UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

SUZANA KAŠNIK

MENTOR: doc. dr. Gregor Petrič
SOMENTOR: asist. dr. Matej Kovačič

SODOBNE TEHNOLOGIJE NADZORA V SLOVENIJI

DIPLOMSKO DELO

Ljubljana, 2006

Zahvaljujem se mentorju dr. Gregorju Petriču in somentorju dr. Mateju Kovačiču za idejne vzpodbude in kritično oceno diplomske naloge.

Posebna zahvala velja tudi fantu Juretu, staršem in bratu za moralno podporo.

Univerza
v Ljubljani
Fakulteta
za družbene vede

Kardeljeva ploščad 5
1000 Ljubljana, Slovenija
telefon 01 58 05 128

IZJAVA O AVTORSTVU
diplomskega dela

Spodaj podpisani/-a SUZANA KAŠNIK, z vpisno številko 21016161,
rojen/-a 3.4.1981 v kraju SLOVENJ GRADEC, sem avtor/-ica diplomskega dela z naslovom:
SODOBNE TEHNOLOGIJE NADZORA V SLOVENIJI

S svojim podpisom zagotavljam, da:

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

V Ljubljani, dne 26.9.2006 Podpis avtorja/-ice: Suzana Kašnik

Sodobne tehnologije nadzora v Sloveniji

Sodobni nadzor konstantno narašča in ni usmerjen le v nadzorovanje posameznikov, temveč tudi na celotno populacijo. Zaradi tega so zmeraj bolj v ospredju vprašanja o zasebnosti ljudi, saj je s pomočjo vedno večje uporabe sodobnih tehnologij nadzora zasebnost posameznikov vedno bolj ogrožena. Državne in komercialne institucije si že lastijo veliko osebnih podatkov, videonadzoru se skorajda ni več mogoče izogniti, novim potnim listom se je pridružila še biometrija... Priča smo vedno novejšim, naprednejšim in bolj sofisticiranim tehnikam nadzorovanja ljudi. Veliki Brat nas ne le gleda, temveč nadzoruje na prijazen način, skrbi za našo varnost, zaradi česar se veliko ljudi nadzora sploh ne zaveda, še manj pa možnih posledic oz. zlorab. Na nezavedanje tehnologij nadzora kažejo tudi ugotovitve raziskave izvedene med študenti izbranih fakultet v Ljubljani. Čeprav ima Slovenija kar nekaj zakonov, ki med drugim skrbijo tudi za varovanje osebnih podatkov, lahko tudi pri nas opazimo različne zlorabe na tem področju, ki pa so velikokrat prav posledica nepoznavanja zakonov.

Ključne besede: tehnologije nadzora, družba nadzora, zasebnost, zavedanje nadzora, podatkovni nadzor.

Contemporary surveillance technologies in Slovenia

Contemporary surveillance grows constantly and focuses not only on individuals, but on entire population. Therefore more and more privacy issues are emerging. With the use of surveillance technologies our privacy is in threat. State and commercial institutions already owe a lot of personal data, CCTV is almost impossible to avoid, new passports have the biometrics data included… Surveillance techniques are getting more advanced and sophisticated. Big Brother not only watches, but also monitors in friendlier manner and takes care of our safety. Therefore many people aren't aware of surveillance technology and the possibilities of its abuse even less. Results of the research taken at selected faculties in Ljubljana also shows, that students are not aware of contemporary surveillance technology. Although Slovenia has several acts, that also regulates personal data, violations are often reported, but usually as a consequence of not knowing the acts.

Keywords: surveillance technology, surveillance society, privacy, surveillance awareness, dataveillance.

KAZALO

1. UVOD **8**

2. PREGLED OBRAVNAVANJA NADZORA **9**

2.1 GLAVNE OBLIKE NADZORA 9

2.2 NADZOROVANJE V PRETEKLOSTI 10

2.3 PANOPTIKON, DRUŽBE DISCIPLINIRANJA, BIOPOLITIKA IN DRUŽBE NADZORA 13

2.4 ZNAČILNOSTI IN OBLIKE SODOBNEGA NADZORA 16

2.4.1 Glavne značilnosti sodobnega nadzora 17

2.4.2 Nadzorovanje državljanov in potrošnikov 19

2.4.3 Problematika osebnih podatkov 21

2.4.4 Nadzorovanje kot družbeno razvrščanje ljudi 23

2.4.5 Konec zasebnosti? 23

3. VRSTE IN ZNAČILNOSTI SODOBNIH TEHNOLOGIJ NADZORA **25**

3.1 VIDEONADZORNI SISTEM 25

3.2 BIOMETRIJA 27

3.3 NADZOR V VIRTUALNEM PROSTORU 30

3.4 SATELITSKI VIDEONADZOR IN GEOLOKALIZACIJA 32

3.5 PRISLUŠKOVANJE 34

3.6 NADZOR S POMOČJO BAZ PODATKOV 35

3.7 PREVLADUJOČA PRAKSA 36

4. SITUACIJA V SLOVENIJI **40**

4.1 PRAVNA UREDITEV V SLOVENIJI 40

4.1.1 Zakon o varstvu osebnih podatkov 40

4.1.2 Zakon o elektronskih komunikacijah 44

4.1.3 Ustava, Kazenski zakonik in ostali zakoni 46

4.2 PODOBE V SLOVENSKIH MEDIJIH 47

4.2.1 Videonadzor v slovenskih mestih 47

4.2.2 Videonadzor na slovenskih cestah 50

4.2.3 Biometrični potni listi in nadzor na slovenskem letališču 51

4.2.4 Prisluškovanje SOVE in nasploh 52

4.2.5 Pametne, trgovske in zdravstvene kartice 53

4.2.6 Nadzor na delovnem mestu 56

4.2.7 Nadzor in zasebnost v virtualnem prostoru 58

5. RAZISKOVALNI OKVIR **59**
5.1 OPIS IN STRUKTURA VZORCA 60
5.2 ZNANJE O UPORABI SODOBNIH TEHNOLOGIJ NADZORA V SLOVENIJI 61
5.3 POJASNJEVALNI MODEL 63
5.4 REZULTATI ANALIZE 66
5.4.1 Preverjanje modela in hipotez 72
5.5 INTERPRETACIJA RAZISKAVE 74
6. RAZPRAVA **75**
7. ZAKLJUČEK **77**
8. LITERATURA IN VIRI **80**
9. PRILOGE **89**

KAZALO TABEL in SLIK

Tabela 5-1: Povprečne vrednosti za oblastna družbena moč (april 2004) 67
Slika 2-1: Jeremy Bentham – Panoptikon in načrt pogleda 14
Slika 3-1: Satelitska video slika Prešenovega trga in tromostovja v Ljubljani (glej maps.google.com 19.8.2006) 33
Slika 5-1: Struktura vzorca po spolu 60
Slika 5-2: Struktura vzorca glede na letnik študija 60
Slika 5-3: Struktura vzorca glede na vrsto fakultete (april 2004, n=283) 61
Slika 5-4: Preverjanje znanje o uporabi sodobnih tehnologij nadzora v Sloveniji – razvrščeno glede na pravilni odgovor, ki je obkrožen (april 2004, n=288) 61
Slika 5-5: Preverjanje znanje o uporabi sodobnih tehnologij nadzora v Sloveniji glede na spol (april 2004, n=280) 62
Slika 5-6: Preverjanje znanje o uporabi sodobnih tehnologij nadzora v Sloveniji glede na letnik študija (april 2004, n=280) 63
Slika 5-7: Pojasnjevalni model dveh neodvisnih (modra barva) in ene odvisne spremenljivke (rumena barva) 64
Slika 5-8: Seštevek indikatorjev v novo spremenljivko svetovanje in vodenje (april 2004, n=289) 68
Slika 5-9: Poznavanje sodobne tehnologije – veljavni deleži (april 2004, n=287) 69
Slika 5-10: Seštevek rekodiranih indikatorjev (v 0 in 1) spremenljivke poznavanje sodobne tehnologije (april 2004, n=287) 69
Slika 5-11: Seštevek rekodiranih indikatorjev spremenljivke zavedanje sodobnih tehnologij nadzora (april 2004, n=289). 71
Slika 5-12: Regresijski model oz. grafični prikaz multiple regresije (metoda Enter) 73

1. UVOD

Družbeno nadzorovanje kot tudi njegovo obravnavanje se je skozi zgodovino spreminjalo. Z razvojem informacijsko-komunikacijske tehnologije pa je dobilo popolnoma drugačen pomen, kot ga je imelo v preteklosti. Sedaj je nadzorovanje skrito, nevidno, neosebno in anonimno (glej Trampuž 2002), pojavlja pa se v vsakodnevnem življenju, pri nakupovanju, telefoniranju itd. Z razvojem videonadzornega sistema se je tako danes skoraj nemogoče gibati v prostoru, ne da bi bili fotografirani ali opaženi; nadzorovani smo na ulici, v trgovinah, na delovnem mestu, v bolnišnicah itd. (glej Trampuž 2002). Nadzorovani pa nismo le s pomočjo kamer, temveč tudi preko interneta, z vse večjo uporabo sodobnih naprav (mobilnih telefonov, digitalnih fotoaparatov, itd.) in s pomočjo ostalih najnovejših tehnologij. Veliko teoretikov opozarja, da gredo trendi nadzora v smer še večjega nadzora, kar pa lahko v družbi pripelje do nepredstavljivih posledic. S tem, ko se povečujejo sredstva namenjena nadzorovanju, narašča tudi znanje o samem človeku, hkrati pa se pojavljajo novi, neznani oziroma neobvladljivi pojavi, ki sprožajo različne pomisleke o posledicah in prihodnosti sodobne družbe. Ena izmed skrbi je zloraba osebnih informacij o posameznikih, ki jih imajo v lasti komercialne ali državne institucije. Za sodobno družbo namreč velja, da kdor ima podatke, informacije, ima tudi moč (glej Trampuž 2002). Namreč, »informacije ima vedno tisti, ki ima moč, in moč ima, kdor ima informacije« (Pečar 1991: 212), potemtakem torej ne gre več za klasično neenakost med kastami ali razredi (glej Gandy v Trampuž 2002). Izkaže se, da postajata nadzor in nadzorovanje ter z njima povezane teme osrednji vprašanji sodobne družbe. Sodobnemu nadzorovanju, predvsem nadzoru, ki ga izvaja država in zasebni sektor ter sodobnim tehnologijam nadzora pa se posvečam v diplomski nalogi. Cilj diplomske naloge je predstaviti uporabo in možno zlorabo sodobnih tehnologij nadzora v Sloveniji. Na začetku predstavljam obravnavanje nadzora v družbi s strani različnih teoretikov. Osredotočam se predvsem na sodobne avtorje in njihov pogled na nadzor. Sledi opis najpogosteje uporabljenih nadzorovalnih tehnik, tudi v praksi. V nadaljevanju opisujem situacijo glede tega področja v Sloveniji. Najprej predstavljam pravni pogled na to tematiko, sledijo najpogostejši incidenti s tega področja v Sloveniji, predvsem na podlagi pregleda slovenskih medijev. Osrednja točka diplomske naloge pa je lastna raziskava o

zavedanju sodobnih tehnologij nadzora med Slovenci, natančneje med študenti. V raziskavi preverjam pojasnjevalni model in dve postavljeni hipotezi o tem kako oblastna družbena moč posameznika in njegovo poznavanje sodobne tehnologije, vplivata na posameznikovo zavedanje sodobnih tehnologij nadzora. Model sem preverjala s pomočjo ankete med študenti in z uni-, bi- in multivariatno statistično analizo. Za konec poskušam glavna vprašanja glede uporabe sodobnih tehnologij nadzora zajeti v razpravi in zaključku.

2. PREGLED OBRAVNAVANJA NADZORA

Vsaka stopnja razvoja družbe je uporabljala različne načine in tehnike nadzorovanja, ki so se skozi zgodovino spreminjale in nadgrajevale, prav tako pa tudi obravnavanje nadzora. Za začetek najprej na kratko predstavljam definicijo in različne oblike nadzora, sledi obravnavanje nadzora v preteklosti, kako se je le-ta v preteklosti vršil ter značilnosti sodobnega nadzorovanja.

2.1 Glavne oblike nadzora

Nadzor je oblika nadzorovanja aktivnosti nečesa (glej Mobbs 2002), je »usmerjen vpliv na zastavljen cilj« (Beniger v Kovačič 2005: 21). Teorije o nadzoru navadno ločujejo predvsem dve obliki nadzorovanja: formalno (državno) in neformalno (nedržavno) (glej Pečar 1995:130), vse bolj pomemben pa je nadzor v zasebnem sektorju. *Neformalno nadzorovanje* poteka med ljudmi, ko nadzorujejo drug drugega in sicer brez vpletanja države (glej Pečar 1991: 17−18). *Formalno družbeno nadzorovanje* pa je tisto, ki se mora v vsakem političnem sistemu truditi in prizadevati za zmanjševanje deviantnosti in za njeno obvladovanje. Tako ima že od nekdaj sredstva in pooblastila, ki jih nima nihče drug (policija, tožilstvo, sodišče, zapori...), torej temelji na moči (Pečar 1988: 36, 39, 55, 102). Zelo pomembno pa je in dobiva tudi na vedno večjem obsegu, potrošniško oz. *komercialno nadzorovanje*, ki ga izvaja zasebni sektor, kapitalistične korporacije, ki želijo čim bolj natančno »ugotoviti potrošnikove želje ter jim prilagoditi ponudbo« (Kovačič 2003: 23). Podlaga za potrošniški nadzor je zbiranje podatkov (glej Lyon v Kovačič 2003: 23) o potrošnikih, deluje pa prijazno, saj v zameno za podatke ponudi ugodnosti, popuste, razna darila in drugo. Skozi celotno diplomsko nalogo se

osredotočam predvsem na formalni nadzor oz. nadzor s strani države ter na nadzor, ki ga izvaja zasebni sektor (več o tem v nadaljevanju).

Obstajajo tudi druge delitve nadzora kot je delitev med *pasivnim* in *direktnim* nadzorom (glej Mobbs 2002). Pasivni nadzor se nanaša na indirektno uporabo tehnik kot je analiziranje zapisov finančnih transakcij; za takšno obliko nadzorovanja so podatki že na voljo. V primeru aktivnega oz. vsiljivega nadzora pa je potrebna direktna intervencija, npr. nastaviti prisluškovalno napravo. Deliti pa moramo tudi med *skritim* in *javnim* nadzorom. Najboljši primer skritega nadzorovanja je razširitev videonadzornega sistema (glej Fitzpatrick 2002 364-365). Policija pa je primer javnega nadzorovanja, ki ima vsa pooblastila, da lahko npr. prestreže in dešifrira vsebine internetnega prometa, če se pojavi utemeljen sum[1] kriminala. Čeprav pa velikokrat tudi policija uporablja prikrite ukrepe. Prav tako ljudje v vsakdanjem življenju niso samo nadzorovani s strani drugih, ampak so tudi sami pripravljeni uporabljati različne tehnične naprave, da bi *sami nadzorovali druge* in tudi sebe. Na trgu takšnih in drugačnih pripomočkov ne manjka (glej Lyon 2006: 10). Tako se danes v splošnem pospešeno uporablja *samonadzorovanje* (glej Marx 2002). To se kaže s pristojnostjo različnih pripomočkov za dom, kot so testi za alkohol, nosečnost in AIDS. Ravno samonadzorovanje pa zabriše mejo med nadzorovanim in nadzornikom (glej Marx 2002:11). Pomembno je tudi nadzorovanje *»od blizu*« in »*od daleč*« (satelitske slike, oddaljeno opazovanje komunikacij in dela) (glej Marx 2002:11).

2.2 Nadzorovanje v preteklosti

V preteklosti so nadzor obravnavali skupaj z razmišljanjem o moči, državi in avtoriteti. Tako se je skozi zgodovino nadzor vedno nanašal na moč, izhajajoč iz režimov in politike. Pojem »nadzorovanje« je prišel v ospredje predvsem v družboslovnih in vedenjskih znanostih, povezanih s pravom, propagando, vladanjem itd.; najverjetneje pa je najbolj pogosto rabljen v sociooloških znanostih (glej Pečar 1988: 60, 61). Prvi, ki je daljnega leta 1896 uporabil pojem »družbeno nadzorstvo«, je bil verjetno E. A. Ross in tako praktično postal ustanovitelj tega področja. Ross je trdil, da »uspešno sodelovanje posameznikov zahteva visoko stopnjo družbenega reda, medtem ko visoka stopnja

[1] Utemeljen sum je več kot samo razlogi za sum; gre za pravni standard, ko sodišče na konkretnem primeru ugotavlja, če obstaja.

organizacije predpostavlja neko vrsto kontrole oz. nadzora« (Kovačič 2000: 4). Kasneje so nadzor obravnavali družboslovci (G. H. Mead, C. H. Cooley, E. Durkheim, S. Freud, J. Piaget, G. Simmel), sčasoma pa družbenega nadzora niso šteli samo za mehanizem za doseganje konformnosti, začelo se je že razmišljati o upiranju, nesoglasju in o odporu zoper nadzor. Po drugi svetovni vojni so nastopili funkcionalisti (T. Parsons, R. Dahrendorf in Robert K. Merton) in tako so začele dobivati osrednjo vlogo družbene vloge in družbeni red. V začetku 70-ih je James Rule že opozarjal na računalniško znanje v nadzorovanju in poudarjal posameznikovo in družbeno svobodo (glej Pečar 1988: 60-66). Določene države so začele v teh letih že sprejemati prve zakone za zaščito zasebnosti. Zvezna republika Nemčija je leta 1970 sprejela prvi zakon o varstvu osebnih podatkov, kasneje še Švedska (leta 1973), ZDA (leta 1977) in Francija (leta 1978) (glej Kovačič 2003: 35−36). Seveda tu ni daleč do Orwelovega 1984 in drugih fikcij o nadzorovanju, do Alwine Tofflerja, ki napoveduje človekovo prihodnost, ter do napovedovanja futurologov (glej Pečar 1988: 60−66). Nadzorovanje tako s pojavom informacijske družbe dobi pomembno mesto v teorijah nadzora tudi tehnologija.

V posameznih družbenih ureditvah in zgodovinskih obdobjih je imela vsaka stopnja razvoja svoje posebnosti glede rabe metod nasilja, zatiranja neposlušnosti, vzdrževanja reda in obvladovanja razmer. Sam nadzor se je namreč skozi zgodovino pogosto pokazal kot zelo »militanten in neizprosen« (glej Pečar 1988: 111). Od starege veka z njegovim izvajanjem kazni, do mučenj v zaporih, vpletanja psihiatrije v nadzorovanje ljudi, spoznamo metode, ki so nasilne. Nekateri takšni načini so (bili) urejeni s pravom (raba orožja, solzilci, vodni curki…), drugi spet ne (glej Pečar 1988: 111). V 15. stoletju je bil t. i. religiozni nadzor pomebna in močna oblika v tedanji družbi, predvsem z iskanjem heretikov, hudičev in čarovnic kot tudi z ostalimi religioznimi pravili kot so ženitve, arhivi in ohranjanje registrov rojstev, porok, krstitev in smrti (glej Marx 2002: 18). Takšen način se je nadaljeval kar nekaj stoletij (glej Marx 2002: 18). Družbe starega sveta je Foucault označil kot družbe spektakla, saj je bilo izvrševanje oblasti vezano na javno prikazovanje moči (glej Trampuž 2002). Tako je na primer kaznovanje na mestnem trgu postalo spektakel, s katerim je kralj izrazil svoje maščevanje in z mučenjem obsojenca utrjeval svojo oblast (glej Trampuž 2002: 351). V 16. in 17. stoletju je nastanek in razvoj prvih še ne čisto razvitih, držav povečalo potrebo po zbiranju in

uporabi informacij. Tako je politični nadzor postal zmeraj bolj pomemben v primerjavi z religioznim (glej Marx 2002: 18). V drugi polovici 18. stoletja je vse bolj prihajalo do odpora proti nasilnemu javnemu načinu kaznovanja in do zahtev o odpravi le tega. Nova strategija izvajanja kaznovalne oblasti: "Kaznovala naj ne bi nič manj, pač pa naj bi kaznovala bolje; nemara naj bi kaznovala manj strogo, zato pa naj bi kaznovala bolj univerzalno" (Foucault v Trampuž 2002: 351). Temu novemu tipu oblasti je ustrezal zaporniški model t.i. panoptični model, ki ga je predlagal Bentham (v nadaljevanju) (glej Trampuž 2002: 352). V 19. stoletju pa je postala populacija predmet znanstvene obravnave. »Tako se je prvič govorilo, da je nemogoče vladati državi brez poznavanje njene populacije« (Foucault v Trampuž 2002: 352), saj so bili ljudje merjeni, postavljeni v razrede in tako bolj podvrženi nadzoru (glej Taylor v Trampuž 2002: 52). Tako so se začele razvijati prave države, kot jih poznamo danes. Kazali so se postopni premiki k širši »upravljalski« družbi, kjer so predstavniki držav, industrije in trgovine izvrševali kontrolo nad zmeraj večjimi družbenimi in geografskimi območji. Država je tako morala razširiti popis prebivalstva, izboljšati shranjevanje podatkov, policijski register, identifikacijske dokumente in inšpekcije. Tako se osebni podatki niso zbirali le za obdavčenje, vojaško obveznost, uveljavljanje zakonov in nadzor državnih meja, ampak tudi za določitev državljanstva, demokratične participacije in družbenega planiranja (glej Marx 2002). V 19. in 20. stoletju se je z rastjo birokracije in državne blaginje nadzor še bolj poglobil v osebne podatke, z urejanjem različnih zakonov in ostalih zadev kot je npr. zdravstveno zavarovanje (glej Marx 2002). Tako se je prvotni nadzor s strani države in vlade, prenesel tudi na ostala področja vsakdanjega življenja, na delovno mesto, potrošnjo in zdravstvo. Danes pa si je sodobno potrošniško državo že »težko predstavljati brez zbiranja mase osebnih podatkov« (Marx 2002: 17−18), tako v javnem in zasebnem sektorju.

Pojem družba nadzora (*angl. surveillance society*) je prvič v 80-ih letih prejšnjega stoletja uporabil Gary T. Marx, kmalu zatem pa je leta 1989 zgodovinar in eden prvih pooblaščencev za varstvo osebnih podatkov v Kanadi David Flaherty pripomnil, da so postale zahodne države družbe nadzora (glej Lyon 2006). Lyon (2006: 6−8) omenja glavne modele kako nadzorovanje dejansko deluje, ki so:

- **Orwell**ovi organi totalitarne države iz knjige 1984[2];
- Panoptikon Jeremy **Bentham**a;
- Panoptikon je postal kasneje neizbežen v Michael **Foucault**ovi študiji discipline v modernem svetu;
- Za razumevanje sodobnega nadzorovanja pa je pomemben tudi Gilles **Deleuze**.

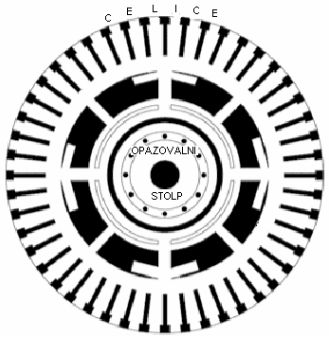
V nadaljevanju najprej predstavljam Benthamov Panoptikon, Foucaultove družbe discipliniranje in biopolitike ter Deleuzovo pojmovanje družb nadzora.

2.3 Panoptikon, družbe discipliniranja, biopolitika in družbe nadzora

Zasluge za model načrta zapora Panoptikon ima **Jeremy Bentham** leta 1791. Načrt zapora predstavlja okroglo stavbo z zaporniškimi celicami v obrobju (glej Slika 0-1). Celice so med seboj ločene v tolikšni razdalji, da se med zaporniki prepreči kakršnakoli komunikacija. V centru je »nadzorna loža« ali opazovalni stolp, skozi katerega lahko pazniki vidijo v vsako celico, brez da bi bili pri tem opaženi (glej Bentham v Land in Bayne 2002), hkrati pa lahko slišijo vsak šepet v celici (glej Kovačič 2005: 22). Osebe, ki so nadzorovane se morajo tako vedno čutiti pod nadzorom (glej Kovačič 2005: 22). Cilj je doseči kontrolo s pomočjo izolacije in stalnega (nevidnega) nadzorovanja (glej Bentham v Land in Bayne 2002). Zapor pa je odprt tudi obiskovalcem, ki nadzorujejo tako zapornike kot tudi paznike. Ključno torej je, da je pod nadzorom vsakdo in temelji na nezaupanju (glej Foucault v Kovačič 2005: 22). Bentham je tudi predlagal, da bi idejo Panoptikona uporabili še v bolnišnicah, šolah, norišnicah in politični skupnosti, saj je po njegovem mnenju z njim mogoče izboljšati moralo, ohraniti zdravje, utrditi ekonomijo. V Panoptikonu je namreč mogoče »vse preračunati, izmeriti vsak učinek in vzpostaviti polje popolne predvidljivosti« (Kovačič 2005: 23), hkrati pa se od zapornika (v primeru zapora) tudi pričakuje, da se obnaša kot je od njega zahtevano, in da zapornik sploh ne bi pomislil, da bi storil kaj narobe (glej Foucault v Kovačič 2005: 23). Takšen zapor pa v resnici ni bil nikoli zgrajen (glej Kovačič 2003: 106) in v realnosti verjetno nikoli ne bi

[2] George Orwell v delu 1984 opisuje totalitarno družbo, kjer posameznike Veliki Brat nadzoruje preko telekranov, posamezniki pa nikoli ne vedo kdaj so nadzorovani in kdaj ne (glej Kovačič 2003: 21).

deloval kot je bilo zamišljeno, saj je Bentham pozabil »na odpor posameznikov in je predpostavil, da so zaporniki povsem pasivna bitja« (Foucault v Kovačič, 2005: 22).



Slika 0-1: Jeremy Bentham – Panoptikon in načrt pogleda

Michael Foucault je svojo teorijo zgradil na modelu načrta zapora Panoptikon. Foucault je poudarjal, da je Panoptikon – tehnologija za nadzorovanje - model discipliniranja (glej Trampuž 2002: 352), je nekakšen laboratorij oblasti, kjer se z opazovalnimi mehanizmi povečata njegova učinkovitost in zmožnost za prodiranje v obnašanje ljudi (glej Trampuž 2002: 51). Vendar pa je Panoptikon mogoče uporabiti tudi zunaj zapora. Tako ne služi le za poboljševanje zapornikov, pač pa tudi za negovanje bolnikov, poučevanje šolarjev, itd.; gre torej za način postavljanja teles v prostor, hierarhično organiziranje, določanja sredstev oblasti in načinov poseganja (glej Trampuž 2002: 352). Tako je Foucault (glej Deluze 1990/2002) družbe suverenosti nasledil z *družbami discipliniranja* in jih umestil v 17. in 18. stoletje, višek pa so dosegle v začetku 20. stoletja. Delujejo s pomočjo zapiranja, torej prehajanja iz enega zaprtega okolja v drugo (družina, šola, kasarna in tovarna), vsako izmed teh okolij pa ima svoje zakone. Cilji in funkcije družbe suverenosti so bile povsem drugačne od disciplinirane, prehod pa se je zgodil postopoma (glej Deluze 1990 v 2002), torej prehod od kaznovanja k nadzorovanju (glej Salecl 1993: 36). Nova metoda nadzora dejavnosti teles, t.j. disciplina »najprej točno določi mesto posameznika v prostoru. Organizira zaprt, urejen prostor, kjer je možen popoln nadzor nad posameznikom. Panoptična arhitektura s celičnim, urejenim prostorom ustvari pogoje za delovanje nadzorovalnih dejavnosti, ko posameznik nikoli ne ve, kdaj ga oblast gleda« (Salecl 1993: 37). Discipline so tako imele opraviti s posameznikom in z njegovim telesom, torej gre za »prilagoditev mehanizmov oblasti nad posameznim telesom z nadzorovanjem in dresuro« (Foucault 1976/2003: 156, 159). »Nova« kaznovalna oblast tako ni temeljila več na oblasti, ki se razkazuje, temveč na oblasti, ki te gleda. Gre za to,

kako npr. zapornike čimbolj učinkovito izpostaviti pogledu, in kako celoten družbeni prostor napraviti pregleden in dostopen kontroli (glej Dolar v Trampuž 2002: 50). »Bistvo kazni postane, da popravlja in zdravi« (Foucault v Kovačič 20005: 24) ter da posameznike »celo odvrača od nepravilnih ravnanj« (Kovačič 2005: 24). Foucault je pokazal, da je Benthamov Panoptikon privilegiran kraj, ki omogoča eksperimentiranje z ljudmi in analiziranje njihovih sprememb. Uporabljali bi ga lahko vedno, kadar bi želeli v ne preobsežnih mejah prostora obdržati pod nadzorom določeno število oseb (glej Foucault v Trampuž 2002: 79). Tako je bila v 18. stoletju oblast oz. nadzor usmerjen h konkretnemu posamezniku (glej Kovačič 2005: 24).

Konec 18. stoletja pa je predmet znanstvene obravnave postala populacija. »Prvič se je govorilo, da je nemogoče vladati državi brez poznavanje njene populacije« (Foucault v Trampuž 2002: 352), saj so bili ljudje merjeni, postavljeni v razrede in tako bolj podvrženi nadzoru (glej Taylor v Trampuž 2002: 52). Ta nova tehnologija oblasti »se s pomočjo te predhodne disciplinarne tehnike dejansko utrdi« in disciplinarne tehnike ne izključuje, »temveč jo zaobseže, integrira, deloma spremeni« (Foucault 1976/2003: 153), z njo deluje vzporedno (glej Kovačič 2005: 25). Gre torej za novo tehnologijo oz. *biopolitiko*, biooblast, ki se vzpostavlja (Foucault 1976/2003: 154) in izvaja »regulacijske ukrepe na ravni celotne populacije« (Kovačič 2005: 24). Tako se disciplinarna tehnika osredotoči »na telo, ima individualizirajoče učinke, s telesom manipulira kot z žariščem sil, ki jih mora napraviti hkrati uporabne in ubogljive« (Foucault 1976/2003: 158), na drugi strani pa je nova tehnologija, regulacija, ki »se ne osredotoči na telo, temveč na življenje; tehnologijo, ki ureja učinke množice, značilne za neko populacijo, in ki skuša kontrolirati (morebiti spremeniti) njihovo verjetnost, vsekakor pa uravnovesiti njihove učinke« (Foucault 1976/2003: 158), stremi k nekakšni homeostazi z globalnim ravnovesjem, povprečjem: »varnost skupnosti glede na njene notranje nevarnosti« (Foucault 1976/2003: 159). »Gre torej za statistično spremljanje pojavov, iskanje globalnih kazalcev in povprečnih vrednosti ter uvedbo regulacijskih mehanizmov na tej globalni ravni« (Kovačič 2005: 25). Tako paznik postane birokrat, ki namesto posameznikov pregleduje družbo (Whitaker v Kovačič 2005: 25). Foucault (1976/2003:

161) omenja tudi normalizacijsko družbo[3], družbo kjer se sekata disciplina in regulacija. **Gilles Deleuze** pa meni, da je danes posameznik objekt *nadzorovalne oblasti*. Gre za družbe, kjer sta na delu »tako disciplina kot tudi regulacija« (Kovačič 2005: 27) oz. kot bi rekel Foucault biopolitika. Tudi sam Foucault je opozoril, da ravnokar zapuščamo disciplinske družbe (glej Deleuze 1990/2002: 171). Nadzor je tako »kratkega roka in hitrega kroženja, toda tudi nenehen in brezmejen« (Deluze 1990/2002: 176). Vstopamo torej v družbe nadzora, za katere je značilen nenehen nadzor, ki delujejo s pomočjo informacijskih strojev in računalnikov. Z družbo nadzora posameznika ne označuje matična številka ali število, ampak koda oz. šifra – »numeričen jezik nadzora je sestavljen iz kod, ki dopuščajo in zavračajo dostop do informacij« (Trampuž 2002: 55). Tako je za nadzorovalno družbo značilna uporaba računalnika, človek pa je postal podatek za identifikacijo, postal je kartoteka (glej Trampuž 2002: 55). Računalnik tako »zabeleži dopustno ali nedopustno mesto vsakega« (Deluze 1990/2002: 178). Nadzorovalna družba je tudi družba porabe, prodaje uslug, ki jo obvladujejo delnice, kreditne kartice. Marketing je postal »instrument nove družbene kontrole in tvori novo nesramno raso naših gospodarjev. Če je bil v disciplinski družbi človek zapornik, pa je v nadzorovalni družbi postal zadolženec« (Deleuze v Salecl 1993: 47-48), kar predstavlja novo obliko »kontrole« nad populacijo. »Ravno zaradi hkratnega delovanja discipline in regulacije se nadzor danes pojavlja v obliki nadziranja ljudi, ki se ga v glavnem poslužujejo države in nosilci oblasti, ter v obliki zbiranja podatkov o ljudeh (glej Lyon v Kovačič 2005: 28), ki so glavna domena zasebnega sektorja.

2.4 Značilnosti in oblike sodobnega nadzora

Danes so prizadevanja za nadzor posameznika usmerjena na nadzor posameznika v njegovem vsakdanjem življenju. S tem posameznik ni le tisti, ki je v službi, zaporu, vojski kot je opazoval Foucault, ampak tudi posameznik doma, pri igri, vseh običajnih dejavnostih vsakdanjika (glej Trampuž 2002: 53, 54). Sodobne tehnologije pa niso usmerjene le k nadzorovanju določenih posameznikov, temveč so usmerjene k nadzorovanju celotnega prebivalstva, populacije (glej Trampuž 2000: 138). V

[3] Norma se na nek način nanaša tako na telo kot tudi na populacijo, "omogoča hkrati nadzorovati disciplinarni red telesa in naključne dogodke v biološki množici … je tisto, kar se aplicira tako na telo, ki ga hočemo disciplinirati, kot na populacijo, ki jo hočemo regulirati" (Foucault 1976/2003: 161).

nadaljevanju opisujem značilnosti sodobnega nadzora, predvsem s strani zasebnega sektorja in države. Posebej poudarjam tudi problematiko osebnih podatkov, družbenega razvrščanja ljudi in vprašanj o zasebnosti.

2.4.1 Glavne značilnosti sodobnega nadzora

Gary T. Marx in Gordon (glej Kovačič 2000) sta prepričana, da danes vsi živimo v nekakšnem elektronskem Panoptikonu, se pravi nas stalno nekdo opazuje. Poster vidi svet elektronskega nadzorovanje kot Superpanoptikon, Wiliam Bogard pa govori o hipernadzoru oz. nadzoru brez omejitev (glej Lyon 2003: 176). Tudi že omenjeni Deleuze pravi, da danes živimo v družbi nadzora. Tako je danes nadzorovanje dosti bolj nevidno in nevarno, dosti manj javno in na splošno – težko se mu je izogniti (glej Pečar 1988: 131); nadzorovanje je postalo neosebno in anonimno, objekt opazovanja je posameznikovo telo in njegovo gibanje (glej Trampuž 2002: 352, 353) v vsakdanjem življenju, pri nakupovanju, telefoniranju, itd. Tudi Lyon (v Kovačič 2000) pravi, da je večina današnjega nadzora nevidnega.

Tudi Gary T. Marx (2002: 14-16) predlaga, da živimo v družbi nadzora. Osredotoča se na razlike novega in tradicionalnega nadzora, predvsem glede na značilnosti tehnologije in proces zbiranja podatkov. Opozarja še, da tradicionalni načini niso izginili, ampak so se dopolnili z novimi:

- novi nadzor se je razširil na čute (npr. zmožnost videti ponoči, skozi telesa, stene in preko ogromnih razdalj) in je slabo viden ali celo neviden;
- je bolj verjetno neprostovoljen;
- zbiranje podatkov je velikokrat integrirano v rutinsko dejanje;
- bolj verjetno vključuje manipulacijo kot direktno vsiljevanje;
- zbiranje podatkov je bolj verjetno avtomatsko s pomočjo naprav;
- je relativno poceni na enoto zbranega podatka;
- zbiranje podatkov se pogosto vrši na daljavo kot na mestu samem (oddaljeno shranjevanje podatkov) in podatki pogosto pripadajo drugim (npr. zunanji izvajalci);

- podatek je dostopen v realnem času, zbiranje podatkov je lahko nepretrgano, ponudijo se informacije iz preteklosti, sedanjosti in prihodnosti (statistične predikcije);
- predmet zbranih podatkov se od individualnih osumljencev »nadaljuje« na celotne kategorije (profiliranje);
- posameznik kot predmet zbiranja podatkov utegne postati tudi objekt intervencije;
- med odkritjem informacije in akcijo utegne biti zelo kratek interval.

Novo nadzorovanje je bolj intenzivno in obsežno, razširilo se je na čute, je manj vidno, neprostovoljne narave, oddaljeno, cenejše (glej Marx 2002: 15-16) in konstantno narašča (glej Lyon 2006). Hkrati pa je sistematično nadzorovanje postalo rutina in neizbežen del sodobnega življenja, ki je bolj kot kadarkoli prej odvisno od informacijsko-komunikacijske tehnologije in je zato danes smiselno govoriti o družbah nadzorah (glej Lyon 2006). Hiter razvoj tehnologije v kombinaciji z novimi vladnimi in komercialnimi strategijami vodijo k novim načinom hitrega širjenja nadzorovanja, kateremu je težko slediti, kaj ga šele regulirati. Vedno več različnih nadzorovalnih naprav je dostopnih tudi za navadne ljudi, vendar pa Lyon (2006) omenja, da je takšen način nadzorovanja, ki je ponavadi namenjen le eni osebi, zanemarljiv v primerjavi z institucionalnim, širšim, sistematičnem nadzorovanjem. Slednji je avtomatski in odvisen od moči računalniške tehnologije ter iskanja pravih informacij v bazi podatkov. Nadzorovalna tehnologija tako omogoča, da je nadzorovanje rutinsko in avtomatsko (glej Lyon 2006).

Kovačič (2005: 30) opisuje, da ni nujno, da »nadzor obstaja v obliki enega orwellovskega Velikega Brata, pač pa je nadzor razpršen«. Tudi Lyon (2001) omenja, da nove študije zaradi razpršenosti, decentralizacije in globalizacije nadzora, predlagajo nove modele (ne več orwellovske in Foucaultove perspektive o centraliziranem razumevanju nadzora). Nadzor se danes bolj širi kot »korenina oz. plezalka kot pa centralno drevesno deblo z razširjenimi vejami« (glej Deleuze in Guattari v Lyon 2001). Haggerty in Ericson (glej Lyon 2001) omenjata, da je to veliko ljudi prepričalo, da vidijo nadzor bolj »svoboden«, prilagodljiv in nepretrgan kot pa kot centralen. Omenjata, da se nadzor ne izvaja več le hierarhično kot je značilno za Orwella in Foucaulta (posamezniki ali skupine, ki imajo moč, nadzorujejo večino), temveč »koreninasto«, razvejeno (*angl. rhizome*), za katerega je značilna druga, preoblikovana hierarhija nadzora in omogoča tako preiskovanje, opazovanje tako tistih z močjo kot tudi splošne populacije (glej Haggerty in drugi 2000).

Tudi Kovačič (2005: 36) opisuje, da nadzor lahko izvajajo tudi posamezniki na oblast oz. nosilce moči, ne le obratno, vendar pa so v družbi nadzora »bistveno bolj izpostavljeni posamezniki kot pa so ji predstavniki oblasti, tehnologija nadzorovanja posameznikov pa je bolj učinkovita in razvita kot tehnologija nadzorovanja oblasti«. Seveda pa danes imeti moč pomeni, imeti podatke, informacije (glej Trampuž 2002: 354). Tako je nadzor posameznikov tesno povezan z močjo, vendar »mora biti moč v demokratični družbi podvržena demokratičnemu nadzoru, da ne prihaja do zlorab« (Kovačič 2003: 31). Če povzamem, se nadzor ne širi le iz ene samega centra oz. v obliki enega Velikega Brata, temveč si ga moramo predstavljati v obliki več »Malih Bratov«, kjer nadzorujejo tako nosilci moči kot splošna populacija drug druge, le da je nadzorovanje s strani nosilcev moči bolj razvito in pogostejše kot pa obratno. Nadzor pa bo zaradi povezovanja različnih baz podatkov v prihodnosti najverjetneje spet bolj centraliziran.

Čeprav v diplomski nalogi izpostavljam večinoma le negativne plati nadzora, ne smemo pozabiti tudi na pozitivne strani. Nadzor namreč »pomaga pri zagotavljanju varnosti in vzdrževanja reda, v povezavi z organizacijo pa služi tudi urejanju življenja v družbi« (Kocačič 2003: 23). Danes je tako nadzor zamenjava za grobo fizično silo značilno za preteklost, saj se uporablja kot sredstvo vzdrževanja reda in koordiniranja aktivnosti širše populacije (glej Lyon v Kovačič 2000), kar trdita tudi Deleuze in Foucault. Prav tako pa uporaba sodobne tehnologije omogoča, da s pomočjo nje zasebnost tudi varujemo, npr. v primeru interneta s sistemi za preprečevanje vdorov, šifrirnimi sistemi in s pomočjo še veliko drugih načinov zaščite (glej Kovačič 2005: 37).

Za nadzor v 21. stoletju je tako značilno omrežje, policentrizem in multimenzionalnost, ki vključuje tako biometrijo in video tehnike, kot tudi bolj običajno zbiranje osebnih podatkov (glej Lyon 2003: 172). Lyon tako omenja nujnost proučevanja vprašanj o zasebnosti, oblikah družbenega razvrščanja in diskriminaciji med skupinami, ki so različno klasificirane (glej Lyon 2006: 12), kar v grobem predstavljam v nadaljevanju. Najprej pa opisujem delitev med državnim nadzorom in nadzorom zasebnega sektorja, ki se tudi najbolj prepletata skozi celotno diplomsko nalogo.

2.4.2 Nadzorovanje državljanov in potrošnikov

Nadzor izvajata tako **država** kot tudi **zasebni sektor**, saj informacije o posameznikih zbirajo kapitalistične korporacije in tudi vladne službe (Kovačič 2003: 23). Kovačič

(2005: 32) opisuje, da je že omenjeni Foucaultovi funkciji nadzora (disciplinska in regulacijska) mogoče zaznati v javnem in zasebnem sektorju. Pravi, da »država disciplinski nadzor izvaja s pomočjo represivnih organov, regulacijskega pa preko državne statistike in tajnih služb ... zasebni sektor disciplinski nadzor izvaja na delovnem mestu, regulacijskega pa nad potrošniki s pomočjo marketinga« (Kovačič 2005: 32). Skratka nadzorovani smo tako kot državljani kot tudi potrošniki. Namreč, ambicije države in zasebnega sektorja je videti in nadzorovati vse (glej Kovačič 2003: 23), čeprav se države in nosilci oblasti v glavnem poslužujejo nadzora v obliki nadzorovanja ljudi, zasebni sektor pa v obliki zbiranja podatkov (glej Lyon v Kovačič 2003: 23), ti podatki pa predstavljajo veliko tržno vrednost (glej Kovačič 2003: 31). Nadzor s strani policije, državnih organov in drugih javnih oblasti, torej formalni nadzor, kot omenja Pečar, lahko delimo na naslednje oblike (glej Home Office 2006):

- *Nadzor komunikacijskih (prometnih) podatkov*: Te podatke posedujejo telekomunikacijska podjetja in ponudniki internetnih storitev. Primeri komunikacijskih prometnih podatkov vključejo: ime, naslov, telefonsko številko, IP naslov, geografsko lokacijo klicajoče naprave. Nadzorovanje komunikacijskih podatkov pa ne obsega tudi vsebine. Tovrstno nadzorovanje je pomembno orodje policije, državnih organov in ostalih organov oblasti, ki je namenjeno predvsem za nacionalno in javno varnost, prepečitev kriminala in javnega nereda.
- *Usmerjeni nadzor* (*angl. Directed surveillance*): Oblika prikritega nadzora, kjer državni organi spremljajo in posnamejo posameznikovo gibanje. Uporablja se predvsem v primerih osumljencev, ki so že oz. še bodo storili kriminalno dejanje.
- *»Vsiljiv« nadzor* (*angl. Intrusive surveillance*): Oblika nadzorovanja s fizično (skrivno) prisotnostjo posameznika ali podtikanjem raznih naprav za nadzorovanje. Tukaj je mišljeno predvsem sledenje osumljencu ali podtikanje raznih prisluškovalnih in drugih naprav v njegovem domu, avtomobilu in drugih osebnih prostorih.
- *Prestrezanje komunikacij*: Gre za prestrezanje komunikacijskih podatkov, še preden dosežejo svoj cilj. Za razliko od nadzora komunikacijskih podatkov, prestrezanje komunikacij obsega tudi vsebino. Prestrezajo se klici mobilnih in stacionarnih telefonov ter navadna in elektronska pošta. Država podatke prestreza

večinoma v primeru ogrožanja nacionalne varnosti in resnih kriminalnih dejanj na podlagi zakonskih pooblastil.

Seveda pa omenjeni (državni) načini nadzorovanja niso nujno le tehnika državnih organov in oblasti, saj lahko npr. elektronsko pošto prestreže tudi posameznik, ki je bolje poučen o tem področju, prav tako pa lahko podatke o uporabnikih interneta preglejuje tudi operater internetnega dostopa. Lyon (2003: 172 in 2001) v prihodnosti vidi povečanje prav *komercialnega nadzora* oz. nadzora, ki ga izvaja zasebni sektor. Ta se »nežno« vrši pri nakupu v trgovini, pri telefoniranju in surfanju po internetu; po teh podatkih pa velikokrat poseže tudi država. Danes se namreč vse giblje v čim bolj individualno obravnavo potrošnikov (profiliranje), ki je navidez namenjeno v prid in prijazno potrošnikom, vendar pa lahko na podlagi zbranih podatkov prihaja do njihove diskriminacije (glej Kovačič 2003: 26, 32). »Profiliranje je do posameznika na videz prijazno, saj potrošnika potiska, kamor si sam želi, oziroma ga zalaga z dobrinami in vsebinami, ki ustrezajo njegovemu okusu in potrebam« (Kovačič 2003: 33). Velikokrat pa se takšnemu nadzoru niti ne moremo odpovedati, če želimo npr. pridobiti kartico ugodnosti neke trgovske družbe. Tako se posamezniki nadzoru podrejajo celo prostovoljno (glej Kovačič 2005: 34). »Potrošniki in državljani tako živimo v svetu, v katerem se moramo nujno odpovedati delu svoje zasebnosti na račun večje funkcionalnosti in obvladovanja kompleksnosti življenja v sodobni družbi« (Kovačič 2005: 34). Tako postaja zasebni sektor vedno večja grožnja zasebnosti (glej Kovačič 2005: 33), saj ima ta danes »na voljo vedno več sredstev za obdelavo osebnih podatkov kot država« (Flaherty v Kovačič 2005: 33).

2.4.3 Problematika osebnih podatkov

Obseg podatkov, ki se lokalno, nacionalno in internacionalno pretakajo skozi elektronska omrežja, stalno narašča (glej Lyon 2006: 16). Današnja t. i. napredna družba meji na shranjevanju podatkov, opazovanju in nadzorovanju s strani različnih agencij in organizacij. Načini zbiranja, shranjevanja, procesiranja in obnavljanja osebnih podatkov pa so odvisni ravno od nove tehnologije (glej Lyon 2003) in so tudi relativno enostavno izvedljivi (glej Marx 2002: 15). Tudi Stadler (2002) se strinja, da je kreiranje, zbiranje in procesiranje osebnih podatkov že skoraj vsakdanji pojav. Roger Clarke (glej Lyon 2006: 16) je za nadzor s pomočjo podatkov uvedel pojem podatkovni nadzor (*angl.*

dataveillance) oz. »sistematično nadzorovanje človeških dejanj ali komunikacij s pomočjo informacijske tehnologije« (Lyon 2003: 168). Osebni podatki se pretakajo povsod, ob nakupu v trgovini z bančno kartico, pri surfanju na internetu in po ostalih storitvah, ki jih ponuja, z uporabo RIFD etikete, mobilnega telefona, skratka podatki konstanto krožijo in se beležijo. Zaradi tega so možne tudi zlorabe osebnih podatkov, npr. kraja identitete (angl. *identity theft*), ki je zelo pogost pojav v ZDA. Seveda pa osebni podatki krožijo tudi na mednarodni ravni, za izmenjavo policijskih podatkov ali za zunanje izvajanje (angl. *outsourcing*)[4] (glej Lyon 2006: 17-19). Tako je marketing z bazami podatkov multimiljarderska industrija, ki išče osebne podatke glede potrošniških navad pri zapravljanju denarja, pri njihovi izbiri in življenjskem stilu, z namenom profilirati ter zaslediti trenutnega in potencialnega potrošnika na različnih področjih življenja (glej Lyon 2003: 162). Stadlerja pa najbolj skrbijo zdravstveni podatki posameznikov in možne zlorabe, predvsem s strani delodajalcev in zdravstvenih zavarovalnic.

Najostrejša zakonodaja o osebnih podatkih je značilna ravno za Evropo, ki se precej razikuje od »milejše« zakonodaje v ZDA (glej Stadler 2002: 120−121). Evropska zakonodaja namreč dovoljuje zbiranje in obdelovanje osebnih podatkov le ob vnaprejšnji privolitvi posameznika, na katerega se ti podatki nanašajo, značilne pa so tudi visoke omejitve glede posredovanja teh podatkom drugim subjektom (glej Marn 2006). Za razliko je v ZDA prodajanje osebnih podatkov že običajna praksa (glej Marn 2006).

Danes se tako pojavlja nova tehnologija za zbiranje osebnih informacij, ki prodira globlje, širše, bolj sofisticirano in posamezniku prijazno kot tradicionalne metode. Moč nadzorovanja pa je ravno v tem, da je vse zbrane podatke možno povezati, in s tem pridobiti nove vredne podatke in informacije, ki so lahko škodljive ali celo nevarne za posameznika (glej Čebulj v Kovačič 2003: 27). Pri zbiranju podatkov pa obstajajo tudi druge nevarnosti, kot so »nenatančnost, nepopolnost ali neažurnost zbranih podatkov«, preventivno zbiranje podatkov, obstoj baz podatkov, za katere posamezniki sploh ne vedo ali pa vanje nimajo vpogleda (glej Kovačič 2003: 36). Tako se podatki danes ne samo zbirajo in popravljajo, ampak tudi analizirajo, iščejo, združujejo, trgujejo, znotraj in med organizacijami (Lyon 2006: 22), pri tem pa so možne tudi različne zlorabe in druge nevarnosti.

[4] Oddaja dela zunanjim izvajalcem.

2.4.4 Nadzorovanje kot družbeno razvrščanje ljudi

Družbeno razvrščanje oz. profiliranje ljudi je že staro, neizogibno človeško dejanje, ki pa je danes postalo rutina, sistematično, avtomatsko dejanje, podprto s tehnologijo (glej Lyon 2006: 22). Pri profiliranju gre dejansko za to, da »posameznika uvrstijo v neko kategorijo, kjer je na podlagi svojih karakteristik, ne pa dejanj, označen za sumljivega oz. vrednega pozornosti« (Kovačič 2003: 30). »Klasifikacija mogoče zgleda nedolžno in človeku koristna, vendar je lahko tudi osnova za nepravičnost in neenakost« (Lyon 2006: 22). Idealen pripomoček za takšno razvrščanje je računalnik, sploh ker se večina današnjega nadzora nanaša na informacijsko-komunikacijsko tehnologijo (IKT). Marketinške tehnike in razne varnostne meritve uporabljajo IKT za identificiranje skupin in posameznikov za interese organizacij. Z zbiranjem podatkov o ljudeh in njihovih aktivnostih ter analiziranjem sekundarnih podatkov iz drugih baz, lahko trgovec načrtuje svojo oglaševanje. Uporaba osebnih podatkov za namene varnosti pa prav tako uporablja podobne strategije za nadzorovanje osumljencev, ki so bili že identificirani ali pa samo ustrezajo profilu osumljenca (glej Lyon 2006: 22). Takšno nadzorovanje je usmerjeno v prihodnost; temelji na simulaciji in modeliranju situacij, ki se še niso zgodile; ne more delovati brez omrežja, baz podatkov in iskanja po njih (glej Lyon 2006: 22). Z različnimi podatki (video, tekstovne datoteke, biometrični podatki, genske informacije, ...) se manipulira za izdelavo profila in nevarnih kategorij posameznikov. Družbeno razvrščanje pa je najbolj problematično takrat, kadar organizacije, ki zbirajo takšne podatke, direktno vplivajo tudi na življenja ljudi (glej Lyon 2006: 22). Williams in Johnstone (glej Surette 2004: 162) navajata, da operaterji videonadzornega sistema selektivno nadzorujejo tiste družbene skupine, ki so bolj verjetno deviantne; predvsem mlade temnopolte moške. Za takšna dejanja se uporablja pojem rasno profiliranje. Torej, večinoma se profiliranje nanaša na demografsko razvrščanje nadzorovanih oseb in zbiranje podatkov, bolj glede na to, kdo so, kot pa kaj dejansko počnejo. Trend družbenega razvrščanje oz. profiliranja pa je še posebej izrazit po dogodkih 11. septembra v ZDA (glej Lyon 2006: 25).

2.4.5 Konec zasebnosti?

Banisar in drugi (glej Kovačič 2003: 34) pravico do zasebnosti določajo kot mejo, »do katere družba lahko vdre v posameznikove zadeve«. Alan Westin (glej Lyon 2006: 20) pa pravico do zasebnosti definira kot »posamezniki, skupine in institucije imajo pravico

kontrolirati, spreminjati, upravljati in brisati informacije o sebi in odločati kdaj, kako in v kakem obsegu so te informacije posredovane drugim«. Med teoretiki danes prevladuje mnenje, da vedno bolj izgubljamo zasebnost, ne kažejo pa se kakšni trendi, da bi se ta proces upočasnil (glej Stadler 2002). Sodobna tehnologija je namreč pospešila zbiranje in obdelavo podatkov (glej Kovačič 2003: 35). V času elektronskega trgovanja in kroženja mase osebnih podatkov se zelo pogosto uporablja citat »Zasebnosti je konec. Sprijaznite se!« (angl. *Privacy is dead. Get over it!*) (Scott McNealy v Lyon 2006: 20). Ljudi bo v prihodnje vedno bolj skrbelo za njihovo zasebnost in svobodo (Pečar 1991:361), saj je z razvojem novih tehnologij zasebnost še bolj ogrožena kot je bila včasih (glej Čebulj v Kovačič 2000: 1022). Namreč, nadzorovanje je že sedaj avtomatsko, saj ga posameznik sproži sam (glej Trampuž 2000: 139), hkrati pa je tudi nevidno (glej Lyon 1994: 5 in Pečar 1988: 131). Naša družba je tako zmeraj bolj organizirana kot omrežja, podprta z digitalnimi informacijami in komunikacijsko tehnologijo (glej Castells v Stalder 2002). Zanimivo pa je, da je večina ljudi na splošno gledano zaskrbljena o svoji zasebnosti, v praksi pa jih zelo malo poskrbi za ustrezno zaščito (glej Stalder 2002). Mellors (glej Kovačič 2003: 37) preventivo vidi v tem, da ni bistvo zaščite v tem, da oni (omenja državo) vedo manj o nas, temveč, da mi vemo več o njih (vemo, kaj oni vedo o nas, kako te informacije uporabljajo).

Ravno nasprotno pa meni Gary Rowden, ki je v 90-ih letih prejšnjega stoletja sodeloval pri postavitvi videonadzora v Veliki Britaniji. V intervjuju za Delo (Krašič 1. 3. 2004) je povedal, da se miselnost ljudi spreminja: »ljudje so mnogo let ob omembi Velikega Brata najprej pomislili na nezaželeno opazovanje s kamerami, zadnjih pet do deset let so govorili, da je to vdor v zasebnost«, danes pa so prepričani, da «jih Veliki Brat ne zgolj opazuje, temveč jim pomaga«. Dodaja tudi, da se sistema bojijo samo tisti, »ki bi radi storili nekaj, česar ne želijo, da bi kamere opazile«. Tako danes obstaja kar nekaj pravnih omejitev, ki pa so velikokrat opuščena z argumentom: *Če nimaš kaj skriti, se nimaš česa bati* / *If you've got nothing to hide you've got nothing to fear* (John Major, premier Velike Britanije v Norris and Armstrong v Surette 2004). Posledice potemtakem nosimo vsi, tako nedolžni kot tudi krivi ali osumljeni kakšnega kriminalnega dejanja (Lyon 2001). Ključno pa je, da postaja Veliki Brat prijazen in pomaga ali kot pravi Kovačič (2005: 21) nadzorovanje je dobilo »hinavski obraz«, saj je postalo »neopazno, a posvod prisotno, postalo je prijazno in prostovoljno« (v primeru različnih potrošniških kartic ugodnosti) ali

kot pravi Whitaker (glej Kovačič 2005: 21) »'Veliki Brat te opazuje! / Big Brother is watching you!' se spreminja v 'Veliki Brat skrbi zate / Big Brother is watching out of you'.« Sicer lahko s sodobno tehnologijo zasebnost res tudi varujemo (glej Kovačič 2005: 37), npr. s šifrirnimi sistemi, videonadzorom doma itd., vendar pa se zdi, da je to le reakcija na mogoče že kakšno slabo izkušnjo ali pa preventivna želja po večji varnosti ljudi.

Torej mnenja o vedno manjši zasebnosti ali celo njenem koncu so deljena, nagibajo pa se v smeri, da se zasebnost ljudi zmanjšuje. Ob upoštevanju zgornje definicije pravice do zasebnosti, pa lahko trdim, da imamo Evropejci več zasebnosti kot državljani ZDA, zaradi veliko bolj ugodne zakonodaje na področju varstva osebnih podatkov. Tudi Informacijska pooblaščenka je v intervjuju za Studio City (3. 7. 2006) povedala, da je Slovenija (glede videonadzora) še raj.

3. VRSTE IN ZNAČILNOSTI SODOBNIH TEHNOLOGIJ NADZORA

Prvotno je različne naprave za nadzorovanje uporabljala vojska in policija, nato večje organizacije in vladne ustanove, danes pa je namenjena tudi za civilne, lokalne in družinske namene (glej Lyon 2006:11). Sodobna tehnologija nadzora se dandanes izredno hitro razvija, razširja, izpopolnjuje, poleg tega pa v današnji družbi dobiva na vedno večjem pomenu, saj si brez nje že zelo težko predstavljamo življenje; zato pa lahko vedno več različnih vrst te tehnologije kupimo kar v za to specializiranih trgovinah ali preko spleta. Kupimo lahko različne vrste video kamer, pripomočke za prisluškovanje, GPS naprave itd. Skratka, tehnologij za nadzorovanje je zelo veliko. Velikokrat pa se uporablja tudi več načinov oz. tehnologij nadzora hkrati (glej Marx 2002: 9, 15). Za začetek najprej predstavljam glavne načine oz tehnologije nadzora, ki pa nikakor niso edine, saj se sodobna tehnologija ves čas izpopolnjuje in nadgrajuje.

3.1 Videonadzorni sistem

Videonadzorni sistem (*angl. Closed Circuit Television System - CCTV*) so prvič javno uporabili v 60-ih letih v Angliji. Ravno zaradi visoke javne podpore v Anglijis so ga kasneje posvojile tudi ZDA (glej Surette 2004: 153). Poznamo tri generacije

videonadzornih sistemov: prvo, drugo in najnovejšo – tretjo. **Prva generacija videonadzornega sistema** izvira iz leta 1950. Sestavljala jo je črno-bela kamera z nizko resolucijo, ki je bila na glavni zaslon povezana s koaksialnim kablom. Takšen sistem je ostal nespremenjen do leta 1980, ko so se pojavile kompaktnejše mestne kamere, videorekorderji in omrežna oprema. Seveda pa je takšen sistem spremljajo vrsto težav: napake na opremi, premajhna kvaliteta posnetkov, zapletena in draga namestitev opreme, nezmožnost snemanja in pregledovanja posnetkov hkrati, zelo majhna zmožnost gibanja ob morebitnem odkritju, zapleten proces arhiviranja (glej On-Net Surveillance Systems 2006). Že s prvo generacijo videonadzornih sistemov pa se je pojavila zaskrbljenost – najprej angleške – javnosti, glede izgube zasebnosti, nadzora video slik, zlorabljene uporabe tehnologije in razvrščanja državljanov glede na to, kdo bo nadzorovan (glej Hones in Charman v Surette 2004: 154).

Zaradi precejšnjih pomanjkljivosti prve generacije so v začetku 90-ih letih začeli sistem izboljševati. Razvili so digitalne video rekorderje, ki so bili poglavitni za razvoj **druge generacije** t.i. *digitalnega nadzorovanja*, ki je omogočalo snemanje v večji ločljivosti. (glej On-Net Surveillance Systems 2006). Glavni cilji druge generacije so obdelava slik, avtomatska identifikacija s pomočjo primernih programov, kjer digitalni sistem in določen program avtomatsko prepoznata nenavadne situacije, ki pritegnejo pozornost monitorjev (glej Surette 2004: 157). Druga generacija želi tako predvsem:

- individualno identificirati pribežnike in nepooblaščene osebe;
- prepoznavati dejanja (pretepi, kraje, vlomi);
- prepoznavati predmete, objekte (zapuščena prtljaga in orožje)

Vendar se pa tudi druga generacija sooča z različnimi problemi kot so poplava podatkov (preveliko število slik in informacij) in z že omenjenim demografskim razvrščanjem ljudi (glej Surette 2004: 157, 161-162).

V javnosti se pojavlja že **tretja generacija** videonadzornega sistema t. i. *IP nadzorovanje*. Značilnost tega sistema je povezava v popolno digitalno omrežje in omogočanje popolne kontrole in upravljanja IP videonadzornih kamer preko LAN, WAN omrežij in interneta. Gre torej za digitalno snemanje, ki je hkrati povezano v odprta omrežja (intranet in internet), torej daljinski nadzor, kjer je trenutna dogajanja možno pregledovati preko interneta. Glavne prednosti videonadzornih sistemov tretje generacije so (glej On-Net Surveillance Systems 2006): oddaljeno opazovanje (dostop preko LAN

omrežja, intraneta in interneta), integracija ostalih sistemov v omrežje (alarmov proti požaru ali vlomom, biometrične funkcije), nizki stroški namestitve in vzdrževanja ter verjetno še kaj. S sodobno tehnologijo je tako mogoče »posnetke nadzornih videokamer primerjati med sabo, shranjevati in povezovati« (Kovačič 2003: 15).

Končni tehnološki cilj videonadzornega sistema je tako ustvariti inteligentni decentraliziran sistem kamer, ki so del še večjega omrežja, hkrati pa bi kamere imele zmožnost neodvisnega analiziranja (glej Surette 2004: 157). Zanimivo pa je, da se kljub promoviranju videonadzora kot anti-kriminalnega sredstva v boju proti resnim kriminalom (terorizmu), v praksi uporablja in je tudi bolj učinkovit le za manjše prestopke, kot so onesnaževanje okolja, nadzor prometa, alkoholiziranosti, kajenja, napačnega parkiranja itd. Seveda pa učinek nadzora po določenem času popusti, če ni pravih ukrepov, ali pa se kriminalna dejanja le prestavijo na kakšen drug prostor. Takšna praksa se je izkazala na londonski podzemni železnici, kjer se je ob začetku namestitve kamer število tatvin zelo zmanjšalo, vendar je učinek po enem letu popustil (glej Webb, Laycock 1992 in Mayhew 1979 v Surette 2004: 156). Ključni argument za postavitev videonadzora je torej *zmanjšanje kriminala*, ki pa je odvisno od vrste dejavnikov (glej Surette 2004: 160-162):

- koliko so potencialni storilci pripravljeni tvegati, da bi jih oblasti ujele;
- stopnje vidnosti nadzorovanega območja;
- kvalitete opazovanja;
- sodelovanje policije oz. 'redarjev', ki lahko storilce ujamejo.

K hitremu širjenju videonadzora pa delno prispeva tudi dejstvo, da gre za nekakšno *modno muho* in delno tudi zaradi *obupa* (glej Surette, 2004: 154). Namreč, mesta uporabljajo videonadzor, ker ga uporabljajo tudi sosednja, prav tako pa mislijo, da je ravno tehnologija tista, ki lahko reši urbane probleme (glej Davies 1996 v Surette 2004: 154). K širjenju uporabe videonadzora pa močno vplivajo tudi *politični* in *komercialni pritiski.*

3.2 Biometrija

Med najnovejšo nadzorovalno tehnologijo spada biometrija (*angl. biometrics*). Njena značilnost je uporaba telesnih značilnosti kot načina identifikacije in nadzorovanja (glej Fitzpatrick 2002: 370-372). Gre torej za »proces zbiranja, procesiranja in shranjevanja

podatkov o posameznikovih fizičnih lastnostih z namenom identifikacije« (Kovačič 2003: 14, 103). Z biometrijo smo identificirani skozi fizične značilnosti kot je glas, obraz, oči, prstni odtis, DNK itd. Med seboj se najbolj ločimo po DNK, šarenici, mrežnici in prstnih odtisih, manj pa po obliki dlani, obrazu, govoru, podpisu, hoji, načinu tipkanja. Uporabimo jo lahko v dveh primerih: *za identifikacijo* ali prepoznavanje posameznika z vsemi, ki so v bazi, ter *za verifikacijo* oz. potrditev, torej ali gre res za tisto osebo, za katero se izdaja (glej Miko v Ona 1.6.2004). Jain in ostali (2002) opisujejo različne načine identifikacije in verifikacije oseb:

- *Prstni odtisi* so grafični vzorci, prisotni na človeškem prstu, ki naj bi bili edinstveni za vsakega človeka (vzorci se razlikujejo tudi glede na vsak prst).
- *Prepoznavanje obraza:* obraz je najbolj sprejemljiv biometrični podatek in je najbolj splošna metoda identifikacije, ki jo ljudje uporabljajo pri vizualni komunikaciji. Vendar se mora tudi ta tehnologija spopadati z različnimi težavami kot so procesi staranja, obrazno izražanje itd.
- *Geometrija rok* glede na obliko roke, npr. velikosti prstov.
- *Šarenica:* vsak posameznik ima edinstveno strukturo šarenice (glede na vsako oko). Pri odvzemanju vzorca ni potreben kontakt s kamero, nujno pa je sodelovanje posameznika t.j. oko je oddaljeno za določeno razdaljo. Napak pri tehnologiji za identificiranje šarenice je izjemno malo.
- *Mrežnico* razumejo kot najbolj varen biometrični podatek.
- *Preverjanje podpisa:* način pisanja je značilnost vsakega posameznika, ki pa je velikokrat odvisen od trenutnega čustvenega in fizičnega stanja posameznika. Gre za statično (le geometrijska oblika podpisa, npr. velikost in oblika črk) in dinamično (ne samo oblika podpisa, ampak tudi hitrost, način pisanja) verifikacijo podpisa.
- *Prepoznavanje glasu* je odvisno predvsem od kvalitete mikrofona in komunikacijskega kanala, prav tako pa tudi od posameznikovega zdravja (prehlad itd.), stresnih in emocionalnih situacij.
- *Infrardeča toplotna identifikacija obraza in ostalih delov telesa - termogram:* človeško telo oddaja toploto in ta vzorec toplotnih žarkov predstavlja značilnosti vsakega posameznika.

- *Dinamika tipkanja:* vsak posameznik na tipkovnico tipka na svojevrsten način. Ta dinamika temelji na časovnih presledkih med tipkanjem.
- *Prepoznavanje hoje:* svojevrstne način hoje, ki pa ni edinstvena za vsakega posameznika, vendar je zadostna značilnost za identificiranje. Seveda pa se skozi obdobja spreminja (pridobitev telesne teže, ob alkoholiziranosti, itd.).
- *Vonj:* vsak posameznik izloča vonj, torej posebne značilnosti kemične sestave vonja.
- *Biometrija ušesa* je ločevanje glede na obliko in strukturo uhlja, vendar pa vsak posameznik nima edinstvenega ušesa.
- *DNK:* je zares edinstvena koda vsakega posameznika (razen enojajčnih dvojčkov, ki imata isti DNK vzorec).

Vsaka zgoraj omenjena metoda ima svoje prednosti in slabosti. Biometrija dlani se sicer uporablja že vrsto za let, vendar je za splošno rabo neprimerna, saj se dlani med sabo ne razlikujejo dovolj. Prav tako tudi 5% ljudi nima čitljivega prstnega odtisa, bodisi zaradi genskih napak, zaradi obrabe ali nesreč, elektronske čitalnike pa je mogoče prelisičiti s pomočjo toplega in vlažnega zraka ter z drugimi načini, npr. želatine iz katere so narejeni gumi-medvedki[5]. Prepoznavanje obraza temelji na 30 obraznih točkah, vendar tudi ta sistem ne deluje brezhibno. Za ugotavljanje identifikacije je tako najbolj primerno analiziranje DNK, šarenice in mrežnice. Ravno odčitavanje šarenice je dovolj zanesljiva metoda, kjer hkrati tudi ni potreben fizični stik kot npr. pri oddajanju prstnih odtisov (glej Miko 1. 6. 2004).

Za večjo verodostojnost se raziskovalci nagibajo k multibiometričnim sistemom, torej kombinaciji različnih biometričnih metod. ZDA so izbrale skeniranje prstnih odtisov in prepoznavanje obraza (glej Miko 1. 6. 2004), temu sledi Evropa, tudi Slovenija z novimi potnimi listi zaradi zahtev ZDA (več o tem v nadaljevanju). S preverjanjem več biometričnih podatkov hkrati se tako poveča zanesljivost preverjanja ljudi. »Ni dvoma,

[5] Japonski kriptograf Tsutomu Matsumoto je iz želatine (kupljene v obliki gumi-medvedkov) naredil obliko prsta. Želene prstne odtise je pobral iz kozarca, nad odtise pa spustil pline iz tube sekundnega lepila, da je odtis postal bolj kontrasten. Odtis je fotografiral ter v Photoshopu povečal kontrastnost, nato pa odtis natisnil na prosojnico, vzel foto-občutljiv PCB, nanj položil prosojnico ter pustil, da se je v baker izrezljala oblika odtisa. To je pritisnil na želatino in tako ponaredil prstni odtis, s čimer se lahko pretenta kar 80% vseh naprav za prepoznavanje prstnega odtisa (glej Slo-Tech.com 20. 5. 2002). Tudi Marie Sandström je v magistrski nalogi preverjala čitalce prstnih odtisov. S pomočjo umetnih prstnih odtisov iz želatine je preverila devet čitalcev na sejmu CEBIT v Nemčiji, kjer pa je bilo vse sisteme možno pretentati (glej Slo-Tech.com 30. 6. 2004).

da biometrija izrazito povečuje možnosti nadzora posameznikov« (Kovačič 2005: 15). Seveda pa so tudi pri biometriji možne napake, saj so tudi računalniki zmotljivi, programi pa lahko prav tako vsebujejo napake. Težave se bodo pojavile »pri računalniškem odčitavanju biometričnih podatkov, zapisanih v dokumentu, in primerjavi s fizično izmerjenimi podatki« (glej Alkalaj v Miko 1. 6. 2004). Mišo Alkalaj (glej Miko v Ona 1.6.2004) opozarja, da se bodo policisti hitro navadili bolj verjeti računalniku kot lastni pameti in zaradi tega se bo med rešetkami lahko pojavila tudi nedolžna oseba. Problem se pojavi tudi v tem, kako se bodo podatki v praksi uporabljali, in ali se bodo tudi izkoriščali. Alkalaj tudi poudarja, da ni nikakršnega zagotovila, da podatkov državni organi ne bodo povezovali v enotno bazo, s tem pa se začne nenehno spremljanje vsakogar in omejevanje pravice do zasebnosti.

3.3 Nadzor v virtualnem prostoru

Internet je postal dostopen že skoraj vsakomur. Postal je orodje zabave, velik vir informacij, pomembno orodje marketinga in velik elektronski trg s številnimi elektronskimi transkacijami vsako sekundo (glej STOA 2004). Ravno zaradi tega je možnosti nadzorovanja, pregledovanja in prestrezanja podatkov na spletu zelo veliko, sploh zaradi sledi, ki jih vsak uporabnik pušča pri surfanju na internetu za sabo. Omenila bom le najpomembnejše tehnike nadzorovanja.

Uporabnik interneta največ **elektronskih sledi** pusti pri svojem ponudniku interneta: kdaj in katere storitve interneta je uporabljal, skupaj z uporabniškim imenom, IP številko, telefonsko številko oz. drugo vstopno točko, preko katere se je povezal na internet (glej Kovačič 2003: 44). Vsi ti podatki se zbirajo v datotekah aktivnosti (*angl. log files*). Ponudnik interneta si lahko beleži, katere spletne strani uporabnik obiskuje in na podlagi tega izdela profiliranje teh uporabnikov (glej Kovačič 2003: 44). Takšne datoteke aktivnosti pa vzdržujejo tudi ponudniki različnih internetnih storitev, predvsem spletnih strani. Zapišejo si lahko vsaj IP naslov uporabnika in spletno stran ter podstran, ki jo obiskuje, kot tudi tip uporabnikovega spletnega brskalnika, vrsto operacijskega sistema itd. (glej Kovačič 2003: 44). Nekateri spletni brskalniki pošiljajo spletnim stranem več podatkov o uporabnikih kot drugi, to imenujemo *browser's chattering* (glej Kovačič 2003: 45). Eden izmed teh je Microsoft Internet Explorer, ki naj bi celo razkril ali ima porabnik nameščene programe kot so Word, Excel ali Power Point (glej Kovačič 2003: 45).

Ob vstopu na spletno stran se računalniku avtomatsko dodeli tudi piškotek (*angl. cookie*), ki nato ob naslednjem obisku te strani prepozna uporabnikov računalnik (glej Kovačič 2003: 46). Ti ne prepoznajo samega uporabnika, temveč le računalnik. S pomočjo piškotkov lahko ponudnik internetne strani ugotavlja obiske in navade obiskovalcev, npr. katere vsebine so najbolj zanimive. Tako se na strežniku shranjujejo preko ID številke podatki o registriranih uporabniških imenih in nastavitvah, kdaj je bil uporabnik nazadnje na spletni strani in kaj je gledal (glej Kovačič 2003: 47). Najpreprostejši primer piškotkov je mogoče opaziti pri spletnem nakupovanju, kjer ob nakupu izpolnimo obrazec, piškotek vse te podatke shrani, tako nam pri naslednjem nakupu teh informacij ni potrebno še enkrat vnašati (glej Kovačič 2003: 47).

Uporabnik se takšnim sledem zelo težko izogne, lahko pa nadzor vsaj delno omili s poznavanjem interneta, računalnika in storitev, ki jih splet ponuja. Do teh sledi je mogoče priti tudi po izbrisu npr. elektronske pošte, internetnih povezav, datotek, informacij o trajanju in vsebini povezav na spletu za obdobje več tednov (glej Baebler 23. 5. 2005). Veliko skrbi okoli takšnega nadzora pa vzbuja ravno nadzorovanje na delovnem mestu. Pri nas nič od tega legalno ne smejo storiti, če uslužbenec o tem ni prej obveščen.

Drug problem nadzorovanja na internetu pa so **povezovanje, zbiranje in prestrezanje podatkov**. Sicer velika večina podatkov na internetu med seboj ni povezanih, kar pa še ne pomeni, da jih ni mogoče povezovati (glej Kovačič 2003: 50). Za ta namen obstaja veliko tehnik povezovanja baz. Že omenjeni podatkovni nadzor, npr. povezovanje elektronskih sledi, ima veliko prednosti, saj je poceni za vzdrževanje in hkrati učinkovit (glej Clarke v Kovačič 2003: 50-51). Privlačno pa je tudi zbiranje javno dostopnih (brezplačnih) osebnih podatkov, npr. iskanje elektronskih naslovov po spletnih straneh in forumih. Tudi za to obstajajo posebni javno dostopni programi t. i. roboti, pajki in črvi (glej Kovačič 2003: 51). Velikokrat pa se podatki zbirajo preko registracije brezplačnih programov, podtaknjenih virusov ali pa s preprostimi triki, kot je nagradna igra ali pa zahteva osebnih podatkov v zameno za kakšne druge ugodnosti ali uporabo (glej Kovačič 2003: 52). Torej ločiti moramo med zbiranjem in povezovanjem podatkov, saj lahko s slednjim pridobimo popolnoma nove informacije, ki so lahko za posameznika škodljive (npr. povežemo ime in bolezen).

Podatke po omrežju je mogoče prestreči s pomočjo tehnike, kjer »napadalec prestreza in analizira promet po tujih računalnik«, metodo pa je zaradi pasivne narave težko odkriti

(glej Kovačič 2003: 52-53). V zadnjem času pa se pojavlja tudi vse več kraj v zvezi z dostopom do interneta, napadi na omrežja in prestrezanjem elektronske pošte. Čeprav je javna enkripcija[6] telekomunikacij danes že zelo razširjena in nudi veliko stopnjo zasebnosti, se lahko zaradi tehničnega napredka sporočilo prestreze še pred enkripcijo (glej Marx 2002: 21). Zmeraj novejših in boljših tehnik prestrezanja podatkov in vdiranja v sisteme torej ne manjka. Seveda pa lahko določene podatke na računalniku zasežemo na čisto preprost način t.j. s **fizičnim dostopom** do računalnika. Eden izmed načinov, kako se pred tem zavarovati, je pravilna izbira gesla in ostalih varnostnih ukrepov; na trgu namreč že reklamirajo prenosne računalnike z dostopom preko prstnega odtisa. Seveda pa je podatke možno zaseči tudi z neposrednim dostopom do diska na računalniku, za kar pa niti pravilna izbira gesla ni dovolj dobra.

3.4 Satelitski videonadzor in geolokalizacija

Satelitski nadzor se v grobem deli na komunikacijski (podatkovni, avdio) in video satelitski nadzor. V zadnjem času v uporabo vse bolj stopa satelitski videonadzor. Uporablja se za različne zadeve: spremljanje vremena, pri poročanju s kriznih žarišč, pogleda v sovražnikovo ozemlje, ugotavljanja obsega in škode ob naravnih nesrečah, pri gradnji cest in mostov ter celo pri odkrivanju črnih gradenj (glej Kovačič 2000: 18). Seveda pa so na voljo že komercialni sistemi, ki imajo sposobnost razpoznati predmete v velikosti manjši od enega metra. Satelitsko sliko oz. fotografije naših kontinetov pa lahko danes spremlja vsak uporabnik interneta in sicer na maps.google.com ali s programom Google Earth. Sicer je ločljivost oz. približevanje slike odvisno od konkretnega področja sveta, ampak v najboljšem primeru je možno precej dobro videti hiše, ceste in avtomobile kot prikazuje spodnja, ne ravno najnovejša, satelitska slika Prešernovega trga v Ljubljani.

[6] Šifriranje podatkov oz. postopek, pri katerem odprto sporočilo spremenimo v prikrito sporočilo.

Slika 0-1: Satelitska video slika Prešenovega trga in Tromostovja v Ljubljani (glej maps.google.com 19. 8. 2006)

Satelitski nadzor pa je lahko z uporabo GPS naprav bolj uporaben tudi za običajne ljudi. Za to se uporablja pojem geolokalizacija[7] (*angl. geolocalization*). Ob uporabi GPS sledilca ali sistema se uporablja satelit, s pomočjo katerega GPS ugotovi svojo lokacijo glede na satelit, na primer za iskanje lokacije, kjer se posameznik trenutno nahaja. Najbolj uporabna je takšna naprava v avtomobilu, ki nam pomaga pri navigaciji, še vedno pa ne deluje brezhibno, tako da je potrebno upoštevati tudi zdravo pamet. Tudi v Sloveniji je že na voljo uporaba navigacijskih naprav, zaradi pred kratkim izdelanim digitalnim zemljevidom in vodljivo karto, ki pa se ves čas nadgrajuje. Čeprav je GPS naprava v avtomobilu že cenovno dostopnejša, se pri nas proda izjemno malo takšnih avtomobilov. V tujini pa takšne GPS naprave v avtomobilu obveščajo tudi o prometnih informacijah, npr. zastojih na cesti (glej Jure Mohorič na Val 202 26. 6. 2006).

Z GPS napravo na mobilnem telefonu lahko prav tako do nekaj metrov natančno določimo, kje se oseba nahaja. Zadeva je idealna za nadzorovanje uslužbencev, saj »sedaj ne zasledujemo več vozil, ampak uslužbenca samega« (Baebler 23. 5. 2005). Tako se lahko GPS lokacija posreduje v center preko npr. mobilnega telefona.

Kovačič (2003: 12) opisuje dva glavna načina za ugotavljanje lokacije mobilnega telefona: terminalska (lokacijo ugotovi in v omrežje sporoči mobilni telefon sam) in omrežna rešitev (lokacijo mobilnega telefona ugotovi omrežje samo), Lokacijo mobilnega telefona pa je možno ugotoviti tudi s strani mobilnih operaterjev in ne le s

[7] Določitev točke na zemeljski površini ali v bližini nje, z analiziranjem radio-frekvenčnih signalov, ki jih oddajajo različne naprave (Teleparc, 19.8.2006).

pomočjo satelita. Predvsem policija v nekaterih državah uporablja takšno sledenje za določanje lokacije uporabnikov mobilnega telefona (v primeru klica na pomoč, osumljencev kriminalnih dejanj). V svetu pa postajajo zmeraj bolj aktualni tudi t. i. *Location Service Providers*, ki starše in ostale preko mobilnih telefonov obveščajo, kje se njihov otrok v tistem trenutku nahaja (glej Ahlert in drugi 2005). V Sloveniji zaenkrat takšne možnosti še ni na trgu. V mobilni telefon se lahko vgradi tudi sledilna naprava, ki po elektronski pošti in s SMS sporočilom obvešča starše. Poseben vmesnik lahko namestijo tudi v avtomobil, s pomočjo katerega lahko ugotovijo tudi, kako hitro se njihov otrok pelje (glej Lotrič 22. 9. 2005). Zaradi takšnega nadzora otrok in najstnikov s strani staršev, pa že tečejo debate o tem, koliko zasebnosti sploh lahko imajo otroci in najstniki.

3.5 Prisluškovanje

Obstajata dve vrsti prisluškovanja: *telekomunikacijsko* in v *prostoru*, poleg tega tudi najrazličnejše vrste prisluškovalnih naprav. Banisar in drugi (glej Kovačič 2003: 16) omenjajo, da nadzor komunikacijskih sredstev omogoča t. i. »prijazno prisluškovanje«, torej prijazno in preprosto za prisluškovalca. Najenostavnejša naprava za prisluškovanje sta že t. i. babysitter in navadni mobilni telefon. S slednjim lahko prisluškovalec le-tega skrije nekam v prostor, utiša zvonjenje in pokliče na to telefonsko številko telefona ter s tem posluša dogajanje v prostoru. Na internetu se lahko zelo preprosto nabavijo tudi ostale preproste naprave za prisluškovanje. Eden od teh je tudi t. i. spy phone, ki navidez zgleda kot mobilni telefon in ob klicanju s točno določene številke klic prevzame brez zvonjenja in kakšnih motenj, ob prekinitvi pa prisluškovanje konča. Stane okoli 300 dolarjev. Obstajajo pa seveda tudi bolj izpopolnjene metode prisluškovanja, od vrhunskih prisluškovalnih naprav za mobilne telefone, katerih cena se giblje od 300.000 do 500.000 evrov, pa vse do dostopa do telefonskih pogovorov preko satelita (glej Cvetek 16. 4. 2004). Slednje uporabljajo predvsem države, delujejo pa na podlagi avtomatskega snemanja ob besedah kot so terorist, orožje, itd. (glej Cvetek 16. 4. 2004). »Profesionalne službe seveda poskrbijo za čim boljšo zaščito in varen prenos informacij, za napravo, ki si jo lahko priskrbi tudi vsak državljan in ki s kodiranjem signala poskrbi za telefonski klepet brez dodatnih ušes, pa je treba odšteti 5.000 evrov in več» (glej Cvetek 16. 4. 2004). Kupiti prisluškovalno napravo je še najenostavneje, več znanja je potrebno za

njeno namestitev, še več pa za njeno odkritje (glej Cvetek 16. 4. 2004). Tako v Sloveniji ni omejena prodaja prisluškovalnih naprav, čeprav je nezakonito prisluškovanje v zasebnih prostorih prepovedano (glej Kovačič 2003: 15).

3.6 Nadzor s pomočjo baz podatkov

Z razvojem sodobne tehnologije so se razvijale in dopolnjevale tudi različne baze podatkov. Lyon (glej Kovačič 2003: 22) zato govori o družbi dosjejev oz. proizvodnji dosjejev o posameznikih, saj če posameznik obstaja, obstaja o njem tudi kakšna evidenca. Tako so baze podatkov namenjene preverjanju posameznikove identitete, nadzorovanju financ, potrošnikov ali čemu drugemu. Večina držav (predvsem v Evropi in ZDA) ima shranjene podatke o skoraj vsakemu prebivalcu svoje države. Predvsem registri popisov prebivalstva in ostale baze državnih organov vsebujejo precej informacij o svojih državljanih. Velika specializirana podjetja za določene dejavnosti zbirajo finančne podatke o posameznikih, kjer pa navadno ne ostane le pri podatkih o finančnem stanju (glej STOA 2004). Obstaja pa še veliko drugih baz, od telefonskega imenika, imenika mest, register volivcev in veliko drugih javnih in privatnih registrov, iz katerih se lahko priskrbi profil želene osebe (STOA 2004). Zelo aktualne so marketinške baze, ki jih Lyon (2003: 162) opiše kot »industrijo vredno več milijard dolarjev, ki išče osebne podatke o potrošniških navadah, o nakupih, izbiri in življenjskem stilu, z namenom profilirati in izslediti trenutnega in potencialnega potrošnika na veliko različnih področjih življenja«. Današnjo družbo si je zato težko predstavljati brez različnih nakupovalnih kartic, kartic zvestobe in ostalih identifikacijskih kartic, od osebne, zdravstvene, bančne, kreditne in drugih kartic, ki imajo zapisane podatke o identiteti posameznika, kot tudi pametnih kartic, ki imajo pomnilnik za poznejše zapise (glej Kovačič 2003: 14). Lyon (glej Kovačič 2003: 14) ugotavlja, da »uporaba pametnih kartic omogoča zlivanje javnih, državnih in zasebnih komercialnih baz«. Obstajajo namreč različne tehnike osebne identifikacije, ki pomagajo pri povezovanju podatkov s posamezniki: glede na ime, šifro (kako posameznika poimenujejo organizacije), znanje (kaj posameznik zna) in biometričen podatek (videz, fizično konstrukcijo telesa...) (glej STOA 2004). V Sloveniji je v določenih primerih ta identifikacijska oznaka EMŠO številka, v ZDA pa Social Security Number (glej Kovačič 2003: 28). Povezovanje različnih baz med seboj

nepovezanih podatkov pa predstavlja tudi največjo skrb. Namreč, deliti moramo med zbiranjem podatkov, ki se shranjujejo v baze podatkov in med povezovanjem teh podatkov. Kot sem že omenila, lahko s povezovanjem različnih podatkov (ki kot nepovezani še morda ne delujejo škodljivo na posameznika), pridobimo popolnoma nove informacije, ki povzročajo še večjo skrb (npr. zdravstvene zavarovalnice pridobijo podatke o našem zdravstvenem stanju). Prav tako pa 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). Skratka vsa naša dejanja se z uporabo interneta, mobilnega telefona in identifikacijskih kartic beležijo, za sabo torej puščamo sledi, s tem pa se vsa naša ravnanja in dejanja shranjujejo v baze podatkov, ki jih imajo v svojih arhivih banke, podjetja, ponudniki internetnih storitev in drugi. Vendar najbolj nas mora skrbeti ravno povezovanje vseh teh podatkov in možne zlorabe.

3.7 Prevladujoča praksa

V nadaljevanju se osredotočam na prevladujočo prakso uporabe tehnologij nadzora predvsem v ZDA in Evropi. Namreč, ravno dogodki 11. septembra leta 2001 v ZDA so poostrili državno nadzorovanje, posledice pa je občutil cel svet, tudi evropske države. Namreč, na določenih predelih (letališčih, javnih športnih dogodkih) se je nadzor okrepil, prav tako tudi splošna antiteroristična zakonodaja v določenih državah Evrope, ZDA in Kanade (glej Lyon 2003: 168). V ZDA so predvsem na letališčih poostrili varnostne ukrepe, tako da so na različnih mestih letališča namestili kamere, mimo katerih naj bi potnik šel vsaj enkrat. S tem skenirajo vse potnike, ne da bi za to sploh vedeli in jih primerjajo z obrazi iz baze podatkov. Vse potnike, ki niso identificirani, pa naj bi avtomatično izbrisali (glej I. N. in Kurier 24. 4. 2002). Tudi policija in ostali organi oblasti so v ZDA dobili večjo moč in imajo dovoljenje za hitrejši odziv na »teroristični« napad (glej Lyon 2001). Tako so razširili prisluškovanje in prestrezanje elektronske pošte pri ljudeh, ki naj bi bili osumljeni »terorizma«. Nastale so nove vrste ID kartic, kot so imigracijske kartice, tečejo pa že debate o t. i. pametnih karticah, s katerimi bi lahko še natančneje spremljali posameznike (glej Lyon 2001). Nameščati so že začeli naprave za skeniranje šarenice, sprva le na letališču v Amsterdamu, kasneje tudi drugod. Opazimo

lahko tudi vedno več video kamer na javnih mestih, ne samo v ZDA, ampak tudi drugod po svetu, po možnosti podprtih s tehniko prepoznavanja obraza. Shranjujejo se tudi DNK baze z genskimi informacijami, ki so primerne za identificiranje znanih »teroristov« ali osumljencev (glej Lyon 2001). Po teh dogodkih se tako bolj izrazito kaže trend družbenega razvrščanja ljudi (glej Lyon 2006: 25).

Omenjeni dogodki so tudi povečali zavedanje o tveganjih, tako o tehnoloških tveganjih (npr. o biološkem terorizmu) kot tudi zavedanja, s katerimi se civilna populacija sooča ob večjem nadzoru (npr. izguba zasebnosti) (glej Lyon 2003: 169-174). Lyon tudi dodaja, da se najbolj hitro širi komercialna sfera nadzora. Tudi država pri iskanju administrativnih podatkov zmeraj pogosteje posega v komercialne vire (npr. podatki o klicih preko telefona, transakcije s kreditno kartico). Tako je nadzor po 11. septembru: bolj razpršen kot centraliziran, bolj vsiljiv, tehnološko usmerjen in se bolj osredotoča na preventivo kot preiskavo po dejanju (glej Lyon 2001).

Nadzor se vse bolj vrši tudi na delovnem mestu, vendar pa je v primeru nadzora zaposlenih evropska zakonodaja bolj naklonjena pravici posameznika na delovnem mestu kot zakonodaja v ZDA (glej Kovačič 2005a). Za Evropo je značilno, da morajo podjetja razkriti razsežnosti nadzora (prisluškovanje, snemanje itd.), ki ga izvajajo na delovnem mestu, prav tako pa morajo zaposleni tudi vedeti, kdaj in zakaj jih nadzorujejo. Prikrito lahko nadzorujejo le, če želijo z njim preprečiti zločin ali zlorabo. Podobno je zakonsko urejeno tudi pri nas. Po mnenju ameriškega združenja za managment, pa naj bi kar 40% podjetij v ZDA kontroliralo svoje zaposlene s skrito kamero, katera opazujejo gibanja zaposlenih med delovnim časom (glej L.V. 12. 3. 2002). V ZDA delavce tudi gensko testirajo in redno preverjajo, če niso odvisniki. Nekatera podjetja so že razvila lastna pravila o prepovedi takšnih dejanj, čeprav naj bi bile to le redke izjeme (glej L.V. 12. 3. 2002). Kovačič (2005a) pa opozarja, da lahko ima povečanje nadzora na delovnem mestu negativne učinke in da če že nadzor nad zaposlenimi, potem mora biti izveden zakonito, kar pomeni (pisno) soglasje zaposlenega.

Tudi v Veliki Britaniji se kaže trend povečanja nadzora in zaostrovanja zakonodaje. Ravno Britanci naj bi bili po nekaterih podatkih najbolj elektronsko nadzorovana populacija na svetu (glej Armitage v Surette 2004), predvsem zaradi vsem znanih video kamer na javnih mestih. Razlog za takšen izbruh videonadzornega sistema v Angliji v 80-

ih in 90-ih letih, je kulturna raznolikost in strah pred zunanjimi grožnjami, ki so pripomogle k naraščanju sprejemljivosti formalnega nadzorovanja (glej Surette 2004), glavni razlog pa je IRA. Vendar pa je videonadzorni sistem v Veliki Britaniji po novem bolj reguliran: opozorilni znaki, ki naznanjajo uporabo videonadzora; pravica posameznika o ogledu posnetkov, katere mu morajo operaterji po zakonu tudi posredovati; posnetki se naj ne bi hranili več kot 30 dni, kar pa je odvisno od tveganja institucije (npr. banke) (glej Krašič 1. 3. 2004). Drugod po Evropi je pravno urejanje videonadzora odvisno od države do države. Tudi pri nas so ga ustrezno zakonsko uredili v letu 2005, kar opisujem v naslednjem poglavju.

Omenila sem le nekaj konkretnih primerov uporabe sodobnih tehnologij nadzora po svetu, jasno pa je, da to niso edini načini uporabe te tehnologije. Primeri jasno kažejo na že omenjeno razliko med zakonodajo v Evropi in ZDA, v prid Evropi, kjer so osebni podatki dejansko last posameznika. Kot je že omenil Lyon, je po 11. septembru tudi bolj opazno razvrščanje ljudi v kategorije in večje zavedanje ljudi o tveganjih. Zaskrbljujoča pa je napoved Lyona o naraščanju komercialnega oz. privatnega nadzora, saj kot sam pravi, se ljudje manj zavedajo trgovskih kartic zaupanja, s katerimi trgovci nudijo popuste ali članske privilegije, hkrati pa zbirajo njihove podatke o nakupih. Ljudje se veliko bolj zavedajo nadzorovanja na letališčih, kjer gredo skozi večkratno preverjanje (skeniranje prtljage, pregled potnega lista in letalske karte) (glej Lyon 2006: 1-10). Ob vsem napisanem se kažejo trendi nadzorovanja v smeri zaostrovanja zakonodaje in spreminjanja sodobne tehnologije. Prav tako pa ljudje v vsakdanjem življenju niso samo nadzorovani s strani drugih, ampak so tudi sami zmeraj bolj pripravljeni uporabljati različne tehnične naprave, da bi sami nadzorovali druge in tudi sebe (glej Lyon 2006: 10). Danes je namreč na trgu zelo preprosto kupiti najnovejšo različico videonadzornega sistema za varovanje doma, enostavno prisluškovalno napravo ali test za preverjanje alkohola v telesu.

Torej nadzor po besedah Lyona (2006: 1) konstantno narašča, saj se »procesi kvalifikacije, zbiranja in zapisovanja podatkov in informacij neprenehoma množijo, življenja navadnih posameznikov pa postaja čedalje bolj transparentna« (Kovačič 2003: 23). Potemtakem nas bo v prihodnosti lahko še bolj skrbelo za svojo zasebnost in svobodo (glej Pečar 1991: 361), saj nadzorovalna tehnologije na podlagi zbranih osebnih

podatkov ne le nadzoruje, temveč lahko že predvideva naša naslednja dejanja (glej Marx 2002: 16). »Sodobna panoptična tehnologija ne čaka, da se nekaj zgodi, pač pa ukrepa že vnaprej na podlagi zbranih podatkov in ocenjenih predvidevanj; posameznike razvršča v kategorije tveganja« (Whitaker v Kovačič 2005: 30). Lep primer takšnega predvidevanja je bilo mogoče videti v ameriškem filmu Minority report, kjer so s pomočjo tehnologije predvidevali naslednja kriminalna dejanja. Drug problem tehnologije nadzora pa je tudi ta, da lahko čisto nepovezane dogodke poveže in prikaže na tak način, da neka oseba postane sumljiva (glej Kovačič 13. 7. 2006). Tako naraščanje nadzorovanja ljudi opazimo tudi v Evropi, ki že išče tesnejše poti za sodelovanje med policijo in obveščevalnimi službami v primeru novih »terorističnih« napadov v Evropi. Iskanje ravnotežja med osebnimi pravicami in varnostjo je osrednja tema tudi v Evropi, kjer njeni predstavniki že napovedujejo tesnejše in bolj neposredno izmenjavo podatkov med policijami držav članic. Čeprav se politiki strinjajo, da bodo in morajo biti pravice posameznika »uravnotežene s pravico do kolektivne varnosti« (John Reid na SLO 1 16. 8. 2006). Med državami članicami naj bi stekla tudi izmenjava biometričnih podatkov letalskih potnikov, prstnih odtisov in osebnih podatkov. Unija te že posreduje ZDA, Kanadi in Avstraliji. Ostrejši nadzor pa bo uvedla tudi na svetovnem spletu, predvsem na straneh, ki podpihujejo nasilje in sovraštvo (glej SLO 1 16. 8. 2006).

Evropska komisija je objavila tudi študijo o vplivih biometrične tehnologije na družbo (glej M. B. / STA 2. 4. 2005). »Biometrični sistemi za vstop v šolsko jedilnico, vžig avtomobila s pomočjo skenerja prstnih odtisov ali sistemi prepoznavanja obraza na avtobusih lahko kmalu postanejo realnost v vsakdanjem življenju Evropejcev« (M. B. / STA 2. 4. 2005). Čeprav je Evropa v primerjavi z ZDA veliko bolj zadržana in trenutno ne zaseda dominantnega položaja na tem področju, naj bi hitro dohitela ZDA, predvsem v bančnem sektorju. Študija omenja tudi negativne učinke: negotovost glede stroškov, zaščite zasebnosti in velika akumulacija moči tistih, ki bodo nadzirali biometrične podatke, in opozarja evropske politike, da se začnejo pripravljati na novo tehnologijo čimprej, pri tem pa morajo biti pozorni na možnosti zlorabe podatkov in vdora v zasebnost. Biometrija bo čez 10 let intenzivno navzoča v gospodarstvu, zdravstvu, pri mejnih kontrolah, na vsakdanjih mestih kot so javni prevozi, v šolskih jedilnicah, v kuhinji. Tudi otroci bodo imeli biometrične igrače, ki bodo prepoznale uporabnika.

Skeniranje šarenice naj bi se v večji meri uporabljalo za dostop do dragocenih podatkov (glej M. B. / STA 2. 4. 2005). Umislili si bomo lahko tudi popolni nadzor nad bivalnim okoljem s t. i. inteligentimi hišami, ki se sicer že pojavljajo tudi v Evropi. Takšna hiša poveže vse sisteme, kot so ogrevanje, razsvetljavo, alarmno napravo in ostalo. Vse funkcije so daljinsko vodene in jih je mogoče nadzirati preko interneta ali mobilnega telefona (glej T. S. 7. 10. 2003). Nekoliko hitreje, že leta 2007, pa želi britanska policija in notranje ministrstvo uvesti tudi elektronsko identifikacijo vozil (EVI); gre za senzorje ob cestah, ki bodo beležili vsako kršitev mimo vozečih vozil na tistem odseku ceste. Vozila bodo imela vgrajena mikrovezja, katera bodo dolžni izdelovalci avtomobilov vgraditi v vsa nova vozila; v stara vozila pa bodo to vgradili ob prvem tehničnem pregledu. S pomočjo senzorja se bodo tako ob vsakem prekršku samodejno izpisal plačilni nalog. Še bolj zaskrbljujoče pa je, da o takšnem elektronskem načinu identifikacije vozil razmišljajo tudi na sedežu EU v Bruslju (glej Triglav 2004: 65-66). Na podlagi konkretnih primerov lahko vidimo, da se nadzorovalna tehnologija zmeraj bolj integrira v vsakdanje življenje ljudi.

4. SITUACIJA V SLOVENIJI

Za predstavitev situacije nadzora in uporabe nadzorovalnih tehnologij v Sloveniji, najprej predstavljam pravno ureditev tega področja pri nas, v nadaljevanju pa še nekaj konkretnih primerov uporabe in zlorabe tehnologij nadzora pri nas, ki sem jih zasledila v medijih.

4.1 Pravna ureditev v Sloveniji

V nadaljevanju na kratko predstavljam pravno ureditev na področju nadzorovanja in zasebnosti v Sloveniji. Zakonov oz. njenih poglavij iz tega področja je kar precej, saj se nadzorovanje in zasebnost prepletata na različnih področjih življenja. Najpomembnejši pa je Zakon o varstvu osebnih podatkov.

4.1.1 Zakon o varstvu osebnih podatkov

Nov zakon o varstvu osebnih podatkov (ZVOP-1) je začel veljati s 1. januarjem 2005. Potreben je bil zaradi »uskladitve z evropsko direktivo o zaščiti posameznikov pri obdelavi osebnih podatkov in prostem gibanju takšnih podatkov« (Bogataj v Ceglar v

Delu 11.3.2005). Državni nadzornik oz. nekdanji glavni inšpektor Jože Bogataj omenja bistvene spremembe kot so splošne definicije, povečale so se pristojnosti Državnega nadzornega organa za varstvo osebnih podatkov, ki po novem dovoljuje tudi uvedbo biometričnih ukrepov v zasebnem sektorju. Zakon je uredil več področij: neposredno trženje, videonadzor, evidence vstopov in izstopov iz prostorov, uporabo javnih knjig, povezovanje zbirk osebnih podatkov, strokovnega nadzora in avtomatizirane obdelave. Tako se inšpektorji po novem imenujejo državni nadzorniki za varstvo osebnih podatkov.
S 1. 1. 2006 je v Sloveniji začel delovati tudi *Informacijski pooblaščenec*, ki je nastal z združitvijo Pooblaščenca za dostop do informacij javnega značaja in Inšpektorata za varstvo osebnih podatkov. Nov urad bo do leta 2009 vodila dosedanja pooblaščenka za dostop do informacij javnega značaja Nataša Pirc Musar. Kot dosedaj bo upravljala delo na področju dostopa do informacij javnega značaja, novost pa je delo glavnega državnega nadzornika na področju varstva osebnih podatkov. Njeno delo je med drugim (glej ip.virtua.si 2006 in M. B. in STA 31. 12. 2005): izvaja inšpekcijski nadzor nad izvajanjem določb ZVOP-1, sodeluje z drugimi državnimi organi in pristojnimi organi EU pri obdelavi osebnih podatkov, sodeluje z mednarodnimi organizacijami, tujimi nadzornimi organi, zavodi, združenji, nevladnimi organizacijami, itd. glede vseh vprašanj, ki so pomembna za varstvo osebnih podatkov (47. člen), opravlja preventivni inšpekcijski nadzor pri upravljavcih osebnih podatkov s področja javnega in zasebnega sektorja, vodi in vzdržuje register zbirk osebnih podatkov in skrbi, da je register ažuren in javno dostopen prek svetovnega spleta (28. člen), izvaja nadzor nad iznosom osebnih podatkov v tretje države (70. člen)... (glej M. B. in STA 31. 12. 2005). V nadaljevanju na kratko opisujem ključne značilnosti novega zakona.
V 6. členu zakona je opredeljen *osebni podatek*, ki je «katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko v kateri je izražen« (ZVOP-1 2004). Tako npr. video posnetki spadajo v zbirke osebnih podatkov. Tudi če se hranijo le kratek čas, gre že za zbirko, omenja Bogataj (glej Jerman 18. 3. 2005). »Pomembno je, da je posameznik določena ali določljiva fizična oseba in da za to niso potrebni veliki stroški ali veliko časa«, kar pa je odvisno od primera do primera (glej Bogataj v Ceglar 11. 3. 2005). Najbolj značilni osebni podatki so identifikacijski podatki (ime, datum rojstva, EMŠO, davčna številka, naslov bivališča, prstni odtis, fotografija), izobrazba, zaposlitev, podatki

o socialnem in ekonomskem položaju, dejavnostih v prostem času, družinskih razmerjih, itd. Podatki kot so politična, verska prepričanja, podatki o rasnem in drugem izvoru, kazenske obsodbe, zdravstveni podatki, spolno vedenje in pripadnost sindikatu pa morajo biti še posebej zavarovana (glej Volk 12. 3. 2002). Zakon določa, da se lahko osebni podatek obdeluje le za določene in zakonite namene (za zgodovinsko, statistično in znanstveno-raziskovalne namene) ali če posameznik v to privoli. V zasebnem sektorju pa se lahko obdelujejo tudi tisti podatki posameznikov, ki so sklenili pogodbo ali jo nameravajo. *Občutljivi podatki* (podatki o rasi, narodnosti, političnem, verskem ali filozofskem prepričanju, članstvu v sindikatu, zdravstvenem stanju, spolnem življenju, vpisu v kazensko evidenco ali izbrisu, vpisu za evidenco za prekrške in izbrisu) morajo biti posebej označeni in zavarovani, to pomeni, da nepooblaščeni do njih nimajo dostopa. Prav tako je potrebno posameznike, o katerih se podatki zbirajo, tudi obvestiti o namenu obdelave (glej T. S. 21. 12. 2004), torej kdo in zakaj jih upravlja. Shranjujejo pa se le toliko časa, dokler je treba za dosego namena, nato se zbrišejo ali anonimizirajo (razen če gre za arhivsko gradivo). Tisti, ki podatke obdelujejo, so dolžni varovati tajnost osebnih podatkov (glej T. S. 21. 12. 2004). Bogataj omenja, da lahko npr. internetni ponudniki zbirajo tudi IP številke uporabnikov interneta, če so ti podatki nujni za izpolnjevanje naročniških pogodb. Lahko pa jih pridobijo s pisno privolitvijo posameznikov.

Zakon ureja tudi *neposredno trženje*. Prepovedano je posredovanje elektronskih naslovov tretjim osebam, razen če posameznik to tudi dovoljuje. Posameznik lahko v vsakem trenutku tudi prepove nadaljnjo uporabo osebnih podatkov za neposredno trženje. Bogataj (glej Ceglar 11. 3. 2005) razlaga: »Podjetje mora elektronski naslov dobiti na zakonit način, za kar obstajata dve poti: posameznik svoj naslov podjetju zaupa sam, ali pa ga podjetje dobi iz javno dostopnih virov, vendar mora v tem primeru dobiti soglasje posameznika za uporabo za namene neposrednega trženja«, kar predpisuje Zakon o varstvu potrošnikov (glej Bogataj v Ceglar 11. 3. 2005). Posameznik pa lahko svoje osebne podatke za neposredno trženje kadarkoli prekliče (glej Pirc Musar 27. 3. 2006).

Vsak posameznik ima tudi **pravico vpogleda v osebne podatke, ki se nanašajo nanj**. To mu mora upravljalec omogočiti v 15 dneh ali pa mu v teh dneh pisno obrazloži, zakaj do tega ne bo prišlo. Prav tako mu mora izpis omogočit v 30 dneh. Omejene pravice ima

posameznik le v primeru evidenc policije, Sove ali Urada za preprečevanje pranja denarja (glej Bogataj v Ceglar 11. 3. 2005).

Glede *biometričnih podatkov* v javnem sektorju se smejo ti zbirati le, če to določa zakon. V zasebnem sektorju je to mogoče le, če sta izpolnjena dva pogoja pravi Bogataj (glej Ceglar v Delu 11.3.2005). »Prvič: zbiranje biometričnih podatkov mora biti nujno za varovanje ljudi, premoženja ali tajnih podatkov in tega varovanja ni mogoče zagotoviti z milejšimi ukrepi. Drugič: pred začetkom izvajanja biometričnih ukrepov mora podjetje dobiti odločbo Državnega nadzornega za varstvo osebnih podatkov« (Bogataj v Ceglar 11. 3. 2005).

Zanimivo je, da ZVOP-1 *videonadzora* sploh ne opredeli. Sicer naj bi se za njegovo opredelitev zavzemalo kar nekaj pobudnikov, vendar tega niso podprli (Jerman 18. 3. 2005). V 74. členu je zapisano, da je za izvajanje videonadzora potrebno obvestilo (da se izvaja videonadzor; naziv tistega, ki ga izvaja; telefonsko številko za pridobitev informacij, kje in koliko časa se informacije shranjujejo in da mora biti zavarovan pred dostopom do nepooblaščenih oseb). Seveda pa ima vsakdo, ki so ga posneli tudi pravico do vplogleda (30. in 31. člen): »Če so nekoga posneli, mu morajo omogočiti pravico do vpogleda, ali pa ga obvestiti, zakaj tega ne bodo storili« (Bogataj v Jerman 18. 3. 2005). Drugače imajo dostop do posnetega gradiva še državni organi kot so npr. državni nadzornik, policija ali sodišče. Znotraj določenega podjetja morajo določiti tudi odgovornega za posamezno zbirko, katerega določi sam direktor. Tako je v zakonu določeno, da delovnih prostorov ni mogoče videonadzorovati, razen v izjemnih primerih. Tako je **videonadzor v delovnih prostorih dopusten le izjemoma**, »kadar je nujen za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ter poslovne skrivnosti in tega ni možno doseči z milejšimi sredstvi« (T. S. 21. 12. 2004). Prepovedan je v delovnih prostorih zunaj delovnega mesta, predvsem v garderobah, dvigalih ali sanitarijah, zaposleni pa morajo biti pred začetkom izvajanja videonadzora o njem vnaprej pisno obveščeni (glej T. S. 21. 12. 2004). Če pa npr. turist snema s kamero, to ni predmet ZVOP. Če je turist osebo posnel proti njegovi volji, se ga lahko preganja zaradi nepooblaščenega snemanja, natančneje 149. člena Kazenskega zakonika (glej Jerman 18. 3. 2005). Tudi zasebno snemanje (npr. snemanje sosedovega vhoda) ni v pristojnosti Urada, ampak neposredno sodno varstvo na sodišču, za kar so lahko tudi zelo visoke

odškodnine, vendar se takšen primer zaenkrat še ni znašel na sodišču pri nas (glej Pirc Musar 3. 7. 2006).

Informacijska pooblaščenka Nataša Pirc Musar in državni nadzornik za varstvo osebnih podatkov Jože Bogataj v letnem poročilu za leto 2005 (ip.virtua.si 31. 5. 2006) opozarjata na nepoznavanje Zakona o varstvu osebnih podatkov. Predvsem podjetja ne poznajo oz. se ne posvečajo dovolj zakonodaji. Kar petina od vseh 91-ih prijav in pritožb posameznikov pa se je nanašala na sum kršitve zakonskih določil o izvajanju videonadzora. Prav tako pa upravljavci ne izdelajo katalogov zbirk osebnih podatkov in ne sporočajo v register zbirk, kar je možno tudi v elektronski obliki. Na Uradu namreč vzpostavljajo register baz osebnih podatkov. Vsakdo, ki ima kakršnokoli bazo osebnih podatkov, jo mora registrirati na Uradu informacijske pooblaščenke. Baza služi temu, da lahko vsak posameznik pogleda, katere institucije obdelujejo kakšne osebne podatke (npr. če nekdo vstopa v pogodbeni odnos z neko večjo trgovsko družbo, lahko na spletni strani Urada vidi, katere osebne podatke ima ta trgovska družba npr. zaradi kartice ugodnosti) (glej Pirc Musar 27. 3. 2006). Tako mora vsak upravljavec osebnih podatkov za vsako zbirko osebnih podatkov vzpostaviti katalog zbirke osebnih podatkov (26. člen) ter podatke o njem sporočiti Informacijskemu pooblaščencu (glej Marn 2006). Pooblaščenka pravi, da želijo v Uradu postaviti mejo, do kje lahko v primeru videonadzora kamere še varujejo premoženje nekega lastnika in da se ne smejo postaviti na nobeno stran (ali na stran nadzorovanih ali nadzornikov). »Osnova varstva osebnih podatkov je načelo sorazmernosti, torej zbiraj tiste podatke, ki jih potrebuješ za upravljanje svojega dela, in zbiraj toliko podatkov, da ne posežeš pretirano v zasebnost. Kako to določiti, je strašno naporno in težko delo« (Pirc Musar 3. 7. 2006). Bistvenega pomena pa je informirati obdelovalce osebnih podatkov kdaj, koliko in na kakšen način lahko osebne podatke obdelujejo (glej Pirc Musar 27. 03. 2006).

4.1.2 Zakon o elektronskih komunikacijah

Zakon o elektronskih komunikacijah (ZEK 2004), ki ga je Državni zbor sprejel leta 2004, se nanaša na delovanje in poslovanje elektronskih komunikacij kot so zagotavljanje konkurence, uporabo številk, pravice uporabnikov, zbiranje podatkov o naročnikih ter

uporabo le-teh. Tako lahko operaterji[8] zbirajo podatke o naročnikih, ki so v skladu s poglavjem o tajnosti in zasebnosti elektronskih komunikacij (101.–112. člen), poleg tega pa še tiste podatke, ki so »nujni za izpolnjevanje pogodbenih obveznosti in prometne podatke (na primer klicane številke), vendar le do popolnega plačila storitve in najdlje do zastaralnega roka, kar pomeni približno pet let« (Bogataj v Ceglar 11. 3. 2005). Bogataj (glej Ceglar 11. 3. 2005) omenja tudi primere o zbiranju ali posredovanju osebnih podatkov pri mobilnih operaterjih, internetnih ponudnikih in ostalih IKT podjetij. Večinoma je šlo za nezakonito obdelavo osebnih podatkov, uporabo osebnih podatkov za namene neposrednega trženja in pošiljanja propagandnega gradiva. Tako lahko operaterji o naročnikih zbirajo le naslednje podatke (110. člen): ime in priimek oz. firmo naročnika; EMŠO; naslov; naročniško številko; dejavnost in strokovni, akademski naziv naročnika na njegovo željo; davčno številko ter na podlagi plačila še dodatne podatke, če to želi naročnik in se s tem ne poseže v pravice tretjih oseb. Te podatke pa lahko uporabljajo le za sklepanje, izvajanje, spremljanje in prekinitev naročniške pogodb, zaračunavanje storitev ter pripravo in izdajanje naročniških imenikov v skladu s tem zakonom.

Prav tako je operater dolžan varovati zaupnost komunikacij (vsebino komunikacij, podatke o prometu in lokacijske podatke, dejstva in okoliščine neuspešnih poskusov vzpostavljanja zvez). Če operater te podatke mora pridobiti, ker so nujno potrebni za izvajanje dejavnosti, mora o tem ob sklenitvi naročniškega razmerja obvestiti uporabnika. Vse oblike prestrezanja kot so poslušanje, prisluškovanje, snemanje, shranjevanje in posredovanje komunikacij so prepovedane (103. člen), razen v primeru odredbe pristojnega organa (107. člen). Tudi lokacijski podatki[9] se smejo obdelovati le v brezosebni obliki ali s soglasjem uporabnika, ki pa lahko to kadarkoli prekliče (106. člen).

Vendar pa lahko kmalu tudi v Sloveniji pričakujemo spremembno Zakona o elektronskih komunikacijah, zaradi nove **direktive EU o hrambi prometnih podatkov**[10]. S sedanjim zakonom je namreč prepovedano shranjevanje prometnih podatkov. Takoj, ko je te

[8] Operater je fizična ali pravna oseba, ki zagotavlja javna komunikacijska omrežja ali z njimi povezane zmogljivosti oziroma izvaja javne komunikacijske storitve.

[9] Lokacijski podatki po tem zakonu so kakršnikoli podatki, obdelani v elektronskem komunikacijskem omrežju, ki kažejo na zemljepisni položaj terminalske opreme uporabnika javne komunikacijske storitve.

[10] Podatki o prometu so kakršnikoli podatki, ki se obdelujejo zaradi prenosa komunikacij v elektronskem komunikacijskem omrežju ali zaradi njegovega obračunavanja.

podatke operater obdelal in shranil, jih je moral izbrisati in anonimizirati, razen če jih je potreboval za obračun in za plačila v zvezi z medomrežnim povezovanjem oz. le z naročnikovim soglasjem v primeru trženja podatkov; seveda pa ima naročnik možnost to tudi kadarkoli prekiniti. Z omenjeno direktivo pa se tudi Slovenija pridružuje ostalim državam EU, da bodo morala vsa telekomunikacijska podjetja hraniti prometne podatke, ki se nanašajo na dostop do interneta, internetno telefonijo in internetno elektronsko pošto. Tako bo imela država vpogled tudi v »komunikacije novinarjev, kar bi ji še zlasti koristilo v primerih kritičnega poročanja ali razkrivanja nepravilnosti in tajnih dokumentov« (www.privacyblog.net 4. 5. 2006).

4.1.3 Ustava, Kazenski zakonik in ostali zakoni

Že **Ustava RS** določa *pravico do osebnostnih pravic in zasebnosti* (34. člen), ki pa ni posebej podrobneje dodelana: »Zagotovljena je nedotakljivost človekove telesne in duševne celovitosti, njegove zasebnosti ter osebnostnih pravic« (Ustava RS 1991). O zagotavljanju *varstva osebnih podatkov* govori 38. člen Ustave, ki dodaja, da je prepovedana njihova uporaba v nasprotju z njihovim zbiranjem, da se ima vsakdo pravico seznaniti z zbranimi osebnimi podatki ter pravico do sodnega varstva v primeru zlorabe (glej Ustava RS 1991). Omeniti je še potrebno, da Ustava in zakon »enako ščitita zasebnost in osebne podatke vseh ljudi, ne glede na njihov položaj v družbi«, torej so enako zaščiteni podatki in zasebnost običajnih državljanov in drugih javnih oseb kot tudi osumljencev, obtožencev in obsojencev (glej Bogataj v Jakopec in Kajzer 26. 1. 2004).

V *Kazenskem zakoniku* 149. člen opisuje, da se kaznuje neupravičeno snemanje posameznika ali njegovih krajev brez njegove privolitve in se s tem poseže v njegovo zasebnost, drugače se kaznuje z denarno kaznijo ali zaporom do enega leta.

Zakon o Sovi pa je bil ravno to leto predmet debat v Državnem zboru. Poslanci pa so se ukvarjali s podaljševanjem časa tajnega nadzora Sove. Sova bo tako lahko po odredbi predsednika vrhovnega sodišča (prej predsednika sodnika okrožnega sodišča) do 2 leti nadzorovala pošto in prisluškovala telefonskim pogovorom tistih, ki bodo domnevno ogrožali varnost države (glej RTV SLO in STA 31. 5. 2006). Pred tem je imela pravico takšnega početja le do 6 mesecev (glej RTV SLO in STA 31. 5. 2006). Seveda pa je

potrebno omeniti, da lahko legalno prisluškujejo le policija, Sova in Obveščevalno-varnostna služba Ministrstva za obrambo, za ostale je prisluškovanje kaznivo.
Vsekakor pa je vse odvisno od konkretne situacije v povezavi z nadzorovanjem, saj se lahko določen problem nanaša še na vrsto drugih zakonov in poglavij, ki jih v tem delu nisem omenila, npr. Zakon o zasebnem varovanju, Zakon o varstvu potrošnikov, Zakon o delovnih področjih in verjetno še kateri.

4.2 Podobe v slovenskih medijih

V tem poglavju predstavljam različne zlorabe v povezavi tehnologij nadzora v Sloveniji, ki so odmevale v slovenski javnosti preko medijev. Vsekakor pa to niso edini dogodki v povezavi z nadzorovanjem pri nas.

4.2.1 Videonadzor v slovenskih mestih

Pri videonadzoru v slovenskih mestih se osredotočam na konkretne primere videonadzorovanja tako na javnih prostorih, v šolah, trgovinah, na avtobusih kot tudi v privatni okolici. Zanimivo je, da naj bi bilo v Ljubljani postavljenih kar 4.000 kamer, od katerih je 800 usmerjenih na javne površine (glej Mazzini 1. 10. 2002). Kar nekaj jih je mogoče zaslediti tudi na spletu: Dalmatinova ulica, Kolodvorska ulica, križišče Štajerske in Brnčičeve ulice[11]. Vsekakor to niso edine kamere, ki snemajo dogajanja na ulicah ali cestah. V začetku leta 2005 so se za videonadzor središča mesta odločili tudi v Piranu. Na Tartinijevem trgu naj bi postavili tri kamere, ki bi neprekinjeno snemale dogajanja na trgu. Razlog je bil zmeraj pogostejši vandalizem mladih (glej B. Š. 26. 1. 2005). Poleg kamer v živo, pa v Sloveniji narašča tudi ponudba storitev videonadzora, saj je že na spletu možno najti kar nekaj takšnih podjetij. Cene paketov se začnejo že pri slabih 30 tisočakih. O zaščiti svojega doma tako razmišlja vedno več Slovencev, čeprav se posamezniki za tehnično varovanje odločijo šele takrat, ko doživijo kakšno slabo izkušnjo (glej Delo Stik 28. 9. 2001). Tako se veliko ljudi odloči za videonadzor lastnega

[11] Primeri videokamer na spletu: http://www.bit.si/ldvn/- , http://www.bit.si/ldvn/kolodvorska.html in http://www.spica.si/company/kamera.aspx.

doma, kjer pa lahko oko kamere opazi tudi sosedovo površino. V tem primeru se ni mogoče sklicevati na Zakon o varstvu osebnih podatkov, saj ta ne posega v sfero zasebnosti v primeru, ko se posamezniki odločijo za videonadzor za domačo uporabo. V tem primeru lahko oseba sproži postopek po Kazenskem zakoniku o neupravičenem slikovnem snemanju ali vloži odškodninsko tožbo na sodišču. V primeru snemanja sosedove hiše ima tudi policija zelo omejene pristojnosti, saj lahko ukrepa le v primeru kaznivega dejanja o neupravičenem snemanju po Kazenskem zakoniku. Vendar pa policija nima pravice in pristojnosti kamere odstranjevati, takšno ovadbo le posreduje pristojnemu državnemu tožilstvu, ko zbere ustrezne dokaze in predloži tožilstvu v nadaljnji postopek (Val 202 19. 7. 2006). Odstranitev kamere bo morala oseba zagotovo doseči po sodni poti preko civilne tožbe (Val 202 19. 7. 2006). Torej brez vpletanja sodišča je v tem primeru skoraj nemogoče odstraniti video kamero.

14. februarja 2005 je želel občan Velenja ženskemu kolektivu v podjetju za valentinovo podariti drobna darilca, zato se je odpravil v vrtnarski center na Koroški cesti v Velenju pišejo v Več (glej Jerman 18. 3. 2005). Tri dni kasneje ga je žena doma zaslišala, če je mogoče kaj kupoval v tem centru. Namreč, ženi je videoposnetke pokazal njen sorodnik, ki je tam zaposlen kot varnostnik. Prizadeti omenja, da ni imel vrtnarski center nikjer na vhodu označeno, da je objekt pod videonadzorom. Prav tako pa meni, da gre za grob poseg v njegovo zasebnost, početje varnostnika pa je bilo zelo neodgovorno in nestrokovno. Primer je podal naprej na Ministrstvo za notranje zadeve, posredoval pa ga je tudi novinarjem. Vodja poslovne enote tega vrtnarstva zatrjuje, da pri njih ne snemajo. Sicer naj bi imeli kamere pripravljene, vendar te ne snemajo, ampak samo spremljajo dogajanja, saj videonadzora še nimajo v celoti nameščenega. Po njihovem mnenju žena sploh ni mogla videti posnetka, ker dejansko ne obstaja, zato imajo pri anonimni prijavi popolnoma čisto vest. Po podatkih Jožeta Bogataja to področje ureja 74. in 77. člen Zakona o varstvu osebnih podatkov, da je za izvajanje videonadzora potrebno obvestilo, in člen, ki se nanaša na videonadzor v delovnih prostorih. Ker definicija videonadzora dejansko ne obstaja, Bogataj razmišlja, da je težko reči, da gre v tem primeru za videonadzor, saj varnostnik samo gleda, torej gre za nekakšno televizijo zaprtega kroga. Čeprav se po drugi strani tudi strinja, da gre za videonadzor in bi ga morali v vrtnarstvu tudi ustrezno označiti. S 27. januarjem 2004 so na dveh mestnih ljubljanskih avtobusih

poskusno uvedli videonadzorne kamere (glej Krašič 20. 2. 2004). Zanje so se odločili zaradi pogostejših napadov na voznike in strmega naraščanja vandalizma. Podatke so snemali na trdi disk in jih hranili 24 ur (glej Krašič 20. 2. 2004). Avtobus je imel na vstopnih vratih tudi ustrezno označeno nalepko za videonadzor. Seveda pa je v letu 2004 veljal še stari zakon o varstvu osebnih podatkov. Tudi dejstvo, da lahko po zakonu o Slovenski obveščevalno varnostni agenciji in Zakonu o policiji le ta dva organa nadzorujeta javne površine, bi lahko inšpektor izdal odločbo za odstranitev vseh drugih naprav. Vendar pa videonadzor na avtobusih naj ne bi bil pravno sporen, saj naj bi varovanje avtobusov sodilo v sklop varovanja premoženja in ni sporno, če ima izvajalec licenco za varovanje premoženja (31. člen Zakona o zasebnem varovanju). Tako lahko po mnenju Štefana Gostiča, sekretarja na Ministrstvu za notranje zadeve, zasebna varnostna podjetja pri opravljanju nalog varovanja izvajajo številne ukrepe, tudi videonadzor (glej M. A. K. 25. 2. 2004). Tako naj bi bilo na ljubljanskih mestnih avtobusih nameščenih že 22 kamer, 16 pa jih lahko pričakujemo še v prihodnje (Praš 18. 9. 2006).

Konec junija 2006 pa je razburila vest Informacijske pooblaščenke Nataše Pirc Musar (glej RTV SLO 26. 6. 2006) o snemanju garderob v trgovski hiši Emporium v Ljubljani. V zakonu je jasno opredeljeno, da je snemanje v delovnih prostorih zunaj delovnega mesta, zlasti v garderobah, dvigalih in sanitarnih prostorih, nedopustno, tudi z opozorilno nalepko. Emporium je na opozorilo pooblaščenke nemudoma odstranili štiri vrtljive kamere usmerjene na slačilne kabine, hkrati pa tudi poostril nadzor nad sobo, kjer posnetke shranjujejo. Tako je danes soba pod ključem, dostop do nje pa ima le nekaj izbranih ljudi. Omeniti še velja, da je videonadzor v Emporiumu opravljala za to usposobljena varnostna služba, vendar kljub temu v takšnem primeru odgovornost nosi naročnik, v tem primeru Emporium. Vsekakor je ta novica vzbudila veliko zanimanja v medijih in s tem opozorila tudi vsa ostala podjetja in trgovske družbe, ki tako ali drugače nezakonito posegajo v zasebnost potrošnikov ali delavcev.

Zanimivo pa je, da o videonadzoru razmišljajo tudi nekatere slovenske šole. Argument je, da je »učinkovit ukrep za zagotavljanje osebne varnosti učencev« (Novak v Mazi 14. 2. 2005). Tako imajo nekatere šole poleg varnostnikov tudi videonadzor. Čeprav je navdušenja o videonadzoru s strani staršev in prav tako učiteljev precej manj, dilem glede varnostnikov in receptorjev na šoli skoraj ni. Starši si sicer želijo večje varnosti svojih

otrok, a si ne želijo nenehnega nadzora (glej Čakš 6. 12. 2004). Vprašanje pa je, če bo zaradi več kamer na šoli tudi manj vrstniškega nasilja.

4.2.2 Videonadzor na slovenskih cestah

Na slovenskih cestah je možno zaslediti precej kamer, ki snemajo razmere na njih, pri katerih je možno tudi spremljanje v živo preko spleta[12]. Tudi Dars (2006) ima na avtocestah nameščenih precej kamer, na njihovi strani je na razpolago spremljanje 35-ih avtocestnih kamer. Seveda pa je tudi Dars zavezan k spoštovanju zakona o izvajanju videonadzora. 74. člen ZVOP-1 določa, da mora za izvajanje videonadzora pripeti obvestilo. Po podatkih spletnega portala slo-tech.com (glej Marn 5. 12. 2005) pa je takšno obvestilo moč videti le na kabinah cestninskih postaj. Zanemarjeni naj bi bili številni odseki (odprti oz. polodprti), ki ne zahtevajo plačevanja cestnine (npr. gorenjska avtocesta do cestninske postaje in ostale), zato voznik z videonadzorom ni seznanjen, saj ni prečkal cestninske postaje. »V kolikor videonadzorne kamere s svojo ločljivostjo in/ali možnostjo približevanja omogočajo razbiranje registrske oznake na vozilu, Dars na teh odsekih z ne-označitvijo izvajanja videonadzora, krši zgoraj citirani 2. odstavek 74. člena ZVOP-1.« (Marn 5. 12. 2005). S tem pa se strinja tudi Jože Bogataj, ki dodaja, da kršitve Darsa ne veljajo, če bi izvajanje videonadzora dovoljeval še kakšen drug zakon, ki pa ga v tem primeru ni. Dars pravi, da "na vseh cestninskih postajah je na vidnem mestu (kabina) označeno izvajanje videonadzora. Videonadzorni sistemi v predorih pa se izvajajo na osnovi smernic EU glede varnosti v predorih." Pred kratkim pa je Dars že postavil opozorilne table še na ostalih vhodih na avtocesto.

Avtor članka dodaja, da še niso uspeli poiskati dokazov, da Darsov videonadzorni sistem dejansko tudi razpoznava registrske oznake, ki so v tem primeru po ZVOP-1 osebni podatek. Na podlagi podatkov o ločljivosti Darsovih kamer pa je mogoče sklepati, da je prepoznavanje registrskih oznak možno, če je vozilo dovolj blizu kameri in če posamezna kamera omogoča približevanje.

Shranjevanje podatkov na Darsu traja od 1 do 7 dni, odvisno od vrste in starosti sistema za shranjevanje takšnih posnetkov. Omenjajo pa še, da nimajo centraliziranega sistema,

[12] Primeri videokamer na slovenskih cestah: http://www.pro-vreme.net/index.php?ID=12, http://freeweb.siol.net/dusanbo/ in http://www.spica.si/company/kamera.aspx.

torej se posnetki kamer na cestninskih postajah shranjujejo kar na lokaciji teh postaj, posnetki iz kamer ob avtocesti in predorih pa se shranjujejo na lokaciji centrov za nadzor in upravljanje prometnih tokov ali na najbližji cestninski postaji.

V letu 2004 pa naj bi Dars na podlagi odredbe preiskovalnega sodnika organom pregona posredoval 98 videoposnetkov, do konca julija 2005 96 videoposnetkov. Dars sme posnetke organom pregona posredovati le z odredbo preiskovalnega sodnika, čeprav pa je v 236. členu Zakona o varnosti cestnega prometa zapisano, da »Ministrstvo za notranje zadeve, policija, upravna enota in javna agencija imajo v zvezi s svojim delom pravico pridobiti in uporabljati podatke o imetnikih vozniških dovoljenj, kandidatih za voznike motornih vozil, vozilih, prekrških in kaznivih dejanjih voznikov, storjenih v cestnem prometu, ter o izrečenih kaznih in ukrepih.« Marn razmišlja, »ali je Slovenija preko 236. člena ZVCP-1 dejansko uzakonila obvezno hrambo ter posredovanje videoposnetkov cestnega prometa« (Marn 5. 12. 2005).

7. novembra 2005 je policija v sodelovanju z Darsom izvajala tudi preventivno akcijo umirjanja prometa na štajerski avtocesti med Vranskim in Blagovico. Predstavnik policije je povedal, da je policija za "za ugotavljanje kršitev in za opazovanje uporabila tudi posnetke iz kamer, ki so že inštalirane na temu odseku avtoceste, pod pogojem, da bodo ti posnetki zagotavljali identifikacijo kršitelja in vse potrebne podatke za dokazovanje kršitve" (Marn 5. 12. 2005). Torej je razpoznavanje registrskih oznak vendarle mogoče.

4.2.3 Biometrični potni listi in nadzor na slovenskem letališču

V jeseni 2006 bodo v Sloveniji začeli izdelovati biometrične potne liste. Pogoj za takšno izdelavo so določile ZDA za vse tiste države, ki za njen obisk ne potrebujejo vizuma (glej Piano 25. 4. 2004). Med njimi je tudi Slovenija, katere državljani lahko do 90 dni po ZDA potujejo brez vizuma. V novih potnih listih bosta dva biometrična identifikatorja: posnetek obraza in prstni odtisi, shranjena v posebnem čipu (glej Miko 1. 6. 2004). Slovenija je prve potne liste začela tiskati 28. 8. 2006. Sprva bo v njem shranjen le posnetek obraza, prstni odtis pa bodo dodali leta 2009. Prav tako bo imel vsak potni list tudi navodila za uporabo, saj bo potni list zaradi priloženega čipa bolj ranljiv. Čeprav vlada trdi, da bodo podatki zelo dobro varovani, je Evropo prestrašil nemški raziskovalec, ki mu je uspelo kopirati in prenašati podatke v evropskih potnih listih, ki so se v Nemčiji

začeli izdajati že leta 2005. Pri tem je uporabil standarde, ki so objavljeni na spletni strani Mednarodne organizacije za civilno letalstvo. Na Cetisu, ki naše dokumente tudi izdeluje, pravijo, da je v tem trenutku biometrični potni list 100% varen, varnost pa bodo okrepili in nadgradili še ob dodanem prstnem odtisu. Dodali so tudi, da bodo imeli »pošteni ljudje z biometričnim potnim listom manj težav, kriminalci pa vsekakor več« (Mauer na Val 2002 10. 8. 2006). Tako naj bi biometrični sistemi za preverjanje potnih listov, legitimacij in vizumov državam pomagali v boju proti ponarejanju osebnih podatkov, nezakonitemu priseljevanju in terorizmu. Nasprotniki pa opozarjajo, da so napake pri vsaki biometriji še vedno mogoče. Gre tudi za globok poseg v zasebnost, saj tukaj ne gre za običajno geslo, ampak podatke, ki so unikatni vzorec posameznika (glej Miko 1. 6. 2004).

Bojan Lučovnik, vodja varnosti in zaščite pri Aerodormu Ljubljana, je za Nedelo (glej Sušnik 22. 2. 2004) povedal, da na letališču Brnik za zdaj še ni standardov za biometrijo, ki bi »postopek kontrole verjetno precej poenostavila in pospešila«. Strinja pa se, da bodo biometrične meritve v prihodnosti igrale pomembno vlogo, ker je s tem sistem skoraj nemogoče prelisičiti. Tako EU že pripravlja tehnične standarde za biometrijo, na nekaterih letališčih pa že potekajo testne faze takšnega uvajanja. Drugače je nadzor celotnega letališča podprt z videonadzornim sistemom, ki je usmerjen na prehode, del kamer pa nadzira tudi širšo okolico. Lučovnik tudi dodaja, da njihov »namen vseeno nikoli ni bil iz letališča narediti trdnjavo«.

4.2.4 Prisluškovanje SOVE in nasploh

V tedniku Mladina (glej Praprotnik 9. 10. 2001) so pred leti zapisali, da imajo trdne dokaze, da se je Sova po terorističnih napadih z odredbo sodišča oglasila pri upravljavcih strežnikov elektronske pošte ter zahtevala, naj jim omogočijo nadzor telekomunikacij določenih oseb. Po zakonu o Sovi je takšen poseg mogoč le, če je v Sloveniji izkazana velika verjetnost, da je varnost države ogrožena. Po drugi strani pa je svet za nacionalno varnost presodil, da je ogroženost Slovenije po 11. septembru majhna. V Sovi so na to odgovorili, da je »svoje zakonsko določene naloge vedno izvajala z veljavnimi predpisi« (Praprotnik 9. 10. 2001). Če je vse to res, potem verjetno ne gre samo za nadzorovanje elektronske pošte. Legalno pa lahko prisluškujejo le policija, Sova in Obveščevalno-

varnostna služba Ministrstva za obrambo, za ostale je prisluškovanje kaznivo. »Dokaze, da vašim telefonskim pogovorom prisluškujejo državne službe, je zelo težko dobiti«, meni lastnik detektivskega podjetja Nikola Prokšelj (glej Cvetek 16. 4. 2004), nekoč delavec Službe tajne varnosti. Le z vabo se je mogoče prepričati, torej lansirati neke informacije in potem počakati na reakcijo. Dodaja tudi, da če posameznik nima dragocene in pomembne informacije, potem je za prisluškovanje nezanimiv.

Prisluškovanje je nekaj vsakdanjega v gospodarstvu, ravno detektivska stroka pa naj bi delala izključno zanje. V takšnih podjetjih preverjajo lojalnost zaposlenih, zlorabe bolniškega dopusta in tatvine v službi, premoženje dolžnikov. Do teh informacij se je zelo težko prikopati s prisluškovanjem (glej Cvetek 18. 4. 2004). Drugače pa je samo podjetje za prisluškovanje najbolj zanimivo v času sprememb, kar lahko zelo vpliva na poslovanje podjetja, npr. zamenjavo uprave. Menedžerji se naj bi tega vse premalo zavedali. Najbolj zanimiva so hitro rastoča podjetja in skupine podjetij, grozdi. Najpogostejše metode pa se je mogoče naučiti prav iz filmov. Ena izmed teh je ta, da ima prisluškovalec v podjetju zaveznika. S pridobivanjem informacij pa je povezano pridobivanje denarja oz. drugih koristi. Največkrat so najbolj zanimive informacije cene (56%) in razvojni program (33%).

Lastnik detektivske agencije Franc Sterle (glej Cvetek 18. 4. 2004) meni, da tudi država posega v zasebnost državljanov, saj lahko po digitalnih linijah prisluškuje tudi v prostoru: »Telefonski aparati, ki so jih z napeljavo linije ISDN dajali zastonj, so narejeni tako, da lahko po telefonski liniji prisluškujejo v prostoru, kjer je aparat.« Uroš Spruk, ki se prav tako ukvarja s »protiprislušnimi« pregledi, ugotavlja, da si ljudje »sploh ne predstavljajo, koliko je nepooblaščenega zbiranja podatkov«. »Ljudje zelo podcenjujejo odtok informacij in imajo površen odnos do varovanja podatkov« (Spruk v Cvetek 18. 4. 2004).

4.2.5 Pametne, trgovske in zdravstvene kartice

Trend neanonimnega (negotovinskega) kupovanja se širi s spletnih trgovin tudi v klasične trgovine z nakupovanjem s kreditnimi karticami, karticami zvestobe, popusti v zameno za osebne podatke. Ravno osebni *podatki o kupcih* pa pomenijo konkurenčno prednost, zaradi česar so trgovci "v zameno za njih pripravljeni ponuditi premijo v obliki popustov, daril ali sodelovanja v nagradnih igrah" (Marn 2006). V največjih slovenskih trgovinah

kot so Mercator, Spar, E.Leclerc in Tuš ves čas ponujajo različna darila in popuste za zveste kupce. Pri Mercatorju ta hip ponujajo za dovolj veliko zbrano število nalepk atraktivno darilo popolnoma zastonj, v zameno pa želijo le osebne podatke (ime, naslov, davčno številko). Aljaž Marn (glej www.privacyblog.net 7. 2. 2005) opisuje koristi od teh kartic s strani trgovcev s pomočjo vprašalnika, ki so ga poslali družbam Merkur, Mercator, Rudnidis (E.Leclerc) ter Engrotuš (Tuš). Odgovore so dobili le iz Merkurja in Mercatorja, le slednji pa je poslal popolne odgovore. Mercator nudi dve vrsti kartic, eno je kartica ugodnosti, druga pa je plačljiva. Za pridobitev takšne kartice je potrebno soglasje s splošnimi pogoji in posredovanje osebnih podatkov (ime in priimek, bivališče, datum rojstva, ponavadi pa še kakšna izobrazba, zaposlitev), v primeru plačljive kartice pa je obseg osebnih podatkov tudi večji. »Ena izmed osnovnih koristi izdajateljev tovrstnih kartic je nedvomno privabljanje kupcev oziroma preprečevanje bega kupcev h konkurenci« (Marn na www.privacyblog.net 7. 2. 2005). Poleg tega pa vse zbrane podatke uporabljajo vsaj za interne raziskave. Povsem mogoče pa je, da z zbranimi podatki ustvarijo profil kupca, glede na pogostost obiskovanja trgovine, kupljene izdelke, porabljen denar. V Mercatorju se ob nakupu s kartico zabeležijo podatki o vrednosti, času in mestu nakupa ter podatki o kupcu. Dovoljenje za zbiranje podatkov so podpisali vse imetniki teh kartic, pošiljajo pa jim tudi obvestila o posebni Mercatorjevi ponudbi. Zakon trgovce tudi zavezuje, da teh podatkov ne smejo posredovati tretji osebi. Sicer podatkov o posameznih kupljenih izdelkih še ne spremljajo. O uporabi zbranih podatkov za tržne raziskave so povedali: »zbrani podatki nam predstavljajo osnovo za njihovo analizo, rezultati le–te pa nam omogočajo ustrezno pripravo nadaljnjih aktivnosti za naše kupce, saj želimo najbolj zvestim kupcem ponuditi tudi druge posebne ugodnosti in pozornosti« (Marn na privacyblog.net 7.2.2005). Razvoj gre torej zmeraj bolj v smer »personalizirane obravnave posameznega kupca znotraj določene skupine s podobnimi specifičnimi lastnostmi in navadami (profiliranje)" (Marn 2006), sploh zaradi nižanja cen informacijske tehnologije.

Omeniti pa velja tudi zmeraj bolj aktualne RFID etikete[13]. V skladu z evropsko zakonodajo mora vsaka družba, ki uporablja tovrstno tehnologijo, o tem obvestiti potrošnika, da izdelek vsebuje takšno etiketo ter kako jo odstraniti in priti do zapisanih podatkov v njej. Največja skrb evropskih potrošnikov zaradi takšnih etiket je namreč že omenjeno profiliranje kupcev (glej www.privacyblog.net 23. 3. 2005).

Prvo *pametno kreditno kartico* je pri nas ponudila Banka Koper. Kartica poleg klasičnega magnetnega zapisa vsebuje tudi čip, s katerim želijo v banki zmanjšati možne zlorabe. Nanje je možno shraniti osebne podatke in digitalne certifikate, poleg tega pa tudi službene podatke, beležke, adresar, priljubljene spletne strani (glej Viršek 18. 2. 2004).

Od maja 2006 se na slovenskih *zdravstvenih karticah* nahajajo tudi podatki o zdravilih, ki jih pacienti prejmejo na recept. Ker so podatki o izdanih zdravilih občutljivi osebni podatki, je zavod zagotovil visoko stopnjo njihovega varovanja. Vpogled do teh podatkov imata le zdravnik in farmacevt v lekarni. Medicinska sestra do teh občutljivih podatkov nima dostopa, razen če jo pooblasti zdravnik (glej Val 202 5. 6. 2006). Posameznik sicer lahko vpogled prepove farmacevtu, zdravniku pa zaradi narave zbiranja takšnih podatkov ne more (glej Val 202 5. 6. 2006). Namen je torej vse večja varnost bolnikov, saj ti uporabljajo vedno več zdravil, hkrati pa tudi racionalizacija pri stroških za zdravila. Podatki o zdravilih se bodo začeli zapisovati ob prvem potrjevanju kartice na samopostrežnem terminalu (glej Val 202 5. 6. 2006). Na kartico se bo lahko zapisalo največ 46 zapisov zdravil, ko pa bo kartica zapolnjena, se bo ob novem zapisu izbrisalo najstarejše zdravilo. Seznam občutljivih zdravil (npr. zdravilo za zdravljenje HIV) bo sestavila Komisija RS za medicinsko etiko in se na kartico ne bodo zapisovala. Na zdravstvenih karticah pa se bo v prihodnje zapisovalo še več pomembnih podatkov kot so »zapis težkih alergijskih reakcij in preobčutljivostnih reakcijo na zdravila, ki bodo namenjeni zdravnikom, farmacevtom in drugim zdravstvenim delavcem za pravilno ukrepanje v urgentni situaciji, ko bolnika ne poznajo. Končni cilj, ki so si ga zastavili, pa je uvedba elektronskega recepta« (Poklič 11. 4. 2006). Takšni podatki bodo v primeru nesreč res v korist ponesrečenemu, vendar pa se je potrebno zavedati tudi možnih zlorab,

[13] RFID oz. RadioFrekvenčna IDentifikacija je etiketa, ki vsebuje tiskano vezje in anteno, sprejema in oddaja podatke, ki jih lahko poljubno obdelujemo. RFID etike naj bi postopno izrinile črtno kodo. Na primer nakupovalno košarico samo postavimo na ustrezno mesto in RFID sprejemnik v hipu samodejno ugotovi seznam predmetov v košarici. (sl.wikipedia.org 20. 8. 2006)

saj lahko dobijo podatke v roke zdravstvene zavarovalnice ali direktor podjetja, v katerem je posameznik zaposlen.

4.2.6 Nadzor na delovnem mestu

Nova tehnologija omogoča delodajalcem zmeraj bolj podroben nadzor na zaposlenimi. Crossman in Lee-Kelley (glej Stanković 21. 12. 2005) opozarjata, da lahko ima nadzorovanje na delovnem mestu tudi negativne učinke, saj lahko zmanjša motivacijo zaposlenih. To je ugotovila tudi britanska vlada, ki se strinja, da povečani nadzor zmanjšuje produktivnost zaposlenih, s tem poveča stres ter zmanjša zmožnost učinkovitega organiziranja dela (glej L. V. 12. 3. 2002). Z nadzorom želijo delodajalci zavarovati podjetja, zaradi vedno več informacij na spletu, tudi virusov; drug namen pa je vrednotenje posameznikove uspešnosti (glej Baebler 23. 5. 2005). V Sloveniji se zaposleni največkrat pritožujejo »zaradi nadzorov bolniške odsotnosti, uporabe alkotestov, videonadzora na delovnem mestu in celo spremljanja gibanja službenih vozil« (Kocmur 11. 9. 2005). Državni nadzornik pa je ugotovil, da veliko delodajalcev zbira tudi podatke »o narodnosti, o imenu očeta, o osebni izkaznici, o članstvu v raznih organizacijah, o stanovanjskih in socialnih razmerah, o prostočasni dejavnosti« (glej Bogataj v Volk 12. 3. 2002) ali celo o družinskih članih kandidatov za zaposlitev. Razlog za takšno zbiranje je velikokrat nezadostno poznavanje in razumevanja zakona (glej Bogataj v Volk 12. 3. 2002).

Precej bolj strog pravilnik so dobili tudi na Inštitutu RS za varovanje zdravja ob prihodu takratnega novega direktorja Andreja Marušiča leta 2002, omenjajo v Nedelu (glej Kocmur 11. 9. 2005). Navedene so bile hujše kršitve zaposlenih, npr. prihod na delo pod vplivom alkohola (dovoljena meja je 0,0 promila), prepovedanih drog, kajenje na delovnem mestu in v okolici, nespoštovanja navodil zdravnika med odsotnostjo zaradi bolezni, poškodbe ali dojenja. Zagrožena je bila celo redna ali izredna prekinitev pogodbe, sicer pa zaposlen najprej dobi pisno obvestilo (glej Kocmur 11. 9. 2005). Lahko bi celo rekli, da gre za kratenje človekovih pravic, saj v dokumentu ni opredeljena beseda okolica, torej bi konec koncev to lahko pomenilo tudi prepovedano kajenje v sosednjem lokalu, prav tako pa lahko alkotest pokaže več kot 0,0 promila ob zaužitju kakšne hrane. Svetovalka za pravne zadeve na IVZ Zdenka Jakopanec (glej Kocmur 11. 9. 2005) meni, da »spiti kozarec vina med kosilom ni več zaželeno, zaposleni, ki bi v nedeljo zvečer,

denimo, praznoval rojstni dan, v ponedeljek pa bi bilo v njegovi krvi še kanček alkohola, pa naj vnaprej razmišlja o posledicah.« Dodaja še, da bodo preganjali zares problematične pivce in ne vse povprek. Glavni republiški inšpektor za delo Borut Brezovar je v dokumentu našel številne pomanjkljivosti ali celo nezakonita določila. Vodilni naj bi sicer imeli pravico preverjati alkoholiziranosti ali drogiranosti zaposlenih, vendar le če je za to utemeljen sum kršitve, kar pa mora biti v pravilniku jasno zapisano. Meni, da je 0,0 promila alkohola v krvi dovoljena zahtevka, ampak skrajno neživljenjska in bi bila smiselna v prometu in ostalih poklicih, npr. pri šoferjih. Prav tako pa je prepovedano pošiljanje laičnega nadzora in detektivov kar vse povprek nad zaposlene, ki so npr. v bolniški. Spremljanja gibanja službenih vozil se sme uporabljati zgolj za nadzor nad stroški med delovnim časom, ni pa dovoljeno nadzorovanje zaposlenega, ki vozilo uporablja med prostim časom.

Primer *videonadzora na delovnem mestu* se je zgodil tudi v podjetju Comet, kjer so stavkajoči delavci med drugim zahtevali tudi njegovo odstranitev (glej Repovž 21. 4. 2004). Kamere so bile postavljene v proizvodnih prostorih. Inšpektorat za delo je ugotovil, da je videonadzor postavljen v skladu s pravili, vendar pa mora uprava namestiti še ustrezna obvestila o videonadzoru, saj so bili delavci o njem obveščeni le preko internetnega glasila. Videonadzor se sme v delovnih prostorih izvajati le za »zagotavljanje varnosti ljudi in premoženja ob pogoju, da je to edini način, s katerim je mogoče zagotoviti to varnost«, omenja Jože Bogataj (glej Repovž 21. 4. 2004). Prav tako pa je prepovedano snemanje prostorov kot so garderobe, dvigala in sanitarije, zaposleni pa morajo biti o videonadzoru pisno obveščeni. Videonadzora ne smejo uporabljati za nadzor delovne discipline ali za prisluškovanje zaposlenim (glej Kocmur 11. 9. 2005).

V Merkurju so od začetka leta 2005 uvedli nov sistem delovnega časa in elektronsko evidetiranje, med drugim tudi elektronsko evidenco dostopa v prostore (glej Volk 21. 12. 2004). Marsikatero podjetje meni, da mora vodstvo svojim zaposlenim bolj zaupati, tega pa se ne da nadomestiti z nadzorom, ampak le s pogosto komunikacijo med zaposlenimi in vodstvom. S tem se strinja tudi Mobitel, čeprav dodaja, da ukrepi, ki jih izvajajo v podjetju, niso namenjeni nadziranju ljudi, temveč za lažje, hitrejše in varnejše poslovanje, predvsem pa za zavarovanje delavcev in zaščito sredstev (glej Volk 21. 12. 2004).

4.2.7 Nadzor in zasebnost v virtualnem prostoru

Na Arnesu pravijo, da na mesec dobijo okoli 150 prijav (glej Cvetek 28. 5. 2004). Na centru spremljajo le prijave o vdorih ali njihovih poskusih. Če so napadi prišli iz tujine, jih posredujejo tujim ponudnikom, drugače pa o nedovoljenem početju uporabnikov opozorijo slovenske ponudnike. Če je dejanje kaznivo, o tem obvestijo policijo (glej Cvetek 28. 5. 2004).

Precej prahu pa je sprožil tudi spletni naslov *udba.net,* ki je bil registiran v New Yorku 6. marca 2003, strežnik pa se je nahajal na Tajskem v Bangkoku (glej Žerdin 18. 4. 2003 in Primožič 2005: 56). Stran je v slovenski javnosti dvignila veliko prahu, saj je bilo na njej objavljeno več tisoč strani gradiva zaupne narave, med njimi tudi skoraj več sto tisoč imen in priimkov Slovencev skupaj z matičnimi podatki (datum, letnica rojstva, imena staršev, podatki o zaposlitvi, državljanstvu, kaznivih dejanjih, ki jih je nekoč vodila Služba za državne varnosti – SDV, podatki ki se tičejo državne varnosti – številke dosjejev občanov iz evidence SDV s kategorijami kot so sodelavec SDV, nadzorovana oseba itd.). Stran naj bi vsebovala podatke iz Centralne aktivne evidence, ki jo je nekoč upravljal Republiški sekretariat za notranje zadeve iz bivše Socialistične republike Slovenije. SDV se je ukvarjala tako z notranjimi in zunanjimi sovražniki kot tudi tistimi, ki naj bi po njihovem mnenju ogrožali varnost tedanje ureditve. Na strani, na kateri so se pojavila imena znanih in manj znanih oseb, je bilo možno osebe iskati po začetnicah priimka (glej Žerdin 18. 4. 2003 in Primožič 2005: 56). Podatke je bilo kmalu mogoče videti tudi na Kazaa-ju. Podatke za to stran je posredoval častni konzul Slovenije za Avstralijo in Novo Zelandijo Dušan Lajovic (glej STA 24. 4. 2003), ki je v avgustu 2003 izdal tudi knjigo s prečiščeno različico seznamov. Podatke mu je junija 1991 izročil uslužbenec tajne službe, seveda pa Lajovic takrat še ni vedel za kakšne sezname sploh gre. Uspelo mu je razvozlati šifre in tako je po vstopu Slovenije v EU in Nato evidenco objavil na spletu (glej Sever 25. 8. 2003).

Kmalu po objavi podatkov na spletu je inšpektor za varstvo osebnih podatkov od domačih ponudnikov interneta ustno zahteval, naj v skladu z Zakonom o varstvu osebnih podatkov preprečijo dostop do te strani, vendar ustna prepoved zakonsko ni bila dovolj, zato so stran lahko internetni uporabniki še nekaj časa pregledovali (glej Primožič 2005: 57). Tudi če bi internetni ponudniki preprečili dostop do strani slovenskim uporabnikom,

bi ti do nje še vedno lahko dostopali preko javnih strežnikov (glej Primožič 2005: 57). Naslednji problem pa je bila Tajska, saj odklopa strežnika niso mogli doseči, ker Tajska še ni imela zakona o varstvu osebnih podatkov (glej Ceglar 11. 3. 2005) oz. je bil še v pripravi, torej objava osebnih podatkov po njihovi zakonodaji ne pomeni kršitve. Zaradi prepovedi glavnega inšpektorja za varovanje osebnih podatkov Jožeta Bogataja so stran le uspeli umakniti (glej STA 24. 4. 2003).

Zaradi te strani se je javnost začela spraševati, zakaj je država zbirala in ohranila takšne podatke, kako in zakaj so ti podatki sploh prišli v javnost, kdaj je bila neka oseba opredeljena kot tista, ki ogroža državo, ali so imeli sploh pravno podlago za takšno zbiranje podatkov in nasploh o avtentičnosti tega dokumenta. V javnosti pa so se pojavila tudi vprašanja o pravilnem ukrepanju takratnega inšpektorja za varstvo osebnih podatkov. Boštjan Makarovič (glej Primožič 2005: 58) meni, da inšpektor po zakonu nima pristojnosti nad internetnimi ponudniki, ki niso upravljavci ali obdelovalci osebnih podatkov, ampak zgolj posredniki pri njihovem prenosu. Druga stvar pa se je nanašala na dejstvo, da omejevanje dostopa do tujih strani ni razširjena v demokratičnih državah, saj bi s tem internet izgubil naravo globalnega okolja in bi si državljani v skrajnem primeru lahko ogledovali le tiste strani, katere bi država označila kot primerne. Takšen primer je Kitajska.

5. RAZISKOVALNI OKVIR

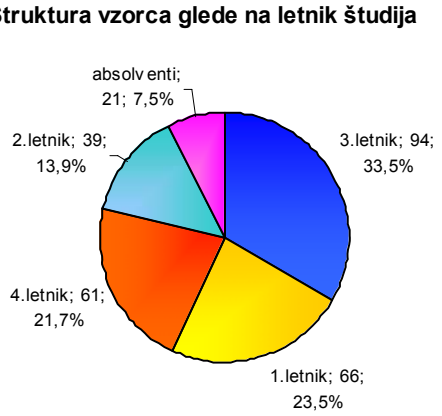
V nadaljevanju predstavljam lastno raziskavo iz področje nadzorovanja in novih tehnologij, kjer se osredotočam predvsem na posameznikovo *zavedanje sodobnih tehnologij nadzora*. Preučevanja tega pojava je pomembno, saj je uporaba informacijsko-komunikacijske tehnologije – ki je lahko hkrati tudi tehnologija nadzora – že tako zasidrana v naša življenja, da si brez nje sploh ne predstavljamo več vsakdanjika, s tem pa se povečujejo možnosti za nadzorovanja ljudi in s tem tudi vprašanja o zasebnosti. Z zavedanjem takšnih tehnologij, lahko nadzor posamezniki vsaj nekoliko ublažimo in posledično lahko tudi ukrepamo, če menimo, da gre za pretiran poseg v zasebnost, saj je zasebnost »temelj človeškega dostojanstva« (Kovačič 2003: 34). S tem imamo možnost soodločati, kakšni podatki se bodo o nas zbirali, in ukrepati v primeru zlorab, saj danes dejansko ne obstajamo, če nismo vodeni v kakšni evidenci. Pojav sem preučevala s

pomočjo ankete, ki je bila med slovenskimi študenti izbranih fakultet opravljena v prvi polovici leta 2004.

5.1 Opis in struktura vzorca

Na anketo[14] je skupno odgovarjalo 293 študentov, vendar pa je kakšen študent določeno vprašanje tudi (ne)namerno izpustil. Ti neodgovori v analizo podatkov niso vključeni. Med anketiranimi študenti so prevladovala *dekleta* (71,9% oz. 202 študentki) in študenti *3. letnikov* (33,5% oz. 94 študentov).

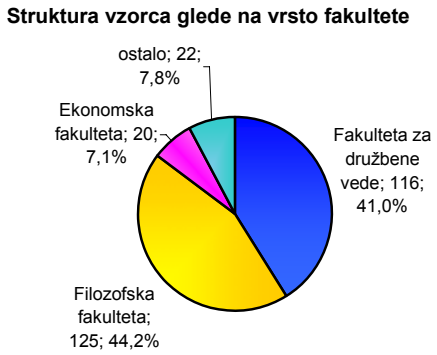
Slika 0-1: Struktura vzorca po spolu (april 2004, n=281)



Slika 0-2: Struktura vzorca glede na letnik študija (april 2004, n=281)

Anketiranje je potekalo na *Filozofski fakulteti* in *Fakulteti za družbene vede* v Ljubljani, vendar pa so v vzorec zbrani tudi študenti drugih fakultet, saj so se vprašalniki delili med drugim tudi v avli fakultete, kjer so se zadrževali še ostali študenti. Na vprašanja so tako večinoma odgovarjali študenti Filozofske fakultete (44,2% oz. 125 študentov) in Fakultete za družbene vede (41,0% oz. 116 študentov); 7,1% je bilo študentov Ekonomske fakultete; 7,8% študentov pa je študiralo tudi na drugih fakultetah, kjer so najbolj izstopale Biotehnična fakulteta, Fakulteta za upravo in Pedagoška fakulteta. Vse omenjene fakultete so v večini zastopala dekleta.

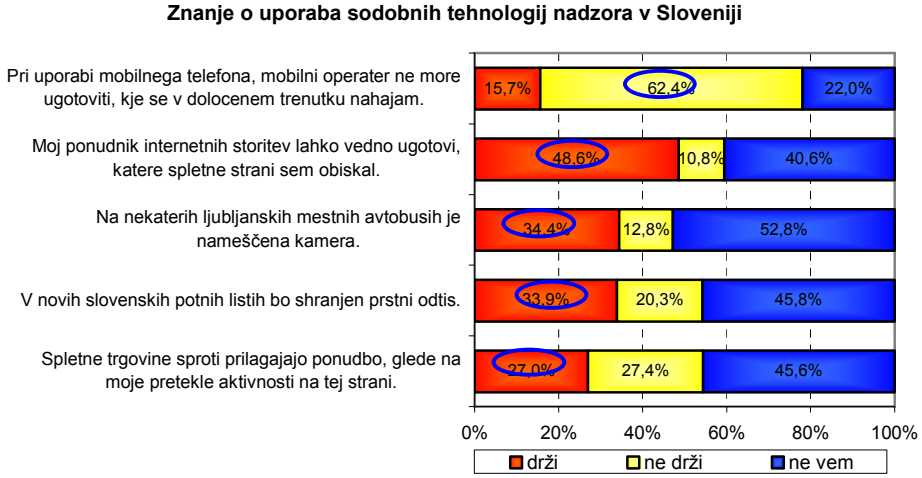
[14] Anketni vprašalnik je vseboval 6 sklopov zaprtega tipa in 1 sklopa odprtega tipa vprašanj o uporabi IKT v vsakdanjem življenju. Od tega sem za empirično analizo uporabila le 3 sklope, ki sem jih predstavila v prilogi (glej prilogo B). Vprašalnik je vseboval tudi 3 osnovne demografske spremenljivke (spol, letnik študija in ime fakultete).



Slika 0-3: Struktura vzorca glede na vrsto fakultete (april 2004, n=283)

5.2 Znanje o uporabi sodobnih tehnologij nadzora v Sloveniji

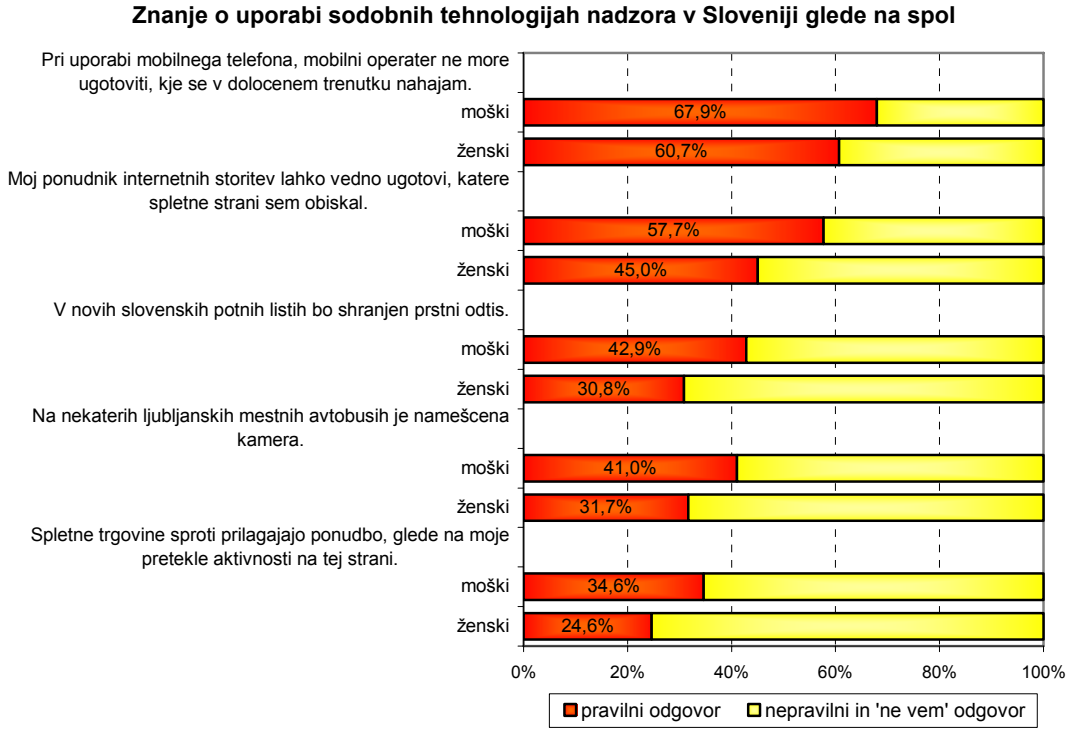
Študenti so se splošno gledano slabo odrezali v poznavanju uporabe sodobnih tehnologij nadzorovanja v Sloveniji, saj so prevladovali napačni ali »ne vem« odgovori (glej spodnjo sliko). Izstopali so edino v znanju uporabe mobilnega telefona in možnosti ugotavljanja lokacije s strani mobilnega operaterja, s čimer se je pravilno strinjalo kar 62% študentov. Slaba polovica (48,6%) je pravilno sklepala, da lahko ponudnik internetnih storitev ugotovi, katere spletne strani je študent obiskal[15]. Zelo slabo so bili seznanjeni z nameščeno kamero na nekaterih mestnih avtobusih v Ljubljani (34,4%), s prstnimi odtisi v novem potnem listu (33,9%) ter s prilagajanjem ponudbe uporabnikom na spletnih trgovinah (27,0%).



Slika 0-4: Preverjanje znanje o uporabi sodobnih tehnologij nadzora v Sloveniji – razvrščeno glede na pravilni odgovor, ki je obkrožen (april 2004, n=288)

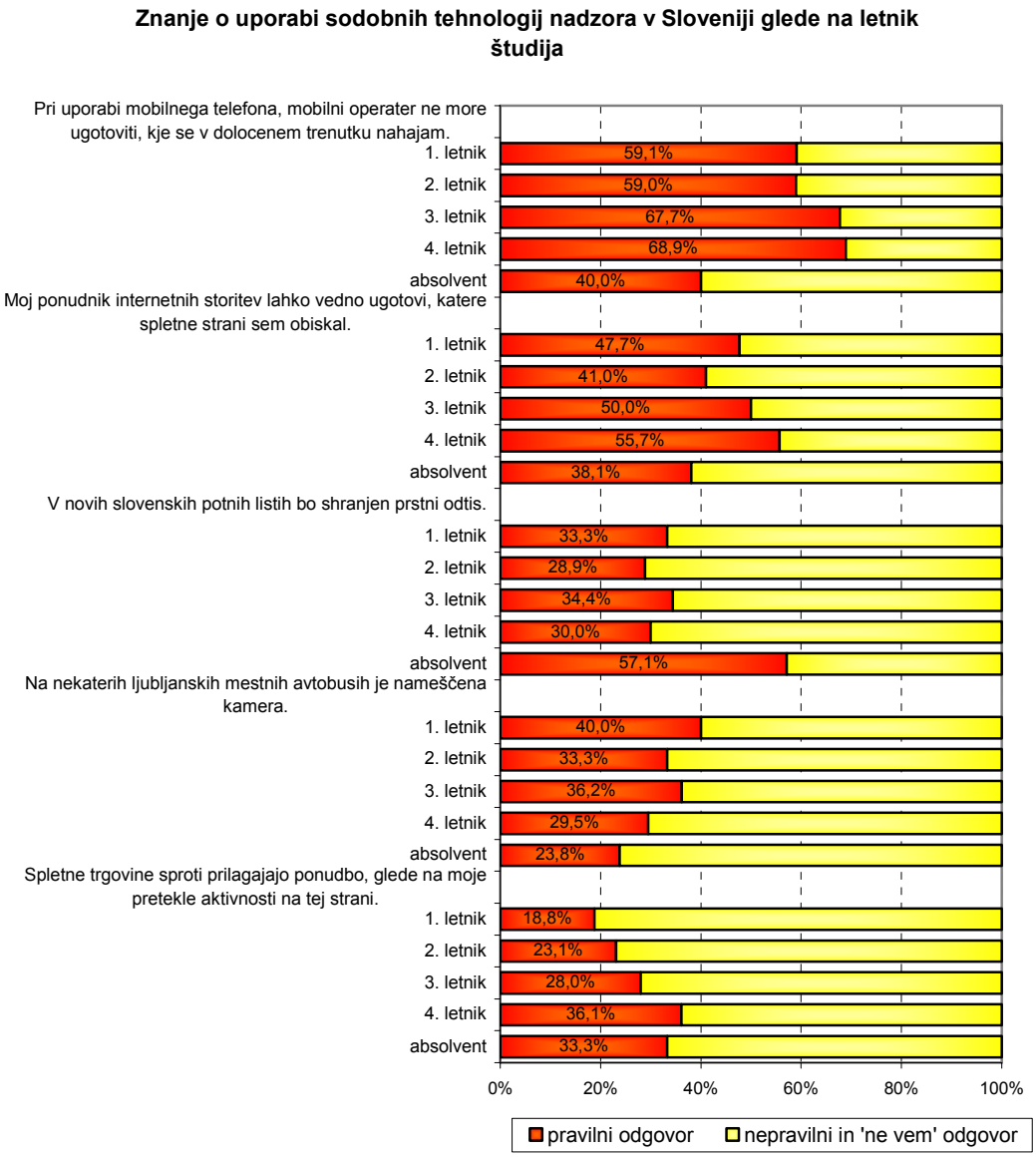
[15] Spletne trgovine lahko sproti prilagajajo ponudbo glede na pretekle aktivnosti uporabnika; ni pa nujno, da to počno vse.

Študenti moškega spola so bili bolj seznanjeni z uporabo sodobnih tehnologij nadzora v Sloveniji od študentk, saj je njihov delež pravilnih odgovorov pri vseh že zgoraj omenjenih trditvah višji (glej spodnjo sliko).



Slika 0-5: Preverjanje znanje o uporabi sodobnih tehnologij nadzora v Sloveniji glede na spol (april 2004, n=280)

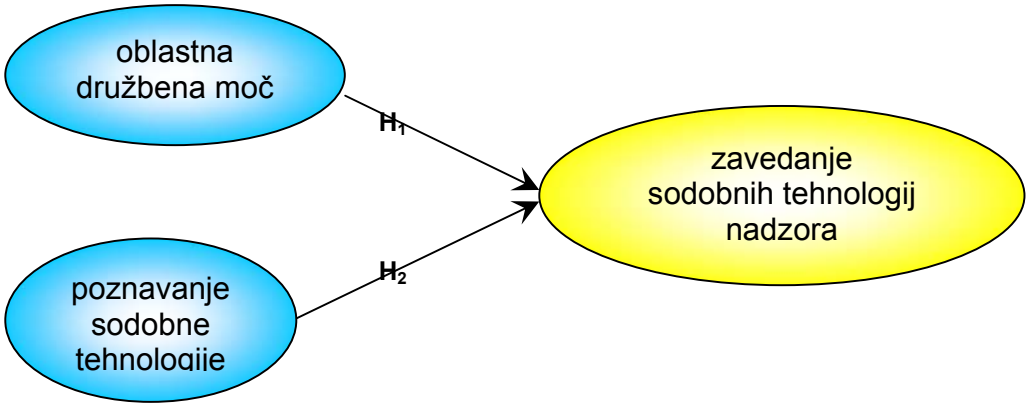
Deleži se o znanju uporabe sodobnih tehnologij nadzora med letniki študija gibljejo zelo raznoliko, saj **ni** mogoče opaziti določenega trenda kot npr. večja poučenost študentov višjih letnikov. Velikokrat so se ravno absolventi izkazali za najslabše poznavalce nadzorovalne tehnologije, predvsem pri ugotavljanju lokacije mobilnega operaterja (40%), prilagajanju ponudbe uporabnikom na spletnih trgovin (38,1%) in nameščeni kameri na nekaterih ljubljanskih avtobusih (23,8%). Najbolj pozitivno so presenetili pri védenju o shranjenih prstnih odtisih v novih potnih listih (57,1%).



Slika 0-6: Preverjanje znanje o uporabi sodobnih tehnologij nadzora v Sloveniji glede na letnik študija (april 2004, n=280)

5.3 Pojasnjevalni model

V nadaljevanju predstavljam pojasnjevalni model, kjer natančneje preverjam hipotezi, kako oblastna družbena moč posameznika in njegovo poznavanje sodobne tehnologije vplivata na posameznikovo zavedanje sodobnih tehnologij nadzora.



Slika 0-7: Pojasnjevalni model dveh neodvisnih (modra barva) in ene odvisne spremenljivke (rumena barva)

Najprej je dobro, da predstavim pomen oz. definicije omenjenih spremenljivk v pojasnjevalnem modelu:

Oblastna družbena moč: *Oblastna moč je moč, ki jo uporabljajo posamezniki, ko izdajajo zavestna namerna navodila in jim morajo slediti tisti, ki so jim namenjena – npr. nogometaš, ki sledi navodilom sodnika, da mora zapustiti igrišče* (glej Mann v Haralambos in Holborn 1999: 552-553).

Poznavanje sodobne tehnologije: *Poznavanje sodobne tehnologije je vednost o računalnikih in telekomunikacijah; širše povedano gre za elektronske naprave, s katerimi sprejemamo, shranjujemo, obdelujemo, ponujamo in prenašamo informacije* (glej Heeks 1998).

Zavedanje sodobnih tehnologij nadzora: *Zavedanje sodobnih tehnologij nadzora je védenje, da obstajajo sodobne tehnologije nadzorovanja, ki so »sestavljen sistem tehnične in programske opreme, ki vključuje sredstva za zaznavanje, merjenje, shranjevanje, obdelavo in izmenjavanje informacij in védenja o okolju. Ta sredstva so namenjena različnim ciljem od opazovanja prisotnosti ali odsotnosti oseb ali objektov do določanja njihove identitete ali statusa, z njihovim mišljenjem vred. Za ta namen naj bi se uporabljale kamere, prisluškovalni aparati, znanstveni instrumenti (za proučevanje telesnih tekočin in genetskega materiala na molekularni ravni). Skupna lastnost teh sredstev je, kot pravi Gandy, da so bolj izpopolnjena kot kadarkoli prej in presegajo nekdanje omejitve časa, prostora in razdalje pri zbiranju informacij o posamezniku«* (glej Gandy v Trampuž 2000: 138-139).

V realnem življenju na omenjeno odvisno spremenljivko o zavedanju sodobnih tehnologij nadzora vplivajo različni dejavniki in ne samo omenjeni spremenljivki v zgornjem modelu. V raziskavi pa sem se vendarle omejila le na ti dve neodvisni spremenljivki in tako preverjala naslednji hipotezi z argumenti:

Hipoteza 1: *Večja kot je oblastna družbena moč posameznika v družbi, bolj se ta zaveda sodobnih tehnologij nadzora.*

Čebulj pravi, da so se danes (z uvedbo IKT in računalniških zbirk podatkov) začeli ljudje bolj zavedati nevarnosti, kot v času ročno vodenih evidenc, saj je nova tehnologija ogroženost zasebnosti še potencirala (glej Kovačič 2000: 1022). S pomočjo sodobnih tehnologij nadzorovanja se tako pojavi vedno več možnosti spremljanja življenja, navad, okusov posameznikov (glej Trampuž 2000: 140), zaradi tega je zaupanje do nadzorstva vse manjše. Vendar pa so nekateri posamezniki močneje nadzorovani kot drugi, z nekaterimi nadzorstvo blagohotneje ravna kot z drugimi, spet drugi pa so zaradi družbene moči nedosegljivi, saj imajo več možnosti, da se izognejo hujšim posledicam (glej Pečar 1986: 549, 556). Posameznik z večjo družbeno močjo je tako bližje centru odločanja, ki ima dostop do informacij, dostop do celotnega nadzora; čeprav se zaradi tega, ker je bližje centru, bolj zaveda nadzora, ima večji pregled nad celotnim nadzorom, je sistem nadzora vseobsegajoč, kar pomeni, da so nadzorovani vsi člani družbe. (glej Pečar 1988: 49-50)

Hipoteza 2: *Bolj kot posameznik pozna sodobno tehnologijo, bolj se zaveda sodobnih tehnologij nadzora.*

Vsak posameznik si lahko na internetu postavi svojo predstavitveno stran, kjer navadno objavijo tudi svoje osebne podatke, vendar pa se pogosto ne zavedajo, da je z današnjo informacijsko-komunikacijsko tehnologijo na internetu mogoče vse javno objavljene podatke avtomatsko zbrati in povezati. »Čeprav je zbiranje na prvi pogled nenevarno, pa se bo slovenski uporabnik interneta te nevarnosti zavedel najkasneje takrat, ko bo njegove podatke zbrala marketinška agencija in mu v njegov elektronski predal pričela pošiljati 'junk mail'. « Prav tako se lahko z elektronskimi kolački ugotovi, ali je uporabnik na spletni strani že bil in kaj je na njej počel, lahko se tudi uporabljajo za sledenje uporabnikov iz enega spletnega strežnika na drugega ali razkrijejo identiteto uporabnika.

Uporabnik spleta običajno tudi ni seznanjen s t. i. datotekami aktivnosti (log files), kjer se vse aktivnosti posameznega uporabnika interneta (kdaj je prebral e-mail,....) avtomatsko zapisujejo na strežniku uporabnikovega ponudnika dostopa do interneta. Tudi elektronsko pošto lahko bere upravitelj sistema, ki sumi, da pošiljatelj načrtuje napad na sistem itd. (glej Kovačič 2000: 1024-1027). Tako je novo nadzorovanje avtomatsko, saj ga posameznik sproži sam, ko npr. z magnetno kartico vstopi v garažo ali pisarno, pošlje elektronsko pošto, pri telefoniranju, vstopi v vidno polje kamere itd. (glej Trampuž 2000: 139).

Poudarila bi, da se nisem omejila le na internet, pač pa nasploh na sodobno tehnologijo. Prav zaradi tega predpostavljam, da se tisti posamezniki, ki bolj poznajo, kako sodobna tehnologija (internet, mobilni telefon, videonadzorni sistem, biometrija...) deluje, tudi bolj zavedajo sodobnega nadzora, saj je »nova tehnologija ogroženost zasebnosti še potencirala in privedla do tega, da so se ljudje nevarnosti pričeli zavedati bolj kot v času ročno vodenih evidenc« (glej Čebulj v Kovačič 2000: 1022).

5.4 Rezultati analize

Vsako izmed navedenih spremenljivk sestavlja več indikatorjev oz. različnih vprašanj, ki skupaj tvorijo vsebinsko celoto. Spremenljivko **oblastna družbena moč** sestavlja sedem indikatorjev, ki so bili merjeni na ordinalni lestvici od 1 do 5, kjer višja vrednost pomeni večjo oblastno družbeno moč. Povprečne vrednosti v spodnji tabeli kažejo, da se anketiranci večinoma strinjajo s spodnjimi trditvami, saj so vrednosti indikatorjev povečini večje od 3; nikakor pa ta vrednost ne presega 4. V tem primeru imajo anketiranci le malo oblastne moči. Najbolj se strinjajo s trditvijo, da ko poskušajo njihovi prijatelji rešiti kakšen problem, jih ti prosijo za nasvet. Ker ta spremenljivka meri stališča študentov, sem izvedla tudi **faktorsko analizo** in sicer Metodo glavnih osi. S pomočjo *"Scree diagrama"* sem določila najprimernejše število najpomembnejših komponent, to sta dve komponenti[16], ki sem ju poimenovala **svetovanje** in **vodenje**.

[16] Razpršenost podatkov je bila v prvih dveh komponentah največja, zato lahko z njima pojasnimo kar največ podatkov, kajti pojasnjujeta nam približno 47,1% celotne variance.

Tabela 0-1: Povprečne vrednosti za oblastna družbena moč (april 2004)[17]

Anketno vprašanje	n	min	max	povprečje	std. odklon	faktor 1: **svetovanje**	faktor 2: **vodenje**
Večkrat se znajdem v situaciji, ko odločam kaj naj bi drugi ljudje počeli.	288	1	5	2.92	1.101	0.010	**0.439**
Kadar razpravljam z drugimi, jih le redko prepričam v svoj prav.[18] ®	287	1	5	3.64	0.794	-0.051	**0.457**
Ko poskušajo moji prijatelji rešiti kakšen problem, me prosijo za nasvet.	287	1	5	3.82	0.716	0.014	**0.544**
Prijatelji pri izbiri filma, ki se predvaja v kinu, navadno upoštevajo moje mnenje.	289	1	5	3.31	0.874	**0.786**	-0.190
~~Če grem jaz na zabavo, gredo tudi prijatelji.~~	288	1	5	3.26	0.937	0.328	0.228
Večkrat me prijatelji vprašajo za nasvet pri izbiri filmov, knjig ali glasbe.	287	1	5	3.34	0.898	**0.597**	0.077
~~Prijatelji so pripravljeni spremeniti svoje navade samo zato, da bi mi ugajali.~~	289	1	4	2.00	0.840	0.214	0.207

Spremenljivka **svetovanje** opisuje dajanje nasvetov prijateljem, zanesljivost tega faktorja pa se je izkazala za zmerno. [19] Novo spremenljivko sestavljata naslednja indikatorja:

- *Prijatelji pri izbiri filma, ki se predvaja v kinu, navadno upoštevajo moje mnenje.*
- *Večkrat me prijatelji vprašajo za nasvet pri izbiri filmov, knjig ali glasbe.*

Vodenje opisuje vodstvene »zmožnosti« študenta; malce izstopa le zadnji spodaj navedeni indikator. Vsekakor pa ta faktor predstavlja bolj »ostrejšo« moč kot svetovanje:

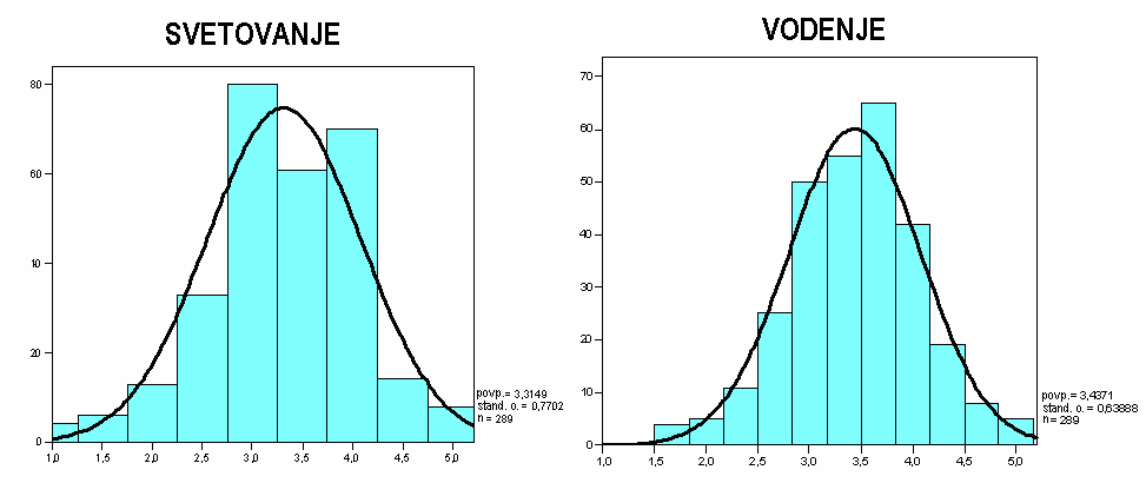
- *Večkrat se znajdem v situaciji, ko odločam kaj naj bi drugi ljudje počeli.*
- *Kadar razpravljam z drugimi, jih pogosto prepričam v svoj prav.*
- *Ko poskušajo moji prijatelji rešiti kakšen problem, me prosijo za nasvet.*

Zanesljivost merjenja je v tem primeru malenkost slabša.[19]

V nadaljevanju v teoretskem modelu ne bo več zastopana spremenljivka **oblastna družbena moč**, temveč novi dve: **svetovanje** in **vodenje**[20]. Spremenljivka vodenje ima malenkost višje povprečje (3,44) kot spremenljivka svetovanje (3,31), kar pomeni, da imajo študenti malenkost večje vodstvene ambicije kot svetovalne. Razlog za takšen

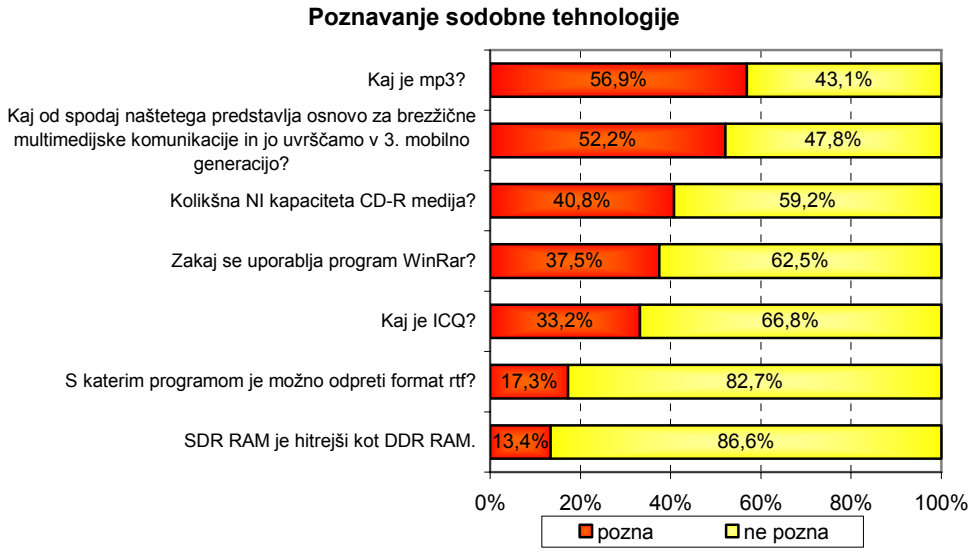
[17] Dva indikatorja sem iz analize izločila, saj nista imela dovolj velikih uteži – v tabeli prečrtana.
[18] Vsebinsko obrnjeno vprašanje.
[19] Zanesljivost nam pove, v kolikšni meri s ponovljenim merjenjem (v enakih pogojih in na istih enotah) dobimo enake rezultate. V primeru faktorja 'svetovanje' je *Cronbach-ov Alpha* 0,616, v primeru 'vodenja' pa 0,449.
[20] Za poznejšo bivariatno in regresijsko analizo sem indikatorje posameznega faktorja seštela in jih delila s številom spremenljivk in tako dobila novi spremenljivki svetovanje in vodenje, ki sta pa na lestvici od 1 (ne svetuje, ne vodi) do 5 (veliko svetuje, vodi).

rezultat je lahko tudi višjih delež anketiranih študentov med višjimi letniki, prav tako pa so anketo večinoma zastopali le študenti Fakultete za družbene vede in Filozofske fakultete, kar lahko dodatno vpliva na končne rezultate analize (glej poglavje o strukturi vzorca).



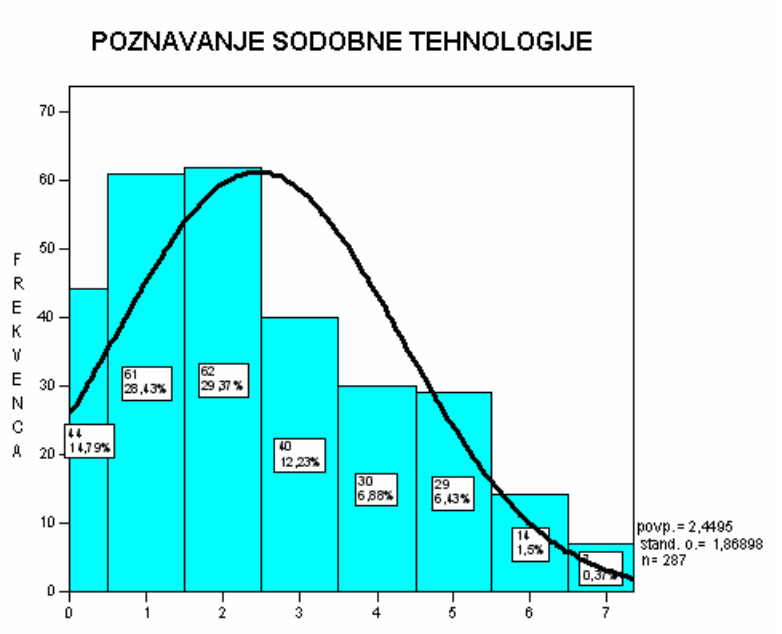
Slika 0-8: Seštevek indikatorjev v novo spremenljivko svetovanje in vodenje (april 2004, n=289)

Spremenljivko **poznavanje sodobne tehnologije** sestavlja prav tako sedem indikatorjev oz. vprašanj in ponazarja test, se pravi le eden od možnih odgovorov je pravilen. Anketirancev, ki na določeno vprašanje niso odgovorili, nisem upoštevala pri nadaljnji analizi. Iz spodnje slike lahko opazimo, da respondenti v večini sodobne tehnologije ne poznajo, poznajo le zakaj se uporablja MP3 (56,9%) in kaj uvrščamo v 3. mobilno generacijo (52,2%).



Slika 0-9: Poznavanje sodobne tehnologije – veljavni deleži (april 2004, n=287)

Ob seštetju vseh odgovorov te spremenljike[21] sem dobila dober pregled nad poznavanjem sodobne tehnologije med študenti. Kot sem že zgoraj omenila, študenti zelo slabo poznajo sodobno tehnologijo, saj je povprečje le 2,4 na lestvici do 7 (glej spodnjo sliko).



Slika 0-10: Seštevek rekodiranih indikatorjev (v 0 in 1) spremenljivke poznavanje sodobne tehnologije (april 2004, n=287)

[21] Nova spremenljivka poznavanje sodobne tehnologije je na lestvici od 0 (sploh ne pozna sodobno tehnologijo) do 7 (popolnoma pozna sodobno tehnologijo).

V poznavanju sodobne tehnologije glede na spol najbolj izstopajo fantje, kar se je izkazalo tudi za statistično značilno povezavo. V primeru poznavanja glede na fakulteto in letnik študija ni mogoče opaziti značilne povezave. Kljub temu pa glede na fakulteto ni večjih izstopanj, glede na letnik študija malenkost izstopajo le študenti 4. letnikov.

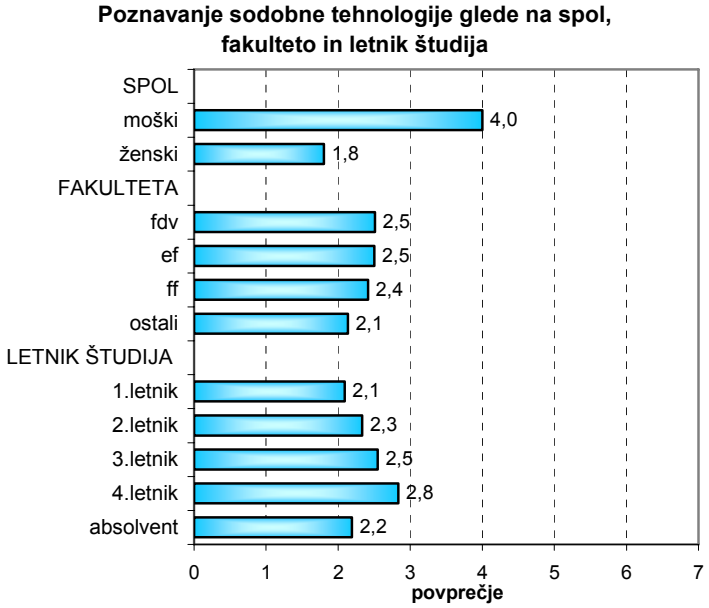
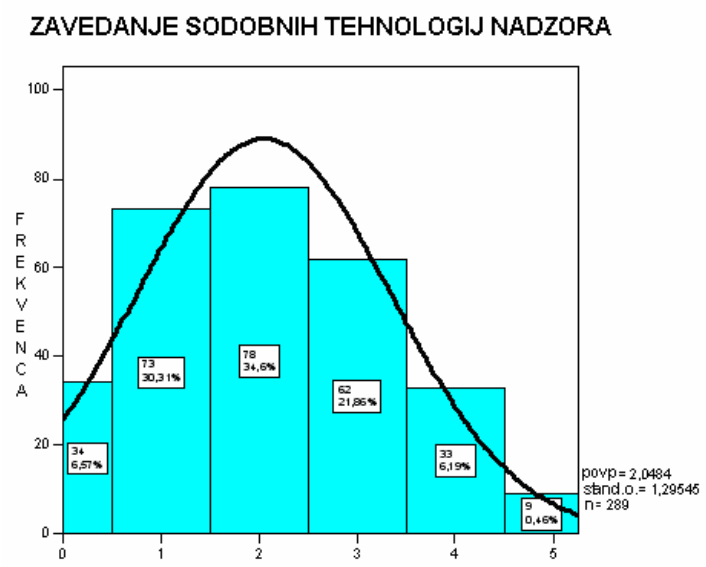


Figure 0-1: Poznavanje sodobne tehnologije glede na spol, fakulteto in letnik študija – povprečna ocena na lestvici od 0 „sploh ne pozna sodobno tehnologijo“ do 7 „popolnoma pozna sodobno tehnologijo“ (april 2004, n=281)

Odvisna spremenljivka **zavedanje sodobnih tehnologij nadzora** zopet predstavlja nekakšen test, se pravi le eden izmed možnih odgovorov je pravilen. Posamezne indikatorje oz. vprašanja sem predstavila že v poglavju *Znanje o uporabi sodobnih tehnologij nadzora v Sloveniji* (glej **Slika 0-4**), ki kot celoto skupaj predstavljajo spremenljivko zavedanje sodobnih tehnologij nadzora. V tem delu sem vse indikatorje med seboj seštela in tako ugotovila, da se anketiranci zelo slabo oz. ne zavedajo sodobnih tehnologij nadzora, saj je povprečje le 2,0 na lestvici od 0 do 5, kjer 0 pomeni »se sploh ne zaveda« in 5 »se popolnoma zaveda« sodobnih tehnologij nadzora.



Slika 0-11: Seštevek rekodiranih indikatorjev spremenljivke zavedanje sodobnih tehnologij nadzora (april 2004, n=289).[22]

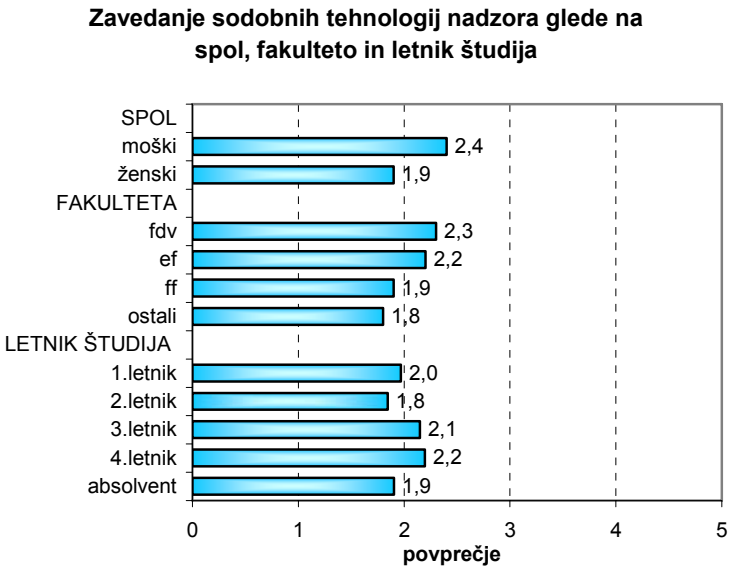


Figure 0-2: Zavedanje sodobnih tehnologij nadzora glede na spol, fakulteto in letnik študija – povprečna ocena na lestvici od 0 „se sploh ne zaveda sodobnih tehnologij nadzora“ do 5 „se popolnoma zaveda sodobnih tehnologij nadzora“ (april 2004, n=283)

[22] Indikatorje sem za kasnejšo analizo pretvorila pravilni odgovor v 1 (anketiranec se zaveda sodobnih tehnologij nadzora) ter nepravilni odgovor in ne vem v 0 (anketiranec se ne zaveda sodobnih tehnologij nadzora). Tudi tukaj nisem upoštevala anketirancev, ki na kakšno vprašanje niso odgovorili. Nova spremenljivka je na lestvici od 0 (se sploh ne zaveda sodobnih tehnologij) do 5 (se popolnoma zaveda sodobnih tehnologij nadzora).

Statistično značilna povezava se je izkazala le za spol in odvisno spremenljivko. Torej fantje se v primerjavi z dekleti bolj zavedajo sodobnih tehnologij nadzora. V primeru fakultete in letnika študija pa statistične značilnosti ni. Kljub temu pa se malenkost bolj zavedajo študenti Fakultete za družbene vede in študenti 4. letnikov.

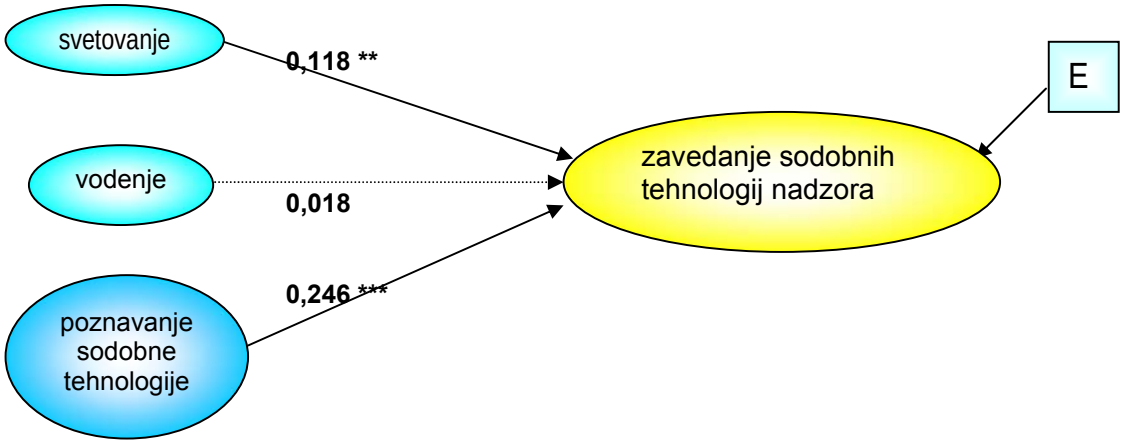
Na podlagi bivariatne analize oz. analize dveh spremenljivk (glej prilogo A) je mogoče zaznati povezanost odvisne spremenljivke zavedanje sodobnih tehnologij nadzora in neodvisne poznavanje sodobne tehnologije v smeri, da večja kot je vrednost neodvisne spremenljivke, večja je vrednost odvisne spremenljivke. Torej, bolj kot posamezniki poznajo sodobno tehnologijo, bolj se zavedajo sodobnih tehnologij nadzora, kar pa sem predpostavila tudi v teoretskem modelu. V primeru (novih) neodvisnih spremenljivk – svetovanje, vodenje – pa je stopnja značilnosti le v primeru svetovanja dovolj majhna, tako da sta odvisna spremenljivka in svetovanje pozitivno povezani pri stopnji značilnosti 0,05. To pomeni, da večjo »svetovalno« moč imajo posamezniki, bolj se zavedajo sodobnih tehnologij nadzora. Spremenljivka vodenje ni povezana z odvisno spremenljivko, saj je stopnja značilnosti prevelika. Med sabo sta povezani tudi obe novi spremenljivki moči, prav tako pa tudi neodvisni spremenljivki vodenje in poznavanje sodobne tehnologije.
Izkazalo se je tudi, da sta s spremenljivko spol povezani spremenljivki zavedanje sodobnih tehnologij nadzora in poznavanje sodobne tehnologije.[23] Torej, dekleta se v primerjavi s fanti veliko slabše spoznajo na sodobno tehnologijo, prav tako pa se sodobnih nadzorovalnih tehnologij manj zavedajo.

5.4.1 Preverjanje modela in hipotez

Teoretski model sem preverjala s pomočjo regresijske analize, s katero lahko analiziramo odnos med odvisno in vsako neodvisno spremenljivko[24]. Glede na vrednost testne statistike F se model dobro prilega podatkom (glej prilogo), odstotek pojasnjene variance pa je le 6,9%, kar pomeni delež variiranja odvisne spremenljivke, ki je pojasnjen z

[23] Povezanost sem preverjala z ANOVA testom. V primeru zavedanja sodobnih tehnologij nadzora in spola je bila stopnja značilnosti 0,004, v primeru poznavanja sodobne tehnologije in spola pa 0,000.
[24] Pogoj za izvedbo regresijske analize pa je linearen odnos med odvisno in neodvisnima spremenljivkama, ki se je v tem primeru izkazal za spremenljivki svetovanje in poznavanje sodobne tehnologije.

neodvisnimi spremenljivkami, torej le 6,9% sem pojasnila z neodvisnimi spremenljivkami, ostalo pa predstavlja nepojasnjen del kot so nevključene spremenljivke, napake, itd. Tako lahko preverim hipotezi, ki sem ju postavila na podlagi teorije.[25]



Slika 0-12: Regresijski model oz. grafični prikaz multiple regresije (metoda Enter)[26]

Regresijska analiza je pokazala vpliv istih neodvisnih spremenljivk na odvisno kot bivariatna analiza zgoraj (gledano le za teoretski model). Na zavedanje sodobnih tehnologij nadzora tako pozitivno vplivata poznavanje sodobne tehnologije in svetovanje. Spremenljivka vodenje pa se ni izkazala za statistično značilno povezana z odvisno spremenljivko. V celoti lahko potrdim hipotezo: *Bolj kot posameznik pozna sodobno tehnologijo, bolj se zaveda sodobnih tehnologij nadzora.* V primeru druge hipoteze: *Večja kot je oblastna družbena moč posameznika v družbi, bolj se ta zaveda sodobnih tehnologij nadzora*, pa se stvari malo zapletejo. V tej hipotezi je omenjena neodvisna spremenljivka oblastna družbena moč, ki pa se je tekom raziskave razdelila na dve: svetovanje (milejšo moč) in vodenje (ostrejšo moč). Hipotezo pa lahko potrdim le v primeru milejše moči oz. svetovanja in sicer v smeri, da večja kot je vrednost neodvisne spremenljivke, večja je vrednost odvisne spremenljivke. Torej, večja kot je »svetovalna« moč posameznika v družbi, bolj se ta zaveda sodobnih tehnologij nadzora. V primeru

[25] Regresijsko analizo sem naredila s pomočjo metode »enter«, ki hkrati oceni model z vsemi neodvisnimi spremenljivkami, torej v regresijski model vključi vse izbrane spremenljivke.

[26] Vrednosti, zapisane ob puščicah na regresijskem modelu, predstavljajo parcialne koeficiente korelacije. Ti koeficienti kažejo vpliv neodvisne spremenljivke na odvisno spremenljivko brez vpliva ostalih spremenljivk. V modelu je prikazan tudi člen napake oziroma motnje – označen je z E, na katerega vlivajo »nezajeti vplivi«, torej predvsem vse ostale spremenljivke, ki jih v model nisem vključila.

»vodstvene« moči regresijska analiza ni pokazala statistično značilne povezave z odvisno spremenljivko.

5.5 Interpretacija raziskave

Anketo so leta 2004 reševali izključno študenti in še to predvsem študenti Fakultete za družbene vede in Filozofske fakultete. Tudi sama anketa je bila prilagojena njim. Ker se je vprašalnik nanašal na informacijsko tehnologijo, lahko sklepamo, da bi študenti le-to malce bolje poznali kot bi jo poznal povprečen Slovenec. Vendar pa je analiza podatkov pokazala, da študentje še vedno ne poznajo preveč dobro sodobne tehnologije. Pri tem statistično značilno izstopajo predstavnice ženskega spola. Analiza je tudi pokazala, da na zavedanje sodobnih tehnologij nadzora pozitivno vplivata poznavanje sodobne tehnologije in »svetovalna« družbena moč. Študente namreč prijatelji veliko sprašujejo za mnenja in nasvete, torej imajo nekakšno bolj neformalno moč. Ti morajo imeti določene informacije, saj dajejo nasvete drugim, zaradi tega pa so bliže centru moči in se posledično tudi bolj zavedajo sodobnih tehnologij nadzora kot tisti, ki teh informacij nimajo. Razlog za vpliv le spremenljivke svetovanje in ne vodenje na odvisno spremenljivko je lahko anketirana populacija. Namreč, posamezniki z »ostrejšo« oz. »vodilno« močjo zasedajo v družbi tudi vodilne položaje, da sploh lahko vodijo. Anketiranje pa je potekalo le med študenti in le malo študentov zaseda vodilne in vplivne položaje. Prav tako pa je bila zanesljivost te spremenljivke tudi malo nižja.

Na zavedanje sodobnih tehnologij pa vpliva tudi poznavanje sodobne tehnologije. Čeprav študenti le-to slabo poznajo, predvsem dekleta, nam je tehnologija vedno bližja in jo tudi na široko uporabljamo, ne da bi sploh vedeli kako je sestavljena in kako deluje, saj so sodobne naprave že tako preproste in enostavne za uporabo. Že skoraj vsak študent ima svoj računalnik, dostop do interneta in mobilni telefon, saj bi brez teh pripomočkov težje študiral in si organiziral delovni dan. Hkrati pa le malo kdo ve, kako so te naprave dejansko sestavljene, kako delujejo in kaj vse še zmorejo. O teh stvareh se redko sprašujemo. Analiza je pokazala, da se na sodobno tehnologijo najbolj spoznajo fantje, za katere sklepam, da jih takšne stvari tudi bolj zanimajo kot dekleta. Ravno zaradi rutinskega odnosa do sodobne tehnologije, je potrebno za večje poznavanje vložiti nekaj zanimanja in radovednosti. S poznavanjem sodobne tehnologije si posamezniki tako

širijo obzorja možne uporabe tehnologije. S tem so bolj verjetno poučeni tudi o nadzorovalnih tehnologijah, saj se med sabo velikokrat prepletata, npr. ob vsakdanji uporabi računalnika je potrebno vedeti, kako ga in se zaščititi pred možnimi zlorabami, kot so nezaželena sporočila, zloraba kreditnih kartic, bančnih računov itd.

Rezultati ankete bi bili verjetno boljši ob večjem vzorcu in krajši anketi, kar bi pripomoglo k resnejšemu sodelovanju anketirancev, sploh ker so študenti anketo reševali sami. Prav tako pa je vzorec predstavljalo kar 71,9% žensk, kar je zopet lahko vplivalo na končne rezultate, saj se je izkazalo, da slabo poznajo sodobno tehnologijo in se manj zavedajo nadzorovalnih tehnologij kot fantje. Prav tako bi na končne rezultate lahko vplivalo tudi anketiranje na večih fakultetah, saj bi se verjetno s Fakulteto za računalništvo povprečje poznavanja in zavedanja dvignilo. V vsakem primeru pa tudi na podlagi potrjene hipoteze ne morem posploševati na celotno študentsko populacijo Slovenije, kaj šele na vse Slovence, saj vzorec ni reprezentativen. Namreč, anketirali smo samo študente na dveh fakultetah in še te samo v Ljubljani. Anketo bi bilo zanimivo raziskati tudi glede na splošno populacijo Slovenije, kjer bi bili vključeni tudi posamezniki z različnim družbenim položajem in močjo. Zanimivo bi bilo izvesti tudi spletno anketo, saj bi bilo poznavanje in zavedanje sodobnih nadzorovalnih tehnologij najverjetneje višje. Vsekakor pa niso to edine neodvisne spremenljivke v pojasnjevalnem modelu, ki bi lahko vplivale na zavedanje sodobnih tehnologij nadzora.

6. RAZPRAVA

Skozi celotno diplomsko nalogo je mogoče opaziti razmerje med zasebnostjo proti varnosti, vsaj v primeru državnega nadzora, ki se je še posebej izrazit po 11. septembru. Tako se velikokrat pri uporabi novih tehnologij nadzora poudarja varnost države in njenih državljanov. Državni aparati Velikega Brata predstavljajo na nežen, sofisticiran, neopazen, nevsiljiv način, torej Veliki Brat čuva tudi vas, ampak s tem posega tudi v vašo zasebnost (glej Pirc Musar 3. 7. 2006). Država želi z nadzorovalnimi tehnologijami le prijeti nepridiprave in tako omogočiti lepše in varnejše življenje za vse ostale, poštene ljudi, ki se nadzora tako ne rabimo bati, saj je namenjen le nepridipravom, kriminalcem. Torej, če bi se »država odločila za snemanje na javnih mestih, seveda v želji večje varnosti državljanov, bomo pač morali to vzeti v zakup. Edini način, kako se izogniti

takšnemu snemanju je, da pač ne gremo tja« (Pirc Musar 3. 7. 2006). V takšnih trenutkih se zdi, da kot državljani sploh nimamo možnosti izbire, saj se takšnemu nadzoru v veliko primerih niti ne moremo izognit. Čeprav je v Sloveniji zasebnost in varovanje osebnih podatkov posameznikov precej dobro zakonsko urejeno, še posebej v primerjavi z ZDA, pa lahko tudi pri nas opazimo povečano uporabo tehnologije za nadzorovanje državljanov, potrošnikov, delavcev in drugih običajnih ljudi. Torej nismo nadzorovani le kot državljani, ampak tudi vedno bolj kot potrošniki, katerih nadzor se vrši na še bolj prijazen način kot državni. Tako Lyon meni, da se vse premalo zavedamo trgovskih kartic, ki nudijo različne ugodnosti, s tem pa trgovskim družbam omogočimo, da poglobljeno analizirajo naše potrošniške in življenjske navade. V bistvu se mu podrejamo celo prostovoljno in nam celo ugaja, da nam olajša nakup, npr. z izbiro artikla v spletni trgovini ali pa ponudi kakšne druge ugodnosti. Ravno komercialni nadzor pa se bo po besedah Lyona tudi najbolj razširil v prihodnosti.

Profesor dr. Gorazd Trpin iz Pravne fakultete meni, da se »ljudje še ne zavedajo možnosti novih tehnologij« (Krašič 27. 11. 2003), kar je pokazala tudi omenjena raziskava na študentih izbranih ljubljanskih fakultet. Sicer se je izkazalo, da poznavanje sodobne tehnologije pozitivno vpliva na zavedanje sodobnih tehnologij nadzora, prav tako tudi oblastna družbena (svetovalna) moč. Torej posameznik, ki npr. pozna, kako deluje računalnik, internet, kakšne vse pasti ga lahko pri tem čakajo, se zna pred tem ustrezno zaščiti in se zaradi tega tudi bolj zaveda sodobnih nadzorovalnih tehnologij kot pa nepoznavalci. Prav tako se bolj zavedajo tudi osebe, ki imajo večjo oblastno družbeno moč, so bliže centru moči, vendar ta moč je bolj svetovalne narave, milejša, v obliki informacij in dajanj nasvetov. In kdaj se bodo posamezniki začeli zavedati nadzora? Trpin pravi, da ko bodo nove tehnologije že uvedene, se bomo šele zavedali njihovih nevarnosti, sedaj ob uvajanju se bolj poudarjajo prednosti. »Šele ko se ljudje zavedo nevarnosti neke tehnologije, začno razmišljati, kako bi se pred njenimi slabostmi zavarovali« (Trpin v Krašič 27. 11. 2003). Dodaja tudi, da se v sodobnem svetu ravno na račun varnosti zmanjšuje zasebnost, »varnost se lahko sprevrže v lastno nasprotje, mehanizmi varnosti postanejo mehanizmi nadzora in obvladovanja« (Krašič 27. 11. 2003). Informacijska pooblaščenka pa dodaja, da se posamezniki že zavedamo nadzora, vendar še vedno premalo, saj še vedno vse povprek dajemo svoje osebne podatke, EMŠO

in davčno številko ter izpolnimo kar vse podatke, ki jih nek obrazec zahteva (glej Pirc Musar 27. 3. 2006). Tudi Kovačič (2003: 28) meni, da »se posamezniki ne zavedajo obsega nadzorovanja v tolikšni meri, kot bi se ga lahko sicer«. Posamezniki namreč sami s svojimi dejanji sprožajo sisteme za nadzorovanje, npr. z nakupom s kreditno kartico, vstopom v vidno polje nadzorne kamere, »hkrati pa ti sistemi podatke in informacije tudi iščejo in preverjajo sami« (Lyon v Kovačič 2003: 28). Pričakujemo torej lahko vedno večjo uporabo tehnologij nadzora in s tem neko drugo obliko zasebnosti. Namreč, že danes se je skoraj nemogoče gibati, brez da bi za sabo puščali sledi, bili neopaženi, vsa naša dejanja pa se shranjujejo v baze podatkov. To pomeni, da nas oko kamere že skoraj na vsakem koraku snema, mobilni telefon, bančne kartice, internet in druge tehnologije (nadzora) uporabljamo večkrat dnevno; brez njih si niti ne moremo več predstavljati življenja. Kako se torej lahko zavarujemo, obdržimo vsaj nekaj informacij zase in s tem zavarujemo svojo zasebnost? Prvi korak je zavedanje, da takšne tehnologije sploh obstajajo in kako delujejo, na kakšen način, kdo izvaja takšen nadzor itd. Drugi korak pa je zavedanje svojih pravic, npr. kako je pravno urejeno zbiranje osebnih podatkov, kdo jih lahko zbira, kakšne podatke in v kakšne namene, kako preprečiti zlorabo in kam se obrniti v primeru zlorabe. Seveda pa velikokrat potrošniki nadzora v zasebnem sektorju sploh ne smatrajo kot nadzor, saj jim nudi dosti ugodnosti in se mu zaradi tega podrejajo celo prostovoljno. Kljub temu, da se velikokrat nadzoru ne moremo izogniti, je Evropski uniji varstvo osebnih podatkov višja prioriteta kot ZDA (glej Kovačič na RA 1 13. 7. 2006), prav tako pa imamo tudi Informacijsko pooblaščenko, ki zelo aktivno skrbi za morebitne zlorabe Zakona o varstvu osebnih podatkov v Sloveniji.

7. ZAKLJUČEK

Večina teoretikov se danes strinja, da živimo v družbi nadzora, nadzorovanje pa je usmerjeno na celotno populacijo in ne le na posameznika. V diplomski nalogi sem skušala predstaviti problematiko uporabe sodobnih tehnologij nadzora v Sloveniji. Na začetku sem se osredotočila bolj na teoretski pregled, kjer sem predstavila predvsem negativne plati nadzora: problematiko zbiranja in povezovanja osebnih podatkov v baze, profiliranja ljudi, ki je še posebej izrazito po 11. septembru, in vse do pravic do zasebnosti, kjer se zdi, da jih vse bolj izgubljamo. Ločila sem tudi več vrst delitev

nadzora, kjer sta skozi celotno nalogo najbolj v ospredju in se tudi ves čas prepletata ravno državni in komercialni nadzor. Opisala sem tudi najpomembnejše vrste in značilnosti sodobnih tehnologij nadzora, ki pa nikakor niso edine. Empirični del naloge sem predstavila z zakonsko ureditvijo uporabe nadzora in nadzorovalnih tehnologij v Sloveniji, kjer sem se osredotočila predvsem na najnovejši Zakon o varstvu osebnih podatkov, ki ureja tako osebne podatke kot tudi videonadzor in biometrijo. Konkretno uporabo in zlorabo nadzorovalnih tehnologij pri nas pa sem predstavila skozi oko medijev. Opozoriti moram, da je predstavljenih le nekaj primerov, zgolj za ilustracijo, da se tudi v Sloveniji vrši nadzor nad ljudmi na različne načine. Na koncu pa sem predstavila tudi lastno raziskavo med študenti izbranih ljubljanskih fakultet, kjer se je izkazalo, da se študenti sodobnih tehnologij nadzora ne zavedajo. Zavedanje je večje pri tistih, ki bolj poznajo sodobno tehnologijo in tistih, ki imajo večjo svetovalno družbeno moč, v obliki informacij, ki pa danes predstavljajo moč. Vendar pa se je danes nadzoru, ki temelji na sodobni tehnologiji, veliko težje izogniti kot včasih, sploh s pojavom in hkratno uporabo vedno novejših tehnik nadzorovanja. Velikokrat tudi nimamo izbire, saj se videonadzornim kameram po mestu zelo težko izognemo, če želimo potovati potrebujemo biometrični potni list in smo podvrženi nadzoru na letališčih, ob nakupovanju in brskanju po spletu se ne moremo izogniti elektronskim sledem itd. Tudi v prihodnosti ne kaže, da se bo nadzorovanje zmanjšalo, niti komercialni kot meni Lyon (2006), niti državni nadzor, saj nikjer po svetu ne pričakujejo manj kriminala, pričakujejo pa »več terorizma, nasilja in raznih pojavov s političnimi, rasnimi, verskimi in narodnostnimi sestavinami« (glej Pečar, 1988: 390). Vendar pa nikoli ne bomo dosegli totalitarne družbe, kakršno je opisal Orwell v 1984 (Gary Rowden v Krašič 1. 3. 2004). »Popolnoma prosojno družbo« v prihodnosti vidi ameriški znanstvenofantastični pisec David Brin (glej Pahor 13. 10. 2003), v kateri bi bili pod videonadzorom vsi, hkrati pa imeli tudi vsi dostop do teh posnetkov in ne samo policisti in varnostniki. S tem bi zagotavljali popolno informacijsko odprtost (glej Pahor 13. 10.2003). Organi pregona bi se morali po njegovem mnenju ukvarjati s kršilci za transparentnosti, torej tistimi, ki bi se še vnaprej zavzemali za zasebnost (glej Rizman 8. 5. 2003). Tudi Rowden se strinja, da bo uporaba videonadzora še naprej rasla (Krašič 1. 3. 2004). Nekateri pa vidijo prihodnost v vedno večji uporabi biotehnologije. Eden izmed teh je tudi Francis

Fukuyama (2002), ki pa ne nasprotuje uporabi takšne tehnologije, temveč le opozarja, da je potrebno uporabo omejiti za določene namene (zdravljenje bolnih itd.). Kot kaže se v prihodnosti ne bomo mogli večno upirati vedno večji uporabi sodobnih tehnologij nadzora. V tem primeru je pomembno le ozaveščanje ljudi, da se ti bolj zavedajo takšnega nadzora in ukrepajo v primeru zlorab. Še vedno pa se zdi, da posledic uporabe tehnologij nadzora še nismo začutili, zato se še vedno obnašamo, kot da tega nadzora sploh ni, in da nam je prav malo mar za našo zasebnost. Vendar pa moramo vedeti, da se je potrebno za svobodo stalno boriti (glej Marx 2002: 25).

8. LITERATURA in VIRI

- Ahler, Cristian; Nash, Victoria in Marsden, Chris (2005): Implications of the Mobile Internet for the Protection of Minors. Dostopno na http://www.forumti.it/fti/downloads/Ahlert_Nash_Marsden.pdf (16.3.2006).
- B. Š. (2005): Pirančane bodo nadzirale kamere. Delo, 26. 1. 2005. Dostopno na http://www.delo.si/index.php?sv_path=43,50&src=mm (17. 1. 2006).
- Baebler, Jasna (2005): Strogo nadzorovani uslužbenci. Delo, 23. 5. 2005. Dostopno na http://www.delo.si/index.php?sv_path=43,50&src=mm (17. 1. 2006).
- Čakš, Aleš (2004): Nad nasiljem brez nasilja. Delo, 6. 12. 2004. Dostopno na http://www.delo.si/index.php?sv_path=43,50&src=mm (17. 1. 2006).
- Ceglar, Miha (2005): "Siol očitno krši zakon". Delo, 11. 3. 2005. Dostopno na http://www.delo.si/index.php?sv_path=43,50&src=mm (17. 1. 2006).
- Cvetek, Olga (2004): Internet, anonimni pljuvalnik. Več, 28. 5. 2004. Dostopno na http://www.delo.si/index.php?sv_path=43,50&src=mm (17. 1. 2006).
- Cvetek, Olga (2004): Vam prisluškujejo in zakaj ne.Več, 16. 4. 2004. Dostopno na http://www.delo.si/index.php?sv_path=43,50&src=mm (17. 1. 2006).
- Delo Stik (2001): Tehnično varovanje: za noči brez skrbi. Delo, 28. 9. 2001. Dostopno na http://www.delo.si/index.php?sv_path=43,50&src=mm (17. 1. 2006).
- Deluze, Gilles (1990/2002): Družba nadzora. Filozofski vestnik XXIII(3), 167-177.
- Fitzpatrick, Tony (2002): Critical theory, information society and surveillance tehnologies. Information, Communication & Society 5: 3, 357-378.
- Foucault, Michael (1976/2003): Predavanje 17. marca 1976. Filozofski vestnik, XXIV(3), 151-169.
- Fukuyama, Francis (2002): Konec človeštva: Posledice revolucije v biotehnologiji. Ljubljana: Učila.
- Haralambos, Michael in Holborn, Holborn (1999): Sociologija: Teme in pogledi. Ljubljana: DZS.

- Heeks, Richard (1998): Definicija sodobne tehnologije. University of Manchester. Dostopno na http://www.commerce.uq.edu.au/isworld/ teaching/msg.02-12-1998.html (27. 2. 2004).
- I. N. in Kurier (2002): Kamera vas bo videla, vašim očem pa bo skrita. Delo, 24. 4. 2002. Dostopno na http://www.delo.si/index.php?sv_path=43,50&src=mm (17. 1. 2006).
- Jain, Anil; Bolle, Ruud in Pankanti, Sharath (2002): Biometrics: Personal Identification in Networked Society. New York, Boston, Dordrecht, London, Moscow: Kluwer Academic Publishers.
- Jakopec, Marko in Kajzer, Rok (2004): Nevarno omejevanje pravice javnosti. Delo, 26. 1. 2004. Dostopno na http://www.delo.si/index.php?sv_path=43,50&src=mm (17. 1. 2006).
- Jerman, Vladimir (2005): Na skrivaj nam gledajo vrtičke. Več, 18. 3. 2005. Dostopno na http://www.delo.si/index.php?sv_path=43,50&src=mm (17. 1. 2006).
- Kocmur, Helena (2005): Z alkotesti nad uradnike, z detektivi nad bolnike in doječe matere. Nedelo, 11. 9. 2005. Dostopno na http://www.delo.si/index.php?sv_path=43,50&src=mm (17. 1. 2006).
- Kovačič, Matej (2000): Zasebnost v informacijski družbi. Diplomska naloga, Ljubljana.
- Kovačič, Matej (2003): Zasebnost na internetu. Ljubljana: Mirovni inštitut.
- Kovačič, Matej (2005): Zasebnost in nadzor na internetu. Doktorska disertacija, Ljubljana.
- Kovačič, Matej (2005a): Nadzor zaposlenih – ZDA ali Evropa? Konferenca Infosek, Inštitut IZIV.
- Krašič, Marko A. (2004): Veliki brat na mestnih avtobusih. Delo, 20. 2. 2004. Dostopno na http://www.delo.si/index.php?sv_path=43,50&src=mm (17. 1. 2006).
- Krašič, Marko A. (2003): "Varnost se lahko sprevrže v lastno nasprotje". Delo, 27. 11. 2003. Dostopno na http://www.delo.si/index.php?sv_path=43,50&src=mm (17. 1. 2006).

- Krašič, Marko A. (2004): "Veliki brat ne opazuje – varuje". Delo, 1. 3. 2004. Dostopno na http://www.delo.si/index.php?sv_path=43,50&src=mm (17. 1. 2006).
- L.V. (2002): Veliki brat vas gleda. Delo, 12. 3. 2002. Dostopno na http://www.delo.si/index.php?sv_path=43,50&src=mm (17. 1. 2006).
- Land, Ray in Bayne, Siân (2002): Screen or Monitor? Surveillance and disciplinary power in online learning environments. Dostopno na http://www.malts.ed.ac.uk/staff/sian/surveillancepaper.htm (5. 7. 2006).
- Lotrič, Tatjana (2005): Veliki starš te gleda. Delo, 22. 9. 2005. Dostopno na http://www.delo.si/index.php?sv_path=43,50&src=mm (17. 1. 2006).
- Lyon, David (2001): Surveillance after September 11. Dostopno na http://www.fine.lett.hiroshima-u.ac.jp/lyon/lyon2.html (17. 6. 2006).
- Lyon, David (2003): Surveillance Technology and Surveillance. Modernity and Technology, 161-183. Dostopno na http://www.greylodge.org/occultreview/glor_012/Surveillance.pdf#search=%22%22Surveillance%20Technology%20and%20Surveillance%22%22 (15. 5. 2006).
- Lyon, David (2006): Surveillance, Power and Everyday Life. Poglavje iz Oxford Handbook of Information and Communication. Dostopno na http://www.queensu.ca/sociology/Surveillance/files/oxford_handbook.pdf (5. 5. 2006).
- M. A. K. (2004): Stoletnica vodovoda – Videonadzor na avtobusih ni pravno sporen. Delo, 25. 2. 2004. Dostopno na http://www.delo.si/index.php?sv_path=43,50&src=mm (17. 1. 2006).
- M. B. / STA (2005): Biometrija – kmalu še ena stalnica? Delo, 2. 4. 2005. Dostopno na http://www.delo.si/index.php?sv_path=43,50&src=mm (17. 1. 2006).
- M.B. in STA (2005): Dobili smo informacijsko pooblaščenko. Delo, 31. 12. 2005. Dostopno na http://www.delo.si/index.php?sv_path=43,50&src=mm (17. 1. 2006).
- Marn, Aljaž (2005): Videonadzor na slovenskih avtocestah. Slo-Tech.com, 5. 12. 2005. Dostopno na http://www.slo-tech.com/clanki/05016/ (31. 5. 2005).

- Marn, Aljaž (2006): Informacijska zasebnost za potrošnike. Informatika za managerje, februar 2006. Dostopno na http://www.gambit.si/izm/2006/izm140406/izm140406_clanki.htm#zanimivo (31. 5. 2006).
- Marx, Gary T. (2002): What's New About the »New Surveillance«? Classifying for Change and Continuity. Surveillance & Society, 9-29. Dostopno na http://www.surveillance-and-society.org/articles1/whatsnew.pdf (14. 6. 2006).
- Mazi, Nina (2005): Videonadzor je lahko sporen. Delo, 14. 2. 2005. Dostopno na http://www.delo.si/index.php?sv_path=43,50&src=mm (17. 1. 2006).
- Mazzini, Miha (2002): Snemani vedno in povsod. Delo, 1. 10. 2002. Dostopno na http://www.delo.si/index.php?sv_path=43,50&src=mm (17. 1. 2006).
- Miko, Klavdija (2004): Zaradi računalniške napake se lahko znajdete tudi v zaporu. Ona, 1. 6. 2004. Dostopno na http://www.delo.si/index.php?sv_path=43,50&src=mm (17. 1. 2006).
- Mobbs, Paul (2002): Glossary and Cross-Reference Index. GreenNet Civil Society Internet Rights Project. Dostopno na http://www.fraw.org.uk/library/005/gn-irt/glossary.html#directed_surv (19. 8. 2006).
- Pahor, David (2003): Muhe Jerryja Springerja. Delu, 13. 10. 2003. Dostopno na http://www.delo.si/index.php?sv_path=43,50&src=mm (17. 1. 2006).
- Pečar, Janez (1986): Uspešnejše nadzorovanje – mit ali resničnost. Teorija in praksa 23(3), 549-565.
- Pečar, Janez (1988): Formalno nadzorstvo: kriminološki in kriminalpolitični pogledi. Ljubljana: Delavska enotnost.
- Pečar, Janez (1991): Neformalno nadzorstvo: kriminološki in sociološki pogledi. Radovljica: Didakta.
- Pečar, Janez (1995): Nadzorovanje kot najpomembnejša dejavnost. Teorija in Praksa 32(1/2), 130-137.
- Piano, Brane (2004): Veliki brat bo še malo počakal. Nedelo, 25. 4. 2004. Dostopno na http://www.delo.si/index.php?sv_path=43,50&src=mm (17. 1. 2006).

- Poklič, Milena B. (2006): Zapis zdravil na zdravstvene kartice. Novi tednik, 11.4.2006. Dostopno na http://www.novitednik.com/zapisi.php?id=173&id_zapis=617&m=04&l=2006 (5. 6. 2006).
- Praprotnik, Rok (2001): Sovin pogled v elektronsko pošto. Delo, 9. 10. 2001. Dostopno na http://www.delo.si/index.php?sv_path=43,50&src=mm (17. 1. 2006).
- Praš, Urša (2006): Skrito nasilje na avtobusih. Dnevnik, 18. 9. 2006, 30.
- Primožič, Rok (2005): Internet in pravica do zasebnosti. Specialistično delo, Ljubljana. Dostopno na http://www.cek.ef.uni-lj.si/specialist/primozic122.pdf (15. 5. 2006).
- Repovž, Grega (2004): Videonadzor pri delu pravno še neurejen. Delo, 21. 4. 2004. Dostopno na http://www.delo.si/index.php?sv_path=43,50&src=mm (17. 1. 2006).
- Rizman, Rudi (2003): Konec zasebnosti ali politični ekshibicionizem? Delo, 8. 5. 2003. Dostopno na http://www.delo.si/index.php?sv_path=43,50&src=mm (17. 1. 2006).
- RTV SLO in STA (2006): Sova lahko prisluškuje dve leti. RTV SLO portal, 31. 5. 2006. Dostopno na http://www.rtvslo.si/modload.php?&c_mod=rnews&op=sections&func=read&c_menu=1&c_id=110016 (31.5.2006).
- Salecl, Renata (1993): Zakaj ubogamo oblast?: Nadzorovanje, ideologija in ideološke fantazme. Ljubljana, Državna založba Slovenije.
- Sever, Jani (2003): Udbovske sence. Mladina, 25. 8. 2003. Dostopno na http://www.mladina.si/tednik/200334/clanek/uvod03-34/ (15. 5. 2006).
- Soban, Branko (2004): Pravica velikega brata. Delo, 18. 2. 2004. Dostopno na http://www.delo.si/index.php?sv_path=43,50&src=mm (17. 1. 2006).
- Stadler, Felix (2002): Opinion. Privacy is not the antidote to surveillance. Surveillance & Society, 9-29. Dostopno na http://www.surveillance-and-society.org/articles1/opinion.pdf (14. 5. 2006).

- Stanković, Tanja (2005): "Veliki brat" vas gleda ali kako se povečuje nadzor. Delo, 21. 12. 2005. Dostopno na http://www.delo.si/index.php?sv_path=43,50&src=mm (17. 1. 2006).
- Surette, Ray (2004) The thinking eye: Pros and cons of second generation CCTV surveillance systems. An International Journal of Police Strategies & Managment, 28(1), 152-173. Dostopno na http://www.emeraldinsight.com (6. 5. 2006).
- Sušnik, Dragica (2004): Varnostni ukrepi na letališčih se bodo v prihodnje le še zaostrovali. Nedelo, 22. 2. 2004. Dostopno na http://www.delo.si/index.php?sv_path=43,50&src=mm (17. 1. 2006).
- T. S. (2004): Nova pravila nadzora. Delo, 21. 12. 2004. Dostopno na http://www.delo.si/index.php?sv_path=43,50&src=mm (17. 1. 2006).
- T. S. (2004): Snemanje ljudi je skorajda prepovedano. Delo, 21. 12. 2004. Dostopno na http://www.delo.si/index.php?sv_path=43,50&src=mm (17. 1. 2006).
- T.S. (2003): Inteligentna hiša, kot jo ima Bill Gates. Delu, 7. 10. 2003. Dostopno na http://www.delo.si/index.php?sv_path=43,50&src=mm (17. 1. 2006).
- Trampuž, Martina (2000): Moderne tehnologije nadzorovanja. Javnost, Vregov zbornik 7, 133-144.
- Trampuž, Martina (2002): "Izguba skritosti z nadzorovanjem": Bentham in nove tehnologije nadzorovanja. Teorija in praksa 39(3), 346-357.
- Trampuž, Martina (2002): Izguba skritosti z nadzorovanjem: Bentham in nove tehnologije nadzorovanja. Magistrska naloga, Ljubljana.
- Triglav, Joc (2004): EVI – tehnologija za šoferje na vrvici. Življenje in tehnika letnik LV 3, 65-66.
- Viršek, Damnjana (2004): Bolj varne kartice s čipi. Delo in dom, 18. 2. 2004. Dostopno na http://www.delo.si/index.php?sv_path=43,50&src=mm (17. 1. 2006).
- Volk, Linda (2002): Delodajalca ne sme zanimati družina zaposlenega. Delo, 12. 3. 2002. Dostopno na http://www.delo.si/index.php?sv_path=43,50&src=mm (17. 1. 2006).

- Volk, Linda (2004): Dovoljeno je vse, kar je splošna norma. Delo, 21. 12. 2004. Dostopno na http://www.delo.si/index.php?sv_path=43,50&src=mm (17. 1. 2006).
- Žerdin, Ali H. (2003): Udba.net. Mladina, 18. 4. 2003. Dostopno na http://www.mladina.si/dnevnik/33843/ (15. 5.2006).
- (1991) Ustava Ustava Republike Slovenije. Dostopno na http://www.dz-rs.si/?id=150&docid=1&showdoc=1 (29. 5. 2006).
- (2002) Slo-Tech.com: Falus pa biometrija, 20. 5. 2002. Dostopno na http://www.slo-tech.com/script/forum/izpisitemo.php?threadID=136729#neprebrano (12. 9. 2006).
- (2003) STA: O aferi udba net. Portal Mladina, 24. 4. 2003. Dostopno na http://www.mladina.si/dnevnik/33984/ (17. 5 2006).
- (2004) Kazenski zakonik Republike Slovenije. Dostopno na http://www.uradni-list.si/1/objava.jsp?urlid=200495&stevilka=4208 (18. 8 2006).
- (2004) Slo-Tech.com: Biometrija na letališču, 30. 6. 2004. Dostopno na http://www.slo-tech.com/script/forum/izpisitemo.php?threadID=129790#neprebrano (12. 9. 2006).
- (2004) STOA: Development of surveillance technology and risk of abuse of economic information. European parliament, Scientific and Technological Options Assessment. Dostopno na http://cryptome.org/dst-1.htm#3.2 (18. 8. 2006).
- (2004) Zakon o elektronskih komunikacijah. Dostopno na http://www.uradni-list.si/1/objava.jsp?urlid=200443&stevilka=1925 (29. 5. 2006).
- (2004) Zakon o varstvu osebnih podatkov. Dostopno na http://www.uradni-list.si/1/objava.jsp?urlid=200486&stevilka=3836 (29. 5. 2006).
- (2005) www.privacyblog.net, 23. 3. 2005. Dostopno na http://www.privacyblog.net/index.php?p=34 (31. 5. 2006).

- (2005) www.privacyblog.net, 7. 2. 2005. Dostopno na http://www.privacyblog.net/_Publish/_Articles/Pamfil_Trgovske_kartice.html (31. 5. 2006).
- (2006) Dars - Kamere na avtocestah. Dostopno na http://www.dars.si/?id=155&PHPSESSID=2966a2ce2ed4529690978425048836b9 (4.6.2006).
- (2006) Gostja Nataša Pirc Musar na Studio City, TV SLO 2, 3. 7. 2006. Dostopno na http://www.rtvslo.si/modload.php?&c_mod=rplayer (26. 7. 2006).
- (2006) Home Office: Types of surveillance. Dostopno na http://www.homeoffice.gov.uk/security/surveillance/types-of-surveillance (13. 8. 2006).
- (2006) Informacijski pooblaščenec. Dostopno na http://ip.virtua.si (31. 5. 2006).
- (2006) Izvorne celice Evrope: Nadzor zasebnosti Evropejcev v boju proti terorizmu. RA 1, 13. 7. 2006. Dostopno na http://www.rtvslo.si/modload.php?&c_mod=rplayer (26. 7. 2006).
- (2006) Kje vas čevelj žuli. RA 2 – Val 202, 19. 7. 2006. Dostopno na http://www.rtvslo.si/modload.php?&c_mod=rplayer (20. 7. 2006).
- (2006) maps.google.com, 19. 8. 2006. Dostopno na http://maps.google.com (19. 8. 2006).
- (2006) On-Net Surveillance Systems: The Evolution of Video Surveillance - from CCTV to IP-Based. Dostopno na http://www.onssi.com/knowledgebase/evolution.php?pvc= (18. 5. 2006).
- (2006) Razlaga z razlogom: Biometrija. RA 2 – Val 202, 10. 8. 2006. Dostopno na http://www.rtvslo.si/modload.php?&c_mod=rplayer (10. 8. 2006).
- (2006) RTV SLO: Emporium snemal preoblačenje kupcev. RTV SLO portal, 26. 6. 2006. Dostopno na http://www.rtvslo.si/modload.php?&c_mod=rnews&op=sections&func=read&c_menu=1&c_id=112484&tokens=emporium (26. 6. 2006).
- (2006) Strokovnjak svetuje: Pooblaščenka za dostop do informacij javnega značaja Nataša Pirc Musar. RA 2 – Val 202, 27. 3. 2006. Dostopno na http://www.rtvslo.si/modload.php?&c_mod=rplayer (26. 7. 2006).

- (2006) Strokovnjak svetuje: Uporaba navigacijskih naprav prinaša boljše in napredno informiranje in s tem tudi boljšo varnost v prometu. RA 2 – Val 202, 26. 6. 2006. Dostopno na http://www.rtvslo.si/modload.php?&c_mod=rplayer (26. 6. 2006).
- (2006) Teleparc: Glossary. Dostopno na http://www.teleparc.net/html/en/glossary.html (19. 8. 2006).
- (2006) Varnost pred zasebnostjo. TV Dnevnik, SLO 1, 16. 8. 2006. Dostopno na http://www.rtvslo.si/modload.php?&c_mod=rplayer (18. 8. 2006).
- (2006) www.privacyblog.net, 4. 5. 2006. Dostopno na http://www.privacyblog.net/index.php?p=34 (31. 5. 2006).
- (2006) Zdravstvene kartice in zapis zdravil. RA 2 – Val 202, 5. 6. 2006 (ob 11:10).

9. PRILOGE

PRILOGA A: Pearsonovi koeficienti korelacije in rezultati regresijske analize

Tabela 0-1: Povezanost med spremenljivkami – Pearsonovi koeficienti korelacije med preučevanimi spremenljivkami (april 2004)

		zavedanje sodobnih tehnologij nadzora	svetovanje	vodenje	poznavanje sodobne tehnologije
zavedanje sodobnih tehnologij nadzora	Pearson koef.	1			
	St. značilnosti	.			
svetovanje	Pearson koef.	0.131(*)	1		
	St. značilnosti	0.026	.		
vodenje	Pearson koef.	0.068	0.164(**)	1	
	St. značilnosti	0.249	0.005	.	
poznavanje sodobne tehnologije	Pearson koef.	0.253(**)	0.038	0.124(*)	1
	St. značilnosti	0.000	0.518	0.036	.

OPOMBA: ** Korelacija je značilna pri stopnji značilnosti 0.01 (dvostransko).
* Korelacija je značilna pri stopnji značilnosti 0.05 (dvostransko).

Tabela 0-2: Rezultati regresijske analize ob odvisni spremenljivki: zavedanje sodobnih tehnologij nadzora (april 2004)

Neodvisne spremenljvike	Nestandardizirani regresijski koeficient B	Standardizirani regresijski koeficient Beta	t-statistika	stopnja značilnosti[27]
svetovanje	0.199	0.118	2.048	0.041 **
vodenje	0.037	0.018	0.308	0.758
poznavanje sodobne tehnologije	0.171	0.246	4.280	0.000 ***
KONSTANTA	0.843	- -	1.748	0.082

R = 0.281 R^2 = 0.079 R^2pop = 0.069 **F = 8.086*****

[27] Statistična značilnost t-statistike je lahko naslednja:
$p < 0{,}01 \rightarrow$ *** $0{,}05 \leq p < 0{,}1 \rightarrow$ *
$0{,}01 \leq p < 0{,}05 \rightarrow$ ** $p \geq 0{,}1 \rightarrow$

PRILOGA B: Anketna vprašanja

Zanima nas vaše poznavanje naslednjih stvari: (za vsako vprašanje obkrožite izbrano vrednost)

SDR RAM je hitrejši kot DDR RAM.	**a**. DRŽI **b.** NE DRŽI **c.** ne vem
Kaj od spodaj naštetega predstavlja osnovo za brezžične multimedijske komunikacije in jo uvrščamo v 3. mobilno generacijo?	**a.** NMT **b.** GPRS **c.** HSCDSD **d.** UMTS **e.** GSM **f.** ne vem
Zakaj se uporablja program WinRar?	**a.** za tabelne kalkulacije **b.** za pregled elektronske pošte **c.** za arhiviranje in stiskanje podatkov **d.** za snemanje zvoka **e.** ne vem
Kaj je mp3?	**a.** algoritem za stiskanje zvoka **b.** program za poslušanje glasbe **c.** vrsta tekstovnih datotek **d.** multimedijski protokol **e.** ne vem
Kolikšna NI kapaciteta CD-R medija?	**a.** 650 Mb **b.** 700 Mb **c.** 500 Mb **d.** 800 Mb **e.** ne vem
Kaj je ICQ?	**a.** program za mobilno komunikacijo **b.** program za pošiljanje elektronske pošte **c.** ponudnik internetne pošte **d.** program za neposredno komunikacijo **e.** ne vem
S katerim programom je možno odpreti format rtf?	**a.** Acrobat Reader **b.** ACDSee **c.** Word **d.** WinAmp **e.** ne vem

Ali spodnje trditve držijo? (v vsaki vrstici obkrožite izbrano vrednost)

	1 – drži	2 – ne drži	3 – ne vem
Na nekaterih ljubljanskih mestnih avtobusih je nameščena kamera.	1	2	3
Moj ponudnik internetnih storitev lahko vedno ugotovi, katere spletne strani sem obiskal.	1	2	3
V novih slovenskih potnih listih bo shranjen prstni odtis.	1	2	3
Spletne trgovine sproti prilagajajo ponudbo, glede na moje pretekle aktivnosti na tej strani.	1	2	3
Ob uporabi mobilnega telefona, mobilni operater ne more ugotoviti, kje se v določenem trenutku nahajam.	1	2	3

V kolikšni meri se strinjate s spodnjimi trditvami. Vsako trditev ocenite na lestvici od 1- sploh se ne strinjam do 5- popolnoma se strinjam (v vsaki vrstici obkrožite izbrano vrednost.)

	1 – sploh se ne strinjam	2 – se ne strinjam	3 – se niti ne strinjam niti strinjam	4 – se strinjam	5 – popolnoma se strinjam
Večkrat se znajdem v situaciji, ko odločam kaj naj bi drugi ljudje počeli.	1	2	3	4	5
Kadar razpravljam z drugimi, jih le redko prepričam v svoj prav.	1	2	3	4	5
Ko poskušajo moji prijatelji rešiti kakšen problem, me prosijo za nasvet.	1	2	3	4	5
Prijatelji pri izbiri filma, ki se predvaja v kino, navadno upoštevajo moje mnenje.	1	2	3	4	5
Če grem jaz na zabavo, gredo tudi prijatelji.	1	2	3	4	5
Večkrat me prijatelji vprašajo za nasvet pri izbiri filmov, knjig ali glasbe.	1	2	3	4	5
Prijatelji so pripravljeni spremeniti svoje navade samo zato, da bi mi ugajali.	1	2	3	4	5

Demografija(obkroži, dopiši)

Spol: M Ž, ***Letnik študija***:_____, ***Fakulteta***:_____.