiljuje sužnje z železnimi verigami, toda pravi politik jih precej krepkeje zveže z verigo njihovih lastnih idej; na trdno raven razuma pripne prvi konec; ta vez je toliko bolj trdna, ker ne poznamo njene teksture in ker mislimo, da je naše delo ... na mehkih vlaknih možganov pa stoji neomajen temelj najtrdnejših cesarstev«* (Servan v Foucault 2004, 102).

2.4 DISCIPLINARNA OBLAST

[17] *Takšno nadzorovanje je kajpak specifično moderno, namreč panoptično: posameznik ima vtis, da je lahko kjer koli in kadar koli objekt kvazi božjega nadzorstvenega pogleda. Vsakdo, s katerim stopi v stik, je lahko potencialni špicelj. Tudi subjektivna reakcija na domnevo, da si podvržen sekularizirani totalni kontroli, je pogosto specifično moderna: ponotranjeni strah okrepi samonadzor (self-policing). Na družbeni ravni pa se to izrazi v »mentaliteti tabujev«, ki povzroča negativno magično pogojevanje: posameznik se nauči ustvarjati videz, da je učinkovito nadzorovan (da je »naš«, sistemski človek, mini apartčik, ki se iz notranjega prepričanja giblje v sferi družbeno sprejemljivega)* (Kanduč 2003, 267).

[18] Uničevanje gotovosti lahko vodi v družbeno atomizacijo oziroma anomično stanje. Še huje, razpad zaupanja predstavlja plodna tla za vznik totalitarnih režimov. Nazoren primer totalitarne družbe, ki učinkovito združuje panoptizem, upravljanje s strahom in izgubo zaupanja med posamezniki, prikazuje George Orwell v znamenitem romanu 1984. V tej »futuristični« viziji sveta vladajo tri frakcije, ki se nenehno bojujejo. Toda vojna je navidezna, uporablja se kot pretveza za vzdrževanje izjemnih (nedemokratičnih) razmer in za upravičevanje vsakršnega državnega nasilja. Glavno načelo vladanja se skriva v popolni vidnosti. V slehernem prostoru so posebne video in zvočne naprave, ki redno prikazujejo propagandni material, hkrati pa izvajajo (kot nekakšne kamere) nadzor nad posamezniki. Poleg tega posamezniki drug drugega izdajajo, vsakdo je lahko potencialni vohun. Na ta način je vzpostavljeno permanentno stanje negotovosti, ki se kaže v zelo učinkovitem (samo)nadzoru. Še več, zunanja oblast je dostikrat zgolj iluzija, a vsekakor dovolj močna, da v glavi slehernega posameznika zgradi kletko samoomejevanja in ponotranjenega nadzora.

Na prehodu iz srednjega veka v moderno se preoblikuje tudi dispozitiv oblasti. Če je fevdalizem vzdrževal red z zastrašujočim karnevalom telesnega kaznovanja, je moderna doba, z nastankom industrijskih mest, državne administracije in kapitalističnega podjetništva, terjala drugačen način nadzorovanja in obvladovanja populacije.
V 18. stoletju je prišlo do odpora proti »spektaklu mučenja«, s katerim se je do tedaj obredno razkazovala oblast (Foucault 2004, 59), kar se je v drugi polovici istega stoletja izrazilo skozi reformo kazenskega prava. *»Nova oblast naj ne bi kaznovala nič manj, temveč bolje; nemara naj bi kaznovala manj strogo, a zato bolj univerzalno in bolj neogibno«* (Foucault 2004, 83). *»Kazen se je iz umetnosti neznosnih občutkov spremenila v ekonomijo odvzetih pravic«* (Foucault 2004, 17), prakso spektakularnega mučenja telesa pa je nadomestilo dresiranje duše.

V tem obdobju se je oblikoval nov »panoptični« diagram oblasti, ki je prvič v zgodovini omogočil zares sistematičen nadzor tako posameznikov kot tudi celotne populacije. Oblast srednjeveških kraljestev je obnavljala svojo vitalnost s potratnim izkazovanjem moči, panoptična oblast nacionalnih držav pa temelji na varčnem in doslednem dresiranju duš. Zato ne preseneča, da je panoptikon oblastni stroj zgodnjega kapitalizma: proizvaja namreč novo vrsto podložnikov-delavcev-državljanov (Haggerty 2006, 27). Nov mehanizem oblasti se usmerja na ljudi in njihovo delo(vanje), njegova najpomembnejša značilnost pa je, da se izvaja konstantno in s pomočjo nadzorovanja (Foucault 2008, 37).
Takšno oblast, ki ni v rokah suverena, pač pa jo izvaja anonimni birokratski stroj, Foucault imenuje »disciplinarna oblast«. Disciplina je po besedah Foucaulta *»nekakšna vrsta oblasti, način, kako se izvaja, ki vsebuje cel skupek instrumentov, tehnik, postopkov, aplikacijskih ravni, tarč; je fizika ali anatomija oblasti, tehnologija«* (Foucault 2008, 213). S pomočjo disciplinarne oblasti posameznike nadzorujemo in dresiramo, če je treba tudi kaznujemo, pri čemer kazen ni samo neposredna, fizična, temveč se je spremenila v ekonomijo odvzetih pravic, njen cilj pa je »izdelati« discipliniranega posameznika. Panoptični nadzor in nova vrsta disciplinarne oblasti sta usmerjena h konkretnemu posamezniku z namenom, da ga ukrotita in podredita (Kovačič 2005, 24).

2.5 BIOPOLITIČNA OBLAST

V 17. in 18. stoletju se je oblikovala disciplinarna oblast, ki se je usmerjala na posameznike. V 19. stoletju pa se je pojavila biopolitična oblast, ki se je usmerjala na populacijo. Foucault pravi, da se

je v tem obdobju *»prvič govorilo, da je nemogoče vladati državi brez poznavanja njene populacije«* (Foucault 2008, 67). Sicer so se prvi poizkusi nadzora populacije pojavljali že v antiki in v srednjem veku (npr. Domesday Book iz leta 1086), vendar so bili relativno nedosledni, nesistematični in zato tudi manj učinkoviti.

Disciplinarna oblast se ukvarja s posameznikom in njegovim telesom. Biopolitična oblast pa se ukvarja s »telesom« populacije, ki jo Foucault definira kot *»multiplo telo s številnimi glavami, če že ne z neskončno mnogimi, pa vsaj s tolikimi, da jih ni nujno mogoče prešteti«* (Foucault 1997/2003, 156). Pri biopolitiki, ki nadzoruje populacijo, gre torej za spremljanje pojavov, ki s svojimi ekonomskimi in političnimi učinki nastopijo ter postanejo umestni zgolj na ravni množice. *»Gre za pojave, ki so, če jih vzamemo same na sebi, torej posamezno, naključni in nepredvidljivi, vendar pa predstavljajo na kolektivni ravni konstante, ki jih je mogoče določiti«* (Foucault 1997/2003, 156).

Biopolitična oblast s pomočjo statističnega spremljanja družbenih pojavov, iskanja globalnih kazalcev in povprečnih vrednosti, uvaja regulacijske mehanizme na globalni ravni. S temi mehanizmi pa bolj ali manj uspešno ohranja globalno ravnotežje in obvladuje naključnosti, ki se jim reče »življenje« (Foucault 1997/2003, 156).

Ker se proces regulacije življenjskih procesov populacije izvaja s pomočjo nove vednosti, ki je svojo formalizirano obliko dobila v statistiki, ne preseneča, da oblikovanje biopolitične oblasti sovpada s časom nastanka in razvoja družboslovnih znanosti, predvsem sociologije in statistike.

Inšpektor postane birokrat (ali celo znanstvenik), namesto posameznikov pa pregleduje družbo (Whitaker 1999, 43). Zato Whitaker pravi, da je 20. stoletje obdobje obveščevalne dejavnosti, ki obsega *»avtomatsko in namensko pridobivanje, urejanje, nadomeščanje, analizo, interpretacijo in zaščito informacij in je v svojem bistvu sistematično organizirana birokratska dejavnost«* (Whitaker 1995, 5).

Vendar pa biopolitična oblast ne nadomesti disciplinarne oblasti. Obe vrsti oblasti namreč delujeta vzporedno, se dopolnjujeta in s tem krepita svojo moč. Foucault pravi, da nova regulacijska oblast disciplinsko *»zaobseže, integrira, deloma spremeni, predvsem pa jo izkorišča za to, da se vanjo nekako vsadi, in se s pomočjo te predhodne disciplinarne tehnike dejansko utrdi«* (Foucault 1997/2003, 153-154). Če *»disciplina poskuša vladati množici ljudi, kolikor more, in mora ta množica razpasti na individualna telesa, ki jih je mogoče nadzorovati, dresirati, izkoriščati ter morebiti kaznovati«*, potem biopolitična oblast *»naslavlja množico ljudi, toda ne, kolikor so ti ljudje zvedeni na telesa, temveč nasprotno, kolikor ta tehnologija oblikuje neko globalno množico, ki jo zadevajo skupni procesi...«* (Foucault 1997/2003, 153-154). S tem nova tehnologija oblasti prejšnjo nadgradi.

Disciplinarna oblast se torej osredotoča na posameznika, na telo, biopolitika pa je usmerjena na življenje, na množico. Poizkuša nadzirati in regulirati *»niz naključnih dogodkov, ki se lahko proizvedejo v živi množici ... poizkuša kontrolirati njihovo verjetnost, vsekakor pa uravnovesiti njihove učinke ... stremi k nekakšni homeostazi, toda ne z individualno dresuro, temveč z globalnim ravnovesjem«* (Foucault 1997/2003, 158-159).
»Ti dve vrsti oblasti sestavljata dva niza: niz telo – organizem – disciplina – institucije; in niz populacija – biološki procesi – regulacijski mehanizmi – država« (Foucault 1997/2003, 159). Ker niza/tehnologiji/vrsti oblasti nista na isti ravni, se med seboj ne izključujeta, pač pa se dopolnjujeta in s tem krepita svojo moč.

Če je družba suverenosti[19] usmrtila ali pustila živeti, potem družba regulacije omogoča življenje ali pa pusti umreti (Foucault 1997/2003, 157). Nova oblast postane pastoralna, začne se uvajanje oblastnih aparatov, ki omogočajo ne le opazovanje, temveč tudi neposredni poseg in manipuliranje z življenjem, s tem pa se začenja oblast nad življenjem, ki deluje tako, da okrog naključnosti namešča varnostne mehanizme, ki ne delujejo na ravni posameznika, temveč na ravni populacije. Zato danes nadzorovanje posameznikov ni zgolj sredstvo disciplinskega nadzora, temveč tudi sredstvo za zagotavljanje pravic družbene participacije; posamezniki smo že s samo participacijo v družbi (uveljavljanje državljanskih, zdravstvenih, zaposlitvenih in drugih pravic) izpostavljeni nadzoru, ta izpostavljenost pa je nujna za naše preživetje. Neprilagojenih posameznikov ni več potrebno neposredno kaznovati, dovolj je le, da jih izvržemo in »pustimo umreti« (Kovačič 2006, 27). Na področju kaznovalne politike pa se specifika regulacijske oblasti kaže predvsem v proaktivni identifikaciji tveganja, kar pomeni, da krivdo ali nedolžnost posameznika čedalje bolj nadomešča tveganje, ki ga neka skupina oziroma posameznik kot njen del predstavlja za organizacijo, državo ali družbo (Whitaker 1999, 22).

2.6 INFORMACIJSKI NADZOR

Družbeni nadzor se je še posebej okrepil[20] z razvojem informacijskih in mikroprocesorskih

[19] Z izrazom »družba suverenosti« Foucault označuje predmoderne (antične in srednjeveške) družbe, ki jim je vladal suveren (vladar).
[20] Razvoj tehnologije je omogočil povečanje in pocenitev zbiranja in obdelave podatkov ter informacij, zato se je nadzor lahko razširil. Hkrati je, predvsem zaradi nadzorovanja potrošnikov, prišlo do tega, da imajo podatki in informacije, ki so bili včasih popolnoma vsakdanji in nezanimivi, zdaj veliko tržno vrednost. Poleg tega se nadzor

tehnologij. V informacijski družbi nadzor ni več le optičen, ampak se pojavlja tudi na območju digitalnih signalov[21]. Če je bil Benthamov panoptikon iz leta 1791 predviden za nadzorovanje in obvladovanje zaprte populacije, je zdaj panoptizem vključen v vsakodnevno življenje slehernega posameznika. To se posebej očitno kaže v množični produkciji dosjejev, ki temelji na praksi obsežnega zbiranja in medsebojnega povezovanja različnih podatkov. Roger Clarke je za tak nadzor uvedel izraz »podatkovni nadzor« (ang. dataveillance), ki je opredeljen kot *»sistematično nadzorovanje človeških dejanj ali komunikacij s pomočjo informacijske tehnologije«* (Clarke v Lyon 2003, 168). Sodobna tehnologija (računalniki, bančne kartice, RFID čipi, mobilni telefoni, GPS, idr.) omogoča nenehno kopičenje podatkov in beleženje najrazličnejših aktivnosti posameznikov, s tehnikami analize omrežji in izkopavanja podatkov pa se gradijo profili celih populacij. Posameznik tako postaja sam svoj dosje in v sodobni družbi praktično ne more obstajati, ne da bi bil nadzorovan. S pomočjo dosjejev je mogoče učinkovito nadzorovati dejavnosti in potrebe ljudi, zapisovanje pa omogoča tudi nadzor nad preteklimi dogodki.

Nadzorovanje v sodobni družbi izvajata tako država kot tudi zasebni sektor. Država uporablja nadzor za vzdrževanje in krepitev svoje moči, kapitalistične korporacije pa za obvladovanje potrošnikov, kar v perspektivi omogoča večji zaslužek. Deleuze (v Salecl 1993, 47-48) pravi, da je potrošniško oglaševanje postalo nov instrument družbenega nadzora, ki državljane obvladuje z zadolževanjem in pripenjanjem na različne (npr. finančne) sheme odvisnosti.
Lyon (2003, 172) je prepričan, da se bo v prihodnosti najbolj povečeval prav »komercialni nadzor«, ki ga »nežno« (pri nakupih v trgovini, pri telefoniranju in brskanju po spletu) izvaja zasebni sektor, čeprav po tako pridobljenih podatkih nemalokrat poseže tudi država. Tak nadzor je utemeljen v praksi profiliranja potrošnikov in je na videz prijazen, saj potrošnika potiska kamor si želi oziroma ga zalaga z dobrinami in vsebinami, ki ustrezajo njegovemu okusu ali potrebam (Kovačič 2003, 33). Nadzor potrošnikov pa je posebej problematičen zato, ker se mu v veliki meri podrejamo

globalizira. Predvsem v zadnjem času je opaziti globalizacijo mednarodnih varnostnih in administrativnih sistemov, pa tudi globalizacijo komercialnega nadzorovanja (Kovačič 2006, 31).

[21] Leta 1983 je David Burnham opozoril na tako imenovano *elektronsko sled*, ki jo posamezniki puščajo za sabo. Vsakič ko posameznik dvigne slušalko, uporabi bankomat ali plačilno kartico, gre na banko, obišče zdravnika, se poroči, uporabi mobilni telefon..., avtomatski sistemi ali institucije ta dogodek *zaznajo* in *zabeležijo*. Elektronska sled je torej informacija, ki se shranjuje rutinsko in kaže dejavnost nekega posameznika. Večina teh podatkov, Burnham jih je poimenoval tudi *transakcijski podatki*, se zapisuje in vsaj nekaj časa tudi hrani. Pomembno je poudariti, da imajo sodobni nadzorovalni sistemi poleg shranjevanja tudi zmožnost kreacije in destrukcije podatkov ter informacij, zato ob tem seveda nastaja vprašanje, ali zaupati shranjenim podatkom. Vendar pa je povečana moč nadzorovanja v tem, da je tako zbrane podatke mogoče povezati. S povezavo in njihovo obdelavo lahko pridemo do novih vrednih podatkov in informacij, kar je za posameznika lahko škodljivo ali celo nevarno – zaradi ogrožanja njegovih pravic. Prav povezavo in kombiniranje različnih podatkov pa omogočajo sodobne informacijsko-komunikacijske tehnologije. Zato se lahko zgodi (če podatki niso ustrezno zavarovani), da naključno ali z nekim namenom zbrani podatki postanejo dostopni osebam ali institucijam, ki jih niso pooblaščene uporabljati, ali pa ti subjekti začnejo podatke uporabljati za drugačne namene (Kovačič 2006, 27).

prostovoljno: lep primer so kartice ugodnosti, ki ponujajo razne popuste in bonitete v zameno za naše osebne podatke. Ali kot pravi Kovačič: *»Potrošniki in državljani živimo v svetu, v katerem se moramo nujno odpovedati delu svoje zasebnosti na račun večje funkcionalnosti in obvladovanja kompleksnosti življenja v sodobni družbi«* (Kovačič 2006, 34). Če je bila v disciplinarnih družbah 18. in 19. stoletja glavni izvajalec nadzora država, potem danes to vlogo čedalje bolj prevzema zasebni sektor.

Primerjavo panoptičnega nadzora v moderni in postmoderni družbi prek povzemanja Deleuza prikaže Klepec (2007, 45-56). Pravi, da imamo v moderni (disciplinarni) družbi podpis, ki napoti na posameznika, in matično številko, ki kaže na njegov položaj v množici. Na drugi strani pa postmoderna (nadzorstvena) družba ne deluje več (le) s pomočjo podpisa ali številke, pač pa s pomočjo gesla oziroma šifre. V disciplinarni družbi je obstajala instanca, ki je izdajala ukaze, in instanca, ki jih je prejemala. V družbi nadzora[22] pa pride do razbitja obeh instanc. Tista, ki izdaja ukaze, postane anonimen sistem, tista ki jih prejema, pa izgubi identiteto, se razcepi in postane dividuelna.

Disciplinarna družba je sestavljena iz prostorsko ograjenih in arhitektonsko prepoznavnih institucij, kjer so meje moči in nadzora jasno začrtane. Ravno nasprotno pa v družbi nadzora ni (več) jasnih ločnic, ni pravega začetka in konca, panoptični nadzor nenehno prežema celotno družbeno tkivo.

Če v disciplinarni družbi prehajamo iz enega zaprtega okolja v drugo, vsako izmed teh okolji pa ima svoje zakone in pravila – najprej družina, nato šola (»Nisi več doma!«), pa nato morebiti kasarna (»Nisi več v šoli!«), zatem tovarna (»Nisi doma, v šoli, v vojski!«), tu in tam bolnišnica, ter, če tako nanese usoda, konec koncev lahko tudi zapor, pa so meje v družbi kontrole sicer vzpostavljene – spomnimo na Guattarijev primer mesta, v katerem bi lahko vsakdo, zahvaljujoč svoji elektronski kartici, ki bi dvignila to ali ono zapornico, zapustil svoje stanovanje, ulico, okoliš - toda pomembne niso meje, prav tako ne osrednji računalnik, ki ves čas beleži mesto znotraj sistema, temveč to, da je tak režim neskončen, da se nenehno širi in spreminja (Klepec 2007, 56).

[22] Izraz »družba nadzora« je v osemdesetih letih skoval Gary T. Marx, devet let kasneje pa ga je uporabil kanadski pooblaščenec za varstvo osebnih podatkov, David Flaherty (v Kašnik 2006, 12). Sama ideja »družbe nadzora« jasno kaže, da je življenje v sodobni družbi prežeto z nadzorom. Panoptično Oko je preseglo utesnjujoče spone zaporov, tovarn, šol, bolnišnic, in razlilo svoj prediren pogled prek vsakdanjega življenja slehernega posameznika. Vendar pa Lyon (1994, 31) opozarja, da ima družba nadzora več kot zgolj en obraz. Lahko se jo interpretira negativno, kot Webrovo »železno kletko« birokratske racionalnosti ali kot Foucaultovo »disciplinarno družbo«. Lahko pa se jo interpretira pozitivno, kot sistem nediskriminatornega zagotavljanja pravic in dolžnosti državljanov.

2.7 ONKRAJ PANOPTIKONA: OMRŽENI NADZOR

V Foucaultovem *Nadzorovanju in kaznovanju* je začrtan osnovni diagram nadzornega mehanizma v moderni družbi. Panoptična paradigma[23] je postavila okvir teoretičnim razmišljanjem o nadzoru. Vendar pa v postmoderni informacijski družbi nastajajo številne »anomalije«, ki jih takšen teoretični model ni zmožen učinkovito pojasniti (Lyon 1994).

Se na obzorju zarisuje nov diagram nadzornega mehanizma? Morda. Trendi namreč kažejo, da se nadzor povečuje, saj se procesi klasifikacije, zbiranja in zapisovanja podatkov in informacij neprenehoma širijo, življenja navadnih posameznikov pa postajajo čedalje bolj transparentna. Razcvet računalništva je skupaj z naprednimi statističnimi metodami in tehnikami za izkopavanje podatkov vzpostavil nove razsežnosti nadzora. Po besedah Kovačiča (2006, 31) nadgradnja naštetih metod in tehnologij s sistemi umetne inteligence omogoča preskok na novo raven, na raven preventive in predvidevanja. Nadzorna tehnologija tako ne čaka, da se zgodi neko dejanje oz. dogodek, pač pa ukrepa že vnaprej na podlagi podatkov in predvidevanj. In ker so za informacijsko družbo značilna omrežja, se zdi verjetno, da nastaja nova oblika[24] *omrežnega nadzora*, ki ni več centraliziran (kot panoptikon ali kot Orwellov Veliki brat), pač pa razpršen na različne formalno ločene sisteme, ki so sposobni med seboj komunicirati. Deleuze in Guattari (v Kašnik 2006, 18) predlagata analogijo z drevesom. Nadzor v disciplinarnih družbah je podoben deblu z vejami, v sodobnih družbah nadzora pa spominja na korenine, ki so skoraj neopazne/prikrite in razvejane/decentralizirane, zato je tudi sodoben nadzor toliko bolj učinkovit, saj nadzirane subjekte zapelje v lažen občutek svobode in neobremenjenosti, hkrati pa zaradi neštetih »panoptičnih očes« na omrežju vzpostavlja skoraj popoln pregled nad življenjem posameznikov in populacij.

[23] Več o paradigmah glej v Kuhn, T. S., Struktura znanstvenih revolucij (1998).

[24] Marx in Gordon (v Bogard 2006, 111) za označevanje nove oblike (hiper)nadzora uporabljata izraz »elektronski panoptikon«, Mathiessen (1997 v Bogard 2006, 111) pa govori o »sinoptikonu«.

3 TEHNOLOGIJE NADZORA

O nadzoru se danes govori predvsem v povezavi s sodobno tehnologijo. Vendar se je ob tem potrebno zavedati, da je nadzor mnogo starejši kot tehnologija in je obstajal tako rekoč od samega začetka človeške zgodovine. Nadzorovanje brez tehnologije je potekalo predvsem s pomočjo opazovanja, prisluškovanja in zasledovanja. Tak nadzor so izvajale in ga še izvajajo tako državne kot tudi zasebne organizacije in sicer s pomočjo vohunov, tajnih agentov, zasliševalcev, policistov, detektivov, zdravnikov, socialnih delavcev, uradnikov, duhovnikov, idr. Na ta način pridobljeni podatki so se beležili v pisnih zapisih (»papirnatih dosjejih«), ki so bili za nadaljnjo analizo in obdelavo mnogo bolj okorni kot sodobni elektronski zapisi. Kljub tehnološkim omejitvam pa so elementarne tehnike nadzora omogočale (z vidika ohranjanja oblasti) učinkovito delovanje nekaterih totalitarnih režimov, ki so bili utemeljeni v praksi nenehnega izvajanja nadzora in sejanja nezaupanja ter strahu (Garton v Murakami Wood 2006, 16).

Razvoj računalniške in informacijske tehnologije v drugi polovici dvajsetega stoletja pa je »navaden« družbeni nadzor dvignil na novo kvalitativno in kvantitativno raven. Računalniki, omrežja, elektronske naprave, RFID kartice, biometrija, sateliti, video kamere in drugi tehnološki produkti so omogočili neprimerno večje in bolj natančno zbiranje, obdelovanje in arhiviranje najrazličnejših podatkov o skupinah in posameznikih. Če je panoptični nadzor temeljil na optični (ne)vidnosti, potem je novi »omrežni« nadzor utemeljen na »elektronski sledi«, ki jo posameznik pušča tako rekoč povsod, kjer pride v stik z računalniško in informacijsko tehnologijo. Tak nadzor ni le bolj obsežen, ampak tudi mnogo bolj učinkovit in z vidika človeških virov manj potraten, saj temelji na uporabi avtomatiziranih procesov in sistemov za samodejno prepoznavo in obravnavo nadzorovanih posameznikov, v primeru množičnega nadzora, ki je utemeljen v statistiki, pa tudi populacij.

3.1 PODATKOVNI NADZOR

Ker nadzor predstavlja eno od normalnih funkcij vsake človeške družbe, je seveda obstajal že dolgo pred razvojem informacijske tehnologije. Čeprav je razvoj birokratskih organizacij v 18. in 19. stoletju vzpostavil prakso sistematičnega zbiranja podatkov o posameznikih in skupinah, je tak nadzor sprva ostal omejen na ustvarjanje pisnih (»papirnatih«) dosjejev, ki jih je bilo ob odsotnosti informacijske tehnologije težko in zamudno analizirati. Nazoren primer slabše učinkovitosti nadzora, ki ni podkrepljen z ustrezno tehnologijo, je popis prebivalstva. Ta se je izvajal že v nekaterih antičnih državah in kraljestvih, v modernih nacionalnih državah pa je sploh postal razširjen. Vendar zbiranje podatkov še ni predstavljalo največje težave. Mnogo bolj problematično in zamudno je bilo razvrščanje, kategoriziranje in preštevanje podatkov, saj je bilo vse tovrstne analize potrebno opraviti ročno.
Konec 19. stoletja pa je Herman Hollerith izumil posebno napravo za obdelavo podatkov. Poimenovali so jo Hollerithov stroj (ang. Hollerith machine) in velja za predhodnika računalnikov. Hollerithov izum so za analizo popisnih podatkov prvič uporabili pri ameriškem popisu prebivalstva leta 1890 in pri tem prihranili okrog pet milijonov dolarjev. Uporaba Hollerithovih strojev je analizo podatkov pocenila in pospešila. To so kmalu spoznale tako vlade drugih držav, kot tudi različna podjetja, ki so začela za analizo svojih podatkov uporabljati tovrstne naprave (Kovačič 2003).

Računalniška in informacijska tehnologija je razvoj bistveno okrepila in poglobila. Podatki se niso več zapisovali v papirnati, pač pa v elektronski obliki, ki je omogočila učinkovitejše zapisovanje, hranjenje, obdelovanje in posredovanje podatkov.
Z razvojem informacijskega nadzora se je pojavila tudi t.i. elektronska sled (nanjo je prvič opozoril David Burnham leta 1983), ki jo ljudje s svojimi dejavnostmi puščamo za sabo. Vsakič, ko posameznik dvigne slušalko, uporabi bankomat ali plačilno kartico, gre na banko, obišče zdravnika, se poroči, uporabi mobilni telefon, avtomatski sistemi ali institucije ta dogodek zaznajo in zabeležijo. Elektronska sled je torej informacija, ki se shranjuje rutinsko in kaže dejavnosti nekega posameznika (Kovačič 2006, 27).
Sodobni »podatkovni« nadzor, ki se ga pogosto označuje z izrazom »dataveillance« (Clarke 1988) in kaže na pomembnost podatkovnih baz, je v veliki meri mogoč prav zaradi množične uporabe osebnih, zdravstvenih, bančnih, nakupovalnih in drugih kartic, ki vsebujejo podatke o identiteti posameznika. Posebej pomembne so tako imenovane pametne kartice, ki imajo pomnilnik za poznejše zapise in omogočajo združevanje podatkov iz državnih in zasebnih podatkovnih baz (Lyon 2003).

Z razvojem sodobne tehnologije so se torej razvijale in dopolnjevale tudi različne baze podatkov.

Zato Lyon (2003) o sodobni družbi govori kot o družbi dosjejev, saj o skoraj slehernem posamezniku obstajajo kakšne evidence, ki služijo preverjanju identitete, finančnega stanja, kupnih navad ali česa drugega. Posebej velja izpostaviti marketinške[25] baze podatkov, ki jih Lyon opisuje kot *»več milijard dolarjev vredno industrijo, ki z namenom profiliranja potrošnikov išče in zbira podatke o posameznikovih navadah, nakupih, izbirah in življenjskih ciljih«* (Lyon 2003, 162).
Podjetja (med najbolj znana sodijo Choice Point, Lexis Nexis, Axciom, Abacus Alliance), ki se ukvarjajo s podatkovnim rudarjenjem v komercialne namene, so razširjena predvsem v Združenih državah, kjer zakonodaja takšno zbiranje, hranjenje in posredovanje podatkov v privatnem sektorju dopušča. Vendar pa tako zbrani podatki niso uporabni le za usmerjeno oglaševanje[26] oziroma (pre)prodajo, ampak se pogosto posredujejo varnostnim, obveščevalnim, davčnim in drugim državnim službam.

Enako pomembno kot ustvarjanje podatkovnih baz, je njihovo medsebojno povezovanje, ki omogoča preskok na novo raven »omrežnega« nadzora. Povezovanje[27] razpršenih podatkov omogoča izdelovanje obsežnih podatkovnih profilov o posameznikih. Uporaba naprednih tehnik za izkopavanje podatkov pa omogoča iskanje »nevidnih« povezav med razpršenimi podatki in na ta način ustvarjanje popolnoma novih informacij.
Povezovanje[28] podatkovnih centrov predstavlja torej enega osrednjih trendov sodobnega nadzora, kar potrjuje tudi podatek, da ZDA za razvoj medsebojno povezanih podatkovnih baz letno porabijo več kot 370 milijonov dolarjev. Še več, analitiki CIA so prepričani, da največjo grožnjo ZDA predstavljajo decentralizirane in geografsko razpršene teroristične, anarhistične in disidentske

[25] Murakami Wood (2006, 20) deli podatke o potrošnikih v štiri osnovne kategorije: (1) Geografski podatki se nanašajo na prostor, kjer deluje ali živi posamezni potrošnik (sem sodijo telefonske številke, poštne številke, internetne domene in URLji); (2) Geodemografski podatki združujejo demografske in geografske podatke (tak primer je GIS – geografski informacijski sistem); (3) Psihografski podatki vključujejo sociološke in psihološke karakteristike potrošnikov (na primer družbeni razred, vrednote, življenjski stil, starost, tip osebnosti); (4) Behavioristični podatki se nanašajo na vedenjske značilnosti potrošnikov.

[26] Usmerjeno oglaševanje je značilno za Google in Yahoo, kjer se oglasi usmerijo na uporabnika iskalnega portala, analizirajo pa ga s pomočjo zgodovine brskanja in emailov, ki se hranijo v podatkovnih bazah. Google, trenutno najbolj znan in razširjen iskalnik, hrani identifikacijske podatke za vsako brskanje po internetu. IP naslovi in iskane fraze se hranijo do 18 mesecev. Google prav tako skenira in analizira vsebino elektronske pošte uporabnikov Gmaila.

[27] Na internetu je dostopno velikansko število podatkov in informacij, večina jih je sicer nepovezanih, kar pa ne pomeni, da se jih ne da povezovati. Baze je mogoče povezovati s pomočjo tehnik računalniškega ujemanja in povezovanja zapisov (angl. computer matching and record linkage), lahko pa so podatkovne baze že v izhodišču zasnovane kot relacijske, kar omogoča povezovanje med njimi. Te tehnike so prvi uporabili vladni oddelki v ZDA v poznih 70. letnih, njihova uporaba pa se je razširila v 90. letnih (Lyon 2006, 9).

[28] Ni odveč poudariti, da je povezovanje podatkovnih baz pogojeno s številnimi nevarnostmi. Ena je ta, da lahko *»zbrani podatki postanejo dostopni osebam in institucijam, ki jih niso pooblaščene uporabljati, ali pa ti subjekti začnejo podatke uporabljati za drugačne namene«* (Kovačič 2003, 27), kar se dogaja predvsem v primerih združevanja državnih (bolnišnice, policije, sodstva, davčne službe) in zasebnih (banke, zavarovalnice, trgovine) podatkovnih baz.

celice, ki jih je praviloma mogoče učinkovito odkriti le s pomočjo analize omrežji in podatkovnim profiliranjem – seveda pa je predpogoj za to množični[29] podatkovni nadzor celotne družbe.

Drugo pomembno orodje podatkovnega nadzora pa je analiza[30] socialnih omrežji. Gre za nekakšne zemljevide posameznikov in skupin, ki prikazujejo medsebojne povezave različnih ljudi. Nekatere spletne strani za družabno mreženje[31] (na primer Facebook[32], MySpace, LinkedIn, Twitter, Orkut, Netlog, idr.) pa analize družbenih omrežji nadgrajujejo še s psihološkimi, behavioristističnimi in sociodemografskimi profili uporabnikov.
Ena od večjih nevarnosti analize in nadzora družabnih omrežji je ta, da se veliko posameznikov ne zaveda takšnega nadzora oziroma podcenjujejo tveganja, ki iz tega izvirajo, zato pristanejo na nadzor tako rekoč prostovoljno. Težava je tudi v tem, da nekatere spletne strani ali storitve brez prostovoljnega posredovanja osebnih ali drugih podatkov sploh niso dostopne. Druga težava pa je trgovanje podatkov v zameno za ugodnosti (npr. kartice ugodnosti v trgovinah in popusti, ki jih omogočajo). Pogosto se uporabniki niti ne zavedajo, da podatke posredujejo tako rekoč zastonj in da bodo ti uporabljeni tudi za nadzor.

3.2 RAČUNALNIŠKI IN INTERNETNI NADZOR

Razvoj računalniške in informacijske tehnologije je dodal nadzorovanju povsem nove razsežnosti. Po eni strani je računalnik povečal učinkovitost že obstoječih tehnik nadzora, po drugi strani pa je vzpostavil novo vrsto nadzora, ki je osredotočena na prestrezanje, klasificiranje in analizo elektronskih podatkov. Izvajanje zakonitega in nezakonitega nadzora nad računalniki in shranjenimi podatki je zanimivo tako za državne kot tudi za zasebne institucije.

---

[29] Eden takšnih poizkusov podatkovnega nadzora celotne populacije je Hancock, ki ga je razvila družba AT&T, deluje pa na podlagi obdelave in filtriranja ogromnega števila podatkov o telefonskih klicih in internetni zgodovini. Program s pomočjo filtrov (podobno kot Echelon) iz množice podatkov izloči tiste, ki so uporabni in jih posreduje človeškim operaterjem v nadzornih centrih.

[30] Ena od raziskav (Soltern in Jones v Firbas 2009, 26) analize spletnih socialnih omrežji je s posebnim preizkusom pokazala, kako je mogoče enostavno in v kratkem času pridobiti veliko število podatkov. Preizkus je bil izveden s pomočjo posebnega programa »crawlerja«, ki je izvajal samodejno indeksiranje zanimivih spletnih strani in iz njih prenašal relevantne podatke. Na ta način je crawler v kratkem času nabral izjemno veliko količino uporabnih podatkov.

[31] Ang. social networking

[32] Facebook je eno najbolj priljubljenih družabnih omrežji in združuje prek 250 milijonov aktivnih uporabnikov iz vsega sveta. Zaradi velikosti in zelo velikega števila uporabnikov je priljubljena tarča napadalcev, ki želijo pridobiti podatke o posameznikih. Ena od nevarnosti Facebooka in podobnih omrežji je tudi v tem, da v ozadju poteka trgovanje s podatki, ki jih uporabniki prostovoljno dajejo na omrežje.

Nezakonit oziroma nepooblaščen dostop do podatkov, ki so shranjeni na posameznem računalniku, je mogoč z uporabo različnih tehnik:

- **Računalniški virus** je ena od osnovnih metod za manipulacijo podatkov na računalniku. Gre za zlonamerni program, ki je namenjen kontaminaciji informacijskih sistemov in računalniške opreme (Kovačič 2003, 57). Virus ponavadi povzroča škodo, pogosto v obliki sistemskih napak ali izgube podatkov, ni pa namenjen neposrednemu nadzorovanju vsebine podatkov (Tulloch v Firbas 2009, 23). Za svojo reprodukcijo potrebuje nek drug program (ponavadi je to izvršitvena datoteka) v katerega se namesti. Ko uporabnik zažene okuženi program, se virus reproducira in na ta način okuži še druge datoteke. Ena od značilnosti virusov je ta, da se reproducirajo eksponentno, zato lahko hitro okužijo ves sistem (Brain v Firbas 2009, 23).

- **Računalniški črv** je še ena pomembna metoda za manipulacijo podatkov na računalniku. Gre za zlonamerno programsko kodo, ki za razliko od virusa za svoje razmnoževanje ne potrebuje »gostitelja« oziroma drugega programa (Tech Faq v Firbas 2009, 24). Računalniški črv za svoje delovanje izkorišča varnostne ranljivosti operacijskih sistemov in programov, ki so povezani z internetom (sem sodijo predvsem spletni brskalniki in odjemalci elektronske pošte). Računalniški črv izkoristi varnostne ranljivosti, se prek njih namesti v nek računalnik in se nato v sistemu razmnožuje (Brain v Firbas 2009, 24). Črvi so pomembni predvsem zato, ker omogočajo ustvarjanje omrežji »botov« (ang. botnet) oziroma računalnikov, ki brez uporabnikove vednosti samodejno izvajajo različne operacije (na primer pošiljajo nezaželeno elektronsko pošto ali izvajajo napade na druge spletne strani) (Firbas 2009, 24).

- **Trojanski konj** je zlonamerni program, ki se ne more razmnoževati samodejno. Največkrat v računalnik vstopi pod krinko drugega »legitimnega« programa. Ko nič hudega sluteč uporabnik tak program zažene, se ob tem na računalnik namesti tudi trojanski konj (Kovačič 2003, 56). Trojanski konji se uporabljajo predvsem za nepooblaščen dostop in upravljanje z okuženim računalnikom.

- **Napad z grobo silo** (ang. brute force attack) predstavlja enega bolj enostavnih načinov dostopa do šifriranih podatkov oziroma gesel. Napad deluje tako, da poseben program z zelo

hitrim preizkušanjem različnih kombinacij znakov ugane geslo. Težava se lahko pojavi takrat, ko je geslo zelo dolgo in zapleteno, kar pomeni, da se proces ugibanja precej zavleče (Firbas 2009, 25).

- **Socialni inženiring**[33] sodi med napredne metode za pridobivanje podatkov iz računalnikov. Gre za obliko napada, ki ne temelji na uporabi tehnologije (čeprav lahko vključuje tudi uporabo tehnologije), ampak izkorišča psihične značilnosti ljudi (zaupljivost, naivnost, nevednost) za manipulativne namene. Pri socialnem inženiringu napadalec skuša žrtev prepričati, da mu zaupa določene informacije, ki omogočajo dostop do informacijskega sistema oziroma napadalcu omogočajo, da zaobide določene varnostne mehanizme (Kovačič 2003, 41-42).

- **Spletno ribarjenje** je eden od načinov pridobivanja osebnih podatkov s pomočjo ponarejanja obstoječih spletnih strani. Napadalec sname izvorno kodo obstoječe spletne strani in jo namesti na svoj strežnik. Prav tako oblikuje URL naslov, ki je čimbolj podoben kopirani strani. Nato napadalec prek elektronske pošte pošlje žrtvi obvestilo, v katerem se pretvarja, da gre za uradno stran in naproša za obisk povezave, ki pa v resnici vodi na lažno stran. Na lažni strani napadalec prosi žrtev za vnos določenih osebnih podatkov, npr. geslo bančnega računa in številko kreditne kartice. Ko žrtev vtipka podatke, jo lažna stran preusmeri na originalno stran, zato veliko ljudi prevare ne opazi (Firbas 2009, 26).

- **Tempest napad** temelji na prestrezanju elektronskih signalov. Računalniška oprema tako kot vse elektronske naprave oddaja elektromagnetne signale, ki jih je mogoče prestrezati s pomočjo anten in širokopasovnih sprejemnikov. V tem smislu so najbolj ranljivi katodni monitorji (CRT) in televizije, kjer je mogoče zajemati informacije z relativno poceni opremo (Kuhn 2004). Prestrezanje signalov pa je mogoče tudi pri novejših LCD monitorjih (Backes in drugi 2008). Izjema niso niti drugi kosi računalniške opreme. Raziskovalcem je z opremo za 60 evrov uspelo izdelati napravo, ki prestreza elektromagnetne signale računalniške tipkovnice. Naprava deluje s pomočjo laserja, ki ga je potrebno usmeriti v tipkovnico ali na prenosni računalnik, deluje pa na razdalji do treh metrov (Mills Abreau v Firbas 2009, 27).

[33] Nekaj primerov socialnega inženiringa (Beaver 2007, 61-62): (1) Napadalec se predstavi kot član podporne službe. Uporabnika ciljnega računalnika skuša prepričati, da mora namestiti nov varnosti popravek – ta je v resnici trojanski konj, ki napadalcu omogoči nedovoljen dostop do računalnika prek interneta; (2) Napadalec skuša pod krinko podporne službe pridobiti administratorjevo geslo, ki omogoča popoln dostop do računalnika; (3) Napadalec skuša s pomočjo metode ribarjenja (ang. phishing) prek elektronske pošte od »žrtev« pridobiti gesla za dostop do računalnikov ali spletnih storitev (npr. bančnega računa, elektronske pošte, idr.).

Ena od nevarnosti tempest napada je razdalja. Z najsodobnejšo opremo je kljub oviram mogoče prestrezati signale do kilometra daleč. NSA to metodo uporablja že kar nekaj časa (Singel v Firbas 2009, 27).

- **Cold boot napad**: V javnosti velja prepričanje, da se podatki v delovnem pomnilniku (RAM) računalnika zbrišejo v trenutku, ko niso več v uporabi. Vendar pa raziskave kažejo, da podatki v pomnilniku ostanejo kratek čas tudi po tem, ko se računalnik izključi oziroma celo v primeru, ko se delovni pomnilnik odstrani iz matične plošče. S hlajenjem pomnilnika pa se podatki lahko obdržijo še dlje. Za izvršitev cold boot napada mora imeti napadalec fizični dostop do računalnika, ki mora biti prižgan. Napadalec nato računalnik izklopi iz električnega omrežja in ga s kratkim časovnim razmikom ponovno priklopi. Iz USB ključa zažene prirejen operacijski sistem, ki omogoči zajem podatkov iz delovnega pomnilnika računalnika. Napad je mogoče izvesti tudi tako, da se iz računalnika fizično odstrani delovni pomnilnik in se ga vstavi v drug (napadalčev) računalnik s prednaloženim prirejenim operacijskim sistemom. S to metodo je mogoče pridobiti praktično vsa gesla, ki jih nek računalnik hrani (Halderman in drugi v Firbas 2009, 28). Pred napadom se je mogoče zaščititi in sicer tako, da ob izklopu računalnik še vedno nadzorujemo vsaj nekaj minut, saj se v tem času podatki iz delovnega pomnilnika navadno izbrišejo (Center for information technology policy v Firbas 2009, 28).

Če so računalniki povzročili kvalitativno spremembo nadzorovanja, to še toliko bolj velja za računalniška omrežja, predvsem za internet. Na začetku devetdesetih let prejšnjega stoletja so bili nekateri sociologi prepričani, da je internet zaradi svojih lastnosti že po svoji naravi odporen proti nadzorovanju s strani države. Po njihovem mnenju naj bi se tehnologija razvijala proti čedalje večji svobodi in neodvisnosti od državnega nadzora (Boyle 1997). To je seveda veljalo samo na začetku, ko internet še ni bil močno razširjen in je bil za državo ter njene organe, pa tudi kapitalistične organizacije, nekaj novega in neobvladljivega. Vendar pa Boyle ugotavlja, da je pojav »tehnologij svobode« vedno potegnil za sabo poostritev mehanizmov nadzora. Danes različne državne zakonodaje čedalje bolj obvladujejo internet, državni organi in podjetja pa celo na novo odkrivajo privlačnost nadzorovanja po internetu (Kovačič 2003, 39).
Ker internet omogoča povezovanje formalno ločenih nadzornih sistemov prek telekomunikacijskih sredstev, se zdi, da je panoptičnost že vgrajena vanj (Kovačič 2003, 40).

Ena najbolj razširjenih komunikacijskih praks na internetu, ki mnogim uporabnikom daje lažen

občutek anonimnosti in zasebnosti, je deskanje po svetovnem spletu, kamor sodi predvsem obiskovanje različnih spletnih strani in iskanje informacij. Pri tem gre praviloma za pasivno prebiranje oziroma opazovanje vsebine spletnih strani, pri čemer uporabnik navidez ne posreduje nobenih informacij strežniku, kjer se nahaja neka spletna stran. Do vidnejše izmenjave informacij pride šele takrat, ko uporabnik obiskani spletni strani izrecno posreduje določene podatke, npr. ko vpiše iskani niz besed v spletni iskalnik ali ko izpolni različne obrazce (Klemenčič 2003, 106).

Čeprav na prvi pogled to ni očitno, že samo deskanje po svetovnem spletu predstavlja vrsto tveganj, ki se nanašajo predvsem na prikrito zbiranje podatkov o uporabniku, kar pa večinoma ni pravno urejeno. Med postopkom običajnega deskanja po spletu namreč svetovno računalniško omrežje in njegovi udeleženci (ponudniki telekomunikacijskih storitev, ponudniki internetnih storitev, lastniki oziroma upravljavci spletnih strani, posebne oglaševalske agencije v internetu, ipd.) zbirajo in obdelujejo vrsto informacij na način, ki je uporabniku skrit (Klemenčič 2003, 106).

Pri dostopu do vsake spletne strani uporabnik nevede praviloma »pusti« vsaj sledeče podatke: vrsto operacijskega sistema v računalniku, tip in različico spletnega brskalnika, protokol, ki je bil uporabljen za deskanje, naslov spletne strani, s katere je uporabnik prišel na trenutno spletno stran, vrsto jezika, ki ga uporabnik uporablja pri deskanju po internetu, vrsto dejavnosti na spletni strani (pregledovanje določene vsebine, iskanje določenega podatka), trajanje obiska spletne strani, piškotke (ang. cookies) (Klemenčič 2003, 106).

Predvsem piškotki predstavljajo posebno vprašanje. Gre za kratke datoteke, ki se običajno brez vednosti uporabnika shranjujejo v računalniku in omogočajo identifikacijo posameznega uporabnika in njegovih navad v svetovnem spletu. Večina komercialnih spletnih brskalnikov sicer omogoča, da zapisovanje in sprejemanje teh datotek uporabnik s programskimi nastavitvami omeji ali izključi, vendar veliko ljudi tega ne ve, dejansko pa taka omejitev tudi oteži deskanje po internetu (uporabniku, ki ne dovoli, da se na njegov disk zapišejo piškotki, mnoge spletne strani sploh ne bodo omogočile dostopa) (Klemenčič 2003, 106). V zadnjem času pa so se pojavili t.i. flash piškotki (ang. flash cookies, ki jih nekateri imenujejo tudi super cookies), ki jih ni mogoče nadzorovati[34] prek standardnih nastavitev za piškotke v spletnih brskalnikih.

Poleg tega gibanje po internetu dosledno beleži tudi uporabnikov računalnik. To posledično pomeni, da je gostiteljskemu računalniku (nosilcu spletne strani, ki jo uporabnik obišče), na voljo tudi ta informacija; ker je komunikacija ob povezavi z internetom dvosmerna, ni nobenih zagotovil (razen ustrezne zaščite programske opreme), da tuj računalnik – brez vednosti uporabnika – ne bo

[34] Če uporabnik v brskalniku izbriše običajne piškotke, s tem ne izbriše tudi Flash piškotkov. Ob ponovnem obisku spletne strani lahko spletni strežnik s pomočjo Flash piškotkov identificira uporabnika in ugotovi, da je uporabnik izbrisal običajne piškote, ki jih spletni strežnik uporablja za sledenje. Spletni strežnik lahko tako izbrisane piškotke »oživi« in jih ponovno pošlje uporabniku (Kovačič 2009).

»pogledal« tudi na disk uporabnikovega računalnika (Klemenčič 2003, 106).

Uporabnik interneta torej v večini primerov ni seznanjen z dejstvom, da se nekateri njegovi podatki oziroma dejavnosti beležijo in nato računalniško obdelajo ter uporabijo v različne namene (Klemenčič 2003, 107).

Sestavni del prikritega zbiranja podatkov na internetu predstavljajo tudi t.i. iskalni roboti (search engines). Najpogosteje temeljijo na računalniških programih – črvih (worms), ki neutrudno potujejo po svetovnem spletu in iščejo informacije. Tovrstna orodja so nujna za izdelovanje indeksiranih kazal podatkov v svetovnem spletu, ki so potem na voljo v znanih internetnih iskalnikih in brez katerih bi bilo iskanje informacij po internetu brezupno. Iskalni roboti predstavljajo manjše tveganje za zasebnost, večjo nevarnost pomeni programska tehnologija, na kateri temeljijo. Tovrstne programe lahko namreč posamezna podjetja, državni organi ali posamezniki usmerijo v iskanje in oblikovanje določenega profila posameznega uporabnika ali skupine uporabnikov interneta (Klemenčič 2003, 107).

Nadzor na internetu izvajajo različni subjekti. Čedalje bolj aktivno vlogo pri tovrstnem nadzoru prevzemajo države in njihovi organi, še posebej po terorističnem napadu na ZDA 11. septembra. Nadzorovanje potrošnikov oziroma zbiranje podatkov o potrošnikih po internetu je prav tako zanimivo za podjetja. Ta imajo tudi velik interes za nadzorovanje on-line aktivnosti svojih zaposlenih, poleg tega pa se nadzorovanja po internetu poslužujejo tudi hekerji. V nasprotju z državo in podjetji, ki nadzor izvajajo z natančno določenimi nameni in cilji, pa hekerji navadno ne vdirajo v računalnike le zaradi finančne koristi[35], pač pa bolj za zabavo, zaradi samodokazovanja ali povzročanja škode (Kovačič 2003, 40).

Med najbolj znane sisteme za nadzor telekomunikacij sodijo Bundestrojaner, Carnivore, Echelon in Magic Lantern:

- **Bundestrojaner** je projekt, ki sta ga skupaj razvila nemška Državna obveščevalna služba (BND ali Bundesnachrechtendienst) in Državni kriminalistični urad (BKA ali

[35] Podjetje Finjan je pred kratkim izdalo zanimivo poročilo o aktivnosti in strukturi kiberkriminalnih organizacij (Q2 2008 Web Security Trends Report). V okviru priprave tega poročila so se tudi pogovarjali z nekaterimi kiberkriminalci ter analizirali nekatere podatke iz primerov prijavljenih hekerskih vdorov. Glede na poročilo se "romantični" časi kiberkriminala nepreklicno končujejo. Namesto ohlapno povezanih individualnih hekerjev so se v zadnjem času pričele pojavljati hierarhično organizirane kriminalne združbe z jasnimi linijami "poveljevanja" in delitvijo nalog. Kriminalne organizacije se poleg vodstvenega dela, ki skrbi za "poslovne usmeritve" in management posameznih "projektov" delijo na t.i. hekerski del, kjer skupine hekerjev skrbijo za pridobivanje podatkov ter prodajni del, kjer "prodajalci" skrbijo za trženje izdelkov in storitev ter stike s kupci. Namen takih združb seveda ni raziskovanje iz radovednosti ali boj za svobodo, pač pa zgolj služenje denarja. Kiberkriminal tako čedalje bolj postaja podoben klasičnemu, celo organiziranemu kriminalu (Kovačič 2008).

Bundeskriminalamt). Gre za trojanskega konja, ki s pomočjo oddaljenega dostopa omogoča namestitev opreme za nadzor sistema in komunikacijskih kanalov na računalnik, s pomočjo keyloggerjev[36] pa omogoča pridobivanje različnih gesel. Državni kriminalistični urad (BKA) najprej ni priznal obstoja in razvoja Bundestrojanerja, kasneje pa je pod pritiskom javnosti to moral storiti. To je dvignilo veliko polemik v nemški javnosti glede kršitev varovanja osebnih podatkov in vdora v zasebnost. Zato je nemški parlament sprejel zakon, da je to orodje dovoljeno uporabljati le z nalogom sodišča (Spiegel online v Firbas 2009, 31).

- **Carnivore**: Od junija 2000 v ZDA deluje sistem Carnivore (uradno se imenuje DCS 1000). To je program za nadzor internetne komunikacije, ki ga je razvil ameriški Zvezni preiskovalni urad (FBI). Uporablja se za nadzor vseh oblik internetnega prometa. Vendar pa je program najprej potrebno namestiti na »žrtvin« računalnik. Zato v osnovi ne gre za množični, pač pa za specifični (»target«) nadzor, kjer je pozornost usmerjena na točno določeno vrsto ljudi, predvsem osumljence terorizma, otroške pornografije, vohunjenja in informacijske kriminalitete (StopCarnivore v Kovačič 2003, 44; Ventura in drugi v Firbas 2009, 32).

- **Echelon**: Največji in najbolj razvpit sistem za nadzor telekomunikacij se imenuje Echelon. Sistem je bil zgrajen v okviru sodelovanja Ameriške nacionalne varnostne službe (National Security Agency oziroma NSA) in obveščevalno varnostnih služb Velike Britanije, Kanade, Avstralije ter Nove Zelandije. Glavni cilj Echelona je ažurno prestrezanje in zajemanje podatkov iz vseh telekomunikacijskih kanalov z namenom boja proti organiziranemu kriminalu (Schneier 1999). Po nekaterih ocenah zmore Echelon dnevno obdelati tri milijarde komunikacij. To obsežno množico podatkov sistem s pomočjo metod podatkovnega rudarjenja prečisti in uporabne informacije posreduje človeškim nadzornikom (Schneier 2005).

- **Magic Lantern** je še eden od projektov FBI. Gre za keylogger, program, ki beleži – navadno prek tipkovnice – vse vnose uporabnika (Mills Abreu v Firbas 2009, 32). Namesti se s pomočjo trojanskega konja, ki bi ga antivirusni programi sicer morali zaznati, vendar je FBI sklenil dogovor z največjimi proizvajalci antivirusnih programov, zato ga ti ne zaznajo,

[36] Keylogger je program, ki beleži – navadno prek tipkovnice – vse vnose uporabnika in napadalcu omogoča pridobivanje gesel ali drugih uporabnih informacij.

saj omenjeni trojanski konj ni vključen v podatkovne baze znanih virusov ali drugih škodljivih programov (Sposato 2001 v Firbas 2009, 32).

3.3 ZRAČNI IN SATELITSKI NADZOR

Začetki zračnega nadzora segajo v devetnajsto stoletje in so povezani z razvojem prvih balonov, ki so bili dovolj veliki, da so lahko nosili ljudi. Nadzor s pomočjo balonov se je uporabljal predvsem v vojaške namene, na primer za opazovanje premikov sovražnih čet in kot pomoč pri razvrščanju topništva (Short 2009).

Z nastankom in razvojem letal se je učinkovitost zračnega nadzora bistveno povečala. V času prve svetovne vojne so na letala, v nekaterih eksperimentalnih primerih pa celo na rakete, že nameščali fotoaparate. V drugi svetovni vojni je prihajalo do posebnih predelav hitrih lovskih letal, ki so tako postala nekakšni specializirani stroji za izvajanje zračnega nadzora. Hladna vojna pa je postavila temelje sodobnemu zračnemu nadzoru. V tistem času so se pojavila posebna izvidniška in vohunska letala, pa tudi sateliti (Short 2009).

V zadnjih desetletjih so se z razvojem računalniške in fotografske tehnologije, ki omogoča pridobivanje natančnih digitalnih slik in posnetkov, hitro obdelavo ter povezavo podatkov, in tudi računalniško vodenje letal, možnosti zračnega nadzora bistveno povečale.

Utelešen potencial, ki ga premore sodobni zračni nadzor, predstavlja ameriško izvidniško letalo MQ 9 Reaper. Kamere na letalu lahko iz višine 18 kilometrov zaznajo in identificirajo predmet v velikosti navadne steklenice. Infrardeče kamere pa lahko do razdalje 60 kilometrov zaznajo toploto, ki jo seva človeško telo (Fickes 2004).

Vendar Združene države Reaperjev ne uporabljajo zgolj v vojaških operacijah, ampak z njimi izvajajo tudi policijski nadzor državnih mej in drugih območji (McCullagh 2006). V nekaterih ameriških in britanskih mestih policija uporablja računalniško vodena letala in helikopterje celo za nadzor mestnega prometa. V perspektivi pa se razmišlja tudi o »oborožitvi« letečih plovil s solzivcem, kar utegne biti koristno predvsem za razganjanje podivjanih množic in protestnikov (La Franchi 2007; Warwick 2007).

DARPA je pri razvoju zračnega nadzora šla še dlje. V okviru projekta HART (Heterogeneous Aerial Reconnaissance Team) je razvila avtomatiziran sistem, ki koordinira in usmerja večje število

računalniško vodenih letal s ciljem izvajanja sistematičnega nadzora nad določenim območjem (BAA 04-05-PIP: Heterogeneous Airborne Reconnaissance Team).

Za izvajanje zračnega nadzora se uporabljajo tudi sateliti. Satelitski nadzor se že uporablja na številnih področjih, na primer pri poročanju s kriznih žarišč, ugotavljanju obsega in škode ob naravnih nesrečah ter celo pri odkrivanju črnih gradenj (Banisar in drugi 1999). Najprej so satelitski nadzor uporabljali državni organi, kasneje pa se je razširil še na velike komercialne korporacije, ki so v vesolje izstrelile svoje satelite.

V zadnjih desetletjih se je satelitski nadzor močno razvil, kar ne preseneča, saj so po koncu hladne vojne podjetja kot na primer EarthWatch, Motorola in Boeing v razvoj satelitov vložila milijarde dolarjev. Tako je bil v ZDA že leta 1999 izstreljen (v tistem času najzmogljivejši) komercialni satelit Ikonos, ki lahko prepozna predmete v velikosti do enega metra (EPIC 2002, 57).

Sicer pa je uporaba komericalnih satelitov širši javnosti znana predvsem zaradi storitve Google maps, ki uporabnikom spleta omogoča pogled na katerokoli točko zemeljskega površja.

Tehnologija vojaških satelitov je še mnogo bolj napredna, saj po nekaterih ocenah že omogoča izvajanje satelitskega nadzora v vseh vremenskih razmerah (tudi, ko je zelo oblačno), hkrati pa zmorejo najsodobnejši sateliti na površju Zemlje prepoznati predmete v velikosti desetih centimetrov (EPIC 2002, 58).

Razen tega eden od laboratorijev NASE razvija programsko opremo za identifikacijo posameznikov na podlagi gibanja njihovih senc. V osnovi gre sicer za tehniko identifikacije posameznikov glede na način njihove hoje (ang. gait analysis), ki pa je ni mogoče izvajati v primeru, ko je na voljo posnetek posameznikov iz višine (na primer iz satelita). Satelitski posnetki namreč vsebujejo samo posnetek glave in ramen, zato naj bi bili za samodejno identifikacijo posameznikov neuporabni. Adrian Stoica, eden od raziskovalcev NASA, pa je ugotovil, da je dovolj informacij o načinu hoje mogoče dobiti že iz senc posameznikov. New Scientist poroča, da je Stoica napisal programsko opremo, ki je zmožna na video posnetku zaznati človeško senco in ob upoštevanju pozicije sonca ter kota snemanja pridobiti dovolj podatkov za pozitivno identifikacijo posameznika (Kovačič 2008). Razvoj takšne tehnike je sicer še v začetni fazi, vendar nazorno prikazuje potencialne možnosti sodobnega zračnega in satelitskega nadzora.

Prav tako se čedalje bolj razvijajo programi za povezovanje satelitskih posnetkov z geografskimi informacijskimi sistemi (GIS bazami), prek njih pa tudi z drugimi bazami podatkov (EPIC 2002, 58).

3.4 NADZOR TELEFONIJE

Nadzor stacionarne in mobilne telefonije[37] je proces nadzorovanja, razvrščanja in shranjevanja informacij o poteku in vsebini telekomunikacij med napravami in ljudmi. Pri tem se lahko nadzira tako tehnične procese komunikacije kot tudi sporočila oziroma informacije, ki jih ta prenašajo (Murakami Wood 2006, 17).

Razvoj tehnologije za nadzor telekomunikacijskih sredstev omogoča t.i. »prijazno prisluškovanje« (ang. to wiretap friendly), kar pomeni predvsem to, da je prisluškovanje prijazno oziroma preprosto za prisluškovalca (Banisar in drugi 1999). Leta 1994 je v ZDA stopil v veljavo zakon o digitalni telefoniji, ki je od telefonskih družb zahteval, da v svoje telefonske centrale vgradijo zmožnosti za oddaljeno prisluškovanje (t. i. remote wiretapping port), kar je agentom FBI močno olajšalo prisluškovanje. Danes imajo vse nove telefonske centrale že vgrajene tehnične možnosti za prisluškovanje.

Ena prvih in enostavnejših možnosti nadzora telefonije (v ZDA se je pojavila že leta 1987, v Sloveniji pa šele z nastopom GSM mobilne telefonije in ISDN stacionarne telefonije) je identifikacija dohodnih klicev (ang. caller ID). Kmalu po popolni digitalizaciji omrežja v ZDA in uvedbi ISDN telefonije v devetdesetih letih prejšnjega stoletja, so ameriška podjetja začela povezovati kličoče telefonske številke s socioekonomskimi in geodemografskimi podatki. Tako so podjetja ob sprejemu telefonskega klica lahko iz svoje baze podatkov dobila profil kličočega in celo njegove potrošniške preference.

Druga pomembna metoda nadzora mobilne telefonije je iskanje izvora radijskega signala s pomočjo triangulacije. Ker mobilni telefoni oddajajo radijske signale, jih je s pomočjo triangulacije mogoče prostorsko locirati[38]. Večinoma se uporabljata dva načina ugotavljanja lokacije mobilnega telefona.

---

[37] Sem sodi tako analogna kot tudi digitalna telefonija, prav tako pa telefonija, ki temelji na IP protokolu in poteka prek interneta.

[38] Poznavanje lokacije mobilnega telefona oziroma uporabnika predstavlja tržno nišo za operaterje GSM mobilne telefonije, saj omogoča lokalizacijo informacijskih storitev, izvajanje storitev sledenja, navigacijskih storitev, storitev upravljanja z razpršenimi viri po prostoru (Leskovšek v Kovačič 2003, 12). Tako na primer podjetje Streetbeam iz ZDA že trži pošiljanje oglasnih SMS sporočil uporabnikom mobilnih telefonov, ki se približajo njihovim oglasnim točkam. Razvoj tovrstnega oglaševanja bo šel zagotovo v smer interaktivnih oglasnih panojev, ki bodo zaznali in prepoznali uporabnika ter mu predstavili personificiran oglas.
Podjetje World-tracker pa je pred kratkim za britanske naročnike mobilnih storitev operaterjev O2, Orange in Vodafone pričelo ponujati sledenje njihovim mobilnim telefonom. Po prijavi na storitev (prijava je mogoča preko spleta) lastnik mobilnega telefona dobi SMS sporočilo, storitev slednjega pa nato potrdi.
Dostop do podatkov je mogoč preko spletne strani, naročnikom storitve pa so na voljo podatki o lokaciji telefona za vsako minuto (podatki so povezani z Google maps). Sledenje je seveda popolnoma neopazno, saj World-Tracker uporablja podatke o lokacijah z omrežja mobilnega operaterja (Schnier v Kovačič 2008).

En način je terminalska rešitev (ang. terminal-based oziroma handset-based), kjer lokacijo ugotovi in v omrežje sporoči mobilni telefon sam. Drug način pa je omrežna rešitev (ang. network-based), kjer lokacijo mobilnega telefona ugotovi omrežje (Leskovšek v Kovačič 2003, 12). Terminalske rešitve so zelo natančne (od 50 do 5 metrov), vendar razmeroma drage in počasne, saj predvidevajo zamenjavo vseh mobilnih telefonov z novimi, ki bodo imeli vgrajeno podporo ugotavljanja lokacije (npr. s pomočjo satelitskega navigacijskega sistema GPS). Veliko cenejše in hitrejše so omrežne storitve. Nekatere so že na voljo, vendar je njihova natančnost ugotavljanja lokacije tudi manjša, saj niha od 100 do 1100 metrov (Leskovšek v Kovačič 2003, 12).

V kontekstu nadzora so še posebej uporabni mobilni telefoni. Obveščevalne službe ZDA in Velike Britanije razpolagajo s tehnologijo, ki na daljavo aktivira mikrofone v mobilnih telefonih, s tem pa mogoči prisluškovanje[39] pogovorom, ki se odvijajo v bližini telefona.

Ena najbolj enostavnih metod prisluškovanja s pomočjo mobilnega telefona je ta, da prisluškovalec mobilni telefon skrije nekam v prostor, utiša zvonjenje, pokliče na to telefonsko številko in na ta način posluša kaj se dogaja v prostoru. Tudi sicer je mogoče na internetu brez večjih težav nabaviti[40] različne preproste naprave za prisluškovanje. Ena od teh je t.i. Spy phone, ki navidez zgleda kot mobilni telefon in ob klicanju s točno določene številke klic prevzame brez zvonjenja ali drugih motenj, ob prekinitvi pa prisluškovanje konča. Stane okoli 300 dolarjev.

Obstajajo pa seveda tudi bolj izpopolnjene metode prisluškovanja, od vrhunskih prisluškovalnih naprav[41] za mobilne telefone, katerih cena se giblje od 300.000 do 500.000 evrov, pa vse do dostopa do telefonskih pogovorov preko satelita (Cvetek v Kašnik 2006).

Prisluškovalni sistemi, ki jih uporabljajo države, večinoma delujejo samodejno s pomočjo

---

[39] FBI je takšno tehniko prisluškovanja uporabil pri preiskavi dveh domnevnih mafijcev, Johna Ardita in njegovega odvetnika Petra Pelusa. Takšna prisluškovalna naprava, ki obsega tako strojno kot programsko opremo, lahko deluje kadar je telefon vklopljen ali izklopljen. Programsko opremo naj bi bilo mogoče namestiti naskrivaj kar preko mobilnega omrežja. Ob tem je zanimivo tudi dejstvo, da nekaterih telefonov v resnici sploh ni mogoče povsem ugasniti, saj se na primer »zbudijo« ob nastavljenem časovnem alarmu (Schnier v Kovačič 2006).

[40] Kupiti prisluškovalno napravo je še najenostavneje, več znanja je potrebno za za njeno namestitev, še več pa za njeno odkritje (Cvetek v Kašnik 2006). Tako v Sloveniji ni omejena prodaja prisluškovalnih naprav, čeprav je nezakonito prisluškovanje v zasebnih prostorih prepovedano (Kašnik 2006, 34).
Kljub temu da je nezakonito prisluškovanje in nezakonito tajno video snemanje v zasebnih prostorih prepovedano, pa v marsikateri državi – tudi v Sloveniji – ni omejena prodaja audio in video prisluškovalnih naprav. Te naprave so razmeroma poceni in zato dostopne tudi širšemu krogu potrošnikov. Poročilo Privacy & Human Rights navaja oceno iz leta 1996, da v Veliki Britaniji vsako leto prodajo približno 200.000 prisluškovalnih naprav, še več pa v azijskih državah (Banisar in drugi 1999).

[41] Ena bolj znanih naprav za prisluškovanje so t.i. stenice, ki so lahko majhne kot risalni žebljiček, omogočajo pa prisluškovanje pogovorom v prostorih. Najsodobnejše prisluškovalne naprave zmorejo prenašati audio in video signale več kilometrov daleč, so dobro zamaskirane in jih je mogoče skriti tako rekoč kamorkoli. Nekatere takšne naprave imajo celo lasten vir napajanja in lahko ostanejo aktivne deset ali več let. Uporaba stenic in drugih prisluškovalnih naprav je prvotno sodila v domeno policije, vojske, obveščevalnih služb in industrijskega vohunjenja, danes pa zaradi relativno poceni in lahko dostopne tehnologije postaja čedalje bolj priljubljena med navadnimi (»domačimi«) uporabniki (EPIC 2002, 53).

programskih algoritmov, ki aktivirajo ali prekinejo snemanje na podlagi ključnih besed kot so npr. terorist, orožje, droga, idr. (Cvetek v Kašnik 2006).
Vendar pa si lahko ozaveščen posameznik za približno 5.000 evrov zagotovi napravo, ki s kodiranjem signala poskrbi za telefonski klepet brez dodatnih ušes (Cvetek v Kašnik 2006).

Uradno in neuradno prisluškovanje telefonskim pogovorom je po svetu precej razširjeno. V ZDA Communications Assistance For Law Enforcement Act (CALEA) omogoča, da preiskovalne službe lahko nadzorujejo domala vse telekomunikacije. Dve največji telekomunikacijski družbi v Združenih državah, AT&T in Verizon, pa imata s FBI sklenjeno pogodbo o hrambi podatkov o telefonskih klicih. Med leti 2003 in 2005 je FBI z več kot 140.000 pisnimi zahtevki skušal od telefonskih operaterjev pridobiti prometne podatke o telefonskih klicih uporabnikov. Polovica teh zahtevkov se je nanašala na državljane ZDA.
Nadzor telekomunikacij večinoma ne izvajajo več ljudje, pač pa posebni programi, ki omogočajo iskanje ključnih besed in analizo vsebine. Ko iz množice sporočil prefiltrirajo najbolj zanimiva, ta posredujejo človeškim operaterjem v nadzornih centrih (Murakami Wood 2006, 18).
V nekaterih državah se poleg nadzora telekomunikacij čedalje pogosteje pojavlja tudi cenzuriranje[42] vsebine. Tako na primer največji kitajski mobilni telefonski operater, China Mobile, po navodilih državne oblasti pregleduje in prijavlja »nelegalne« SMS-je, kamor sodijo tudi taki, ki omenjajo ali vsebujejo pornografijo, nasilje, prevare, nagovarjanje k terorizmu, spodbujanje k zločinom in kockanju (The Telegraph v Huš 2010).

3.5 VIDEO NADZOR

Video nadzor[43] je proces pridobivanja podatkov s pomočjo video kamer, ki so z žicami ali brezžično povezane z enotami za shranjevanje, obdelovanje, posredovanje in prikazovanje podatkov. Omogoča nadzorovanje oddaljenih ali težko dostopnih lokacij, hkrati pa množi kapaciteto nadzora, ki ga lahko izvaja posameznik. S pomočjo računalniške tehnologije in programske opreme video nadzor postaja čedalje bolj avtomatiziran, zato je človeški faktor v nadzornih centrih vse manj

[42] Ena od oblik takšne cenzure je blokiranje uporabnikov mobilne telefonije. Časnik Southern Metropolis (Huš 2010) poroča, da se to že dogaja, saj so na primer nekemu moškemu iz Dongguana (Kitajska) blokirali telefon, ker so v njegovih SMS sporočilih zaznali nespodobne besede. Telefon bo dobil nazaj v uporabo, ko se bo zglasil na policiji z osebno izkaznico in pisno izjavo, da v prihodnosti ne bo več pošiljal neprimernih SMS sporočil.
[43] Ang. video surveillance, čeprav se pogosto uporablja izraz CCTV oziroma Close Circuit Television.

pomemben.

Kašnik (2006, 25) ob povzemanju Surette (2004) in poročila ON-Net Surveillance Systems (2006) deli razvoj video nadzora v tri generacije:

Prva generacija videonadzornih sistemov se je razvila leta 1950[44]. Jedro takšnih sistemov so sestavljale črnobele video kamere z nizko resolucijo, ki so bile na glavni zaslon povezane s koaksialnim kablom. Takšne konfiguracije so bile v uporabi do leta 1980, ko so se na tržišču pojavile kompaktne videokamere, videorekorderji in mrežna oprema.

Prvo generacijo videonadzornih sistemov so pestile predvsem tehnične napake na opremi, nizka kvaliteta posnetkov, zapletena in draga namestitev opreme, nezmožnost vzporednega snemanja in pregledovanja posnetkov, ter zapleten postopek arhiviranja podatkov (On-Net Surveillance Systems v Kašnik 2006, 26).

Na začetku devetdesetih let pa se je pričela razvijati **druga generacija** videonadzornih sistemov. Novi sistemi so omogočali snemanje v višji resoluciji, hitrejšo obdelavo pridobljenih podatkov in kasneje tudi samodejno identifikacijo določenih parametrov ali situacij (Surette v Kašnik 2006, 26). Sistem druge generacije videonadzornih sistemov je torej že omogočal bolj ali manj zanesljivo samodejno prepoznavo posameznikov, »sumljivih« dejanj (vlomov, tatvin, ropov, nasilja) in predmetov (orožja, razstreliva).

Wright (1988) ugotavlja, da se je tehnologija vizualnega nadzora v zadnjih letih dramatično spremenila, saj so te naprave danes že izredno miniaturizirane, poleg tega pa je s sodobno tehnologijo, predvsem z novimi algoritmi, posnetke nadzornih videokamer mogoče med seboj primerjati, shranjevati in povezovati. Primer take tehnologije so sistemi samodejnega prepoznavanja vozil (ang. Vehicle Recognition System), ki so na trgu že od leta 1994 (Wright 1998). Namenjeni so nadzoru prometa, prek prepoznave registrske številke pa omogočajo spremljanje premikanja vozila po okolici.

Ameriška policija že uporablja skenerje registrskih tablic. Gre za naprave, sestavljene iz kamere v velikosti teniške žogice in računalnika, ki skrbi za prepoznavanje registrskih tablic. Naprave so nameščene v policijske avtomobile in nenehno skenirajo druga vozila, v primeru, ko naletijo na registrsko tablico iz »seznama«, pa policista na to opozorijo z vidnim in zvočnim signalom. Čeprav je bila tehnologija prvotno razvita za iskanje ukradenih vozil, Washington Post poroča, da jo je policija pričela uporabljati tudi v druge namene: za iskanje prekrškarjev in vozil, ki jim je že

[44] Video nadzor se je v javnem prostoru prvikrat uporabil leta 1953 in sicer v Veliki Britaniji ob kronanju kraljice Elizabete II. V poznih šestdesetih letih pa se je že razširil na nekatera območja Londona (Murakami Wood 2006, 18).

potekla registracija (Washintonpost v Kovačič 2008).

Na Univerzi Portsmouth pa so razvili »pametne« kamere, ki se odzivajo na zvočno in slikovno dogajanje v okolici. Kamere s pomočjo algoritmov umetne inteligence razpoznavajo »sumljive« zvoke (npr. zvok razbitega stekla ali vpitja) ali »problematično« dogajanje (pretep, napad). Glavna prednost takšnih videonadzornih kamer je ta, da se, ko zaznajo »sumljiv« zvok ali »prepovedano« besedo, samodejno obrnejo proti izvoru tega zvoka in o tem obvestijo operaterja (Kovačič 2008).

Moč video nadzora se je torej v kombinaciji z uporabo nekaterih drugih tehnologij, na primer detekcije gibanja, uporabe slikovne povečave in infrardečega snemanja, še povečala.

Tretja generacija, ki se razvija v zadnjih letih, pa v videonadzorne sisteme vnaša tehnologijo IP, na kateri temelji tudi internet, in s tem omogoča medsebojno povezovanje[45] videokamer, biometričnih[46] senzorjev in podatkovnih baz v enoten sistem (Kovačič 2003, 15). Tak omrežni sistem omogoča učinkovitejši nadzor, hkrati pa so stroški namestitve, vzdrževanja in uporabe relativno nizki (On-Net Surveillance Systems v Kašnik 2006, 26).

Čeprav je videonadzor prvotno sodil v domeno vojske, policije in obveščevalnih služb, se je kmalu razširil še v zasebni in javni sektor, zadnja leta pa zaradi pocenitve tehnologije postaja čedalje bolj priljubljen med navadnimi uporabniki. Videonadozor javnih površin je v šestdesetih letih prejšnjega stoletja začela prva izvajati Velika Britanija. Ker je britanska javnost takšnemu načinu nadzorovanja mestnih ulic izrazila podporo, se je videonadzor pričel uveljavljati tudi v drugih državah (Surette v Kašnik 2006, 25).

Vendar je še celo zdaj videonadzor najbolj razširjen prav v Veliki Britaniji, ki je imela že leta 2006 več kot 4,2 milijona video kamer, kar z drugimi besedami pomeni eno kamero na štirinajst prebivalcev otoka (Murakami Wood 2006). V devetdesetih letih je Home Office porabil 78% proračunskih sredstev namenjenih za kriminalno prevencijo, za nakup in namestitev sistemov videonadzornih sistemov, v zadnjem desetletju pa je bilo iz javnih sredstev v ta namen porabljenih pol milijarde britanskih funtov (Murakami Wood 2006, 19).

V ZDA se je uporaba videonadzora najbolj razširila po terorističnem napadu 11. septembra 2001. Zato ne preseneča, da Ministrstvo za domovinsko varnost izdatno subvencionira javne institucije na lokalni, državni in zvezni ravni pri nakupu opreme za videonadzor. Tako je mesto Chicago s

[45] Primer takšnega celovitega sistema za zbiranje in obdelavo podatkov je VIRAT (Video Image Retrieval and Analysis Tool), ki ga razvija DARPA. Še en projekt iste agencije se imenuje Combat Zones That See in bo povezoval vse kamere v mestih s centralno nadzorno bazo. Tak sistem bo omogočal spremljanje premikov in identifikacijo vozil, ljudi ter »sumljivih« situacij.

[46] Kombinacija biometrije in videonadzora se najbolj jasno kaže v tehnologiji avtomatske prepoznave obrazov, ki jo že uporabljajo v nekaterih britanskih mestih (Murakami Wood 2006, 24).

pomočjo pet milijonov dolarjev težkega kredita v okviru projekta Operation Virtual Shield, razširilo mrežo videokamer, ki jo sestavlja več kot 1500 kamer na različnih »problematičnih« lokacijah v mestu. V to omrežje pa se lahko povezujejo tudi video kamere iz zasebnega sektorja – kamere iz avtobusov, šol, podzemne železnice, trgovin. Mestne oblasti ponujajo tudi možnost povezovanja tistih kamer, ki si jih posamezniki namestijo v svoja stanovanja. Župan Chicaga, Richard Daley, je vzneseno izjavil, da bo do leta 2016 na vsakem uličnem vogalu vsaj ena video kamera (Spielman 2009).

Še bolj zanimiv je primer Kitajske, ki v okviru projekta Zlati ščit[47] (ang. Golden Shield) gradi videonadzorne sisteme in biometrično bazo celotnega prebivalstva. Cilj Zlatega ščita je implementirati in uporabiti najnovejšo nadzorno tehnologijo, pri tem pa Kitajski pomagajo nekatere zahodne korporacije, med drugim IBM, Honeywell in General Electric.
Ob tem se zaslužek ne izmuzne niti kitajskim proizvajalcem. Naomi Klein (2008) se je pogovarjala z lastnikom tovarne videonadzornih sistemov FSAN, čigar podjetje je v dveh letih in pol doživelo desetkratno rast. Kitajski trg videonadzornih sistemov pa je imel v zadnjem letu 4,1 milijarde dolarjev prihodka. Zaslužke si obetajo tudi proizvajalci AI tehnologije, ki bo nadgradila videonadzorne kamere - podjetje China Security & Surveillance Technology je razvilo za kitajsko oblast nadvse koristno programsko opremo, ki v primeru, da se na videonadzorovanem območju prične zbirati večje število ljudi, o tem nemudoma obvesti policijo.
Pri tem ni pomembna samo količina kamer in kvaliteta video posnetkov, pač pa integracija kamer v enotno nadzorno omrežje in povezava z biometričnimi sistemi. Po načrtih kitajske oblasti bo omrežje vsebovalo osebne podatke, zgodovino zaposlitev, fotografije in biometrične podatke za vsakega državljana Ljudske republike Kitajske - skupno torej podatke o kar 1,3 milijardah oseb. Kitajsko podjetje Pixel Solutions, ki sodeluje z ameriškim podjetjem L-1, v odboru katerega sedi tudi bivši direktor CIE George Tenet, že testira programsko opremo za prepoznavanje obrazov. Načrtujejo, da bodo razvili sistem, ki bo sposoben poiskati sliko obraza osumljenca v podatkovni bazi z desetimi milijoni fotografij v eni sekundi.

Videonadzor javnih površin se uporablja kot orodje za zbiranje podatkov o ljudeh, še pogosteje pa

[47] V tej zvezi velja omeniti eksperiment z nadzorno tehnologijo, ki ga je Kitajska izvedla v mestu Šenžen. Mesto je bilo zgrajeno pred 30 leti tako rekoč iz nič, danes pa ima že 100.000 tovarn in 12,4 milijona prebivalcev. V Šenženu, ki je nekakšna ekonomska cona, proizvajajo vse od prenosnikov, TV aparatov, mobilnih telefonov, iPodov, tiskalnikov in avtomobilov. Kitajska se je v okviru projekta Zlati ščit odločila, da v Šenženu razvije, testira in pilotno uvede obsežno nadzorno tehnologijo. V zadnjih dveh letih (prispevek Naomi Klein o mestu Šenžen je iz leta 2008, op. M.D.) so namestili okrog 200.000 videonadzornih kamer (v prihodnjih letih načrtujejo namestitev do dveh milijonov kamer), kamere pa nameravajo povezati v enotno in centralizirano nacionalno omrežje (Klein 2008).

se »oglašuje« kot učinkovito orožje v boju proti kriminalu in terorizmu. Vendar pa je raziskava, ki so jo leta 2002 izvedli raziskovalci Univerze Hull v Veliki Britaniji, pokazala, da video nadzor nima velikega vpliva na preprečevanje kriminalitete. V najboljšem primeru povzroči premik kriminalnih aktivnosti iz nadzorovanega na nenadzorovano območje (EPIC 2002, 54). Seveda pa je tak nadzor zelo opazen in med ljudmi ustvarja iluzijo varnosti, zato je priljubljen kot sredstvo politične propagande.

3.6 BIOMETRIČNI NADZOR

Izraz biometrija ima dva pomena. Na eni strani označuje kvantitativno merljive biološke ali vedenjske karakteristike človeka (Privacy&Biometrics 2006, 4), na drugi strani pa proces zbiranja, obdelave in shranjevanja podatkov o posameznikovih fizičnih lastnostih z namenom identifikacije (Kovačič 2003).

Različne biometrične metode za identifikacijo posameznikov se v večjem ali manjšem obsegu uporabljajo skoraj v vseh državah. Kar je bilo sprva omejeno na ozko okolje posebnih institucij, npr. vojaških baz, bank in zaporov, se zdaj čedalje bolj širi v javni prostor in v storitve[48], ki jih uporablja celotna populacija (EPIC 2002, 29).

- **Prstni odtisi**: Obstajajo tako uveljavljene kot tudi nove oblike biometrije. Ena najbolj znanih biometričnih metod je identifikacija posameznikov na podlagi prstnih odtisov, ki je v uporabi že od konca devetnajstega stoletja. Razvoj računalniške tehnologije v poznih šestdesetih letih dvajsetega stoletja pa je omogočil nastanek sistemov za samodejno primerjanje prstnih odtisov z odtisi iz podatkovnih zbirk (NSTC 2006, 13).

- **Geometrija rok in prstov**: Identifikacija na podlagi geometrije rok in prstov se je začela razvijati v poznih sedemdesetih letih dvajsetega stoletja. Ta biometrična metoda velja za precej enostavno in zanesljivo, prav tako med širšo javnostjo ni bila deležna večjih kritik.

[48] Španija razvija sistem biometrične identifikacije posameznikov na podlagi prstnih odtisov v okviru celotnega nacionalnega sistema socialne pomoči in zdravstvenega varstva. Rusija razmišlja o uvedbi takšnega sistema na področju bančništva in bančnih storitev. Na Jamajki je identifikacija s pomočjo prstnih odtisov že sestavni del političnih volitev. Francija in Nemčija pa razvijata kreditne kartice, ki bodo uporabljale sistem za identifikacijo na podlagi prstnih odtisov (EPIC 2002, 29).

Pri uporabi[49] takšnega sistema posameznik v poseben terminal vtipka identifikacijsko številko (PIN), nato pa na ploščo za skeniranje položi svojo dlan. Sistem na ta način pridobi odtis dlani in prstov s številnimi karakteristikami, ki jih je mogoče kvantificirati in preoblikovati v digitalni zapis. Program primerja podatke iz digitalnega zapisa z informacijami iz podatkovnih baz in na ta način določi identiteto osebe (NSTC 2006, 17).

- **Prepoznava obraza**: Gre za metodo identifikacije, ki se je razvila v poznih šestdesetih letih prejšnjega stoletja in temelji na iskanju in analizi obraznih karakteristik. Kamera posname obraz, program določi karakteristike, jih kvantificira, zapiše v digitalno obliko in primerja s podatki iz podatkovne baze. Prvi poizkusi uporabe te metode niso bili najbolj uspešni, saj so temeljili na posnetkih nizke kakovosti. Šele v zadnjem času se z uporabo visoko kakovostnih posnetkov zanesljivost identifikacije veča (NSTC 2006, 15). Tehniko prepoznavanja obrazov uporabljajo predvsem v nekaterih mestih[50] v Veliki Britaniji in ZDA, čedalje bolj priljubljena pa je tudi na letališčih. Kljub temu je raziskava ameriškega Ministrstva za obrambo pokazala, da je prepoznava obrazov točna le v 54% primerov (EPIC 2002, 56).

- **Prepoznava šarenice**: Ena od biometričnih metod identifikacije oseb temelji na prepoznavi vzorcev šarenice, ki so individualni. Tak sistem identifikacije uporablja amsterdamsko letališče Shiphol (Amsterdam v Kovačič 2003, 14).

- **Prepoznava čustvenih stanj**: Čedalje bolj se razvijajo tehnike biometrične prepoznave čustvenih stanj, ki sicer niso uporabne za identifikacijo posameznikov, pač pa so namenjene izvajanju specifičnega nadzora, utemeljenega na predpostavki, da se »sumljiva« oseba nenavadno vede ali nehote izraža določena čustva. Metode za prepoznavo čustvenih stanj in vedenj skušajo zaznati in analizirati izraz na obrazu, hitrost govora, ton in višino glasu, pa tudi držo telesa. Eno od zanimivejših metod predstavlja uporaba obraznih termografov, ki zaznavajo spremembo temperature človeškega obraza. Temperatura obraza je namreč povezana s pretokom krvi v obraznih kapilarah, te pa se pogosto razširijo tedaj, ko je oseba razburjena ali živčna.

[49] Tehnologijo za identifikacijo oseb na podlagi geometrije dlani in prstov uporabljajo na mednarodnem letališču Ben Gurion v Tel Avivu (EPIC 2002).

[50] Tak sistem so ZDA uporabile že leta 2001 in sicer v mestih Tampa in Virginia Beach (EPIC 2002).

- **Prepoznava glasu**: Ena od manj znanih biometričnih tehnik, ki se uporabljajo za identifikacijo oseb, je prepoznava na podlagi analize posameznikovega glasu (NSTC 2006, 18).

- **Analiza dinamike podpisa**: Gre za manj znano biometrično metodo, ki temelji predvsem na analizi pritiska in hitrosti, ki ju posameznik uporabi pri podpisovanju svojega imena (NSTC 2006, 19).

- **Prepoznava vzorcev žil**: Raziskovalci so ugotovili, da so vzorci žil med ljudmi različni in da se ne spreminjajo skozi čas. Na tej predpostavki temelji relativno nova biometrična metoda, ki s pomočjo infrardečih žarkov presvetli del človeškega telesa. Te žarke vsrka hemoglobin v krvi, zato se na zaslonu naprave pojavijo temna območja, ki omogočajo analizo in prepoznavo vzorcev. Program primerja pridobljen vzorec s podatki iz podatkovnih baz in na ta način ugotovi identiteto posameznika (NSTC 2006, 20).

- **DNK identifikacija**: Kanada, Nemčija in Združene države razvijajo biometrično metodo identifikacije na podlagi posameznikove DNK. Naštete države že imajo podatkovne baze z vzorci DNK velikega dela splošne populacije. Če se je identifikacijo posameznika na podlagi njegove DNK sprva uporabljajo pri obravnavanju storilcev kaznivih dejanj, se zdaj tak način širi na druge manj problematične družbene skupine. Župan New Yorka Rudolf Giuliani je celo predlagal, da bi se DNK vzorce jemalo že dojenčkom v bolnišnicah. Vrhovni tožilec ZDA Ashcroft je priznal, da je FBI-ju podal zahtevo za razširitev podatkovnih baz z DNK profili posameznikov iz prvotnih 1,5 milijona na 50 milijonov profilov (EPIC 2002, 30).

3.7 RADIOFREKVENČNE IDENTIFIKACIJSKE KARTICE

Radiofrekvenčna identifikacija temelji na uporabi majhnih elektronskih etiket, ki se jih namesti na kartico, predmet ali celo na živ organizem, omogočajo pa identifikacijo oziroma sledenje s pomočjo radijskih valov. Tehnologija je relativno poceni, zato se jo množično uporablja že kar nekaj časa.
Z vidika družbenega nadzora so pomembne predvsem identifikacijske kartice (npr. vozniška dovoljenja, bančne kartice, osebni dokumenti), ki določajo identiteto posameznika.

Nadzor v sodobni družbi v veliki meri temelji prav na uporabi RFID tehnologije. Čeprav so se takšne kartice sprva uporabljale za nadzor določenih kategorij[51] ljudi (Banisar in drugi 1999), so zdaj razširjene na celotno populacijo.
Poleg navadnih identifikacijskih kartic, na katerih so zapisani samo vnaprej pripravljeni podatki, pa se čedalje bolj uporabljajo tudi pametne kartice. Te vsebujejo pomnilnik, kamor se lahko podatki zapisujejo tudi pozneje. Prav tako pametne kartice omogočajo združevanje različnih funkcij (bančništvo, zdravstvo, osebna identifikacija) na eni sami kartici (EPIC 2002, 28).

RFID kartice se v različnih oblikah uporablja v skoraj vseh državah. Nekatere države imajo vzpostavljene celo nacionalne sisteme identifikacije na podlagi RFID kartic, ki omogočajo regulacijo populacije na podlagi rasnih, političnih ali religioznih kategorij. Zdi se, da je strah pred upori in nemiri zaradi verskih, političnih in drugih razlogov eden najpogostejših motivov za razvoj nacionalnih sistemov RFID identifikacije (EPIC 2002, 27).
Sicer pa se nadzor z uporabo RFID tehnologije izvaja tudi v komercialnem sektorju, kjer se s pomočjo RFID etiket sledi tako premikom ljudi, kakor tudi premikom predmetov in vozil. Tako pridobljene podatke se v kombinaciji z geografskimi podatki čedalje pogosteje združuje v geografske informacijske sisteme (GIS), ki omogočajo še bolj temeljit nadzor nad posamezniki in skupinami.

Pomembna je tudi možnost nadzora s pomočjo RFID vsadkov[52], ki se vstavijo v človeško ali živalsko tkivo. Ta metoda nadzora se je v civilnem sektorju najprej uporabljala na dirkalnih konjih, nato pa se je razširila še na ostale domače živali.
Nadzor s pomočjo RFID čipov se že nekaj časa uporablja tudi na ljudeh. Tehnologijo se je v civilnem sektorju, za razliko od vojske in obveščevalnih služb, najprej uporabljajo na starih ljudeh, ki so trpeli za degenerativnimi boleznimi (Murakami Wood 2006, 25). Kmalu pa so si začeli RFID čipe vstavljati raziskovalci in tehnološki navdušenci. Znan je tudi primer mehiškega pravobranilca, ki je od 160 uslužbencev zahteval, da si morajo vstaviti čip za namen identifikacije in dostopa v zgradbe. V zadnjem času pa se pojavljajo lokali in restavracije, ki že omogočajo plačevanje storitev s pomočjo vsajenih RFID čipov (Murakami Wood 2006, 25).

[51] Prve osebne izkaznice, ki so vsebovale fotografijo, prstni odtis in lastnoročni podpis posameznika, so na predlog nizozemskega statistika Jacobusa Lambertusa Lentza uvedli na Nizozemskem med nacistično okupacijo, na njih pa je bilo tudi označeno, ali je oseba Jud ali ne. Black ugotavlja, da so bile omenjene osebne izkaznice prvi korak do izvedbe holokavsta na Nizozemskem, saj so identifikaciji sledile deportacije (Black 2002, 388–389).

[52] Eden bolj znanih in razširjenih RFID vsadkov je Verichip, ki ga izdeluje podjetje Applied Digital Solutions (ADS). Verichip je nekoliko večji kot riževo zrno, pod kožo pa se vstavi s pomočjo injekcije. Čip je obdan s steklenim ovojem, vsebuje pa posebno identifikacijsko oznako, ki jo skener uporabi za dostop do osebnih podatkov iz Verichipove podatkovne baze.

3.8 TEHNOLOGIJA NE OSVOBAJA

Čeprav je družbeni nadzor sestavni del medčloveških odnosov in spremlja človeštvo tako rekoč od samega začetka njegove zgodovinske poti, je problematiziranje nadzora šele v dvajsetem stoletju postalo tako pomembno, da so številni teoretiki sodobno družbo poimenovali kar družba nadzora. Nedvomno je k temu kvalitativnemu in kvantitativnemu preskoku v konfiguraciji družbenega nadzora največ prispevala računalniška, informacijska in komunikacijska tehnologija, ki je po eni strani omogočila zelo hitro in obsežno zbiranje najrazličnejših podatkov o posameznikih, po drugi strani pa je razpršene posameznike vpela v sistematično nadzorovana podatkovna omrežja. Temelji za razvoj informacijskega nadzora so bili sicer položeni že na začetku moderne, ki je z razcvetom racionalizma, birokratskih organizacij in statistične znanosti ustvarila pogoje za nadgradnjo arhaičnih nadzorstvenih praks. Vendar pa je nadzor 18. in 19. stoletja temeljil na t.i. »papirnatih sledeh«, ki so jih posamezniki puščali pri izpolnjevanju različnih dokumentov, zato je bil relativno počasen in z vidika finančnih sredstev tudi precej potraten. Je pa zaradi uporabe statističnih metod že omogočal preskok iz ravni posameznika na raven populacije. Na ta način sta se oblikovala množični nadzor in biopolitika, ki nista bila usmerjena k discipliniranju posameznika, pač pa k regulaciji celotne populacije.

Razvoj računalniške, informacijske in komunikacijske tehnologije v drugi polovici dvajsetega stoletja je nadzor posameznikov in množic dvignil še na mnogo višjo raven. Široka uporaba medsebojno povezanih elektronskih naprav je omogočila beleženje t.i. »elektronskih sledi«, ki jih ljudje pri vsakodnevni rabi elektronskih naprav puščamo za seboj. Ker je elektronskih naprav, ki so povezane v omrežja, vsak dan več, so tudi življenja ljudi čedalje bolj prežeta z nadzorom. Razvoj mikroprocesorjev, programov za napredno statistično analizo in programov za podatkovno rudarjenje pa ni omogočil le intenzivnega nadzora posameznikov, ampak je bistveno nadgradil tudi relativno enostaven množični nadzor iz začetka moderne. Šele z razvojem računalnikov in elektronskih omrežji je učinkovit množični nadzor prvič v zgodovini postal realnost.

Čeprav so tehnološki navdušenci sprva optimistično pozdravljali razvoj široko dostopnega osebnega računalnika in nekoliko kasneje tudi razcvet interneta, se je v realnosti kot že nič kolikokrat doslej izkazalo, da tehnologija kljub številnim potencialom in možnostim osvoboditve posameznika izpod jarma takšne ali drugačne prisile, slej ali prej postane orodje v rokah tistih, ki imajo največ moči. Možnost uporabe tehnologije za krepitev in širitev družbenega nadzora na ravni posameznikov in

populacij so spoznale tako državne organizacije kot tudi zasebne korporacije, ki v zadnjih desetletjih postajajo čedalje močnejše gonilo napredka na področju informacijskega nadzora.

4 ZASEBNOST

Ker sta koncepta družbenega nadzora in zasebnosti tesno prepletena, ni mogoče ustrezno razumeti enega brez poznavanja drugega. Zato je v tem poglavju pozornost namenjena analitičnemu pretresu ideje zasebnosti. Kljub temu, da so mnenja o kulturnem oziroma biološkem izvoru in (ne)univerzalnosti zasebnosti med teoretiki deljena, osnovna ideja zasebnosti zavzema pomembno mesto tako v humanistični in liberalni filozofski zapuščini, kakor tudi v evropskem in ameriškem pravnem redu. Še več, sklicevanje na zasebnost oziroma na pravico do zasebnosti je prisotno v ustavah skoraj vseh držav.

V nadaljevanju besedila je predstavljen zgodovinski razvoj ideje zasebnosti od starih Grkov do danes. Takšen zgodovinski pregled je pravzaprav predpogoj za razumevanje širšega družbenega konteksta, ki je v 19. stoletju privedel do postopnega formalnega oblikovanja pravice do zasebnosti – ta se je naprej pojavila v publikacijah dveh uglednih ameriških pravnikov, približno sto let kasneje pa je že našla svoje mesto v ustavah in zakonih številnih držav.

Poseben poudarek pa ni namenjen le pregledu razvoja pravice do zasebnosti v okviru nacionalnega in mednarodnega prava, ampak tudi predstavitvi veljavne evropske in ameriške zakonodaje s področja varovanja pravice do zasebnosti. Zadnji del poglavja je namenjen predstavitvi sistema pravice do zasebnosti v Republiki Sloveniji. Ob tem so izpostavljene nekatere pomanjkljivosti obstoječega pravnega sistema varovanja pravice do zasebnosti. Dodani so pokazatelji stanja na področju varovanja osebnih podatkov v Republiki Sloveniji, na ta način pa je, čeprav s precejšnjim pridržkom, mogoče sklepati na splošne trende širjenja ali krčenja pravice do zasebnosti.

4.1 IZVOR ZASEBNOSTI

Hirshleifer (1980, 656) na podlagi rezultatov antropoloških, bioloških in ekoloških raziskav išče izvor zasebnosti[53] v prirojeni vedenjski strukturi tistih živalskih vrst, ki posamično ali v skupinah živijo na nekem določenem ozemlju in to ozemlje tudi branijo pred vsiljivci. Številne živali za svoje bivanje potrebujejo ozek osebni prostor, ki ga branijo pred vdori tuje ali lastne vrste. Prav tako so živali, ki imajo svoj teritorij, ponavadi zmožne odbiti napade vsiljivcev in sicer zato, ker se vsiljivci večinoma niso pripravljeni tako vztrajno in dolgo boriti kakor branilci prostora. Hirshleifer (1980, 661-667) v tej vedenjski značilnosti nekaterih živalskih vrst, ki je pogojena z ozemljem, išče izvor etike zasebnosti. Ugotavlja, da so imele številne primitivne družbe zelo dodelan sistem pravic posedovanja predmetov in zemlje. Čeprav so se sistemi pravic med posameznimi kulturami močno razlikovali, pa je poseganje vanje vedno izzvalo ogorčenje in zgražanje. Razvoj menjave blaga in kasneje monetarne trgovine je še dodatno okrepil medsebojno prepoznavo lastninskih pravic, ki naj bi kazale na določeno prirojeno in privzgojeno težnjo posameznikov do zasebnosti oziroma osebne avtonomije znotraj širše družbene skupnosti. Z razvojem jezika se je povečala kompleksnost in subtilnost elementarnih vedenjskih vzorcev, zato se je pojavila potreba po etičnem utemeljevanju in opravičevanju ne le zasebnosti, pač pa tudi drugih pravic in dolžnosti. Tudi antropolog Barrington Moore (v Solove 2009, 65-66) je prepričan, da želja po zasebnosti izvira iz človekove biološke podlage. V številnih primitivnih kulturah se kaže splošna težnja po iskanju zavetja pred skupnostjo v primeru izvrševanja določenih dejavnosti, na primer spolnega občevanja ali izločanja.

Profesor Adam Moore poudarja, da »*človekovo zmožnost nadzorovanja nekaterih impulzov ne smemo enačiti z odsotnostjo teh istih impulzov. Človeška psiha ni prazna plošča, ki bi jo lahko vpliv družbe poljubno popisal«* (Moore v Solove 2009, 66).

Med različnimi kulturami po vsem svetu obstajajo številne podobnosti glede odnosa do zasebnosti. Moore (v Solove 2009, 66) sicer ugotavlja, da se za nekatere kulture na prvi pogled zdi, kot da ne poznajo zasebnosti. Tikopijci so le redko sami, Thlinget Indijanci hodijo nenapovedano drug drugemu v hiše, bivališča Jav pa sploh nimajo vrat. Toda natančnejša analiza kaže, da poznajo celo takšne družbe določene oblike zasebnosti. Moore navaja: »*Jave imajo svoja odmaknjena kopališča, Thlinget Indijanci in Tikopijci pa se skrivajo za psihološkimi zidovi in si na ta način zagotavljajo delček zasebnosti. Prav tako je v vseh treh družbah prisotna časovna omejitev obiskov –*

[53] Etimološko beseda *zasebnost* (ang. *privacy*) izvira iz latinskega pridevnika *privus*, kar pomeni *posamezen*. Latinski izraz se je uporabljal za označevanje posamične in svojske osebe, ki se ne vzpostavlja kot izolirano človeško bitje, pač pa kot posameznik, ki ima v razmerju z drugimi ljudmi svojo avtonomijo in zasebnost (Hirshleifer 1980, 651). Slovar slovenskega knjižnega jezika zasebnost povezuje predvsem z zasebnim premoženjem, v širšem pomenu pa s področjem, ki se vzpostavlja kot nasprotje javnega delovanja.

obiskovanje nekoga sredi noči je navadno prepovedano« (Moore v Solove 2009, 66). Moore zaključi, da je »*zasebnost kulturno univerzalna, saj zagotavlja normalno delovanje družb. Toda konkretna oblika zasebnosti (pravila druženja in razhajanja) pa je kulturno pogojena«* (Moore v Solove 2009, 66).

Meadova (v Schoeman 1984) pa zastopa kulturni relativizem in meni, da je zasebnost vselej kulturno pogojena[54] oziroma odvisna od družbenih, ekonomskih, tehnoloških, ne pa tudi bioloških dejavnikov. Ne glede na to ali sprejmemo nazore, ki iščejo izvor zasebnosti v biološki strukturi ljudi in s tem poudarjajo univerzalnost koncepta, ali pa prisegamo na teorije, ki poudarjajo izključen pomen kulture, je zasebnost v različnih oblikah prisotna v večini človeških družb (DeCew, 1997). Da je zasebnost že dolgo prisotna v kulturni zapuščini človeštva, dokazujejo tudi številni temeljni verski (Biblija[55], Koran) in filozofskih teksti (Laurant 2003, 5).

4.2 JAVNO IN ZASEBNO PRI STARIH GRKIH

Sodobno razumevanje zasebnosti je v marsičem bistveno drugačno kakor antično razumevanje. Kljub temu se je potrebno ozreti nazaj k starim Grkom, ki so vzpostavili delitev življenja v polisu na javno in zasebno področje. V precej obsežno zasebno področje[56] so spadali dom, družina, gospodinjstvo in gospodarstvo. Javno področje pa je obsegalo predvsem politično dejavnost. Poudariti velja, da zasebnost v antiki ni bila visoko cenjena (Lyon 1994, 182). Aristotel je bil prepričan, da je v »*zasebnem življenju človek oropan najvišjih možnosti in najbolj človeških sposobnosti. Kdor torej ni poznal ničesar drugega razen zasebnost – bodisi ker zaradi nizkega družbenega položaja ni smel vstopiti v javnost ali pa kot barbar sploh še ni poznal skupnega javnega – pravzaprav sploh ni bil človek«* (Arendt 1995, 40)

Visoko vrednost je po mnenju Arendtove (1995, 27) pri Grkih imel zgolj politični oziroma javni prostor znotraj polisa. Vendar se je potrebno zavedati, da se je starogrško razumevanje politike precej razlikovalo od modernega razumevanja. Za Grke politika ni bila nekaj, kar je nujno potrebno

[54] V povezavi s kulturnim relativizmom koncepta zasebnosti Schoeman (1984) postavlja dve vprašanji: »*Ali se zasebnost zdi vrednota vsem ljudem ali pa je njena vrednost relativna oziroma kulturno pogojena? Ali obstajajo področja človeške eksistence, kjer zasebnost ni plod družbenih konvencij, pač pa obstaja sama po sebi?«* Žal Schoeman ne ponudi odgovorov na vprašanji.

[55] Npr. zavedanje Adama in Eve, da sta gola, zavedanje o goloti Noeta in povezovanje golote s sramoto (Wagner DeCew v Kovačič 2006, 11).

[56] Antično razumevanje, kolikor nam je sploh še dostopno, zasebno vselej močno povezuje s sfero doma oziroma domačije. To pomeni, da se zasebnost ni enačilo s samoto, z »biti sam«, ampak je vsebinsko obsegala prisotnost širše družine. Zato je v zasebni sferi posameznik morda res našel zaščito pred zunanjim svetom, še zdaleč pa ni nujno, da je našel tudi zaščito pred konflikti in napetostmi znotraj družine (povzeto po Lyon 1994, 182).

za družbeno blagostanje. Prav nasprotno, bila je privilegirano področje človeških zadev, iz katerega je bilo izključeno vse, kar je bilo zgolj nujno ali koristno.

Politični prostor je bil močno povezan z idejo svobode, ki so jo stari Grki povzdigovali zelo visoko. Svoboda[57] je zanje pomenila stanje, ko človek niti ne vlada, niti se mu ne vlada. Vzpostavila se je lahko le tedaj, ko je posameznik – če je sploh imel to možnost – zapustil svoj dom in se podal v politični prostor, kjer je bil med sebi enakimi. Ta »enakost« je pomenila predvsem to, da je posameznik imel opravka s sebi enakimi, kar pa je hkrati predpostavljalo obstoj »neenakih«, torej sužnjev, žensk in otrok.

Vendar pa je bilo zasebno nujni predpogoj za svobodno (so)delovanje v političnem oziroma javnem prostoru. »*Brez prostora, ki bi ga človek zares lahko imenoval svojega lastnega, ne bi mogel biti umeščen*[58] *nikjer v tem svetu. In brez zavarovanja lastnine se ne bi mogel mešati v zadeve skupnega sveta«* (Arend 1995, 32). Posest in obvladovanje zasebnega sta torej predstavljala temelj, ki je šele omogočil nastanek javnega. Ob tem velja poudariti, da sta bila za Grke sila in nasilje opravičljiva zgolj v zasebni sferi, saj sta predstavljala edini način, kako premagati nujnost, ki jo terja življenje, in postati svoboden (Arendt 1995, 33).

4.3 TRI SFERE NOVEGA VEKA: JAVNO, ZASEBNO IN DRUŽBENO

V srednjem veku se je z razcvetom krščanstva človekova pozornost preusmerila iz zunanjega v notranji svet. Ta preskok je vplival na razvoj individualizma, prav tako pa se je tudi področje svobode začelo pomikati iz javne v zasebno sfero (Kovačič 2006, 14).

Vendar se je najopaznejši preobrat na področju javnega in zasebnega zgodil šele v času razsvetljenstva in sovpada z nastankom kapitalizma. Takrat so gospodinjske in gospodarske dejavnosti, ki so v antiki spadale na področje zasebnega, vstopile v javni oziroma politični prostor in s tem postale kolektivne zadeve neke skupnosti. Interesi, ki so bili prej zgolj zasebni, so zdaj postali javni (Habermas 1989, 32; Arendt 1995, 37).

V začetku 18. stoletja se je začela oblikovati tudi ideja kritične javnosti in publicitete. Meščanska javnost, sprva zgolj sfera zasebnikov, zbranih v publiko, se je proti javni oblasti postavila z načelom nadzora, ki se je uresničeval skozi publiciteto in z odzivanjem v javnosti (Habermas 1989, 41).

[57] Svoboda je bila Grkom pogoj tistega, kar so imenovali sreča, eudaimonia. Ta je bila neogibno povezana z zdravjem in bogastvom, ki sta določala objektivni položaj v svetu. Kdor je bil reven ali bolan, je ostal podvržen fizičnemu, tudi če je bil tehnično svoboden (Arendt 1995, 33).

[58] Celo Nietzsche v *Volji do moči* pravi *»da mora kaj imeti, kdor hoče kaj biti«* (Nietzsche 2004, 79).

Predpostavka načela publicitete je bila, da zakoni naj ne bi bili več odvisni od samovolje vladarja, temveč bi postali racionalni in s tem tudi predvidljivi. Skrivno prakso vladanja, ki je temeljila zgolj na vladarjevi (samo)volji, naj bi nadomestila publiciteta, ki bi temeljila na racionalnosti (Habermas 1989, 69). Takšne ideje in nazori so vodile k opazni spremembi razumevanja javnega in zasebnega. Meščanska javnost se je postavila nasproti lastni oblasti (za razliko od grške javnosti, ki ni oporekala lastni vladi), od katere je pričakovala urejanje svojih zasebnih interesov, ki so s tem vstopili v javno sfero (Habermas 1989, 67; Arendt 1995, 70).

Ob tem se je začelo oblikovati novo področje in sicer družbena sfera, ki je svojo dokončno obliko dobila v nacionalni državi in predstavlja *»formo, v kateri se je javno uveljavil in organiziral življenjski proces sam«* (Arendt 1995, 48). S tem javna sfera ni obsegala več zgolj političnega področja, pač pa tudi družbeno. Čeprav so se številne dejavnosti, ki so v antiki sodile v domeno zasebnega, premestile v javni prostor, pa se je v novem veku znotraj zasebne sfere pojavila intimnost. Prav zaradi intimnosti je zasebno področje postalo bolj raznovrstno in zanimivo kot kdajkoli prej. Zato ne preseneča, da se je polje svobode najprej premestilo iz političnega v družbeno, kasneje pa iz družbenega v zasebno oziroma intimno. Ob izvršitvi tega procesa je postala najpomembnejša naloga zasebne sfere zagotavljanje intime (Arendt 1995, 41).
Posledice takšnega razvoja so se v pravu pokazale kot oblikovanje treh skupin temeljnih človekovih pravic, ki se nanašajo na sfero rezonirajoče publike (svoboda mnenja in govora, enaka volilna pravica), svobodni status posameznika, zasnovan v intimni sferi ožje družine (osebna svoboda, nedotakljivost stanovanja in druge pravice, ki se nanašajo na avtonomijo posameznika) in občevanje zasebnih lastnikov v sferi meščanske družbe (enakost pred zakonom, zaščita zasebne lastnine) (Habermas 1989, 99)
Novo vrednost zasebnega slikovito opisuje francoski zgodovinar Georges, ki zasebno sfero dojema kot blagodejno zatočišče[59] pred zunanjim svetom: *»Jasno razmejeno območje je prihranjeno za tisti del človekovega bivanja, ki ima v vsakem jeziku ekvivalent pojmu »zasebno«. Gre za področje imunitete, kamor se lahko umaknemo, prostor, kjer lahko odložimo orožje ali oklep, ki ga potrebujemo na javnih mestih. Tu se sprostimo, spočijemo in zaživimo brez teže napihnjenega oklepa, ki ga nosimo kot zaščito pred zunanjim svetom«* (Duby v Lyon 1994, 182).

Vendar pa nastanek družbene sfere, ki sovpada s prehodom iz srednjega v novi vek, prinaša nove nevarnosti. V srednjem veku so vladali monarhi. V moderni družbi pa se zdi, da ne vlada nihče

[59] Morda je zasebna sfera res služila kot zatočišče pred zunanjim svetom, toda to še zdaleč ne pomeni, kakor je opozoril Lyon (1994, 182), da je posameznik tam našel tudi zaščito pred družinskimi konflikti in napetostmi.

(Arendt 1995, 42). Na to je v *Volji do moči* opozoril celo Nietzsche (2004, 405), ko je zapisal, da v sodobni državi ni nihče več v celoti odgovoren. Oblasti nima več monarh, ampak anonimen birokratski stroj.

Arendtova opozarja, da se posledice nove strukture oblasti v moderni družbi kažejo skozi ravnanje državljanov: »*Če je bilo v antiki značilno predvsem delovanje, potem je danes v ospredju obnašanje, ki ga družba pričakuje od vseh svojih članov v različnih oblikah in za katerega predpisuje nešteta pravila, ki so vsa usmerjena v določeno normiranje in dresuro posameznikov, v modeliranje sprejemljivosti, v preprečevanje spontanega delovanja in izjemnih dosežkov. Takšna množična družba, ki obvladuje vse svoje člane, kaže na zmago družbene sfere in izenačuje v vseh okoliščinah, kar pomeni, da sta postala izjemnost in drugačnost le še privatna zadeva posameznikov«* (Arendt 1995, 43). Ob tem dodaja, da se »*z večanjem števila prebivalstva čedalje bolj zanesljivo uveljavljajo statistične zakonitosti, »odkloni« pa postajajo čedalje manj pomembni«* (Arendt 1995, 48). To med drugim pomeni, da se politična sfera krči, družbena sfera pa doživlja vedno večjo ekspanzijo. Arendtova (1995, 49) vidi v tem precejšnjo nevarnost, saj stalna rast in širitev družbenega že od samega začetka grozi, da bo postopoma izpodrinila najprej politično, nato zasebno, na koncu pa tudi novo področje intimnega.

4.4 NASTANEK IN RAZVOJ PRAVICE DO ZASEBNOSTI

Začetki zakonodaje, ki ščiti zasebnost, segajo v leto 1361, ko je v Angliji zakon *Justices of the Peace act* predvidel kazni za tiste, ki so skrivaj opazovali ali prisluškovali drugim ljudem. S tem so predstavniki družbenih elit želeli predvsem zaščitit svojo čast in dobro ime. Začetki pravne regulacije vladnega preiskovanja zasebnih prostorov segajo v obdobje med leti 1761 in 1765[60]. Leta 1776 pa nastanejo tudi zametki varovanja informacijske zasebnosti, saj je takrat švedski parlament sprejel *Zakon o dostopnosti javnih zapisov*, ki je določal, da morajo biti vsi podatki, ki jih zbere država, uporabljeni zgolj v zakonite namene. Leta 1858 je Francija sprejela ostre kazni za objavo zasebnih informacij o posameznikih (Laurant 2003, 5-6). Norveški kazenski zakonik iz leta 1889 pa je prepovedoval objavo informacij, ki se nanašajo na osebne ali domače zadeve (EPIC, 2002: 6). Ni naključje, da so nekateri vidiki pravice do zasebnosti postali pravno zaščiteni šele v 18. in 19.

[60] Leta 1765 je britanski lord Camden protestiral, ker so preiskovalci želeli vstopiti v njegovo hišo in zaseči neke listine, parlamentarec William Pitt pa je o tem zapisal: *»Tudi najrevnejši človek se v svoji koči lahko upira Kroni. Lahko je slaboten, lahko se maje njegova sreha, v kočo lahko piha veter, vdreta lahko nevihta ali dež, toda kralj Anglije ne sme noter«* (EPIC 2002, 5).

stoletju. Po eni strani je to čas revolucij, ko je meščanstvo s pomočjo človekovih pravic – te so že od samega začetka varovale določene aspekte pravice do zasebnosti – skušalo utrditi nov družbeni red ali vsaj močno omejiti moč plemstva. Po drugi strani pa so se v tem obdobju že pojavile prve oblike informacijske tehnologije, predvsem časopisni tisk in fotografija, ki so predstavljale grožnjo že uveljavljenim pravicam do dostojanstva, dobrega imena in časti.

Prvo sistematično razpravo o konceptu pravice do zasebnosti sta leta 1890 v eseju z naslovom *Pravica do zasebnosti,* napisala ameriška pravnika Samuel Warren in Louis Brandeis (DeCew 1997). Zapis je nastal kot odziv na nevarnosti, ki jih je prinašala nova »informacijska« tehnologija, predvsem tisk in druga sredstva javnega obveščanja. V tem obdobju so že obstajale različne pravice, ki so se dotikale nekaterih vidikov zasebnosti, vendar pa je šele ta esej položil temelj splošni pravici do zasebnosti, ki sta jo avtorja opredelila kot »*pravico posameznika, da se ga pusti pri miru«* in predstavlja predvsem možnost nadzora nad informacijami o sebi (Lyon 1994, 14).
Že leta 1928 je Louis Brandeis zapisal, da »*napredek znanosti omogoča državi nove možnosti nadzora, ki se ne bo ustavil pri prisluškovanju telefonskim pogovorom«* (Brandeis v Lampe 2004, 37). Brandeis je napovedal, »*da bo država nekega dne lahko sodišču predložila reproducirane papirje, ne da bi jih fizično vzela iz obtoženčevega predala«* (Brandeis v Lampe 2004, 37). Svaril je, da bodo fizika in druge znanosti omogočile »*načine za raziskovanje neizraženih mnenj, misli in čustev«* (Brandeis v Lampe 2004, 37). Ob tem se je vprašal: »*Je mogoče, da Ustava ne nudi nikakršnega varstva zasebnosti posameznika pred tovrstnimi vdori?«* (Brandeis v Lampe 2004, 37). Dodal je, da so »*očetje (ameriške) Ustave sklenili zavarovati vse pogoje za iskanje sreče. Priznali so pomen človekove duhovne narave, njegovih čustev in intelekta. Prizadevali so si zaščititi Američane v njihovem verovanju, njihovem mišljenju, njihovih čustvih in njihovih dejanjih. Potrdili so, da nasproti oblasti obstaja »pravica biti sam« - splošna pravica, ki jo civilizirani človek najbolj spoštuje«* (Brandeis v Lampe 2004, 37).
Leta 1965 je Vrhovno Sodišče v ZDA priznalo ustavno[61] pravico do zasebnosti, ki je bila prvič uporabljena v primeru Griswold proti Connecticut. Leta 1969 je William Prosser (1969, 389) skušal sistematično opredeliti[62] pravico do zasebnosti, ki jo razume kot zaščito posameznika pred

[61] Opozoriti velja, da ustava ZDA eksplicitno ne omenja pravice do zasebnosti. Vendar kljub temu varuje nedotakljivost doma in komunikacij pred posegi države. Vrhovno sodišče je odločilo, da četrti amandma ščiti posameznika pred posegi države vselej, ko obstaja »razumno pričakovanje zasebnosti«. Prav tako velja poudariti, da številne zvezne države v ZDA v svojih državnih ustavah eksplicitno priznavajo pravico do zasebnosti (Solove 2009, 3).

[62] Hirshleifer (1980, 2) opozarja, da je Prosserjeva opredelitevi pravice do zasebnosti preozka. Pravi, da bi zasebnost morali razumeti v tesni povezavi z željo in potrebo po avtonomnem položaju posameznika znotraj družbe, kar je nenazadnje ena temeljnih vrednot klasičnega liberalizma. Sicer ni dvoma, da je Prosserjev poizkus sistematične opredelitve pravice do zasebnosti zelo pomemben, vendar pa se osredotoča le na odškodninsko pravo (ang. tort law).

različnimi kršitvami – vdorom v zasebnost, objavo neprijetnih zasebnih informacij, predstavitvijo posameznika v »lažni« luči in prilastitev imena drugega.

Mednarodno pravne temelje varovanja zasebnosti v sodobnem času pa je postavila predvsem Splošna deklaracija človekovih pravic iz leta 1948, ki v 12. členu navaja, 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 takšnim vmešavanjem in takšnimi napadi*«.
Z vidika varovanja zasebnosti je prav tako pomembna Evropska konvencija o človekovih pravicah iz leta 1950, ki v 8. členu (*pravica do spoštovanja zasebnega in družinskega življenja*) pravi, da »*ima vsakdo pravico do spoštovanja svojega zasebnega in družinskega življenja, svojega doma in dopisovanja; da se javna oblast 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*«.
Uveljavitvi človekovih pravic in pravice do zasebnosti v mednarodnem pravu so največ pripomogle prav grenke izkušnje druge svetovne vojne, ko je postalo jasno, kam lahko sistematična kršitev civilizacijskih standardov vodi. V prvih letih po vojni so bili tako rekoč vsi državni in nedržavni akterji (zakonodajna, izvršna in sodna telesa, nevladne organizacije, strokovnjaki in navadni državljani) zainteresirani, da se vzpostavi sistem varoval, ki naj bi omejil samovoljno oblastnikov in tako preprečil, da se svetovna vojna ponovi. Tak sistem varoval so predstavljale človekove pravice, med katere sodi tudi pravica do zasebnosti, ki so prvič v zgodovini postale predmet mednarodnih pravnih dokumentov.

Pravica do zasebnosti zato ni zapisana le v Splošni deklaraciji človekovih pravic in v Evropski konvenciji o človekovih pravicah. Navedena je tudi v 17. členu Mednarodnega pakta o državljanskih in političnih pravicah, kjer piše, da se »*nikomur ne sme nihče samovoljno ali nezakonito vmešavati v zasebno življenje, v družino, v stanovanje ali dopisovanje ali nezakonito napadati njegovo čast in ugled; ter da ima vsakdo pravico do zakonskega varstva pred takim vmešavanjem ali takimi napadi*«. Vsebinsko podobna določba se ponovi v Konvenciji Združenih narodov o pravicah migrantov (14. člen) in v Konvenciji združenih narodov o pravicah otrok (16. člen). Pravni dokumenti, ki varujejo pravico do zasebnosti, so vzpostavljeni tudi na regionalni

Prav tako je Prosserjeva klasifikacija pravice do zasebnosti nastala v času, ko vpliv informacijske tehnologije še ni bil tako izrazit, zato se tudi ne dotika številnih problemov v zvezi z zasebnostjo, ki se pojavljajo danes.

ravni. Primer takšne zaščite predstavlja Ameriški pakt o človekovih pravicah, ki pravico do zasebnosti v 11. členu vsebinsko opredeljuje[63] zelo podobno kot Mednarodni pakt o državljanskih in političnih pravicah.

Za implementacijo in varovanje določb mednarodnih dokumentov o človekovih pravicah skrbijo različna regionalna in mednarodna telesa. Na podlagi Evropske konvencije o varstvu človekovih pravic in svoboščin sta se oblikovala Evropska komisija za človekove pravice in Evropsko sodišče za človekove pravice. Obe instituciji dejavno uresničujeta implementacijo in varovanje pravice do zasebnosti, zato ne preseneča, da sta zelo široko interpretirali vsebino 8. člena Konvencije. Evropska komisija za človekove pravice je leta 1976 zapisala: »*Številnim anglosaksonskim in francoskim avtorjem pravica do spoštovanja zasebnega življenja predstavlja odraz pravice do zasebnosti, pravice do življenja po lastni izbiri in pravice do zaščite pred publiciteto«* (EPIC 2002, 7). Komisija ob tem poudarja, da se »*pravica do spoštovanja zasebnega življenja s tem ne izčrpa. Do določene mere prav tako obsega pravico do vzpostavljanja in razvijanja odnosov z drugimi ljudmi, ki so nujni za razvoj in uresničevanje posameznikove osebnosti«* (EPIC 2002, 7).
V tem kontekstu velja omeniti še dva pomembna mednarodno-pravna instrumenta za varovanje pravice do informacijske zasebnosti. Prvi tak instrument je Konvencija Sveta Evrope o zaščiti posameznika v odnosu do avtomatske obdelave osebnih podatkov iz leta 1981, drugi pa so Smernice Organizacije za ekonomsko sodelovanje in razvoj (OECD) o varovanju informacijske zasebnosti in prekomernega pretoka osebnih podatkov (EPIC 2002, 8).

Razvoj pravice do zasebnosti je dobil nov zagon v sedemdesetih letih. Temu je botroval bliskovit razcvet informacijske tehnologije, ki je močno povečala nadzorni potencial držav. Zato je bilo potrebno oblikovati specifična pravila, ki naj bi urejala zbiranje in upravljanje osebnih podatkov. Prvi zakon za zaščito informacijske zasebnosti je bil sprejet leta 1970 in sicer v Nemčiji v zvezni državi Hesse. Dve leti kasneje je švedska Parlamentarna komisija za javnost in tajnost uradnih dokumentov[64] napisala *Poročilo o računalnikih in zasebnosti*. V istem letu je podobno poročilo napisala tudi kanadska Delovna skupina[65] za zasebnost in računalnike. Leta 1973 je ameriško Ministrstvo[66] za zdravje, izobrazbo in socialo izdalo *Poročilo[67] o zapisih, računalnikih in pravicah*

[63] Vsakdo ima pravico do časti in dostojanstva; nikomur se ne sme nihče samovoljno ali nezakonito vmešavati v zasebno življenje, v družino, v stanovanje ali dopisovanje ali nezakonito napadati njegovo čast in ugled; vsakdo ima pravico do zakonskega varstva pred takim vmešavanjem ali takimi napadi (11. člen Ameriškega pakta o človekovih pravicah).
[64] Ang. Swedish Parliamentary Commission of Publicity and Secrecy of Official Documents.
[65] Ang. Canadian Task Force on Privacy and Computers.
[66] Ang. The American Department of Health, Education and Welfare.

državljanov, Švedska[68] pa je sprejela nacionalni zakon za zaščito informacijske zasebnosti. Leta 1974 je francosko Ministrstvo za pravosodje ustanovilo Komisijo za informatiko in svoboščine (Lyon 1994, 170). Istega leta so zakon za zaščito informacijske zasebnosti sprejele Združene države Amerike. Nemčija je sprejela tak zakon leta 1977, Francija pa leta 1978 (EPIC 2002, 7).
Zakonodaja s področja informacijske zasebnosti se je relativno hitro uveljavila v mednarodnem in nacionalnem pravnem sistemu zaradi treh razlogov. Prvi razlog, ki je imel največjo težo v Evropi, so bile grenke izkušnje druge svetovne vojne, ki so kljub zgodovinski distanci treh desetletji še vedno opozarjale kam lahko pomanjkljivo reguliranje državne oblasti vodi. Drug razlog je bila že obstoječa zakonodaja s področja zasebnosti, zato kodifikacija pravice do informacijske zasebnosti ni predstavljala pravne revolucije, ampak zgolj nadgradnjo že obstoječih in uveljavljenih pravic. Tretji razlog pa so bila močna civilna gibanja, ki so kljub številnim nasprotnikom (ti so prihajali predvsem iz vrst represivnih organov in komercialnih korporacij, ki so v nadzoru potrošnikov že videle zlato jamo dobička) uspela prepričati strokovno in laično javnost, da je varovanje informacijske zasebnosti nujno za ohranjanje temeljnih človekovih pravic in svoboščin.

Tako je pravica do zasebnosti zgolj v nekaj desetletjih pridobila status mednarodne in hkrati človekove pravice, ki je vključena v ustave številnih držav. V ustavi Brazilije npr. piše, da so *»zasebnost, zasebno življenje in čast ljudi, nedotakljivi«* (Solove 2009, 3), v ustavi Južne Afrike pa je zapisano, da *»ima vsakdo pravico do zasebnosti«* (Solove 2009, 3). Razen tega ima večina držav zakone, statute in sodno prakso, ki varujejo pravico do zasebnosti. Tako celo v primerih, ko pravica do zasebnosti ni zapisana v ustavni (tak primer predstavljajo Nemčija, Kanada, Japonska in Indija), sodna prakso to pravico implicitno priznava in jo bolj ali manj učinkovito tudi varuje (Solove 2009, 3).

4.5 POIZKUSI OPREDELITVE PRAVICE DO ZASEBNOSTI

Da je zasebnost pomemben koncept dokazujejo številni poizkusi njenega opredeljevanja. Kljub raznolikim prizadevanjem[69] politolog Colin Bennet opozarja, da »*poizkusi opredeljevanja*

[67] Ang. Report on Records, Computers and the Rights of Citizens.
[68] Švedska je bila poleg nemške zvezne države Hesse prva, ki je sprejela zakon za zaščito informacijske zasebnosti. Temu je botrovala velika zaskrbljenost javnosti glede obsežnih in natančnih popisov prebivalstva, ki jih je izvajala država (Lyon 1994, 170).
[69] Eden od takšnih primerov je bila primerjalno pravna raziskava pravice do zasebnosti, ki jo je leta 1970 UNESCO

zasebnosti niso obrodili sadov« (Bennet v Solove 2009, 2). Tak pesimizem je upravičen, če med »sadove« prištevamo enkratno in dokončno opredelitev zasebnosti, kar najbrž predstavlja podvig, ki je obsojen na neuspeh. Zato Daniel J. Solove (2009, 1) v svoji knjigi *Understanding privacy* uvodoma zapiše, da je zasebnost kompleksen koncept, ki vključuje številne razsežnosti. V sodobnih zahodnih družbah se k vsebinskemu bistvu zasebnosti prišteva predvsem pravico do svobode misli, pravico do uživanja samote v svojem domu, pravico do nadzora nad svojim telesom, pravico do nadzora nad osebnimi podatki, pravico do svobode pred nadzorom drugih, zaščito lastnega ugleda in zaščito pred preiskavami in zasliševanji (Solove 2009, 1).

Čeprav sta Louis Brandeis in Samuel Warren prvič pravno obravnavala pravico do zasebnosti že pred več kot sto leti, velja ta pravica še danes za tisto med človekovimi pravicami, ki jo je najtežje opredeliti[70]. Vsebina, obseg in pomen pravice do zasebnosti so se v času, ko jo je pravo sprejelo v svoj okvir, tudi najbolj spremenili. Kljub številnim spremembam in »prenovitvam«, ki jih je pravica do zasebnosti v času svojega formalnega obstoja doživela, je Šelihova (1999, 41) prepričana, da njeno jedro in temeljni pomen ostajata nespremenjena. Pravica do zasebnosti, ki leži v samem središču svobode moderne družbe, tako ostaja izraz želje po izvzetosti posameznika iz okolja, želje po samoti, intimnosti in anonimnosti, pa tudi želje po razdalji od drugih.

Vsekakor se zasebnost, kakor je nakazal Solove (2009), povezuje[71] s številnimi pojmi in vrednotami. David Flaherty (v Kovačič 2006, 40), eden prvih pooblaščencev za varstvo zasebnost v Kanadi, je ugotovil, da se pravica do zasebnosti povezuje s pravico do osebne avtonomije[72], pravico biti puščen pri miru, pravico do zasebnega življenja, pravico do nadzorovanja informacij o sebi, pravico omejevanja dostopa do sebe, pravico ekskluzivnega nadzora dostopa do zasebnega področja, pravico uživanja samote, pravico uživanja intimnosti, pravico uživanja anonimnosti, pravico uživanja zadržanosti in pravico do tajnosti (Cate 1997, 21).

Lampe v zvezi z zasebnostjo pravi, da bi jo bilo potrebno razumeti kot »*nekaj, kar ni javno«* (Lampe 2004, 39). Po njegovem gre »*v osnovi za nematerialno dobrino, ki jo posameznik nameni le ozkemu krogu točno določenih oseb«* (Lampe 2004, 39).

Urednik *Privacy Journal*, Robert Ellis Smith, pa zasebnost opredeljuje kot »*željo vsakega človeka po fizičnem prostoru, kjer bo varen pred različnimi poizkusi vdora in nadzora, pa tudi pred*

---

poveril Mednarodni komisiji pravnikov. Komisija je v uvodnem delu poročila zapisala, da je »*zasebnost zapleten koncept, ki ga ni mogoče enostavno opredeliti«* (Lampe 2004, 37).

70 Opredelitve pravice do zasebnosti se v posameznih družbenih okoljih nekoliko razlikujejo. Zato je v zakonodaji nekaterih držav pravica do zasebnosti interpretirana zelo ozko, npr. kot načelo, ki ga je potrebno upoštevati pri upravljanju z osebnimi podatki. Po drugi strani pa je v zakonodajah nekaterih drugih držav zasebnost interpretirana širše, kot široko začrtana meja, ki posameznika varuje pred posegi javnih in privatnih akterjev (EPIC 2002, 1).

71 Ruth Gavison meni, da zasebnost – stanje, ki ga je mogoče izgubiti tako po lastni volji kot tudi zaradi vmešavanja drugih - sestavljajo trije elementi: tajnost, anonimnost in samota (Gavison v EPIC 2002, 2).

72 Tudi Edward Bloustein povezuje zasebnost s posameznikovo avtonomnostjo, dostojanstvom in integriteto (Bloustein v EPIC 2002, 2).

razkrivanjem osebnih informacij o sebi« (Smith v EPIC 2002, 2).

Profesor Gross v svojem delu *The Concept of Privacy* razmišlja o zasebnosti kot o »*stanju človekovega življenja, kjer je seznanjanje z osebo ali osebnimi zadevami določenega človeka omejeno«* (Gross v Lampe 2004, 40).

Britanska sekcija Mednarodne pravne komisije je zasebnost definirala kot »*tisto področje človekovega življenja, za katerega razumen človek ob upoštevanju upravičenih potreb družbe meni, da ga je napak kratiti«* (Lampe 2004, 41).

Kalkutski komite (ang. Calcutt Committe) pa je leta 1990 v poročilu o zasebnosti zapisal, da je zasebnost »*pravica posameznika do varstva pred vdori v njegovo zasebno in družinsko življenje«* (EPIC 2002, 2).

V preambuli avstralske listine o zasebnosti je zapisano, da mora »*svobodna in demokratična družba spoštovati avtonomnost posameznika in ob tem omejevati tako moč države kot tudi moč zasebnih organizacij, da ne prestopijo meje posameznikove avtonomije«*. Ob tem preambula dodaja, da je »*zasebnost temeljna vrednota in predstavlja osnovo človekovemu dostojanstvu in drugim temeljnim vrednotam, kot na primer svobodi združevanja in svobodi govora. Zasebnost je osnovna človekova pravica in razumno pričakovanje vsake osebe«* (EPIC 2002, 3).

Westin v svojem odmevnem delu Privacy&Freedom povzame, da je »*zasebnost srce svobode v sodobni družbi«* (Westin v Solove 2009, 79).

Bellottijeva (v Kovačič 2006, 41) skuša definirati pravico do zasebnosti na dva načina. Prva definicija je normativna in govori o tem, da so nekateri vidiki posameznikove narave in njegovih dejavnosti zasebni, kar pomeni, da se jih naj ne bi razkrivalo drugim. Ta definicija je izrazito kulturno in kontekstualno pogojena, saj enaka dejanja[73] v nekaterih kulturah štejejo kot poseg v zasebnost, v drugih kulturah pa so skoraj povsem neproblematična. Podobno je s kontekstom, saj z vidika posega v zasebnost ni vseeno ali se vpleteni ljudje med seboj poznajo ali ne, pa tudi prostor, kjer pride do spornega dejanja, ni nepomemben.

Druga definicija, ki jo uporablja Bellottijeva (v Kovačič 2006, 41) pa je operacionalna in se nanaša na zmožnost nadzora informacij o sebi oziroma na zmožnost nadzora nad odtekanjem informacij. Po tej definiciji je bistvena zmožnost posameznika, da se sam odloči, koliko informacij želi zamenjati z okolico in kdaj. Taka definicija zasebnosti se Bellottijevi zdi bolj ustrezna, saj je

[73] Tipičen primer, ki ponazarja problematičnost normativne definicije zasebnosti, so identifikacijske kartice (osebne izkaznice) in videonadzor. V ZDA in Veliki Britaniji proti identifikacijskim karticam vlada velik odpor, češ da gre za prevelik poseg v zasebnost posameznika, v celinski Evropi pa so osebne izkaznice nekaj povsem vsakdanjega. Po drugi strani javnost videonadzor na javnih mestih v Veliki Britaniji sprejema praktično povsem mirno, prav tako se posameznikom v drugih državah po 11. septembru 2001 uporaba videonadzora na nekaterih posebnih mestih (npr. letališčih) zdi čedalje manj sporna (Kovačič 2006, 41).

situacijsko neodvisna in relacijsko specifična. Podobnega mnenja je tudi Samarijeva (v Kovačič 2006, 41), ki zasebnost definira kot zmožnost eksplicitnega ali implicitnega pogajanja o mejnih pogojih družbenih odnosov, kar zajema nadzor nad odtokom in nadzor nad pritokom informacij ter tudi pobudo za začetek stika. Vendar gre pri obeh poizkusih definiranja pravice do zasebnosti v osnovi za subjektivno presojo posameznika, zato je težko postaviti univerzalne kriterije, ki bi bili splošno sprejemljivi.

Kljub težavnosti opredeljevanja pravice do zasebnosti je Solove (2009, 13) skušal na podlagi analize številnih teoretičnih razprav in sodne prakse določiti temeljne razsežnosti koncepta. Pravico do zasebnosti je tako mogoče razdeliti na šest osnovnih kategorij:

- Pravica biti sam: gre za Warrenovo in Brandeisovo znamenito formulacijo pravice do zasebnosti;
- Pravica omejevanja dostopa do sebe: gre za možnost zaščite samega sebe pred nezaželenim dostopom drugih oseb;
- Pravica do tajnosti: sem sodi prikrivanje nekaterih osebnih zadev pred drugimi ljudmi;
- Pravica do nadzorovanja informacij o sebi;
- Pravica do osebne avtonomije: gre za zaščito lastne osebnosti, individualnosti in dostojanstva;
- Pravica uživanja intimnosti: gre za nadzor nad pripuščanjem drugih v sfero lastne intimnosti.

Poročilo o zasebnosti in človekovih pravicah (EPIC 2002, 3) pa zasebnost deli na štiri medsebojno povezane kategorije:

1) Informacijska zasebnost: Sem sodijo pravila, ki določajo zbiranje in uporabo osebnih podatkov, npr. podatkov o kreditnih karticah, zdravstvenih in kazenskih kartotekah. Informacijsko zasebnost se pogosto enači z varovanjem osebnih podatkov.
2) Telesna zasebnost: Ta vrsta zasebnosti obsega nedotakljivost posameznikovega fizičnega telesa pred posegi kot so genski testi, testi alkoholiziranosti in vsebnosti drog, pregledi telesnih votlin.
3) Komunikacijska zasebnost: Pri tem gre za varovanje zasebnosti komunikacije, ki poteka preko pošte, telefona, elektronske pošte in drugih tehničnih sredstev.
4) Prostorska zasebnost: Pri tej obliki zasebnosti pa gre predvsem za zaščito osebnega,

domačega, delovnega in javnega prostora pred različnimi vdori, npr. preiskavami, video nadzorom, preverjanji identitete.

O tem kaj naj bi zasebnost sploh bila je bilo napisanih veliko razprav. Toda prav zato, ker je »bistvo« zasebnosti težko določljivo in v veliki meri pogojeno s kulturo, tradicijo, tehnologijo, gospodarstvom, politiko in drugimi dejavniki, ki se od družbe do družbe razlikujejo, ni mogoče določiti univerzalne in nespremenljive definicije. Solove (2009, 13) je prepričan, da je večina obstoječih poizkusov opredeljevanja zasebnosti neustreznih, saj so bodisi preozki in zato nezmožni integrirati pomemben del problematike, ki se pojavlja v zvezi z zasebnostjo, bodisi so preširoki in zato tudi premalo uporabni za učinkovito reševanje konkretnih pravnih in političnih problemov s področja zasebnosti. Nekateri bolj skeptični avtorji so celo prepričani, da zasebnosti same po sebi sploh ni, temveč gre le za pojem, ki združuje različne bolj ali manj (ne)povezane pravice (Wagner DeCew v Kovačič 2006, 40). Zato je vsako definiranje pravice do zasebnosti lahko precej arbitrarno in odseva preplet vrednot, interesov in moči. Potemtakem v praksi ne gre za določanje neke absolutne meje, ki je ni dovoljeno prestopiti, pač pa za nenehno regulacijo posegov v zasebnost. Pravo tako le sledi razvoju tehnologije, ki omogoča vedno nove posege v zasebnost, hkrati pa sledi tudi razpoloženju v družbi, ki zasebnosti daje enkrat večjo, drugič manjšo težo (Kovačič 2006, 40).

Kljub težavam in dilemam, ki spremljajo različne poizkuse opredeljevanja zasebnosti, je pravica do zasebnosti v sodobni družbi priznana kot ena temeljnih človekovih pravic. Je mednarodna in ustavna pravica, ki ima javnopravni in civilnopravni značaj. Posameznika varuje pred državno oblastjo, pred javnostjo in pred drugimi posamezniki tako, da zmanjšuje posege v njegovo odločitveno, duševno, prostorsko in informacijsko zasebnost (Lampe 2004, 42). Prav tako predstavlja izhodišče številnim drugim temeljnim človeškim vrednotam[74]. Pravica do zasebnosti je priznana v številnih državah. Na mednarodni ravni je zavarovana s Splošno deklaracijo o človekovih pravicah, z Mednarodno konvencijo o civilnih in političnih pravicah ter številnimi drugimi mednarodnimi in regionalnimi dokumenti. Na nacionalni ravni pa jo večinoma varujejo ustave in splošni ali posebni zakoni (EPIC 2002, 1).

[74] Poročilo (EPIC 2002, 1) prišteva med temeljne vrednote, ki so povezane s pravico do zasebnosti, človekovo dostojanstvo, svobodo združevanja in svobodo govora. Vendar ni odveč poudariti, da gre pri tem predvsem za razsvetljenske in humanistične vrednote, ki so številnim kulturam tuje. Zato pri sklicevanju na »univerzalnost« določena mera previdnosti ne bo odveč (op. M.D.).

4.6 INFORMACIJSKA ZASEBNOST IN VARSTVO OSEBNIH PODATKOV

Velik napredek in razvoj na področju informacijske tehnologije v sedemdesetih in osemdesetih letih dvajsetega stoletja je nedvomno eden glavnih razlogov, da je zasebnost postala predmet obsežnih javnih razprav in da je pravica do zasebnosti našla svoje mesto v zakonodaji številnih držav. Sicer je res, da je bila zasebnost cenjena že na začetku moderne, vendar je takrat sodila predvsem v domeno »viktorijanskih« elit. Šele z razvojem informacijske tehnologije se je težišče nadzora premaknilo od posameznikov na široko množico navadnih državljanov. To širjenje nadzora sta po besedah Šelihove (1999, 43) zaznamovali dve tehnološko-ekonomski usmeritvi, ki sta prispevali k temu, da so se razvile povsem nove oblike komuniciranja in da je komuniciranje dobilo globalno razsežnost. Na eni strani je šlo za združevanje in medsebojno prepletanje telekomunikacijske in računalniške tehnologije, na drugi strani pa za razvoj novih radio-televizijskih tehnik, digitalizacije in kompresije digitalnih signalov. Prva usmeritev je prispevala k nastanku globalnih omrežij, ki s pomočjo svetovnih telekomunikacijskih uslug in cenenih multi-medialnih računalnikov nudijo možnost sodelovanja pri globalni izmenjavi podatkov. Drugo usmeritev pa je omogočila digitalna televizija, ki lahko preko obstoječih satelitov prenaša več sto televizijskih kanalov. Z razvojem tehnologije in nastankom informacijskih omrežji se je začel krepiti množični nadzor, s tem pa je tudi dilema varovanja zasebnosti postala pomembnejša in bolj razširjena (Lyon 1994, 14).

Že leta 1964 je novinar Vance Packard v svoji uspešnici *The Naked Society* zapisal, da »*zasebnost čedalje hitreje izhlapeva«* (Packard v Solove 2009, 4), Myron Brenton pa je oznanjal, da »*stojimo na pragu dobe, ki jo lahko imenujemo doba akvarija*[75]*«* (Brenton v Solove 2009, 4). Tri leta kasneje je Alan Westin v odmevnem delu *Privacy and Freedom* izrazil »*globoko zaskrbljenost glede ohranjanja zasebnosti pod novimi pritiski tehnologij nadzora«* (Westin v Solove 2009: 5). Lyon (1994, 170) ob tem dodaja, da je sedemdeseta leta zaznamovala hladna vojna in napetost med Vzhodnim in Zahodnim blokom. V številnih prozahodnih državah se je pojavljala splošna družbena tesnoba zaradi prikazni »orwellovskih« totalitarnih režimov, ki so se uresničevali pod taktirko komunizma. Zato so nekateri politiki skušali oblikovati zakonodajo, ki bi regulirala zbiranje, obdelovanje, uporabo in posredovanje osebnih podatkov državljanov. Že v tistem obdobju je bilo bolj ali manj jasno, da procesa čedalje večje akumulacije podatkov ni več mogoče ustaviti, zato so se prizadevanja usmerila predvsem v zmanjšanje negativnih učinkov in posledic, ki bi utegnile ob tem nastati (Lyon 1994, 170). Osnovna dilema iskanja ustreznega razmerja med zbiranjem podatkov na eni in pravnim varstvom zasebnosti na drugi strani ostaja v svojem bistvu nespremenjena in nerazrešena še danes.

[75] Ang. The Age of the Goldfish bowl.

Poročilo *Privacy and Human Rights 2002* (2002, 9-10) pa navaja še tri dejavnike oziroma razloge, ki so botrovali hitremu razvoju zakonodaje za zaščito informacijske zasebnosti v sedemdesetih in osemdesetih letih:

- Prvi razlog naj bi bil v odpravljanju krivic[76], ki so jih določene države zagrešile v preteklosti. Ta razlog naj bi vplival predvsem na države Srednje in Vzhodne Evrope, Južne Amerike ter Južne Afrike, ki so s sprejemanjem ustrezne zakonodaje poizkusile »popraviti« sporna ravnanja svojih nekdanjih avtoritarnih režimov.
- Bolj realističen je drugi razlog - promoviranje in širjenje elektronskega poslovanja. Ta razlog je vplival predvsem na nekatere azijske države, ki so se v zadnjih desetletjih izrazito ekonomsko razvile in s svojo trgovino prodrle na tuje trge. Sprejemanje informacijske zakonodaje v takšnih primerih služi predvsem kot sistem regulacije gospodarstva (npr. s postavljanjem enotnih standardov v notranjem gospodarstvu in zagotavljanjem skladnosti storitev in izdelkov s standardi tujih trgov) in vzpostavljanja zaupanja med strankami.
- Tretji razlog pa tiči v procesu usklajevanja državnih zakonodaj z zakonodajo Evropske Unije. Ta razlog pomembno vpliva tako na tiste države, ki se želijo kot članice pridružiti EU, kot tudi na države, ki želijo gospodarsko sodelovati z EU in morajo zato svojo zakonodajo uskladiti s smernicami Konvencije Sveta Evrope in Direktivo za zaščito podatkov EU.

Na nevarnost širjenja nadzora sta sicer že sredi 19. stoletja opozorila ameriška pravnika Samuel Warren in Louis Brandeis (DeCew, 1997). Toda v tem »prvem« obdobju se je zasebnost tolmačila predvsem kot pravica, ki posamezniku zagotavlja, da se ga pusti pri miru. Šele v zadnjih desetletjih 20. stoletja pa se je zaradi bliskovitega razvoja informacijske in komunikacijske tehnologije oblikoval sodobni pojmovni instrumentarij, ki opredeljuje pravico do zasebnosti in mehanizme za njeno varovanje. Pravico do zasebnosti se čedalje pogosteje opredeljuje kot pravico, ki varuje posameznikove podatke in informacije pred različnimi posegi zbiranja, obdelovanja in posredovanja (Šelih 1999, 43). Čebulj (1992, 16) ob tem navaja, da se je pojem zasebnosti v sodobni družbi razvil tako, da obsega poleg zasebnosti v prostoru (pravica biti sam) in poleg zasebnosti osebnosti (pravica do svobode misli in izražanja), tudi informacijsko zasebnost. Bistvo informacijske zasebnosti pa je v pravici[77] posameznika, da zase obdrži informacije o sebi, ker noče,

[76] Ta razlaga se zdi zelo poetična in naivna, zato jo velja sprejeti z določenim pridržkom (op. M.D.).
[77] Uresničevanje pravice posameznika, da obdrži in nadzoruje informacije o sebi, še zdaleč ni enostavno, saj večina

da bi se z njimi seznanili tudi drugi. Ta vrsta zasebnosti stopa v sodobni družbi v ospredje in se povezuje z vprašanji varstva osebnih podatkov. Njen pomen se povečuje z razvojem novih tehnologij, ki bliskovito povečujejo možnosti[78] zbiranja in medsebojnega združevanja podatkov in informacij (Šelih 1999, 43).

Od leta 1972 se je v skladu s predlogi poročila o pravici do zasebnosti, ki ga je izdelala Mednarodna komisija[79] pravnikov, začela oblikovati posebna zakonodaja[80], ki je določila načela za zbiranje in obdelavo osebnih podatkov, pogoje za zbiranje, obdelovanje in posredovanje takšnih podatkov. Prav tako je v ospredje prodrla tudi zamisel o ustanavljanju posebnih teles, ki naj bi nadzirala zbiralce podatkov (Šelih 1999, 42).

Ni dvoma, da je vloga prava pri reguliranju informacijskih in komunikacijskih tehnologij skrajno težavna in nehvaležna. Po eni strani mora pravo postavljati pravila za preprečevanje možnih zlorab in ovire za neomejeno zbiranje ter obdelavo podatkov, po drugi strani pa ne sme pretirano omejevati in krniti razvoja teh istih tehnologij, ki so nujne za obstoj in razvoj sodobne družbe (Šelih 1999, 45).

Lyonov (1994, 171) pogled na vlogo prava pri reguliranju informacijske in komunikacijske tehnologije je precej kritičen. Meni, da so zakonodajni ukrepi sami po sebi nezadostni, saj razvoj pravne regulacije vselej nekoliko zaostaja za razvojem tehnologije nadzora. Ob tem opozarja, da je uporaba[81] računalnikov za namene hranjenja osebnih podatkov sicer res privedla do oblikovanja zakonodaje, ki ščiti osebne podatke, toda hkrati ta zakonodaja regulira predvsem računalniške procese in aplikacije, ne more pa regulirati samih strojev, podatkov in uporabnikov.

Velik del zakonodaje za zaščito informacijske zasebnosti temelji na načelih, ki jih je v poročilu leta 1978 podal britanski »Lindopov[82] komite«. Osrednja ideja teh načel je, da lahko le »*določeni ljudje (in zgolj določeni ljudje) uporabljajo določene osebne informacije (in zgolj določene osebne*

ljudi ne ve natanko, katere informacije o njih se hranijo, obdelujejo, uporabljajo in posredujejo naprej. To jasno kaže, da je posameznikov nadzor nad informacijami o sebi mnogo bolj zapleten in težaven kot kdajkoli prej.

78 Možnosti zbiranja informacij obsegajo kopičenje podatkov o finančnih transakcijah, nakupih, telefonskih pogovorih, medicinskih diagnozah, kaznivih dejanjih in prekrških. S tem pa je omogočeno oblikovanje obsežnih digitalnih dosjejev o posameznikovem življenju in v perspektivi tudi poglobljen množični nadzor – nadzor celih populacij.

79 Ang. International Commission of Jurists.

80 Zakoni, ki obravnavajo področje varstva osebnih podatkov, se med državami sicer razlikujejo. Kljub nekaterim razlikam pa izražajo nek skupni »minimalni« standard, ki v zvezi z zbiranjem, obdelavo in posredovanjem informacij zahteva, da so informacije pridobljene na zakonit način, da se uporabijo zgolj v tiste namene, ki so bili predvideni na začetku, da se pri uporabi ne preseže namena zaradi katerega so bile zbrane, da so natančne in ažurne, da so ustrezno zavarovane in uničene, ko je njihov namen izpolnjen. Prav tako je pomembno, da ima oseba, o kateri se zbirajo podatki, možnost vpogleda v te podatke.

81 Računalniki iz podatkov ustvarjajo informacije, ki jih nato procesirajo in shranijo. Podatek sam po sebi dostikrat ni zanimiv (npr. zgolj ime nekega posameznika). Toda skupek ločenih podatkov (ime, priimek, naslov bivališča, telefonska številka, številka bančnega računa, itd.) pa že lahko predstavlja zanimivo in včasih tudi občutljivo informacijo.

82 Ang. British »Lindop« Committee.

informacije) za določene namene (in zgolj določene namene)« (Lyon 1994, 172). Na teh načelih, ki poudarjajo zakonito in pošteno zbiranje informacij, njihovo časovno omejeno hrambo, vnaprej določen namen uporabe, idr., je utemeljena tudi Konvencija Sveta Evrope. Pomembna značilnost omenjenih načel je tudi ta, da dajejo osebam, o katerih se zbirajo podatki, pravico do vpogleda v te podatke in pravico do spremembe oziroma izbrisa napačnih podatkov (Lyon 1994, 172).

Ena od temeljnih značilnosti zakonodaje za zaščito informacijske zasebnosti je t.i. »tehtanje in ravnotežje interesov«. V osnovi gre za to, da zasebnost ne zavzema mesta absolutne vrednote, ampak je ena od številnih vrednot, ki jih je pri iskanju rešitve nekega pravno oziroma politično opredeljenega problema prav tako potrebno upoštevati (Lyon 1994, 172). Ker iskanje ravnotežja vselej predpostavlja prevlado ene vrednote nad drugo, je tudi vrednost zasebnosti odvisna od številnih okoliščin, interesov in nasprotujočih si vrednot v konkretni situaciji. Kljub vsem morebitnim pomislekom o (ne)učinkovitosti pravnega varstva osebnih podatkov, je pravica do informacijske zasebnosti v veliki meri odvisna prav od stopnje pravnega in političnega razvoja države, pa tudi njenega članstva v kateri od regionalnih organizacij, ki nalaga dolžnost usklajevanja z mednarodnimi pravnimi instrumenti (Šelih 1999, 47).

4.7 SISTEMI PRAVNEGA VARSTVA INFORMACIJSKE ZASEBNOSTI

Poročilo *Privacy & Human Rights 2002* (EPIC 2002, 4-5) o meta-analiza nacionalnih zakonodaj, ki urejajo varstvo pravice do informacijske zasebnosti, navaja štiri osnovne sisteme pravnega varstva zasebnosti. Posamezna država lahko uporablja zgolj en sistem ali pa kombinacijo različnih sistemov:

- Prvi sistem pravne regulacije informacijske zasebnosti: **Splošni[83] zakoni**
  Številne države imajo splošne zakone, ki določajo način in potek zbiranja, uporabe ter posredovanja osebnih podatkov tako v javnem kakor tudi v zasebnem sektorju. Posebna nadzorna telesa skrbijo za uveljavljanje teh zakonov in pravil. Ta model prevladuje v državah članicah Evropske Unije. Posebne različice tega modela imata tudi Kanada in Avstralija, kjer pravila za zaščito zasebnosti razvija predvsem industrija, nadzor pa izvajajo zasebne agencije.

[83] Ang. comprehensive laws.

- Drugi sistem pravne regulacije informacijske zasebnosti: **Sektorski[84] zakoni**

  V tem sistemu ne obstajajo splošni zakoni, ki bi pokrivali področje varovanja informacijske zasebnosti, ampak to vlogo opravljajo sektorski zakoni za posamezna področja. Primer takšne ureditve predstavljajo Združene države Amerike, ki nimajo splošnega zakona o varovanju osebnih podatkov, pač pa imajo sektorske zakone. Ti urejajo specifična področja, npr. področje zvočnih in video zapisov, področje finančne zasebnosti, idr. Glavna slabost takšnega modela je zaostajanje za tehnološkim razvojem. Ko nastane neka nova tehnologija, je potrebno sprejeti nov zakon, ki bo varoval pravico do zasebnosti na novem področju. Dokler pa takšen zakon ni sprejet, je pravica do zasebnosti na področju, ki ga pokriva nova tehnologija, pomanjkljivo zavarovana. Številne države s pridom kombinirajo prvi in drugi sistem. V takšnih primerih splošne zakone dopolnjujejo sektorski zakoni, ki omogočajo bolj obsežno in bolj temeljito zaščito posameznih kategorij informacij in podatkov.

- Tretji sistem pravne regulacije informacijske zasebnosti: **Samoregulacija**

  Zaščito osebnih podatkov je vsaj v teoriji mogoče zagotoviti tudi s pomočjo različnih mehanizmov samoregulacije. V skladu s tem organizacije zasebnega in javnega sektorja vzpostavijo pravila dobre prakse in se zavežejo k internemu nadzoru. V številnih državah, še posebej v ZDA, so se takšna prizadevanja izkazala kot neučinkovita in pomanjkljiva.

- Četrti sistem pravne regulacije informacijske zasebnosti: **Individualna uporaba tehnologije**

  Z razmahom komercialno dostopnih tehnologij je varovanje zasebnosti postalo realna možnost posameznikov. Uporabniki spleta in drugih aplikacij lahko uporabijo širok nabor programov in sistemov, ki skrbijo za zagotavljanje različne stopnje zasebnosti komunikacij. Sem sodijo predvsem enkripcija, anonimni odjemalci pošte, proxy strežniki in digitalni denar.

4.8 GIBANJA ZA ZASEBNOST

Temelji pravice do zasebnosti v kontinentalnem in anglosaksonskem pravnem sistemu izvirajo iz nekaterih že dolgo uveljavljenih pravic, npr. pravice do telesne nedotakljivosti, pravice do

[84] Ang. sectorial laws.

nedotakljivosti stanovanja, pravice do časti in dobrega imena, idr. Vendar pa je šele razvoj informacijske tehnologije sprožil razmislek o posebni pravici do zasebnosti, ki sta jo ob koncu 19. stoletja prvič eksplicitno izpostavila ameriška pravnika Warren in Brandeis. Informacijska tehnologija je namreč že od svojega začetka predstavljala grožnjo posameznikovi zasebnosti, ki jo je bilo potrebno s pravom ustrezno zaščititi.

Kam lahko pripelje pomanjkanje zasebnosti je pokazala druga svetovna vojna z vzponom nacizma, ki je posameznika popolnoma podredil interesom države. Po vojni se je mednarodna skupnost soočila z nujo, da sprejme splošno veljavne civilizacijske standarde, ki so dobili pravno obliko v Splošni deklaraciji človekovih pravic in različnih mednarodnih konvencijah o človekovih pravicah. Pravica do zasebnosti je prav tako dobila svoje mesto v teh mednarodnih pravnih dokumentih, hkrati pa je postala sestavni del številnih državnih ustav, ki so svojo vsebino pogosto oblikovale po vzorcu Splošne deklaracije človekovih pravic.

Sedemdeseta in osemdeseta leta dvajsetega stoletja so z razvojem osebnega računalnika in interneta vnesla pravo revolucijo na področju informacijskega nadzora. Pojavila se je velika potreba po pravni regulaciji informacijske tehnologije in iz nje izvirajočega nadzora. V tem obdobju se je pod vplivom političnih in nevladnih iniciativ (pri tem so sodelovali tako posamezni predstavniki vseh treh vej oblasti, kot tudi nevladne organizacije, strokovnjaki in laična javnost) okrepilo pravno varstvo zasebnosti. Področje, ki naj bi ga varovalo pravo, je s tem sicer postalo bolj urejeno in zaščiteno, toda obenem se je sfera zasebnosti bistveno skrčila. Del zasebnosti, ki jo je užival človek z začetka 20. stoletja, je postal pravno reguliran, še večji del zasebnosti pa se je pod vplivom informacijske tehnologije enostavno preoblikoval v zabrisano pol-javno in pol-zasebno sfero, kjer pravica do zasebnosti pogosto ni več učinkovito zaščitena.

Lyon (1994, 172-174) se zato sprašuje o (ne)učinkovitosti zakonodaje, ki naj bi varovala pravico do zasebnosti. Razmišlja o komplementarnih načinih varovanja zasebnosti, kjer izstopajo predvsem družbena, kulturna in politična gibanja. Ta so se razširila v ZDA in v Evropi že v sedemdesetih letih prejšnjega stoletja, ko je vprašanje zasebnosti predstavljalo eno pomembnejših tem v političnih razpravah. V tistem času se je v Evropi dvignilo močno gibanje proti popisu prebivalstva, ki je bilo najmočnejše na Nizozemskem, kar glede na izkušnjo s popisom in posledicami popisa, ki so ga izvajali med nacistično okupacijo, verjetno ni naključje. Iz tega gibanja se je v poznih osemdesetih letih oblikovala organizacija Privacy Alert (Stichting Waakzaamheid Persoonregistratiie), ki je v naslednjih dvajsetih letih postala največja nevladna organizacija za varstvo zasebnosti v svetovnem merilu. Vendar je leta 1994, prav v času, ko je Nizozemska začela uvajati schengenski sistem nadzora meja, osebne izkaznice in identifikacijske številke za prebivalstvo, organizacija prenehala z delovanjem (Davies 2001, 154).

Podobna usoda je doletela tudi druge organizacije, npr. New Zealand Privacy Foundation, Australian Privacy Foundation in Canadian Privacy Council, ki je propadel tako rekoč takoj po ustanovitvi (Davies 2001, 154-155). V tem pogledu je ena redkih izjem Electronic Privacy Information Center[85] (EPIC) iz Washingtona, ki deluje še danes in združuje številne strokovnjake in aktiviste s področja zasebnosti s celega sveta. EPIC sodeluje tudi s Privacy International[86], ki ima bistveno manjši vpliv, z Electronic Frontier Foundation in z American Civil Liberties Union, ki pa se ukvarjata tudi z drugimi temami. Dodati velja, da gre v primeru EPIC za gibanje, ki je večinoma neinstitucionalizirano, saj gre za mrežo posameznikov, ki med seboj komunicirajo po internetu, in se aktivira le občasno, ob kriznih dogodkih, ki ogrožajo zasebnost (Kovačič 2006, 88).
Številna od teh gibanj so dosegla določene uspehe na področju razreševanja političnih in pravnih problemov, ki so povezani z elektronskim nadzorom in varovanjem pravice do informacijske zasebnosti. Znan je primer iz leta 1985, ko je avstralska vlada predlagala uvedbo posebne elektronske identifikacijske kartice. Aktivisti so kritizirali tako tehnične vidike elektronskih kartic kot tudi morebitno (ne)učinkovitost pri zmanjševanju števila davčnih in drugih utaj. Na svojo stran so pridobili velik del javnega mnenja in medijske pozornosti. Poizkus uvedbe elektronskih kartic je postal odmevna politična zadeva, ki jo je v parlamentu s pridom izkoristila opozicija in naposled preprečila načrte vlade (Lyon 1994, 174).

Kljub občasnim uspehom aktivistov, nevladnih organizacij in gibanj za zasebnost, se čedalje bolj zdi, da je z 11. septembrom 2001 zanimanje za varovanje zasebnosti upadlo. Res je sicer, da se o zasebnosti veliko govori, vendar se ta problematika praviloma ne pojavlja na volilnih programih političnih strank. Prav tako je teroristični napad na WTC okrepil strah pred terorizmom, zato se v zadnjih letih poudarek v javnih razpravah daje predvsem varnosti, pogosto tudi na račun zasebnosti. Razen tega so ljudje kljub načelnemu zavzemanju za zasebnost do nje pravzaprav precej brezbrižni, saj prostovoljno prodajajo osebne podatke za minimalne ugodnosti (npr. razne popuste v trgovinah). V tej povezavi velja poudariti, da se je v zadnjih desetletjih zgodil pomemben premik v razumevanju koristi informacijskega nadzora, kar se posledično kaže v nezainteresiranosti številnih akterjev za pravno varstvo zasebnosti. Tradicionalno je nadzor sodil predvsem v domeno države in

[85] Electronic Privacy Information Center (EPIC) je javni raziskovalni center v Washingtonu. Ustanovljen je bil leta 1994. Vsebinsko se ukvarja s problematiko zasebnosti in pravic, ki so povezane z njo. Prav tako skrbi za obveščanje javnosti o pomembnih zadevah v zvezi z zasebnostjo. EPIC je močno povezan s Skladom za ustavno vladavino (ang. Fund for Constitutional Government), s Transatlantskim dialogom potrošnikov (ang. Transatlantic Consumer Dialog), Globalno kampanijo za svobodo interneta (ang. Global Internet Liberty Campaign), Zavezništvom za svobodno izražanje na internetu (ang. Internet Free Expression Alliance) in Koalcijo za zasebnost na internetu (ang. Internet Privacy Coalition) (http://epic.org).

[86] Privacy International (PI) je skupina strokovnjakov, ki se je oblikovala leta 1990. Pokrivajo področje človekovih pravic in zasebnosti, pri tem pa opravljajo vlogo »čuvajev« tako, da nadzorujejo delo državnih in zasebnih organizacij. Privacy International ima urad v Londonu in Washingtonu (www.privacyinternational.org).

njenega represivnega aparata. Vendar pa je z razvojem osebnega računalnika informacijski razvoj postal zanimiv tudi za komercialni sektor. Korporacijam sta poceni zbiranje in analiza podatkov o potrošnikih omogočila izdelovanje profilov potrošnikov, njihovih vedenjskih vzorcev in okusov. S tem so bili položeni temelji usmerjenega oglaševanja in prirejene ponudbe, kar je omogočilo večji zaslužek. Prav tako je nadzor delodajalcem omogočil bolj učinkovito izkoriščanje kadrovskih virov, zato so, zlasti v ZDA, kjer je privatni sektor slabše reguliran kot v Evropi, podjetja postala eden glavnih nasprotnikov pravice do zasebnosti, kar utegne v prihodnosti bistveno upočasniti in zožiti proces zavzemanja za pravno zaščito zasebnosti.

Po drugi strani se je (več o tem v Kovačič 2006, 89) skrb za pravico do zasebnosti v veliki meri profesionalizirala. Številne Evropske države so uvedle posebne pooblaščence oziroma varuhe pravice do zasebnosti, ki se s področjem varstva zasebnosti ukvarjajo profesionalno. Prav tako se z določenimi segmenti varovanja zasebnosti ukvarjajo tudi strokovnjaki za informacijsko varnost. Zato gibanjem za zasebnost ne preostane drugega, kakor da se osredotočajo na tista vprašanja varstva zasebnosti, ki še niso institucionalizirana. Sem sodijo predvsem problemi s področja zlorab, ki jih državni organi zaradi pomanjkljive zakonodaje ali pa zaradi omejitev, ki izhajajo iz teritorialne pristojnosti zakonodaje, ne preganjajo, in tudi problemi informacijske varnosti in nevarnosti, ki jih prinašajo nove tehnologije. Organizacije in člani gibanj za zasebnost se povezujejo in sodelujejo prek interneta (tipičen primer je EPIC, ki izdaja letno poročilo o zasebnosti, pripravljajo pa ga strokovnjaki z vsega sveta, ki med seboj komunicirajo praktično samo po internetu), ukvarjajo pa se tako s spremembami zakonodaje kot s spremljanjem nevarnosti, ki jih prinašajo nove tehnologije. Čedalje bolj se ukvarjajo tudi s problemi zasebnosti na internetu (Kovačič 2006, 90).
Kljub številnim pomislekom glede (ne)učinkovitosti nevladnih organizacij pri prizadevanju za varovanje zasebnosti, je poročilo *Privacy & Human Rights 2002* (EPIC 2002) bolj optimistično, saj navaja, da *»11. september še ni naznanil konca zasebnosti. Nevladne organizacije po vsem svetu se združujejo v prizadevanjih za preprečitev tistih vladnih predlogov, ki vodijo k oženju zasebne sfere«* (EPIC 2002, 1). Čas bo seveda pokazal ali je tak optimizem (ne)upravičen.

4.9 SVETLA STRAN ZASEBNOSTI

V poročilu ameriškega Ministrstva za zdravje, izobrazbo in socialo (US Department of Health,

Education and Welfare) iz leta 1973 je zapisano, da »*obstaja zelo razširjeno prepričanje, da je zasebnost ključnega pomena za naše fizično, psihološko, socialno in moralno dobro počutje«*. Michael Weinstein pa pravi, da je »*zasebnost dragocena, ker predstavlja način zmanjševanja napetosti, ki je sestavni del družbenih odnosov«* (Weinstein v Solove 2009, 79). Podobno trdi Alan Westin: »*Zasebnost ljudem omogoča oddih od vrtinca aktivnega življenja«* (Westin v Solove 2009, 79). V skladu s temi navedbami je zasebnost koristna predvsem zato, ker spodbuja psihološko zdravje in dobro počutje ljudi.

Nekateri pisci gredo še dlje in poudarjajo, da je zasebnost ključnega pomena za osebni samorazvoj. Tako Paul Freund pravi, da »*zasebnost nudi zatočišče, ki omogoča sprostitev inhibicij, samoraziskovanje, samozavedanje, samousmerjanje, inovacijo, gojenje občutka edinstvenosti in sprostitev od tlake vsakodnevnega življenja«* (Freund v Solove 2009, 79). Westin trdi, da je zasebnost »*instrument za doseganje individualnih ciljev in samouresničenja«* (Westin v Solove 2009, 79). Posamezniku zagotavlja prostor za intelektualno in duhovno kontemplacijo. S tem, ko zasebnost ščiti pred družbenimi pritiski, omogoča posamezniku izražanje sebstva in tiste individualnosti, ki je v nasprotju s prevladujočimi družbenimi normami. Prav zaradi zasebnosti so ljudje lahko bolj ekscentrični in edinstveni, bolj pristni in manj previdni glede izrečenih besed ali storjenih dejanj.

Številni avtorji vidijo vrednost zasebnosti v ustvarjanju ugodnih razmer za vzpostavljanje intimnih odnosov. Robert Gerstein meni, da »*intimni odnosi ne bi mogli obstajati, če družba ne bi zagotavljala trenutkov zasebnosti«* (Garstein v Solove 2009, 80). Jeffrey Rosen pa dodaja, da »*intimni odnosi, ki so osnovani na poglobljenem poznavanju sočloveka, potrebujejo ustrezen prostor in čas, ki ju brez zasebnosti ni mogoče zagotoviti«* (Rosen v Solove 2009, 80).

Drugi, bolj politično usmerjeni pisci, vrednost zasebnosti iščejo v širšem družbenem kontekstu. Ruth Gavison poudarja, da je *»zasebnost nujna za demokratično vladanje, saj spodbuja in goji moralno avtonomijo državljana, kar je predpogoj za dejansko demokracijo«* (Gavison v Solove 2009, 80). Keith Boon pa pravi, da je zasebnost »*ključnega pomena za uresničevanje nekaterih specifičnih vidikov demokratične družbe«* (Boon v Solove 2009, 80). Tako služi kot podlaga volilni svobodi, političnim razpravam in svobodnemu združevanju. Enakih misli je Paul Schwartz (v Solove 2009, 80), ki zasebnost razume kot način ustvarjanja prostora za civilni dialog in demokratično razpravo.

Zasebnost ustvarja prostor, kjer je posameznik varen pred različnimi oblikami prisile in vmešavanjem s strani drugih oseb. Izničenje[87] tega posameznikovega zavetja, ki predstavlja izraz

[87] Izničenje zasebnosti je značilno za številne totalitarne režime. Kot primer: Lenin je leta 1920 naznanil, da (komunisti) »*ne priznamo ničesar zasebnega. Naša morala je popolnoma podrejena interesom proletariata, ki bije*

človekove težnje po avtonomiji in neodvisnosti od družbenega nadzora (Hirshleifer 1980, 651), bi po prepričanju Berlina (1992, 73) vodilo v despotizem in degradiranje človekovega bistva. Hanna Arendt (1995) vidi v tem »room of one`s own« predpogoj političnega delovanja, nujno zavetje, ki ga potrebujemo, da bi se zatopili v dialog s samim seboj takrat, ko moramo misliti in razsojati. Zato Berlin (1992, 71) poudarja, da je potrebno začrtati jasno mejo med območjem zasebnega življenja in območjem javne oblasti. Vendar pa v 21. stoletju delitev med javnim in zasebnim na marsikaterem področju ni več jasna. Habermas (1989) opozarja, da se je z razvojem množičnih občil med politično in zasebno vrinila družbena sfera, ki je pod svoje okrilje vzela velik del tistega, kar je v antiki sodilo v zasebno sfero. Družbena sfera je bila že od samega začetka zabrisana, pol-zasebna in pol-javna, v največji meri definirana s pomočjo javnega mnenja, ki je za posameznikovo zasebnost nemalokrat predstavljalo večjo nevarnost kot državna oblast. Razen tega je razvoj interneta meje med javnim in zasebnim še bolj zabrisal, celo tako, da pogosto ni več mogoče razmišljati o delitvi na javno in zasebno. Zato se pogosto zdi, da pravica do zasebnosti varuje predvsem posameznikovo intimno in otočke zasebnosti v heterogenem informacijskem oceanu, kjer ločnica med javnim in zasebnim izgublja svoj pomen.

4.10 TEMNA STRAN ZASEBNOSTI

Čeprav se zasebnost pogosto razume kot nekaj dobrega, zaželenega in celo nujnega za obstoj demokratične družbene ureditve, se vseskozi pojavljajo kritike, ki opozarjajo na njene temne strani. Ena od kritik na račun zasebnosti, ki je prisotna predvsem v bolj kolektivno usmerjenih in manj individualističnih družbah, opozarja, da zasebnost varuje posameznika na račun celotne skupnosti in s tem predstavlja grožnjo družbeni solidarnosti. Profesor Yao-Huai Lu (v Solove 2009, 80) navaja primer kitajske družbe, kjer še vedno prevladuje mnenje, da je kolektivno bolj pomembno od individualnega, zato v takšni družbi kljub modernizaciji ni zaznati tako izrazite težnje po zasebnosti kot na Zahodu.

Tudi številni vizionarji utopičnih družb si idealno družbo zamišljajo predvsem kot močno povezano skupnost, kjer ni veliko prostora za zasebno življenje. Nazoren primer je *Utopija* Thomasa Mora. V njegovi idealni družbi ni nič skrito, družbeni red pa je osrednjega pomena: *»Ker so ljudje nenehno podvrženi pogledom drugih, nimajo priložnosti za počenjanje nečastnih reči«* (More 1958, 73).

razredni boj« (v Lyon 1994, 186). Nacisti so leta 1930 dejali, da je *»edina zasebna oseba v Nemčiji tista, ki spi«* (v Lyon 1994, 186).

Kritike zasebnosti se usmerjajo tudi v onemogočanje družbenega nadzora. Zasebnost namreč lahko služi prikrivanju nedovoljenih dejavnosti, zmanjšuje posameznikovo odgovornost in krha družbeni red. Psiholog Bruno Bettelheim je ob obisku izraelskih kibucov zapisal, da je »*odsotnost kriminala, delikventnosti in drugega protisocialnega vedenja presenetljiva. Policije sploh ne potrebujejo«* (Bettelheim v Solove 2009, 81). Čeprav ga je pomanjkanje zasebnosti v kibucih dušilo, ni spregledal učinkovitosti popolnega družbenega nadzora.

Sociolog Steven Nock pa opozarja, da zasebnost otežuje vzpostavljanje zaupanja med ljudmi: »*Zaupanje, da drugim verjamemo na besedo, predstavlja eno od osnovnih sestavin družbenega reda. Vendar pa zasebnost otežuje spoznavanje drugih ljudi in njihovega ugleda, kar zelo otežuje presojanje o tem ali naj človeku zaupamo ali ne«* (Nock v Solove 2009, 81).

Po besedah nekaterih kritikov zasebnost ovira odkrivanje in preprečevanje kriminalitete, s tem pa posledično ogroža tudi nacionalno varnost. Profesor prava William Stuntz trdi, da »*učinkovita vlada - tista, ki ščiti državljane in ravna odločno, ko je to potrebno – izumira«* (Stuntz v Solove 2009, 83). Velik delež k temu »izumiranju« po mnenju Stuntza prispeva prav zasebnost. Sodnik Richard Posner (v Solove 2009, 83) relativizira vrednost zasebnosti s sklicevanjem na grožnje terorizma in širjenje orožja za množično uničevanje, ki od države terjajo, da ustvarja obsežne zbirke podatkov o domačih in tujih državljanih.

Kritike zasebnosti prihajajo tudi s strani nekaterih feministk, ki opozarjajo, da zasebnost velikokrat prikriva nasilje moških nad ženskami. Zgodovina kaže, da je bila javna sfera v domeni moških, ženske pa so bile potisnjene v gospodinjstvo, torej v privatno sfero. S tem so bile ženske izključene iz javnega življenja, njihovi problemi pa izvzeti iz javnih razprav. To je razvidno iz prakse sodišč 19. stoletja, ki so si zatiskala oči pred družinskim nasiljem v imenu varovanja zasebnosti.

Zato si del feministk prizadeva, da se zasebnost na novo definira ali celo odpravi, saj je mogoče problematiko družinskega nasilja in nasilja nad ženskami ustrezno reševati šele tedaj, ko se jo prenese iz zasebne v javno sfero, kjer postane predmet družbene in politične razprave. Prav tako odsotnost zasebnosti in širjenje informacijskega družbenega nadzora nekatere zlorabljene ženske varuje[88] pred ponovnimi zlorabami s strani družinskih članov (Lyon 1994, 183).

Caroline Pateman povzema, da »*dihotomija med privatnim in zasebnim prikriva in opravičuje podrejanje žensk znotraj navidezno univerzalnega, egalitarnega in individualističenga reda«* (Pateman v Solove 2009, 82), ki mu v resnici vladajo moški.

Zasebnost nenazadnje lahko omejuje tudi ekonomsko učinkovitost in dobičkonosnost. Fred Cate pravi, da »*zasebnost posega v zbiranje, organiziranje in shranjevanje informacij, ki jih gospodarski*

[88] Takšnih oblik »varovanja« se poslužujejo tudi nekatere etnične manjšine – povečan državni družbeni nadzor jih namreč bolj ali manj učinkovito varuje pred nasiljem drugih družbenih skupin (Lyon 1994, 183).

sektor potrebuje za sprejemanje nekaterih odločitev, na primer dajanje kreditov ali sprejemanje čekov. Zaradi tega zasebnost lahko vpliva na manjšanje produktivnosti, kar lahko vodi k višanju cen izdelkov in storitev« (Cate v Solove 2009, 83).

Virginia Postrel (v Solove 2009, 83) gre pri kritiki zasebnosti še dlje. Pravi, da zasebnost omejuje zbiranje podatkov in pretok informacij, s tem pa krati tudi svobodo govora in tiska.

Ob številnih kritikah ne preseneča, da nekateri avtorji zasebnost dojemajo predvsem kot bolezen, ki razjeda »zdravo« družbeno tkivo. Najdejo pa se tudi takšni, ki zasebnost tolmačijo kot relikt pretekle dobe. Alan Westin pravi, da je bil Warrenov in Brandeisov poziv k formuliranju pravice do zasebnosti pravzaprav le »*protest zagovornikov patricijskih vrednot proti širjenju političnih in kulturnih vrednot množične družbe«* (Westin v Solove 2009, 82).

V množični družbi, kjer informacijska tehnologija prežema vse vidike človeškega življenja in ob tem briše mejo med javnim in zasebnim, vprašanje o pravici do zasebnosti morda kmalu res ne bo imelo več nobenega pomena (Lyon 1994, 16).

5 SISTEM PRAVICE DO ZASEBNOSTI

Zametki pravnega varovanja zasebnosti sicer segajo že v 18. stoletje, toda prva sistematična razprava o konceptu pravice do zasebnosti se je pojavila šele ob koncu 19. stoletja v Združenih državah. Preteči je moralo več kot pol stoletja, da je leta 1965 Vrhovno Sodišče ZDA priznalo ustavno pravico do zasebnosti, čeprav ta še vedno ni eksplicitno zapisana v zvezni ustavi. Šele po drugi svetovni vojni je pravica do zasebnosti postala sestavni del mednarodnih pravnih dokumentov, npr. Splošne deklaracije človekovih pravic in Mednarodnega pakta o državljanskih in političnih pravicah. Zakonodaje posameznih držav pa so pravico do zasebnosti pričele intenzivno varovati šele v sedemdesetih in osemdesetih letih 20. stoletja, ko je razvoj računalnikov in telekomunikacijskih omrežji bistveno okrepil nevarnost informacijskega nadzora. Evolucija pravnega varstva zasebnosti je v anglosaksonskem in kontinentalnem pravnem sistemu potekala nekoliko različno. V ZDA se je zasebnost zavarovala predvsem v razmerju do javnega sektorja, v privatnem sektorju pa je ostala večinoma prepuščena interni regulaciji delodajalcev. Evropska unija je ubrala drugačno pot, saj je posameznikovo zasebnost zaščitila tako v razmerju do države kot tudi v razmerju do privatnega sektorja. Slovenija je sledila razvoju zakonodaje Evropske unije, zato je danes pravno varstvo zasebnosti v Sloveniji primerljivo s pravnim varstvom v drugih razvitih evropskih državah.

5.1 PRAVICA DO ZASEBNOSTI V ZDRUŽENIH DRŽAVAH AMERIKE

Pravica do zasebnosti sicer ni izrecno zapisana[89] v ameriški ustavi, vendar pa je Vrhovno sodišče ZDA leta 1965 v primeru Griswold v. Connecticut priznalo obstoj ustavne pravice do zasebnosti. Pri tem se je izkazalo, da ameriška pravna praksa zasebnosti ne dojema le kot pravice biti sam in kot pravice do zasebnosti komuniciranja, pač pa jo povezuje tudi z avtonomijo posameznika (Kovačič 2006, 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, 86).

Primer Griswold v. Connecticut, ki je bil podlaga za priznanje pravice do zasebnosti v ameriški ustavi, sta 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 zasebnost«, 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, starejša kot naše politične stranke in starejša kot naš šolski sistem«* (Turkington in Allen v Kovačič 2006, 56).

Ustavnost pravice do zasebnosti je še dodatno utemeljil sodnik Goldberg v ločenem pritrdilnem mnenju. Po njegovem mnenju so sestavljavci ustave priznavali še obstoj drugih pravic, ki obstajajo ob pravicah, zapisanih v ustavi in ustavnih amandmajih. Dokaz za to je videl predvsem v devetem amandmaju, ki določa, da naštevanje pravic v ustavi ne sme biti tolmačeno tako, kot da drugih pravic ni, in pri tem izpostavil svoje strinjanje z ugotovitvijo sodišča, da je pravica do zasebnosti temeljna osebna pravica (Turkington in Allen v Kovačič 2006, 56).

Fred H. Cate ameriško ustavno pravico do zasebnosti deli na štiri področja, ki predstavljajo temelj za priznavanje obsega pravnega varstva zasebnosti v ZDA, pa tudi omejitve varovanja zasebnosti.

Prvo področje predstavljajo odločitve Vrhovnega sodišča ZDA, ki se navezujejo na svobodo izražanja, združevanja in religije. Drugo skupino predstavljajo odločitve Vrhovnega sodišča ZDA, ki se nanašajo na preiskavo in zaplembo 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, 52-65).

[89] Je pa zato zapisana v ustavah nekaterih zveznih držav.

Ameriška ustava je zasnovana na predpostavki ščitenja posameznika pred državo, zato podeljuje t.i. negativne pravice, ki določajo, česa država ne sme storiti in s tem ustvarjajo prostor posameznikove svobode. V tej perspektivi ne preseneča specifični razvoj varstva zasebnosti, ki ima za posledico širjenje avtonomije posameznika. Hkrati pa prav ta okoliščina predstavlja poglavitno pomanjkljivost varstva zasebnosti v ZDA, saj preprečuje učinkovito varovanje informacijske zasebnosti. Zakon o zasebnosti (ang. Privacy Act) sicer vsebuje omejitve pri razkrivanju osebnih podatkov, toda te omejitve ne veljajo za Kongres in druge preiskovalne organe, pa tudi za druge vladne agencije ne, ko gre za njihovo t.i. rutinsko uporabo, ki v praksi lahko pomeni pravzaprav katerokoli rabo (Cate 1997, 78).

Pravni okvir varovanja informacijske zasebnosti predstavljata zakon o svobodi informacij (ang. Freedom of Information Act oziroma FOIA) in zakon o zasebnosti, ki pa veljata samo za javni sektor. Glavni problem varovanja informacijske zasebnosti posameznikov v ZDA ne predstavlja javni, ampak zasebni sektor, ki ni podvržen državni regulaciji, pač pa trgu (Kovačič 2006, 57). Zato je v ZDA prostorska, komunikacijska in informacijska zasebnost zunaj doma in zunaj konteksta vladnega preiskovanja in zaplembe slabo varovanja (Cate 1997, 65), pravna ureditev teh področji 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 (Kovačič 2006, 58).

Poseben problem predstavlja tudi t.i. sektorski pristop zaščite zasebnosti, kar pomeni, da v ZDA nimajo splošne zakonodaje za zaščito pravice do zasebnosti, imajo pa sprejete številne zakone in uveljavljenje različne partikularne rešitve. Pomanjkljivost sektorskega pristopa je tudi v tem, da je treba z razvojem vsake nove tehnologije specifično področje zasebnost na novo urediti, zato je sledenje zakonodaje tehnološkim spremembam bistveno upočasnjeno (EPIC 2002).

5.1.1 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 sedemdesetih 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, 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, 529).

V ZDA lahko delodajalec od zaposlenih na delovnem mestu zahteva oddajo telesnih tekočin (za preverjanje vsebnosti drog v organizmu ali kot test nosečnosti). Do leta 1988, ko je bil sprejet Employee Polygraph Protection Act, ki tako početje prepoveduje, so delodajalci lahko izvajali tudi poligrafsko testiranje zaposlenih (Sykes 1999, 144). Prav tako zakon ne preprečuje delodajalcem, da bi zaposlene smeli spraševati tudi najbolj osebna vprašanja (Kovačič 2006, 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[90] O`Connor proti Ortega je Vrhovno sodišče ZDA 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, 59).

Podobno velja tudi za prisluškovanje telefonom, elektronski pošti[91] in uporabi interneta (Klemenčič, 2003, 137). Izkazalo se je namreč, da je leta 1986 sprejeti Electronic Communication Privacy Act (ECPA), ki uravnava prisluškovanje elektronskim komunikacijam, precej pomanjkljiv. ECPA v prvem poglavju sicer prepoveduje prestrezanje elektronskih telekomunikacij, ki poteka hkrati s prenosom podatkov. Vendar pa za nadzorovanje elektronske pošte ni potrebno uporabljati sočasnega prestrezanja. Če delodajalec dostopa do strežnika, v katerem je shranjeno elektronsko sporočilo, s tem zaobide prepoved sočasnega prestrezanja. ECPA namreč v drugem poglavju, ki prepoveduje dostop do shranjenih elektronskih sporočil brez soglasja nadzorovanje osebe, iz prepovedi eksplicitno izključuje »*osebe, ki zagotavljajo žično ali elektronsko komunikacijsko storitev*«. Torej so iz prepovedi izvzeti delodajalci, ki imajo v lasti komunikacijsko opremo podjetja (Sinrod 2004 v Kovačič 2006, 60). V vsakem primeru pa lahko delodajalci kot pogoj za zaposlitev zahtevajo soglasje za nadzor v kakršnemkoli obsegu in v tem primeru je nadzor zaposlenega povsem zakonit.

Organizacija ACLU ugotavlja, da se elektronsko nadzorovanje zaposlenih pogosto sprevrže v

[90] 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 menilo, da uslužbenec v tem primeru upravičeno pričakuje zasebnost na delovnem mestu. Vendar pa je sodišče hkrati ugotovilo, da preiskava ni bila neupravičena (Kovačič 2006, 60).

[91] Leta 1922 se je v Kaliforniji zgodil primer Shoars proti Epson America Inc. Ko je administratorka elektronskega poštnega sistema podjetja Epson ugotovila, da eden od direktorjev prebira elektronsko pošto zaposlenih in ga soočila s tem odkritjem, je bila odpuščena. Alana Shoars je vložila tožbo, vendar se je podjetje branilo, da je sistem za elektronsko pošto v njihovi lasti in imajo zato pravico, da ga upravljajo in nadzorujejo ali se uporablja samo v delovne namene ali ne. Shoarsova je bila prepričana, da bo tožbo dobila, vendar kalifornijsko sodišče njenim argumentom, da je njena zasebnost zaščitena s kalifornijsko ustavo, ni pritrdilo, češ da ustava ščiti samo informacije, ki so osebne, ne pa tudi poslovnih komunikacij. Poleg tega je uporabljala opremo, ki je bila v lastni podjetja (Sykes 1999).

vohunjenje za zaposlenimi. Raziskava American Management Association iz leta 2001 o nadzoru na delovnem mestu je pokazala, da 43% podjetij nadzoruje uporabo telefona, 37% uporablja video nadzor, 36% pregleduje datoteke v računalnikih zaposlenih, 47% pregleduje elektronsko pošto zaposlenih, 63% podjetij spremlja uporabo interneta, 19% pa spremlja uporabo računalnika.
Raziskava je sicer ugotovila, da je nadzor večinoma občasen, vendar se njegov obseg povečuje, hkrati pa postaja čedalje bolj rutinski (Schulman v Kovačič 2006, 61). Po mnenju Schulmana je razlog za premik nadzorovanja posameznikov proti nadzoru celotne populacije zaposlenih ta, da je zdaj celotna delovna sila sumljiva, saj so organizacije čedalje bolj zaskrbljene zaradi t.i. »internih groženj« (Schulman v Kovačič 2006, 62).

5.1.2 VARSTVO INFORMACIJSKE ZASEBNOSTI V ZDA V PRIVATNEM SEKTORJU

Podobno stanje, kot velja na področju zasebnosti na delovnem mestu, v ZDA velja tudi na področju informacijske zasebnosti v privatnem sektorju, kjer je še vedno zelo razširjen lastninski koncept pravice do zasebnosti. Prav tako kot za delodajalca velja, da lahko posega v zasebnost svojih zaposlenih bistveno bolj, kot lahko vlada posega v zasebnost svojih državljanov (Sykes 1999, 147), velja tudi 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, 63). 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, 89-90).
Ko nekdo zbere osebne podatke, so ti njegova last in lahko z njimi počne praktično karkoli, kar 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, kabelsko televizijo, internetne dejavnosti otrok, mlajših od 13 let, podatke o šolanju in izobrazbi, podatke o lastnikih motornih vozil ter podatke, ki jih uporablja telemarketing (Laurant 2003, 526-527). Regulacija obdelave osebnih podatkov v ZDA je v najboljšem primeru podobna gašenju požara, saj se ameriška zakonodaja regulacije tega področja

loteva izrazito kampanjsko – navadno kot odziv na kak razvpit primer[92] zlorabe (Kovačič 2006, 63). Podobno je tudi na področju prisluškovanja elektronskim komunikacijam in tajnemu snemanju pogovorov. Prisluškovanje brez soglasja ali brez sodnega naloga je prepovedano, vendar le, če ga izvaja tretja oseba. ECPA iz leta 1986 namreč določa izjemo, da je razkritje vsebine komunikacij dovoljeno, če se z razkritjem strinja ena stran (Cate 1997, 84). Podobno je Vrhovno sodišče ZDA razsodilo, da je dovoljeno tajno snemanje pogovora, ki ga ima nekdo z drugo osebo, tudi brez sodnega naloga (Kovačič 2006, 64).

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, 64).

Vprašanje obdelave osebnih podatkov v zasebnem sektorju v ZDA torej ni predvsem vprašanje 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, 66).

5.1.3 OBDELAVA IN IZMEVANJA OSEBNIH PODATKOV V ZDA

Dodatno grožnjo informacijski zasebnosti predstavlja obdelava in nadaljnja uporaba zbranih osebnih podatkov, ki v ZDA za zasebni sektor ni regulirana. Razlogi za neregulacijo so predvsem ekonomski interesi t.i. trgovcev z zasebnostjo. Po nekaterih ocenah imajo tri podjetja (Equifax, TRW in Trans Union Corporation), ki se ukvarjajo s kreditnimi poročili, osebne podatke o 90% odraslih Američanov (Etzioni 1999, 128). Podjetje Abacus Alliance iz ZDA je leta 1997 združevalo

[92] Takšen primer je Driver`s Privacy Protection Act iz leta 1994. Zakon so sprejeli kot odziv na umor igralke Rebecce Schaeffer, ki ga je zagrešil njen preveč vneti obožavalec. Ta je podatke o njej dobil s pomočjo zasebnega detektiva iz iz kalifornijskega Urada za motorna vozila. Zakon, ki je bil sprejet kot odziv na ta dogodek, prepoveduje oddajo osebnih podatkov, vendar pa določa štirinajst širokih izjem, ki prvotni namen zakona praktično povsem izničijo, saj med drugim prepoved ne velja za zasebne detektive (Cate 1997, 79).

podatke o nakupih potrošnikov, ki so tisto leto opravili več kot dve milijardi transakcij (Batagelj 1997). Istega leta je podjetje Axciom posedovalo podatke o 196 milijonih Američanov (Whitaker 1999, 132).

Po drugi strani pa neregulaciji tega področja botruje tudi miselnost, ki jo zelo dobro povzema libertarna kritika zasebnosti. Virginia Postrel tako pravi, da sta zbiranje in izmenjava informacij bistvena za svobodno družbo (Sykes 1999, 229). Omejitev obdelave in izmenjave osebnih podatkov naj bi bila tako napad na svobodno novinarstvo, svobodno podjetništvo in svobodo komuniciranja – pri tem ni mišljeno le tržno komuniciranje, ampak tudi pravica, da se posamezniki učimo drug o drugem in širimo informacije. Vendar pa libertarci 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 pa večinoma ni možna, mogoči so le neformalni pritiski javnosti (Kovačič 2006, 67).

Pri tem lahko prihaja do različnih zlorab podatkov. Eden večjih problemov v zadnjem času je 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 - »izvažajo« v Indijo, Pakistan in podobne države, kjer je delovna sila dovolj izobražena, a bistveno cenejša kot v ZDA. Pri tem podjetja pogosto posredujejo v tujino občutljive podatke in pri tem se lahko zaplete (Kovačič 2006, 68).

Eno od nevarnosti pri prodaji osebnih podatkov predstavlja možnost, da te podatke od komericalnih 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, 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 Etzioni 1999, 128; 132; Sykes 1999, 60; Whitaker 1999). David Banisar pa trdi, da se to že dogaja – FBI, DEA in IRS po njegovih trditvah skrivaj kupujejo[93] komercialne zbirke podatkov in jih povezujejo s svojimi preiskovalnimi zbirkami (Banisar v Sykes 1999, 60).

[93] Utemeljenih sumov za to je kar nekaj. Leta 1996 je podjetje Lexis-Nexis za deset dni omogočilo popoln dostop do številk socialnega zavarovanja kar po internetu. Zaradi pritiska javnosti so spletno stran zaprli in to je ustavilo tudi načrte uprave U.S. Social Security, ki je nameravala po internetu ponuditi podatke o osebnih dohodkih in pokojninah vseh imetnikov SSN (Whitaker 1999, 99). Podobno so uradniki več zveznih držav prodali osebne podatke skupaj s fotografijami iz vozniških dovoljenj zasebnemu podjetju, za katerega se je pozneje izkazalo, da je od U.S. Secret Service dobilo približno 1,5 milijona dolarjev in izdatno tehnično pomoč z namenom, da ustvari nacionalno zbirko s fotografijami prebivalstva (Sykes 1999, 60-61).

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).

Zakaj je torej pri zaščiti informacijske zasebnosti v ZDA prišlo do takšnih pomanjkljivosti? Odgovor leži v ostankih lastninskega koncipiranja pravice do zasebnosti ter v libertarni 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 poizkus ameriške države, da bi ustregla korporacijam, četudi so pri tem omejene pravice posameznikov (Kovačič 2006, 70).

5.2 PRAVICA DO 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. 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[94], saj je prvi zakon za zaščito informacijske zasebnosti na svetu, ki je bil sprejet leta 1970 v nemški zvezni državi Hesse, postavil enotna merila za javni in zasebni sektor (Kovačič 2006, 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 preglednosti in načrtovanju, vse skupaj pa veliko potrebo po zbiranju in analizi čedalje večjih količin podatkov. Zato so v sedemdesetih letih 20. stoletja v Evropi nastali

[94] Profesor James Whitman (v Solove 2009, 185) pravi, da je ameriško in evropsko razumevanje zasebnosti zelo različno, zato se tudi zakonodaja, ki ščiti pravico do zasebnosti, med obema kontinentoma razlikuje. Whitman trdi, da *»na obeh straneh Atlantika obstajata dve različni kulturi, ki imata tudi različno senzibilnost glede zasebnosti, posledično pa tudi različno zakonodajo. Ameriška zakonodaja za zaščito zasebnosti je utemeljena na vrednotah svobode (ang. liberty values), med tem ko je evropska zakonodaja utemeljena na pojmu dostojanstva«* (Whitman v Solove 2009, 185). Po tej razlagi naj bi Evropejci večjo skrb namenjali varovanju časti in dostojanstva, Američani pa svobodi posameznika pred nadzorom in poseganjem države. Whitman zaključi, da sta Warren in Brandeis skušala v ameriško pravo uvoziti kontinentalni način razumevanja zasebnosti, kar se je izkazalo kot neustrezna poteza, zato je tudi zasebnost v ZDA relativno slabo varovana.

načrti za centralizacijo, povezovanje in nastanek velikih zbirk podatkov. Take načrte so imeli že leta 1960 na Švedskem, pa tudi v nemški zvezni državi Hesse leta 1970 in na Bavarskem leta 1972. Zaradi negativnih izkušenj iz obdobja druge svetovne vojne je bil odpor proti tem načrtom razumljiv. Zakonodaja se je v začetku ukvarjala predvsem z računalniško obdelavo podatkov in zagotavljanjem točnosti zbranih podatkov. Problem ni bil posameznik in njegove pravice, temveč podatki in uporaba računalniške tehnologije (Kovačič 2006, 74).

Toda razvoj tehnologije se je obrnil v drugo smer. Leta 1963 je DEC[95] razvil prvi miniračunalnik PDP-1, ki je bil precej razširjen po univerzah, leta 1975 pa je nastal prvi poceni miniračunalnik Altair, ki so ga v ZDA prodajali v trgovinah na drobno, zaradi česar je postal široko dostopen (Delaney 1995).

Z razvojem mikroprocesorskih tehnologij uporaba velikih računalniških sistemov ni bila več ekonomsko upravičena. Nastanek množice majhnih, poceni, a zmogljivih računalnikov je 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-Schonberger 2001, 225).

Poleg tega so v drugi fazi razvoja informacijske zasebnosti v ospredje stopile pravice posameznika ali kot pravi Mayer Schonberger, »*zaščita podatkov kot poskus regulacije tehnologije se je spremenila v individualno svoboščino posameznikov*« (Mayer-Schonberger 2001, 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, posamezniki so morali biti obveščeni o namenu zbiranja, imeli so pravico zahtevati spremembo ali celo izbris netočnih podatkov. Hkrati so se pojavili tudi posebni pooblaščenci, katerih naloga je bila skrbeti za izvajanje te zakonodaje, informacijska zasebnost pa je postala ustavna kategorija v Avstriji, Španiji in na Portugalskem (Mayer-Schonberger 2001, 226-227).

Obenem je prišlo še do enega premika. V 60. in 70. letnih 20. stoletja je bila informacijska zasebnost problem večinoma znotraj nacionalnih držav. V 80. letnih in pozneje pa je zaradi razvoja in povečane dostopnosti tehnologije informacijska zasebnost postala izrazito mednarodni izziv (Bennett 2001, 103). Zato je Organizacija za ekonomsko sodelovanje in razvoj (OECD) 23. septembra 1980 sprejela Smernice za zaščito zasebnosti in čezmejni pretok osebnih podatkov. 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

[95] Ang. Digital Equipment Corporation.

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, 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 dosego 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, 411). Poleg tega konvencija daje posameznikom pravico do seznanitve z obstojem in vsebino osebnih podatkov, ki jih zadevajo, ob morebitnih napakah pa pravico zahtevati popravek ali izbris osebnih podatkov (Kovačič 2006, 76).

Vendar se s tem razvoj informacijske zasebnosti ni ustavil. Naslednji pomemben mejnik predstavlja razsodba nemškega ustavnega sodišča iz leta 1983, ki je izpostavila načelo informacijskega samoodločanja[96], sodišče pa je tudi poudarilo, da mora država pojasniti, zakaj potrebuje podatke in kakšne so posledice zavrnitve oddaje osebnih podatkov (Mayer-Schonberger 2001, 229).

Poleg tega se v zadnjem času predvsem na podlagi direktiv EU širijo tudi pristojnosti in pooblastila ter zagotavlja neodvisnost pooblaščencev 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 (Kovačič 2006, 76).

5.2.1 VPLIV DIREKTIV EU NA VARSTVO INFORMACIJSKE ZASEBNOSTI V EVROPI

Kljub temu, da Konvencija Sveta Evrope predstavlja prvi resnejši poizkus poenotenja nacionalnih standardov za zaščito informacijske zasebnosti, pa je v praksi naletela na nekaj težav. Ena večjih je

[96] Ang. information self-determination.

odsotnost definicije, kaj je ustrezna stopnja zaščite osebnih podatkov (Cate 1997, 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/EC140. 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, 77).

Pomen direktive je 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 prepovedati prostega pretoka osebnih podatkov med državami članicami zaradi razlogov«* zaščite zasebnosti (2. točka 1. člena direktive 95/46/EC140). 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 pa to delo opravljajo specializirane agencije, pooblaščenci ali posebni ombudsmani, 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 – ta organ 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 spremljanja tega področja (Kovačič 2006, 78).

5.2.2 IZNOS OSEBNIH PODATKOV IZ EVROPSKE UNIJE V ZDA

Ker bi omejitve pretoka osebnih podatkov, ki jih postavlja Direktiva, 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 in uprava za interni trg Evropske komisije. Tako overjena podjetja bi lahko prejemala osebne podatke iz Evropske unije (Laurant 2003, 17). Sporazum je bil kljub številnim kritikam julija 2000 sprejet, novembra istega leta pa so ameriškim podjetjem že začeli izdajati certifikate (Laurant 2003, 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, 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 zaostrilo z zahtevo ZDA po sporočanju podatkov o letalskih potnikih v ZDA, delno pa tudi z zahtevo ZDA po uvedbi biometričnih potnih listov (Kovačič 2006, 79).

5.2.3 KOMUNIKACIJSKA ZASEBNOST V EVROPI

8. člen Evropske konvencije o človekovih pravicah vsakomur priznava tajnost pisem in drugih občil, ki se razlagajo zelo široko, torej kot telefonske komunikacije, elektronska pošta, sporočila SMS, itd., saj oblika in vsebina sporazumevanja ni pomembna. 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, 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, 249). Pri vprašanju, ali so zaščitena 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 je sodišče 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 zaščitena tudi komunikacijska

sredstva, ki jih na delovnem mestu uporablja zaposleni (Kovačič 2006, 81).

Leta 1997 je bila v EU sprejeta Direktiva o zasebnosti telekomunikacij 97/66/EC, leta 2002 pa Direktiva o zasebnosti in elektronskih komunikacijah 2002/58/EC. Obe direktivi sta nekoliko bolj konkretizirali varstvo zasebnosti na področju telekomunikacij in elektronskih komunikacij.

Direktiva o zasebnosti in elektronskih komunikacijah 2002/58/EC določa, da komunikacij in z njimi povezanih prometnih podatkov ni dovoljeno shranjevati brez soglasja uporabnika, razen za potrebe prenosa ali upravljanja prometa ter zaračunavanja storitev. Izjema je shranjevanje komunikacij za potrebe dokazovanja komercialnih transakcij, pri čemer pa morajo biti uporabniki predhodno obveščeni o shranjevanju, namenu shranjevanja in trajanju hranjenja.

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, 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 pisanja 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, 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, 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, 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, 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, 85).

5.2.4 PRAVICA DO ZASEBNOSTI V EU NA DELOVNEM MESTU

Zasebnost na delovnem mestu je v razvitih evropskih državah precej bolje zaščitena kot v ZDA, saj načeloma velja obveznost delodajalca, da zaposlene vsaj obvesti o možnosti nadzora na delovnem mestu. Poleg tega je v primeru nadzora komunikacij dovoljen samo tisti nadzor, ki se nanaša na delo. Prav tako so delodajalci omejeni tudi pri zastavljanju osebnih vprašanj (Kovačič 2006, 85).

Evropsko sodišče za človekove pravice je leta 1999 obravnavalo dva primera odpusta homoseksualcev iz britanske vojne mornarice. Za Lustig-Preana je leta 1994 Royal Navy Special

Investigations Branch ugotovila, da je homoseksualec, zato so ga poklicali na zaslišanje. Tam je svojo spolno usmeritev priznal, zato je bil po nadaljnji preiskavi proti njemu leta 1995 odpuščen. Enako se je zgodilo Beckettu, ki je svojemu duhovniku priznal svojo spolno usmeritev, pozneje pa je bil o tem vprašanju poklican na zaslišanje k poveljniku. Sodišče je v primeru Lustig-Prean in Beckett proti Veliki Britaniji presodilo, da spraševanje delodajalca o spolni usmeritvi zaposlenega predstavlja poseg v zasebnost. Podobno sicer velja tudi v ZDA, vendar je Vrhovno sodišče ZDA v primeru Able proti Združenim državam leta 1998, ko je posameznik na svojem delovnem mestu sam izjavil, da je homoseksualec, in so ga zato odpustili, menilo, da je vojska ravnala zakonito. Ameriško vrhovno sodišče je obrazložilo, da je »*bistvo vojaške službe podrejanje želja in interesov posameznikov potrebam vojske«*, prepoved homoseksualnosti pa ni sporna, ker »pospešuje kohezivnost enote, povečuje zasebnost in zmanjšuje seksualne napetosti« (Turkington in Allen v Kovačič 2006, 86). S tem so zavzeli skoraj povsem nasprotno stališče kot ESČP.

V Evropi so sodišča, kar zadeva zasebnost komunikacij na delovnem mestu, bolj naklonjena zaposlenim kot v ZDA (Klemenčič 2003, 137). V zvezi z nadzorom na delovnem mestu sta verjetno najpomembnejši odločitvi Evropskega sodišča za človekove pravice Halford proti Veliki Britaniji iz leta 1997 v zvezi s kršitvijo 8. člena EKČP ter odločitev Kasacijskega sodišča Francije v primeru Societe Nikon France, SA proti Onof iz leta 2001. V primeru Halford proti Veliki Britaniji, kjer je policija nadzorovala službeni telefon svoje uslužbenke, je ESČP izrecno zapisalo, da zaposleni na delovnem mestu upravičeno pričakuje zasebnost.

Odločitev francoskega Kasacijskega sodišča v primeru Societe Nikon France, SA v. Onof, št. 99-42.942 z dne 2.10.2001 pa izrecno pravi, da »*delodajalec, ki bere sporočila, ki jih zaposleni pošilja ali sprejema prek 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, na katerih bi delodajalci arbitrarno in brez omejitev izvajali svoje diskrecijske pravice; ne smejo postati okolja totalnega nadzora, v katerih 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, 402).

Klemenčič ugotavlja, da »*se domet pravice do komunikacijske zasebnosti ne ustavi zgolj pri zagotavljanju zaupnosti vsebine sporočanja in podatkov, povezanih z njo, ampak hkrati prepoveduje tudi nesorazmerne prepovedi komuniciranja z zunanjim svetom«* (Klemenčič 2002, 395). Priporočilo Sveta Evrope št. R (89) 2175 namreč določa, da imajo zaposleni na delovnem mestu pravico do vzpostavljanja osebnih in socialnih stikov. Podobnega mnenja je bilo tudi Evropsko sodišče za človekove pravice v primeru Niemietz proti Nemčiji leta 1992, ko je zapisalo, da

»*spoštovanje zasebnega življenja mora vsebovati tudi določeno stopnjo pravice do vzpostavljanja in razvijanja odnosov z drugimi človeškimi bitji«.*

5.3 PRAVICA DO ZASEBNOSTI V REPUBLIKI SLOVENIJI

Zasebnost je v Republiki Sloveniji pravno zavarovana z ustavo, ki v 35. členu zagotavlja varstvo pravic zasebnosti in osebnostnih pravic, v 37. členu varstvo tajnosti pisem in drugih občil, v 38. členu pa varstvo osebnih podatkov. S tem so postavljeni temelji varovanja prostorske, komunikacijske in informacijske zasebnosti, ki je bolj natančno opredeljena in zavarovana s posameznimi zakoni in sodno prakso. Pravico do zasebnosti v Sloveniji namreč varuje kazensko in civilno pravo. Kazenskopravno varstvo zagotavljajo določbe iz šestnajstega in osemnajstega poglavja kazenskega zakonika, ki navajajo več kaznivih dejanj inkriminacije pravice do zasebnosti. Civilnopravno varstvo pa vključuje ugotovitveno tožbo na podlagi Zakona o pravdnem postopku, zahtevek za prenehanje s kršitvami pravice osebnosti in zahtevek za povrnitev negmotne škode na podlagi obligacijskega zakonika (Cvetko 1999, 27).

K razvoju pravice do zasebnosti v slovenskem pravu je pomembno prispevala sodna praksa Ustavnega in Vrhovnega sodišča. Ustavno sodišče je v prvem precedenčnem primeru (Odl. US. Up-32/94), t.i. »posestnem sporu«, prvič opredelilo »človekovo zasebnost«, ki jo sicer zagotavlja 35. člen ustave, kot *»v območju človekovega bivanja bolj ali manj sklenjeno celoto človekovega ravnanja in ukvarjanja, občutij in razmerij, za katero je značilno in konstitutivno, da si jo človek oblikuje in vzdržuje sam ali sam z najbližjimi, s katerimi je v intimni skupnosti, na primer z življenjskim partnerjem, in da v njej biva z občutkom varnosti pred vdorom javnosti ali kogarkoli nezaželenega«* (Odl. US. št. Up-32/94). V drugem precedenčnem primeru (OdlUS št. U-I-25/95 in OdlUS VI/2) pa je Ustavno sodišče pri obravnavanju vprašanja kršitve zasebnosti uporabilo presojo Evropskega sodišča za človekove pravice, ki zasebnost razume kot široko negativno pravico varstva posameznika pred posegi države in tretjih oseb v njegovo zasebno sfero, osebnost in dostojanstvo. Kasneje je Vrhovno sodišče v t.i. primeru »prostozidarske lože« (Sodba VS RS II Ips 460/97) zapisalo, da zasebnost ne obsega le *»ozkega notranjega kroga posameznika in družine«* in s tem – podobno kot Evropsko sodišče za človekove pravice - začrtalo široko razumevanje koncepta zasebnosti. Iz domače zakonodaje in sodne prakse je torej razvidno, da je Slovenija pri razumevanju in varovanju pravice do zasebnosti ubrala podobno pot kot ostale razvite evropske države.

5.3.1 KOMUNIKACIJSKA ZASEBNOST V SLOVENIJI

Temelje komunikacijske zasebnosti v Sloveniji opredeljuje 37. člen ustave, ki zagotavlja tajnost pisem in drugih občil. Pri tem je v skladu z domačo pravno prakso potrebno občila razumeti zelo široko, saj ne gre le za telefonske komunikacije in elektronsko pošto, ampak tudi za komunikacijo, ki poteka prek spletnih socialnih omrežji, forumov in drugih oblik. Pravica do komunikacijske zasebnosti je varovana tudi takrat, ko se za prenos sporočila ne uporablja javno telekomunikacijsko omrežje, ampak zaseben ali celo zaprt telekomunikacijski sistem (Šturm in drugi 2002, 395). Široko razumevanje varstva komunikacijske zasebnosti je razvidno iz razsodbe Upravnega sodišča U 702/99 z dne 21. 3. 2000, kjer je Upravno sodišče zavzelo stališče, da se varstvo zasebnosti, ki ga zagotavlja 37. člen ustave, nanaša tudi na službene telefone, pridobitev in uporaba izpiskov telefonskih klicev službenega telefona s strani delodajalca pa predstavlja kršitev. V nasprotju z ZDA, kjer je zasebnost na delovnem mestu slabo varovana, veljajo v EU (in s tem tudi v Sloveniji) strožja pravila (glej odločitev Evropskega sodišča za človekove pravice *Halford proti Združenemu kraljestvu* iz leta 1997 in odločitev Kasacijskega sodišča Francije št. 99-42.042 z dne 2. 10. 2001).
Razen vsebine komunikacije so varovani tudi t.i. prometni podatki, ki predstavljajo sestavni del komunikacije (Šturm in drugi 2002, 396). To pomeni, da se določbe o varovanju komunikacijske zasebnosti nanašajo tudi na izpiske o telefonskih številkah, podatke o dolžini komunikacije in količini prenesenih podatkov (Kovačič 2003, 80). Ob tem Klemenčič (v Šturm in drugi 2002, 395) ugotavlja, da *»se domet pravice do komunikacijske zasebnosti ne ustavi zgolj pri zagotavljanju zaupnosti vsebine sporočanja in podatkov povezanih z njo, ampak hkrati prepoveduje tudi nesorazmerne prepovedi komuniciranja z zunanjim svetom«*.

Pravica do komunikacijske zasebnosti je v Sloveniji kazenskopravno zavarovana. Zakonit poseg v zasebnost komunikacij je zato mogoč izključno[97] na podlagi odredbe sodišča, če je to potrebno zaradi uvedbe ali poteka kazenskega postopka ali zaradi varnosti države, v Sloveniji pa ga na podlagi Zakona o kazenskem postopku in Zakona o Slovenski obveščevalno-varnostni agenciji izvajata policija in Sova (Kovačič 2003, 92). Ob tem velja dodati, da je Zakon o SOVI, ki pod določenimi pogoji omogoča Slovenski obveščevalno-varnostni agenciji poseganje v pravico do zasebnosti, problematičen v 21. in 24. členu. 21. člen omogoča SOVI *»spremljanje mednarodnih*

[97] Izjema je problematičen 21. člen Zakona o SOVI (ZSOVA).

sistemov zvez« (oziroma z drugimi besedami prisluškovanje, kar nedvomno predstavlja poseganje v človekove pravice) brez odredbe sodišča, saj zadostuje le podpis direktorja obveščevalne službe. 24. člen pa predvideva možnost nadzora pisem in nadzorovanja ter snemanja telekomunikacij v Sloveniji tudi v primeru, če obstaja nevarnost za varnost države, ki se lahko kaže *»v tajnih aktivnostih ... zoper strateške interese Republike Slovenije«*. Pri tem Kovačič (2003, 84) opozarja, da je »strateške interese« mogoče opredeliti bolj ohlapno, kar bi lahko imelo za posledico, da SOVA lažje pride do zakonitega sodnega naloga za prestrezanje komunikacij, s tem pa je tudi možnost morebitnih zlorab večja. Je pa z vidika varovanja zasebnosti bolj spodbudna novela Zakona o kazenskem postopku, ki natančno določa pogoje pod katerimi lahko policija poseže v pravico do zasebnosti. Novela (ZKP-J) je bila 2. oktobra 2009 objavljena v Uradnem listu RS in predstavlja bistveno posodobitev Zakona o kazenskem postopku in modernizacijo slovenskega pravnega reda na področju informacijskega prava.

5.3.2 INFORMACIJSKA ZASEBNOST V SLOVENIJI

Varstvo osebnih podatkov na najbolj splošni ravni zagotavlja 38. člen ustave, ki prav tako prepoveduje uporabo osebnih podatkov v nasprotju z namenom njihovega zbiranja, vsakomur zagotavlja pravico do seznanitve z zbranimi osebnimi podatki, ki se nanašajo nanj, in pravico do sodnega varstva ob njihovi zlorabi. Sicer pa varstvo osebnih podatkov zagotavljajo tudi sistemski in področni zakoni. V skladu s tem t.i. »obdelovalnim modelom« je na področju obdelave osebnih podatkov prepovedano vse, razen tistega, kar je z zakonom izrecno dovoljeno. Posegi v ustavno varovano človekovo pravico do varstva osebnih podatkov so dopustni le v zakonsko določenih primerih, ob tem pa mora biti jasno določen namen obdelave osebnih podatkov, prav tako pa mora biti zagotovljeno ustrezno varstvo osebnih podatkov (Informacijski pooblaščenec 2008, 21).

Informacijska zasebnost (varstvo osebnih podatkov) je kazenskopravno zavarovana. Kazenski zakonik namreč prepoveduje zlorabo osebnih podatkov in sicer za vsakogar, ki uporabi osebne podatke v nasprotju z zakonom, in za vsakogar, ki vdre v računalniško vodeno zbirko podatkov z namenom, da bi zase ali za koga drugega pridobil kakšen osebni podatek (Kovačič 2003, 84).
Varovanje osebnih podatkov pa najbolj celovito urejata Zakon o varstvu osebnih podatkov (ZVOP-

1) in Zakon o telekomunikacijah (ZEKom). Zakon o varstvu osebnih podatkov je Državni zbor sprejel 15. 7. 2004, veljati je pričel s 1. 1. 2005. Sprejetje tega zakona je bilo potrebno predvsem zaradi vstopa Slovenije v EU in s tem povezanega usklajevanja varstva osebnih podatkov z določbami Direktive 95/46/ES Evropskega parlamenta in Sveta o zaščiti posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov. Julija 2007 je bila sprejeta novela ZVOP-1, ki je prinesla dve pomembni novosti s področja administrativnih razbremenitev upravljavcev osebnih podatkov in predpisovanja določenih olajšav za posameznike, na katere se osebni podatki nanašajo (Informacijski pooblaščenec 2008, 22). Ob tem velja dodati, da ZVOP-1 ni le sistemski zakon, ampak je v svojem šestem delu tudi t.i. področni zakon, ki s precej natančno določitvijo pravic, obveznosti, načel in ukrepov, upravljavcem osebnih podatkov daje neposredno zakonsko podlago za obdelavo osebnih podatkov na področju neposrednega trženja, videonadzora, biometrije, evidentiranja vstopov v prostore in izstopov iz njih ter strokovnega nadzora (Informacijski pooblaščenec 2008, 21). Zelo pomemben je 8. člen Zakona o varstvu osebnih podatkov, ki določa, da se smejo osebni podatki zbirati, shranjevati in obdelovati samo, če je tako določeno z zakonom ali če je za obdelavo določenih osebnih podatkov podana osebna privolitev posameznika. Osebe o katerih se zbirajo osebni podatki, morajo biti predhodno seznanjene z namenom zbiranja, osebni podatki pa se smejo zbirati samo za ta namen. Osebni podatki se lahko načeloma shranjujejo in uporabljajo samo toliko časa, kolikor je potrebno za dosego tega namena, nato pa jih je treba izbrisati ali blokirati.

Sicer pa se pri obdelavi osebnih podatkov v Sloveniji uporabljajo tudi določbe Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov. Konvencija je bila ratificirana in objavljena leta 1994, njen namen pa je na ozemlju vsake pogodbenice vsakemu posamezniku, ne glede na njegovo državljanstvo in prebivališče, zagotoviti spoštovanje njegovih pravic in temeljnih svoboščin in v okviru tega še posebej spoštovanje pravice do zasebnosti v primeru avtomatske obdelave njegovih osebnih podatkov (Informacijski pooblaščenec 2008, 21). Najpomembnejši mednarodni standard glede zagotavljanja varstva osebnih podatkov in zasebnosti pa predstavljata dva predpisa Evropske Unije: Direktiva 95/46/EC o varstvu posameznikov pri obdelovanju osebnih podatkov in prostem gibanju takšnih podatkov in Direktiva 97/66/EC o obdelavi osebnih podatkov in varstvu zasebnosti v telekomunikacijskem sektorju (Klemenčič 2003, 128).

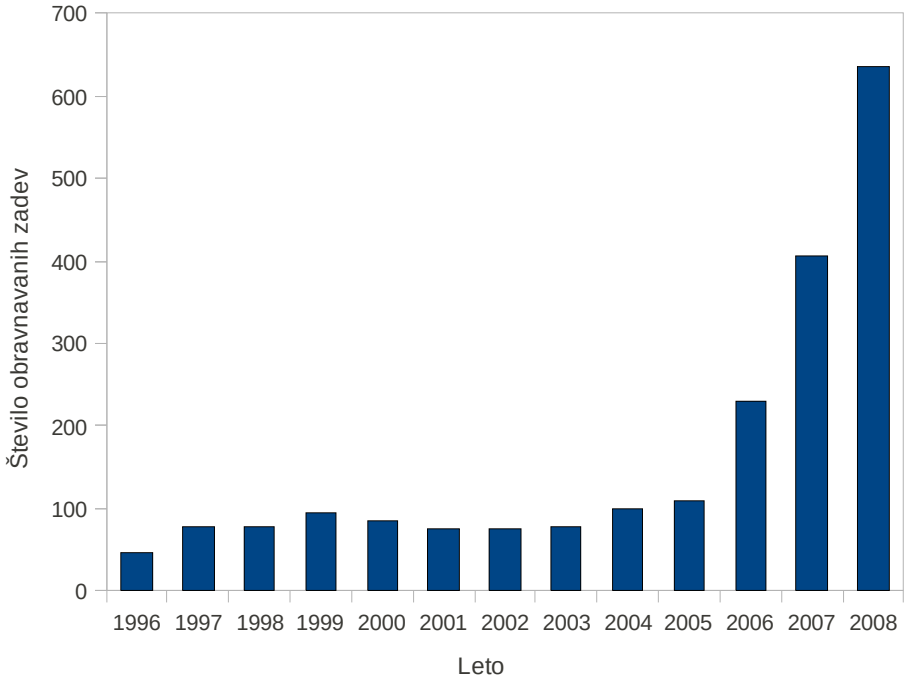
Za urejanje pravice do informacijske zasebnosti oziroma varstva osebnih podatkov je prav tako pomemben Zakon o elektronskih komunikacijah (ZEKom). V 2. členu je zapisano, da je ta zakon namenjen varstvu pravic posameznikov, kar je razvidno iz desetega poglavja, ki je v celoti

posvečeno zaščiti tajnosti in zaupnosti elektronskih komunikacij. Zakon o elektronskih komunikacijah je pomemben zato, ker zagotavlja varnost vsebine sporočila, prometnih podatkov in identifikacije udeležencev. Zakon omejuje tudi obseg informacij, ki so povezane s komunikacijo in ki jih lahko operater omrežja zbira, shranjuje ali obdeluje, predvsem pa omejuje posredovanje teh informacij tretjim osebam (Klemenčič 2003, 122). Prav tako Zakon o elektronskih komunikacijah od operaterjev omrežij zahteva določene varnostne ukrepe za zaščito podatkov pred vdori tretjih nepovabljenih oseb in obenem postavlja osnovna pravila o posegu pooblaščenih državnih organov v pravico do tajnosti občil. Pri tem državnim organom pod določenimi pogoji dovoljuje vpogled v identifikacijske in prometne podatke kot tudi nadzor elektronskih komunikacij v realnem času. Od operaterjev zahteva zagotovitev in namestitev ustrezne programske opreme za zagotovitev nadzora telekomunikacijskega prometa (Klemenčič 2003, 123). Ob tem velja dodati, da je Državni zbor 18. decembra 2009 sprejel novelo Zakona o elektronskih komunikacijah, ki prinaša nekaj sprememb. Najpomembnejša je skrajšan rok za obvezno hrambo prometnih podatkov. Direktiva o obvezni hrambi prometnih podatkov 2006/24/ES, ki jo je v Zakonu o elektronskih komunikacijah sprejela tudi Slovenija, namreč zahteva obvezno hrambo prometnih podatkov telefonskih in internetnih komunikacij ter podatkov o lokacijah mobilnih telefonov, za čas hrambe pa določa od 6 do 24 mesecev. Slovenija je v Zakonu o elektronskih komunikacijah najprej uveljavila obvezno hrambo prometnih podatkov za maksimalno obdobje dveh let. V skladu z novelo pa se je čas hrambe prometnih podatkov na področju telefonije skrajšal na 14 mesecev, hramba internetnih prometnih podatkov pa na 8 mesecev.

5.3.3 DINAMIKA NADZORA IN ZASEBNOSTI V SLOVENIJI

Na trende s področja varovanja zasebnosti je mogoče posredno sklepati tudi iz nekaterih statističnih podatkov. Tako podatki iz poročila Informacijskega pooblaščenca in iz poročila Varuha človekovih pravic kažejo, da se število zadev s področja kršitev pravice do informacijske zasebnosti (varstva osebnih podatkov) iz leta v leto povečuje. To lahko pomeni, da družbeni nadzor čedalje bolj vdira v pravno zavarovano sfero zasebnosti, prav tako pa lahko pomeni, da je področje zasebnosti bolje zavarovano in da se ljudje pomena pravice do zasebnosti vedno bolj zavedajo, zato so jo tudi pripravljeni bolj intenzivno varovati.

Slika 5.4: Število obravnavanih zadev s področja varovanja osebnih podatkov pri Informacijskem pooblaščencu



Podatki iz Letnega poročila Informacijskega pooblaščenca za leto 2008 kažejo relativno stabilen trend naraščanja domnevnih kršitev določb Zakona o varstvu osebnih podatkov. Gibanje števila kršitev je v obdobju med leti 1996 in 2005 relativno stabilno, leta 2006, 2007 in 2008 pa je opazen izjemno velik porast prijav kršitev določb Zakona o varstvu osebnih podatkov (glej sliko 5.4).

Pri interpretaciji podatkov je potrebno upoštevati nekaj pomembnih okoliščin. Inšpekcijsko nadzorstvo nad izvajanjem določb Zakona o varstvu osebnih podatkov se v Republiki Sloveniji opravlja od leta 1992 naprej. Do konca leta 1994 je inšpekcijsko nadzorstvo opravljalo Ministrstvo za znanost in tehnologijo, od leta 1995 naprej pa je to področje prišlo v pristojnost Ministrstva za pravosodje. 24. 7. 2001 je stopil v veljavo noveliran Zakon o varstvu osebnih podatkov, ki je precej spremenil dotedanjo organizacijo nadzora nad izvajanjem določb zakona. Do uveljavitve navedene novele je inšpekcijsko nadzorstvo nad izvajanjem določb zakona opravljal en inšpektor, ki je deloval kot samostojni izvajalec v okviru Ministrstva za pravosodje, z navedeno novelo zakona pa sta bili za opravljanje nadzora nad izvajanjem določb zakona določeni dve instituciji in sicer Inšpektorat za varstvo osebnih podatkov, ki je bil ustanovljen septembra 2001 kot organ v sestavi Ministrstva za pravosodje, in Varuh človekovih pravic, ki je za opravljanje nalog neodvisnega nadzora varstva osebnih podatkov določil svojega namestnika (Informacijski pooblaščenec 2010).

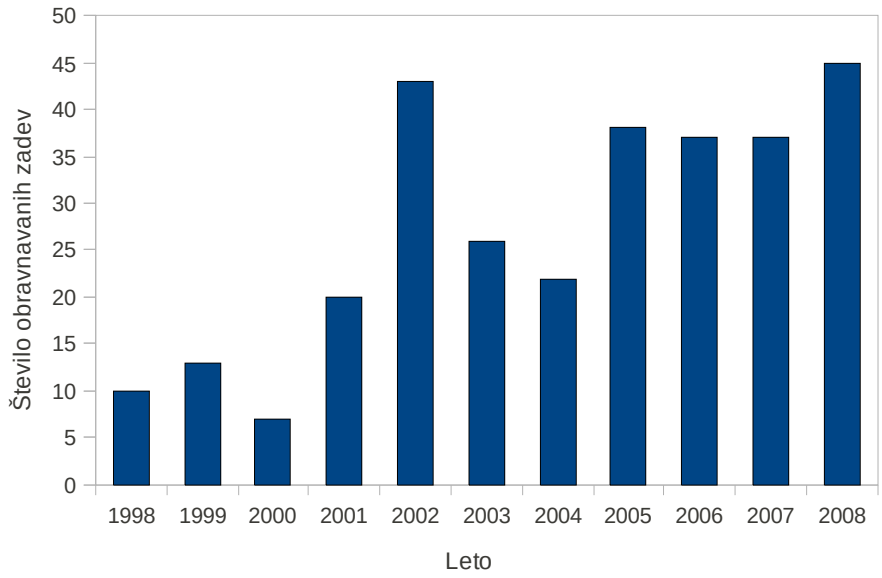
Inšpektorat za varstvo osebnih podatkov je nadzor in druge naloge s področja varstva osebnih podatkov opravljal do 31. 12. 2005, ko je bil ustanovljen Informacijski pooblaščenec, Varuh človekovih pravic pa je neodvisni nadzor na področju varstva osebnih podatkov opravljal do 1. 1. 2005, ko je stopil v veljavo novi Zakon o varstvu osebnih podatkov, za tem pa je po določbah 59. in

60. člena ZVOP-1 pričel opravljati svoje naloge na področju varstva osebnih podatkov v skladu z zakonom, ki ureja varuha človekovih pravic (Informacijski pooblaščenec 2010).

Naraščajoči trend v letih 2006, 2007 in 2008 je torej v veliki meri posledica sprememb zakonodaje in nadzornih institucij s področja varstva osebnih podatkov. Informacijski pooblaščenec, ki je bil ustanovljen 31. 12. 2005, je združil delo dveh organov (Pooblaščenca za dostop do informacij javnega značaja in Inšpektorat za varstvo osebnih podatkov) in s tem bistveno razširil svoje področje dela. Zato podatki za leto 2006, 2007 in 2008 ne prikazujejo le števila prijetih prijav domnevnih kršitev Zakona o varstvu osebnih podatkov, ampak tudi število inšpekcijskih postopkov, ki jih je Informacijski pooblaščenec uvedel po uradni dolžnosti. Kljub temu je število prijetih prijav iz leta v leto močno naraščalo, saj je bilo leta 2005 podanih 91 prijav, leta 2006 231, leta 2007 336 in leta 2008 502 prijav (Informacijski pooblaščenec 2010).

Ena od mogočih interpretacij bi bila, da se je v zadnjih letih izrazito povečalo število posegov na področju informacijske zasebnosti (varstva osebnih podatkov). Vendar pa je bolj verjetno, da se samo število posegov ni bistveno povečalo, se je pa uredila zakonodaja s področja varovanja osebnih podatkov, ki bolj natančno določa kaj predstavlja kršitev in kaj ne, prav tako pa se je – delno tudi zaradi učinkovitega in medijsko odmevnega dela Informacijskega pooblaščenca – povečalo zavedanje javnosti o problematiki nadzora in kršitev s področja varstva osebnih podatkov, zato se je tudi povečalo število prijav domnevnih kršitev Zakona o varstvu osebnih podatkov.

Slika 5.5: Število obravnavanih zadev s področja varstva osebnih podatkov pri Varuhu človekovih pravic



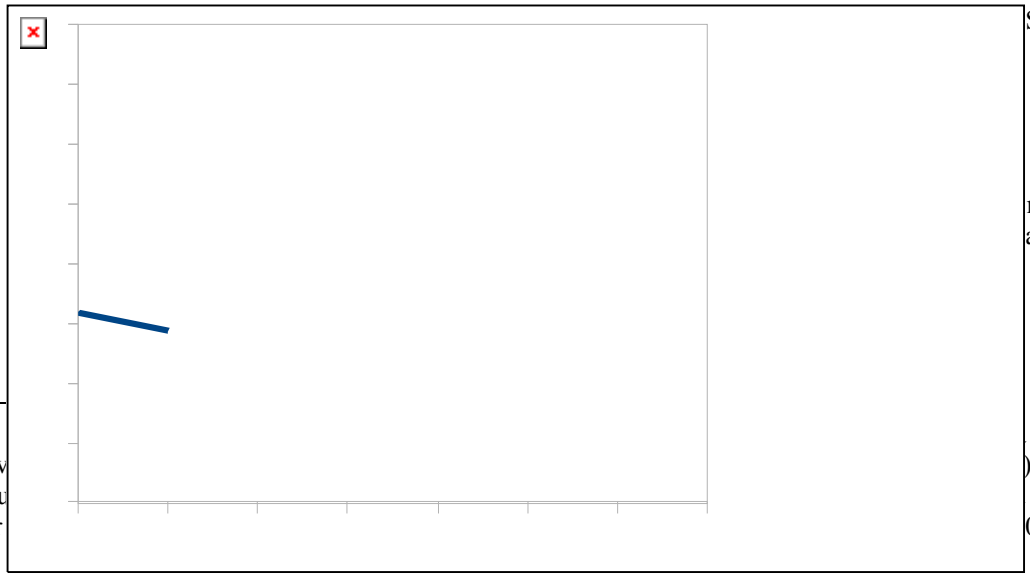
Podatki iz letnih poročil Varuha človekovih pravic kažejo nekoliko nenavadno gibanje števila prijav s področja domnevnih kršitev Zakona o varstvu osebnih podatkov (glej sliko 5.5). V zadnjem

desetletju se število kršitev pravice do informacijske zasebnosti nedvomno povečuje. Vendar pa izstopa izrazito velik porast prijavljenih kršitev v letu 2002. To izstopanje je mogoče pojasniti s spremembami zakonodaje s področja varstva osebnih podatkov. 24. 7. 2001 je namreč stopil v veljavo noveliran Zakon o varstvu osebnih podatkov, ki je za opravljanje nadzora nad izvajanjem določb zakona določil dve instituciji. Ena je bila Inšpektorat za varstvo osebnih podatkov, druga pa Varuh človekovih pravic. Vendar pa ta razširjena pristojnost Varuha ne pojasni, zakaj je v naslednjih dveh letih število prijavljenih kršitev določb Zakona o varstvu osebnih podatkov opazno upadlo. 1. 1. 2006 je stopil v veljavo nov Zakon o varstvu osebnih podatkov, Varuh človekovih pravic pa je pričel svoje naloge na področju varstva osebnih podatkov opravljati v skladu z zakonom, ki ureja varuha človekovih pravic. Po eni strani je mogoče trende pojasniti s spremembami zakonodaje, ki čedalje bolj natančno ureja področje varstva osebnih podatkov, po drugi strani pa se med državljani krepi tudi zavedanje o problematiki zasebnosti.

Tabela 5.1: Numerični pregled nekaterih policijskih ukrepov nadzorovanja

Leto	1998	1999	2000	2001	2002	2003	2004	2005
Policijski nadzor[98]								
Število nadzorovanih telekomunikacijskih sredstev	318	287	318	453	505	472	677	746
Število oseb, ki jim je policija nadzorovala telekomunikacije	176	163	151	199	222	168	167	198

Vir: Kovačič (2006, 202).



Slika 5.6: Grafični pregled nekaterih policijskih ukrepov nadzorovanja

Nedvomn

[98] Podatki je podatke posredov). Gre za vsa telekomu elektronske pošte ter 006, 202).

o so zanimivi podatki o ukrepih nadzora, ki jih je med leti 1998 in 2005 izvedla policija (glej tabelo 5.1 in sliko 5.6). Podatki jasno kažejo, da se število nadzorovanih telekomunikacijskih sredstev iz leta v leto povečuje, hkrati pa število nadzorovanih oseb ostaja podobno. Iz tega je z določenim pridržkom mogoče sklepati, da se interes države za izvajanje nadzora še ne povečuje, saj bi bilo v tem primeru število nadzorovanih oseb iz leta v leto večje. Seveda pa čedalje večje število nadzorovanih telekomunikacijskih naprav potrjuje domnevo, da je sodobni informacijski nadzor tako rekoč vgrajen v elektronske naprave, zato mreža informacijskega panoptikona postaja čedalje bolj gosta in vseprežemajoča. Posameznik je kljub čedalje bolj natančni pravni regulaciji zasebnosti iz leta v leto bolj izpostavljen informacijskemu nadzoru, ki za večino ljudi že postaja sprejemljiv sestavni del vsakdanjega življenja.

5.4 RAZMERJE MED NADZOROM IN ZASEBNOSTJO

Od sedemdesetih let 20. stoletja dalje se zaradi hitrega razvoja informacijske tehnologije formalni družbeni nadzor krepi in posega na številna področja posameznikovega vsakdanjega življenja, ki so bila v preteklosti podvržena kvečjemu neformalnemu nadzoru. Širjenje sistematičnega informacijskega nadzora ni toliko posledica povečanega interesa države za izvajanje nadzora – tak interes je bil v večji ali manjši meri vselej prisoten. Gre bolj za to, da je informacijska tehnologija dvignila nadzor na novo raven, ga pocenila in avtomatizirala, hkrati pa se je k uporabi nadzora zatekel tudi privatni sektor. Navaden državljan je postal z vsako elektronsko napravo tako rekoč podvržen novemu pogledu virtualnega nadzornikovega očesa v nastajajočem digitalnem »superpanoptikonu«. Ker so se elektronske naprave, ki nas obdajajo, v zadnjih letih zelo namnožile, je čedalje bolj zgoščen in celovit tudi nadzor. Tak množični nadzor, ki deluje na podlagi »elektronskih sledi«, ki jih posamezniki puščajo za seboj vsakič, ko uporabijo neko v omrežje povezano napravo, čedalje bolj spodbuja in razvija tudi privatni sektor. »Prednost« privatnega sektorja je v tem, da ga ljudje ne dojemajo kot tradicionalnega sovražnika človekovih pravic, zato na tak nadzor pristajajo tako rekoč prostovoljno oziroma v zameno za zelo majhne ugodnosti. Ob tem vse več ljudi »prostovoljni« nadzor sploh ne dojema več kot nadzor, ampak kot neizbežen in sestavni del vsakdanjega življenja. Uporabniki raznih komercialnih storitev se večinoma ne zavedajo dovolj dobro, da podatki, ki jih podjetja pridobijo na ta način, nemalokrat služijo tudi državi in njenim represivnim aparatom. Zato nadzor, ki ga izvaja privatni sektor, postaja nekakšna nevidna podaljšana roka državne oblasti.

Vendar pa se je kot odziv na trende krčenja zasebnosti bistveno okrepila tudi pravna regulacija pravice do zasebnosti. Analiza instrumentov pravnega varstva jasno kaže, da je pravica do zasebnosti danes bistveno bolj zavarovana kot je bila v času kodifikacije v mednarodne in nacionalne pravne dokumente. Kljub temu ima pravo svoje omejitve, ki v marsičem slabijo zmožnost učinkovite regulacije pravice do zasebnosti. Po eni strani pravo predstavlja »gašenje požara«, vzpostavi se namreč šele z zamikom, ko je neka tehnologija nadzora že posegla na področje zasebnosti. Zato razvoj prava skoraj vedno zaostaja za razvojem informacijskega nadzora. Po drugi strani pravo regulira predvsem nadzor s strani države, ki predstavlja tradicionalnega nasprotnika človekovih pravic in svoboščin. Privatni sektor pa je v precej manjši meri podvržen regulaciji nadzora, še posebej v ZDA. Prav tako se ljudje precejšnjemu delu zasebnosti odpovedujejo prostovoljno, npr. z objavljanjem osebnih podatkov ali intimnih informacij na raznih spletnih forumih, straneh za socialno mreženje in blogih – v teh primerih je pravna regulacija bistveno oslabljena, saj posameznik prostovoljno pristane na posege v zasebnost. Razen tega se je v zadnjem desetletju pojavila nova grožnja zasebnosti in sicer strah pred terorizmom, ki je postal »epidemičen« z napadom na WTC 11. septembra 2001. Terorizem se uporablja kot opravičilo za povečevanje formalnega nadzora, ob tem pa je velik poudarek namenjen pospešeni izmenjavi osebnih podatkov med privatnim in javnim sektorjem.

Povzeti je mogoče, da je pravno varstvo zasebnosti v zadnjih desetletjih doživelo evolucijo, kar pomeni, da je pravica do zasebnosti bolj natančno in tudi bolje varovana kot kadarkoli prej. Po drugi strani pa je tehnologija nadzora v navezavi s strateškimi in komercialnimi interesi bistveno skrčila sfero zasebnosti, zato je ta kljub natančni pravni regulaciji manjša kot je bila kadarkoli v zadnjih treh stoletjih.

6 SKLEP

Raziskovanja problematike množičnega nadzora sem se lotil z dvema eksplicitnima predpostavkama. Domneval sem, da se je družbeni nadzor v zadnjih desetletjih okrepil, sfera zasebnosti pa se je posledično skrčila. Prav tako sem domneval, da pravno varstvo zasebnosti v Republiki Sloveniji ni učinkovito. Obe predpostavki sem v magistrskem delu uporabil kot hipotezi.

1. hipoteza: družbeni nadzor se je v zadnjih desetletjih okrepil, sfera zasebnosti pa se je skrčila

Domači in tuji strokovnjaki, ki v svojih teoretičnih delih obravnavajo problematiko nadzora, se večinoma strinjajo, da je 20. stoletje zaznamovala krepitev družbenega nadzora. K temu je največ pripomogel prav razvoj komunikacijske in informacijske tehnologije. Že konec 19. stoletja sta ameriška pravnika Warren in Brandeis opozarjala na nevarnost rumenega tiska in fotografije za posameznikovo zasebnost. V drugi svetovni vojni se je ta strah izkazal za upravičenega, saj je bila informacijska tehnologija uporabljena kot sredstvo notranjega nadzora, ki ga je s pridom uporabljal zlasti nacizem pri sistematičnem iztrebljanju Judov. Ne preseneča, da je pravica do zasebnosti postala sestavni del Splošne deklaracije o človekovih pravicah. Toda prava revolucija na področju informacijskega nadzora se je zgodila šele v sedemdesetih in osemdesetih letih 20. stoletja – zasluga gre predvsem razvoju osebnega računalnika in interneta, ki predstavljata temeljni gradnik

sodobnega nadzora. Posamezniki pri uporabi elektronskih naprav za seboj puščajo »elektronske sledi«, ki jih različnih sistemi nadzora prek omrežji zbirajo in pretvarjajo v koristne informacije. Čeprav so bili ljudje skozi vso zgodovino podvrženi bolj ali manj intenzivnim oblikam neformalnega nadzora, pa je šele z razvojem telefona, računalnika in interneta formalni nadzor zasedel osrednje mesto. V primerjavi z neformalnim nadzorom je mnogo bolj nevaren, saj poteka načrtno in sistematično. Razen tega ima sodobni informacijski nadzor še dve značilnosti: je (tudi) množičen, kar pomeni, da se ne ukvarja zgolj z določenim številom posameznikov, pač pa s celotno populacijo, prav tako pa je tudi integriran v sodobno tehnologijo, zato je samodejen in tako rekoč »zlit z okoljem«. V preteklosti je moral posameznik, če je želel, da postane tarča formalnega nadzora, nekako izzvati pozornost države. Danes to ni več potrebno, saj je tak nadzor vseprisoten in samodejen. Izvaja se povsod kjer so omrežja in elektronske naprave. Formalni nadzor se je v zadnjih desetletjih torej dejansko okrepil, vendar ne zaradi povečanega zanimanja države za nadzorovanje, ampak zaradi razvoja informacijske tehnologije, ki je arhitekturo panoptičnega stroja vtkala v tkivo celotne družbe. Razen tega je svoje prispeval še komercialni sektor, ki je v nadzoru našel učinkovito in relativno poceni orodje za regulacijo vedenja potrošnikov in v končni instanci za večanje profita.

Drugo vprašanje pa je ali se je sfera zasebnosti skrčila. Na prvi pogled se zdi smiselno, da krepitev nadzora vodi h krčenju zasebnosti. Vendar pregled evropske in ameriške zakonodaje kaže drugačno sliko, saj je pravica do zasebnosti v zadnjih desetletjih postala bistveno bolj normirana in pravno zavarovana kot kadarkoli v preteklosti. Po eni strani se torej nadzor krepi, po drugi strani pa je sfera zasebnosti čedalje bolj pravno opredeljena in zavarovana. Toda to je zgolj navidezno protislovje.
Sfera zasebnosti se je v zadnjih sto letih nedvomno skrčila. K temu je največ pripomogla informacijska tehnologija, ki je posameznikovo zasebnosti čedalje bolj izpostavljala tako javnosti kot tudi različnim akterjem nadzora – med njimi je osrednje mesto najprej zasedala država, zdaj pa čedalje bolj stopa v ospredje komercialni sektor, ki se ukvarja predvsem z nadzorom potrošnikov. Zaradi grožnje informacijskega nadzora se je začelo razvijati pravno varstvo zasebne sfere – v času, ko te nevarnosti še ni bilo, pravica do zasebnosti sploh ni bila formalno pravno priznana. Zasebnost se je po eni strani torej krčila, po drugi strani pa je tisto, kar je sploh še ostalo zasebno, čedalje bolj postajalo predmet pravne regulacije in zaščite. Zasebnosti je danes manj, vendar je ta »preostanek« bistveno bolj pravno zaščiten kot je bil kadarkoli prej, ko grožnja informacijskega nadzora še ni bila prisotna.

Hipoteza 1 je s tem potrjena. Družbeni nadzor se je v zadnjih letih okrepil, sfera zasebnosti pa se

je skrčila. Vendar pa je tisti del zasebnosti, ki je še ostal, danes bistveno bolj pravno normiran in zavarovan kot je bil v preteklosti.

2. hipoteza: pravno varstvo zasebnosti v Republiki Sloveniji ni učinkovito.

Hipotezo o neučinkovitosti pravnega varstva zasebnosti v Sloveniji bi prav lahko zastavil drugače, npr. tako, da bi izhajal iz predpostavke, da je pravica do zasebnosti učinkovito zavarovana. Preden sem se lotil analize domače zakonodaje in sodne prakse s področja varstva zasebnosti, tako rekoč nisem imel utemeljenih razlogov, da bi o slovenski zakonodaji sodil bodisi pozitivno bodisi negativno. Na koncu sem se vendarle odločil za negativno »kritično« pozicijo, saj sem se želel izogniti apologiji veljavne pravne ureditve. A se je med analiziranjem strokovnega gradiva izkazalo, da je kritična pozicija neutemeljena, saj slovenska zakonodaja že od samega začetka samostojnosti države prevzema pravne smernice drugih razvitih evropskih držav. Res je sicer, da so imeli številni zakoni, ki urejajo pravico do zasebnosti, določene pravne praznine in nedorečenosti. Vendar so najnovejše novele teh zakonov prejšnje slabosti večinoma odpravile, zato je trenutna slovenska zakonodaja s področja varstva pravice do zasebnosti primerljiva z zakonodajo razvitih evropskih držav. Prav tako smo prevzeli številne direktive in priporočila Evropske unije in s tem uskladili domačo zakonodajo z evropskimi standardi. Res je sicer, da slovenska zakonodaja, prav tako kot katerakoli druga, ostaja z neke širše družbene perspektive omejena, saj se zasebnost kljub čedalje intenzivnejšemu pravnemu normiranju krči. Toda s primerjalno pravnega vidika, ki se omejuje na primerjavo posameznih pravnih sistemov, je pravno varstvo pravice do zasebnosti v Republiki Sloveniji relativno učinkovito in primerljivo s pravnim varstvom zasebnosti v članicah Evropske unije.

Hipoteza 2 je zavrnjena. Pravna ureditev varovanja pravice do zasebnosti v Republiki Sloveniji je učinkovita.

Na koncu bom zastavil vprašanje, ki sicer ne sodi v raziskovalni okvir te magistrske naloge, a se ob spoznanju, da se zasebna sfera kljub čedalje večji pravni regulaciji krči, vsiljuje samo od sebe: kakšne so širše družbene implikacije krepitve nadzora in krčenja zasebnosti?
Dokončnega odgovora na to vprašanje ni mogoče podati, med drugim zato, ker so scenariji do katerih lahko privede krčenje zasebnosti, precej raznoliki. Nekateri teoretiki pozdravljajo krčenje

zasebne sfere, saj vidijo v tem sredstvo za krepitev transparentnosti, ki naj bi se na lestvici vrednot sodobnih demokratičnih družb uvrščala precej visoko. Določena mera transparentnosti je nedvomno koristna, saj zavira korupcijo, kriminaliteto in druge oblike deviacij. Toda če transparentnost priženemo do njene sicer utopične skrajnosti, utegne postati izredno nevarna. »Popolna transparentnost« namreč predpostavlja, da vsakdo ve vse o vsakomur – vse je javno in ker ni otočkov zasebnosti, je tudi kakršnokoli gojenje individualnosti, ki bi odstopala od povprečnosti množic, onemogočeno. Takšna utopija je nedvomno nerealna, ker človek že po svoji »naravi« potrebuje nek minimum intime in z njo povezane zasebnosti. Vendar pa je nekoliko bolj omiljena oblika transparentnosti, ki je ne uporabljajo državljani za nadzor države, ampak obratno, ki jo država uporablja za nadzor svojih podanikov, zgodovinsko dejstvo. V vojnah in izrednih razmerah je pomanjkanje zasebnosti nekaj popolnoma običajnega. Tudi številni totalitarni režimi so si bolj ali manj uspešno prizadevali razgaljati zasebnost navadnih državljanov. Ob tem pa je težko spregledati nekatere vzporednice, ki se pod vplivom nevarnosti terorizma in kriminala razgrinjajo v sodobnih demokratičnih družbah – tudi tu se informacijski nadzor čedalje bolj povečuje in postaja sestavni del človeških življenj. Čeprav se zdi, da se pravno varstvo zasebnosti krepi, je to morda le utvara, ki ohranja navidezno razmerje med zasebnostjo in nadzorom, čeprav se je v resnici tehtnica že zdavnaj prevesila na stran nadzora.

7 LITERATURA IN VIRI

- Arendt, Hannah. 1995. *Vita Activa*. Ljubljana: Krtina.
- Backes, Michael, Markus Durmuth in Dominique Unruh. 2008. *Compromising reflections or how to read LCD monitors around the corner*. Dostopno prek: http://crypto.m2ci.org/unruh/publications/reflections.pdf (14. januar 2010).
- Banisar, David. 1999. *Privacy & Human Rights 1999*. Dostopno prek: http://www.privacyinternational.org/survey/index99.html (15. oktober 2009).
- Batagelj, Zenel. 1997. *Direktni marketing, oglaševanje in internet*. Dostopno prek: http://www.cati.si/papers/zbymm0003.html (12. januar 2010).
- Beaver, Kevin. 2007. *Hacking For Dummies*. Indianapolis: Wiley Publishing.
- Beck, Ulrich. 2001. *Družba tveganja. Na poti v neko drugo moderno*. Ljubljana: Krtina.
- Beck, Ulrich in Anthony Giddens. 2002. *Reflexive modernization: politics, tradition and aestetics in the modern social order.* Cambridge: Polity Press.
- Bennet, J. Colin. 2001. Convergence Revisited: Toward a Global Policy for the Protection of Personal Data? V *Tecnology and Privacy: The New Landscape*, ur. Philip E. Agre in Marc Rotenberg, 99-123. Cambridge: MIT Press.
- Bentham, Jeremy. 1995. *The Panopticon Writings*. New York: Verso.
- Berlin, Isiah. 1992. Dva koncepta svobode. V *Sodobni liberalizem*, ur. Rudi Rizman, 69-89. Ljubljana: Krt.
- Black, Edwin. 2002. *IBM and the Holocaust*. London: Time Warner.
- Bogard, William. 2006. Surveillance assemblages and lines of flight. V *Theorizing*

Surveillance: The Panopticon and beyond, ur. David Lyon, 97-122. Portland: Willan Publishing.

- Bogataj, Maja. 2003. *Internet in pravo*. Ljubljana: Pravna fakulteta.
- Boyle, James. 1997. Foucault in Cyberspace: Surveillance, Sovereignity and Hardwired Censors. *University of Cincinnati Law Review* 66 (1): 177-205. Dostopno prek: http://www.law.duke.edu/boylesite/foucault.htm (14. december 2009).
- Božovič, Miran. 1995. An utterly dark spot. V *The panopticon writings*, Jeremy Bentham, 1-27. New York: Verso.
- Cate, H. Fred. 1997. *Privacy in the Information Age*. Washington: Brookings Institution Press.
- Clarke, A. Robert. 1988. *Information Technology and Dataveillance*. Dostopno prek: http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html (6. december 2009).
- Cvetko, Aleksej. 1999. *Varovanje zasebnosti v delovnih razmerjih*. Ljubljana: Gospodarski vestnik.
- Čebulj, Janez. 1992. *Varstvo informacijske zasebnosti v Evropi in Sloveniji*. Ljubljana: Inštitut za javno upravo pri Pravni fakulteti v Ljubljani.
- Čebulj, Janez. 2002. 38. člen (varstvo osebnih podatkov). V *Komentar ustave Republike Slovenije*, ur. Lovro Šturm, 408-416. Ljubljana: Fakulteta za podiplomske državne in evropske študije.
- Črnčec, Damir. 2009. *Obveščevalna dejavnost v informacijski dobi.* Ljubljana: Defensor.
- Davies, G. Simon. 2001. Re-ingeneering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Comodity. V *Technology and Privacy*, ur. Philip E. Agre in Marc Rotenberg, 143-165. Cambridge: MIT Press.
- DeCew, J. 1997. *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Ithaca: Cornell University Press.
- Deflem, Mathieu. 2007. *The Concept of Social Control: Theories and Applications*. Dostopno prek: http://deflem.blogspot.com/2007/08/concept-of-social-control-theories-and.html (20. maj 2009).
- Delaney, Frank. 1995. *History of the Microcomputer Revolution*. Dostopno prek: http://www.virtualaltair.com/virtualaltair.com_/vac_history.asp (20. januar 2010).
- Deleuze, Gilles. 2006. *Foucault*. London: Continuum.
- Deleuze, Gilles. 2007. Kaj je dispozitiv? *Problemi* 45 (8-9): 5-14.
- Dvoršak, Helena. 2008. *Kazensko pravno varstvo zasebnosti na delovnem mestu: specialistična naloga*. Ljubljana: H. Dvoršak.

- EPIC in Privacy International, ur. 2002. *Privacy & Human Rights 2002: An International Survey of Privacy Laws and Developments*. Washington: EPIC.
- Eržen, Nejc. 2009. *Prikrite preiskave in zasebnost: magistrsko delo*. Ljubljana: N. Eržen.
- Etzioni, Amitai. 1999. *The Limits of Privacy*. ZDA: Basic Books.
- Fickes, Michael. 2004. *Automated Eye In The Sky*. Dostopno prek: http://govtsecurity.com/mag/automated_eye_sky/ (18. december 2009).
- Firbas, Gregor. 2009. *Varovanje zasebnosti nekoč in danes: diplomsko delo*. Ljubljana: G. Firbas.
- Foucault, Michel. 2003. Predavanje 17. marca 1976. *Filozofski vestnik* 24 (3): 151-169.
- Foucault, Michel. 2004. *Nadzorovanje in kaznovanje: Nastanek zapora*. Ljubljana: Krtina.
- Foucault, Michel. 2008. *Vednost – oblast – subjekt*. Ljubljana: Krtina.
- Foucault, Michel. 2009. *Rojstvo klinike*. Ljubljana: Študentska založba.
- Gellman, Robert. 2001. Does Privacy Law Work? V *Technology and Privacy*, ur. Philip E. Agre in Marc Rotenberg, 193-218. Cambridge: MIT Press.
- Habermas, Jurgen. 1989. *Strukturne spremembe javnosti*. Ljubljana: ŠKUC: Znanstveni inštitut filozofske fakultete.
- Haggerty, D. Kevin. 2006. Tear down the walls: on demolishing the panopticon. V *Theorizing Surveillance: The Panopticon and Beyond*, ur. David Lyon, 23-45. Portland: Willan Publishing.
- Hirshleifer, Jack. 1980. Privacy: its origin, function and future. *The Journal of Legal studies* 9 (4): 649-664. Dostopno prek: www.econ.ucla.edu/workingpapers/wp166.pdf (14. januar 2009).
- Huš, Matej. 2010. *Cenzura na Kitajskem se stopnjuje s prestrezanjem SMS-ov*. Dostopno prek: http://slo-tech.com/novice/t396357#crta (20. januar 2010).
- Informacijski pooblaščenec. 2008. *Letno poročilo Informacijskega pooblaščenca za leto 2008*. Dostopno na: http://www.ip-rs.si/publikacije/porocila/ (6. marec 2010).
- *Informacijski pooblaščenec*. Dostopno prek: http://www.ip-rs.si/ (6. marec 2010).
- Informacijski pooblaščenec. 2010. Prošnja za pojasnilo metodologije zbiranja podatkov o kršitvah določb Zakona o varstvu osebnih podatkov – odgovor. Pisni odgovor informacijskega pooblaščenca z dne 7. 5. 2010, šifra dopisa: 0712-236/2010/2.
- Kanduč, Zoran. 2003. *Onkraj zločina in kazni*. Ljubljana: Študentska založba.
- Kanduč, Zoran. 2007. *Subjekti in objekti (ne)formalne socialne kontrole v kontekstu postmodernih tranzicij*. Ljubljana: Inštitut za kriminologijo pri Pravni fakulteti.

- Kanduč, Zoran. 2009. Nasilje, nadzorovanje in (post)moderna kultura v kriminološki perspektivi. *Revija za kriminalistiko in kriminologijo* 60 (1): 25-40.
- Kašnik, Suzana. 2006. *Sodobne tehnologije nadzora v Sloveniji: diplomsko delo*. Ljubljana: S. Kašnik.
- Kazenski zakonik (KZ-1). Ur. l. RS. 55/2008. Dostopno prek: http://zakonodaja.gov.si/rpsi/r00/predpis_ZAKO5050.html (4. februar 2010).
- Klein, Naomi. 2008. China`s All-Seeing Eye. *Rolling Stone*. Dostopno prek: http://www.rollingstone.com/politics/story/20797485/chinas_allseeing_eye/print (16. december 2009).
- Klemenčič, Goran. 2001. Varstvo elektronske zasebnosti. V *Internet in pravo*, ur. Matjaž Potrč, 129-191. Ljubljana: Pasadena.
- Klemenčič, Goran. 2002. 37. člen (varstvo tajnosti pisem in drugih občil). V *Komentar ustave Republike Slovenije*, ur. Lovro Šturm, 391-408. Ljubljana: Fakulteta za podiplomske državne in evropske študije.
- Klemenčič, Goran. 2003. Internet in pravica do zasebnosti. V *Internet in pravo*, ur. Maja Bogataj, 101-141. Ljubljana: Pravna fakulteta.
- Klemenčič, Goran. 2004. Internet in pravica do zasebnosti. V *Internet in pravo*, ur. Boštjan Makarovič, 101-141. Ljubljana: Pravna fakulteta.
- Klepec, Peter. 2007. Ob mestu in vlogi dispozitiva pri Foucaultu. *Problemi*, 45 (8-9): 29-57.
- *Koran*. 2005. Tržič: Učila International.
- Križaj, Franc. 1989. *Osebne svoboščine in zasebnost v „informacijski družbi“*. Ljubljana: Gospodarski vestnik.
- Kovačič, Matej. 2003. *Zasebnost na internetu*. Ljubljana: Mirovni inštitut, Inštitut za sodobne družbene in politične študije.
- Kovačič, Matej. 2006. *Nadzor in zasebnost v informacijski družbi: filozofski, sociološki, pravni in tehnični vidiki nadzora in zasebnosti na internetu*. Ljubljana: Fakulteta za družbene vede.
- Kovačič, Matej. 2008. *Kiberkriminal je postal dober posel*. Dostopno prek: http://slo-tech.com/novice/t316519#crta (22. januar 2010).
- Kovačič, Matej. 2008. *Identifikacija posameznikov s pomočjo satelitskih posnetkov*. Dostopno prek: http://slo-tech.com/novice/t325255#crta (22. januar 2010).
- Kovačič, Matej. 2008. *Storitev sledenja mobilnim telefonom v Britaniji*. Dostopno prek: http://slo-tech.com/novice/t313366#crta (22. januar 2010).
- Kovačič, Matej. 2008. *Mobilni skenerji registrskih tablic v ZDA*. Dostopno prek: http://slo-

tech.com/novice/t320903#crta (27. januar 2010).

- Kovačič, Matej. 2008. *Britanci razvijajo pametne videonadzorne sisteme*. Dostopno prek: http://slo-tech.com/novice/t317274#crta (27. januar 2010).
- Kovačič, Matej. 2009. *Sledenje s „superpiškotki"*. Dostopno prek: http://hr-cjpc.si/pravokator/index.php/2009/09/ (21. januar 2010).
- Kovačič, Matej. 2009. *Ustavno sodišče odločilo v zadevi SOVA*. Dostopno prek: http://slo-tech.com/novice/t344142 (15. april 2010).
- Kovačič, Matej. 2009. *Komentar določb novele Zakona o kazenskem postopku (ZKP-J), ki opredeljujejo nekatere posege v informacijsko zasebnost*. Dostopno prek: http://hr-cjpc.si/pravokator/index.php/2009/10/21/novela-zakona-o-kazenskem-postopku-posegi-v-komunikacijsko-zasebnost/ (15. april 2010).
- Kovačič, Matej. 2010. *Kaj prinaša novela Zakona o elektronskih komunikacijah?* Dostopno prek: http://hr-cjpc.si/pravokator/index.php/2010/01/28/kaj-prinasa-novela-zakona-o-elektronskih-komunikacijah/ (16. april 2010).
- Kuhn, S. Thomas. 1998. *Struktura znanstvenih revolucij*. Ljubljana: Krtina.
- Kuhn, Marcus G. 2004. *Electromagnetic eavesdropping risks of flat-panel displays*. Dostopno prek: http://www.cl.cam.acuk/~mgk25/pet2004-fpd.pdf (14. januar .2010).
- Kumar, Ranjit. 2005. *Research methodology: a step by step guide for beginners*. New Delhi: Sage Publications.
- La Franchi, Peter. 2007. *UK Home Office plans national police UAV fleet*. Dostopno prek: http://www.flightglobal.com/articles/2007/07/17/215507/uk-home-office-plans-national-police-uav-fleet.html (17. december 2009).
- Lampe, Rok. 2004. *Sistem pravice do zasebnosti*. Ljubljana: Bonex založba.
- Laurant, Cedric, ur. 2003. *Privacy&Human Rights*. Washington: EPIC.
- Lyon, David. 1994. *The Electronic Eye*. Cambridge: Polity Press.
- Lyon, David. 2003. *Surveillance technology and Surveillance*. Dostopno prek: http://www.greylodge.org/occultreview/glor_012/Surveillance.pdf#search=%22% (22. januar 2010).
- Lyon, David. 2006. The search for surveillance theories. V *Theorizing Surveillance: The Panopticon and Beyond*, ur. David Lyon, 3-20. Portland: Willan Publishing.
- Lyon, David. 2007. *Surveillance Studies: An Overview*. Cambrdige: Polity Press.
- Lukšič, Andrej. 2003. *S poti v digitalno demokracijo*. Ljubljana: Študentska založba.
- Makarovič, Boštjan. 2004. *Internet in pravo*. Ljubljana: Pravna fakulteta.
- Mayer-Schonberger, Viktor. 2001. Generational Development of Data Protection in Europe.

V *Technology and Privacy: The New Landscape*, ur. Philip E. Agre in Marc Rotenberg, 219-241. Cambridge: MIT Press.

- McCullagh, Declan. 2006. *Drone aircraft may prowl U.S. Skies*. Dostopno prek: http://news.cnet.com/2100-11746_3-6055658.html (16. december 2009).
- Mitar, Miran. 2007. *Uvod v metodologijo znanstvenega raziskovanja varnostnih pojavov*. Ljubljana: Fakulteta za varnostne vede.
- Murakami Wood, David, ur. 2006. *A Report on the Surveillance Society*. Dostopno prek: http://www.ico.gov.uk (14. september 2009).
- National Science and Technology Council, ur. 2006. *Privacy & Biometrics: Building a Conceptual Foundation*. Dostopno prek: http://www.biometrics.gov/docs/privacy.pdf (21. oktober 2009).
- Negri, Antonio. 2002. Družba nadzora: intervju s Tonijem Negrijem. *Filozofski vestnik*, 23 (3): 167-177.
- Nietzsche, Friedrich. 2004. *Volja do moči*. Ljubljana: Slovenska matica.
- Odločba Ustavnega sodišča, št. Up-32/94 z dne 13. 4. 1995, OdlUS IV/1, str. 205.
- Odločba Ustavnega sodišča, št. U-I-25/95 z dne 27. 11. 1997, Uradni list RS, št. 5/98, str. 292 in OdlUS VI/2, str. 371.
- Sodba VS RS, II Ips 548/96 z dne 26. 3. 1998, Zbirka civilnih odločb 1998, str. 138.
- Sodba VS RS, II Ips 460/97 z dne 30. 10. 1998, Zbirka civilnih odločb 1998, str. 144.
- Orwell, George. 2004. *1984*. Ljubljana: Mladinska knjiga.
- Pečar, Janez. 1988. *Formalno nadzorstvo: kriminološki in kriminalnopolitični pogledi*. Ljubljana: Delavska enotnost.
- Pečar, Janez. 1991. *Neformalno nadzorstvo: kriminološki in sociološki pogledi*. Radovljica: Didakta.
- Pečar, Janez. 1992. *Institucionalizirano nedržavno nadzorstvo: kriminološki, kriminalnopolitični in sociološki pogledi*. Radovljica: Didakta.
- Pirc Musar, Nataša. 2006. *Vstop v zasebnost prepovedan! : varstvo osebnih podatkov.* Ljubljana: Informacijski pooblaščenec.
- Praprotnik, Rok. 2009. Spremembe zakona o Sovi: Janši in Sanaderju se obeta več zasebnosti po telefonu. *Dnevnik*. Dostopno prek: http://www.dnevnik.si/novice/slovenija/1042290141 (14. april 2010).
- Prosser, W. 1995. *Handbook of the Law of Torts*. St. Paul: West
- Ragin, Charles. 2007. *Družboslovno raziskovanje: enotnost in raznolikost metode*. Ljubljana: Fakulteta za družbene vede.

- Roberts, Lucy P. (2005). *The history of video surveillance – from VCRs to eyes in the sky.* Dostopno prek: www.video-surveillance-guide.com (12. januar 2010).
- Salecl, Renata. 1993. Zakaj ubogamo oblast? Nadzorovanje, ideologija in ideološke fantazme. Ljubljana: Državna založba Slovenije.
- Schnier, Bruce. 1999. *ECHELON Technology*. Dostopno prek: http://www.schneier.com/crypto-gram-9912.html (20. januar 2010).
- Schnier, Bruce. 2005. *Uncle Sam is Listening*. Dostopno prek: http://www.schneier.com/essay-100.html (7. januar 2010).
- Schoeman, Ferdinand D., ur. 1984. *Philosophical Dimensions of Privacy*. Cambridge University Press.
- Short, Nicholas M. 2009. *History of Remote Sensing: In the Beginning; Launch Vehicles*. Dostopno prek: http://www.fas.org/irp/imint/docs/rst/Intro/Part2_7.html (20. december 2009).
- Solove, J. Daniel. 2009. *Understanding Privacy*. Cambridge: Harvard University Press.
- Sykes, J. Charles. 1999. *The End of Privacy*. New York: St. Martin`s Press.
- Speilman, Fran. 2009. Surveillance cams help fight crime, city says. *Chicago Sun Times*. Dostopno prek: http://www.suntimes.com/news/politics/1440402,mayor-daley-emergency-surveillance-cameras.article (14. december 2009).
- *Sveto pismo Stare in Nove zaveze: slovenski standardni prevod*. 2007. Ljubljana: Svetopisemska družba Slovenije.
- Šelih, Alenka. 1979. Zasebnost in nove oblike njenega kazenskopravnega varstva. V *Zbornik znanstvenih razprav*, ur. Marijan Pavčnik, 149-181. Ljubljana: Pravna fakulteta.
- Šelih, Alenka, ur. 1999. *Posvet ob 50-letnici Splošne deklaracije OZN o človekovih pravicah*. Ljubljana: Slovenska akademija znanosti in umetnosti.
- Šelih, Alenka. 1999. Zasebnost kot človekova pravica v pogojih informacijske družbe. V *Posvet ob 50-letnici Splošne deklaracije OZN o človekovih pravicah*, ur. Alenka Šelih, 41-51. Ljubljana: Slovenska akademija znanosti in umetnosti.
- Šturm, Lovro, ur. 2002. *Komentar ustave Republike Slovenije*. Ljubljana: Fakulteta za podiplomske državne in evropske študije.
- Thomas, Douglas. 2000. Criminality on the electronic frontier. V *Cybercrime*, ur. Douglas Thomas in Brian D. Loader, 17-35. London: Routledge.
- Toš, Niko in Mitja Hafner-Fink. 1998. *Metode družboslovnega raziskovanja*. Ljubljana: Fakulteta za družbene vede.
- Ustava Republike Slovenije (URS). Ur. l. RS. 33/1991. Dostopno prek:

http://zakonodaja.gov.si/rpsi/r01/predpis_USTA1.html (7. januar 2010).

- Varuh človekovih pravic. 2008. *Letno poročilo Varuha človekovih pravic za leto 2008*. Dostopno prek: http://www.varuh-rs.si/publikacije-gradiva-izjave/letna-porocila/ (10. april 2010).
- Warwick, Graham. 2007. *US police experiment with Insitu, Honeywell UAVs*. Dostopno prek: http://www.flightglobal.com/articles/2007/12/06/220084/us-police-experiment-with-insitu-honeywell-uavs.html (17. december 2009).
- Whitaker, Reg. 1999. *The End of Privacy*. New York: The New Press.
- Wright, Steve. 1998. *An appraisal of technologies for political control*. Dostopno prek: http://cryptome.org/stoa-atpc.htm (12. januar 2010).
- Zakon o elektronskih komunikacijah (ZEKom-UPB1). Ur. l. RS. 13/2007. Dostopno prek: http://zakonodaja.gov.si/rpsi/r00/predpis_ZAKO5120.html (17. februar 2010).
- Zakon o Informacijskem pooblaščencu (ZinfP). Ur. l. RS. 113/2005. Dostopno prek: http://zakonodaja.gov.si/rpsi/r08/predpis_ZAKO4498.html (14. februar 2010).
- Zakon o kazenskem postopku (ZKP-UPB3). Ur. l. RS. 8/2006. Dostopno prek: http://zakonodaja.gov.si/rpsi/r07/predpis_ZAKO4787.html (6. februar 2010).
- Zakon o Slovenski obveščevalno-varnostni agenciji (ZSOVA-UPB1). Ur. l. RS. 20/2004. Dostopno prek: http://zakonodaja.gov.si/rpsi/r09/predpis_ZAKO4019.html (20. februar 2010).
- Zakon o spremembah in dopolnitvah Zakona o kazenskem postopku (ZKP-J). Ur. l. RS. 77/2009. Dostopno prek: http://zakonodaja.gov.si/rpsi/r08/predpis_ZAKO5438.html (8. februar 2010).
- Zakon o telekomunikacijah (ZTel-1). Ur. l. RS. 30/2001. Dostopno prek: http://zakonodaja.gov.si/rpsi/r03/predpis_ZAKO1633.html (20. februar 2010).
- Zakon o varstvu osebnih podatkov (ZVOP-1-UPB1). Ur. l. RS. 94/2007. Dostopno prek: http://zakonodaja.gov.si/rpsi/r05/predpis_ZAKO5245.html (15. februar 2010).
- Zupančič, M. Boštjan. 2002. 36. člen (nedotakljivost stanovanja). V *Komentar ustave Republike Slovenije*, ur. Lovro Šturm, 386-390. Ljubljana: Fakulteta za podiplomske državne in evropske študije.

8 PRILOGA:

ANALIZA SISTEMA PRAVICE DO ZASEBNOSTI V REPUBLIKI SLOVENIJI

Pravica do zasebnosti ima status človekove pravice, ki v mednarodnem pravu izhaja iz 17. člena[99] Mednarodnega pakta o državljanskih in političnih pravicah, in iz 8. člena[100] Evropske konvencije o človekovih pravicah. Hkrati pa pravica do zasebnosti v slovenskem pravnem redu zavzema položaj ustavnopravne oziroma temeljne pravice, ko jo zagotavlja Ustava Republike Slovenije.

Za razliko od mednarodnih dokumentov, ki splošno varstvo zasebnosti obravnavajo na enem mestu in pri tem izpostavljajo nekatere njene pojavne oblike kot so spoštovanje družinskega življenja, stanovanja in dopisovanja, slovenska ustava varstvo zasebnosti zagotavlja z več določbami. Pravico do zasebnosti in tiste osebnostne pravice človeka, ki se med drugim kažejo tudi v nedotakljivosti posameznikove najožje zasebne sfere – duševnosti, podobe, imena in časti – ureja 35. člen ustave, ki je hkrati tudi določba, ki jamči splošno pravico do zasebnosti (Klemenčič 2003, 120). Ta člen ustave vsebinsko pokriva določbo 34. člena, po kateri ima vsakdo pravico do osebnega dostojanstva in varnosti, določbo 32. člena, po kateri ima vsakdo pravico do svobodnega gibanja (tudi ta lahko pomeni vprašanje zasebnosti), določbo 36. člena o nedotakljivosti stanovanja, določbo 37. člena o varstvu tajnosti pisem, določbe 38. člena o varstvu osebnih podatkov in določbo 39. člena o svobodi izražanja. Ta področja so torej že zajeta v širšem pojmu zasebnosti, tako da daje ustava s svojim ponovnim imenovanjem posamezne pravice temu delu samo še večji pomen (Cvetko 1999, 53).

Varstvo zasebnosti v prostoru opredeljuje 36. člen ustave (nedotakljivost stanovanja). Nedotakljivost stanovanja temelji na teritorialni koncepciji zasebnosti, zgodovinsko pogojeni z varovanjem zasebne lastnine, ohranjanjem avtonomije družinskega življenja in fizičnim ločevanjem javne in zasebne sfere bivanja.

Zadnjo in v sodobnih družbah izjemno pomembno kategorijo varstva zasebnosti predstavlja varstvo informacijske zasebnosti, ki jo zagotavlja 38. člen ustave (varstvo osebnih podatkov). Prav varstvo osebnih podatkov je tesno povezano s pravico do komunikacijske zasebnosti. Informacija, pridobljena s posegom v

---

[99] *Nikomur se ne sme nihče samovoljno ali nezakonito vmešavati v zasebno življenje, v družino, v stanovanje ali dopisovanje in ga tudi ne nezakonito žaliti ali škodovati njegovemu ugledu. Vsakdo ima pravico do zakonitega varstva proti takšnemu vmešavanju, žalitvam ali škodovanju* (17. člen Mednarodnega pakta o državljanskih in političnih pravicah).

[100] Pravica do spoštovanja zasebnega in družinskega življenja (8. člen EKČP):
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.

komunikacijsko zasebnost, je namreč praviloma osebni podatek, ki je predmet varstva 38. člena (Klemenčič 2003, 120).

- 35. člen Ustave RS (varstvo pravic zasebnosti in osebnostnih pravic)

  Zagotovljena je nedotakljivost človekove telesne in duševne celovitosti, njegove zasebnosti ter osebnostnih pravic.

- 37. člen Ustave RS (varstvo tajnosti pisem in drugih občil)

  Zagotovljena je tajnost pisem in drugih občil.

  Samo zakon lahko predpiše, da se na podlagi odločbe sodišča za določen čas ne upošteva varstva tajnosti pisem in drugih občil in nedotakljivost človekove zasebnosti, če je to nujno za uvedbo ali potek kazenskega postopka ali za varnost države.

- 38. člen Ustave RS (varstvo osebnih podatkov)

  Zagotovljeno je varstvo osebnih podatkov. Prepovedana je uporaba osebnih podatkov v nasprotju z namenom njihovega zbiranja. Zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa zakon.

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

Drobljenje splošne pravice do zasebnosti na posamezne kategorije in ločene ustavne člene ne sme zavajati. Različne pojavne oblike varstva zasebnosti se kot ustavne pravice razlikujejo, oziroma so v novejših ustavnih dokumentih namensko ločene, zgolj zaradi specifičnih pogojev, ki so se razvili za posege vanje. Tako tudi za 37. člen ustave velja temeljna maksima, da je treba vsako pravico iz področja varstva zasebnosti vedno interpretirati skozi prizmo splošnega in celovitega varstva zasebnosti in osebnostnih pravic ter kompleksnega spektra interesov posameznika, ki jih zasebnost obsega (Klemenčič 2003, 120).

KAZENSKOPRAVNO VARSTVO PRAVICE DO ZASEBNOSTI

Ker je pravica do zasebnosti tudi kazenskopravno zavarovana, v hujših primerih poseg v zasebnost predstavlja celo kaznivo dejanje, pri čemer mora oškodovani posameznik podati ovadbo pristojnemu državnemu tožilcu. Kazenski zakonik v šestnajstem poglavju, kjer so določena in obravnavana kazniva dejanja zoper človekove pravice in svoboščine, in v osemnajstem poglavju, v katerem so določena in obravnavana kazniva dejanja zoper čast in dobro ime, navaja več kaznivih dejanj, ki inkriminirajo različne posege v zasebnost (Klemenčič 2003, 140):

5) Kršitev enakopravnosti (131. člen KZ-1)
6) Neupravičena osebna preiskava (136. člen KZ-1)
7) Neupravičeno prisluškovanje in zvočno snemanje (137. člen KZ-1)
8) Neupravičeno slikovno snemanje (138. člen KZ-1)
9) Kršitev tajnosti občil (139. člen KZ-1)
10) Nedovoljena objava zasebnih pisanj (140. člen KZ-1)
11) Neupravičena izdaja poklicne skrivnosti (142. člen KZ-1)
12) Zloraba osebnih podatkov (143. člen KZ-1)
13) Kršitev moralnih avtorskih pravic (147. člen KZ-1)
14) Kršitev materialnih avtorskih pravic (148. člen KZ-1)
15) Kršitev avtorski sorodnih pravic (149. člen KZ-1)
16) Napad na informacijski sistem (221. člen KZ-1)
17) Vdor v poslovni informacijski sistem (237. člen KZ-1)
18) Izdelovanje in pridobivanje orožja in pripomočkov, namenjenih za kaznivo dejanje (306. člen KZ-1)

CIVILNOPRAVNO VARSTVO PRAVICE DO ZASEBNOSTI

Pravica do zasebnosti je tudi civilnopravno zavarovana. Ena od možnosti civilnopravnega varstva je ugotovitvena tožba v skladu z določbo 181. člena Zakona o pravdnem postopku, druga možnost je zahtevek za prenehanje s kršitvami pravice osebnosti v skladu z določbo 134. člena obligacijskega zakonika, tretja pa je zahtevek za povrnitev negmotne škode v skladu z določbama 178. in 179. člena obligacijskega zakonika (Cvetko 1999, 27).

Zakon o pravdnem postopku v 181. členu določa, da lahko tožnik s tožbo zahteva, da sodišče le ugotovi obstoj ali neobstoj kakšne pravice ali pravnega razmerja ali prisotnost oziroma neprisotnost kakšne listine. Takšna tožba se lahko vloži, če ima tožnik pravno korist od tega, da sodišče ugotovi obstoj ali neobstoj kakšne pravice ali pravnega razmerja oziroma ima kakšno drugo pravno korist od vložitve takšne tožbe. Taka tožba je sicer bolj teoretična možnost, saj je treba vsekakor ugotavljati pravno korist, kar je lahko v zvezi z varstvom pravice do zasebnosti še posebej zahtevna naloga (Cvetko 1999, 27).

Druga možnost je zahtevek za prenehanje s kršitvami pravice osebnosti po določbi 134. člena obligacijskega zakonika. Ta določa, da ima vsak pravico zahtevati od sodišča ali drugega pristojnega organa, da odredi prenehanje dejanja, s katerim se krši nedotakljivost človekove osebnosti, osebnega ali družinskega življenja ali kakšna druga pravica njegove osebnosti. Pri tem lahko sodišče ali drug organ odredi, da kršitelj preneha z dejanjem, ker bo sicer moral prizadetemu plačati določen denarni znesek, odmerjen skupaj ali od časovne enote. V nasprotju z odškodninsko odgovornostjo v takem primeru ni potrebna krivda, ampak zadošča že

sama kršitev. Seveda pa pri takem varstvu, ki je lahko pomembno predvsem zato, ker ni vezano na dolgotrajnejši postopek ugotavljanja civilne odgovornosti, odškodninski zahtevek ni izključen (Cvetko 1999, 28).

V 178. členu obligacijskega zakonika je določeno, da lahko, če gre za kršitev osebnostne pravice, sodišče odredi na stroške oškodovalca objavo sodbe oziroma popravka ali odredi, da mora oškodovalec preklicati izjavo, s katero je storil kršitev, ali kaj drugega, s čimer je mogoče doseči namen, ki se doseže z odškodnino. V 179. členu pa je določba o tem, v katerih primerih in kako je mogoče zahtevati denarno odškodnino za negmotno škodo. V teh primerih se poseg v pravico do zasebnosti obravnava kot civilni delikt, izpolnjene pa morajo biti tudi predpostavke odškodninske odgovornosti (Cvetko 1999, 28).

SODNA PRAKSA IN RAZVOJ PRAVICE DO ZASEBNOSTI

K razvoju pravice do zasebnosti v slovenskem pravu je največ prispevala pravna praksa Ustavnega in Vrhovnega sodišča. Za samo pojmovanje in definicijo pravice do zasebnosti je pomemben prvi precedenčni primer Ustavnega sodišča (Odl. US. Up-32/94) oziroma tako imenovani »posestni spor«. V tej odločbi je Ustavno sodišče prvič definiralo »človekovo zasebnost«, ki jo zagotavlja 35. člen Ustave RS, kot *»v območju človekovega bivanja bolj ali manj sklenjeno celoto človekovega ravnanja in ukvarjanja, občutij in razmerij, za katero je značilno in konstitutivno, da si jo človek oblikuje in vzdržuje sam ali sam z najbližjimi, s katerimi je v intimni skupnosti, na primer z življenjskim partnerjem, in da v njej biva z občutkom varnosti pred vdorom javnosti ali kogarkoli nezaželenega«* (Odl. US. št. Up-32/94).

Ustavno sodišče je opozorilo na različne vsebine zasebnosti (36., 37. in 38. člen Ustave RS) in na oblikovanje zavesti o pravni doktrini in praksi »globalne človekove pravice do zasebnosti«, v katero je pravno dopustno posegati le tedaj, ko je na tehtnici javni interes ali pravica drugega (Lampe 2004, 266).

V drugem precedenčnem primeru (OdlUS št. U-I-25/95 in OdlUS VI/2) je Ustavno sodišče pri obravnavanju vprašanja kršitve zasebnosti in pojmovanja zasebnosti uporabilo sodno presojo Evropskega sodišča za človekove pravice, ki zasebnost pogosto razume kot široko negativno pravico varstva posameznika pred posegi države in tretjih oseb v njegovo zasebno sfero, osebnost in dostojanstvo. Ustavno sodišče je v tej odločbi navedlo ugotovitve konference nordijskih pravnikov v Stockholmu leta 1967, ki je pravico posameznika v sferi zasebnosti opredelilo preko poseganja vanjo. Poseg v zasebnost pa so opredelili kot *»poseganje v zasebno in družinsko življenje ter dogajanje v domu kot poseg v telesno in duševno nedotakljivost, ali moralo in duševno svobodo, poseg zoper čast in dobro ime, odkrivanje neugodnih okoliščin iz zasebnega življenja, zasledovanje, opazovanje, prisluškovanje in sumničenje, zlorabo pisnih in ustnih zasebnih sporočil, pridobivanje informacij, ki pomenijo poklicno skrivnost«.*

Čeprav gre predvsem za javnopravne vidike varstva pravice do zasebnosti, je iz okvirnega seznama posegov

v pravico do zasebnosti mogoče izluščiti tudi civilnopravne vidike varstva te pravice. Pravica do zasebnosti posameznika ne varuje le pred posegi državne oblasti, temveč tudi pred posegi drugih ljudi. Vsak poseg v pravico do zasebnosti ima tudi civilnopravne posledice, zato prizadetemu subjektu civilno pravo nudi specifičen instrumentarij varstva (Lampe 2004, 267).

Vrhovno sodišče Republike Slovenije pa je v svojem presedanu obravnave pravice do zasebnosti zapisalo, da je *»posamezniku z ustavno močjo pridržana sfera zasebnega življenja oziroma njegovega zasebnega življenjskega okolja. Zagotovljena je nedotakljivost njegove zasebnosti, kar pomeni, da obstaja nedotakljivo področje človekove svobode, ki je odtegnjeno vplivu države ter toliko bolj seveda posegu drugih posameznikov«* (Sodba VS RS, II Ips 460/97).
V istem primeru (t.i. primer »prostozidarske lože«) je Vrhovno sodišče zapisalo, da zasebnost ne obsega le *»ozkega notranjega kroga posameznika in družine«*, s tem pa je začrtalo široko razumevanje koncepta zasebnosti (Lampe 2004, 267).

V drugem precedenčnem primeru (Sodba VS RS št. II Ips 548/96) je Vrhovno sodišče leta 1998 dosodilo, da je oseba, ki je brez tožnikovega pooblastila posredovala psihiatrično izvedensko mnenje tretjim osebam, s tem posegla v tožnikovo pravico do zasebnosti in je zato odškodninsko odgovorna. V istem primeru je Vrhovno sodišče sprejelo tudi pravno mnenje na podlagi 35. člena Ustave in 199. ter 200. člena Zakona o obligacijskih razmerjih, kjer je bilo zapisano, da so *»podatki iz psihiatrovega izvedenskega mnenja o tožnikovem zdravljenju, diagnozi njegove duševne bolezni, osebnostnih lastnostih in siceršnjih osebnih in družinskih razmerah po svoji naravi zaupni in je zaradi posredovanja le-teh tretjim osebam toženec posegel v tožnikovo pravico do zasebnosti in mu je zato odškodninsko odgovoren«* (Lampe 2004, 268).

Slovenska civilnosodna praksa tako dobiva vse daljši katalog primerov, kjer so sodišča dosodila različne oblike sankcij zaradi kršitve osebnostnih pravic, med katere sodi tudi pravica do zasebnosti. V tem katalogu so tudi primeri dodeljevanja denarne odškodnine za nematerialno škodo zaradi duševnih bolečin, ki so nastale kot posledica kršitve pravice do zasebnosti (Lampe 2004, 268).

SISTEMATIZACIJA PRAVICE DO ZASEBNOSTI V SLOVENSKEM PRAVU

Ustavno varovana pravica do zasebnosti vsebinsko obsega različne osebnostne pravice, med katerimi je potrebno izpostaviti predvsem pravico do nedotakljivosti stanovanja, pravico do tajnosti pisem in drugih občil ter pravico do tajnosti osebnih podatkov (Lampe 2004, 269).
Ker je področje, ki sodi pod okrilje splošne pravice do zasebnosti precej široko, se številni pravni in drugi strokovnjaki sprašujejo, kako čimbolj učinkovito in pregledno sistematizirati pravico do zasebnosti.

Lampe (2004, 270) predlaga štiri kategorije pravice do zasebnosti:

1) Prostorska zasebnost: sem spada predvsem pravica do nedotakljivosti stanovanja in drugih prostorov;
2) Informacijska zasebnost: sem sodi pravica do tajnosti pisem in drugih občil ter pravica do varstva osebnih podatkov;
3) Psihična zasebnost: obsega pravico do spolne integritete in pravico do nedotakljivosti osebnega in družinskega življenja;
4) Odločitvena zasebnost: vsebuje tiste pravice, ki pokrivajo različne aspekte posameznikovih zasebnih odločitev.

Košir (1999 v Dvoršak 2007, 33) pravi, da je prostorska zasebnost utemeljena na načelu razumno pričakovane zasebnosti in posamezniku zagotavlja fizični prostor, kjer lahko živi, deluje in se giba svobodno – neizpostavljen fizičnim vdorom in opazovanju s strani drugih ljudi. Prostorska zasebnost je potemtakem pravica do nedotakljivosti fizičnega prostora.
Košir (1999 v Dvoršak 2007, 33) psihično zasebnost opredeli kot pravico do nadzora nad dostopom do naših intimnih razmišljanj in čustvovanj. O odločitveni zasebnosti pa pravi, da posamezniku zagotavlja predvsem pravico do sprejemanja in uresničevanja avtonomnih odločitev, torej brez pritiskov okolice.
Ker pa je poudarek v tem besedilu namenjen informacijskemu družbenem nadzoru, bo bolj ustrezna Kovačičeva (2003, 79) sistemizacija pravice do zasebnosti, ki loči:

1) Prostorsko zasebnost
2) Komunikacijsko zasebnost
3) Informacijsko zasebnost

Za razliko od splošne opredelitve zasebnosti kot pravice posameznika, *»da se ga pusti pri miru«* (v tem primeru gre torej za pravico izrazito negativnega statusa, ki druge ljudi izključuje), pravica do komunikacijske in informacijske zasebnosti izpostavlja vrednoto svobodnega vzpostavljanja in vzdrževanja socialnih stikov posameznika z zunanjim svetom. Pravica do zasebnosti je v veliki meri pomembna vrednota tudi zato, ker s prepovedjo posegov »cenzure« v njeno varovano območje *»pospešuje izmenjavo informacij z drugimi ljudmi, ustvarjanje in utrjevanje družbenih vezi in ne zgolj zaradi zagotavljanja neodvisnosti in izolacije od drugih«* (Klemenčič 2003, 121).

PROSTORSKA ZASEBNOST

Nedotakljivost stanovanja oziroma prostorska zasebnost predstavlja prvi pravno zavarovani aspekt zasebnosti. Izvira iz angleške domneve o nedotakljivosti državljanovega doma, ki jo nekoliko lirično

izražena z rekom *»a man`s home in a man`s castle«*.

Zupančič (v Šturm in drugi 2002, 387) ugotavlja, da je šlo pri prostorski zasebnosti prvotno le za teritorialno varstvo stanovanja. Kasneje pa se je zaradi razvoja nadzorne tehnologije področje, ki ga pokriva prostorska zasebnost, bistveno razširilo. Uveljavilo se je namreč načelo zaščite razumno pričakovane zasebnosti (ang. reasonable expectation of privacy), ki besede »stanovanje« ne tolmači ozko, pač pa pod tem izrazom razume vse prostore v katerih državljan lahko razumno pričakuje zasebnost (Kovačič 2003, 79).

Klemenčič (v Šturm in drugi 2002, 401) ob tem ugotavlja, da *»pravo ne ščiti zgolj prostorov, lastnine in lastnikov, temveč posameznike, ki v določenem trenutku v določenem prostoru ali pri določenem ravnanju (upravičeno) pričakujejo svojo zasebnost«*.

Prostorska zasebnost je v slovenskem pravnem redu eksplicitno varovana s kazenskim zakonikom. 138. člen KZ-1 prepoveduje neupravičeno slikovno snemanje druge osebe ali njenih prostorov, če se pri tem občutno poseže v njeno zasebnost, 141. člen KZ-1 (kot neposredna kazenskopravna konkretizacija 36. člena Ustave) pa določa sankcije pri kršitvi nedotakljivosti stanovanja, ki se nanaša na nezakonit vstop ali preiskavo zasebnih prostorov, kazniv pa je tudi poizkus (Kovačič 2003, 80).

KOMUNIKACIJSKA ZASEBNOST

Ustava v 1. odstavku 37. člena zagotavlja tajnost pisem in drugih občil, pri čemer je občila potrebno pojmovati zelo široko. Med občila lahko štejemo telefonske komunikacije, elektronsko pošto[101], SMS sporočila, komunikacijo na spletnih socialnih omrežjih (npr. Facebook, Netlog), komunikacijo na spletnih forumih, idr., saj oblika in vsebina sporazumevanja ni pomembna. Poleg tega tudi ni nujno, da se za prenos sporočila uporabi javno telekomunikacijsko omrežje, pač pa je komunikacijska zasebnost varovana tudi takrat, ko se sporočilo prenaša preko zasebnih ali zaprtih telekomunikacijskih sistemov (Šturm in drugi 2002, 395). To je razvidno npr. iz razsodbe št. U 702/99 z dne 21. 3. 2000, v kateri je Upravno sodišče RS zavzelo stališče, da se varstvo zasebnosti, zagotovljeno v 37. členu Ustave RS, nanaša tudi na službene telefone, pridobitev in uporaba izpiskov telefonskih klicev službenega telefona s strani delodajalca pa predstavlja kršitev.

V nasprotju z Združenimi državami, kjer je zasebnost na delovnem mestu slabo varovana oziroma je zaposleni pogosto sploh ne morejo pričakovati, v Evropski Uniji veljajo strožja pravila (glej odločitev Evropskega sodišča za človekove pravice *Halford*[102] *proti Združenemu kraljestvu* iz leta 1997). Kljub temu je

[101] Posebej velja izpostaviti elektronsko pošto, ki je v današnjem življenju postala ena od najbolj pomembnih oblik korespondence. Čeprav gre tehnično gledano za popolnoma drugačno obliko dopisovanja kot s »klasičnimi« pisemski občili, je potrebno elektronsko pošto v civilnopravnem smislu obravnavati kot klasično pisemsko pošiljko. Elektronsko sporočilo mora biti v fazi pošiljanja in sprejemanja načeloma tajno, tretje osebe pa niso upravičene posegati v elektronsko korespondenco posameznika – to pravico ima v zakonsko natančno določenih primerih le država (Lampe 2004, 300).

[102] Halford proti Veliki Britaniji iz leta 1997 (Halford v. Velika Britanija, odločba z dne 25. 6. 1997): v tem primeru je

npr. v primeru, ko zaposleni uporablja telekomunikacijsko omrežje podjetja, obseg varovanja komunikacijske zasebnosti manjši. Poleg same vsebine komunikacije so varovani tudi t.i. prometni podatki, ki so integralni del komunikacije (Šturm in drugi 2002, 396). To pomeni, da se določbe o varovanju komunikacijske zasebnosti nanašajo tudi na razne izpiske telefonskih številk, podatke o dolžini komunikacije, količini prenesenih podatkov, itd. (Kovačič 2003, 80).

V vsakem primeru korespondenca predstavlja pomemben vidik posameznikove pravice do zasebnosti. Korespondenca je načeloma tajna in naj bi takšna tudi ostala, saj je v njej lahko izraženo marsikaj iz področja posameznikove intime, kar ni namenjeno širšemu krogu javnosti, ampak le specifičnim osebam. Tajnost korespondence je torej zavarovana že z ustavo, ki zagotavlja pravico do tajnosti korespondence vsakomur, ki pri svojem ravnanju upravičeno pričakuje zasebnost, pri tem pa je vseeno, ali gre za prestrezanje v realnem času ali pa za zaseg (npr. poštne pošiljke). Poseg v pravico nastane že s tem, da nekdo nezakonito prestreže komunikacijo in se seznani z njeno vsebino, pa čeprav te informacije pozneje ne uporablja (Šturm in drugi 2002, 398).

Vendar pa Klemenčič (v Šturm in drugi 2002, 395) ugotavlja, da *»se domet pravice do komunikacijske zasebnosti ne ustavi zgolj pri zagotavljanju zaupnosti vsebine sporočanja in podatkov povezanih z njo, ampak hkrati prepoveduje tudi nesorazmerne prepovedi komuniciranja z zunanjim svetom«*. Odločitev Kasacijskega sodišča Francije št. 99-42.042 z dne 2. 10. 2001 izrecno pravi, da *»delodajalec, ki bere sporočila, ki jih zaposleni pošilja ali sprejema preko službenega računalnika, krši temeljne pravice delavca, kot jih določa 8. člen EKČP. 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«* (Šturm in drugi 2002, 402).

Podobno stališče glede omejitev nadzora na delovnem mestu je Kasacijsko sodišče Francije zavzelo tudi v primeru Philippe K. v. Cathnet-Science. V tem primeru je delodajalec na mizi zaposlenega po naključju našel erotične fotografije, zaradi česar so posumili, da ima zaposleni na računalniku shranjene pornografske vsebine. Sledila je preiskava računalnika, na katerem so res našli pornografske vsebine in posledično zaposlenega odpustili. Nižja sodišča so odločitev delodajalca podprla, Kasacijsko sodišče Francije pa je presodilo, da sum prisotnosti pornografije na računalniku ne predstavlja opravičljivega razloga za preiskavo (Cate 2007). Zato bi tudi vsak poseg države, ki bi nesorazmerno prepovedal uporabo kriptografije ali

policija nadzorovala službeni telefon svoje uslužbenke z namenom, da bi zbrala gradivo za svojo obrambo v postopku zaradi diskriminacije. Ga. Halford je imela v svoji pisarni dva telefona, eden pa je bil namenjen tudi za osebno rabo, čeprav sta bila oba del policijskega internega omrežja. Glede uporabe telefona ni bilo postavljenih nikakršnih pravil. Službene zadeve je pogosto urejala tudi od doma in policija ji je plačevala del njenih domačih stroškov za telefon. Britanska vlada je trdila, da ga. Halford nima upravičenega pričakovanja zasebnosti na delovnem mestu, delodajalec pa bi moral imeti načelno možnost prisluškovati pogovorom zaposlenih brez njihove vednosti. Evropsko sodišče za človekove pravice je presodilo, da zaposleni na delovnem mestu upravičeno pričakuje zasebnost.

anonimnih poštnih strežnikov, lahko pomenil poseg v ustavno zajamčeno komunikacijsko zasebnost (Šturm in drugi 2002, 395).

Pravica do komunikacijske zasebnosti je tudi kazenskopravno zavarovana, saj 139. člen Kazenskega zakonika, ki je »podaljšana roka« ustavne garancije varstva tajnosti pisem in drugih občil (Lampe 2004, 299), določa sankcije zaradi kršitve tajnosti občil. Ta člen prepoveduje neupravičeno odpiranje tujih pisem oziroma drugih pošiljk in prestrezanje sporočil, ki se prenašajo po telekomunkacijskem omrežju, oziroma seznanjanje z njihovo vsebino, tudi če se pisma ali pošiljke ne odpre. Prav tako je prepovedano neupravičeno seznanjanje s sporočilom, ki se prenaša po telefonu ali po kakšnem drugem telekomunikacijskem sredstvu. V istem členu je sankcionirano tudi neupravičeno posredovanje tujega pisma tretjim osebam, 140. člen pa prepoveduje javno objavo zasebnega pisanja brez dovoljenja pooblaščene osebe. Zakoniti poseg v zasebnost komunikacij je mogoč izključno na podlagi odredbe sodišča, če je to potrebno zaradi uvedbe ali poteka kazenskega postopka ali zaradi varnosti države, v Sloveniji pa ga na podlagi zakona o kazenskem postopku in zakona o Slovenski obveščevalno-varnostni agenciji izvajata policija in Sova (Kovačič 2003, 92).

O nadzoru telekomunikacijskega prometa govorita 103. in 107. člen Zakona o elektronskih komunikacijah (ZEKom), kjer je navedeno tudi, da morajo operaterji na lastne stroške zagotoviti ustrezno programsko opremo in primerne vmesnike.
Zakon o poštnih storitvah (ZPSto-2) pa v 55. členu od izvajalcev poštnih storitev zahteva, da na podlagi sodne odredbe pristojnemu organu omogočijo dostop do vsebine poštnih pošiljk. Hkrati morajo operaterji telekomunikacijskih storitev in izvajalci poštnih storitev zagotoviti neizbrisno registracijo posegov. Vendar pa se pristojnosti državnih organov glede posegov v zasebnost razlikujejo. Zakon o kazenskem postopku v 151. členu Zakona o kazenskem postopku jasno določa tista kazniva dejanja[103], kjer je nadzor komuniciranja, sporočil, prisluškovanja in tajnega opazovanja, sledenja ter snemanja dovoljen (Kovačič 2003, 82).

Precej bolj problematičen pa je Zakon o Slovenski obveščevalno-varnostni agenciji (ZSOVA), ki v 24. členu predvideva možnost[104] nadzora pisem in nadzorovanja ter snemanja telekomunikacij v Republiki Sloveniji

[103] To so: (1) kazniva dejanja zoper varnost Republike Slovenije in njeno ustavno ureditev in kazniva dejanja zoper človečnost in mednarodno pravo, za katera je v zakonu predpisana kazen zapora petih ali več let; (2) kazniva dejanja ugrabitve, neupravičene proizvodnje in prometa z mamili, omogočanja uživanja mamil, izsiljevanja, neupravičenega sprejemanja ali dajanja daril, ponarejanja denarja, pranja denarja, tihotapstva, jemanja ali dajanja podkupnine, hudodelskega združevanja, nedovoljene proizvodnje in prometa orožja ali razstrelilnih snovi ter ugrabitve letala ali ladje; (3) druga kazniva dejanja, za katera je v zakonu predpisana kazen zapora osmih ali več let.

[104] 24. člen Zakona o Slovenski obveščevalno-varnostni agenciji predvideva možnost nadzora pisem in nadzorovanje ter snemanje telekomunikacij v Republiki Sloveniji, če je podana verjetnost, da obstaja nevarnost za varnost države, ki se kaže v: (1) tajnih aktivnostih zoper suverenost, neodvisnost, državno celovitost in strateške interese Republike Slovenije; (2) tajnih aktivnostih, načrtih in pripravah za izvedbo mednarodnih terorističnih akcij zoper Republiko Slovenijo ter drugih nasilnih dejanjih proti državnim organom in nosilcem javnih funkcij v Republiki Sloveniji ter tujini; (3) posredovanju podatkov in dokumentov, ki so v Republiki Sloveniji opredeljeni kot državna tajnost, nepooblaščeni osebi v tujini; (4) pripravah na oborožen napad na Republiko Slovenijo; (5) obveščevalni dejavnosti posameznikov, organizacij in skupin v korist tujine; (6) mednarodni organizirani kriminalni dejavnosti; in je utemeljeno pričakovati, da se v zvezi s to aktivnostjo uporablja določeno telekomunikacijsko sredstvo ali bo to

tudi v primeru, če obstaja nevarnost za varnost države, ki se lahko kaže *»v tajnih aktivnostih ... zoper strateške interese Republike Slovenije«*. Poznavalci (glej Kovačič 2003, 84) opozarjajo, da je »strateške interese« mogoče opredeliti bolj ohlapno, kar bi lahko imelo za posledico, da Sova lažje pride do zakonitega sodnega naloga za prestrezanje komunikacij, s tem pa je tudi možnost morebitnih zlorab večja.

Problematičen je tudi 21. člen Zakona o Slovenski obveščevalno varnostni agenciji, ki SOVI omogoča »spremljanje mednarodnih sistemov zvez« (oziroma z drugimi besedami prisluškovanje, kar nedvomno predstavlja poseganje v človekove pravice) brez odredbe sodišča, saj zadostuje le podpis direktorja obveščevalne službe. Prav tako se v skladu z 21. členom ZSOVA »spremljanje mednarodnih sistemov zvez ne sme nanašati na določljiv priključek komunikacijskega sredstva ali na določenega uporabnika tega priključka na območju Republike Slovenije«.

Poudariti velja, da je na podlagi 21. člena ZSOVA Slovenska obveščevalno varnostna agencija v preteklih letih prisluškovala več kot 3000 telefonskim številkam v tujini (Praprotnik 2009), prav tako pa je leta 2004 posnela pogovore med Janezom Janšo in Ivom Sanaderjem o incidentih v Piranskem zalivu.

21. člen ZSOVA se je zdel sporen nekdanjemu predsedniku vrhovnega sodišča, Francu Testenu, ki je prvi vložil zahtevo za oceno ustavnosti Zakona o SOVI. Ustavno sodišče je zahtevo zavrnilo. Kasneje je zahtevo za oceno ustavnosti istega zakona vložila Informacijska pooblaščenka Nataša Pirc Musar, ki je med inšpekcijskim pregledom na SOVI ugotovila, da SOVA izvaja nadzor mednarodnih sistemov zvez tako, da prisluškovanje odobri direktor SOVE. 21. člen Zakona o SOVI sicer določa, da lahko odredbo za prisluhe mednarodnim sistemom zvez izda direktor SOVE (in ne sodišče), vendar je po mnenju Pooblaščenke to neustavno, saj 37. člen Ustave izrecno zahteva odredbo sodišča. Informacijska pooblaščenka je prav tako ugotovila, da SOVA krši tretji odstavek 21. člena, saj v nekaterih primerih prisluškuje konkretnim telefonskim številkam in torej ne gre zgolj za spremljanje zadeve, ampak za nadzor točno določenih posameznikov.

Ustavno sodišče si je za odločanje vzelo skoraj leto dni, nato pa je odločilo, da Pooblaščenkino zahtevo za oceno ustavnosti zakona zavrže. V obrazložitvi je Ustavno sodišče zapisalo, da je Pooblaščenka v okviru inšpekcijskega postopka ugotovila, da je SOVA v primeru pogovorov med Janšo in Sanaderjem osredotočeno spremljala tuj telekomunikacijski priključek. To je po mnenju Ustavnega sodišča v neskladju z odločitvijo U-I-216/07, kjer je Ustavno sodišče pojasnilo, da se spremljanje mednarodnih sistemov zvez kot del obveščevalne dejavnosti SOVE lahko nanaša le na območje zunaj državnega območja Republike Slovenije in da gre za spremljanje zadeve in ne konkretnega posameznika. Po mnenju Ustavnega sodišča pa Zakon o SOVI Pooblaščenki ne preprečuje, da izpolni svojo zakonsko nalogo nadzora nad izvajanjem predpisov, ki urejajo varstvo osebnih podatkov. Prav tako po mnenju Ustavnega sodišča Pooblaščenka ni izkazala, da se je vprašanje ustavnosti izpodbijanih zakonskih določb pojavilo v zvezi s postopkom, ki ga je vodila. Iz navedenih razlogov so njeno pobudo za oceno ustavnosti zavrli (Kovačič 2009).

---

sredstvo uporabljeno, pri tem pa je mogoče utemeljeno sklepati, da podatkov ni mogoče pridobiti drugače oziroma bi njihovo pridobivanje na drug način lahko ogrozilo življenje in zdravje ljudi.

NOVELA ZAKONA O KAZENSKEM POSTOPKU

Z vidika pravnega urejanja komunikacijske zasebnosti je nedvomno pomembna novela Zakona o kazenskem postopku (ZKP-J), ki je bila 2. oktobra 2009 objavljena v Uradnem listu RS. Novela predstavlja bistveno posodobitev Zakona o kazenskem postopku in modernizacijo slovenskega pravnega reda na področju informacijskega prava. Novela je v Zakon o kazenskem postopku vnesla dva nova člena (219.a in 223.a), ki opredeljujeta postopke forenzičnega zasega podatkov v kazenskem postopku in nekatere posege v komunikacijsko zasebnost. Gre za pomembne spremembe, ki urejajo predvsem področje preiskave kiberkriminala.

Pobudo za spremembo zakona je dalo Ustavno sodišče. Leta 2008 je v razsodbi Up-106/05 presodilo, da poseg v svobodo komuniciranja ni dovoljen brez predhodnega dovoljenja sodišča in da so prometni podatki sestavni del vsebine komunikacije, s tem pa tudi del komunikacijske zasebnosti. Ustavno sodišče je namreč odločalo o pritožbi posameznika, ki je bil pred Okrožnim sodiščem v Novi Gorici obsojen za kaznivo dejanje neupravičenega prometa z mamili. V kazenskem postopku je zatrjeval, da so bili podatki, ki so se nahajali na zaseženi SIM kartici, pridobljeni brez odredbe preiskovalnega sodnika, zato naj bi šlo za nedovoljene dokaze. Policija je pritožniku med zakonito izvedeno preiskavo zasegla mobilni telefon in ga nato, vključno s SIM kartico, pregledala. Po pritožnikovem mnenju pa naj bi bilo to preiskovanje nezakonito, saj policija ni pridobila še dodatne odredbe za nadzor telekomunikacij.

Ustavno sodišče je v odločitvi ugodilo pritožniku in s tem postavilo jasne meje posegov v tajnost občil. Posebej je tudi poudarilo stališče, da je treba predmet varstva komunikacijske zasebnosti razlagati širše, in sicer tako, da le-ta vključuje tudi prometne podatke, ki so sestavni del komunikacije. To razumevanje prometnih podatkov je bilo v nekaterih pravnih krogih sicer nekoliko kritizirano, dejstvo pa je, da je skladno z razsodbo Evropskega sodišča za človekove pravice iz leta 1984, ko je ESČP v primeru Malone proti Veliki Britaniji (Malone v. Velika Britanija, odločba z dne 2. 8. 1984) zapisalo, da so prometni podatki integralni element telefonskih komunikacij. Ameriški pravni sistem ima do tega vprašanja nekoliko drugačno stališče, saj je Vrhovno sodišče ZDA leta 1979 v primeru Smith proti Maryland (Smith v. Maryland, 242 U.S. 735 (1979)) presodilo, da prometni podatki o telefonskih pogovorih niso zaščiteni s četrtim amandmajem in s tem uvedlo ločevanje prometnih podatkov od same vsebine komunikacije (Kovačič, 2009).

Iz omenjene razsodbe Ustavnega sodišča je postalo jasno razvidno, da varstvo komunikacijske zasebnosti obsega tudi izpise iz telefona in SIM kartice oziroma podatke shranjene v naročnikovi terminalni napravi. S tem je Ustavno sodišče posredno opozorilo, da je pravna ureditev tovrstnih posegov v zasebnost v času novih tehnologij zastarela in potrebna dopolnitve. Zato se je v začetku leta 2009 pričel pripravljati predlog sprememb Zakona o kazenskem postopku, ki naj bi zapolnil novo »odkrito« pravno praznino. Novela je bila po besedah Mateja Kovačiča, ki je aktivno sodeloval pri posodobitvi Zakona o kazenskem postopku,

pripravljena na podlagi tehtnih strokovnih razmislekov in ob upoštevanju varstva človekovih pravic. Prav tako poleg visokih standardov varstva zasebnosti dokončno postavlja tudi ustrezne standarde glede uporabe načel digitalne forenzike v kazenskih postopkih (Kovačič, 2009).

219.a/1 člen ZKP-J

(1) Preiskava elektronskih in z njo povezanih naprav ter nosilcev elektronskih podatkov (elektronska naprava), kot so telefon, telefaks, računalnik, disketa, optični mediji in spominske kartice, se zaradi pridobitve podatkov v elektronski obliki lahko opravi, če so podani utemeljeni razlogi za sum, da je bilo storjeno kaznivo dejanje in je podana verjetnost, da elektronska naprava vsebuje elektronske podatke:
– na podlagi katerih je mogoče osumljenca ali obdolženca identificirati, odkriti ali prijeti ali odkriti sledove kaznivega dejanja, ki so pomembni za kazenski postopek, ali
– ki jih je mogoče uporabiti kot dokaz v kazenskem postopku.

Člen najprej jasno opredeli elektronske naprave, ki vključujejo tudi nosilce elektronskih podatkov, pri čemer se ne omejuje na trenutno znane naprave, pač pa je za definicijo elektronske naprave bistveno, da vsebuje elektronske podatke. Nadalje je določen namen preiskave, ki je predvsem pridobiti podatke v elektronski obliki. S tem se zakon jasno osredotoča na zaseg podatkov in ne več na zaseg nosilcev podatkov. Za kazensko preiskavo so namreč bistveni elektronski podatki, ki imajo tudi status dokaza, ne pa konkreten fizični medij, na katerem se nahajajo. Določba opredeljuje kdaj je preiskava elektronskih naprav dopustna in pri tem podaja ustrezen zahtevani dokazni standard (Kovačič 2009).

219.a/2 člen ZKP-J

(2) Preiskava se opravi na podlagi vnaprejšnje pisne privolitve imetnika ter policiji znanih in dosegljivih uporabnikov elektronske naprave, ki na njej utemeljeno pričakujejo zasebnost (uporabnik), ali na podlagi obrazložene pisne odredbe sodišča, izdane na predlog državnega tožilca. Če se preiskava opravi na podlagi odredbe sodišča, se izvod te odredbe pred začetkom preiskave izroči imetniku oziroma uporabniku elektronske naprave, ki naj se preišče.

V drugem odstavku 219.a člena novela ZKP določa pravno podlago za izvedbo preiskave. To je lahko soglasje imetnika oziroma vseh znanih in dosegljivih uporabnikov, ki na tej napravi utemeljeno pričakujejo zasebnost ali obrazložena pisna odredba sodišča. Prva možnost bo uporabna v vseh tistih primerih, ko gre za elektronske dokaze na napravi v lasti žrtve kaznivega dejanja, npr. za preiskavo računalnika na katerega je nekdo vdrl ali iz njega ukradel neke podatke. Pomembno je, da se v tem primeru zahteva soglasje vseh znanih in dosegljivih uporabnikov in ne zgolj lastnika ali trenutnega imetnika naprave. Dikcija, ki bi predvidevala zgolj soglasje imetnika ali lastnika naprave bi lahko privedla do zlorab, zlasti v primeru podjetij ali posameznikov, ki so lastniki poštnih strežnikov. Ideja je sicer povzeta iz tuje sodne prakse, konkretno iz primera Steve Jackson Games v. U.S. Secret Service (Steve Jackson Games v. U.S. Secret Service, 36 F.3d

457 (1994)), kjer je Vrhovno sodišče ZDA ugotovilo, da zaplemba in uničenje elektronske pošte uporabnikov, ki niso ničesar osumljeni, uporabljajo pa isti strežnik kot osumljenec, predstavlja kršitev in je zato nedopustna. Druga možnost, uporaba obrazložene pisne odredbe sodišča, izdane na predlog državnega tožilca, pa bo prišla prav v primerih »klasičnih« kazenskih preiskav, ob čemer je seveda upoštevana zgoraj omenjena zahteva Ustavnega sodišča po predhodnem dovoljenju sodišča za poseg v komunikacijsko zasebnost (Kovačič 2009).

219.a/3 člen ZKP-J

(3) Predlog in odredba o preiskavi elektronske naprave morata vsebovati:
– podatke, ki omogočajo identifikacijo elektronske naprave, ki se bo preiskala;
– utemeljitev razlogov za preiskavo;
– opredelitev vsebine podatkov, ki se iščejo;
– druge pomembne okoliščine, ki narekujejo uporabo tega preiskovalnega dejanja in določajo način njegove izvršitve.

Tretji odstavek 219.a člena določa elemente, ki jih morata vsebovati predlog in odredba o preiskavi elektronske naprave. Eden izmed zahtevanih elementov je tudi opredelitev vsebine podatkov, ki se iščejo. Gre za pomembno določbo, ki odpira možnosti za modernizacijo razumevanja elektronske naprave kot listine. V dosedanji praksi je za pregled npr. računalnika veljalo razumevanje računalnika kot spisa. Pregled tako ni bil osredotočen samo na določene podatke, pač pa je preiskava lahko obsegala preiskavo celotnega računalnika. S tem se je vzpostavila analogija z zaprtim prostorom, kjer velja, da ko je odredba za preiskavo odobrena, je na tej podlagi mogoče preiskati celoten zaprt prostor in pri tem v kazenskem postopku uporabiti vse dokaze v zvezi s kaznivimi dejanji, ki jih organi pri tem odkrijejo (Kovačič 2009).

219.a/4 in 219.a/5 člen ZKP-J

(4) Če se preiskava elektronske naprave odredi v odredbi za hišno ali osebno preiskavo, za izdajo tega dela odredbe in njeno izvršitev veljajo pogoji in postopki iz tega člena. V tem primeru tudi predlog za hišno ali osebno preiskavo poda državni tožilec.
(5) Izjemoma, če pisne odredbe ni mogoče pravočasno pridobiti ter če obstaja neposredna in resna nevarnost za varnost ljudi ali premoženja, lahko preiskovalni sodnik na ustni predlog državnega tožilca odredi preiskavo elektronske naprave z ustno odredbo. O predlogu državnega tožilca in odredbi preiskovalni sodnik izdela uradni zaznamek. Pisna odredba mora biti izdana najpozneje v dvanajstih urah po izdaji ustne odredbe, sicer policija, ki je odredbo izvršila, zapisniško uniči ali izbriše shranjene ali kopirane podatke in o tem v osmih dneh obvesti preiskovalnega sodnika, državnega tožilca in imetnika oziroma uporabnika elektronske naprave, če je znan.

219.a/6 člen ZKP-J

(6) Imetnik oziroma uporabnik elektronske naprave mora omogočiti dostop do naprave, predložiti šifrirne ključe oziroma šifrirna gesla in pojasnila o uporabi naprave, ki so potrebna, da se doseže namen preiskave. Če noče tako ravnati, se sme kaznovati oziroma zapreti po določbi drugega odstavka 220. člena tega zakona, razen če gre za osumljenca ali obdolženca ali osebo, ki ne sme biti zaslišana kot priča (235. člen) ali se je v skladu s tem zakonom odrekla pričevanju (236. člen).

6. odstavek 219.a člena uvaja pomembne varovalke pri varstvu človekovih pravic. Odstavek sicer določa, da mora imetnik oziroma uporabnik elektronske naprave na zahtevo preiskovalcev predložiti šifrirne ključe in pojasnila o uporabi naprave, za osebe, ki tega ne bi želele storiti, pa so predvidena tudi prisilna dejanja (celo zapor). Vendar je ob tem potrebno poudariti, da ta določba velja samo za t.i. priče v postopku, ne pa tudi za osumljence ali obdolžence, njihove zakonce in bližnje krvne sorodnike (skratka, vse osebe iz 236. člena ZKP) oziroma osebe, ki ne smejo biti zaslišane kot priče (osebe iz 235. člena ZKP), s čimer se izrecno upošteva privilegij zoper samoobtožbo (Kovačič 2009).

219.a/7 in 219.a/8 člen ZKP-J

(7) Preiskava se opravi tako, da se ohrani integriteta izvirnih podatkov in možnost njihove uporabe v nadaljnjem postopku. Preiskava mora biti opravljena na način, s katerim se v najmanjši možni meri posega v pravice oseb, ki niso osumljenci ali obdolženci, in varuje tajnost oziroma zaupnost podatkov ter ne povzroča nesorazmerna škoda.

(8) Preiskavo opravi strokovno usposobljena oseba. O preiskavi se napravi zapisnik, ki med drugim obsega:

– identifikacijo elektronske naprave, ki je bila pregledana;

– datum ter uro začetka in konca preiskave oziroma ločeno za več preiskav, če preiskava ni bila opravljena v enem delu;

– morebitne sodelujoče in navzoče osebe pri preiskavi;

– številko odredbe in sodišče, ki jo je izdalo;

– način izvedbe preiskave;

– ugotovitve preiskave in druge pomembne okoliščine.

Bistvena novost, ki jo prinašata 7. in 8. odstavek 219.a člena ZKP je uzakonitev oziroma zahteva po spoštovanju postopkov digitalne forenzike pri preiskavi. Ob tem se izrecno zahteva zagotovitev integritete podatkov ter vodenje ustrezne dokumentacije (t.i. skrbniške verige, ang. chain of custody) v obliki zapisnika. Le po pravilih forenzične stroke zaseženi podatki, ki ohranijo svojo integriteto, imajo namreč lahko status veljavnega dokaza.

Pomembno določilo je tudi tisto, ki določa, da mora biti preiskava opravljena na način, s katerim se v najmanjši možni meri posega v pravice oseb, ki niso osumljenci ali obdolženci, in varuje tajnost oziroma zaupnost podatkov ter ne povzroča nesorazmerna škoda. Določba je pomembna zlasti v primeru preiskav na večuporabniških sistemih, hkrati pa preiskovalcem nalaga, da se potrudijo podatke zaseči čim hitreje in na

način, ki je kar najmanj obremenilen za lastnika naprave. V nasprotnem primeru bi se namreč lahko zgodilo, da žrtve kiberkriminala kaznivih dejanj ne bi želele prijavljati, saj bi se lahko bale, da jim bo preiskava povzročila dodatno škodo v obliki poškodovanja naprave ali onemogočenja njene uporabe za čas trajanja kazenskega postopka. Preveč restriktivno postopanje policije pri preiskovanju elektronskih naprav, bi namreč lahko žrtvam povzročalo dodatno (poslovno) škodo, posledica pa bi bil lahko povečan upad interesa za prijavo kaznivih dejanj iz področja računalniške kriminalitete (Kovačič 2009).

219.a/9, 219.a/10 in 219.a/11 člen ZKP-J

(9) Če se pri preiskavi najdejo podatki, ki niso v zvezi s kaznivim dejanjem, zaradi katerega je bila preiskava odrejena, temveč kažejo na drugo kaznivo dejanje, za katero se storilec preganja po uradni dolžnosti, se zasežejo tudi ti. To se navede v zapisnik in takoj sporoči državnemu tožilcu, da začne kazenski pregon. Ti podatki pa se takoj uničijo, če državni tožilec spozna, da ni razloga za kazenski pregon in tudi ne kakšnega drugega zakonskega razloga, da bi se morali podatki vzeti. O uničenju se sestavi zapisnik.
(10) Če v tem členu ni določeno drugače, se za odreditev in izvršitev odredbe o preiskavi elektronske naprave smiselno uporabljajo določbe tretjega in četrtega odstavka 215. člena ter četrtega, petega in sedmega odstavka 216. člena tega zakona.
(11) Če je bila preiskava elektronske naprave opravljena brez odredbe sodišča ali v nasprotju z njo ali brez pisne privolitve iz drugega odstavka tega člena, sodišče svoje odločbe ne sme opreti na zapisnik o preiskavi in na tako pridobljene podatke.

223.a/1 člen ZKP-J

(1) Če se zaseže elektronska naprava (prvi odstavek 219.a člena) zaradi oprave preiskave, se podatki v elektronski obliki zavarujejo tako, da se shranijo na drug ustrezen nosilec podatkov na način, da se ohrani istovetnost in integriteta podatkov ter možnost njihove uporabe v nadaljnjem postopku ali se izdela istovetna kopija celotnega nosilca podatkov, pri čemer se zagotovi integriteta kopije teh podatkov. Če to ni mogoče, se elektronska naprava zapečati, če je mogoče, pa samo tisti del elektronske naprave, ki naj bi vseboval iskane podatke.

Prvi odstavek 223.a člena ZKP določa digitalno forenzična pravila za zaseg podatkov. Pri tem ni bistveno na katerem nosilcu podatkov se podatki nahajajo, bistveno je, da se ohrani istovetnost in integriteta podatkov. Šele če kopiranje podatkov iz elektronske naprave ni mogoče, je dovoljeno zaseči celotno napravo oziroma po možnosti samo tisti del, ki vsebuje iskane podatke.
Določba tako omogoča, da imetnik elektronske naprave le-to čim prej dobi vrnjeno nazaj (oziroma vsaj nekatere njene dele), hkrati pa preiskovalcem ni potrebno hraniti nepotrebnih naprav, pač pa lahko hranijo samo tisto, kar je za kazenski postopek pravzaprav bistveno – istovetne kopije podatkov (Kovačič 2009).

223.a/2 člen ZKP-J

(2) Če je bila elektronska naprava zasežena brez odredbe sodišča in je bila zaradi zavarovanja podatkov izdelana njihova kopija, vendar sodišče v dvanajstih urah ni izdalo odredbe za preiskavo po petem odstavku 219.a člena tega zakona oziroma ni bila dana privolitev po drugem odstavku 219.a člena tega zakona, policija zapisniško trajno uniči izdelano kopijo in o tem v osmih dneh pisno obvesti preiskovalnega sodnika, državnega tožilca in imetnika oziroma uporabnika elektronske naprave, če je znan.

223.a/3 člen ZKP-J

(3) Imetnik, uporabnik, upravljavec ali skrbnik elektronske naprave oziroma tisti, ki ima do nje dostop, mora na zahtevo organa, ki jo je zasegel, takoj ukreniti, kar je potrebno in je v njegovi moči, da se onemogoči uničenje, spreminjanje ali prikrivanje podatkov. Če noče tako ravnati, se sme kaznovati oziroma zapreti po določbi drugega odstavka 220. člena tega zakona, razen če gre za osumljenca, obdolženca ali osebo, ki ne sme biti zaslišana kot priča (235. člen) ali se je v skladu s tem zakonom odrekla pričevanju (236. člen).

Podobno kot v 219.a/6 členu, ki opredeljuje dolžnost izročitve šifrirnih ključev in pojasnil o delovanju naprave, tudi ta člen opredeljuje dolžnosti oseb, ki imajo do naprave dostop oziroma z njo upravljajo. Dolžnost teh oseb (z enakimi izjemami kot v 219.a/6 členu) je predvsem, da takoj ukrenejo vse potrebno in kar je v njihovi moči, da se zavarujejo dokazi oziroma da se onemogoči uničenje, spreminjanje ali prikrivanje podatkov. Tipičen primer uporabe določbe tega člena bi bila npr. zahteva za zavarovanje dnevniških zapisov, ki se v informacijskih sistemih hranijo določen čas, po preteku določenega časa pa se starejši zapisi izbrišejo (Kovačič 2009).

223.a/4 in 223.a/5 člen ZKP-J

(4) Imetnika naprave se povabi, naj bo sam, njegov zastopnik, odvetnik ali strokovnjak navzoč pri zavarovanju podatkov po prvem odstavku tega člena. Če se ne odzove vabilu, če je odsoten ali če ni znan, se zavarovanje podatkov in izdelava istovetne kopije opravi v njegovi nenavzočnosti. Zavarovanje podatkov opravi ustrezno usposobljena oseba.

(5) Pri zavarovanju podatkov se v zapisnik zapiše tudi kontrolna vrednost, oziroma se na drug ustrezen način v zapisniku zagotovi možnost naknadnega preverjanja istovetnosti in integritete zavarovanih podatkov. Izvod zapisnika se izroči osebi iz prejšnjega odstavka, ki je bila navzoča pri zavarovanju podatkov.

Navedeni odstavek daje imetniku naprave možnost, da je prisoten pri zavarovanju oziroma zasegu podatkov (ne pa tudi pri sami preiskavi). Kopiranje podatkov po pravilih digitalno forenzične stroke namreč zahteva tudi izračun t.i. kontrolne vsote. Gre za poseben postopek, ki na podlagi matematičnega algoritma izračunavanja kontrolnih vsot (ang. hash values) izračuna unikatni digitalni prstni odtis podatkov v obliki števila. Za kopijo podatkov, ki ima enako kontrolno vsoto velja, da je istovetna originalnim podatkom. Če pa pride do kakršnekoli pooblaščene ali nepooblaščene, namerne ali nenamerne spremembe podatkov, se kontrolna vsota teh podatkov spremeni in ne moremo več govoriti o istovetni kopiji, posledično pa tak dokaz

ni več veljaven. Z izračunom kontrolne vsote in prisotnostjo imetnika naprave se zagotovi, da je zagotovljena integriteta zaseženih podatkov in da je kasneje mogoče dokazati ali je prišlo do spremembe podatkov (npr. podtikanja ali prikrivanja dokazov s strani preiskovalcev ali drugih oseb) ali ne. Ker gre seveda za postopek, pri katerem je potrebno določeno tehnično znanje, je v zakonu imetniku naprave dana možnost, da k zavarovanju dokazov povabi tudi strokovnjaka, ki mu zaupa (Kovačič 2009).

223.a/6 ZKP-J

(6) Zaseg in zavarovanje podatkov morata biti opravljena na način, s katerim se v najmanjši možni meri posega v pravice oseb, ki niso osumljenci ali obdolženci, in varuje tajnost oziroma zaupnost podatkov ter se ne povzroča nesorazmerna škoda zaradi nezmožnosti uporabe elektronske naprave.
Podobno kot v 219.a/7 členu je tudi tukaj navedena varovalna določba glede zasega in zavarovanja podatkov.

223.a/7 ZKP-J

(7) Kopije zaseženih podatkov se hranijo, dokler je to potrebno za postopek. Elektronska naprava se hrani, dokler podatki niso shranjeni na način, ki zagotovi istovetnost in integriteto zaseženih podatkov, vendar ne več kakor tri mesece od dneva pridobitve. Če izdelava takšne kopije podatkov ni mogoča, se elektronska naprava ali del elektronske naprave, ki vsebuje iskane podatke, hrani, dokler je to potrebno za postopek, vendar ne več kakor šest mesecev od dneva pridobitve, razen če je bila zasežena elektronska naprava uporabljena za izvršitev kaznivega dejanja oziroma je sama elektronska naprava dokaz v kazenskem postopku.

Precejšnjo novost predstavlja tudi sedmi odstavek 223.a člena. Določa namreč pravila glede hrambe kopije podatkov in vračanja pridobljene elektronske naprave. Osnovno načelo, ki ga uveljavlja zakon je, da se sama naprava čim hitreje vrne imetniku, kopija podatkov pa se hrani dokler je to potrebno za kazenski postopek. Vsekakor je napravo potrebno shraniti vsaj dokler podatki niso v skladu s pravili digitalno forenzične stroke ustrezno zaseženi (prekopirani). To obdobje pa lahko traja največ tri mesece, nato pa se naprava imetniku vrne. Seveda pa je mogoča tudi situacija, ko kopije digitalnih podatkov ni mogoče izdelati, ko gre npr. za kakšno posebno elektronsko napravo, ki ne omogoča prenosa podatkov na zunanji medij. V tem primeru je uveljavljeno načelo, da se elektronska naprava oziroma – če je mogoče – samo njen del, hrani dokler je to potrebno za postopek. Tudi tukaj zakon uvaja varovalko – hramba je omejena na največ šest mesecev – a s pridržkom: razen če je bila zasežena elektronska naprava uporabljena za izvršitev kaznivega dejanja oziroma je sama elektronska naprava dokaz v kazenskem postopku. Zakon torej uveljavlja načelo, da se elektronska naprava čim prej po zasegu podatkov na njej vrne imetniku, saj za kazenski pregon ni bistven nosilec podatkov, pač pa vsebina podatkov (Kovačič 2009).

223.a/8 člen ZKP

(8) Kopije podatkov, pridobljene v skladu z določbami tega člena, ki se ne nanašajo na kazenski pregon in za katere ni kakšnega drugega zakonskega razloga, da bi se smeli hraniti (498. člen), se izločijo iz spisa, če je to mogoče in se zapisniško uničijo, o čemer se v osmih dneh obvestijo preiskovalni sodnik, državni tožilec in imetnik elektronske naprave.

INFORMACIJSKA ZASEBNOST (VARSTVO OSEBNIH PODATKOV)

Koncept varstva osebnih podatkov v Sloveniji temelji na določbi 38. člena Ustave RS, po kateri je varstvo osebnih podatkov v državi ena izmed ustavno zagotovljenih človekovih pravic in temeljnih svoboščin. Določba 38. člena Ustave RS zagotavlja varstvo osebnih podatkov, prepoveduje uporabo osebnih podatkov v nasprotju z namenom njihovega zbiranja, vsakomur zagotavlja pravico do seznanitve z zbranimi osebnimi podatki, ki se nanašajo nanj, ter pravico do sodnega varstva ob njihovi zlorabi.
Za normativno urejanje varstva osebnih podatkov je zlasti pomemben drugi odstavek 38. člena Ustave RS, v katerem je določeno, da zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa zakon (splošen - sistemski[105] zakon in področni[106] zakoni). Gre za t.i. »obdelovalni model« z določenimi pravili za urejanje dopustne obdelave osebnih podatkov na zakonski ravni. Po tem modelu je na področju obdelave osebnih podatkov prepovedano vse, razen tistega, kar je z zakonom (na področju zasebnega sektorja tudi z osebno privolitvijo posameznika) izrecno dovoljeno. Vsaka obdelava osebnih podatkov namreč pomeni poseg v ustavno varovano človekovo pravico do varstva osebnih podatkov. Tak poseg je zato dopusten, če je v zakonu določno opredeljeno, kateri osebni podatki se smejo obdelovati, jasno pa mora biti določen tudi namen obdelave osebnih podatkov, zagotovljeno mora biti ustrezno varstvo in zavarovanje osebnih podatkov. Namen obdelave osebnih podatkov mora biti ustavno dopusten, obdelovati pa se smejo le tisti osebni podatki, ki so primerni in nujno potrebni za uresničitev zakonsko opredeljenega in ustavno dopustnega namena (Informacijski pooblaščenec 2008, 21).

Varovanje osebnih podatkov je zavarovano s kazenskim zakonikom, ki v 143. členu prepoveduje zlorabo osebnih podatkov in sicer za vsakogar, ki v nasprotju z zakonom uporabi osebne podatke ter za vsakogar, ki

[105] Ureditev varstva osebnih podatkov v sistemskem zakonu je potrebna zaradi enotne določitve načel, pravil in obveznosti ter zaradi zapolnitve pravnih praznin, ki bi lahko nastale v področnih zakonih. Poleg tega ni potrebno, da bi se npr. definicije, obveznosti in ukrepi v zvezi z zavarovanjem osebnih podatkov, katalogi zbirk osebnih podatkov, registracijo zbirk osebnih podatkov v zvezi s pravicami posameznika do seznanitve s podatki, ki se nanašajo nanj, ter vprašanja glede nadzora in pristojnosti nadzornega organa vedno predpisovali tudi v področnih zakonih. Namen sistemskega zakona torej ni podrobnejše predpisovanje načinov obdelave osebnih podatkov po posameznih področjih, temveč predvsem to, da se v njem enotno določijo splošne pravice, obveznosti, načela in ukrepi, s katerimi se preprečujejo neustavni, nezakoniti in neupravičeni posegi v zasebnost in dostojanstvo posameznika pri obdelavi osebnih podatkov (Informacijski pooblaščenec 2008, 21).

[106] Področni zakoni morajo jasno določati, katere zbirke osebnih podatkov se bodo vzpostavile in vodile na posameznem področju, vrste osebnih podatkov, ki jih bodo posamezne zbirke vsebovale, način zbiranja osebnih podatkov, morebitne omejitve pravic posameznika, zlasti pa namen obdelave zbranih osebnih podatkov. Z vidika varstva posameznika je zelo priporočljivo, da se v področnem zakonu določi tudi čas shranjevanja osebnih podatkov (Informacijski pooblaščenec 2008, 21).

vdre v računalniško vodeno zbirko podatkov z namenom, da bi zase ali koga drugega pridobil kakšen osebni podatek. Poleg tega 221. člen prepoveduje vdor v zaščiteno bazo podatkov, spreminjanje in kopiranje podatkov iz nje ter vnašanje virusov (Kovačič 2003, 84).
Še bolj pomembno pravno varstvo osebnih podatkov pa zagotavljata Zakon o varstvu osebnih podatkov (ZVOP-1) in Zakon o telekomunikacijah (ZEKom).

Zakon o varstvu osebnih podatkov (ZVOP) je Državni zbor RS sprejel 15.7.2004, veljati pa je pričel s 1.1.2005. Sprejetje zakona je bilo potrebno predvsem zaradi vstopa Republike Slovenije v Evropsko Unijo in s tem povezane dolžnosti uskladitve varstva osebnih podatkov z določbami Direktive 95/46/ES Evropskega parlamenta in Sveta o zaščiti posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov. Julija 2007 je bila sprejeta novela ZVOP-1, to je Zakon o spremembah in dopolnitvah zakona o varstvu osebnih podatkov. ZVOP-1A pa je uvedel dve pomembni novosti, in sicer z vidika administrativnih razbremenitev upravljavcev osebnih podatkov ter predpisovanja določenih olajšav z vidika oblik dostopa posameznikov do njihovih osebnih podatkov. Novela je bistveno zožila krog zavezancev za vpis zbirk osebnih podatkov v register in je prinesla določene pozitivne rešitve, predvsem olajšave za posameznike, na katere se osebni podatki nanašajo (Informacijski pooblaščenec 2008, 22).

Zakon o varovanju osebnih podatkov pa ni le sistemski zakon, ampak je v svojem VI. delu tudi t.i. področni zakon, ki s precej natančno določitvijo pravic, obveznosti, načel in ukrepov upravljavcem osebnih podatkov daje neposredno zakonsko podlago za obdelavo osebnih podatkov na področju neposrednega trženja, videonadzora, biometrije, evidentiranja vstopov v prostore in izstopov iz njih ter strokovnega nadzora (Informacijski pooblaščenec 2008, 21).
Zakon govori izključno o osebnih podatkih[107], torej o podatkih, ki kažejo na lastnosti, stanje ali razmerja posameznika, med drugim pa določa tudi pogoje za zakonito obdelavo osebnih podatkov, pravice posameznika v zvezi z njegovimi osebnimi podatki, pogoje za iznos podatkov iz države ter nadzor nad varstvom osebnih podatkov (Kovačič 2003, 84).
8. člen zakona določa, da se smejo osebni podatki zbirati, shranjevati in obdelovati samo, če je tako določeno z zakonom (in ne s podzakonskimi predpisi) ali če je za obdelavo določenih osebnih podatkov podana osebna privolitev posameznika. Osebe o katerih se zbirajo osebni podatki, morajo biti predhodno seznanjene z namenom zbiranja, osebni podatki pa se smejo zbirati samo za ta namen. Osebni podatki se lahko načeloma shranjujejo in uporabljajo samo toliko časa, kolikor je potrebno za dosego tega namena, nato pa jih je treba izbrisati ali blokirati.
20. člen v zvezi s povezovanjem osebnih podatkov iz različnih baz prepoveduje uporabo istega

[107] Med osebne podatke spadajo identifikacijski podatki (ime in priimek, rojstni datum, EMŠO, davčna številka, naslov bivališča, prstni odtis, fotografija), izobrazba, zaposlitev, podatki o socialnem in ekonomskem položaju, podatki o dejavnostih v prostem času, podatki o družinskih razmerjih, idr. Podatki o političnih in verskih prepričanjih, podatki o rasnem in drugem izvoru, podatki o kazenskih ovadbah, zdravstveni podatki, podatki o spolnem vedenju in podatki o pripadnosti sindikatu pa morajo biti še posebej zavarovani (Volk v Kašnik 2006, 42).

povezovalnega znaka v zbirkah podatkov s področja javne varnosti, državne varnosti, obrambe države, pravosodja in zdravstva, sicer pa velja, da je takšno povezovanje dovoljeno le v posebnih primerih, ki jih določa zakon (npr. za odkritje in pregon kaznivega dejanja po uradni dolžnosti, da se zavaruje življenje ali telo posameznika ali da se zagotovi izvajanje nalog obveščevalnih in varnostnih organov) oziroma če se je posameznik s tem predhodno pisno strinjal. Poleg tega mora upravljavec zbirke osebnih podatkov v najmanj 15 dneh po prejemu zahteve posamezniku brezplačno omogočiti vpogled v njegove osebne podatke ter njihovo prepisovanje, oziroma mu na podlagi zahteve v 30 dneh posredovati njegov izpis. Če tega ne stori, ga mora v tem času pisno obvestiti o razlogih za to (31. člen) (Kovačič 2003, 85).

Če posameznik dokaže, da so bili osebni podatki zbrani nezakonito, jih mora upravljavec osebnih podatkov izbrisati oziroma jih dopolniti ali popraviti, če se izkaže, da so nepopolni, netočni ali zastarani. Tudi te stroške nosi upravljavec zbirke osebnih podatkov. Poleg tega mora upravljavec zbirke osebnih podatkov za vsako zbirko zagotoviti poseben katalog, v katerem mora biti med drugim natančno zapisano, kateri osebni podatki se zbirajo in kako, namen njihove uporabe in čas njihovega shranjevanja, uporabnike zbranih podatkov, opis zavarovanja osebnih podatkov itd. (26. člen). Informacijski pooblaščenec, ki je pristojen za varstvo osebnih podatkov, vodi in vzdržuje register zbirk osebnih podatkov, podatke za ta register pa mora Informacijskemu pooblaščencu prav tako posredovati upravljavec zbirke (27. člen) (Kovačič 2003, 85).

Iznos osebnih podatkov iz države je mogoč samo v tiste države, ki imajo urejeno varovanje osebnih podatkov (63. člen), razen v nekaterih posebnih primerih (npr. če se posameznik pisno strinja z iznosom podatkov in je seznanjen s posledicami), ki jih v 70. členu določa Zakon o varovanju osebnih podatkov. Prenašanje nekaterih občutljivih vrst osebnih podatkov (tistih, ki se nanašajo na rasno in drugo poreklo, politična, verska in druga prepričanja, pripadnost sindikatu, spolno vedenje, kazenske obsodbe in zdravstvene podatke) prek telekomunikacijskih omrežji pa 14. člen zakona dovoljuje samo, če so podatki zavarovani s kriptografskimi metodami in digitalnim podpisom. Zakon za izjemne primere s področja nacionalnega varnosti, obrambe, javne varnosti, preprečevanja, odkrivanja in preganjanja kaznivih dejanj, ki pa morajo biti določeni z zakonom, lahko omeji pravice posameznika do vpogleda ali prepisa izbranih podatkov. Poleg tega določa tudi inšpekcijsko nadzorstvo nad izvajanjem določb tega zakona, Informacijski pooblaščenec pa je dolžan državnemu zboru predložiti letno poročilo o svojem delu (Kovačič 2003, 86).

Sicer pa se pri obdelavi osebnih podatkov v Republiki Sloveniji poleg Ustave, Zakona o varovanju osebnih podatkov, Zakona o Informacijskem pooblaščencu in zakonov, ki podrobneje predpisujejo obdelavo osebnih podatkov na posameznem področju, neposredno uporabljajo tudi določbe Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov. Ta je bila ratificirana in objavljena leta 1994. Namen omenjene konvencije Sveta Evrope je na ozemlju vsake pogodbenice vsakemu posamezniku, ne glede na njegovo državljanstvo in prebivališče, zagotoviti spoštovanje njegovih pravic in temeljnih svoboščin ter v okviru tega še posebej spoštovanje pravice do zasebnosti v primeru avtomatske obdelave njegovih osebnih podatkov (Informacijski pooblaščenec 2008, 21). Konvencija in ZVOP-1 določata, da je v zvezi z zbiranjem in obdelavo osebnih podatkov prepovedano vse, kar ni izrecno dovoljeno (Šturm in drugi

2002, 411). Konvencija v 5. členu določa, da osebni podatki, ki se avtomatsko obdelujejo:

a) morajo biti pridobljeni in obdelani pošteno in zakonito;
b) smejo biti shranjeni za določene in zakonite namene in ne smejo biti uporabljeni na način, ki ni združljiv s temi nameni;
c) morajo biti primerni, ustrezni in ne smejo biti pretirani glede na namene, za katere so bili shranjeni;
d) morajo biti točni in, kjer je to nujno, do dneva ažurni;
e) smejo biti shranjeni v obliki, ki dopušča identifikacijo posameznika, na katerega se nanašajo podatki, le toliko časa, kot je to potrebno za namene, zaradi katerih so bili shranjeni.

Najpomembnejši mednarodni standard glede zagotavljanja varstva osebnih podatkov in zasebnosti pa predstavljata dva predpisa Evropske Unije: Direktiva 95/46/EC o varstvu posameznikov pri obdelovanju osebnih podatkov in prostem gibanju takšnih podatkov in Direktiva 97/66/EC o obdelavi osebnih podatkov in varstvu zasebnosti v telekomunikacijskem sektorju (Klemenčič 2003, 128).

Prav tako pomemben za urejanje pravice do informacijske zasebnosti oziroma varstva osebnih podatkov je Zakon o elektronskih komunikacijah (ZEKom). 2. člen zakona med drugim poudarja, da je namen zakona varstvo pravic posameznikov. To je nenazadnje razvidno iz X. poglavja, ki je v celoti posvečeno zaščiti tajnosti in zaupnosti elektronskih komunikacij (101. do 112. člena).
Zakon o elektronskih komunikacijah je pomemben tudi zato, ker zagotavlja varnost vsebine sporočila, prometnih podatkov in identifikacije udeležencev. Zakon prav tako omejuje obseg informacij, ki so povezane s komunikacijo in ki jih lahko operater omrežji zbira, shranjuje ali obdeluje, predvsem pa omejuje posredovanje teh informacij tretjim osebam (Klemenčič 2003, 122).
Prav tako ZEKom od operaterjev omrežij zahteva določene varnostne ukrepe za zaščito podatkov pred vdori tretjih nepovabljenih oseb in obenem postavlja osnovna pravila o posegu pooblaščenih državnih organov v pravico do tajnosti občil. Pri tem državnim organom pod določenimi pogoji dovoljuje vpogled v identifikacijske in prometne podatke kot tudi nadzor elektronskih komunikacij v realnem času. Od operaterjev zahteva zagotovitev in namestitev ustrezne programske opreme za zagotovitev nadzora telekomunikacijskega prometa (Klemenčič 2003, 123).
Pomemben je tudi 104. člen zakona, ki določa, da lahko operater prometne podatke, ki se nanašajo na naročnike ali uporabnike, uporablja za trženje svojih storitev le na podlagi naročnikovega ali uporabnikovega predhodnega soglasja. V 106. členu pa ZEKom ureja področje varstva lokacijskih podatkov, ki ga predhodni Zakon o telekomunikacijah ni ustrezno urejal.
Poudariti velja, da je državni zbor na seji 18. decembra 2009 sprejel novelo Zakona o elektronski komunikacijah, ki vnaša nekaj sprememb. Najpomembnejša je zagotovo skrajšan rok za obvezno hrambo prometnih podatkov[108]. Direktiva o obvezni hrambi prometnih podatkov 2006/24/ES, ki jo je v Zakonu o

[108] Vsako komunikacijo lahko delimo na dva dela – vsebino komunikacije in prometne podatke. Pri telefonskem pogovoru je vsebina komunikacije pogovor (poseg v vsebino komunikacije pa prisluškovanje), prometni podatki (ali

elektronskih komunikacijah sprejela tudi Slovenija, zahteva obvezno hrambo prometnih podatkov telefonskih in internetnih komunikacij (vključno z naslovi elektronske pošte) ter podatkov o lokacijah mobilnih telefonov, za čas hrambe pa določa od 6 do 24 mesecev. Slovenija je v ZEKom najprej uveljavila obvezno hrambo prometnih podatkov za maksimalno obdobje dveh let. V skladu z novelo ZEKom pa se je čas hrambe prometnih podatkov na področju telefonije skrajšal na 14 mesecev, hramba internetnih prometnih podatkov pa na 8 mesecev.

Druga pomembnejša novost[109] zadeva posredovanje prometnih in lokacijskih podatkov v primerih varovanja življenja in telesa. V primerih varstva življenjskih interesov posameznika je sedaj v skladu z noveliranim zakonom operater policiji na podlagi njene pisne zahteve (v nujnih primerih se lahko zahtevo pošlje tudi po telefaksu) dolžan posredovati zadnje lokacije opreme te osebe za mobilno komunikacijo (ID celice bazne postaje in njeno lokacijo, itd…). Vsekakor gre za precej občutljivo določbo, ki bi jo bilo mogoče tudi zlorabiti. Zato ima varovalko, in sicer je v primerih takih zahtev policija dolžna osebo, za katero je zahtevala in pridobila podatke o lokaciji, o tem pisno seznaniti (razen v izjemnih in v zakonu posebej določenih primerih).

Novost predstavlja tudi sprememba 107.č člena. Ta namreč predstavlja varovalko, saj določa, da morajo operaterji zagotoviti hrambo vseh posredovanj prometnih podatkov (policiji, SOVI ali OVS). Do sedaj je veljalo, da mora biti hramba teh posredovanj trajna, sedaj pa je ta rok skrajšan na 10 let.

Zakon nekaj več pristojnosti na področju nadzora in podajanja mnenj (npr. glede načina posredovanja določenih podatkov, itd.) nalaga tudi Informacijskemu pooblaščencu, s čimer se nad hrambo in uporabo prometnih podatkov vzpostavlja še nekoliko bolj temeljit nadzor. Nadzorno funkcijo pa predstavljajo tudi določbe, ki določajo, da morajo sodišča voditi ustrezne statistike o odredbah za dostop do prometnih podatkov in o številu posredovanj prometnih podatkov, zbrane statistike pa morajo posredovati Ministrstvu za pravosodje. To mora vsako leto najkasneje do 20. februarja pripraviti poročilo, ki se ga potem posreduje Evropski komisiji (Kovačič 2010).

Kljub nekaterim pozitivnim spremembam je Zakon o elektronskih komunikacijah še vedno nekoliko nepregleden, saj vsebuje t.i. „poslovni“ del (določbe, katerih namen je zagotavljanje učinkovite konkurence na trgu elektronskih komunikacij, ohranjanje učinkovite uporabe radiofrekvenčnega spektra in številskega prostora, zagotavljanje univerzalne storitve in varstvo pravic uporabnikov) ter t.i. “pravosodni” (*law enforcement*) del, ki vsebuje določbe o tajnosti komunikacij in obvezni hrambi prometnih podatkov. Kovačič (2010) meni, da bi bilo bolj smotrno, če bi vsak del predstavljal samostojen zakon, saj se v primeru trenutne

dejstva o okoliščinah komunikacije) pa so telefonska številka kličočega, telefonska številka klicanega, začetek in konec pogovora, v primeru mobilne telefonije morda še lokacija obeh udeležencev (Kovačič 2010).

[109] Določbo vsekakor velja pozdraviti, žal pa je potrebno dodati, da je bila sprejeta predvsem zato, ker v preteklosti nekateri operaterji v primerih pogrešanih oseb policiji niso hoteli sporočiti lokacije njihovih mobilnih telefonov. Pri tem so se napačno sklicevali na Zakon o varstvu osebnih podatkov, ki da jim takšno sporočanje prepoveduje, povsem spregledali pa so 12. člen ZVOP-1, ki dopušča obdelavo osebnih podatkov v primeru varovanja življenjskih interesov posameznika. (Po neuradnih podatkih je bil v nekaterih primerih pravi razlog žal lenoba, oz. nepripravljenost nekaterih operaterjev zagotoviti dežurstvo za posredovanje teh podatkov v času dela prostih dni in praznikov.) (Kovačič 2010).

ureditve lahko v praksi zaplete tudi pri tem, katero ministrstvo je pristojno za zakon (Ministrstvo za gospodarstvo ali Ministrstvo za pravosodje) in ali je le-to kompetentno za oba dela zakona ali ne.

INFORMACIJSKI POOBLAŠČENEC

Z Zakonom o dostopu do informacij javnega značaja (ZDIJZ) je bil ustanovljen samostojen in neodvisen državni organ, Pooblaščenec za dostop do informacij javnega značaja, ki je začel delovati 1. 9. 2003. Pooblaščenec za dostop do informacij javnega značaja je bil po izrecni zakonski določbi samostojen državni organ, imel pa je tudi status državnega funkcionarja, ki ga je imenoval Državni zbor na predlog predsednika Republike Slovenije. Pooblaščenec je imel strokovno službo, ki je bila z zakonom omejena do 15. 7. 2005 na dva svetovalca. Organizacijsko-administrativne naloge za Pooblaščenca pa je zagotavljalo (nekdanje) Ministrstvo za informacijsko družbo (Informacijski pooblaščenec).

1. 1. 2005 je stopil v veljavo Zakon o varstvu osebnih podatkov (ZVOP-1). Ta je v slovenski pravni red prenesel Direktivo 95/46/ES Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov in prostem pretoku osebnih podatkov. Po ZVOP-1 je bil predviden glavni državni nadzorni organ za varstvo osebnih podatkov; postopek za imenovanje naj bi se začel 1. julija 2005, državni nadzorni organ naj bi začel delovati najkasneje s 1. januarjem 2006. Državni nadzorni organ za varstvo osebnih podatkov je po ZVOP-1 samostojen državni organ. Pred uveljavitvijo ZVOP-1 pa je bil za varstvo osebnih podatkov pristojen Inšpektorat za varstvo osebnih podatkov, kot organ v sestavi Ministrstva za pravosodje. Inšpektorat je tako bil v razmerju do ministrstva organ prve stopnje. Po Zakonu o informacijskem pooblaščencu (ZInfP), ki je stopil v veljavo 31. 12. 2005, pa sta se Inšpektorat za varstvo osebnih podatkov in Pooblaščenec za dostop do informacij javnega značaja združila (Informacijski pooblaščenec).

Ob uveljavitvi Zakona o Informacijskem pooblaščencu je Pooblaščenec za dostop do informacij javnega značaja nadaljeval delo kot Informacijski pooblaščenec, ki je prevzel inšpektorje in druge uslužbence Inšpektorata za varstvo osebnih podatkov, pripadajočo opremo in sredstva. Hkrati je prevzel tudi vse nedokončane zadeve, arhive in evidence, ki jih je vodil Inšpektorat za varstvo osebnih podatkov. S tem so se pristojnosti organa, ki je skrbel za nemoteno izvajanje dostopa do informacij javnega značaja, močno spremenile in se razširile še na pravno področje varstva osebnih podatkov. Informacijski pooblaščenec je tako postal tudi samostojen in neodvisen državni nadzorni organ za varstvo osebnih podatkov. Delo je začel 1. januarja 2006. Predstojnika Informacijskega pooblaščenca, ki je funkcionar, imenuje Državni zbor RS na predlog predsednika RS. Organ Informacijski pooblaščenec od ustanovitve dalje vodi Nataša Pirc Musar (Informacijski pooblaščenec 2008, 1).

Vendar je potrebno opozoriti, da je združitev funkcij Pooblaščenca za dostop do informacij javnega značaja (kot pritožbenega organa na podlagi ZDIJZ) in Inšpektorata za varstvo osebnih podatkov (kot inšpekcijskega organa na podlagi ZVOP) v en sam organ problematična, saj omogoča konflikt interesov, ki zakonsko (še) ni odpravljen in se preprečuje le z aktivnim delovanjem Informacijske pooblaščenke. Kljub morebitnim pomislekom v Letnem poročilu Informacijskega pooblaščenca za leto 2008 (2008, 1) piše, da je trenutna ureditev poenotene prakse dveh organov primerljiva z ureditvijo v razvitih evropskih državah, prispevala pa naj bi k večjemu zavedanju pravice do zasebnosti in pravice vedeti.

Informacijski pooblaščenec je po 2. členu Zakona o Informacijskem pooblaščencu pristojen za (Informacijski pooblaščenec 2008, 1):

1) Odločanje o pritožbi zoper odločbo, s katero je organ zavrgel ali zavrnil zahtevo ali drugače kratil pravico do dostopa ali ponovne uporabe informacije javnega značaja ter v okviru postopka na drugi stopnji tudi za nadzor nad izvajanjem zakona, ki ureja dostop do informacij javnega značaja, in za nadzor na podlagi le-tega izdanih predpisov (pritožbeni organ na področju dostopa do informacij javnega značaja).
2) Inšpekcijski nadzor nad izvajanjem zakona in drugih predpisov, ki urejajo varstvo ali obdelavo osebnih podatkov oziroma iznos osebnih podatkov iz Republike Slovenije, ter opravljanje drugih nalog, ki jih določajo ti predpisi.
3) Odločanje o pritožbi posameznika, kadar upravljavec osebnih podatkov ne ugodi zahtevi posameznika glede njegove pravice do seznanitve z zahtevanimi podatki, do izpisov, seznamov, vpogledov, potrdil, informacij, pojasnil, prepisovanja ali kopiranja po določbah zakona, ki ureja varstvo osebnih podatkov.
4) Informacijski pooblaščenec lahko na Ustavnem sodišču Republike Slovenije vloži zahtevo po presoji ustavnosti zakonov, drugih predpisov ter splošnih aktov, izdanih za izvrševanje javnih pooblastil, če se pojavi vprašanje ustavnosti in zakonitosti v zvezi s postopkom, ki ga vodi – tako na področju dostopa do informacij javnega značaja kot varstva osebnih podatkov.

Na področju dostopa do informacij javnega značaja ima Informacijski pooblaščenec tudi pristojnosti, ki mu jih podeljuje Zakon o medijih (45. člen). Po Zakonu o medijih se zavrnilni odgovor organov zavezancev na vprašanje, ki ga zastavi predstavnik medija, šteje kot zavrnilna odločba. Molk organa zavezanca ob takem vprašanju pa je prekršek in hkrati tudi razlog za pritožbo. O pritožbi zoper zavrnilno odločbo odloča Informacijski pooblaščenec po določbah Zakona o dostopu do informacij javnega značaja. Informacijski pooblaščenec je tudi prekrškovni organ, pristojen za nadzor nad izvajanjem ZInfP, ZDIJZ v okviru pritožbenega postopka, določbe 45. člena Zmed in ZVOP-1 (Letno poročilo 2008, 1).

Informacijski pooblaščenec ima pristojnosti tudi na podlagi Zakona o elektronskih komunikacijah, in sicer

(Informacijski pooblaščenec 2008, 2):

- Izvajanje inšpekcijskega nadzora nad hrambo prometnih in lokacijskih podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javnih komunikacijskih omrežij ali storitev v skladu s 107.a do 107.e členom ZEKom (drugi odstavek 112. člena ZEKom);
- Na področju, ki ga nadzoruje, odločanje o prekrških za kršitev ZEKom in na podlagi le-tega izdanih predpisov kot prekrškovni organ v skladu z zakonom, ki ureja prekrške (147. člen ZEKom);
- Skrb za preprečevanje zlorab ter za pravilno izvajanje evropske Direktive o zasebnosti in elektronskih komunikacijah 2002/58/EC oziroma novega predloga direktive o hrambi telekomunikacijskih prometnih podatkov, ki je bila 15. 12. 2005 sprejeta v Bruslju na predlog ministrov držav članic.

Z vstopom Republike Slovenije v schengensko območje je Informacijski pooblaščenec prevzel tudi nadzor nad izvajanjem 128. člena Konvencije o izvajanju Schengenskega sporazuma in je neodvisen nadzorni organ za nadzor prenosa osebnih podatkov za namene te konvencije. Na podlagi 114. člena Schengenske konvencije namreč vsaka pogodbenica imenuje nadzorni organ, ki je po nacionalni zakonodaji pristojen za izvajanje neodvisnega nadzora podatkovnih zbirk nacionalnega dela schengenskega informacijskega sistema (SIS) in za preverjanje, da obdelava in uporaba podatkov, vnesenih v SIS, ne pomeni kršenja pravic oseb, na katere se podatki nanašajo. Za nadzor nad izvajanjem tehničnega podpornega dela SIS je glede varstva osebnih podatkov pristojen skupni nadzorni organ, za nadzor nacionalne podatkovne zbirke pa nacionalni nadzorni organ vsake pogodbenice – v Sloveniji je to Informacijski pooblaščenec (Informacijski pooblaščenec 2008, 2).