UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Aleksander Debelak

DIGITALIZACIJA NADZORA

Diplomsko delo

Ljubljana, 2007

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Aleksander Debelak
Mentorica: doc. dr. Tanja Oblak
Somentorica: doc. dr. Sandra Bašić Hrvatin

DIGITALIZACIJA NADZORA

Diplomsko delo

Ljubljana, 2007

Hvala vsem, ki so mi med študijem stali ob strani.

Digitalizacija nadzora

Bentham je predstavil idejo panoptikona, zapora, kjer so zaporniki na očeh paznika, le ti pa njega ne morejo videti. Idejo je prevzel Foucault, ki pa je panoptikon utemeljil s psihičnim pritiskom, ki prisili posameznika v samonadzor. Moderne tehnologije so omogočile nov vidik, prisotne so lahko povsod in ne potrebujejo človeških upraviteljev. Problem, ki ga digitalizacija predstavlja, je predvsem vprašanje zasebnosti. Če je bil prej nadzor omejen na posamezne institucije, je danes lahko vseprisoten. Nadzor ni več samo klasični fizični nadzor, ampak se upravlja tudi nadzor nad podatki. Video nadzor je postal kompleksno orodje, ki lahko s pomočjo računalnika in zbirke podatkov reagira samostojno. Nadzor je v interesu tako politike kot tudi ekonomskega sektorja. Prvi nadzirajo državljana, drugi pa potrošnika. Odnos posameznika, ki je nadziran, do nadzora je pogojen z koristmi, ki jih določena oblika nadzora prinaša. Racionalizacija je ena od najpomembnejših koristi. Naloga države je, da nadzor regulira. Le tako lahko onemogoči kršenje svoboščin.

Ključne besede: panoptikon, nadzor, digitalizacija, zasebnost, video nadzor

Digitalization of Surveillance

Bentham introduced the idea of Panopticon, of prison where guard can see all convicts but they can not see the guard. Foucault based his view of Bentham's Panopticon on psychological pressure, that forces individual to self-control. New technologies enabled new perspective, they can be applied almost everywhere and do not need human supervising. The main problem that occurs with digitalization is privacy issue. If surveillance before was restricted only to some institutions, is now omnipresent. Surveillance now is not just physical anymore. It is implemented in our existing data and also other video, audio or other information about us. CCTV becomes a complex tool, which can act on its own with help of computer and database. Surveillance works in interest of politics and also economic sector. First puts citizen under surveillance and the second puts consumer. Relation of individual towards surveillance depends on benefits he gets from different forms of surveillance. Government’s duty is to regulate surveillance, because this is the only way to preserve human freedoms.

Key words : panopticon, surveillance, digitalization, privacy, CCTV

Kazalo

Kazalo slike, shem in tabel

1. Uvod

Pisatelj Bo Aikens pride v idilično mestece, Black River, kjer so vsi srečni in prijazni. Vendar videz vara. Po vsem mestu so nameščene kamere, ki jih upravlja računalnik. Računalnik, ki se imenuje Periklej, hoče ustvariti popolno mesto in svojih meščanov ne spusti izven njegovih meja. To je oris zgodbe filma Black River (2001), posnetega po noveli znanega pisatelja Deana Koontza. Koncept filma ni nov v znanstveni fantastiki, saj isto temo obravnava mnogo znanstveno fantastičnih zgodb, filmov in nanizank. Za večino je značilno, da je nadzor totalen. Ker deluje v skladu s svojimi programi, računalnik ne diskriminira in odloča tudi o tem, kdo bo živel in kdo umrl.

Prednost računalnikov je, da pri svojem delovanju nimajo moralnih pomislekov, ne diskriminirajo in so neprimerno hitrejši od ljudi, saj obdelujejo samo informacije, bistvene za analizo.

Če se vrnemo k literarnim predlogam, ki zelo nazorno prikazujejo naš strah pred popolnim nadzorom. V Orwellovem delu 1984 je Winston Smith živel v večnem strahu pred Velikim Bratom in njegovim pogledom s tele zaslona. Nikoli ni vedel, kdaj je pod nadzorom in kdaj ni. Če bi Orwell pisal svoje delo danes, bi bil Winston pod neprestanim nadzorom. Računalniški sistemi bi vsako odstopanje od normalnih vzorcev zabeležili in po možnosti tudi posredovali. Svetovno znani fizik Stephen Hawking večkrat pravi, da je znanstvena fantastika tista, ki daje znanstvenikom ideje za iskanje alternativnih možnosti. Mnoge ideje opisane v znanstveno fantastičnih delih so danes že uporabljene v praksi[1].

Orwell je predpostavil klasičen panoptičen nadzor, ko nadzorovani ne ve, kdaj je nadzorovan, vendar ga nadzornik v vsakem trenutku lahko vidi oz. sliši.

Sodobne teorije nadzorovanja v glavnem temeljijo na Benthamovi ideji panoptičnega nadzora. Zapor, kjer nadzirani ne vidijo nadzornika in ne vedo kdaj, in če sploh, so nadzorovani, je ideja, ki jo moderne teorije in seveda tehnologije s pridom

[1] Korejska družba Samsung Techwin je s pomočjo korejske vlade naredila Robota za nadzor in varovanje (Intelligent Surveillance & Security Guard Robot). Opremljen je z najsodobnejšo nadzorno in sledilno tehnologijo ter orožjem
(http://www.samsungtechwin.com/product/features/dep/SSsystem_e/SSsystem.html)

izkoriščajo. Foucault je preoblikoval Benthamov koncept panoptikona in z njim označil naravo modernega nadzora (Kim 2004: 195).

Danes bi bilo lahko drugače. Nadzor bi bil lahko stalen, čuvajevo funkcijo pa bi prevzel računalnik. Algoritmi bi določali normalne parametre, vsa odstopanja bi pomenila izvajanje novih algoritmov in reakcijo na dejanja. Če Winston ni vedel, ali je nadzorovan ali ni, se danes ne bi ukvarjal s tem problemom, vedno bi bil pod nadzorom. Vendar pa ne bi mogel biti podvržen diskriminaciji, kot bi lahko bil v primeru, če bi se zameril nadzorovalcu. Algoritmi namreč ne morejo diskriminirati (Graham in Wood 2003: 232). Sicer to ne pomeni, da ne diskriminira programer; program le izvršuje ukaze.

»Eno pomembnejših sociooloških vprašanj o tehnologiji in družbi je,« piše Kim »kako in v kolikšni meri tehnologija vpliva na našo družbo« (2004: 194). Danes tehnologiji popolnoma zaupamo, vendar to zaupanje ni upravičeno. Kot piše Neumann:

> *Živimo v svetu, ki vsebuje tekmovanje med korporacijami, kriminalce in nepoštene ljudi*[2]*. Zato obstaja potreba za varovanje sistemov pred zlorabami, prav tako je potreba po nadzoru. Vseeno pa mora biti nadzor pod drobnogledom, saj lahko kmalu postane nedružben in nevaren, tvegan. V posameznih primerih primerna kontrola ni možna, zato se je potrebno odločiti ali naj omejujemo zasebnost in nadzor. V vsakem primeru pa moramo paziti, da identificiramo in minimiziramo tveganja, ko skušamo prepoznati in zadovoljiti nasprotujoče zahteve (1993: 122).*

Nadzor je torej, kljub vsemu pomemben in lahko rečemo, da za to niso krivi, kot pravi Neumann, korporacije, kriminalci in nepošteni ljudje (1993: 122), ampak celotna družba, ki z nadzorom udejanja norme in pravila obnašanja. Za poenostavitev, večina se, če ni nadzora, vede drugače in ponavadi ravna iz sebičnih razlogov. Če bi se tveganj zavedali že preden storimo kaj, kar ni dovoljeno, se ne bi spraševali glede zasebnosti, saj bi bila ta samoumevna.

Birokratski in elektromehanski nadzor se vedno bolj umikata digitalnemu nadzoru. Tako imenovani podatkovni nadzor[3] s pomočjo digitalnih tehnologij in algoritmov omogoča pravzaprav popolni nadzor. Ob zbranih podatkih in povezanih

[2] Originalno: clandestinely dishonest people – skrivno nepoštene ljudi
[3] Ang. dataveillance

bazah podatkov se lahko na podlagi določenih parametrov samodejno odloča za svoje delovanje.

Kot posledica nadzora velikokrat trpi naša zasebnost. Vendar se ji velikokrat odrečemo tudi sami. Kot piše Elmer, imamo dostikrat koristi, če posredujemo podatke (2003:232). V trgovinah dobimo kartice popusta, možnost za sodelovanje v nagradnih igrah, nikoli pa se ne vprašamo, kaj počnejo z zbranimi podatki. Kljub temu, da nam zagotavljajo, da podatkov ne bodo uporabljali v druge namene, se podatki o nas vseeno zbirajo. Kartice popustov tako prodajalcu povedo kaj kupujemo in kolikokrat. Zasebnosti se odrekamo zaradi različnih vzrokov. Kot pravi Kim v svoji analizi odnosa med tehnologijo, zasebnostjo in družbenim nadzorom na primeru vpeljave elektronske identifikacijske kartice v Južni Koreji, je to lahko zaradi: podpore tehnološke industrije, kot v primeru Južne Koreje zaradi kolektivistične tradicije, državna varnost, zanemarjanja socialnih pravic zaradi ekonomske konkurenčnosti in brezbrižnosti do politike (Kim 2004: 206–207).

Nadzor nad infrastrukturo je v bistvu še najmanj nevaren, če ga seveda ne uporabljamo za sledenje dela, gibanja in komuniciranja posameznikov ali skupin. Ponavadi je namenjen uravnavanju, usmerjevanju in urejanju prometa. Kljub vsemu pa tehnologije omogočajo, da jih lahko brez posebnih težav uporabimo za nadzor nad posamezniki.

Zlivanje in povezovanje tehnologij je omogočilo, da je nadzor vedno bolj zakrit. Včasih se ga iz različnih vzrokov niti ne želimo zavedati. Tako je lahko mobilni telefon, poleg tega, da je komunikacijski aparat, še odličen oddajnik naše lokacije ipd.

Ali pa ga uporabimo kot izgovor, da smo videni. Fizična prisotnost je zamenjana s tele-prisotnostjo[4] (Virilio v Koskela 2003: 294). To je najbrž vzrok za popularnost oddaj tipa Veliki brat. Nastopajoči so tam, da bi bili videni, gledalci pa prevzamejo vlogo nadzornika in nastopajoče tudi kaznujejo, če se ti ne obnašajo, ali samo niso takšni kot, se od njih pričakuje.

[4] ang. tele-presence

1. 1 Predstavitev naloge

Cilj te naloge je predvsem predstaviti oblike nadzora, ki so postale mogoče z digitalizacijo. Kljub temu, da sta Benthamov panoptikon in Foucaultovo razumevanje tega bistvena za sodobne razlage nadzora, se bom predvsem posvetil modernim teoretskim razlagam.Večina avtorjev ima razumevanje Benthamovega panoptikona za samoumevnega, medtem, ko bi bila analiza Foucaultovega razumevanja lahko delo zase. Tako bom najprej predstavil osnovne točke panoptikona po Benthamu in Foucaultu. V nadaljevanju bodo predstavljene sodobne teorije in tehnološke spremembe, ki zahtevajo novo razumevanje konceptov ter vplivajo na obliko nadzorovanja, razumevanje zasebnosti in zbiranje osebnih podatkov.

Drugi del naloge bo namenjen praktičnim vidikom modernega nadzora. Video nadzor, ki je temelj prostorskega nadzora, in problemi, ki jih ta prinaša, predvsem v odnosu do zasebnosti. Podatkovni nadzor bo naslednja tema, posebno problematičen je zaradi uvedbe »super« identifikacijskih kartic, v katerih so shranjeni naši osebni podatki, tudi biometrični. Hkrati pa so ključ do velikih baz podatkov, ki združujejo vse podatke, ki jih razne institucije shranjujejo o nas. V nadaljevanju bodo opisani nadzor komunikacij in informacij, ki jima bo sledil nadzor prometa. V poglavju o regulaciji bo predstavljena predvsem regulacija video nadzora, ker je ta najbolj očiten in prisoten. Regulacija nadzora je tesno povezana z zakoni o zasebnosti, oz. je del njih. Ker je večina hitrih sprememb v oblikah nadzora posledica dogodkov 11. septembra 2001, se bo naloga nadaljevala z analizo sprememb zakonodaje in uporabe tehnologij v času po 11.9. Konec bo posvečen javnomnenjskim raziskavam stališč do nadzora, na kanadskem primeru, in koliko so te sploh zanesljive. Z nalogo bom skušal pokazati, da ljudje namenoma spregledajo vdor v njihovo zasebnost, zaradi racionalizacije in pohitritve storitev, ki jih nove tehnologije omogočajo.

2. Teoretski pristopi

2. 1 Panoptikon

Večina sodobnih teorij nadzorovanja, v prebranih delih, temelji na Benthamovi ideji panoptičnega nadzora. Zapor, kjer nadzirani ne vidijo nadzornika in ne vedo kdaj, in če sploh, so nadzorovani, je ideja, ki jo moderne teorije in seveda tehnologije s pridom izkoriščajo. Foucault je tisti, ki je prevzel Benthamov koncept in z njim označil naravo modernega nadzora. Subjekt nadzora, zaradi neusmiljenosti opazovalca, začne s samonadzorom in dopusti, da se nadzor raztelesi (Foucault v Kim 2004: 195). Tako razumevanje panoptikona, pravi Kim, lahko razumemo kot prehod s tradicionalnega na moderni način nadzora, z javnega, zunanjega in kaznovalnega na skritega, notranjega in preventivnega (2004: 196).

Slika 2. 1. 1: Panoptikon

(vir: www.uweb.ucsb.edu)

Bentham in Foucault imata, kljub temu, da prvi podpira telesno kaznovanje, kot je fizična osamitev, drugi pa bolj psihološko raven nadzora, skupno to, da nadzor temelji na vizualnem opazovanju (Kim 2004:196). Poleg tega, da so nadzorovani v panoptikonu videni, se moč nadzorovalca kaže tudi v enostavni arhitekturni postavitvi, ki nadzorovane ločuje in hkrati klasificira s pomočjo dokumentacije (Elmer 2003: 234).

Nadzor je za Foucaulta (1984: 138) urjenje teles. Družbe so oblikovale sredstva discipliniranja, v katerih so vedno navzoče tehnike in strategije moči, ki jih Foucault imenuje »disciplinske družbe«. Cilj discipline pa je oblikovanje podrejenih, izurjenih, krotkih teles (Foucault 1984: 137-138).

Moderne tehnologije so prinesle mnoge novosti v tehnike nadzorovanja. Čeprav je Foucaultov koncept »panopticizma« še vedno dominanten v znanosti, pa ga moramo po Posterju še enkrat preveriti (Graham in Wood 2003: 230). Foucault namreč ni upošteval procesa digitalizacije. Razvoj tehnologije in infrastrukture konec 20. stoletja je kvalitativno drugačen od njegovih primerov:

> Današnji način komunikacije in baze podatkov, ki jih pri tem ustvarja, oblikujejo Superpanoptikon, sistem brez zidov, oken, stolpov ali čuvajev. Kvantitativni napredek v tehnologijah nadzora ima za posledico kvalitativno spremembo v mikrozgradbi (*mikrophysics*) moči (Poster, po Graham in Wood 2003: 230).

To »panoptično strmenje« je vedno bolj razširjeno in prisotno v vseh možnih prostorih, še v kopalnici kot piše Gary Marx (Kim 2004:196). Kovačič (2003) piše, da je nadzor hkrati dober in slab, saj je danes nadzorovanje posameznikov tako sredstvo družbenega nadzora, kot tudi sredstvo za zagotavljanje pravic participacije. Ravno tako ne moremo mimo tesne povezanosti nadzora s tehnologijo, saj so informacijske tehnologije namenjene zbiranju in obdelavi vseh vrst podatkov in informacij o okolju in družbi v kateri živimo. Tako ima informacijska tehnologija danes velik pomen za nacionalno varnost. »Informacijska družba je družba nadzora« (Kovačič 2003:11).

Nadzor postaja globalen, kot pravi Lyon (2004: 139), danes ne vidimo več s kom menjamo oz. sodelujemo v interakciji. Vsi so geografsko oddaljeni od nas. Bolj ko se družbeni odnosi širijo, vedno bolj interakcije in transakcije, zaradi vpliva novih komunikacijskih tehnologij, postajajo abstraktne in raztelešene, kar ogroža zaupanje, ki je nekoč temeljilo na osebnem in istočasnem stiku .

Nadzor postane očiten šele takrat, ko se ljudje začnejo zavedati, da so opazovani. Nadzor je lahko očiten, kot je na primer nadzor s kamerami (CCTV), ali bolj metaforičen, kot so prijave na letališčih, plačevanje v trgovinah, internetni piškotki, kadar pokažemo vozniško dovoljenje policistu ipd. (Lyon 2004: 135).

Nove tehnike nadzora se uporabljajo tudi za nadzor potrošnikov. Moderne revizije za razliko od večine kritik, ki se predvsem zaradi preveč dobesednega razumevanja Foucaulta, osredotočajo predvsem na kritiko zapora kot prostora, po Elmerju (2003: 232), ponujajo za razlago panoptikona tri razumevanja.

Prvo se osredotoči na premik arhitekturni in kategoričnih lastnosti nadzora iz zaprtega prostora, kot je zapor, v baze podatkov o potrošnikih (Elmer 2003: 232). To je tako imenovani »dataveillance«, ki zadeva predvsem družbene vplive panopticizma na zasebnost.

Druga skupina strokovnjakov dvomi, da so posamezniki prisiljeni v to, da oddajo svoje podatke. Oddajo jih zavedno, zaradi koristi, ki jih pri tem dobijo[5]. Whitaker celo pravi: »Panoptikon nagrajuje sodelovanje« (Elmer 2003: 232).

Za tretje razumevanje pa Elmer piše, da mnogi avtorji govorijo o novi obliki panoptikona, sinoptični nadzor, ko mnogi nadzorujejo maloštevilne. Fiske primerja novo stanje s stadionom, kot »obrnjenem panoptikonu«, kjer zaradi možnosti individualizacije, segmentiranja in upravljanja, navijači dobijo moč, znanje in zadovoljstvo[6] (Elmer 2003: 232).

Meje med temi pogledi so v bistvu zelo zabrisane in se med seboj prepletajo. Vloga panoptikona ni več samo discipliniranje, oz. kaznovanje, ampak lahko tudi nagrajuje (Elmer 2003: 245). Kar se vidi predvsem na primeru potrošnikov.

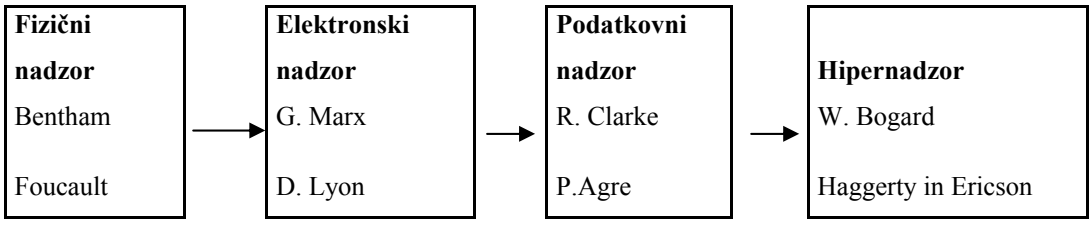
[5] Nagrada, popust ali posebne storitve (Elmer, 2003: 232)
[6] Še posebej kadar je posredovana z mnogih zornih kotov na televiziji (Fiske, po Elmer, 2003: 232).

2. 2 Digitalizacija nadzora

Napredek v tehnologiji je omogočil hkrati velikanski skok v nadzorovalnih tehnikah. V Benthamovem času je nadzor pomenil fizično prisotnost nadzorovalca. Z nastankom modernih držav je sledila birokratizacija in s tem nadzor z zbiranjem podatkov, ki se mu je v drugi polovici 20. stoletja priključili še elektromehanski nadzorni sistemi. Kljub vsemu pa je bil za nadzor še vedno potreben nadzornik, ki je pridobljene podatke filtriral, posredoval ali drugače uporabil.

Kim (2004) naredi analizo razvoja razprav o nadzornih tehnologijah in njihovem družbenem vplivu (Shema 1). Z njo pokaže, kako se z novimi tehnologijami spremeni odnos do družbenega nadzora, kar vpliva na teorijo.

Shema 2. 2. 1: Družbeni vpliv nadzornih tehnologij



(Vir: Kim 2004: 195)

Bentham in kasneje Foucault predpostavljata fizični nadzor. Foucault prepozna Benthamov panoptikon kot arhitekturni izraz moderne želje po opazovanju, nadzoru in vladanju (Kim 2004:196). Vpliv panoptikona pa je mogoč zaradi nevednosti, ali je nadzornik prisoten ali ni. Na elektronski nadzor lahko gledamo kot na izboljšavo tradicionalnih nadzornih sistemov. Vpliv elektronskega nadzora na družbo in bistveno drugačen od tradicionalnih nadzornih orodij. Razlikuje se le v stopnji koliko podatkov lahko shranimo, ne da bi nadzor pretirano vplival na družbo (glej Kim 2004: 201). Procesi podatkovnega nadzora povzročijo premik človeškega telesa izven prostorskih omejitev in ustvarjajo »digitalno persono«, ki temelji na podatkih zbranih o posamezniku. Hipernadzor gre še korak dlje. Bogard napove nadzor, ki ne samo, da bo

videl vse, ampak bo lahko to počel vnaprej. To bo počel s simulacijo (glej Kim 2004, Lyon 2001, Lyon 2003). Teoretski pristopi se prilagajajo novim tehnologijam in kmalu si lahko predstavljamo nadzorne sisteme, ki bodo tako izpopolnjeni, da bodo omogočali tudi hipernadzor[7].

2. 2. 1 Lyon in štiri veje v teoriji

Po Lyonu (2001: 329) lahko ločimo štiri veje v teoriji, ki so vse povezane s klasičnimi predstavami modernosti.

Nadzor lahko razumemo v povezavi z nacionalno državo, z birokracijo, s tako imenovano tehnološko logiko in politično ekonomijo. Pri vseh je poudarek na sistematični in usmerjeni pozornosti organizacij na posameznikovo življenje. Digitalizacija vsem tem tipom omogoči, da se dodatno razširijo in poglobijo.

1.) Nadzor, ki je potreben na nivoju nacionalne države, se osredotoča na politične cilje znotraj geopolitičnih in vojaških bojev (Lyon 2001: 329). V zadnjem času lahko opažamo, kako se države vrivajo v nadzorne sisteme, jih oblikujejo ter instituciolizirajo elektronske sisteme, pod pretvezo boja proti kriminalu in terorizmu (Shields 2006: 22). Teoretično se nadzor na ravni nacionalne države naslanja na teorijo Mosce, Pareta, Sorela in Michelsa, ki trdijo, da je notranji nadzor, kljub namenu, da bi izboljšal sistem, boj med državami (Lyon 2001: 329) oziroma proti kriminalu in terorizmu, ki pa sta dandanes globalna in ju lahko razumemo kot zunanjo silo. Če primerjamo današnji nadzor z metodami tajne policije v ZSSR in Vzhodni Nemčiji, pred padcem Berlinskega zidu, so lahko danes metode bolj prikrite, nadzor pa še bolj učinkovit.

2.) Druga veja je tesno povezana s prvo in se nanaša na opis birokratske organizacije Maxa Webra. Weber vidi nadzor ne kot boj med državami, ampak kot proces racionalizacije. Birokratizacija pomeni povečanje učinkovitosti sistema (Lyon 2001: 330). Danes se ta sistem razvije v t.i. »dataveillance«, podatkovni nadzor. Računalniki omogočajo resnično racionalizacijo, saj lahko povezujejo veliko število baz podatkov v trenutku.

[7] Kot primer novih tehnologij lahko omenimo kvantni računalnik, ki naj bi že deloval in naj bi omogočal neverjetno večje število simulacij kot navadni digitalni računalniki(http://www.dwavesys.com).

3.) Elullov način razumevanja družbe kot tehnološke družbe (La Technique), je tretja veja. La Technique integrira stroj v družbo in ustvarja svet kot ga stroj potrebuje (Lyon 2001: 331). To lahko opažamo v današnjem hitrem razvoju, ko ljudje v bistvu ne sledimo več posameznim spremembam. To govori v prid tistim, ki zagovarjajo strožji nadzor komunikacijskih poti po 11. septembru, saj so bile metode, ki so jih uporabljali, zastarele. (Shields 2006). Ellulov pristop prikazuje bolj kot zmagoslavje moči La Technique, njeno usmeritev. Vendar so bili njegovi strahovi, še posebej kar se uporabe tehnologij tiče zelo upravičeni (Lyon 2001: 331). Tehnološke rešitve uporabljamo danes na vsakem koraku. Vsak nakup, vsako iskanje informacij se zabeleži v baze podatkov.

4.) Politična ekonomija je četrta veja v moderni teoriji nadzora. Predvsem v kapitalističnih organizacijah je nadzor zelo močan. Nadzor je tu strateško sredstvo za reprodukcijo enega razreda in njegovih interesov nad ostalimi (Lyon 2001: 331). Tako lahko lastniki podjetij vzamejo podatke s telesa posameznikov, da jih sledijo znotraj organizacije, natančno spremljajo njihovo delo (štetje pritiskov tipk na tipkovnici). Na ta način izvejo več o delavcu kot bi izvedeli z intervjujem (Ball 2005: 91). Politično ekonomski pogled se v 70ih in 80ih letih prejšnjega stoletja usmeri v potrošniško fazo. Z analizo zbranih podatkov o vedenju potrošnika skušajo uravnavati potrošnjo. Z zbranimi podatki pa skušajo potrošnike tudi razvrstiti v različne skupine in s tem ustvarjajo neenakost (Lyon 2001: 334). Na ta način lahko razumemo odločitev Walmarta v Zda, da se bolj približa vsem demografskim skupinam. Za Walmart je značilna populacija kupcev z dohodki nižjimi od povprečja. Zdaj pa trgovine oblikujejo ne več po načelu ena za vse, ampak jih prilagajajo vsaki demografski skupini posebej.

2. 2. 1 Elementi nadzora

Kirstie Ball v svojem delu Elements of Surveillance (2002) (Ball 2005: 93) opiše štiri elemente nadzora. 'Predstavljanje' se nanaša na tehnološki element, in ponazarja kako lahko nadzorovalne tehnologije predstavijo podatke, ki so bili zbrani pri viru ali preko drugega tehničnega medija. 'Pomen' se nanaša na potencial nove nadzorne tehnologije, da omogoči nove interpretacije življenja, kot tudi nove interpretacije nadzora samega. Nadzoru pripisujemo vsaj tri pomene: nadzor kot znanje, nadzor kot informacija in nadzor kot varovanje pred grožnjo. Naslednji element je 'manipulacija',

ki se nanaša na neizogibnost odnosov moči pod nadzorom. Odnosi moči so vidni v tem kako nadzorne institucije ali skupine lahko regulirajo pretok informacij in znanja o nadzorovanem področju med različnimi strankami; strategije upora skrbijo za prekinjanje in motenje tega pretoka ter ustvarjajo prostorsko-časovne vrzeli med opazovalcem in opazovanim. Četrti element so 'posredniki', to so udeleženci nadzorovanega področja. V procesu posredovanja se pripisujejo pomeni, tehnologije znova predstavijo informacije, tu deluje moč/upor in se mreže povezujejo.

2. 2. 3 Lastnosti novih tehnologij

Z digitalizacijo se začne nova doba. Nadzor je vedno bolj avtomatičen. Kot pišeta Lianos in Douglas se je delo človeških upravljavcev, iz neposrednega posredovanja in lastnega preudarka, spremenilo v oblikovanje, programiranje, nadzor (ang. Supervision) in vzdrževanje avtomatskega ali polavtomatskega nadzornega sistema (Graham in Wood 2003: 228).

V svoji analizi sodobnih literature je Gary Marx (Kim 2004: 198) opazil porast naslednjih znanstvenih in tehničnih pristopov k družbenemu nadzoru:

- zmožne so premagati velike razdalje, pomanjkanje svetlobe in ostalih fizičnih omejitev;
- so brezčasne[8];
- zahtevajo predvsem kapital in ne delovne sile;
- osredotočajo se na vse možne kršitelje, ne na posamezne poglede kršitev;
- namenjene so predvsem na preprečevanju[9] kršitev in ne na njihovemu preganjanju;
- so decentralizirane, zato spodbujajo samonadzor in zaviranje
- so v bistvu nevidne;
- poglabljajo in širijo nadzor na nova področja.

[8] Ang. able to transcend time
[9] Ang. prevention

Agre našteje glavne družbene in tehnološke spremembe, ki so omogočile hitro rast bolj nevarnih a manj vsiljivih in obvladljivih tehnologij. Najpomembnejše so :

- novi digitalni mediji, ki oblikujejo nove in nove vrste družbenih odnosov;
- nastanek globalnih digitalnih omrežij;
- ljudje so vzeli nove tehnologije za svoje do take stopnje, da v glavnem ni možno videti škodljivih učinkov;
- erozija odnosa med javnim in zasebnim, še posebej zaradi združevanja prostorov, ki so bili včasih ločeni;
- paradoksalno neujemanje med relativno visokim moralnim ozaveščenjem glede zasebnosti in nizko ravnjo praktične skrbi za zasebnost (Agre 1994).

V preteklosti so bile jasno določene meje med zasebnim in javnim. Vendar se pomen teh mej s časom manjša. Večina kulturnih in moralnih tabujev postaja primernih v vsakdanjem življenju. Digitalizacija bo prinesla nov pogled na svet. V tem na novo skonstruiranem življenjskem svetu[10] bodo ljudje navajeni na neprestan nadzor in jih bo v bistvu strah, da ne bi bili varovani znotraj digitalnih omrežij (Kim 2004: 204).

Za digitalne nadzorne tehnologije je značilno, da so zelo fleksibilne in protislovne. Po eni strani so lahko oblikovane, da

> *... izključujejo na osnovi avtomatskih sodb ali ekonomske vrednosti; po drugi strani pa so isti sistemi lahko programirani, da premagajo družbene meje in procese marginalizacije. Širše družbene in politične posledice digitalnega nadzora so tako mogoče. Ker so fleksibilne, je možno, da so pod vplivom političnih, ekonomskih in družbenih razmer, ki oblikujejo načela, vpeta v njihovo (DNT) oblikovanje in uporabo (Graham in Wood 2003: 229).*

2. 2. 4 Lastnosti digitalnega nadzora

Očitna razlika med elektromehanskim oz. analognim in digitalnim nadzorom je v količini in hitrosti shranjevanja podatkov. Računalniški trdi diski lahko shranijo

[10] Kim tu uporabi *life-world*

mnogo več podatkov, hitreje in v primernejši obliki. A kot pravita Graham in Douglas, je temeljna razlika v načinu, kako lahko zbrane podatke uporabimo (2004: 231).

Pri digitalnem nadzoru potekata dva temeljna procesa. Da bi bil nadzor čimbolj učinkovit, mora biti senzor[11] povezan z bazo podatkov, hkrati pa mora potekati primerjava med svežimi in shranjenimi podatki. Drugi proces je algoritemski nadzor[12]. Ta na podlagi zgornje primerjave podatkov določi napoved ali celo reakcijo[13] (Graham in Wood 2003: 231).

> *Algoritmi so v bistvu matematični oz. logični termin za skupek navodil. Lahko jih razdelimo na trivialne in ne-trivialne tipe. Prvi so navodila, ki so uporabni samo za specifične situacije, ali nalogo, ki potrebuje dodatno razlago. Drugi pa so navodila, ki posredujejo odgovore, če je vnos kompatibilen. Algoritme pogosto primerjajo z recepti, kot primerno metaforo za razumevanje koncepta, čeprav je v tem primeru nenatančen: recept je bolj program (Introna in Wood, 2004: 180).*

Računalnik namreč algoritmov sam ne razume in morajo biti prevedeni v njemu znan jezik. Ta jezik so programi. Programi so torej sestavljeni iz več algoritmov z namenom, da proizvedejo želeni produkt s strojno opremo (Introna in Wood 2004: 180).

Gary T. Marx zagovarja tezo, da algoritemski nadzor daje možnost za odstranitev potencionalne korupcije in diskriminacije. Tako na primer rasistični policist ne bi mogel aretirati posameznika le na podlagi rasnih značilnosti, če ga sistem ne bi prepoznal kot iskano osebo (Graham in Wood 2003: 232).

Kljub vsemu pa algoritemski sistemi, ko je izvzet človeški faktor, pomenijo grožnjo. Pri avtomatskih odzivnih sistemih, lahko pomeni to smrt brez razlage ali možnega ugovora (Graham in Wood 2003: 232). Vseeno pa bi še poudaril, da algoritmi oziroma programi sami po sebi niso zmotljivi, vendar ker jih programirajo ljudje je možnost napake vseeno velika.

Nadzor je postal pomemben del vladanja. Obvladuje družbene odnose in prispeva k oblikam družbene ureditve. In to počne s t.i. naravno močjo[14], ki ustvarja

[11] Npr. closed circuit TV (nadzorna kamera + snemalni sistem)
[12] npr. avtomatiziran (Debelak)
[13] Zelo dober primer za to bi bil ameriški protiraketni ščit. Ko sateliti zaznajo izstrelitev, ga sistem preveri v bazi podatkov. Če jo prepozna kot medcelinsko balistično raketo, izstreli protibalistično raketo.
[14] Ang. biopower

ljudi s tem, da jih klasificira v posamezne kategorije. Te kategorije pomenijo tako tveganje kot tudi nove priložnosti (Lyon 2000: 8).

> *Kategorizacija je star proces vendar je postal bistven v družbeni zgradbi v modernem svetu. Ljudje z dogovori in navadami sprejemajo svoje mesto znotraj hierarhije ali se naučijo videti sebe v primerjavi s statusom drugih. Kaj se zgodi, ko se podrejo tradicionalne vrste oblasti in odnosov, da jih zamenjajo birokratska pravila in organizacijske prakse? S časoma so sprejete, čeprav so zdaj veliko bolj spremenljive (Lyo, 2000: 9).*

Kot pravi Lyon (2000: 9-10), so računalniško podprti sistemi klasificiranja za klasificiranje so postali samoumeven del infrastrukture, ki jo imenujemo informacijska družba. Nadzor je tu neskončen sistem v katerem se zbirajo in obdelujejo podatki za razne namene, od policijskih do varnostnih namenov ter do potrošnje in zabave. (Lyon 2000: 10).

Moderna tehnologija pa poleg klasičnega nadzora, to je nadzora, ki ga vršijo organizacije nad posameznikom, omogoča tudi tako imenovani sousveillance[15] oz. nadzora od spodaj. Posameznik je v tem primeru tisti, ki nadzira organizacijo. Primer tega je zloglasni primer, ko je prebivalec Los Angelesa posnel policijo, ki je pretepla taksista Rodneya Kinga[16] (glej Mann in ostali 2003: 331-334). Sousveillance je v dojemanje dogajanja s posameznikove perspektive oz. osebna izkušnja. Je obrnjen nadzor. Če na sousveillance gledamo s pravnega, etičnega ali policijskega vidika, ga lahko razložimo na primeru snemanja telefonskega klica. Če bi snemal klic eden od udeležencev pogovora, bi bil to sousveillance. V primeru, da pa bi ga snemal nekdo, ki ne bi bil del pogovora, bi bil to nadzor (ang. surveillance).

Digitalizacija kot vidimo, prinese mnoge spremembe v načinu nadzora. Nadzor je postal avtomatičen in neopazen, čeprav nas spremlja na vsakem koraku. Če so se prej podatki o posamezniku zbirali in hranili na enem mestu, se zdaj lahko zbirajo kjerkoli in hranijo na enem mestu. Tako sta njihova obvladovanje in analiza lažja. Poleg tega, da iste tehnologije dajo moč oblasti, jo dobijo tudi posamezniki, tako da nadzirajo oblast in njene organe.

[15] iz francoščine, sous(spodaj)
[16] Posnetek je povzročil v Zda razpravo o brutalnosti in rasizmu v policiji.

2. 3 Zasebnost, s poudarkom na osebnih podatkih

Uporaba novih tehnologij za nadzorovanje vpliva na dosti aspektov našega življenja. Predvsem se izpostavi vprašanje zasebnosti posameznika in kako se posameznik spoprijema s povečano močjo nadzora. Sicer je razprava glede zasebnosti in tehnologije že razmeroma stara. Začelo se je člankom iz leta 1890, v katerem Samuel Warren in Luis D. Brandeis razpravljata o novih izumih in popularnem tisku. Ta novi izum je bilo takojšnje razvijanje fotografij in njihova objava v časopisih. Označila sta ga kot »vdor v sveto območje zasebnega in domačega življenja. (Radwanski 2001).

Nadzor je po Dotyu v glavnem povezan s politično in ekonomsko močjo; problem zasebnosti je poudarjen prav v povezavi z njima (Kim 2004: 197).

Turn naslednjo definicijo zasebnosti: »pravica posameznika do zbiranja, shranjevanja, obdelave, širjenja in uporabe svojih osebnih podatkov« (Kim 2004:197). Posameznik mora namreč določene podatke posredovati, da je deležen določenih storitev in ugodnosti. Družba pa mu mora jamčiti, da podatkov ne bo uporabila v napačne in nebistvene namene (Kim 2004:197). Doty pravi, da se moramo izogniti klasični delitvi javno/zasebno, saj zasebnost ne gradi in oblikuje na enostavnem atomističnem individualizmu, ampak na človeški interakciji (Kim 2004:197).

Vseeno pa se vprašamo zakaj je potrebno zasebne podatke varovati. Sookman omeni primer na kanadskem sodišču iz leta 1988, kjer so zaključili, da ideja o zasebnosti (podatkov) izhaja iz predpostavke, da so vse informacije o posamezniku v bistvu njegove. Posameznik se sam odloči, kako bo z informacijami o sebi razpolagal in komu jih bo posredoval (2001). Brez zasebnosti ni prave svobode. Kot pravi Radwanski: »Zasebnost je tista pravica iz katere izhajajo ostale, kot so svoboda govora, svoboda združevanja, svoboda izbire, torej vse svoboščine, ki jih imamo« (2001: 5). Zasebnost je »bistvo svoboščin v moderni državi« in je zasnovana na »dostojanstvu in integriteti posameznika« (Sookman 2001).

2. 3. 1 Osebni podatki

Ko brskamo po internetu nas večkrat, če skušamo ustvariti račun za kakšno storitev vprašajo za osebne podatke. Podjetja pa se ponavadi zavežejo da bodo podatke varovala in jih bodo uporabljala le za lastno evidenco. Kateri pa so podatki, ki so zaščiteni.

Kanadska zakonodaja našteje naslednje osebne podatke, ki so zaščiteni:

- ime, starost, teža, višina,
- zdravstvene kartoteke,
- dohodki, nakupi in nakupovalne navade,
- rasa, etnična skupina in barva kože,
- krvni tip, DNK, prstni odtisi,
- zakonski stan in vera,
- izobrazba,
- domači naslov in telefonska številka (Sookman 2001).

V Sloveniji za varstvo osebnih podatkov skrbi Zakon o varstvu osebnih podatkov, ki :

> *...načelno določa, da je varstvo osebnih podatkov namenjeno preprečevanju nezakonitih in neupravičenih posegov v informacijsko zasebnost posameznika na vseh relevantnih področjih. Določa tudi, da je na ozemlju Republike Slovenije vsakemu posamezniku, ne glede na državljanstvo in prebivališče, zagotovljeno varstvo osebnih podatkov. Smisel varstva osebnih podatkov torej ni varovanje osebnih podatkov kot takih, temveč varovanje pravic posameznika, na katerega se podatki nanašajo (http://www.ip-rs.si).*

Nadalje je v zakonu opredeljeno, kdaj se lahko podatki uporabljajo in kdo jih lahko uporablja:

> *Osebni podatki se lahko obdelujejo le, če je njihova obdelava določena z zakonom, ali če ima upravljavec zbirke podatkov pisno privolitev posameznika. Za pravne ali fizične osebe, ki opravljajo javno službo ali dejavnost po zakonu, ki ureja gospodarske družbe, pa velja, da lahko že neposredno na podlagi tega zakona,*

torej brez izrecne podlage v nekem drugem zakonu ali pisne privolitve posameznika, obdelujejo osebne podatke oseb, s katerimi so v pogodbenem razmerju, vendar le, če gre za osebne podatke, ki jih potrebujejo za izpolnjevanje pogodbenih obveznosti ali uveljavljanje pravic iz pogodbenega razmerja. Za državne organe, organe lokalnih skupnosti in nosilce javnih pooblastil je ureditev drugačna, saj lahko obdelujejo le tiste osebne podatke, za katere je tako določeno z zakonom. Posameznik, čigar osebni podatki se obdelujejo na podlagi njegove pisne privolitve, mora biti predhodno pisno seznanjen z namenom obdelave podatkov, njihove uporabe in časom shranjevanja (http://www.ip-rs.si).

V zakonu so predpisane tudi pravice, ki jih ima posameznik. Tako mora upravljavec baze podatkov omogočiti posamezniku vpogled v katalog zbirke osebnih podatkov. Potrditi, ali se podatki v zvezi z njim obdelujejo ali ne, in mu omogočiti vpogled v osebne podatke, ki so vsebovani v zbirki osebnih podatkov in se nanašajo nanj, ter njihovo prepisovanje ali kopiranje; posredovati izpis osebnih podatkov, ki so vsebovani v zbirki osebnih podatkov in se nanašajo nanj; posredovati seznam uporabnikov, katerim so bili posredovani osebni podatki, kdaj, na kakšni podlagi in za kakšen namen; dati informacijo o virih, na katerih temeljijo zapisi, ki jih o posamezniku vsebuje zbirka osebnih podatkov, in o metodi obdelave; dati informacije o namenu obdelave in vrsti osebnih podatkov, ki se obdelujejo, ter vsa potrebna pojasnila v zvezi s tem; pojasniti tehnične oziroma logično-tehnične postopke odločanja, če izvaja avtomatizirano odločanje z obdelavo osebnih podatkov posameznika (http://www.ip-rs.si). Več lahko vidimo v zbirki desetih Splošno sprejetih principov o zasebnosti[17] (glej prilogo A).

Če primerjamo slovensko zakonodajo s kanadsko, lahko vidimo, da se v bistvu prekrivata. V Sloveniji med varovane podatke spada EMŠO, ki predstavlja datum rojstva, starost in spol. Davčna številka določi posameznika s tem, da se povezuje z vsemi davki tega posameznika. Domača telefonska številka in tudi IP naslov, ki je dandanes v bistvu virtualni naslov posameznika. Plače so razen plač uradnih uslužbencev tajnost. Prav tako spadajo zdravstveni podatki med občutljive osebne podatke in je njihova obdelava možna samo pri določenih primerih (glej prilogo B).

Prav tako so zaščiteni podatki etažnih lastnikov, biometrični podatki ter tudi podatki o umrlih (www.ip-rs.si).

[17] ang. Generally Accepted Privacy Principles

Kot vidimo so to podatki, ki jih neprestano posredujemo. Pa naj bo to na internetu, ali pri pridobivanju kartice popustov v trgovini, ali odpiranju bančnega računa. Za primer, bančni računi so danes nujnost, ne moremo si privoščiti, da bi zaradi strahu pred izdajo osebnih podatkov ostali brez računa. Ko podjetje podatke dobi še ne pomeni, da lahko z njimi razpolaga po mili volji. Tu nastopi zakonodaja. Naloga zakonodaje je, da omejuje razpolaganje s podatki (Radwanski 2001).

Evropska Unija je izdala direktivo o varovanju podatkov (Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov), ki je vodilo zakonom v državah članicah. V njej lahko ločimo tri kategorije principov, kako naj države članice oblikujejo zakone o varstvu podatkov:

1. Prva kategorija se nanaša na dovoljenja kako bodo podatki procesirani in temeljijo na ideji da mora biti obdelava podatkov podprta z zakonom in poštena.
2. Druga kategorija zadeva kvaliteto podatkov, podatki morajo biti točni, popolni in sveži (posodobljeni)
3. Tretji princip zadeva pravice posameznikov; posameznik mora imeti pravico, da ve kateri podatki se zbirajo o njem, da lahko do njih svobodno dostopa in jih spreminja (Dubbeld 2005: 550-551).

2 .3. 2 Uporaba osebnih podatkov

Varnost osebnih podatkov odvisna od države, kjer smo, oziroma od države, kjer je postavljen strežnik oz. sedež podjetja, ki mu posredujemo podatke. Ta aspekt pomemben zato, ker opravljamo danes dosti storitev na svetovni ravni. Od elektronske pošte na tujih strežnikih do nakupov v spletnih trgovinah. Največja nevarnost, ki nastopi je posredovanje podatkov tretjim osebam oziroma podjetjem. Obstajajo podjetja, ki se ukvarjajo z zbiranjem in posredovanjem podatkov. Razvoj pa prinaša nove skrbi in nove tehnologije, sledilne naprave, brezžični prenos podatkov, biometrija ipd. Po 11. septembru 2001, se je začelo neselektivno zbiranje podatkov o vseh, ki stopijo na ozemlje Združenih držav Amerike, po vsem svetu se zaradi strahu pred podobnimi dogodki zasebnost posameznikov omejuje na račun večje varnosti.

Na tem mestu bi spomnil na misel Benjamina Franklina: »Vsaka družba, ki se bi odrekla malo svobode, da bi pridobila malo varnosti, si ne zasluži nobene in bo izgubila obe« (po Civilization 4 2006).

Osebni podatki so zelo pomembni, ker nas določajo. Zloraba naših podatkov ni le naš problem ampak je to družbeni problem, saj to povzroča dvom v sistem in njegove dele.

2. 4 Podatkovni nadzor

Roger A. Clarke je podatkovni nadzor[18] definiral, kot » sistemsko uporabo osebnih podatkovnih sistemov za raziskovanje in nadziranje ene ali več oseb« (Elmer 2003: 236). Podatkovni nadzor se od konvencionalnega elektronskega nadzora razlikuje po tem, da ne nadzira posameznika in njegovih dejanj, ampak podatke o njem (Kim 2004: 199).

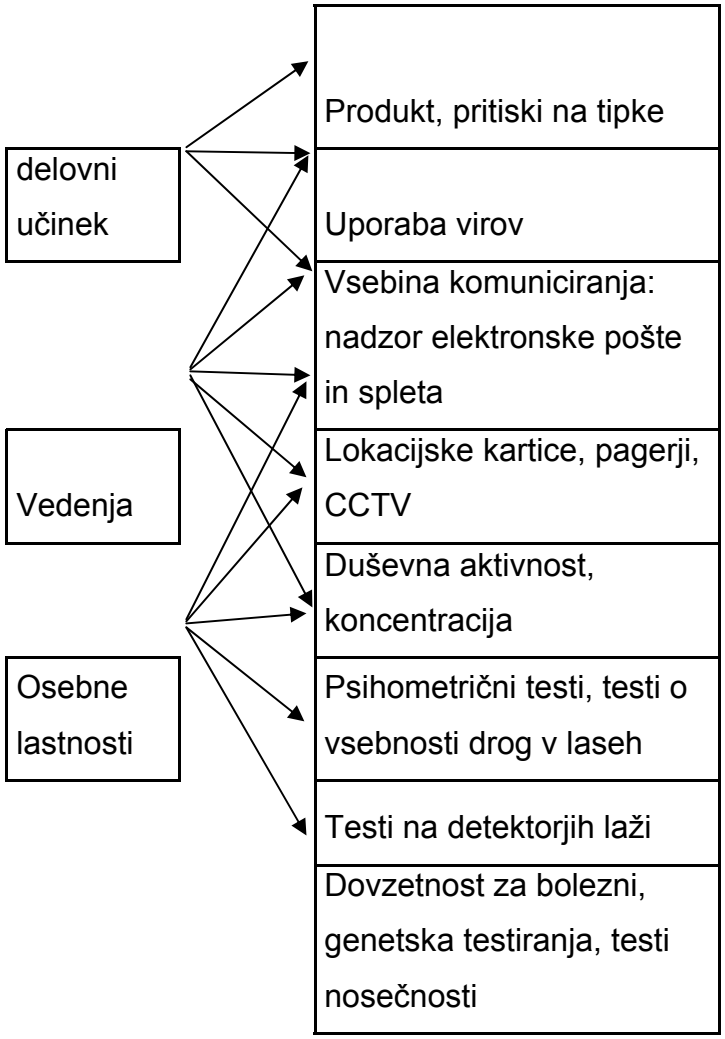
> *V primerjavi s konvencionalnim fizičnim ali elektronski nadzorovanjem je podatkovni nadzor poceni in postaja vedno cenejši zahvaljujoč razvoju IT[19]. Dalje podatkovni nadzor je priljubljen zaradi neomejenih načinov uporabe, ko so surovi podatki zbrani. …(rast uporabe)[20] je rezultat trenutnega stanja »informacijske poplave«. Do zdaj so bili pod podatkovnim nadzorom samo določeni deli populacije, vendar ne zaradi pomanjkljivosti tehnologije ampak zaradi pomanjkanja bistvenih podatkov* (Kim 2004: 199–200).

Konvergenca tehnoloških sistemov in posledična prisotnost nadzornih tehnik in tehnologij v družbi, so napeljali Lyona, da govori o t. i. »puščajočih posodah[21]«. Ta metafora se nanaša na omrežne tehnologije in ničnosti varovanja podatkovnih baz ter potrošnikove zasebnosti (Elmer 2003: 237).

Podatkovni nadzor pa ni namenjen samo nadzoru potrošnikov ampak tudi za nadzor zaposlenih, osumljencev, državljanov,… Z uporabo biometričnih podatkov postane tak nadzor še posebej učinkovit. Tako je nadzor zaposlenih v neki organizaciji predvsem odvisen od njegove učinkovitosti, ki jo nadzira računalnik[22]. Ballova po Reaganovi povzame naslednjo shemo (Ball 2005: 91):

[18] Ang. *dataveillance*
[19] informacijska tehnologija
[20] dodal Debelak
[21] ang. leaky container
[22] monitoring

Shema 2. 4. 1: Tehnike nadzora zaposlenih



(Vir: Reagan po Ball 2005:91)

Zbiranje zasebnih podatkov je povezano s skladiščenjem in križnim nanašanjem[23] z drugimi podatki. Tu gre predvsem za podatke o prodaji, inventarju in distribuciji (Elmer 2003: 237). Vprašanje je kako prepričati posameznika, da posreduje podatke. Elmer da za primer kartice popustov, ki imajo dvojno vlogo, če posameznik izpolni podatke dobi nagrado v obliki popusta, če jih ne ga čaka kazen, občutno višje cene (2003: 237). Po drugi strani pa je oddaja podatkov za nacionalne osebne izkaznice obvezna. Nove tehnologije omogočajo samodejno zapisovanje in obdelavo podatkov.

[23] cross-referencing, ang.

Tako se postavi vprašanje ali posamezniki še imajo možnost, da odločajo katere podatke bodo posredovali.

Še pomembnejše od kartic popustov so kreditne kartice, ki so v današnjem času nuja. Plačevanje z odlogom je za mnoge edini način s katerim se lahko prebijajo skozi življenje. Dostikrat je plačevanje s kreditnimi karticami tudi edini možni način plačevanje, npr. spletni nakupi oz. plačevanje spletnih storitev. Kreditna kartica je odraz potrošniške družbe v kateri živimo. Da pa ta sistem kreditiranja lahko nemoteno deluje so potrebne ogromne baze podatkov in tudi njihovo medsebojno nanašanje. Tako obstajajo podjetja specializirana za zbiranje podatkov o bančnem stanju in kreditnih zmožnostih posameznikov. Na podlagi le teh točkujejo, točke prodajo ponudnikom kreditnih kartic ti pa na podlagi točk določijo obresti in ali je posameznik sploh zmožen plačevanja svoje kreditne kartice (Rummel in Kheyfets 2006). Tako se z zbiranjem podatkov in matematično formulo lahko razdeli ljudi na skupine. Na tej stopnji poteka mehanska diferenciacija in mnogokrat tudi diskriminacija ljudi.

Podatki o nas se zbirajo tudi ko brskamo po internetu. Strežniki hranijo naše IP naslove, elektronske naslove, naše brskalne navade ter s tem omogočajo personalizacijo strani, hkrati pa kopičijo podatke o nas.

Lahko rečemo, da nas v življenju ne predstavlja več naša fizična podoba ampak podatki o nas. Vse upravne, bančne in ostale storitve temeljijo na podatkih o nas. Na podatkih, ki smo jih oddali prostovoljno in podatkih, ki so bili zbrani brez naše vednosti ali posredno.

3. Digitalni nadzor v praksi

To poglavje se ukvarja s praktičnimi primeri modernih oblik nadzora. Poskušalo bo opisati okoliščine, ki omogočijo razvoj in uporabo nadzora, in vpliv na nadzorovane. Najprej bo analiziran video nadzor, ki je še najbolj podoben klasični predstavi panoptikona. Digitalizacija omogoči razne nove rešitve, kot so prepoznavanje obrazov, gibanja in drže. Drugi primer bo analiza podatkovnega nadzora na pametnih osebnih izkaznicah. Pametne osebne izkaznice bodo vsebovale podatke o posamezniku, tudi npr. prstne odtise. Naslednji bo nadzor informacij in komunikacij. Tehnološke rešitve, kot je mobilni telefon, omogočajo poleg prisluškovanja pogovorom tudi sledenje dejavnosti in gibanja (lociranje) lastnika. Analiza komunikacij na internetu je še posebej enostavna, avtomatizirani programi tako sami iščejo določene besede ipd. Mednarodni kriminal, ilegalni prebežniki in seveda terorizem so velik problem, zato bo sledila analiza nadzora mej in transporta.

3. 1 Video nadzorni sistemi

Modernih mest si dandanes ne moremo zamišljati brez vseh mogočih nadzornih sistemov. Nadzora trgovskih centrov, poslovnih stavb, javnih prostorov, ulic in tudi zasebnih posestev in prostorov, si danes ne moremo več predstavljati brez nadzornih kamer. Če je bil za elektromehanski nadzor značilen predvsem pasiven nadzor, je digitalizacija z avtomatizacijo prinesla, da so nadzorni sistemi postali aktivni. Kamera povezana z računalnikom omogoča, da se sistem samodejno odzove na vsako nepravilnost.

Navadna spletna kamera povezana z osebnim računalnikom lahko postane močno orodje nadzorovalca. T.i. spycams[24], so postavljene na mestih, kjer jih ne pričakujemo, od oblačilnic, kopalnic do spalnic. V veliki večini primerov gre tu za namerni vdor v zasebnost posameznikov in tudi nadzora ne vršijo organizacije ampak drugi posamezniki. V nekaterih primerih lahko govorimo, da gre za sousveillance,

[24] vuhunske kamere

večino pa jih lahko umestimo med klasičen nadzor. Tak je npr. nadzor varušk ali delavcev.

Kot se vidi v številu spletnih kamer, tako javnih kot zasebnih, lahko recipročno opazimo željo po vidnosti. Čeprav velja biti pod nadzorom za neprostovoljno dejanje, lahko opazimo, da si mnogi želijo biti videni. Vizualne reprezentacije so pogosto povezane s spolnostjo.

Z video nadzorom je lahko povezanih veliko sistemov za razvrščanje in analizo. Van der Ploeg izpostavi dva, prepoznavanje obrazov in gibanja. Obe sta biometrični tehniki, ki temeljita na prepoznavanju telesnih karakteristik in sledov, ki jih telo pušča (Graham in Wood 2003: 235).

3. 3. 1 Tipi digitalnega video nadzora

1.) Sistem za prepoznavanje obrazov so v Veliki Britaniji začeli uporabljati v treh velikih mestih: Londonu, Birminghamu in Manchestru. Zasnovan je tako da primerja obraze ljudi na ulici z obrazi znanih prestopnikov v bazi podatkov. Za prepoznavanje uporablja sistem imenovan FaceIt, ki na podlagi več algoritmov ustvari »obrazni odtis[25]«. Ta naj bi bil specifičen za vsakega posameznika. Izdelovalci programa pravijo, da program določi bistvene oblike in poteze obraza ter loči posameznika med milijoni (Graham in Wood 2003: 235–236). Podobno storitev ponujajo tudi na internetni strani[26], ki ponuja na podlagi poslane slike prepozna sliko posameznika v svoji bazi. Program je trenutno še v demo fazi in primerja obraz le z znanimi osebnostmi in izračuna podobnost z njimi.

Kot lahko vidimo, je potreben za prepoznavanje obraza že zapisan »odtis«. Vendar pa je v primerjavi z ostalimi biometričnimi identifikacijskimi znaki, kot je npr. prstni odtis, pri obrazu drugače (glej Introna in Wood 2004: 178). Vsaka identifikacijska kartica, za katero zaprosimo, vsebuje ponavadi tudi našo sliko. Obraz je tisti, na podlagi katerega se ljudje ločujemo med sabo. V zahodnih družbah zakrivanje obraza avtomatsko postane sum za krivdo (Introna in Wood 2004: 178). Problem nastane, ko postane obraz kodiran v računalniško kodo. Digitalni zapis ima to lastnost,

[25] ang. faceprint
[26] www.myheritage.com (december 2006)

da ga kljub sprva benignim načinom uporabe, kot je npr. lajšanje storitev v državni upravi za občane, lahko hitro prilagodimo še v druge namene.

Vendar pa tehnologija za prepoznavanje obrazov še potrebuje čas za razvoj. Ameriška unija državljanskih svoboščin tako obvešča, da imajo programi za prepoznavanje obrazov veliko težav, ob spremembi barve las, brade, brkov, staranju, izgubi ali pridobitvi teže in tudi pri enostavnem maskiranju. Veliko je napak tudi pri idealnih pogojih, kjer posameznik gleda neposredno v kamero pri dobri osvetlitvi (Gray 2003: 316).

2.) Drugo pomembno področje biometričnega nadzora je nadzor gibanja. Ti sistemi so relativno enostavni in temeljijo delčkih barve, ki ostajajo konstantni v vzorčnih okvirjev CCTV slike. Takšni sistemi se uporabljajo za upravljanje množic, vendar je sistem postal zanimiv zaradi možnosti za zmanjšanje samomorov na londonski podzemni železnici. Samomorilci imajo namreč »navado, da čakajo do deset minut na peronu in izpuščajo mimo vozeče vlake, preden se odločijo za zadnji korak« (Graham-Rowe v Graham in Wood 2003: 236).

3.) Še zanimivejši je sistem za prepoznavanje drže. Ta pomeni oživitev viktorijanskih načel, da lahko človeku glede na vizualne karakteristike določimo kriminalno vedenje. Vendar zaradi publicitete projekt ni napredoval do uporabe v komericalne namene (Graham in Wood 2003: 236).

4.) Tako imenovani H-sistem, ki ga imajo na Japonskem, za nadzor prometa, ki beleži podatke o avtomobilih, ki vozijo mimo. Njegova naloga je, da primerja številke na registrskih tablicah s podatki o ukradenih avtomobilih. Vendar pa lahko policija z njim učinkovito spremlja naše vsakodnevno gibanje (Abe 2004: 220). Podobni so tudi avtomatski sistemi za merjenje hitrosti na naših cestah ter uporaba kamer na semaforjih v mestih, kamer na avtocestah in na kritičnih odsekih cest. Čeprav so vse te instalacije namenjene predvsem nadzoru prometa, pa jih lahko uporabimo tudi za nadzor gibanja posameznikov ali skupin.

3. 3. 2 Zanesljivost video nadzornih sistemov

Zanesljivost video nadzornih sistemov je vprašljiva. FaceIt, program za prepoznavanje obrazov, je npr. samo 53% učinkovit v kontroliranem okolju[27], medtem ko za nadzor na ulicah ni dokazano, da je učinkovit. Hkrati pa Lianos in Douglas poudarita problem povečevanja diskriminacije določenih sosesk in skupin ljudi (Graham in Wood 2003: 237). V Lyonu, v Franciji so tako namestili kamere v predelu mesta, za katerega je značilno nasilje in visoka stopnja kriminala. Vendar pa kamer niso namestili v kritične predele, ampak v prestižne ulice. V tem primeru je postala pravica do življenja in lastnine sekundarnega pomena. Primaren je bil interes trgovcev, ki ga je legitimirala mestna oblast (Martinais in Betin 2004: 365).

Sistem za prepoznavanje obrazov so namestili na dveh mednarodnih letališčih na Japonskem, Narita in Kansai. Nikjer ni bilo znaka, ki opozoril, da poteka te vrste nadzor. Kljub temu niso z njegovo pomočjo, do konca leta 2002, ujeli nobenega zločinca (Abe 2004: 226). Problematično pri tem je, da je bil vpeljan brez podpore javnosti (Abe 2004: 221) in možne škode, ki bi lahko nastala ob morebitni zlorabi podatkov.

Video nadzor je še najbližji Benthamovemu panoptikonu. Kamera je oko nadzorovalca, dokler je kamera samo elektronski vmesnik med človekom in nadzorovanim okoljem ima vse hibe in prednosti neposrednega nadzora. Ko pa se priklopi na računalnik, postanejo algoritmi tisti, ki vršijo nadzor. Nadzor postane stalen. Kamere na določenih mestih tako neposredno vplivajo na naše pravice in svoboščine. Tako kamera v predavalnici vpliva na akademsko svobodo ipd.

[27] letališča

3. 2 Podatkovni nadzor, identifikacijske kartice

Podatkovni nadzor je ena najpogostejših oblik nadzora danes in tudi ena najbolj problematičnih. Podatki o nas se zbirajo vsepovsod, dostikrat niti ne vemo zakaj bodo ti podatki uporabljeni. Tega načina se ljudje tudi najmanj zavedamo, hkrati pa se ne zavedamo niti posledic, ki jih podatkovni nadzor prinaša. Kot eden primerov primerov podatkovnega nadzora so pametne identifikacijske kartice. Identifikacijske kartice (osebne izkaznice) so, po definiciji, oznake članstva; nacionalna identifikacijska izkaznica kažejo, da so njihovi lastniki v državi legalno in imajo pravico do dela, do zdravstvene oskrbe, izobrazbe in ostalih ugodnosti (Lyon 2004: 3).

3. 2. 1 Digitalna osebna izkaznica v Južni Koreji

Kim obravnava južnokorejski načrt za vpeljavo nove digitalne osebne izkaznice. Kartica naj bi vsebovala 42 podatkov iz šestih baz podatkov. Baze, ki bi jih uporabljala, so osebni podatki, vozniško dovoljenje, zdravstveno zavarovanje, državna pokojnina, prstni odtisi in ostalo (posebne opombe zdravstvenega zavarovanja). Zasnovana je bila kot kartica s čipom, z veliko kapaciteto, in enostavna za povezljivost z ostalimi bazami podatkov. Država je kot njeno prednost poudarjala to, da je najnaprednejša osebna izkaznica na svetu (Kim 2004: 206). Ker sprva ni bilo nobene reakcije javnosti, so strokovnjaki ugotovili, da je to zaradi: 1.) močne tehnološke in industrijske podpore politiki elektronske kartice, 2.) pomanjkanja skrbi glede zasebnosti, zaradi kolektivistične tradicije, 3.) skrbi za državno varnost zaradi neurejenih odnosov s Severno Korejo 4.) zanemarjanja socialnih pravic na račun povečane ekonomske konkurenčnosti, 5.) brezbrižnosti, zaradi običajnih političnih praks (vse odločitve prihajajo z vrha) (Kim 2004: 206–207).

Kljub vsemu se je upor proti uvedbi kartice začel, ko so se ljudje zavedli negativnih posledic. Zmanjšanje stroškov, administracijska učinkovitost in boljše socialne storitve so bili argumenti zagovornikov, ki pa so jih premagali naslednji argumenti nasprotnikov: vdor v zasebnost, zloraba osebnih podatkov in zanemarjanje človekovih pravic. Nasprotniki so prihajali iz različnih sektorjev družbe, od sindikalnih,

profesionalnih, verskih skupnosti do raznih političnih združenj. Vlada je program zaradi nasprotovanj nato ukinila (Kim 2004: 207).

3. 2. 2 Zdravstvene baze podatkov

Drugi primer podatkovnega nadzora so baze v zdravstvenem sistemu. Tu se zaradi lažjega in hitrejšega zdravljenja podatki kopičijo. Pojavljajo se želje, da bi se zdravstvene baze povezale s policijskimi. Rose pravi, da bi tako postalo delo forenzikov, zaradi vedno večje uporabe DNK analiz, lažje in hitrejše (Graham in Wood 2003: 241). Vendar pa glavne težave ne predstavljajo državne službe, ampak, kot pravita Graham in Marvin, zasebni sektor, ki ima vedno večji vpliv medicinski oskrbi. Zavarovalnice bi tako, če bi dobile genetske podatke o rizičnih posameznikih, lahko povišale premijo ali celo zavrnile zavarovanje (Graham in Wood 2003: 241–242).

3. 2. 3 Velika Britanija kot država baz podatkov

Osebna izkaznica se nam zdi samoumevna, vendar ni vsepovsod tako. Kot zanimivost lahko omenimo, da so prve osebne izkaznice, ki so vsebovale tudi fotografijo, prstni odtis in lastnoročni podpis osebe, uvedli na Nizozemskem med nacistično okupacijo, na njih pa je bilo označeno, ali je ta oseba Jud ali ne. Ta na videz nedolžna uvedba nove tehnološke rešitve v vsakdanje življenje je v tistem času pravzaprav pomenila prvi korak do izvedbe holokavsta v tej deželi, saj so identifikaciji sledile deportacije. V Veliki Britaniji so leta 2003 predstavili shemo za uveljavitev obvezne osebne izkaznice na državni ravni (glej tudi Lyon 2004). Kmalu oziroma hkrati s predstavitvijo se je začela tudi NO2ID kampanja, to je organizacija, ki se trudi preprečiti vpeljavo osebnih izkaznic. Njihovo temeljno vodilo je, da ustavijo osebne izkaznice in državo baz podatkov (ang. Database state).

Država baz podatkov je stremljenje k uporabi računalnikov za upravljanje družbe tako, da nadzira ljudi (www.no2id.net). Problem britanske nacionalne sheme je, da bi se vse baze med sabo povezale v Nacionalne osebnem registru (National Identity Register, NIR). Številka NIR bi omogočala vpogled v posameznikovo življenje. Ker bi

bili podatki med sabo povezani, bi lahko informacija, ki jo bi posredovali neki uradni osebi postala dostopna v celotnem sistemu (www.no2id.net).

Planirani sistem vsebuje naslednje:

- biometrične potne liste, ki beležijo potovanja,
- centralizirano bazo zdravstvenih kartotek,
- biometrijo v šolah,
- identifikacijske centre,
- pobiranje prstnih odtisov v pubih,
- otroška baza podatkov,
- obcestno pobiranje prstnih odtisov, policisti bodo lahko preverjali identiteto posameznikov s prenosnimi čitalci prstnih odtisov,
- razširjenje urada zbiranje podatkov o kriminalnih dejanjih,
- snemanje vseh potovanj z avtom s pomočjo cestnega nadzornega sistema (www.no2id.net).

Kot lahko opazimo se s posameznimi deli predvidenega britanskega sistema lahko poistovetimo tudi v Slovenji. Tako se je tudi v Sloveniji začela izdaja biometričnih potnih listov.

Tehnologija, na kateri temeljijo biometrični potni listi RFID[28]. Med drugim se uporablja za registracijo prihoda v službo v nekaterih podjetjih, ABC sistem cestninjenja na slovenskih avtocestah odklepanje avtomobilov ipd. Tehnologija uporablja radijske valove za avtomatsko identifikacijo, shranjevanje in iskanje podatkov na daljavo. RFID čip je sestavljen iz silikonskega čipa in antene. Poznamo aktivne RFID oddajnike in pasivne, ki potrebno energijo za delovanje pridobijo z radijskimi valovi. Pasivni v zadnjem času postajajo nadomestilo za črtne kode, saj omogočajo hitrejšo obdelavo v skladiščih ter v trgovinah. Biometrični potni listi torej uporabljajo RFID tehnologijo, to pomeni da lahko podatke o nas dobijo še preden potegnemo potni list iz žepa. To lahko stori tudi oseba, ki za to no avtorizirana. Kot praktični primer lahko omenim kraje avtomobilov z RFID ključi. Tat prisluškuje frekvencam na katerih deluje ključ, kopira njegov signal in ga kasneje posreduje avtomobilu.

[28] ang. Radio frequency identification

Ker so elektronski podatki enostavno prenosljivi, lahko država ali kdorkoli enostavno spremlja in beleži naša potovanja zunaj države. Podobno bo tudi z nameravanim pobiranjem cestnin za avtoceste. Zaradi vzpostavitve tako imenovanega pravičnega sistema pobiranja cestnin, bo mogoč neprestan nadzor naše vožnje. Naprava za nadzor naše vožnje po avtocestah bo vsebovala GPS in GPRS/UMTS, ki bosta sistemu javila kdaj je naše vozilo prestopila virtualna vrata, ki jih bo določila Državna agencija ta avtoceste RS. Vrata bodo lahko poljubno prestavljali npr v primeru prekvalifikacije določenega dela ceste. Ker pa so vrata virtualna oziroma programsko ustvarjenja, ne predstavlja sistem nobene ovire, da ne bi nadzirali celotne naše poti.

V britanskih šolah se uveljavlja sistem pobiranja prstnih odtisov v šolah. Tako otroku ni treba imeti knjižnične izkaznice, vse kar rabi je prst ki ga potegne čez čitalec. K algoritmu ki predstavlja prstni odtis je ponavadi še priložena slika (www.leavethemkidsalone.com)

Slika 3. 2. 3. 1: »Poleg vloma dolguješ še £2.50 za tisto Noddyjevo knjigo«

(Vir: Colin Shelbourn 2006. Dostopno na www.no2id.net).

V angleških lokalih se vzpostavlja baza podatkov s katero se hočejo delavci v lokalih informirati o svojih strankah in lahko s tem predvidijo in nadzorujejo njihova dejanja. Sistem je zasnovan na pobiranju prstnih odtisov strank. V prihodnosti pa ga hočejo povezati z video nadzorom. Celotni sistem za zdaj deluje v Yeovilu pod okriljem lokalnih oblasti, vendar je zanimanje zanj tudi v večjih mestih (Ballard 2006).

Zanimiva je tudi otroška baza podatkov. V njej bodo zbrani podatki o otrocih. Predviden začetek obratovanja baze je v letu 2008. Vsebovala bo naslednje podatke:

- otrokovo ime, spol, datum rojstva in naslov,
- identifikacijsko številko otroka,
- imena in naslove staršev oziroma skrbnikov,
- podatke o otrokovem zdravniku, patronažni sestri ipd.,
- podatke o šolah (oziroma izobrazbi, ki jo pridobivajo, če niso v šoli),
- podatki o storitvah, ki ji otrok uporablja ter datum začetka in konca storitve (http://www.arch-ed.org).

Podatke bodo zbirali tako, da jih bo vpisal vsak, ki je imel uradno opravka z otrokom. To so šole, zdravniki, svetovalci, policija in drugi. Kljub temu, da imajo organizacije že svoje baze podatkov ta nova pomeni združitev vse, čeprav naj bi vsebovala le osnovne podatke (http://www.arch-ed.org).

Vse te baze bodo znotraj skupnega sistema, ki ga bo nadzoroval Državni osebni register. Podatke, kot so prstni odtisi, nameravajo zbirati v Identifikacijskih centrih. Vsaka oseba stara nad 16 let bo, ko bo zaprosila za svoj odrasli potni list morala v takšen center, kjer jo bodo preverili. Primerjali njeno zgodbo z uradnimi podatki, jo fotografirali in vzeli prstne odtise (NO2ID 2006).

3. 2. 4 Učinki novih oblik nadzora

Na moderno (informacijsko) družbo z različnih kotov lahko opazimo tri sodobne tipe odziva na nadzor, ki jih Kim zazna, pri poskusu vpeljave digitalne osebne izkaznice v Južni Koreji (Tabela 1) (Kim 2004: 209). Tabela predstavi diskurz, ki se pojavi, ko govorimo o raznih odzivih, ko razpravljamo o nadzoru. Med razpravo, o vpeljavi digitalnih osebnih izkaznic, je javnost najprej, kljub *koristim*, zmotila možnost vdora v zasebnost, ki bi postala možna z nelegitimno uporabo osebnih podatkov. Tu se postavi udobje nasproti tveganju. Želja po *varovanju* zasebnosti je večja od javne blaginje, ki jo utegne prinesti nova kartica. Zakonodajni del razprave v razpravi niso posebej

izpostavljali, kljub temu, da ta zadeva kontrolni odzivni okvir, t.j. na diskurz med avtonomno in avtoritarno (ang. coercive) podobo družbe, oz. med notranjo in zunanjo kontrolo.

Tabela 3. 2. 4. 1: Odzivni okvir in diskurz v razpravi pri vpeljavi digitalne osebne izkaznice

Odzivni okvir	**Diskurz**
Koristi	Udobje proti tveganju
Varovanje	Javna blaginja proti zasebnosti
Kontrola	Notranja proti zunanji kontroli

(Vir: Kim 2004:209)

Na vprašanje kdo pridobi z uvajanjem takšnih osebnih izkaznic, na NO2ID (2006) odgovarjajo:

> *Oblast. Vse oblasti, vseh prepričanj, v vseh državah neprestano iščejo način za povečanje moči in nadzora – pogosto zaradi čisto nenevarnih razlogov, pogosto pa tudi ne.*
>
> *Velika podjetja. Ona hrepenijo po tem, da bi bili vsi njihovi porabniki »prijavljeni«, zapisani in klasificirani glede na demografski in potrošniški profil.*

Zagovorniki takšnega načina nadzora se izgovarjajo na to, če nimaš ničesar za skriti se ti ni treba ničesar bati.

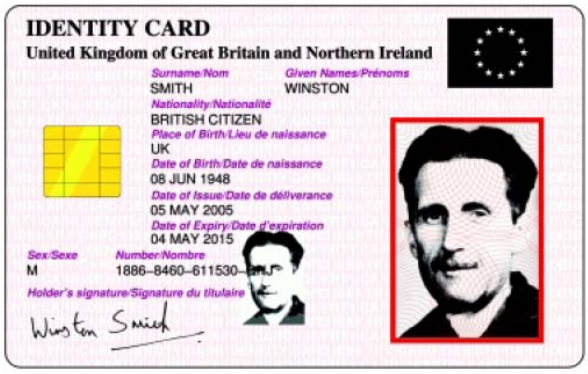
> *Dober način za grafično predstavitev slabosti tega argumenta je nasprotni primer: »Torej ne boste nasprotovali kameri v vsaki sobi v vaši hiši, vključno s spalnico in bo povezana neposredno na policijsko nadzorno postajo? Namreč veliko kriminala se dogaja za zaprtimi vrati. Izkoriščanje otrok, priprava kriminalnih dejanj, tatovi si delijo plen, preprodajalci drog idr. Policija bi na tak način lahko preprečila mnogo kriminala na tak način… (NO2ID 2006)*

Temu dodajo še bolj realističen odgovor, s katerim hočejo razložiti nesmotrnost uporabe osebnih izkaznic. Osebne kartice bodo namreč kriminalizirale na tisoče navadnih ljudi. Zakon pa tudi vzpostavi veliko število novih kriminalnih dejanj in kazni s katerimi bi zagotovili da se bi ljudje podredili. Tako bodo velike kazni prisilile ljudi,

da bodo sproti sporočale spremembe podatkov in vedno nosile s sabo osebno izkaznice. Kazen za neplačanje kazni je dve leti zapora.

Tisto kar dela osebno kartico drugačno od na primer kreditnih kartic je to, da so zadnje prostovoljne, prve pa obvezne. Poleg tega pa bodo imele osebne izkaznice za sabo veliko bazo podatkov v kateri bodo zbrani vsi naši podatki.

Slika 3. 2. 4. 1: Primer osebne izkaznice z ironično ponazoritvijo Orwellovega Winstona Smitha



(Vir: NO2ID 2006).

Kljub vsemu pa lahko dvomimo, da bodo kartice res omogočile zmanjšanje kriminala. Kartice vsemu zasnovane na čipu in programski opremi, ki jo je mogoče spremeniti. Tako bodo kriminalci, kot vedno našli način, da bodo obšli varnostne parametre. Prav tako ne bo to ustavilo teroristov. Dostikrat se zgodi, da so teroristi tudi prebivalci države v kateri dejanje storijo (bombni napad v Oklahoma Cityu, snovalci napada na podzemno železnico v Londonu…) (NO2ID 2006). Po drugi strani pa je problematičen neposredni dostop do vseh podatkov na enem mestu. Policija lahko brez potrebnega naloga izve vse o posamezniku. Tudi stvari, ki v raziskavi niso pomembne.

3. 3 Nadzor informacij in komunikacij

Nove tehnologije so prinesle tudi nove storitve. Nadzor informacij in komunikacij je v glavnem namenjen boljši pretočnosti in boljši kvaliteti storitev. Algoritmi skrbijo, da so storitve dodeljene različnim uporabnikom na različnih ravneh (Graham in Wood 2003: 237).

Pri vsem tem ne gre za tehnologije specializirane za nadzor, ampak za takšne, ki so v redni uporabi ali pa kmalu bodo. Prikaz številke kličočega je eden takšnih primerov. K nam je prišel z uvedbo GSM in ISDN telefonije. Z uvedbo te storitve se je npr. zmanjšalo število opolzkih klicev in nadlegovanja po telefonu v Kanadi (Lyon v Kovačič 2003: 12). Da pa se spet navežem na »dataveillance«, v ZDA so po uvedbi ISDN podjetja kmalu začela povezati številke kličočega z »socioekonomskimi in geodemografskimi podatki«(Kovačič 2003: 12).

Vsaka naprava, ki oddaja radijske valove omogoča sledljivost s pomočjo triangulacije. Ker mobilni telefoni oddajajo radijske valove, jih lahko tudi »prostorsko lociramo«(Kovačič 2003: 12).

Vsak mobilni telefon vsebuje še posebno IMEI (International Mobile Equipment Identity) številko, s katero lahko znotraj omrežja najdemo telefon, če je bil ukraden. Tako je možno locirati oziroma preprečiti komunikacijo neposredno na aparatu. Mobilni telefon pa je mogoče uporabiti za prisluškovanje tudi kadar je ta izključen, o tem piše Matej Saksida:

> *Ameriški zvezni preiskovalni urad (FBI) je javnosti razkril novo metodo tajnega prisluškovanja z mobilnimi telefoni, ki jo je uporabili v boju zoper organiziran kriminal. Gre za t.i. metodo potujoče miniaturne prisluškovalne naprave, ki omogoča snemanje pogovorov v okolici izključenega mobilnika. Tajno prisluškovanje je mogoče z mobilnimi telefoni podjetij Nextel, Samsung in Motorola, saj jih lahko vključimo na daljavo brez vednosti uporabnika. Namenski program seveda aktivira le tiste elektronske dele aparata, ki so nujno potrebni za prisluškovanje. Čeprav je nova metoda FBI-ju omogočila aretacijo številnih zločincev, bi jo v bližnji prihodnosti lahko s pridom koristili tudi nepridipravi za izvajanje raznovrstnih kriminalnih dejanj. Na to opozarjajo strokovnjaki podjetja*

Sophos, ki so pred časom pripomogli k aretaciji zlikovca, ki je s trojanskim konjem skrito vključeval spletne kamere naključnih žrtev (2006).

Komunikacijske naprave omogočajo, kot lahko vidimo, poleg prisluškovanja, prestrezanja podatkov ipd. tudi odkrivanje naše lokacije in povezovanje z zbirkami podatkov.

Nadzor nad informacijami lahko uporabljajo v raznih podjetjih za nadzor nad delavci. Tako lahko podjetja filtrirajo elektronsko pošto , ki vsebuje seksualne izraze ali datoteke z igrami (Wood 1999: 3). Vendar pa je tak nadzor logičen, saj delavec pri tem uporablja službeno opremo v službenem času. Bolj kritičen je nadzor delavcev na domu. Delo na domu, piše Fairweather, je dobro tako za zaposlenega in delodajalca. Delodajalcu ni treba plačevati za pisarne, delavec pa se ne utrudi s potovanjem na delo. Hkrati pa lahko čas, ki bi ga namenil za potovanje porabi kako drugače. Delavec lahko tako več ur časa dnevno nameni službi. Ker pa delovni čas na domu ni čisto definiran, se lahko zgodi da uporablja računalnik za zasebne zadeve ali ga sploh ne uporablja. Delodajalci se poslužujejo različnih tehnik nadzora nad delavci doma. Od štetja pritiskov na tipke, dolžine telefonskih klicev (Fairweather 1999: 3) do nadzora e-pošte in obiskanih strani na internetu.

Še bolj očiten je nadzor na internetu. Pametni usmerjevalniki podeljujejo povezave najprej večjim in komercialno pomembnejšim uporabnikom, medtem ko malim uporabnikom ostanejo minimalni prenosi ali celo sporočila o nedosegljivosti[29] (Graham in Wood 2003: 237–238). Vendar je to samo en vidik nadzora na internetu. Uporabnik interneta je lahko vedno pod nadzorom. Ker ima vsak računalnik povezan v internet svojo specifično IP številko, ga lahko na podlagi obiskanih strani in zahtev izsledimo. Uporabniki dobivajo od internetnih strani piškotke[30], z njimi si lahko personalizira podatke, ki jih dobiva od ponudnika, hkrati pa ponudnik vedno ve kdaj je uporabnik prijavljen na njegovi spletni strani. Možnosti nadzora preko interneta je veliko, da trojanskih konjev[31] sploh ne omenjam.

Vsak računalnik povezan v omrežje torej pridobi svoj virtualni naslov, IP številko (glej Kovačič 2003: 42-43). Pred uvedbo širokopasovnih povezav, ko so je

[29] *bandwidth exceeded, web page unavailable …*
[30] ang. cookies
[31] virusi, ki pustijo odprta vrata za vstop do uporabnikovega računalnika od zunaj.

uporabljal predvsem klicni dostop s pomočjo modema, je računalnik pridobil z vsakim priklopom nov IP naslov. Pri širokopasovnih povezavah pa imamo možnost statičnih naslovov, ko je naša številka vedno enaka, ali pa tudi dinamični naslov, kjer ponudnik po določenem času spremeni naš naslov. Računalnik pa ni nujno povezan v internet neposredno, takrat nam usmerjevalnik[32] dodeli lokalni IP[33]. Kljub vsemu pa je pot do posameznih računalnikov vseeno mogoča, ker je treba za uporabo določenih programov odpreti vrata na strežniku oz. usmerjevalniku, ki prepuščajo podatke neposredno do določenega računalnika.

Poznavanje IP številke računalnika je bistveno za potencialne vdore v računalnik. Vsekakor je identifikacija računalnika z dinamičnim naslovom in računalnika brez neposredne poveza v internet težja. Vendar pa obstajajo tudi programi, ki pošiljajo našo IP številko zunanjim klientom. Tako lahko postavimo svoj ftp[34] ali http[35] strežnik, v NATu odpremo vrata za dostop do našega računalnika. Program, ki ga imamo nameščenega na računalniku pošilja našo IP številko ponudniku domene. Če je naslov dinamičen, potem ponudnik samo spremeni naš naslov in pripisuje novo IP številko isti domeni. Primera takšnih ponudnikov sta npr. www.no.ip.com in www.dyndns.com. Določeni ponudniki omogočajo blokiranje posameznih vrat na svojem strežniku, tako ta deluje kot NAT[36].

Vseeno pa je identifikacija znotraj domačega omrežja zelo enostavna. V okolju Windows lahko v Omrežni soseščini vidimo vse računalnike v našem lokalne omrežju. V primeru, da dokumenti v skupni rabi niso primerno zaščiteni lahko pride do njih kdor koli v omrežju. Podjetja lahko tako nadzorujejo kdaj je posameznik prižgal računalnik ipd. Danes je v uporabi vedno več brezžičnih omrežij, saj se z njimi izognemo kablom, vrtanju lukenj ter drugim fizičnim posegom v prostoru. Vdor v brezžična omrežja je zelo enostaven, še posebej, če lastnik ne uporablja varnostnih algoritmov za dostop do podatkov in njihov prenos. V nezaščiteno omrežje lahko vdre vsakdo, ki ima primerno opremo.

[32] ang. router
[33] računalnik je tu skrit za posebnim vmesnikom NAT (ang. Network Address Translation) (Kovačič, 2003: 42)
[34] File Transfer Protocol (protokol za pošiljanje datotek)
[35] Hypertext Transfer Protocol (osnovni protokol za delovanje spleta oz world wide weba)
[36] http://www.t-2.net/?ctxID=00216A&funcID=1

Posamezen računalnik v omrežju lahko izsledimo s pomočjo enostavnega ukaza ping in s z njim spremljamo, če je določen IP prijavljen v omrežje. Nekateri programi in spletne strani omogočajo lociranje našega naslova. To lahko najlažje opazimo, ko vstopamo na tujo stran, ki s Slovenijo nimajo nobene veze, vendar ponujajo slovenske reklame. Obstajajo pa tudi specializirane strani, ki omogočajo neposredno lociranje IP naslova posameznika, oz. lokacije njegovega ponudnika[37].

Svoj IP lahko skrijemo z uporabo anonimnih zastopniških strežnikov[38], ti delujejo kot vmesni člen med nami in spletno stranjo, tako se ponudniku spletne strani pokaže IP naslov zastopniškega strežnika. Da bi se izognili anonimnim prijavam in omogočili personalizacijo spletnih strani, je Lou Montulli za podjetje Netscape leta 1994 (Kovačič 2003: 46) razvil zgoraj omenjene piškotke (ang. cookies). Piškotki so podatki, ki jih ponudnik pošilja brskalniku, ta jih shrani in po potrebi pošilja nazaj ponudniku (glej Kovačič 2003: 46). Piškotki omogočajo neposredne prijave na zaščitene strani in pa tudi sledenje posameznika po omrežju in njegovih brskalnih navad.

> *Te podatke lahko povežemo z elektronskim naslovom in celo s t.i. »off-line« identiteto. Fizično »off-line« identiteto uporabnika je mogoče ugotoviti tako, da uporabnik svoje podatke posreduje katerikoli spletni strani v omrežju, ti podatki pa se potem povežejo z identifikacijsko številko piškotka.*
>
> *Povezovanje brskalnih navad z elektronskim naslovom posameznika pa lahko poteka tako, da podjetje razpošlje množico elektronskih sporočil s personaliziranimi povezavami /.../Pošiljatelj torej natančno ve, na kateri naslov je poslal katero povezavo.Ko torej uporabnik klikne na personalizirano povezavo, lahko prejemnik ta klik zabeleži in tako s pomočjo piškotka poveže elektronski naslov identifikacijsko številko naslova.(Kovačič 2003:48).*

Nadzor komunikacij je že od nekdaj zanimiv v različne namene, predvsem za pridobivanje prednosti pred nasprotniki, ki jo dobiš s poznavanjem njegovih informacij. Danes je to še posebej enostavno, saj lahko z različnimi algoritmi določimo samodejno filtriranje relevantnih besed in s tem pogovorov. Tako ni potrebno neposredno prisluškovanje ali pregledovanje elektronskih sporočil, saj program sam izloči ne-relevantne pogovore.

[37] npr. http://www.geobytes.com/IpLocator.htm
[38] ang. Proxy server

3. 4 Nadzor mednarodnega in notranjega prometa

V zadnjih letih lahko spremljamo velike spremembe v nadzoru meja. Pomen meja skozi čas vidimo predvsem v vojaškem nadzoru določenega ozemlja, predpisov in zakonov, ki veljajo tam ter obdavčitvah in carinah na tem ozemlju. Današnji pomen pa se nanaša na nepretrgano linijo, ki označuje teritorij in suvereno oblast države (Walters 2006: 193).

Meje onemogočajo prost prehod ljudi in blaga. Kljub temu, da se meje odpirajo, se odpirajo predvsem znotraj »varnih« območij, kot je recimo Evropska unija. Države imajo usklajeno zakonodajo, zato je prost prehod omogočen. Vendar pa lahko kljub želji po čim večji povezanosti vidimo strah pred prehitrim pretokom cenejše delovne sile iz novih članic EU. Kljub vsemu pa pretok delovne sile znotraj EU ni velik problem, saj je povečini legalen in ima dobrodelen učinek na gospodarstvo.

Problem so ilegalni prebežniki. Z njimi so obremenjene predvsem zahodne družbe. Prebežniki iz revnih držav vidijo rešitev iz bede v Evropi in Zda. Medtem, ko se Evropa ukvarja predvsem s prebežniki iz Afrike, Vzhodne Evrope in Azije, imajo v Zda probleme predvsem s prebežniki iz Mehike in iz držav Južne Amerike. Največji problem poleg prebežnikov pa je tudi tihotapljenje prepovedanih drog, cigaret in ostalih predmetov.

Kot je že zgoraj omenjeno omogoča mobilna telefonija sledenje. Vsak telefon ohranja stik z bližnjimi oddajniki. Vsaka mobilna centrala[39] shranjuje podatke v mobilnih telefonih trenutno v njenem območju. Najpomembnejši podatek, ki ga ta zbirka podatkov hrani pa je t.i. LAI (identiteta lokalne območja)[40]. LAI označuje kateri oddajnik pokriva območje znotraj katerega je mobilnik. Tako ponudniki mobilne telefonije lahko omogočajo storitev triangulacije in sporočijo lokacijo posamezniku, na njegov telefon. Mobilni telefon, v povezavi s GPS tehnologijo, omogoča do centimetra natančno določitev lokacije. To vidimo v prej omenjenemu modelu e-cestninjenja.

Za sledenje se lahko uporabljajo tudi pripomočki, ki so namenjeni zabavi. Tako so se lotili raziskovalci iz Washingtonske Univerze skupnega projekta podjetja Nike, izdelovalca športnih čevljev in podjetja Apple. Komplet vsebuje iPod, športne čevlje

[39] MSC (ang. Mobile Switching Centre)
[40] ang. Local Area Identity

Nike in Nike + iPod Sport Kit. iPod Sport Kit vsebuje senzorje, ki s pomočjo RFID tehnologije pošiljajo podatke enoti na iPodu. Pomembna razlika od navadnih RFID čipov je, da imajo Applovi čipi domet tudi do skoraj 20 metrov[41]. Pripomoček je drugače namenjen štetju korakov, izračunavanju porabljenih kalorij, razdaljo ipd. Ker oddaja vsak RFID edinstven identifikator, lahko posameznika sledimo. Raziskovalci so sestavili napravo v vrednosti 250$, ki je lahko spremljala gibanje osebe. Glede na postavitev sprejemnikov so lahko projicirali gibanje osebe v GoogleMaps (Saponas in drugi, 2006). Tako lahko vidimo, da lahko s pomočjo tehnologije, ki je v bistvu namenjena zabavi naredimo resno napravo za nadzor gibanja ljudi.

Transportna podjetja in avtomobilska podjetja vgrajujejo v svoja vozila satelitske oddajnike, ki sporočajo podjetju s pomočjo GPS sprejemnika njihovo natančno lokacijo. Lastniki transportnih podjetij uporabljajo sledilne sisteme predvsem za optimizacijo transporta, medtem ko se v osebnih avtomobilih uporablja predvsem v primeru kraje. V avte se vgrajujejo tudi varnostni sistemi, ki pokličejo policijo in sporočijo lokacijo v primeru nesreče[42]. Pri sledenju vozil gre skoraj vedno še za vzporedno zbiranje podatkov, kje se vozilo nahaja, kako hitro se premika. Vendar pa nove tehnologije omogočajo beleženje tudi ostalih parametrov, od npr. vsebnosti alkohola v izdihanemu zraku voznika do tega, če se vozniku drema.

Vojna proti terorizmu je omogočila še hitrejšo vpeljavo modernih tehnologij. Za nadzor meja se tako uporabljajo nadzor podatkov, CCTV[43], najnovejše uporabne biometrične oblike nadzora in seveda klasični fizični način nadzora.

[41] 60 čevljev
[42] http://www.daveheinzel.com/suv/photos1.php
[43] Closed Circut television ang., video nadzorni sistem

4. Regulacija nadzora

Ker je postavljanje nadzornih sistemov očitno vdiranje v zasebnost državljanov, se seveda vprašamo kako države regulirajo to področje. Velika Britanija ima postavljenih okoli 4 milijone kamer, kar jo postavlja na prvo mesto na svetu (glej Gras 2004: 216-229). Postavljajo se vprašanja glede regulacije števila kamer. Hille Koskela v svojem članku (2003) poda tabelo, v kateri razloži razširjenost nadzora (Tabela 3. 1. 1) v mestih v državah, kjer nadzor ni zelo reguliran. Javni prostori so tisti so v javni uporabi in javni lasti. Pol-javni prostori pa so prostori, ki niso v celoti odprti za javno uporabo in so le delno, ali pa sploh ne, v javni lasti.

Tabela 4. 1: »Sprehod s Foucaultom«, groba kategorizacija urbanih prostorov pod nadzorom v mestih, kjer je regulacija nizka

	Javno	**Pol-javno**
nadzorovano	Ulice, trgi, tržnice, območja za pešce	Nakupovalna središča, trgovine, terminali, vozila javnega prevoza, Banke, bolnice, knjižnice, šole, nekatere cerkve
nenadzorovano	Večina parkov in urbanih gozdov	Male trgovinice, nekatere šole, cerkve in večina restavracij

(Vir: Koskela 2003: 295).

Na Danskem so nadzorne kamere v splošnem prepovedane. Uporabljajo jih lahko edino lastniki bencinskih črpalk ter policija. Policija jih lahko uporablja tudi prikrito. V Nemčiji zaradi federalne strukture obstaja več rešitev, v glavne pa lahko prepoznamo tri tipe dežel:

- dežele, ki ne poznajo regulacije,
- dežele, ki dovolijo nadzor s kamerami v točno določenih situacijah,

- ter dežele v katerih imajo policija in javne ustanove širšo zakonsko podlago za postavljanje kamer, snemanje in shranjevanje posnetkov za dlje časa (Weinbrenner v Gras 2004: 219).

Postavitev kamer v Nemčiji ne zadeva samo javnih ustanov, ampak tudi lastnino zasebnikov, ki je dostopna javnosti. Zasebnik pa mora za varovanje osebne lastnine ob postavitvi kamer tudi upoštevati določene kriterije. Postavitev kamere ne sme biti v nasprotju s pravico to svobodnega razvoja osebnosti, ki je zapisana v ustavnem zakonu. Pravica do osebnosti pa vsebuje tudi pravico to svoje slike (Gras 2004: 219).

V Veliki Britaniji policija lahko opazuje posameznika in ga tudi identificira, medtem ko to v Nemčiji ni možno, saj je v navzkrižju z ustavo. Nadzor s kamerami je torej, kadar nima zakonske podlage ilegalen.

V Franciji se mora za vzpostavitev nadzornega sistema sestati komisija, ki na podlagi podatkov ugotovi ali neko se na nekem območju res zgodi več kraj in napadov. Predlogi prihajajo predvsem iz bank, bencinskih črpalk in trgovin (Gras 2004: 223), prostorov v katerih se nam zdijo kamere čisto nekaj normalnega.

Vsako instalacijo kamer na Švedskem mora odobriti Okrožni administrativni odbor. Prošnja mora vsebovati natančen načrt postavitve in prostora nadzora. Hkrati pa mora vsebovati še dovoljenja zaposlenih. Da je prostor nadzorovan mora biti natančno označeno. Kamere so tam za preprečevanje in odkrivanje kriminala in morajo biti nepremične in brez možnosti zoomiranja. Bankam ni treba prositi za dovoljenje, vendar morajo postavitev javiti odboru (Gras 2004: 223).

Za evropske države je na splošno značilno da mora biti nadzorovano območje jasno označeno, kar pomeni, da se vsaka oseba, ki vstopi v to območje z nadzorom strinja (Gras 2004: 225).

Slovenska zakonodaja prav tako regulira video nadzor. Video nadzor spada v področje, ki ga pokriva Zakon o varstvu osebnih podatkov in s tem informacijska pooblaščenka. Oseba, ki izvaja nadzor, mora objaviti trajno obvestilo o video nadzoru. To obvestilo mora vsebovati:

1. da se izvaja video nadzor;
2. naziv osebe javnega ali zasebnega sektorja, ki ga izvaja;

3. telefonsko številko za pridobitev informacije, kje in koliko časa se shranjujejo posnetki iz videonadzornega sistema (www.ip-rs.si).

Zakonodaja določa tudi, kje se video nadzor lahko vrši in kje ne.

Regulacija varovanja osebnih podatkov pa je že razložena pri definiciji osebnih podatkov.

4. 1 Vojna proti terorizmu

Sprememba zakonodaj na področju varnosti in nadzora je v veliki meri posledica vojne proti terorizmu, po 11. septembru 2001. Napad na Svetovni trgovinski center in Pentagon je kriv za drastično povečanje nadzora po vsem svetu. Lyon opazi predvsem dve stvari, ki se zgodita po 11. septembru:

1. Razširitev že obstoječega obsega nadzornih tehnik in praks, ki nas definirajo in pomagajo oblikovati naš družbeni obstoj.
2. Težnja k zaupanju novim tehnološkim nadgradnjam nadzornih sistemov (tudi, če je nejasno ali delujejo in če rešujejo problem zaradi katerega so bili vzpostavljeni) (Lyon 2001: 3).

Spremembe nadzora so vidne na dveh področjih pravnem in tehničnem. V ZDA se je to pokazalo s »Patriot actom« (glej Lyon 2001: 3). »Patriot act«oziroma Zakon za zedinjenje in jačanje Amerike z določitvijo primernih orodij za prekinitev in onemogočanje terorizma, 2001 (ang. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001) je zakon, ki je vstopil v veljavo po napadih 11. septembra. Zakon je dal ameriškim organom nadzora (policija, varnostno obveščevalne agencije …) večja pooblastila za boj proti terorizmu doma in v tujini. Med drugim je omogočal odkrivanje in kaznovanje domnevnih potencialnih zločinov, kot je npr. dajanje napačnih informacij o terorizmu (glej http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107). Zvezno sodišče je dele zakona razglasilo za neustavne, zato so marca 2006 zakon prenovili (glej http://www.whitehouse.gov/

infocus/patriotact/). Mnogo držav je sledilo Zda v pripravi zakonov, ki bi omejili teroristične napade.

Takrat se pojavijo ideje o vpeljavi biometričnih podatkov v identifikacijske dokumente. Slovenija je tako ena izmed držav, ki ima potne liste s čipom, ki vsebuje sliko lastnika.

> *Biometrični potni listi morajo biti interoperabilni, kar pomeni, da morajo biti podatki na čipu zapisani tako, da jih lahko prebere mejni organ katere koli tuje države, ne glede na to, kakšno strojno in programsko opremo uporablja na svojih mejnih prehodih. Za zagotovitev interoperabilnosti je vsebina podatkov na čipu točno določena. Na čipu so zapisani le tisti podatki, ki so tudi sicer vidno zapisani v potnem listu (osebno ime, državljanstvo, datum rojstva, spol, država izdaje, številka potnega lista in datum poteka) in fotografija, ki je na potnem listu.*
>
> *Fotografija odprtega biometričnega potnega lista z biografsko stranjo, v kateri je nevidno shranjen brezkontaktni čip.*
>
> *Dostop do podatkov na čipu omogoča le obkrožen OCR-B zapis. (http://www.mnz.gov.si/fileadmin/mnz.gov.si/pageuploads/SOJ/word/BPLpriloga1.pdf/)*

Do leta 2009 pa naj bi čip poleg slike vseboval tudi dva prstna odtisa.

Kot vidimo vojna proti terorizmu ni vplivala samo na neposredno prizadete države ampak na ves svet, saj sprememba zakonodaje pri prestopu mej v Zda vpliva na ves svet. Hkrati pa je ista zakonodaja omogočila razvoj podobne zakonodaje v ostalih državah. Biometrični potni listi in pametne identifikacijske kartice, bi vseeno prišle v uporabo, vendar bi lahko pred tem poteklo še veliko časa.

4. 2 Javnomnenjske raziskave stališč o nadzoru

Vseskozi pa imamo občutek, da vsa zakonodaja, ki zadeva nadzor, nastaja s splošnim konsenzom. Zakonodajalci se pri tem opirajo predvsem na javnomnenjske raziskave. Velikokrat se pojavi dvom v zanesljivost podatkov pridobljenih z javnomnenjskimi raziskavami, še posebej pa v primeru raziskave stališč o nadzoru.

Ena pomembnejših kritik javnomnenjskih raziskav je, da silijo ljudi, da podajajo mnenja o stvareh o katerih niso premišljevali in so za njihovo vsakdanje življenje

relativno nepomembne. Včasih jih vprašanja presenetijo in na njih odgovarjajo, kasneje pa se pojavi skrb glede zaupnosti podanih podatkov. Kot pišeta Haggerty in Gaszo (2005: 173), se je to zgodilo na Univerzi v Alberti, v njihovem Laboratoriju za populacijske raziskave. Anketiranec je poklical naslednji dan v skrbeh glede varovana svoje identitete zaradi dela vprašanj o zasebnosti, razvoju nadzora in kako osebe uporabljajo nadzorno tehnologijo za varovanje.

Moderni postopki, ki jih raziskovalci uporabljajo pri ugotavljanju javnega mnenja so izdelani do potankosti. Metode so v smiselnih okvirih tudi avtomatizirane in strokovnjaki vedo, kako izvesti kvalitetno vzorčenje. Vendar rezultati javnomnenjske raziskave, kot rezultati vsake druge meritve, s seboj nosijo določeno merilno negotovost. Z dopolnjevanjem ustreznega vzorčenja in statistične obdelave lahko anketne rezultate danes že precej dobro ovrednotimo. Javnomnenjske raziskave so tako dobile plebiscitarno vlogo, kljub temu da nimajo nobene zakonske podlage. Politiki se na njihovi osnovi odločajo o svojih novih potezah (glej Haggery in Gaszo 2005: 174).

Eden od pomembnejših faktorjev, ki vplivajo veljavnost raziskav, je stopnja tistih, ki se odločijo za sodelovanje v raziskavi[44]. Ta je zelo pomembna še posebej pri raziskavah o zasebnosti in nadzoru (Heggerty in Gazso 2005: 174). Javnomnenjske raziskave so se iz golega opisovanja spremenile v analitično sredstvo z uporabo naključnega (glej Splichal, 1997:296). Za oblikovanje vzorca raziskovalci najraje uporabljajo telefonske imenike, ker lahko tako najhitreje pridejo do podatkov. Posamezniki, ki so zaskrbljeni zaradi povečevanja nadzora in manjšanja zasebnosti, bodo z večjo verjetnostjo umaknili svojo številko iz telefonskega imenika[45]. To bi jih izključilo iz raziskave. Podobno velja tudi za internetne raziskave potencialni anketiranci so ponavadi zbrani v komercialnih zbirkah, kjer podobno kot v imenikih ni zaskrbljenih oz. jih je manj. Če pa bi do teh potencialnih anketirancev le prišli, bi ti z večjo verjetnostjo odklonili anketiranje (Haggerty in Gaszo 2005: 175).

Kot še pišeta Haggerty in Gazso so raziskave: »v bistvu oblika nadzora, ki jo nekateri posamezniki interpretirajo kot vdor v zasebnost«(2005: 175-176).

[44] ang. response rate

[45] podobno se je zgodilo že leta 1936, ko je Literary Digest napovedal zmago predsedniškega kandidata Landona, protikandidata Roosveltu, kar se seveda ni zgodilo. Literary Digest je opravil telefonsko raziskavo. Raziskava je bila očitno pristranska saj so bili Roosveltovi volivci predvsem manj izobraženi in revnejšidržavljani , ki niso imeli telefon (glej Splichal, 1997: 258, Wikipedia)

Kanadski časopis, The Globe and Mail, je naročil javnomenjsko raziskavo o kanadskih stališčih in mnenjih o varnosti in svoboščinah. Eden od pomembnejših izsledkov je bil da 72% respondentov podpira video nadzor na javnih mestih. Niso pa navedli odstotka kontaktiranih oseb in ne odstotka, koliko od kontaktiranih je odgovarjalo na anketna vprašanja. Odstotek tistih, ki so odgovarjali je bil le 11,6%. To pomeni, da so za anketiranje 1056 oseb morali poklicati čez 12000 številk. Večina teh ni odgovorila na klic ali pa so imeli vzpostavljeno preusmeritev klica na telefonsko tajnico /.../. Končno 4356 posameznikov je odgovorilo in so bili vabljeni k sodelovanje. 3300 je zavrnilo sodelovanje, kar predstavlja 76%. Glede na te številke lahko upravičeno sumimo, da obstajajo diskriminatorne lastnosti povezane proti nadzornimi in pro-zasebnostnimi mnenji med veliko večino ljudi, ki niso mogli biti kontaktirani ali so odklonili sodelovanje. To pomeni da ta in primerljive študije sistematično ne pokažejo stopnje javne skrbi glede teh tem (Haggerty in Gazso 2005: 176).

Kot vidimo je vprašanje nadzora in zasebnosti v javnomnenjskih raziskavah zelo problematično, saj zelo težko dobimo dober naključni vzorec anketirancev. Za analizo bi bilo bolje, če bi na podobno temo obstajalo več raziskav. Tako bi lahko zanesljivo vedeli v kolikšni meri se ljudje v resnici strinjajo s povečevanjem nadzora.

4. Zaključek

Po vsem prebranem lahko rečemo, da se kljub vsemu iz Benthamovih časov pa do danes bistveno ni spremenilo. Še vedno obstaja potreba po nadzoru in še vedno so nadzorovani deležni kazni, če kršijo pravila. Spremenil se je le način. V Bentham je podpiral telesno kaznovanje, kot je fizična osamitev. Kasneje pa je Foucault s svojo interpretacijo panoptikona poudaril bolj psihološko raven nadzora. Skupno obema je, da nadzor temelji na vizualnem opazovanju.

Foucault pa kljub vsemu ni dojel vseh prednosti modernih tehnologij. Oblikoval se je tako imenovani Superpanoptikon, ki ga oblikujejo moderna omrežja in tehnologije, ki so vedno bolj zlite med samo. Ta kvantitativen napredek v tehnologiji pomeni tudi kvalitativno spremembo v mikrofiziologiji moči (Poster, po Graham in Wood 2003: 230). Nadzor ni več omejen na samo eno stavbo ali prostor, ampak se je razširil na praktično vsa, predvsem urbana, območja. To je seveda, če gledamo predvsem vizualni tip nadzora. Video nadzor je spremenil način kako se obnašamo na javnih prostorih. Zakonodaja je tista, ki mora onemogočati, da bi se z video nadzorom preveč vdiralo v našo zasebnost in mora določiti, kje in v kolikšni meri je ta nadzor dovoljen.

Podatkovni nadzor se lahko vrši nad celoto populacijo. Nadzor ni več domena v glavnem države ampak ga uporabljajo predvsem zasebna podjetja, korporacije. Nadzor je vedno bolj nadzor nad potrošniki. Ti se za dostikrat za oddajo podatkov odločijo zavestno. Podatke damo dostikrat zaradi obljubljene nagrade, kot so popusti, praktične nagrade ipd., ali pa posledične kazni kot je dražji nakup ali omejen dostop do informacij itd. Velikokrat namerno pozabimo na varovanje zasebnosti. V glavnem zaradi gornjih razlogov, lahko pa tudi iz kulturnih, gospodarskih ali celo ideoloških.

Zanimivo pa je, da noben avtor ne poudari bistvene razlike, ki jo prinaša digitalni nadzor. Za panoptikon velja, da posameznik ne ve, kdaj je nadzorovan in kdaj ne ter, da se samodiscplinira prav zaradi tega. Digitalizacija (algoritemski nadzor) pa omogoči stalen nadzor, brez izjem. Program neprestano išče določene lastnosti posameznika, da ga prepozna v sistemu.

Za varovanje zasebnosti se bi morali ljudje bolj zavzeti, predvsem z uvedbo dodatnih, kot pravi Kim, tehnologij za ojačevanje zasebnosti (ang. privacy-enhancing technologies, PET), z njimi bi pripomogli pri varovanju zasebnosti in dopuščali uporabo samo potrebnih podatkov (2004: 210). Kot primer take tehnologije, so npr. elektronski certifikati, čeprav se vprašanje o zasebnosti ponovi, glede na to, da ima podjetje, ki jamči za nas z izdajo certifikata, podatke o nas. Pravzaprav smo nekakšnem začaranem krogu, ki je posledica zlivanja tehnologij in interesov, tako političnih kot ekonomskih.

Digitalizacija je omogočila varnostnim sistemom, da delujejo avtomatsko. Nadzorni programi, kljub svoji »naravni nediskriminatornosti«, niso popolnoma objektivni. Programe ustvarjajo programerji iz različnih multinacionalk, ki programe pišejo in definirajo na enem koncu sveta, prodajajo pa jih v države na drugem koncu sveta z časovno zamudo (Graham in Wood 2004). Hkrati pa tudi programerji, kot sem večkrat poudaril, niso objektivni.

Kot izgovor za nadzor se velikokrat uporablja, racionalizacija procesov. Kot tak je logičen pri usmerjanju komunikacij, pretoku informacij in prometu. Klub vsemu pa tehnologije omogočajo, da hkrati z racionalizacijo tudi diskriminacijo in sledenje posameznikov. Tako določeni ljudje ali skupine zaradi ekonomskih ali političnih razlogov nimajo dostopa do informacij. Ali pa se tehnologije, iz istih razlogov, uporabi za nadzor njihovega gibanja in navad tako v realnem kot virtualnem svetu.

Za moderne tehnološke rešitve na področju nadzora je značilna ta dihotomija. Po eni strani se razvija, da bi olajšala delo, povečala varnost in zadovoljstvo ljudi. Po drugi strani pa lahko isto tehnologijo uporabimo za sledenje in spremljanje dela posameznika, za vdor v njegovo zasebnost in s tem tudi občutek zadovoljstva (glej tudi Jones 2000).

Po dogodkih 11. septembra, lahko govorimo o pospešeni uporabi novih tehnologij za nadzor. Vendar pa lahko z gotovostjo trdimo, da bi do podobne stopnje prišli tudi, če se teroristični napadi ne bi zgodili. Mogoče bi za to potrebovali le kakšno leto več. Moderni način življenja namreč temelji na racionalizaciji. Hitro življenje posameznika prisili, da se odloči za kompromise. Tako je kreditna kartica kompromis, ki ga sprejmemo, da lahko pohitrimo in olajšamo naše plačilne posle. Z vstopom v prostor z video nadzorom se sprijaznimo, kljub temu, da je naša podoba shranjena. Napredne identifikacijske izkaznice bodo s časoma realnost, kljub temu, da bo to

pomenilo, da so vsi naši podatki zbrani na enem mestu. Zasebnost se umika racionalizaciji, ena kartica zavzame manj prostora kot deset drugih.

Vsekakor pa je digitalizacijo prinesla dosti sprememb v družbi in v njenem razumevanju, kar se vidi predvsem v odnosu do zasebnosti, ki je hkrati velika moralna vrednota, hkrati pa se ji odrečemo vsakič, ko nam ponudijo popust v trgovini. Nadzorovalne tehnologije sprejemamo kot nekaj samoumevnega, zato se lahko zgodi, da se čez nekaj let ne bomo več obremenjevali z zasebnostjo. Veliki Brat bo vsepovsod. Za konec še šala Stevena Wrighta: »Vsake toliko časa se nagnem skozi okno in se nasmehnem v nebo … za satelitsko fotografijo«(1985).

Priloge

Priloga A

Splošno sprejeti principi o zasebnosti

(povzeto po:
http://infotech.aicpa.org/Resources/Privacy/Generally+Accepted+Privacy+Principles/Generally+Accepted+Privacy+Principles/)

1. princip:

Prvi princip Splošno sprejetih principov o zasebnosti je upravljanje. Ta princip zahteva, da se definira, dokumentira in določi odgovornost bistva zasebnostnih politik in procedur

2. Princip: Objava

Ta princip zahteva, da se objavijo politike in postopki ter se identificirajo razlogi zaradi katerih se zbirajo, uporabljajo, shranjujejo in razkrivajo podatki.

3.Princip: Izbira in odobritev

ta princip zahteva, da se opišejo posamezniku dostopne možnosti in se pridobi implicitna ali eksplicitna odobritev zbiranja, uporabe in razkritja osebnih podatkov.

4. Princip: Zbiranje

Ta princip zahteva, da se podatki zbirajo za namene opisane v obvestilu.

5. Princip: Uporaba in shranjevanje

Ta princip zahteva, da se omeji uporaba osebnih na samo razloge omenjene v objavi in za katere je dal posameznik implicitno ali eksplicitno dovoljenje.

6. Princip: Dostop

Ta princip zahteva, da se posamezniku omogoči dostop do njihovih osebnih podatkov, da jih pregleda in posodobi.

7. Princip: Razkritje tretjim osebam

Ta princip zahteva, da se osebne informacije tretjim osebam lahko razkrijejo, le z razlogom navedenim v obvestilu in samo z implicitnim ali eksplicitnim dovoljenjem posameznika.

8. Princip: Varovanje zasebnosti

Ta princip zahteva, da osebne informacije varujejo pred neautoriziranim dostopom (tako fizičnim kot računalniškim).

9.Princip: Kvaliteta

Ta princip zahteva, da se zbirajo natančni, popolni in relevantni osebni podatki z razlogi navedenimi v obvestilu.

10. Princip: Nadzor in uveljavljanje

Ta princip zahteva, da se nadzira skladnost s politikami in procedurami, hkrati pa mora imeti procedure s katerimi naslavlja preiskave in spore glede zasebnosti.

Generally Accepted Privacy Principles (v originalu)

Principle 1: Management

The first principle of the Generally Accepted Privacy Principles (GAPP) is Management. This principle requires that the entity define, document, communicate, and assign accountability for its privacy polices and procedures.

Principle 2: Notice

The second principle of the Generally Accepted Privacy Principles (GAPP) is Notice. This principle requires that the entity provide notice about its privacy policies and procedures and identify the purpose for which personal information is collected, used, retained, and disclosed.

Principle 3: Choice and Consent

The third principle of the Generally Accepted Privacy Principles (GAPP) is Choice and Consent. This principle requires that the entity describe the choices available to the individual and obtain implicit or explicit consent with respect to the collection, use, and disclosure of personal information.

Principle 4: Collection

The fourth principle of the Generally Accepted Privacy Principles (GAPP) is Collection. This principle requires that the entity collect personal information only for the purposes identified in the notice.

Principle 5: Use and Retention

The fifth principle of the Generally Accepted Privacy Principles (GAPP) is Use and Retention. This principle requires that the entity limit the use of personal information to the purpose identified in the notice and for which the individual has provided implicit or explicit consent.

Principle 6: Access

The sixth principle of the Generally Accepted Privacy Principles (GAPP) is Access. This principle requires that the entity provide individuals with access to their personal information for review and update.

Principle 7: Disclosure to Third Parties

The seventh principle of the Generally Accepted Privacy Principles (GAPP) is Disclosure to Third Parties. This principle requires that the entity disclose personal information to third parties only for the purposes identified in the notice and only with the implicit or explicit consent of the individual.

Principle 8: Security for Privacy

The eighth principle of the Generally Accepted Privacy Principles (GAPP) is Security for Privacy. This principle requires that the entity protect personal information against unauthorized access (both physical and logical).

Principle 9: Quality

The ninth principle of the Generally Accepted Privacy Principles (GAPP) is Quality. This principle requires that the entity maintain accurate, complete, and relevant personal information for the purposes identified in the notice.

Principle 10: Monitoring and Enforcement

The tenth principle of the Generally Accepted Privacy Principles (GAPP) is Monitoring and Enforcement. This principle requires that the entity monitor compliance with its privacy policies and procedures and have procedures to address privacy-related inquiries and disputes.

Priloga B

Zdravstveni podatki (http://www.ip-rs.si/index.php?id=552)

Zdravstvene podatke ZVOP-1 šteje za občutljive osebne podatke. To pa pomeni, da je njihova obdelava možna le v naslednjih primerih:
1. če je posameznik za to podal izrecno osebno privolitev, ki je praviloma pisna, v javnem sektorju pa tudi določena z zakonom;
2. če je obdelava potrebna zaradi izpolnjevanja obveznosti in posebnih pravic upravljavca osebnih podatkov na področju zaposlovanja v skladu z zakonom, ki določa tudi ustrezna jamstva pravic posameznika;
3. če je obdelava nujno potrebna za varovanje življenja ali telesa posameznika, na katerega se osebni podatki nanašajo, ali druge osebe, kadar posameznik, na katerega se osebni podatki nanašajo, fizično ali poslovno ni sposoben dati svoje privolitve iz 1. točke tega člena;
4. če jih za namene zakonitih dejavnosti obdelujejo ustanove, združenja, društva, verske skupnosti, sindikati ali druge nepridobitne organizacije s političnim, filozofskim, verskim ali sindikalnim ciljem, vendar le, če se obdelava nanaša na njihove člane ali na posameznike, ki so v zvezi s temi cilji z njimi v rednem stiku, ter če se ti podatki ne posredujejo drugim posameznikom ali osebam javnega ali zasebnega sektorja brez pisne privolitve posameznika, na katerega se nanašajo;
5. če je posameznik, na katerega se nanašajo občutljivi osebni podatki, te javno objavil brez očitnega ali izrecnega namena, da omeji namen njihove uporabe;
6. če jih za namene zdravstvenega varstva prebivalstva in posameznikov ter vodenja ali opravljanja zdravstvenih služb obdelujejo zdravstveni delavci in zdravstveni sodelavci v skladu z zakonom;
7. če je to potrebno zaradi uveljavljanja ali nasprotovanja pravnemu zahtevku;
8. če tako določa drug zakon zaradi izvrševanja javnega interesa.

ZVOP-1 za prekomerno obdelavo občutljivih osebnih podatkov določa globo 1.000.000 do 3.000.000 SIT za pravno osebo ali samostojnega podjetnika posameznika in 200.000 do 500.000 SIT za odgovorno osebo.

Zdravstvene kartoteke

V praksi Informacijskega pooblaščenca (prej tudi Inšpektorata za varstvo osebnih podatkov) se pogosto izkaže, da predvsem zdravstvene institucije, ki bi za zavarovanje zdravstvenih podatkov posameznikov morale najbolj skrbeti, tega ne storijo. Državni nadzorniki v zdravstvenih domovih tako še vedno odkrivajo zdravstvene kartoteke, ki ležijo v odklenjenih ali celo odprtih omarah na hodnikih in do katerih imajo dostop vsi. Zato Pooblaščenec poziva vse, ki imajo opravka z zdravstvenimi (in drugimi občutljivimi) osebnimi podatki – ne zgolj zdravstvene domove –, da takoj in kar se da učinkovito uredijo zavarovanje zdravstvenih kartonov posameznikov, izdanih receptov, evidence bolnikov itd.

Pooblaščenec opozarja tudi na dejstvo, da ima vsak posameznik pravico vpogledati v svoj zdravstveni karton, saj gre pri tem za uresničevanje pravice posameznika do vpogleda v lastne osebne podatke. Zdravnik pa je, na drugi strani, dolžan posamezniku omogočiti vpogled v njegovo zdravstveno kartoteko.

Pooblaščenec tudi opaža, da se posamezniki pogosto ne zavedajo pomena varovanja lastnih osebnih podatkov. Zato svetuje, da ob vsakem zahtevku po vašem zdravstvenem podatku, za katerega menite, da ni utemeljen, vprašate, zakaj tisti, ki od vas takšen podatek zahteva, tega potrebuje, kako ga bo hranil in kaj bo z njim počel.

Pretok informacij med zdravstvenim osebjem

Prav tako se je v praksi že izkazalo, da je za zdravstveno stanje posameznika izvedelo več zdravstvenega osebja, kot bi ga lahko. Pooblaščenec opozarja, da se lahko zdravstveno stanje posameznika razkrije samo tistim zdravstvenim delavcem, ki so v proces zdravljenja neposredno vključeni. Razkritje zdravstvenega stanja zdravstvenemu osebju, ki ni vključeno v proces zdravljenja, pomeni prekomerno obdelavo osebnih podatkov.

Literatura in viri:

- Abe, Kiyoshi (2004): **Everyday Policing in Japan**. *Surveillance, Media, Government and Public Opinion*. V: International Sociology. 19(2), 215-231. SAGE.
- Philip E. Agre (1994): **From high tech to human tech**: *Empowerment, measurement, and social studies of computing*. V: Computer Supported Cooperative Work (CSCW). 3(2), 167-195. Springer Netherlands.
- Ball, Kirstie (2005): **Organization, Surveillance and the Body**: *Towards a Politics of Resistance*. V: Organization articles, Volume 12(1): 89-108. SAGE.
- Cook, Julie, 1999. **Big brother goes to work**. V: Office Systems; Aug 1999, 43-45. SAGE.
- Dubbeld, Lynsey (2005): **Protecting Personal Data in Camera Surveillance Practices**. V: Surveillance & Society'People Watching People' 2(4), 546-563. Dostopno na: http://www.surveillance-and-society.org (24. januar 2007).
- Elmer, Greg (2003):**A diagram of panoptic surveillance**. V: New media & society 5(2), 231–247. SAGE.
- Fairweather,N. Ben, (1999): **Surveillance in employment**: *The case of teleworking*. V: Journal of Business Ethics 22(1), 39-40. ABI/INFORM Global
- Finn, Jonathan (2005): **Photographing Fingerprints**: *Data Collection and State Surveillance*. V: Surveillance & Society 3(1), 21-44 Dostopno na http://www.surveillance-and-society.org/ (24. januar 2007).
- Foucault Michel (1984): **Nadzorovanje in kaznovanje**. Ljubljana: Delavska skupnost.
- Graham, Stephen in David Wood (2003): **Digitizing surveillance: categorization, space, Inequality. V:** Critical Social Policy 23(2), 227–248. SAGE.
- Gras, Marianne L. (2004): **The Legal Regulation of CCTV in Europe**. V: Surveillance & Society CCTV Special 2(2/3), 216-229. Dostopno na: http://www.surveillance-and-society.org (24. januar 2007).

- Gray, Mitchell (2003): **Urban Surveillance and Panopticism**: *will we recognize the facial recognition society?*. V: Surveillance & Society 1(3), 314-330. Dostopno na: http://www.surveillance-and-society.org (24. januar 2007).
- Haggerty, Kevin D. in Amber Gazso (2005): **The Public Politics of Opinion Research on Surveillance and Privacy**. Surveillance & Society 'Doing Surveillance Studies' 3(2/3), 173-180. Dostopno na: http://www.surveillance-and-society.org/ (24. januar 2007).
- Introna, Lucas D. in David Wood (2004): **Picturing Algorithmic Surveillance**: *The Politics of Facial Recognition Systems*. V: Surveillance & Society CCTV Special 2(2/3): 177-198. Dostopno na: http://www.surveillance-and-society.org/cctv.htm (24. januar 2007).
- Jones, Richard (2000): **Digital Rule**, *Punishment, Control and Technology*. V: Punishment & Society 2(1), 5-22. SAGE.
- Kim, Mun-Cho (2004): **Surveillance Technology, Privacy and Social Control.** *With Reference to the Case of the Electronic National Identification Card in South Korea.* V: International Sociology 19(2), 193–213. SAGE.
- Koskela, Hille (2003): **'Cam Era' – the contemporary urban Panopticon**. V: Surveillance & Society 1(3), 292-313. Dostopno na http://www.surveillance-and-society.org (24. januar 2007).
- Kovačič, Matej (2003): Zasebnost na internetu. Ljubljana: Mirovni inštitut.
- Lyon, David (2001): **New directions in theory**. Monitoring Everyday Life.Buckingham: Open university press.
- Lyon, David (2003): **Surveillance Technology and Surveillance Society.** V: Modernity and Technology. Cambridge: The MIT Press.
- Lyon, David (2004a): **Globalizing Surveillance**, *Comparative and Sociological Perspectives*. V: International Sociology 19(2), 135–149. SAGE.
- Lyon, David, (2004b): **Identity cards**: *social sorting by database*. V: Oxford Internet Institute, Internet Issue Brief No. 3, November 2004. The University of Oxford for the Oxford Internet Institute. Dostopno na www.oii.ox.ac.uk/resources/publications/ (21. januar 2007).
- Mann, Steve, Jason Nolan in Barry Wellman (2003): **Sousveillance***: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance*

Environments. V: Surveillance & Society 1(3), 331-355. Dostopno na: http://www.surveillance-and-society.org (24. januar 2007).

- Martinais, Emmanuel in Christophe Bétin (2004): **Social Aspects of CCTV in France**: *the Case of the City Centre of Lyons*. V: Surveillance & Society, CCTV Special 2(2/3): 361-375. Dostopno na http://www.surveillance-and-society.org (24. januar 2007).
- Neumann, Peter G. (1993): **Risks of surveillance.** V:Association for Computing Machinery. Communications of the ACM; Aug 1993.p. 122. SAGE.
- Shields, Peter (2006): **Electronic Networks, Enhanced State Surveillance and the Ironies of Control**. Journal of Creative Communications 1:1: 22-38. SAGE.
- Splichal Slavko (1997): Javno mnenje. Ljubljana: fakulteta za družbene vede.
- Walters, William (2006): Border/Control. V: European Journal of Social Theory 9(2): 187-203. SAGE.

Viri:

- Caplan, J. in J. Torpey (2001): Identity and Anonymity: Some Conceptual Distinctions and Issues for Research In, Documenting Individual Identity. Princeton University Press. Dostopno na http://web.mit.edu/gtmarx/www/identity.html (16. januar 2007).
- Espiner, Tom (2006): Nike+iPod raises RFID privacy concerns. Dostopno na http://news.com.com/NikeiPod+raises+RFID+privacy+concerns/2100-1029_3-6143606.html (14. december 2006).
- Franklin, Benjamin (2006): Civilization 4. Firaxis games
- Lyon, David (2001): **Terrorism and Surveillance**: *Security, Freedom, and Justice after September 11 2001*. Predavanje v sklopu Privacy Lecture Series. Dostopno na http://privacy.openflows.org (12. januar 2007).
- Lyon, David (2000): Everyday Surveillance: **Personal data and social classifications.** Poročilo v okviru delavnice Challenges and oppurtunities of a knowledge-based economy (KBE). Dostopno na http://pacific.commerce.ubc.ca/kbe/lyon_surveillance.pdf (27. januar 2007).

- Radwanski, George (2001): Address by the Privacy Commissioner of Canada delivered to the Privacy Lecture Series. Predavanje v sklopu Privacy Lecture Series. Dostopno na http://privacy.openflows.org (24. januar 2007).
- Rummel, David in Nelli Kheyfets (2006): Secret history of the credit card. Dostopno na http://www.pbs.org/wgbh/pages/frontline/shows/credit/etc/script.html (18. januar 2007).
- Saksida, Matej (2006): Tajno prisluškovanje z izključenimi mobilnimi telefoni. Dostopno na http://www.racunalniske-novice.com/main/ (18. januar 2007).
- Saponas, T. Scott, Jonathan Lester , Carl Hartung in Tadayoshi Kohno (2006): **Devices That Tell On You**: *The Nike+iPod Sport Kit*. Department of Computer Science and Engineering,University of Washington, Seattle. Dostopno na http://www.cs.washington.edu/research/systems/nikeipod/tracker-paper.pdf (24. januar 2007).
- The European Counterweight Part 1: A Leaderless Superpower (2006). Dostopno na http://www.realtruth.org/articles/413-tec.html (18. januar 2007).
- MICHEL FOUCAULT, INFO. Dostopno na http://foucault.info/ (23. december 2006).
- NO2ID. Dostopno na http://www.no2id.net/ (11. januar. 2007).
- Patriot act (2006). Dostopno na http://www.whitehouse.gov/ infocus/patriotact/ (18. januar 2007).
- Privacy Lecture series. Dostopno na http://privacy.openflows.org/archive.html (18. januar 2007).
- Samsung Techwin Dostopno na http://www.samsungtechwin.com/product/features/dep/SSsystem_e/SSsystem.html (18. januar 2007).
- Spletna stran informacijskega pooblaščenca Republike Slovenije. Dostopno na http://www.ip-rs.si/index.php (16. januar 2007)
- UCL BENTHAM PROJECT. Dostopno na: http://www.ucl.ac.uk/Bentham-Project/ (23. december 2006).
- Panopticon: www.uweb.ucsb.edu/~brentongieser/thirdpage.html (4. december 2006).