UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Aleksandra Doroteja Rettinger

Elektronski nadzor zaposlenih: sociološko-pravni vidik

Diplomsko delo

Ljubljana, 2008

UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Aleksandra Doroteja Rettinger

Mentorica: Izr. prof. dr. Dana Mesner-Andolšek

Somentorica: Asist. dr. Barbara Rajgelj

Elektronski nadzor zaposlenih: sociološko-pravni vidik

Diplomsko delo

Ljubljana, 2008

”I WAS BORN STANDING UP
AND TALKING BACK”

ELVIS PRESLEY: TROUBLE

KONSTANCI RETTINGER

ELEKTRONSKI NADZOR ZAPOSLENIH: SOCIOLOŠKO-PRAVNI VIDIK

Z napredkom tehnologije se razvijajo tudi nove oblike elektronskega nadzora zaposlenih. V diplomskem delu sem obdelala dva vidika elektronskega nadzora zaposlenih: sociološkega in pravnega. Sociološko-filozofske teorije o Panoptikonu, o 'popolnem mestu' in o Velikem bratu imajo skupno rdečo nit: možnosti nadzora ljudi s pomočjo arhitekture in dane tehnike. Ustava in zakoni ter podzakonski akti skušajo zavarovati pravico posameznika do zasebnosti in intime na delovnem mestu. Kako pa je z nadzorom zaposlenih v praksi? Pri pregledu pravne in dejanske ureditve pri nas in v svetu sem opisala najpogostejše oblike elektronskega nadzora zaposlenih, nato pa za dokaz o (ne)delovanju zakonskih omejitev še obiskala dve organizaciji. Dejstvo je, da je elektronski nadzor zaposlenih od podjetja do podjetja različen; prilagojen je dejavnosti, s katero se ukvarjajo. Očitno je, da kljub zakonskim omejitvam še vedno prihaja do kršitev in bo verjetno prihajalo tudi v bodoče. Človekova narava (delodajalčeva in delavčeva) je namreč taka, da išče bližnjice in skuša prelisičiti dane omejitve pri veljavnem pravnem sistemu.

Ključne besede: elektronski nadzor, nadzor zaposlenih, pravice delavca na delovnem mestu, Panoptikon

THE ELECTRONIC SURVEILLANCE OF EMPLOYEES: SOCIOLOGICAL AND LEGAL ASPECT

With the progress of technology new forms of electronic surveillance of employees are emerging. In my diploma work, I was dealing with two aspects of electronic surveillance of employees: sociological and legal. Sociological-philosophical theories of Panopticon, of the 'perfect city' and of Big brother have one thing in common: they all treat the possibilities of monitoring people by means of architecture and available technology. The Constitution and laws are trying to protect the right of individuals to privacy and intimacy on the work place. But how are employees monitored in reality? I reviewed the Slovenian and some foreign judicial systems and the actual state of electronic monitoring of employees; I also described some popular forms of electronic monitoring of employees. To investigate the reality of such surveillance, I visited two organizations in Ljubljana. The forms of monitoring of employees vary from organization to organisation, as it best suits their organizational activity. It is obvious that violations of laws are detected and they will probably be detected in the future. It is in the human nature that human beings (employers and employees) are trying to avoid limitations given by the Constitution and laws.

Keywords: electronic surveillance, monitoring of employees, rights of employees, Panopticon

KAZALO

KAZALO SLIK

1 UVOD

V današnjem svetu poostrenega nadzora in prevlade varnosti nad svobodo, se sprašujem, ali se je vredno odpovedati tako velikemu kosu svobode za lažen občutek varnosti? In čigave varnosti - varnosti vseh ljudi ali varnosti tistih, ki ta nadzor uporabljajo? Važno je namreč vedeti, za koga in za kaj je nadzor tako pomemben in zakaj se ga vedno pogosteje uporablja na skoraj vsakem koraku.

Navaden državljan je dandanes spremljan z vsakovrstnim elektronskim nadzorom na vsakem koraku: na poti do službe, v službi, v trgovini, v osebnem avtomobilu, na avtobusih in lahko celo v lastnem domu. Načini elektronskega opazovanja ali nadzorovanja posameznika so z napredkom v tehnologiji finančno in prostorsko lažje dostopni in opazovani osebi skoraj nevidni. Možnost spremljanja gibanja neke osebe prek videokamere, pa tudi prek vklopljenega mobitela ali GPS-a, se sedaj v tujini zdi že vsakdanja praksa. Kako pa je z elektronskim nadzorom oseb pri nas?

V diplomskem delu se bom poglobila v elektronski nadzor zaposlenih, ki je sicer le del nadzora, ki ga ljudje doživljajo, vendar so mu podvrženi cel delavnik (osem do tudi dvanajst ur dnevno), kar predstavlja znaten del dneva.

Elektronski nadzor zaposlenih ima polno pasti in možnosti zlorabe. Te pasti bom skušala najprej prikazati s pomočjo nekaterih sociooloških teorij o nadzoru, nato pa še s pregledom pravne podlage v Sloveniji in svetu. V nadaljevanju bom predstavila več oblik elektronskega nadzora zaposlenih, ki so trenutno aktualne. Poleg definicij oblik elektronskega nadzora bom podala njihove zakonske omejitve in razširjenost uporabe pri nas in v tujini.

Za popoln oris trenutne situacije pri nas bom naredila raziskavo v dveh različnih podjetjih, kjer imajo veliko zaposlenih in kjer obdelujejo (ter hranijo) veliko količino osebnih podatkov. Pri tem se bom osredotočila na naslednja vprašanja: katere oblike elektronskega nadzora raziskovane organizacije uporabljajo; če je zakonit; ali so zaposleni z njim obremenjeni oziroma kako ga doživljajo; ali elektronski nadzor, pravno gledano, krati delavčevo osebno svobodo in pravico do zasebnosti na delovnem mestu; kaj vse se nadzoruje in kaj se zgodi z zbranimi podatki, ki jih elektronski nadzor dá.

Skušala bom ugotoviti tudi, ali so podatki zbrani tako, da lahko kakorkoli škodujejo zaposlenemu; ali preidejo v njegovo osebno mapo in mu tako potencialno škodijo; in ali je elektronski nadzor izvajan izključno zato, da zavaruje delavca in delodajalca pri potencialnih pritožbah strank, ali pa ga delodajalec uporablja še za druge namene.

Glavna omejitev pri raziskovalnem delu diplomskega dela bo najti podjetja, ki bodo pripravljena sodelovati in odgovarjati na vprašanja, ki jih večina organizacij dojema kot poslovno skrivnost.

1.1 Hipoteze

Glavni hipotezi, ki ju bom skušala v diplomskem delu dokazati ali ovreči sta:

- Elektronski nadzor zaposlenih je v teoriji z zakoni dovolj omejen, vendar se v praksi uporablja tudi nedovoljene oblike nadzora, ki jih država ne uspe pravočasno sankcionirati.
- Transparentnost nadzora zaposlenih se z uporabo modernih tehnologij zmanjšuje, možnost zlorabe pa se s strani delodajalca povečuje.

1.2 Uporabljena metodologija

Pri pisanju diplomskega dela si bom pomagala z analizo primarnih in sekundarnih virov, s primerjalno-pravno analizo, z lastnim raziskovanjem, ki bo obsegalo več intervjujev in opazovanje ter s kritično analizo zbranih podatkov.

Za te metode sem se odločila, ker me zanima tako teoretična kot praktična plat izbrane tematike. Z njihovo pomočjo se bom poglobila v sociološke in pravne vidike elektronskega nadzora ter si pridobila dovolj znanja, da bom potem v procesu raziskovanja lahko odkrila napake in ocenila celotno situacijo v sodelujočih organizacijah.

2 SOCIOLOŠKI VIDIKI ELEKTRONSKEGA NADZORA ZAPOSLENIH

V sociologiji je težko najti teorijo, ki bi se ukvarjala samo z (elektronskim) nadzorom zaposlenih. Veliko jih proučuje družbeni nadzor in njegove posledice, jaz pa sem se usmerila v nadzor ožje skupine ljudi: zaposlenih v organizaciji, zato so bile te teorije zame v veliki meri neuporabne. Čistih sociooloških teorij o nadzoru delavcev nisem našla, zato sem svoje iskanje razširila še na filozofijo. Posledično sem izbrskala teorije o Panoptikonu, o 'popolnem mestu' in o Velikem bratu.

Ugotovila sem, da se za na videz preprostimi arhitekturno-sociološko-filozofskimi idejami skrivajo teorije o popolnem nadziranju skupin ljudi in njihovega sveta. Vse navedene teorije imajo namreč isto vodilno nit: hočejo prikazati, kako se dá z izbrano vrsto nadzora[1] spremeniti ljudi in njihovo obnašanje.

Teorije sem razporedila po stopnji nadzora: od nadzora manjšega dela populacije (npr. vseh zapornikov v enem zaporu) prek nadzora večjega deleža prebivalstva (npr. celotnega mesta) do nadzora celotne države.

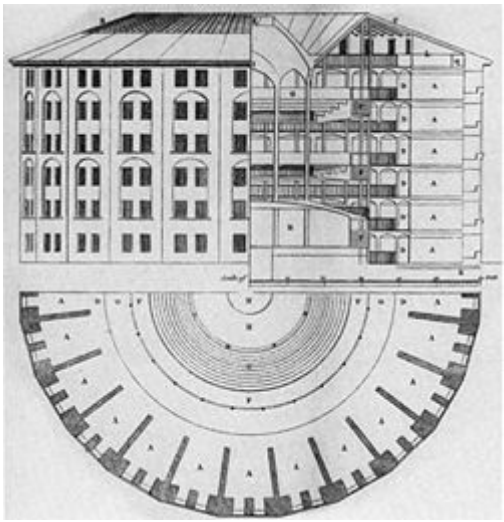
2.1 Jeremy Bentham

Leta 1791 je britanski filozof Jeremy Bentham predstavil arhitekturno inovativno idejo o novemu, modernemu, varnemu in, po njegovih besedah, humanemu zaporu: Panoptikonu[2] (v originalu: Panopticon; Slika 2.1 na naslednji strani) (Engberg 1996). Ime zapora, čigar struktura zgradbe naj bi se po njem in Foucaultu v prihodnosti uporabljala tudi za bolnišnice, šole, vojašnice in tovarne, je sestavljeno iz besede pan-, ki pomeni vse in iz besede –opticon: opazovati (Wikipedia 2008e).

[1] Ne-elektronskega (npr. s pomočjo arhitekture) ali elektronskega (s pomočjo videokamer) nadzora.

[2] Idejo o Panoptikonu je Jeremy Bentham razvil, ko je videl bratov načrt za vojaško šolo v Parizu (Wikipedia 2008e).

Slika 2.1: Panoptikon



Vir: http://en.wikipedia.org/wiki/Panopticon (19.5.2008).

Bentham si je zamislil krožno strukturo zapora, v čigar sredini bi stal opazovalni stolp. Na stolpu bi bila velika okna, s katerih bi se dalo opazovati notranjost celic, ki bi stale v krogu. Celice bi bile med seboj ločene z zidovi, na notranji (obrnjeni prosti stolpu) in zunanji strani bi bilo okno. Zunanje okno bi omogočalo vir svetlobe, tako da bi bil zapornik v celici viden opazovalcu iz opazovalnega stolpa, opazovalec pa ne bi bil viden zaporniku. Glavna ideja tega zapora je bila vidnost in opazovanje; zaporniki bi bili vedno vidni in pod nadzorom, nadzornik ali opazovalec pa ne bi bil viden, in zaradi tega mu tudi ne bi bilo treba biti neprestano prisoten. Učinek, ki ga ta nenehni nevidni nadzor sproži, je samodejno delovanje oblasti na zapornike: zapornik postane svoj ječar, ki sam regulira svoje vedénje in obnašanje (Foucault 2004, 219-221). Skozi ta načrt zapora je Bentham izpopolnil svoje utilitaristično naziranje o samokontroli posameznikov (Engberg 1996). Menil je tudi, da se dá s Panoptikonom "izboljšati moralo – ohraniti zdravje – okrepiti industrijo - … - utrditi ekonomijo - … - vse s preprosto idejo v Arhitekturi!" (Bentham v Kovačič 2006, 24).

Čeprav Panoptikona niso nikoli zgradili, je ideja o zgradbi popolnega nadzora ostala. Po Benthamovi smrti je nastalo po vsem svetu kar nekaj zaporov,[3] ki spominjajo na

[3] Za ogled teh zaporov glej: Panopticon-inspired prisons na http://en.wikipedia.org/wiki/Panopticon

panoptično strukturo, vendar so s pomočjo moderne tehnologije nekateri naredili še korak naprej[4] (Wikipedia 2008e).

2.2 Claude-Nicolas Ledoux

Vendar pa ideja o popolnem nadzoru oseb s pomočjo zgradbe oziroma gradbene strukture ni bila lastna Benthamu. Že med letoma 1775-1779 je Claude-Nicolas Ledoux razvil in predstavil idejo o 'popolnem mestu' (La cité idéale), ki bi nastalo na področju solin d'Arc et Senans (Slika 2.2). Z izgradnjo popolnega mesta je Ledoux želel prek urbanizma in arhitekture izboljšati družbo.

Slika 2.2: 'Popolno mesto'

Vir: http://en.wikipedia.org/wiki/Claude_Nicolas_Ledoux#The_Royal_Saltworks_at_ Arc-et-Senans_.281774-1779.29 (22.7.2008).

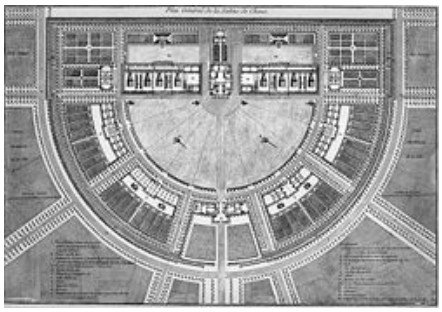
Mesto Chaux[5] pa ni bilo nikoli zgrajeno do konca zaradi francoske revolucije leta 1789. Namesto celotne krožnice zgradb so tako zgradili samo polovico kroga,[6] kjer so delovale Kraljevske soline. V sredini polkroga stoji direktorjeva hiša s kapelo, okrašena z velikim okulusom (okroglim oknom), skozi katerega je lahko direktor ob katerikoli uri dneva in noči nadzoroval delavce. Na obodu krožnice pa je postavljenih deset poslopij, v katerih so bili tovarna, administracija, bivališča delavcev in zapor (Slika 2.3, str. 13).

[4] S kontrolo vrat celic, z videonadzornim sistemom in z vgrajenimi zvočniki lahko sedaj iz opazovalnega stolpa tudi ukazujejo in obvladujejo gibanje zapornikov (Wikipedia 2008e).

[5] Tako je poimenovano to popolno mesto; Chaux je tudi drugo ime za te soline.

[6] Idealno mesto bi bilo postavljeno v obliki kroga, ki bi poleg popolne geometrične oblike predstavljal tudi simbol za harmonijo popolnega mesta, simbol harmonije skupnega dela in simbol poti sonca. Istočasno je bilo s to krožno obliko možno zagotoviti nadzor delavcev in prebivalcev popolnega mesta.

Slika 2.3: Soline d'Arc et Senans



Vir: http://en.wikipedia.org/wiki/Claude_Nicolas_Ledoux#The_Royal_Saltworks_at_ Arc-et-Senans_.281774-1779.29 (22.7.2008).

V svojem načrtu popolnega mesta je Ledoux načrtoval vsako najmanjšo podrobnost: od sodišča do 'hiše zabave' (oziroma bordela), pa tudi cerkev in veličastno krožno pokopališče. Želel je to konceptualno in konstrukcijsko zamisel o idealnem mestu prenesti v realno življenje in jo oživeti tudi drugod po državi in svetu (Copans in Neumann 2007; Wikipedia 2008a).

Smrt ga je prehitela, da bi kdaj uspel uresničiti ta načrt.

2.3 Michel Foucault

Michel Foucault, francoski filozof, sociolog, zgodovinar in kritik, je Benthamovo strukturo Panoptikona popeljal korak dlje, in jo uporabil kot metaforo modernega, vsepričujočega nadzora. Panoptična zgradba namreč lahko že samo z izgledom doseže, da so učinki nadzora stalni, da se ljudje neprestano zavedajo tega nadzora, in se zaradi tega zavedanja obvladajo kar sami (Foucault 2004, 221). Panoptikon po Foucaultu postane neke vrste stroj, ki avtomatizira in dezindividualizira oblast in posledično tvori homogene učinke nadzora ali oblasti[7] (Foucault 2004, 221-222).

[7] Odvisno od tega, kdo nadzor izvaja. Foucault namreč razširi idejo o Panoptikonu na višjo raven: na oblast, ki izvaja nadzor nad svojimi 'podložniki' (Foucault 2004, 234).

Foucault meni, da se lahko Panoptikon uporabi kot stroj za opravljanje poskusov; z njegovo pomočjo lahko preverimo na delavcih,[8] katera tehnika opravljanja določenega dela je boljša. Istočasno meni, da bi bila panoptična struktura lahko tudi aparat, ki nadzoruje svoje lastne mehanizme, saj bi, v primeru tovarne, direktor lahko neprestano opazoval, nadzoroval in usmerjal svoje zaposlene, on pa bi bil tudi brez težav opazovan[9] (Foucault 2004, 224).

Foucault je bil tudi mnenja, da je to panoptično opazovanje, ki je v moderni družbi najbolj prisotno in opazno pri zapornikih od prestajanja kazni v zaporu, prek pogojnega izpusta, javljanja policiji, nadzora učiteljev, do rehabilitacije v vsakodnevnem delu in življenju, neke vrste 'zaporniški kontinuum'. Vsi ti ljudje so namreč povezani s tem, da (namerno ali nenamerno) nadzorujejo in/ali so nadzorovani (Wikipedia 2008č). To, ob boljšem premisleku, sedaj ne velja samo za zapornike, ampak že kar za vse ljudi.

2.4 George Orwell

Britanski pisec George Orwell, s pravim imenom Eric Arthur Blair (Wikipedia 2008b), je s svojim slovitim delom 1984 predstavil javnosti novo obliko nadzora: popolni nadzor, ki nosi obraz Velikega brata. "Bila je to ena tistih podob, ki so izdelane tako, da ti oči sledijo, medtem ko se premikaš. VELIKI BRAT TE OPAZUJE, se je glasil napis pod njim." (Orwell 1967, 5)

V 1984 je Orwell opisal totalitarni sistem nove vrste. Glavna in edina stranka Stranka je z njihovim vodjo Velikim bratom in ostalimi institucijami (Ministrstvom resnice, Ministrstvom miru, Ministrstvom Ljubezni, Ministrstvom obilja, Zvezo mladine, Miselno policijo, policijskimi patrolami in najmlajšimi Vohuni) obvladovala ne samo gibanje in početje ljudi, temveč tudi njihove misli. Gibanje in pogovore je Miselna policija lahko spremljala prek "telekrana"[10](Orwell 1967, 5), ki je bila pravokotna kovinska ploščica, podobna potemnelemu ogledalu, nameščena na steno v vsakem

[8] Delavci so samo ena od navedenih skupin, ki jih Foucault omenja. Na njih sem se sklicevala predvsem zato, ker se moje diplomsko delo ukvarja z (elektronskim) nadzorom zaposlenih.

[9] V primeru kakšnega zunanjega nadzora, bi bila inšpektorju že na prvi pogled jasna celotna situacija znotraj tovarne/podjetja (Foucault 2004, 224).

[10] Telekran nas nehote spomni na sedanje videokamere in, z vidno a nepreverljivo možnostjo nadzora, na Panoptikon.

stanovanju (Orwell 1967, 5); misli pa so sistematično spremljali in ovajali tudi otroci, ki so bili vsi včlanjeni v Vohune.[11] Miselna policija, ki je lahko kadarkoli brez človekovega vedenja preiskala njegovo lastnino (Orwell 1967, 6-26), je skušala ljudi nadzorovati tudi s Strankinim najnovejšim ter najbolj prefinjenim izumom: spremembo jezika (Orwell 1967, 257-287). "Namen Novega jezika ni bil samo ta, da oskrbi sredstvo za izražanje svetovnega nazora in mentalnih navad, /…/, temveč da onemogoči vse druge načine mišljenja." (Orwell 1967, 275)

Orwellova ideja Velikega brata je sedaj bolj aktualna kot takrat, ko je izšla. Svari nas pred pretiranim nadzorom, in to ne samo na delovnem mestu, temveč na vsakem koraku. Opozarja nas tudi na to, kaj lahko peščica ljudi na oblasti z dobrim nadzornim sistemom lahko doseže. Od nas samih je odvisno, ali bomo pustili, da do tega v prihodnosti pride.

[11] "Najhujše od vsega je bilo to, da so jih s takimi organizacijami, kot so bili Vohuni, sistematično preobražali v neobvladljive male divjake, pa vendar to v njih ni budilo nikakršne težnje, da bi se uprli strankini disciplini. Nasprotno, oboževali so Stranko in vse v zvezi z njo. /…/ Vso krutost so preusmerili navzven, proti sovražnikom države, proti tujcem, izdajalcem, saboterjem, miselnim zločincem. Bilo je skoraj običajno, da so se ljudje, stari nad trideset let, bali lastnih otrok." (Orwell 1967, 25-26)

3 PRAVNI VIDIKI ELEKTRONSKEGA NADZORA ZAPOSLENIH

Pravice zaposlenih in nadzor oziroma elektronski nadzor zaposlenih hodijo z roko v roki in so določeni v mnogih zakonskih in podzakonskih aktih. V tem delu se bom posvetila predvsem Ustavi Republike Slovenije (URS; v nadaljevanju: Ustava); naštela bom tudi vse zakone, akte, priporočila, in smernice, ki vplivajo na obravnavano področje. V podrobnosti pa se bom poglobila in jih razčlenila v poglavju Vrste elektronskega nadzora zaposlenih.

3.1 Ustava Republike Slovenije

Ustava je pravni akt, ki je nad zakoni in določa osnovne pravice in svoboščine državljanov. Noben zakonski ali podzakonski akt ne sme kakorkoli posegati v pravice, pridobljene z Ustavo. To nam zagotavlja 15. člen (uresničevanje in omejevanje pravic):

> *Človekove pravice in temeljne svoboščine se uresničujejo neposredno na podlagi ustave.*
> *Z zakonom je mogoče predpisati način uresničevanja človekovih pravic in temeljnih svoboščin, kadar tako določa ustava, ali če je to nujno zaradi same narave posamezne pravice ali svoboščine.*
> *Človekove pravice in temeljne svoboščine so omejene samo s pravicami drugih in v primerih, ki jih določa ta ustava.*
> *Zagotovljeni sta sodno varstvo človekovih pravic in temeljnih svoboščin ter pravica do odprave posledice njihove kršitve.*
> *Nobene človekove pravice ali temeljne svoboščine, urejene v pravnih aktih, ki veljajo v Sloveniji, ni dopustno omejevati z izgovorom, da je ta ustava ne priznava ali da jo priznava v manjši meri.* (URS 1991, 15. člen)

Novejše sociološke teorije o pravu preučujejo dve razsežnosti ustave, ki sta pomembni tudi na področjih elektronskega nadzora zaposlenih in pravic zaposlenih do zasebnosti na delovnem mestu, in to sta: "ustava kot izraz družbenih odnosov, ki izhaja iz življenja (life in law) in ustava kot se uresničuje v življenju kot praksi (law in life)" (Kocjančič in drugi 1998, 37). To nam pove, da ustava spremlja moderni način življenja in se mu s spremembami tudi prilagaja. Kako je naša Ustava pripravljena na porast tehnologije v

varovalne in nadzorovalne namene, pa tudi kako varuje pravice zaposlenega do zasebnosti, bomo videli v pregledu pomembnejših členov Ustave.

Najpomembnejši členi v Ustavi Republike Slovenije, ki zagotavljajo varstvo posameznikove zasebnosti in intime, pa tudi varnosti, tako na delovnem mestu kot doma so:

* 34. člen (pravica do osebnega dostojanstva in varnosti):"Vsakdo ima pravico do osebnega dostojanstva in varnosti." (URS 1991, 34. člen)

Rudi Kocjančič v delu Ustavno pravo Sloveniji meni, da je potrebno to pravico razumeti v povezavi z varstvom osebne svobode in človekove osebnosti ter dostojanstva. Pravico do varnosti pa razlaga zlasti kot varstvo človekovega življenja in njegove osebne svobode (Kocjančič in drugi 1998, 116).

* 35. člen (varstvo pravic zasebnosti in osebnostnih pravic):"Zagotovljena je nedotakljivost človekove telesne in duševne celovitosti, njegove zasebnosti ter osebnostnih pravic." (URS 1991, 35. člen)

Ustava s tem členom zagotavlja nedotakljivost človekove telesne in duševne celovitosti, njegove zasebnosti ter osebnostnih pravic. Človekova telesna in duševna nedotakljivost je v Ustavi zavarovana tudi z drugimi pravicami in svoboščinami, kot so varstvo osebne svobode, prepoved mučenja, varstvo človekove osebnosti in dostojanstva in podobno. Človekova zasebnost je v Ustavi med drugim zavarovana tudi z nedotakljivostjo stanovanja, varstvom tajnosti pisem in drugih občil ter z varstvom osebnih podatkov posameznika. Osebnostne pravice pa je treba po Kocjančiču razumeti tudi kot civilnopravne pravice, ki uživajo odškodninskopravno varstvo (Kocjančič in drugi 1998, 116)

* 37. člen (varstvo tajnosti pisem in drugih občil):
  Zagotovljena je tajnost pisem in drugih občil.
  Samo zakon lahko predpiše, da se na podlagi odločbe sodišča za določen čas ne upošteva varstvo tajnosti pisem in drugih občil in nedotakljivost človekove

zasebnosti, če je to nujno za uvedbo, ali potek kazenskega postopka ali za varnost države. (URS 1991, 37. člen)

Ustavno varstvo tega člena poleg klasičnih občil, kot so zaprta pisma in telefonski pogovori, zajema tudi moderna občila, kot so telefaks, elektronska pošta in podobne. Pod določenimi pogoji Ustava dopušča omejitev pravice do varstva tajnosti pisem in drugih občil, če je to nujno v kazenskem postopku ali za varnost države (Kocjančič in drugi 1998, 116-117).

* 38. člen (varstvo osebnih podatkov):
  Zagotovljeno je varstvo osebnih podatkov. Prepovedana je uporaba osebnih podatkov v nasprotju z namenom njihovega zbiranja.
  Zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa zakon.
  Vsakdo ima pravico seznaniti se z zbranimi osebnimi podatki, ki se nanašajo nanj, in pravico do sodnega varstva ob njihovi zlorabi. (URS 1991, 38. člen)

Varstvo osebnih podatkov je tudi ena izmed oblik varstva zasebnosti posameznika. Tovrstno varstvo pojmujemo kot kup načel, pravil in ukrepov, katerih namen je preprečiti nezakonite posege v posameznikovo zasebnost in s tem v njegovo osebno in/ali družinsko življenje (Kocjančič in drugi 1998, 117). Republika Slovenija je ena izmed redkih držav, ki s svojo ustavo zagotavlja varstvo osebnih podatkov (Kocjančič in drugi 1998, 117).

Vse te pravice so pravice negativnega statusa, kar pomeni, da se z njimi preprečuje posege državnih organov v temeljne vrednote posameznika. Te pravice so znane tudi kot svoboščine, ki varujejo neponovljivost in celovitost človeka kot posameznika. Po izvoru so najstarejše pravice; izoblikovale so se v zgodovinskem procesu omejevanja državnih posegov v temeljne vrednote posameznika in so čez čas postale temeljna pravna načela (Kocjančič in drugi 1998, 111-112).

Zadnji obravnavani člen je člen 39, ki obravnava svobodo izražanja. Ta pravica spada pod politične pravice in svoboščine, katerih nosilci so praviloma državljani (Kocjančič in drugi 1998, 118).

* 39. člen (svoboda izražanja):
  Zagotovljena je svoboda izražanja misli, govora in javnega nastopanja, tiska in drugih oblik javnega obveščanja in izražanja. Vsakdo lahko svobodno zbira, sprejema in širi vesti in mnenja.
  Vsakdo ima pravico dobiti informacijo javnega značaja, za katero ima v zakonu utemeljen pravni interes, razen v primerih, ki jih določa zakon. (URS 1991, 39. člen)

Svoboda izražanja je po Ustavi zagotovljena pravica in vsebuje več pravic oziroma svoboščin, kot so: svoboda izražanja misli, govora in javnega nastopanja, svoboda tiska in drugih oblik javnega obveščanja in izražanja (Kocjančič in drugi 1998, 119).

Kako so vsi ti navedeni členi Ustave preneseni v zakone in posledično v prakso, bomo videli v nadaljevanju.

3.2 Zakonski in podzakonski akti

Zakonski in podzakonski akti, ki določajo, dovoljujejo, prepovedujejo ali kakorkoli vplivajo na oblike elektronskega nadzora zaposlenih so:

* Zakon o varstvu osebnih podatkov, ur. l. RS 94/2007, v nadaljevanju: ZVOP-1

Zakon o varstvu osebnih podatkov ureja pravice, obveznosti, načela in ukrepe, ki preprečujejo neustavne in nezakonite posege v zasebnost in dostojanstvo posameznika pri zbiranju in obdelavi osebnih podatkov. Določa pravne podlage za obdelavo osebnih podatkov v javnem in zasebnem sektorju, namene zbiranja osebnih podatkov in njihovo hrambo ter varovanje. Na področju elektronskega nadzora zaposlenih ureja video nadzor, biometrijo in evidenco vstopov in izstopov iz prostorov, njihovo dopustnost v javnem in zasebnem sektorju ter kazni v primeru kršitev z zakonom določenih varnostnih ukrepov ali možnosti uporabe (ZVOP-1 2007, 1.-101. člen). Poleg vsega

tega ZVOP-1 definira besedno zvezo osebni podatek, ki se pogosto pojavlja v diplomskem delu in je posledica izvajanja elektronskega nadzora zaposlenih, kot "katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen." (ZVOP-1 2007, 6. člen)

* Zakon o Informacijskem pooblaščencu, ur. l. RS 113/2005, v nadaljevanju: ZInfP

Z Zakonom o informacijskem pooblaščencu se v pravni red Republike Slovenije prenaša 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. Informacijski pooblaščenec je samostojni in neodvisni državni organ, ki v skrbi za nadzor nad izvajanjem zakona, ki ureja dostop do informacij javnega značaja ter inšpekcijski nadzor nad izvajanjem zakona (in drugih predpisov), ki urejajo varstvo ali obdelavo osebnih podatkov. Ta zakon je pomemben za obravnavano temo, ker določa Informacijskega pooblaščenca za organ, ki bdi nad izvajanjem Zakona o varstvu osebnih podatkov. Poleg tega je Informacijski pooblaščenec tisti, ki daje (pozitivne ali negativne) odločbe za izvajanje biometrijskih ukrepov v zasebnem sektorju in ima možnost, da delodajalce ob neprimernem elektronskem nadzoru zaposlenih kaznuje z opozorilom, z denarno kaznijo ali z ukazom odstranitve neprimernega/nedovoljenega nadzora (ZInfP 2005, 1. in 2. člen).

* Zakon o elektronskih komunikacijah, ur. l. RS 43/2004, v nadaljevanju: ZEKom

Za elektronski nadzor zaposlenih pomembno področje je zaščita tajnosti in zaupnosti elektronskih komunikacij, ki jo ureja Zakon o elektronskih komunikacijah. ZEKom definira (elektronsko) komunikacijo kot "izmenjavo in prenos informacij, ki si jih končno število strank izmenja ali pošlje s pomočjo javne komunikacijske storitve" (ZEKom 2004, 3. člen). Pod zaupnost elektronskih komunikacij šteje ZEKom tako vsebino komunikacij in podatke o prometu (na primer račune za opravljene elektronske komunikacije) kot tudi lokacijske podatke (na primer kraj telefoniranja ali kraj pošiljanja elektronskega sporočila). Prepoveduje vse oblike njihovega prestrezanja ali nadzorovanja, ki so: poslušanje, prisluškovanje, snemanje, shranjevanje in posredovanje, razen dopustnih oblik (v primeru policije ali drugih organov za zagotavljanje pomoči) (ZEKom 2004, 103. člen). Predpisuje tudi kazni v primeru

kršitev določil zakona s strani delodajalcev ali drugih uporabnikov (ZEKom 2004, 151.-155. člen).

* Zakon o zasebnem varovanju, ur. l. RS 126/2003, v nadaljevanju: ZZasV

Zakon o zasebnem varovanju govori o zasebnem varovanju ljudi in premoženja, ki ga ne zagotavlja država (ZZasV 2003, 1. člen). Predpisuje postopke za pridobivanje, ohranjanje in izgubo licenc za varnostnike, varnostne tehnike in pooblaščene inženirje varnostnih sistemov ter operaterjev varnostno-nadzornih centrov (ZZasV 2003, 16.-42. člen). Za elektronski nadzor zaposlenih pomembna tema, ki je tudi obravnavana v ZZasV, je pravica subjekta v zasebnem sektorju do video nadzora in evidence o vhodih in izhodih v poslovne prostore ter čas hrambe z elektronskim nadzorom pridobljenih podatkov (ZZasV 2003, 43. člen). V Zakonu o zasebnem varovanju je tudi člen, ki poudarja zavezanost ljudi, ki delajo na področju varovanja (od varnostnikov do operaterjev varnostno-nadzornih centrov), k molčečnosti (ZZasV 2003, 39. člen), kar je pomemben vidik varovanja osebnih podatkov, pridobljenih z elektronskim nadzorom zaposlenih.

* Zakon o dostopu do informacij javnega značaja, ur. l. RS 51/2006, v nadaljevanju: ZDIJZ-UPB2

Zakon o dostopu do informacij javnega značaja obravnava prost dostop do informacij javnega značaja, torej informacij, ki izvirajo iz delovnega področja javnega organa, v obliki dokumentov, zadev, dosjejev, registrov, evidenc in dokumentiranega gradiva, ne pa tudi (poslovnih) tajnosti (ZDIJZ-UPB2 2006, 1. in 4. člen). Ta zakon torej omogoča vpogled v pritožbe o elektronskem nadzoru, ki jih je prejel Informacijski pooblaščenec, v njegovo odločanje o biometriji in podobno.

* Zakon o javnih uslužbencih, ur. l. RS 56/2002, v nadaljevanju: ZJU

Zakon o javnih uslužbencih urejuje zaposlovanje v javnem sektorju (ZJU 2002, 1. člen). Omenja kadrovske evidence in centralno kadrovsko evidenco, ki se vodi kot informatizirana baza podatkov (ZJU 2002, 46.-51. člen). Pomembno za elektronski nadzor zaposlenih je obseg osebnih podatkov, ki so zbrani v teh evidencah (ime, priimek, EMŠO, izobrazba, prebivališče, sedanje in prejšnja delovna mesta, delovna doba, priznanja in nagrade, dovoljenje za ravnanje s tajnimi podatki in tako dalje) (ZJU

2002, 47. člen). Zasebnost javnih uslužbencev na delovnem mestu je manjša od uslužbencev v zasebnem sektorju že zaradi narave dela. Varovanje njihovih osebnih podatkov obravnava Zakon o varovanju osebnih podatkov v posebnem poglavju (glej ZVOP-1, 9. člen).

* Zakon o delovnih razmerjih, ur. l. RS 42/2002, v nadaljevanju: ZDR

Zakon o delovnih razmerjih ureja pogodbo o zaposlitvi med delodajalcem in delojemalcem. Pomembne določbe za elektronski nadzor zaposlenih s strani delodajalca so sledeče: zagotoviti mora pogoje za varnost in zdravje delavcev, varovati in spoštovati mora delavčevo osebnost in dostojanstvo, varovati mora osebne podatke zaposlenih, ščititi ter upoštevati zasebnost delavca. Delavec pa je po ZDR dolžan upoštevati navodila delodajalca, spoštovati predpise o varnosti in zdravju pri delu, obveščati delodajalca o vsaki grozeči nevarnosti za življenje ali zdravje pri delu in ne sme mu škodovati, poleg tega pa je dolžan varovati poslovne skrivnosti (Kresal in drugi 2002, 140-171). S temi določili je tako predpisana dovoljena meja (elektronskega) nadzora nad zaposlenimi in nujna meja varovanja delavca, njegove osebnosti in njegovih osebnih podatkov.

* Konvencija o varstvu človekovih pravic in temeljnih svoboščin, ur. l. RS (13.6.1994) MP, št. 7-41/1994 (RS 33/1994), v nadaljevanju: Konvencija

Konvencija o varstvu človekovih pravic in temeljnih svoboščin določa temeljne človekove pravice in svoboščine. Za elektronski nadzor zaposlenih sta najpomembnejša dva člena: osmi in deseti člen, ki določata pravico do spoštovanja zasebnosti in družinskega življenja ter svobodo govora (Konvencija 1994, 8. in 10. člen). Pomembna sta za elektronski nadzor zaposlenih, ker obravnavata pravico do spoštovanja dopisovanja oziroma korespondence in sporočanje obvestil brez vmešavanja javne oblasti (torej tudi države v vlogi delodajalca).

S Konvencijo o varstvu človekovih pravic in temeljnih svoboščin je ustanovljeno Evropsko sodišče za človekove pravice, ki je pomembno tudi na področju varovanja osebnih podatkov zaposlenih (Konvencija 1994, 19. člen). Za delodajalca ugodno določilo Konvencije je Protokol h Konvenciji o varstvu človekovih pravic in svoboščin, ki v prvem členu daje pravico vsaki fizični in pravni osebi do varovanja lastnine

(Konvencija, Protokol h Konvenciji, 1. člen), torej na nek način dopušča oblike elektronskega nadzora delovnih prostorov in zaposlenega za namen varovanja lastnine delodajalca.

* Konvencija o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov, ur. l. RS (28.2.1994)-MP, št. 3-18/1994 (RS 11/1994), v nadaljevanju: Konvencija 108

Konvencija o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov je bila v okviru Sveta Evrope sprejeta leta 1981, Republika Slovenija pa jo je ratificirala leta 1994 (Bogataj v Pirc Musar in drugi 2006, 24). Konvencija 108 določa načine pridobitve in hranjenja osebnih podatkov, o njihovi zaščiti ter varstvu posameznikov, o katerih se osebni podatki zbirajo ter obdelujejo (Konvencija 108 1994, 5. in 7. člen). Za elektronski nadzor zaposlenih postavlja temelj zaščite osebnih podatkov ter možnost vpogleda v posamezne avtomatske zbirke podatkov, ki jih morajo države podpisnice prenesti v svoj pravni red (Konvencija 108 1994, 7. in 8. člen).

* 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, ur. l. L 281 , 23/11/1995 str. 0031 – 0050, v nadaljevanju: Direktiva 95/46/ES

Direktiva 95/46/ES obravnava pravico do zasebnosti pri obdelavi osebnih podatkov, varovanje temeljnih svoboščin in pravic fizičnih oseb (torej tudi zaposlenih) in obdelavo osebnih podatkov, ki morajo biti kakovostni in primerni (ne pretirani ali napačni). Prepoveduje pa obdelavo takih podatkov, ki bi kakorkoli kazali na rasni ali etnični izvor, politična mnenja, verska ali filozofska prepričanja, pripadnost sindikatu ter obdelavo osebnih podatkov, povezanih z zdravjem ali spolnim življenjem posameznika (Direktiva 95/46/ES 1995, 1., 6. in 8. člen). Direktiva 95/46/ES je v slovenski pravni sistem prenesena z Zakonom o Informacijskem pooblaščencu in z Zakonom o varstvu osebnih podatkov (Pirc Musar in drugi 2006, 16).

* Direktiva 2002/58/ES z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij, ur. l. L 201, 31/07/2002 str. 0037 – 0047, v nadaljevanju: Direktiva o zasebnosti in elektronskih komunikacijah

Direktiva o zasebnosti in elektronskih komunikacijah dopolnjuje Direktivo 95/46/ES in usklajuje določbe držav članic, ki so potrebne za zagotovitev enakovredne ravni varstva temeljnih pravic in svoboščin, zlasti pa pravice do zasebnosti v zvezi z obdelavo osebnih podatkov na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah 2002, 1. člen). Na področju elektronskega nadzora zaposlenih je pomembna, ker določa, naj države članice s svojo zakonodajo zagotovijo zaupnost sporočil in podatkov o prometu ter prepovejo prisluškovanje, poslušanje in shranjevanje informacij, pridobljenih z elektronskim nadzorom. Istočasno se Direktiva o zasebnosti in elektronskih komunikacijah zavzema za prepoved drugih vrst nadzora ali prestrezanja komunikacij in z njimi povezanih podatkov o prometu brez privolitve osebe, ki komunikacijo opravlja (Direktiva o zasebnosti in elektronskih komunikacijah 2002, 5. člen).

* Pravilnik o metodologiji vodenja registra zbirk osebnih podatkov, ur. l. RS 28/2005, v nadaljevanju: Pravilnik

Pravilnik o metodologiji vodenja registra zbirk osebnih podatkov določa način vodenja registrov zbirk osebnih podatkov. Določa vsebino in obliko registra, način posredovanja podatkov iz katalogov ter način vodenja in objave registra (Pravilnik 2005, 1. člen). Pravilnik tudi določuje, da mora upravljalec registra (v našem primeru delodajalec) posredovati Državnemu nadzornemu organu zapise o nazivu zbirke osebnih podatkov in zapis, ali je zbirka osebnih podatkov vzpostavljena na podlagi osebne privolitve posameznika (na pogodbeni ali kakšni drugi ravni). Vsebovati mora zapis podatkov o upravljalcu, navedbo vseh vrst osebnih podatkov, ki se vodijo v zbirki, namen zbiranja teh podatkov, osebe, s katerimi bodo ti podatki dostopni in opis splošnega varovanja teh podatkov (Pravilnik 2005, 2.-4. člen).

Pravilnik o metodologiji vodenja registra zbirk osebnih podatkov je pomemben, ker se z njim varuje pridobljene osebne podatke pred zlorabo in nepooblaščeno spremembo, pridobi se standard varovanja (z navedbo pooblaščenih oseb in zapisom načina

varovanja osebnih podatkov) in ker pooblašča državni organ, da ima pregled nad zbirkami in nad osebnimi podatki, ki se zbirajo.

* Mnenja Informacijskega pooblaščenca[12] in
* mnenja Delovne skupine (iz člena) 29.[13]

Iz večine teh pravnih virov bom črpala informacije, ko bom opisovala oblike elektronskega nadzora.

[12] Mnenja Informacijskega pooblaščenca, ki bodo v nadaljevanju navedena in citirana, niso obvezujoča, razlagajo pa sporne zadeve z vidika naše zakonodaje, zato se mi zdijo dovolj verodostojna, da sem jih postavila za zglede.

[13] Mnenja Delovne skupine "niso zavezujoča, so le priporočila in neke vrste smernice, predvsem za delo Evropske komisije pri sprejemanju zakonodaje s teh področij." (Nataša Pirc Musar, 29.8.2008)

4 VRSTE ELEKTRONSKEGA NADZORA ZAPOSLENIH

Vrst elektronskega nadzora zaposlenih je veliko, trendi v svetu pa se tudi zelo hitro spreminjajo. Za večjo preglednost se bom osredotočila na najpogostejše, ki so: video nadzor, pametne kartice, prisluškovanje in/ali snemanje telefonskih pogovorov, prebiranje in sledenje elektronski pošti, blokada, opazovanje in beleženje obiskov internetnih strani, biometrija ter geolokalizacija.

Za lažje razumevanje napisanega pa bom najprej opredelila elektronski nadzor zaposlenih.

4.1 Opredelitev elektronskega nadzora zaposlenih

Besedna zveza elektronski nadzor zaposlenih se v tem diplomskem delu uporablja za nadzor s pomočjo moderne tehnologije, ki vsebuje videokamere in vse ostale pripomočke, s pomočjo katerih se lahko nadzoruje, opazuje ali kakorkoli drugače posega v zasebnost in intimo zaposlenega na delovnem mestu in njegovi bližini. Poleg dejanskega nadzora pod elektronski nadzor zaposlenih štejem še hrambo in obdelavo z nadzorom ali v procesu uvajanja nadzora pridobljenih podatkov.

4.2 Video nadzor

4.2.1 Definicija

Video nadzor je definiran kot "funkcijsko povezana specialna tehnična sredstva, ki s sprejemanjem, prenašanjem, obdelavami, arhiviranji in prikazi sprejetih slik omogočajo vizualno opazovanje in nadzor ter kasnejše analize dogajanja v varovanih prostorih." (Golob 1997, 213)

Video nadzor se izvaja s pomočjo videokamer. Z aktivnostjo (video) nadzora s kamerami so prvi začeli Nemci leta 1942, ko so dokumentirali lansiranje raket V2. Prve kamere za vsakdanjo uporabo pa so se pojavile v Združenih državah Amerike in v Veliki Britaniji v šestdesetih in sedemdesetih letih prejšnjega stoletja (Prijamovič 2008, 1).

Z napredkom tehnologije se je izboljšala tudi videokamera; postala je boljša in cenovno dostopnejša večjemu številu ljudi. Sedaj nas spremlja že na vsakem koraku: v trgovini, na mestnem avtobusu, na domofonih, na ulicah in cestah, na letališču, v službi, v šolah

ali pred njimi in tudi doma, če uporabljate spletno ali navadno kamero. Tako rekoč je videokamera postala del vsakdana modernega človeka.

Za elektronski nadzor zaposlenih se uporablja več različnih vrst kamer. Sodeč po različnih spletnih straneh, ki ponujajo prodajo in instalacijo video nadzornega sistema, je na voljo od lažnih kamer do infrardečih ter kupolastih kamer (Slike 4.1-4.4) (enaA.com 2008).

Slika 4.1: Lažna notranja kupolasta kamera

Slika 4.2: Dnevno nočna 'cevna' kamera

Vir: http://www.enaa.com/oddelki/racunalniskiDodatki/dept.asp?dept_id=2006&sortField=stNakupov&sortType=desc (19.9.2008).

4.3: Skrite kamere

4.4: Infrardeča kamera

Vir: http://www.videonadzori.net/kamere.html (19.9.2008).

4.2.2 Pravna ureditev v Sloveniji

Video nadzor je v Sloveniji pravno urejen z Zakonom o varstvu osebnih podatkov. Prvi odstavek 75. člena ZVOP-1 določa, da lahko javni in zasebni sektor izvajata video nadzor dostopa v njihove službene oziroma poslovne prostore, če je to potrebno za varnost ljudi ali premoženja, zaradi zagotavljanja nadzora vstopa ali izstopa v ali iz poslovnih prostorov ali če zaradi narave dela obstaja možnost ogrožanja zaposlenih. Odločitev sprejme pristojni oziroma pooblaščeni posameznik osebe javnega ali zasebnega sektorja. V pisni odločitvi morajo biti obrazloženi razlogi za uvedbo video nadzora. Uvedba video nadzora se lahko določi tudi z zakonom ali s predpisom, sprejetim na njegovi podlagi (ZVOP-1 2007, 75. člen).

V tretjem odstavku istega člena Zakona o varstvu osebnih podatkov je še določeno, da je potrebno o izvajanju video nadzora pisno obvestiti vse zaposlene v javnem ali zasebnem sektorja, ki opravljajo delo v nadzorovanem prostoru (ZVOP-1 2007, 75. člen; Pirc Musar 2007); delodajalec pa se mora pred njegovo uvedbo v delovnih prostorih posvetovati tudi z reprezentativnim sindikatom (ZVOP-1 2007, 77. člen).

Zakon o varstvu osebnih podatkov v drugem odstavku 74. člena tudi določa, da "mora oseba javnega ali zasebnega sektorja, ki izvaja videonadzor, o tem objaviti obvestilo. Obvestilo mora biti vidno in razločno objavljeno na način, ki omogoča posamezniku, da se seznani z njegovim izvajanjem najkasneje, ko se nad njim začne izvajati videonadzor." (Pirc Musar 2007)

V nadaljnjih odstavkih 74. člen Zakona o varstvu osebnih podatkov določa, da mora obvestilo iz prejšnjega odstavka vsebovati naslednje informacije:

1. da se izvaja video nadzor,
2. naziv osebe javnega ali zasebnega sektorja, ki ga izvaja in
3. telefonsko številko za pridobitev informacije, kje in koliko časa se shranjujejo posnetki iz videonadzornega sistema (ZVOP-1 2007, 74. člen).

V 77. členu ZVOP-1 so določila o video nadzoru znotraj delovnih prostorov. Prvi odstavek določa, da se lahko video nadzor znotraj delovnih prostorov izvaja le v izjemnih primerih: kadar je to nujno potrebno za varnost ljudi ali premoženja ali za

varovanje tajnih podatkov ter poslovne skrivnosti, tega namena pa ni možno doseči z milejšimi sredstvi (ZVOP-1 2007, 77. člen).

V drugem in tretjem odstavku sta določbi o tem, da se lahko video nadzor izvaja le v tistih delih poslovnih prostorov, kjer je potrebno varovati interese iz prejšnjega odstavka in da je prepovedano izvajati tovrstni nadzor v delovnih prostorih izven delovnega mesta, zlasti v garderobah, dvigalih in sanitarnih prostorih (ZVOP-1 2007, 77. člen).

4.2.3 Video nadzor zaposlenih v Sloveniji

O kršitvah zakonskih določil o video nadzoru v letu 2007 poroča Informacijski pooblaščenec sledeče:

> *Pri opravljanju inšpekcijskega nadzora nad izvajanjem videonadzora je bila tudi v letu 2007 najpogosteje ugotovljena nepravilnost, da izvajalci videonadzora niso objavili ustreznih obvestil o izvajanju videonadzora, predstojniki pa pred začetkom izvajanja videonadzora niso izdali ustrezne pisne odločitve za izvajanje videonadzora oziroma v tej odločitvi niso pojasnili razlogov za njegovo uvedbo. Delodajalci zaposlenih pred začetkom izvajanja videonadzora o tem niso pisno obvestili, velikokrat pa je bilo ugotovljeno, da izvajalci videonadzora za evidenco posnetkov videonadzornega sistema niso zagotovili kataloga zbirke osebnih podatkov in teh podatkov niso posredovali Informacijskemu pooblaščencu*. (Pirc Musar 2008a)

Blaž Pavšič, raziskovalec pri Informacijskem pooblaščencu, mi je povedal, da se zgoraj omenjene kršitve določil ZVOP-1 različno obravnavajo in da je kazen za kršitev odvisna od okoliščin in od inšpektorja, ki primer obravnava. Delodajalec v primeru napačnega video nadzora lahko dobi opomin ali opozorilo, plača globo (za vsako kršitev se plača globa; če je zaznanih več enakih kršitev se globe seštevajo), ali pa inšpektor ugotovi nadaljevalni prekršek. Pripomnil je tudi, da je spremembam v zakonodaji treba slediti, še posebej pa na področju varstva osebnih podatkov zaposlenih (Blaž Pavšič, 27.8.2008).

Kakšne so lahko posledice kršitev določil Zakona o varstvu osebnih podatkov o video nadzoru, pa si lahko ogledamo na primeru RTV Slovenije: sindikat RTV Slovenija je svoje delodajalce prijavil pri Informacijskemu pooblaščencu, ker se delodajalec pred

uvedbo video nadzora ni posvetoval z reprezentativnim sindikatom in še zaradi nekaterih manjših kršitev, povezanih z video nadzorom. Informacijski pooblaščenec je ugotovil, da video nadzor ni bil nameščen pravilno in v skladu z Zakonom o varstvu osebnih podatkov, zato je izdal dopolnilno odločbo, da se mora na vseh delovnih mestih na RTV Sloveniji video nadzor med delovnim časom prenehati izvajati (Cerar 2006).

4.2.4 Video nadzor zaposlenih v tujini

V Združenih državah Amerike je lani kar oseminštirideset odstotkov podjetij, ki je sodelovalo v raziskavi o elektronskem nadzoru zaposlenih (2007 Electronic Monitoring & Surveillance Survey), uporabljalo video nadzor za preprečevanje tatvin, nasilja in sabotaž; le sedem odstotkov pa je video nadzor uporabljalo zgolj za nadzor zaposlenih in njihovih delovnih dosežkov. Večina od delodajalcev je, v primeru nadzora za varovanje lastnine in ljudi oseminsedemdeset odstotkov, pri nadzoru zaposlenih za povišanje produktivnosti pa devetinosemdeset odstotkov, svoje zaposlene o video nadzoru vnaprej opozorilo (Business Wire 2008). Kljub temu je zaskrbljujoča informacija, da ostali delodajalci svojih zaposlenih o izvajanju video nadzora niso obvestili.

V Evropski uniji ima večina držav članic že sprejeto zakonodajo na področju varovanja zasebnosti in omejevanja oziroma dovoljenega video nadzora na delovnem mestu. Večinoma se mora za uvedbo video nadzora vnaprej dobiti dovoljenje ali soglasje od državnega organa; pomembno pa je tudi to, da so zaposleni o izvajanju video nadzora na delovnem mestu obveščeni (ARTICLE 29 – Data Protection Working Party 2004, 9 in 25).

V Nemčiji pripravljajo vedno nove predpise, s katerimi varujejo delavčevo zasebnost; po njihovi zakonodaji je tako nesprejemljivo nadzorovanje in spremljanje zaposlenih z video nadzorom, če za to delodajalec nima upravičenega razloga. V primeru video nadzora za spremljanje delovnega procesa ali za vzdrževanje varnosti je tovrstni elektronski nadzor zaposlenih dovoljen, vendar moja biti delavci o njegovem izvajanju obveščeni (Cvetko 1999, 132-133).

Zanimiv je podatek, da je po številu nadzornih videokamer na prebivalca, ne le na zaposlenega, vodilna Velika Britanija, saj ima eno kamero na štirinajst prebivalcev, kar

pomeni, da imajo v celoti okoli 4,5 milijonov kamer nameščenih povsod po državi (Prijamovič 2008, 1).

4.3 Pametne kartice

4.3.1 Definicija

Pametno kartico je leta 1974 je izumil francoski novinar Juan Moreno. Narejena je iz plastike, njena posebnost pa sta vgrajeni mikroprocesor in pomnilnik. Nanjo se lahko shrani osebne podatke, identifikacijo in podrobnosti bančnega računa, tako da jo lahko uporabljamo kot kreditno[14] ali debetno[15] kartico. Na kartico nakažemo denar, ki ga potem elektronsko porabimo, nato pa po potrebi naložimo novega (Wikipedia 2008d).

S pametno kartico v vsakdanjem jeziku poimenujemo tudi kartice, ki nimajo v celoti istih lastnosti kot 'originalna' pametna kartica; tako se čip kartice, brezkontaktne kartice pa tudi RFID kartice[16] skrivajo za imenom pametna kartica.

S pametno kartico so običajno omogočeni vhodi in izhodi v poslovno stavbo, pa tudi prehodi v notranjosti. Zaposleni imajo namreč omogočene prehode do sektorjev oziroma do tistih nadstropij ali sob, do koder imajo pooblaščen vstop. Če dovoljenja za dostop nimajo, se morajo obrniti na varnostno ali na kadrovsko službo, da se jim začasno (ali za stalno)[17] poveča pooblastila dostopa. Pametne kartice se uporabljajo tudi pri procesu evidentiranja prihodov in odhodov na delo.

4.3.2 Pravna ureditev v Sloveniji

V slovenski zakonodaji se pametne kartice ne pojavijo, pojavi pa se njihova funkcija: evidenca vstopov in izstopov iz prostorov. Kartice se med seboj razlikujejo po funkciji:

[14] "Kreditna kartica je kartica, kjer se nakup v okviru odobrenega limita poravnava s časovnim zamikom v višini izbrane vrednosti 10, 20 ali 33 odstotkov v zaporednih mesečnih obrokih. To pomeni, da se mesečno poravnava le del obveznosti v izbranem deležu in ne celoten nakup." (Konstanca Rettinger, 7.9.2008)

[15] "Debetna kartica je kartica osebnega računa, ki omogoča tekoče opravljanje transakcij plačilnega prometa in dvig gotovine iz osebnega računa (TRR), pri čemer je osebni račun obremenjen z izvedeno transakcijo takoj, brez zamika plačila." (Konstanca Rettinger, 7.9.2008)

[16] RFID je kratica za radiofrekvenčno identifikacijo (http://www.spica.si/, 4.9.2008).

[17] Dostop je odvisen od delovnih nalog uslužbenca in njegovih pooblastil.

nekatere namreč beležijo prihode, odhode in prehode same, nekatere pa pri vhodih in izhodih podajo identifikacijo lastnika kartice in se nato podatki zabeležijo v računalniški program, ki nudi podporo čitalcem pametnih kartic.

Evidenca vstopov in izstopov iz prostorov je v slovenskem pravu določena z 82. členom Zakona o varstvu osebnih podatkov, ki določa, da delodajalci javnega ali zasebnega sektorja lahko vodijo evidenco vstopov in izstopov za namene varovanja premoženja, življenja ali telesa posameznikov ter reda v poslovnih prostorih. Pri vodenju evidenci lahko delodajalec (ali v primeru obiskovalca: institucija) zahteva vse ali nekatere osebne podatke (ime, priimek, vrsto in številko osebnega dokumenta, naslov stalnega ali začasnega prebivališča in zaposlitev ter uro vstopa/izstopa) ter razlog vstopa/izstopa. Po potrebi lahko osebne podatke preveri z osebnim dokumentom posameznika. Tako pridobljeni osebni podatki se lahko hranijo najdlje tri leta, nato pa se morajo izbrisati ali na kak drug način uničiti (seveda če zakon ne določa drugače) (ZVOP-1 2007, 82. člen).

Najvišja globa, ki jo določa Zakon o varstvu osebnih podatkov, je od 2.080 do 4.170 evrov za tiste pravne osebe, samostojne podjetnike ali posameznike, ki evidence po preteku treh let ne uničijo ali izbrišejo (ZVOP-1 2007, 101. člen).

4.3.3 Stanje v Sloveniji in svetu

Težko je oceniti, koliko delodajalcev uporablja pametne kartice za dostop do poslovnih prostorov in za evidenco vhodov in izhodov za zaposlene, ker v Sloveniji še ni bilo izvedene nobene raziskave v tej smeri. Po lastnih izkušnjah pa lahko sklepam, da večina podjetij, ki se ukvarja z bančništvom, komunikacijami, informacijsko tehnologijo, varnostjo in tako dalje, pametne kartice uporabljajo. Podobno je z uporabo pametnih kartic v tujini.

4.4 Prisluškovanje telefonskim klicem in njihovo snemanje

4.4.1 Pravna ureditev v Sloveniji in svetu

Vprašanja o prisluškovanju in snemanju telefonskih pogovorov oziroma do zasebnosti komunikacij na delovnem mestu se je prva lotila Konvencija o varstvu človekovih pravic in temeljnih svoboščin. Po osmem členu Konvencije ima vsak posameznik pravico do dopisovanja, v katero se javna oblast ne sme vmešavati, razen če je to določeno z zakonom ali če je nujno zaradi državne varnosti (Konvencija 1994, 8. člen).

Nadzorovanje telefonskih klicev, četudi omejeno na 'datum, čas in trajanje klica' ter 'klicane številke', predstavlja kršitev 8. člena konvencije, saj so ti podatki 'sestavni del telefonskega klica'. Kršitev 8. člena konvencije torej niso le nezakoniti prisluhi oziroma prestrezanje vsebine elektronskih komunikacij. Četudi so informacije o telefonskih klicih pridobljene legalno v obliki telefonskega računa, nadzorovanje in analiziranje klicev še zmeraj predstavlja kršitev 8. člena konvencije. Še več, kršitev istega člena predstavlja tudi shranjevanje teh podatkov. Pri tem ni pomembno, da podatki niso bili razkriti ali uporabljeni v disciplinskem oziroma kakršnemkoli drugem postopku. (Caf 2008)

Ta člen Konvencije je upoštevalo britansko sodišče, ko je razsojalo v primeru Halford proti Veliki Britaniji. Predmet obravnave je bilo prestrezanje telefonskih klicev delavca na delovnem mestu. Sodišče je v sodbi zapisalo, da je prisluškovanje in/ali prestrezanje telefonskih pogovorov zaposlenega kršitev osmega člena Konvencije o varstvu človekovih pravic in temeljnih svoboščin. Telefonski pogovori iz poslovnih prostorov namreč spadajo pod 'zasebno življenje' in 'dopisovanje', kot so definirani v osmem členu Konvencije (ARTICLE 29 – Data Protection Working Party 2002, 8).

(Zasebno) dopisovanje je v sodobnem svetu dobilo razširjen pomen; pod ta pojem spadajo sedaj tako pisma kot poslovni ali zasebni telefonski klici in elektronska pošta, poslana iz službenega računalnika (ARTICLE 29 – Data Protection Working Party 2002, 8).

Prisluškovanje telefonskim klicem in njihovo snemanje v Sloveniji pa ureja tudi Zakon o elektronskih komunikacijah. ZEKom v petem odstavku 103. člena pravi, da so vse oblike nadzora ali prestrezanja, kot so poslušanje, prisluškovanje, snemanje, shranjevanje in posredovanje komunikacij (njihove vsebine, podatkov o prometu in o lokaciji ter dejstva in okoliščine neuspešnih poskusov vzpostavljanja zvez) prepovedane, razen če je to dovoljeno ali če je taka oblika nadzora ali prestrezanja potrebna za prenos sporočil - na primer za SMS sporočila in podobno (ZEKom 2004, 103. člen).

Sedmi odstavek istega člena pa pravi, da je dovoljeno snemanje komunikacij v okviru zakonite poslovne prakse z namenom, da se zagotovijo dokazi o tržni transakciji ali katerikoli drugi poslovni komunikaciji. Dovoljeno je tudi snemanje telefonskih klicev v

okviru organizacij, ki sprejemajo klice v sili, in to zaradi njihove registracije lažje identifikacije in reševanja (ZEKom 2004, 103. člen).

4.4.2 Stanje v Sloveniji in svetu

V Sloveniji se je zadnja večja afera v zvezi s pretiranim elektronskim nadzorom zaposlenih na področju zasebnosti telefonskih pogovorov in posledično kršitvijo človekovih pravic na delovnem mestu zgodila v začetku letošnjega leta. V to afero je bilo vključeno Ministrstvo za zunanje zadeve in eden ali več zaposlenih z istega Ministrstva. Začelo se je s posredovanjem internega dokumenta iz elektronskega sistema Ministrstva medijem. Ministrstvo za zunanje zadeve je odredilo notranji nadzor zaradi kršitve obveznosti diplomatov. S pregledom izhodnih in dohodnih klicev v okviru telefonske centrale stacionarnega omrežja Ministrstva in nekaterih primerjav javno dostopnih številk so odvzeli službeni namizni računalnik enemu od osumljencev (RTVSLO.SI 2008).

Ko je celotna zadeva prišla v javnost, je Informacijski pooblaščenec dvema zaposlenima na ministrstvu za zunanje zadeve sporočila, da sta zaradi nezakonite obdelave prometnih podatkov telefonskih klicev zaposlenih na Ministrstvu osumljena prekrška (Dnevnik 2008). Na dokončen razplet afere še čakamo.

Pred skoraj desetimi leti, leta 1999, je v Nemčiji že bilo prepovedano prisluškovanje v katerikoli obliki, saj je pomenilo kršitev splošnih osebnostnih pravic. Prepovedano je bilo tudi v primeru, ko je delodajalec skušal preprečiti uporabo službenega telefona za zasebne pogovore. V Izraelu je bila podobna situacija: nadzor nad telefonskimi pogovori zaposlenega ni bil dopusten (Cvetko 1999, 132-134). Situacija se v teh državah, in tudi v (ostalih) državah Evropske unije, za zasebnost zaposlenih ni poslabšala.

V Ameriki pa je stanje drugačno. Leta 2007 je šest odstotkov anketiranih delodajalcev[18] odpustilo zaposlene zaradi zlorabe službenega telefona ali zaradi njegove zasebne uporabe. Petinštirideset odstotkov delodajalcev je nadzorovalo klicane številke delavca in čas klicanja, šestnajst odstotkov pa je telefonske pogovore kar snemalo. Večina

[18] Rezultati ankete so podani v raziskavi o elektronskem nadzoru zaposlenih (2007 Electronic Monitoring & Surveillance Survey).

delodajalcev (štiriinosemdeset odstotkov) je sicer opozorila podrejene o nadzorovanju službenega telefona, vendar jim učinek grožnje nadzorovanja zaposlenih ni zadostoval, zato so telefonskim pogovorom redno prisluškovali (Business Wire 2008).

4.5 Elektronska pošta in internet

4.5.1 Pravna ureditev v Sloveniji

Ker sta elektronska pošta in internet močno povezana, ju bom obravnavala skupaj. Varuje in obravnava ju isti osmi člen Konvencije o varstvu človekovih pravic in temeljnih svoboščin, ki obravnava zasebnost telefonskega pogovora na delovnem mestu. Kako pa je v slovenskem pravnem prostoru?

Informacijski pooblaščenec o elektronski pošti in varovanju njene vsebine meni, da

> */.../ elektronski naslov posameznika načeloma lahko pomeni osebni podatek (izjema bi bila, četudi en elektronski naslov v takšni zbirki ne bi bil osebni podatek), več elektronskih naslovov posameznikov pa se da tudi urediti v strukturiran niz podatkov, saj se jih da obdelovati po abecednem vrstnem redu, po datumu prejema ali oddaje, po velikosti ipd. Pogosto se da iz vhodne in izhodne elektronske pošte (predvsem iz podatkov o pošiljatelju in po navedeni zadevi – subject) ugotoviti tudi druge osebne podatke posameznika, kot so zdravstveno stanje posameznika, versko prepričanje (janez.novak@rkc.si), politično pripadnost (janez.novak@lds.si ali sds.si ali sns.si, sindikalno pripadnost (joze.novak@sindikatxy.si) (vsi ti podatki so tudi občutljivi osebni podatki), sorodstvena (npr. Subject/Zadeva: Prosim te za sestrsko uslugo) in drugačna razmerja, premoženjsko stanje (npr. Subject/Zadeva: Kdaj bo nakazilo – sem brez denarja) itd.* (Pirc Musar 2006b)

Informacijski pooblaščenec pravi tudi, da:

> */o/dprta dilema pa ostaja ob vprašanju, kakšno stopnjo zasebnosti lahko delojemalec na delovnem mestu upravičeno pričakuje in kdaj pomeni poseg v komuniciranje zaposlenega poseg v nedotakljivost njegove zasebnosti. V takšni situaciji je na eni strani prisoten interes delodajalca, ki ima pravico do oblasti*

nad svojimi sredstvi in pravico, da nadzira, ali je ta oprema uporabljena skladno z namenom, za katerega je bila zaposlenemu dana v uporabo. Na drugi strani pa obstaja interes posameznika (zaposlenega), ki utemeljeno pričakuje določeno stopnjo zasebnosti in zaupnosti na delovnem mestu /.../. Da ima delavec pravico do zasebnosti na delovnem mestu je poudarilo tudi Kasacijsko sodišče Francije (Pooblaščenec opozarja, da primer navaja zgolj kot zanimivost, nanj pa se zaradi nepristojnosti kasacijskega sodišča v Republiki Sloveniji ne opira). To je zapisalo, da ima delavec tudi med delovnim časom in na delovnem mestu pravico do spoštovanja zasebnega življenja, vključno s pravico do tajnosti občil. Delodajalec, ki bere sporočila, ki jih zaposleni pošilja ali sprejema preko službenega računalnika, krši temeljne pravice delavca, kot jih določa 8. člen EKČP[19] *... Uporaba računalniške tehnologije resda že sama po sebi predstavlja in omogoča izvajanje nadzora nad zaposlenimi s strani nadrejenih, vendar pa je nujno, da kljub oženju zasebnega prostora na delovnem mestu delček zasebnega življenja – tako pomemben za svobodo in osebnost posameznikov – preživi tudi na delovnem mestu ... Čeprav je tehnično povsem mogoče, da delodajalci, zato da bi se izognili različnim težavam in zlorabam, delavcu prepovedo uporabo službenih računalnikov v osebne namene (in izvajanje prepovedi nadzirajo), je tovrstna prepoved – kot ugotavljajo strokovnjaki – v 21. stoletju povsem nerealna*. (Pirc Musar 2006b)

Zaključek Informacijskega pooblaščenca se glasi:

V skladu z vsem navedenim delodajalec torej nima nikakršne pravne podlage, da lahko vpogleda v t. i. prometne podatke o elektronski pošti (torej, kdo vam je elektronsko pošto poslal, oziroma komu ste jo poslali vi). Seveda pa to ne pomeni, da vam ne more omejiti uporabe vašega službenega elektronskega naslova, če bi se iz drugih razlogov (ne z vpogledom v zasebno pošto, pač pa denimo na podlagi odzivov tretjih oseb na vaša sporočila, počasno delovanje omrežja zaradi pošiljanja slikovnih ali zvočnih datotek, povečano število virusov ...) izkazalo, da vašega elektronskega naslova ne uporabljate v skladu z vsem

[19] EKČP je kratica za Evropsko konvencijo o človekovih pravicah in je drugo ime za Konvencijo o varstvu človekovih pravic in temeljnih svoboščin (Kuhelj 2004, 12).

navedenim in v skladu s politiko delodajalca glede uporabe službenih sredstev. Kot je že navedeno, sta namreč oprema in službeni elektronski naslov last delodajalca, delavec pa ima kot imetnik zgolj pravico do uporabe; zato lahko delodajalec prosto omejuje dostop do službenega elektronskega naslova. (Pirc Musar 2006b)

Za odločitev za prosti dostop do vseh internetnih strani (ali za blokiranje določenih domen) je odgovoren delodajalec. Delovna skupina 29 priporoča preventivo in svari pred nadzorovanjem dostopa internetnih strani, kjer dá delodajalec svojim zaposlenim proste roke. Delovna skupina predlaga, da se s preventivami, kot je blokiranje nekaterih nezaželenih ali škodljivih spletnih strani ali z opremo z opozorili omejenega dostopa delavce odvrne od nedovoljene uporabe interneta. Poleg tega Delovna skupina 29 meni, da taki ukrepi niso nujno potrebni, saj se z vpogledom na dostopane strani delodajalec lahko prepriča, da je uporaba interneta v zasebne namene kratka, včasih pa tudi nezaželena s strani delavca (na primer zaradi lažnega predstavljanja določenih spletnih strani) (ARTICLE 29 – Data Protection Working Party 2002, 24-25).

4.5.2 Stanje v Sloveniji in svetu

Večina slovenskih delodajalcev uporablja blokado neprimernih spletnih vsebin, kot so pornografija, kupovanje po spletnih trgovinah, dražbe, iskanje dela, orožje, kockanje in rasizem (Kavran 2004) ali tistih spletnih strani, ki predstavljajo grožnjo upočasnitve računalniškega sistema ali okužbe z virusi.

Pritožb čez delodajalce zaradi pregledovanja elektronske pošte pa je v Sloveniji veliko. Pri zahtevi za pregledovanje elektronske pošte gre namreč za navzkrižje interesa delodajalca, ki ima pravico, da nadzoruje, ali je službena oprema zaposlenega uporabljena skladno z namenom, za katerega mu je bila dana v uporabo, ter interesa zaposlenega, ki na delovnem mestu pričakuje določeno stopnjo zasebnosti in zaupnosti. Delodajalec nima pravne podlage za vpogled v prometne podatke o elektronski pošti zaposlenih (kdo je elektronsko pošto poslal komu). Z vpogledom v te podatke delodajalec krati pravico zaposlenega do varstva osebnih podatkov, z vpogledom v vsebino elektronske pošte pa krati tudi pravico do zasebnosti in pravico do tajnosti občil, ki sta varovani tudi z ustavo (Informacijski pooblaščenec 2007, 47).

Nezakonita obdelava prometnih podatkov se kaznuje po ZVOP-1 (Blaž Pavšič, 27.8.2008); zagrožene kazni pri ugotovitvi teh prekrškov pa so od 4.170 do 12.510 evrov (ZVOP-1 2007, 91. člen).

V Združenih državah Amerike, sodeč po raziskavi o elektronskem nadzoru zaposlenih (2007 Electronic Monitoring & Surveillance Survey), so delodajalci najbolj zaskrbljeni zaradi neprimerne uporabe interneta na delovnem mestu. Šestinšestdeset odstotkov delodajalcev zato nadzira spletne povezave svojih zaposlenih, petinšestdeset odstotkov podjetij pa neprimerne povezave na internetu kar zablokira. Največ jih zablokira strani s seksualno, romantično ali pornografsko vsebino (Business Wire 2008).

4.6 Biometrija

4.6.1 Definicija

Beseda biometrija izhaja iz starogrške besede bios-, ki pomeni življenje in –metron: meritev (Informacijski pooblaščenec 2008a). Biometrija je torej veda "o načinih prepoznave ljudi na podlagi njihovih telesnih, fizioloških ter vedenjskih značilnosti, ki jih imajo vsi posamezniki, so edinstvene in stalne za vsakega posameznika posebej in je možno z njimi določiti posameznika." (Informacijski pooblaščenec 2008a)

Biometrija je danes samo eden izmed načinov ugotavljanja oz. preverjanja identitete, vendar, glede na to, da preverja 'tisto, kar oseba je',[20] tudi najbolj učinkovit. Največkrat se biometrija izvaja z uporabo prstnega odtisa, šarenice, očesne mrežnice, obraza, ušesa in DNK.[21] Takšen način preverjanja identitete posameznika ima prednost pred ostalimi v tem, da se biometrične lastnosti načeloma ne spreminjajo, se ne morejo izgubiti in, najpomembneje, težko jih je posnemati ali reproducirati (Informacijski pooblaščenec 2008a).

[20] Osebi lastna vedenjska in/ali telesna značilnost.

[21] V "Veliki Britaniji se je izkazalo, da imata lahko dve osebi enak celo del zapisa DNK (v konkretnem primeru na šestih mestih), za kar je sicer teoretično izračunana verjetnost kar 1:37.000.000. Zato je na mestu opozorilo, da biometrija tudi s tega vidika ni vsemogočen in nezmotljiv način identifikacije in ji zato ne gre slepo zaupati." (Informacijski pooblaščenec 2008a)

4.6.2 Pravna ureditev v Sloveniji

Biometrija je v Sloveniji zakonsko obravnavana v 78., 79., 80. in 81. členu Zakona o varstvu osebnih podatkov (ZVOP-1 2007, 78.-81. člen). Zakon loči med preverjanjem identitete posameznika (istovetnostjo) in med izvrševanjem identifikacije posameznika (prepoznavo), vendar oba postopka poimenuje biometrični ukrep (Informacijski pooblaščenec 2008a).

V Zakonu o varstvu osebnih podatkov so biometrični ukrepi dovoljeni v javnem sektorju le, če so določeni z zakonom, in če:

- so nujni za varnost ljudi ali premoženja ali

- za varovanje tajnih podatkov

- za varovanje poslovnih skrivnosti in

- če jih ni možno doseči z milejšimi sredstvi (ZVOP-1 2007, 79. člen).

V zasebnem sektorju so pogoji za izvajanje biometrije sledeči:

- če so nujno potrebni za opravljanje dejavnosti ali

- za varnost ljudi in premoženja ali

- za varovanje tajnih podatkov ali

- za varovanje poslovnih skrivnosti (ZVOP-1 2007, 80. člen).

Biometrijske ukrepe lahko delodajalec izvaja samo nad svojimi zaposlenimi in še to, če so bili o tem vnaprej pisno obveščeni (ZVOP-1 2007, 80. člen). V tem zakonu obstaja še eno varovalo: delodajalec, ki želi izvajati biometrijo, mora pred uvedbo te tehnologije posredovati Informacijskemu pooblaščencu opis nameravanih ukrepov in vzroke za njihovo uvedbo. Informacijski pooblaščenec nato v svoji odločbi obvesti delodajalca o svoji odločitvi. Če se izvaja biometrične ukrepe brez dovoljenja Informacijskega pooblaščenca je prekršek; zagrožena globa je od 4.172,93 do 12.518 evrov za pravno osebo in od 1.251,88 do 2.086,46 evrov za odgovorno osebo (Informacijski pooblaščenec 2008a).

4.6.3 Stanje v Sloveniji

Po pregledu evidence Informacijskega pooblaščenca sem ugotovila, da je od leta 2005 kar 50 podjetij zaprosilo za odločbo za izvajanje biometričnih ukrepov (Informacijski pooblaščenec 2008b), enemu podjetju pa je leta 2006 zaradi zaznanih nepravilnosti pozitivna odločba prenehala veljati. Delodajalec, pri katerem je bila zaznana kršitev, je moral po odločbi prenehati uporabljati biometrično prepoznavo zaposlenih in odstraniti vse biometrične čitalce (Informacijski pooblaščenec 2008e).

Leta 2005 je Informacijski pooblaščenec presojal o sedmih prošnjah za uvedbo biometrije (od sedmih je zavrnil le dve), leta 2006 o enajstih (od tega jih je pet zavrnil, tri ugodil in tri ugodil le delno), leta 2007 pa jih je obravnaval kar devetindvajset. V celoti je ugodil osemnajstim, dvema le delno, devet jih je zavrnil. Letos je Informacijski pooblaščenec do 3. septembra 2008 obravnaval le tri prošnje (Informacijski pooblaščenec 2008b): ugodil je podjetjema Actual Informacijske tehnologije d. o. o. (Informacijski pooblaščenec 2008d) in Shell Adria d. o. o. (Informacijski pooblaščenec 2008c); podjetju CGP, cestno gradbeno podjetje d. d. pa je ugodil le delno (Informacijski pooblaščenec 2008č).

Po številu prošenj sodeč je bilo za biometrijo največ zanimanja leta 2007, letošnje leto pa je drastično upadlo. Za to je mogočih več vzrokov: da so vsa podjetja, ki so se zanimala za to tehnologijo, svojo prošnjo že oddala in bila bodisi uslišana v celoti bodisi delno. Drugi vzrok je lahko ta, da leta 2008 še ne moremo v celoti ocenjevati, ker se še ni izteklo; tretji pa, da so se morda podjetja za enkrat odločila za uvedbo alternativnih vrst elektronskega nadzora zaposlenih, ki niso tako invazivni in ki so predvsem cenejši.

4.6.4 Stanje v svetu

Delovna skupina 29 v svojem delovnem dokumentu o biometriji poroča o primerih po Evropi, kjer so želeli uvesti različne biometrične ukrepe, in to ne samo za zaposlene, temveč tudi za stranke. V Franciji je, na primer, odgovorni organ zavrnil uporabo prstnega odtisa, ki bi omogočal vstop otrok (in zaposlenih) v šolsko jedilnico, strinjal pa se je z uporabo zunanjega obrisa dlani. V Angliji pa takemu ukrepu - identifikaciji in omogočanju prehoda s prstnim odtisom učenca – odgovorni organi niso nasprotovali (ARTICLE 29 – Data Protection Working Party 2003, 7).

Na Portugalskem so želeli na neki fakulteti uvesti biometrične ukrepe za nadzor točnosti profesorjev tudi za dneve, ko niso predavali. Ukrep je bil zavrnjen zaradi neproporcialnosti in prekomernosti (ARTICLE 29 – Data Protection Working Party 2003, 7).

V Združenih državah Amerike so naredili korak dlje pri storitvah za stranke. Že kar šest odstotkov vseh podjetij uporablja eno od oblik biometrije. Pri West Seattle Thriftway (trgovina z živili)[22] so uvedli možnost biometričnega plačila: nakupovalec položi svoj kazalec na skener, ki v bazi registriranih kupcev poišče in preveri podatke, zabeleži opravljen nakup in stranki izstavi račun. Pri McDonaldsu so poskusno uvedli plačilo s pomočjo biometrije, Qantas Airways pa razvija samopostrežni prijavni sistem z uporabo prstnega odtisa ter razpoznavo obraza in irisa[23] s pomočjo skenerja. ING Direct (banka, ki posluje prek spleta, telefona in elektronske pošte)[24] pa je že uvedla možnost preverjanja identifikacije stranke s prstnim odtisom (Brennan 2001).

Delovna skupina 29 pa poroča, da podjetja na področju elektronskega nadzora zaposlenih in varovanja tako poslovne zgradbe kot lastnine, poleg biometrije uvajajo še dodatne varnostne ukrepe, s katerimi se še dodatno prepričajo o istovetnosti zaposlenega. To naredijo na primer s kombinacijo biometrije, pametne kartice in gesla (na primer PIN-a ali česa podobnega) ali z združevanjem dveh ali več biometričnih identifikatorjev (na primer: prepoznava obraza in glasu) (ARTICLE 29 – Data Protection Working Party 2003, 3-4). Ostale podatke o podjetjih, ki uporabljajo biometrijo kot del elektronskega nadzora zaposlenih, je težko pridobiti.

4.7 Geolokalizacija

4.7.1 Definicija

Geolokalizacija pomeni ugotavljanje podatkov o lokaciji posameznika. V drugem členu Direktive 2002/58/ES o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij so podatki o lokaciji opredeljeni kot "vsakršni podatki, obdelani v elektronskem komunikacijskem omrežju, ki podajajo zemljepisni položaj

[22] Več o West Seattle Thriftway na: http://www.westseattlethriftway.com/.

[23] Beseda iris je grškega izvora in pomeni očesno šarenico (Bunc 1963, 201).

[24] Več o ING Direct na: http://home.ingdirect.com/.

terminalske opreme uporabnika javno razpoložljive elektronske komunikacijske storitve" (ČLEN 29 Delovna skupina za varstvo osebnih podatkov 2005, 2).

Geolokalizacijo se dá opraviti s pomočjo elektronskih sledi, ki jih puščajo avtomati za izdajo vozovnic v transportnem sektorju, GPS,[25] bančne kartice, mobilni telefoni, pa tudi osebni računalniki (ČLEN 29 Delovna skupina za varstvo osebnih podatkov 2005, 2).

4.7.2 Pravna ureditev v Sloveniji

Podatki, ki se jih pridobi z geolokalizacijo, se nanašajo na določeno ali določljivo osebo, zato zanje veljajo določbe o varstvu osebnih podatkov iz Direktive Evropskega parlamenta in Sveta 95/46/ES (ČLEN 29 Delovna skupina za varstvo osebnih podatkov 2005, 4). V tej Direktivi so postavljeni standardi varovanja osebnih podatkov pri njihovi obdelavi in o prostem pretoku teh podatkov.

Osebni podatki morajo biti pošteno in zakonito obdelani, zbrani za določene in zakonite namene ter ne smejo biti pretirani. Shranjeni so lahko v obliki, ki dopušča identifikacijo posameznikov, na katere se osebni podatki nanašajo in to le toliko časa, kolikor je potrebno za namene, s katerimi so bili zbrani (Direktiva 95/46/ES 1995, 6. člen). Prvi odstavek sedmega člena Direktive pa še določa, da se mora za obdelavo takih podatkov pridobiti posameznikovo nedvoumno privolitev (Direktiva 95/46/ES 1995, 7. člen).

Za varovanje pridobljenih podatkov Direktiva v 17. členu poziva države članice, da same določijo, kakšne tehnične in organizacijske ukrepe za varovanje osebnih podatkov mora upravljalec podatkov[26] izvajati (Direktiva 95/46/ES 1995, 17. člen). Zakon, ki v slovensko pravo prenaša Direktivo Evropskega parlamenta in Sveta 95/46/ES o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov, je Zakon o elektronskih komunikacijah. 106. člen govori o geolokalizaciji:

> *(1) Lokacijske podatke, ki niso hkrati podatki o prometu in se nanašajo na uporabnike ali naročnike, se sme obdelovati le v takšni obliki, da se ne dajo*

[25] GPS pomeni Global Positioning System – Globalni sistemi za določanje položaja. Razvila ga je ameriška vojska. Podatki o lokaciji se izračunajo s triangulacijo in se pošljejo direktno osebi z GPS-jem (ČLEN 29 Delovna skupina za varstvo osebnih podatkov 2005, 2).

[26] V našem primeru je to človek, ki ima vpogled v geolokalizacijske podatke posameznika.

povezati z določeno ali določljivo osebo, ali pa na podlagi predhodnega soglasja uporabnika ali naročnika v obsegu in trajanju, ki sta potrebna za izvedbo storitve z dodano vrednostjo. Uporabnik ali naročnik lahko to soglasje kadarkoli prekliče.

(2) Uporabnik ali naročnik mora biti pred izdajo soglasja v zvezi z obdelavo podatkov iz prejšnjega odstavka, seznanjen z:

1. vrsto teh podatkov, ki bodo obdelani,

2. namenom in trajanjem takšne obdelave,

3. možnostjo posredovanja teh lokacijskih podatkov tretji osebi zaradi izvedbe storitve z dodano vrednostjo.

(3) Uporabnik ali naročnik, ki je soglašal z obdelavo podatkov iz prvega odstavka tega člena, ima možnost, da na preprost in brezplačen način začasno zavrne obdelavo takšnih podatkov pri vsaki priključitvi na omrežje ali za vsak prenos komunikacije.

(4) Podatke iz prvega odstavka tega člena smejo v skladu s prejšnjimi odstavki tega člena obdelovati le osebe, ki so pod nadzorom operaterja ali tretje osebe, ki izvaja storitev z dodano vrednostjo, pri čemer mora biti ta obdelava omejena na to, kar je potrebno za izvedbo storitve z dodano vrednostjo. (Zakonodaja.com 2008)

Izjeme v Zakonu o elektronskih komunikacijah:

(5) Pri klicih na enotno evropsko številko za klice v sili "112" in številko policije "113" mora operater v skladu z drugim odstavkom 72. člena tega zakona pristojnim organom posredovati lokacijske podatke iz prvega odstavka tega člena tudi v primerih, ko je uporabnik ali naročnik začasno zavrnil obdelavo podatkov iz prvega odstavka tega člena ali ni izdal soglasja za njihovo obdelavo.

(6) Določbe prvega do četrtega odstavka tega člena se ne uporabljajo za lokacijske podatke, ki niso hkrati podatki o prometu, za katere ta zakon določa obveznost hrambe. (Zakonodaja.com 2008)

4.7.3 Geolokalizacija zaposlenih

Delovna skupina 29 opaža razvoj sistemov, ki podjetjem omogočajo določitev položaja zaposlenih v določenem trenutku ali neprestano – z geolokalizacijo predmetov, ki jih ima zaposleni v lasti, na primer bančne kartice, mobilnega telefona, pa tudi pametne kartice (ČLEN 29 Delovna skupina za varstvo osebnih podatkov 2005, 10-11).

Delovna skupina je tudi mnenja, da naj se geolokalizacijski podatki obdelujejo le za posebne namene in da "mora obdelava podatkov o lokaciji zaposlenih ustrezati posebni potrebi podjetja, povezani z njeno dejavnostjo" (ČLEN 29 Delovna skupina za varstvo osebnih podatkov 2005, 11). Po njihovem mnenju je obdelava geolokacijskih podatkov opravičljiva, če je opravljena kot del spremljanja prevoza ljudi ali blaga ali če se želi doseči večja varnost v zvezi z zaposlenimi, blagom ali vozili (ČLEN 29 Delovna skupina za varstvo osebnih podatkov 2005, 11).

Pomembno je tudi, da delodajalec, ki je uvedel geolokalizacijske ukrepe, ne zbira podatkov o lokaciji zaposlenih zunaj delovnega časa, zato naj se v vozilih, ki so namenjena tudi zasebni rabi zaposlenih, omogoči izključitev funkcije geolokalizacije (ČLEN 29 Delovna skupina za varstvo osebnih podatkov 2005, 11).

4.7.4 Stanje pri nas in v svetu

Poleg znanega GPS-ja obstaja še nekaj sistemov določanja pozicije posameznika prek satelita, ki so: ruski GLONASS; kitajski Beidou, ki deluje le na področju Kitajske in Galileo, ki je evropski sistem določanja položaja posameznika. Galileo se razvija od leta 2004 in skuša po pokritosti in natančnosti dohiteti ameriški GPS sistem (Wikipedia 2008c).

Po pregledu nekaterih internetnih strani sem odkrila veliko podjetij, ki ponujajo storitev elektronskega nadzora zaposlenih: sledenje službenim vozilom. V Sloveniji je eden od takih Sledenje.com, ki ima za stranke Pivovarno Union, Žito d. d. in Plinarno Maribor d. d. (http://www.sledenje.com/, 4.9.2008). Nekateri ostali večji slovenski delodajalci, kot so Telekom, Pošta in Vlada Republike Slovenije, pa so svoje vozne parke za sledenje službenim vozilom opremili z GPS sistemi (Albreht 2008).

V Evropski uniji je na področju geolokalizacije zaposlenih krovna Direktiva Evropskega parlamenta in Sveta 95/46/ES. Delovna skupina člena 29 opozarja evropske delodajalce, da mora biti vsaka vrsta elektronskega nadzora zaposlenih, tudi geolokalizacija, ustrezna oziroma primerna, potrebna in ne pretirana, vsekakor pa mora biti izvedena na najmanj možen vsiljiv način (ARTICLE 29 – Data Protection Working Party 2001, 2 in 4). Podatki o razširjenosti lokalizacije zaposlenih z elektronskimi pripomočki v Evropi pa žal niso dosegljivi.

V Ameriki so delodajalci, ki uporabljajo GPS ali kakšno drugo obliko geolokalizacije zaposlenih, v manjšini. Osem odstotkov ameriških delodajalcev uporablja GPS za sledenje službenim vozilom, trije odstotki pa uporabljajo GPS za nadzor mobilnih telefonov njihovih zaposlenih. En odstotek delodajalcev pa GPS uporablja za nadzor pametnih kartic in tako pridobijo informacije o trenutni lokaciji zaposlenih (Business Wire 2008).

5 RAZISKOVALNI DEL

Zakonski in podzakonski akti dokaj rigorozno dovoljujejo in prepovedujejo dele obravnavanega elektronskega nadzora zaposlenih. Da bi lahko v celoti preverila svoje hipoteze, ki sem jih v uvodu postavila, in da bi se prepričala o dejanskem stanju elektronskega nadzora zaposlenih v Sloveniji, sem opravila manjšo raziskavo v dveh organizacijah.

5.1 Kriteriji

Za izbiro raziskovanih organizacij sem postavila nekaj kriterijev, ki bi mi omogočili lažjo izbiro med podjetji in večjo možnost posplošitve na slovensko delovno okolje.

Kriteriji so bili sledeči:

- tri popolnoma različna področja poslovanja,
- veliko število zaposlenih,
- veliko število strank,
- obdelava in hramba velikega števila osebnih podatkov (tako od zaposlenih kot od strank)
- sedež organizacije v Ljubljani in
- velikost organizacije: srednja do velika.

Sledeč kriterijem sem izbrala tri področja poslovanja: bančništvo, komunikacije in šolstvo.

Za pritegnitev k sodelovanju organizacij iz teh področij sem napisala veliko prošenj; na področju komunikacij in šolstva sem pridobila organizaciji, s področja bančništva pa se ni odzvalo nobeno podjetje, ki je bilo s kriteriji izbrano.[27]

[27] Pravzaprav mi od petih bank niso poslale nobenega odgovora kar tri. Ostale so zavrnile sodelovanje zaradi varstva osebnih podatkov svojih strank in zaradi strahu pred izgubo zaupanja sedanjih in bodočih komitentov.

Organizaciji, ki sta privolili v sodelovanje, želita ostati anonimni zaradi občutljivosti teme elektronskega nadzora zaposlenih,[28] zato bo organizacija s področja komunikacij v nadaljevanju poimenovana Organizacija A, organizacija s področja šolstva pa Organizacija B.

5.2 Organizacija A

5.2.1 O organizaciji

Organizacija A[29] je delniška družba s področja komunikacij. Ustanovljena je bila v drugi polovici devetdesetih let; ima nekaj velikih ter mnogo malih delničarjev. Ima več področij dejavnosti (od komunikacij do splošnih gradbenih del) in nekaj hčerinskih podjetij.

Organizacija A sodi med velike delodajalce v Sloveniji; njeni zaposleni zagovarjajo timsko delo in inovativnost. V prihodnosti organizacija A načrtuje optimizacijo in regionalizacijo poslovanja.

5.2.2 Elektronski nadzor v organizaciji A

O elektronskem nadzoru v organizaciji A bom pisala v dveh delih. Prvi del bo vseboval odgovore zaposlenih in opis poslovnih prostorov obiskane organizacije, v drugem delu pa bom napisala kritične ugotovitve o elektronskem nadzoru zaposlenih in opisala morebitne kršitve zakonov.

5.2.2.1 Rezultati obiska in pogovorov v organizaciji

Podatke o organizaciji A sem dobila z intervjuji z vodjo varnostne službe, s pravnico, z varnostnikom in s kadrovnico s pomočjo odprtega strukturiranega vprašalnika. Z njimi sem se pogovarjala ločeno in v različnih časovnih obdobjih, tako da nihče ni vedel za ostale odgovore. Ogled prostorov v organizaciji sem opravila prvega septembra 2008.

[28] Veliko podjetij to področje dojema kot poslovno skrivnost in se zaradi tega noče izpostavljati s svojim imenom. Javno pisanje o tej temi bi lahko zaradi opisa metod nadzora in varovanja podatkov zmanjšalo ugled organizacije v očeh dosedanjih uporabnikov in strank.

[29] Podatke o organizaciji A sem dobila na njihovi spletni strani. Zaradi njihove želje po anonimnosti je ne morem navesti kot vir.

Organizacija A izvaja več vrst elektronskega nadzora zaposlenih, kar je vidno že ob vstopu v poslovne prostore. Za zaposlene in za obiskovalce obstaja evidenca vstopov in izstopov; za prve je vstop omogočen s tako imenovano pametno ali brezkontaktno kartico, ki omogoča vstope tudi v prostore, kamor običajni obiskovalec ne more. Vsak zaposleni ima namreč v pametni kartici določena področja, kamor lahko dostopa. Evidenco vstopov in izstopov za obiskovalce pa vodi receptor; podatki obiskovalca (ime, priimek in številka osebnega dokumenta) se napišejo na list, ki se na koncu dneva uniči. Evidenca vstopov in izstopov za zaposlene pa se hrani tri mesece; s pomočjo te evidence se kontrolira delovna obveznost in obračuna mesečna plača.

Takoj ob vstopu v organizacijo je vidna še ena oblika elektronskega nadzora zaposlenih: video nadzor. Videokamere snemajo vhod iz zunanje in notranje strani; kamera ob recepciji snema prihode zaposlenih in obiskovalcev, vpogleda v območje delovnega prostora receptorja pa ne zajema. Video nadzor se izvaja še po hodnikih (povprečno štiri kamere na hodnik), v skladiščih ter skupnih prostorih. Večina kamer je v obliki 'fish-eye' ali ribjega očesa, redke so običajne oblike ('cevne' kamere), obstaja pa tudi nekaj kamer, ki so samo nameščene in ne vklopljene (navidezne kamere). Delujoče videokamere ne snemajo neprestano; aktivirajo se ob zaznavi gibanja ali luči.

Pred uvedbo elektronskega nadzora se je uprava organizacije posvetovala z reprezentativnimi sindikati in uslužbenci. Sprejela je tudi pravilnik o varstvu osebnih podatkov ter sklep o izvajanju video nadzora v poslovnih prostorih organizacije. O izvajanju elektronskega nadzora zaposlenih se je uprava organizacije odločila zaradi varovanja ljudi in premoženja ter reda v prostorih organizacije; zaposlene je o uvedbi nadzora obvestila s pisnim obvestilom in z obvestilom preko intranetnih strani.

Poleg video nadzora in kontrole pristopov, ki ju je organizacija A uvedla leta 1996, se v organizaciji od leta 2007 uporablja tudi biometrijo in snemanje telefonskih pogovorov. Vhodne klice se snema tam, kjer imajo zaposleni največ stikov s strankami in uporabniki; posnetkov se ne nadzira, nekatere pa se uporabi za učne zglede pri uvajanju novih zaposlenih. Biometrija je bila uvedena zaradi želje po povišanju stopnje varnosti organizacije, za varovanje opreme in kritične infrastrukture. Zaposleni, ki so bili vključeni v biometrijo, so bili obveščeni o poostrenih varnostnih in nadzornih ukrepih

ter podpisali izjavo, da se z njimi strinjajo. Biometrijo[30] se v organizaciji A izvaja v kombinaciji s pametno kartico.

Ostale oblike elektronskega nadzora zaposlenih organizacija A uporablja v manjši meri. Internetni dostop do 'sumljivih' strani, kot so pornografija, igre na srečo ter strani z orožjem, ni blokiran, vendar se vsi obiski internetnih strani beležijo na požarni zid. Ti podatki se potem dnevno analizirajo za delovanje omrežja. Če je ugotovljeno, da je katera od dostopanih strani povzročila škodo[31] organizaciji, se jo zablokira. Uporaba elektronske pošte za zasebne namene, uporaba spletne elektronske pošte (kot sta gmail in yahoo) ter uporaba interneta za neslužbene namene je dovoljena v skladu z določili internega akta o uporabi interneta, to je do te mere, da ne vpliva na produktivnost delavca in da ne povzroča tako posredne kot neposredne škode delodajalcu.

Geolokalizacije na zaposlenih, ki uporabljajo njihova službena vozila, organizacija A ne izvaja. Odgovornim se zdi geolokalizacija nesorazmeren ukrep nadzora, zato kontrolirajo le porabo goriva in kilometrino. Odločitev, da elektronskega nadzora zaposlenih ne izvajajo, če zanj ni potrebe ali če z njim ne bi pridobili nobene koristi, upoštevajo dosledno.

5.2.2.2 Ugotovitve

Na vhodu v organizacijo je nalepljeno opozorilo o video nadzoru z napisom imena izvajalca in telefonsko številko. Video nadzora ne vršijo v dvigalih, garderobi ali toaleti, kar je tudi skladno z zakonom, čeprav so razmišljali o uvedbi kamer v dvigalih. Po mnenju Informacijskega pooblaščenca ta želja ni uresničljiva: "/k/er določba 3. odstavka 76. člena ZVOP-1 natančno našteva, kje se videonadzor lahko izvaja (dostop do vhodov in izhodov večstanovanjskih stavb ter skupni prostori), dvigala pa po zgoraj navedeni definiciji ne sodijo med skupne prostore, je mogoč le zaključek, da uporaba video nadzornih kamer v dvigalih ni dovoljena." (Pirc Musar 2006a)

Posnetke, ki so pridobljeni z video nadzorom, ima organizacija A primerno zavarovane pred nepooblaščenimi osebami z naslednjimi ukrepi: s pooblaščenimi dohodi s pametnimi karticami, z zagotovljeno revizijsko sledjo, z zaklepanjem vrat in z video

[30] Organizacija A se je odločila za identifikacijo posameznika s pomočjo prstnega odtisa palca.

[31] Škodo so na organizaciji A opredelili kot okuženje računalnikov z virusi ali z vohunskimi programi.

nadzorom. Evidence vstopov in izstopov zaposlenih in obiskovalcev se hranijo, kolikor je potrebno in določeno z zakonom; podobno je z ostalimi podatki, pridobljenimi z elektronskim nadzorom zaposlenih.

Vsak zaposleni v organizaciji ima zagotovljen dostop do podatkov, ki se o njem zbirajo; če zaposleni meni, da se z elektronskim nadzorom posega v njegovo zasebnost, ima možnost pritožbe. Take pritožbe se v organizaciji A jemljejo resno in jih razrešijo v najkrajšem možnem času.

Biometrični varnostni ukrepi so v organizaciji A še dokaj redki, vendar služijo svojemu namenu. Za uvedbo biometrije v organizaciji je potrebno pridobiti odločbo Informacijskega pooblaščenca, kajti

> */d/ržavni nadzorni organi za varstvo osebnih podatkov se vse prepogosto srečujejo s primeri, ko se osebni podatki prvotno zbirajo z enim namenom, a se kasneje uporabljajo s povsem drugimi. Druga zelo pomembna izkušnja državnih nadzornih organov je, da večina posameznikov ne ceni svoje zasebnosti, dokler ni kompromitirana. In ko se to zgodi, mora posameznik znova in znova vlagati napore, da zasebnost ohranja. Težko bi trdili, da je uporaba biometričnih podatkov na to kakorkoli imuna.* (Informacijski pooblaščenec 2008a)

Organizacija A je pridobila odločbo in legalno izvaja biometrične ukrepe.

Blokiranje internetnih strani pri obravnavani organizaciji ni v navadi, prav tako ne prebirajo ali prestrezajo elektronske pošte. Zdi se, da v tem oziru ne sledijo trendom v tujini in ne uvajajo nevidnega elektronskega nadzora, ki je ponekod v svetu že postal del vsakdana.

Zadnji ukrep elektronskega nadzora v organizaciji A, ki ga bom obravnavala, me je tudi najbolj osebno pritegnil: snemanje dohodnih telefonskih klicev. Informacijski pooblaščenec pravi, da:

> */…/ zakon*[32] *v določbah 103. člena uzakonja zaupnost komunikacij in v šestem odstavku izpostavljenega člena določa, da lahko naročnik ali uporabnik komunikacijo snema, vendar mora pošiljatelja oziroma prejemnika komunikacije*

[32] Zakon o elektronskih komunikacijah.

o tem obvestiti ali pa delovanje snemalne naprave prilagoditi tako, da je o njenem delovanju pošiljatelj oziroma prejemnik komunikacije obveščen (npr. avtomatski odzivniki). (Pirc Musar 2006c)

Iz mnenja Informacijskega pooblaščenca je razvidno, da je snemanje telefonskih pogovorov z vnaprejšnjim obveščanjem kličočega dovoljeno in tudi legalno.

Glede na videno in slišano moram zaključiti, da nikjer nisem zaznala kakršnekoli kršitve zakonov ali priporočil Informacijskega pooblaščenca. Dejstvo pa je, da organizacija A izvaja veliko vrst elektronskega nadzora, in to ne samo za varovanje ljudi in premoženja, ampak tudi za dejanski nadzor zaposlenih.

5.3 Organizacija B

5.3.1 O organizaciji

Organizacija B[33] je članica Univerze v Ljubljani. Ustanovljena je bila v drugi polovici dvajsetega stoletja in se neprestano spreminja, da ostaja v koraku s časom in potrebami študentov. Ima več kot 240 zaposlenih. V vseh letih obstoja je na njej diplomiralo več kot 6300 diplomantov, več kot 210 pa jih je doktoriralo. Organizacija B teži k politični in nazorski neodvisnosti ter skuša z razvijanjem oblik vseživljenjskega izobraževanja postati prepoznaven in ugleden center dodiplomskega in podiplomskega izobraževanja v Evropi.

5.3.2 Elektronski nadzor v organizaciji B

O elektronskem nadzoru v organizaciji B bom pisala v treh delih. Prvi del bo vseboval odgovore zaposlenih, v drugem delu bom opisala poslovne prostore obiskane organizacije, v tretjem delu pa bom napisala kratek povzetek videnega in slišanega ter kritične ugotovitve o morebitnih kršitvah zakonov.

[33] Podatke o organizaciji B sem dobila na njihovi spletni strani, ki pa je zaradi njihove želje po anonimnosti ne morem navesti kot vir.

5.3.2.1 Odgovori zaposlenih

V imenu organizacije B mi je odgovarjal zaposleni z visoko stopnjo odgovornosti[34] v organizaciji. Odgovore sem dobila s pomočjo vnaprej pripravljenega odprtega vprašalnika. Odgovorni mi je povedal, da se elektronskega nadzora na svojem delovnem mestu ne zaveda, niti se mu ne zdi pretiran, kajti edina oblika elektronskega nadzora so videokamere, ki so nameščene pred vhodi in v skupnih prostorih. Kamere so nameščene tudi v učilnicah, vendar so vklopljene samo ponoči med dvaindvajseto uro zvečer in šesto uro zjutraj. Vse videokamere so bile prvotno nameščene kot del varnostnega in ne nadzornega sistema.

Ob uvedbi videokamer leta 2007 zaposleni niso dobili v podpis aneksa k pogodbi o zaposlitvi;[35] odgovorni so vse zaposlene, vključno s sindikatom, obvestili o načinu video nadzora, njegovem obsegu, lokacijah kamer, času snemanja ter o odgovornih osebah, ki imajo vpogled v video posnetke. O tej problematiki je razpravljal tudi senat organizacije.

V podatke, pridobljene z video nadzorom, imajo vpogled s strani vodstva pooblaščene osebe, ki so: varnostnik, računalniški center in vodstvo. Zbrani podatki se hranijo tri mesece, nato se izbrišejo. Video nadzor izvaja organizacija B v sodelovanju z zunanjim izvajalcem; pridobljene podatke se varuje z različnimi gesli, z vodenjem evidence dostopov do teh informacij, z zaklepanjem dostopnih vrat in videokamerami.

V organizaciji B, po besedah mojega sogovornika, nimajo drugih vrst elektronskega nadzora, niti evidence vstopov in izstopov zaposlenih ali obiskovalcev. Edina oseba, ki ima nek pregled nad obiskovalci in zaposlenimi, je receptor na glavnem vhodu, ki pa opravlja več nalog obveščanja kot nadzorovanja ali opazovanja.

Za uvedbo elektronskega nadzora s pomočjo videokamer se je odločilo vodstvo v investicijskem načrtu ob izgradnji novih prostorov v šolskem letu 2005/2006.

---

[34] Zaradi želje anonimnosti sogovornika ne morem zapisati niti njegovega imena niti njegovega delovnega mesta.

[35] Njihova pogodba o zaposlitvi vsebuje izjavo posameznika, da se strinja s tem, da se njegovi podatki uporabljajo za potrebe, ki so vezane nanj. Pod to izjavo se lahko upošteva tudi zavedanje o videonadzoru ter o podatkih, ki so z njim pridobljeni.

5.3.2.2 Obisk organizacije

Obisk organizacije sem opravila 22. avgusta 2008. Organizacija B ima dva vhoda: glavnega in stranskega, oba sta pokrita z videokamerami z notranje strani; pri glavnem vhodu je recepcija. Na obeh vratih visi opozorilo o video nadzoru z imenom izvajalca in telefonsko številko. V notranjosti so videokamere vidne še v učilnicah v novem delu, na hodnikih pred kabineti, v skupnih prostorih, v vhodu v dekanat ter v veži pred knjižnico. Prostori (kabineti, vhodi, knjižnica) so poleg kamer varovani še s ključavnicami. Nikjer ni vidnega terminala za uporabo pametnih kartic; prehodi v prostore so prosti.

Iz pogovora z nekaterimi zaposlenimi sem dobila občutek, da elektronski nadzor resnično ni pretiran, ker se primarno izvaja v varovalne namene in še to le ponoči. Ostale vrste elektronskega nadzora se v organizaciji B ne izvajajo. Delavcem se obisk internetnih strani ne blokira, elektronska pošta se ne pregleduje niti ne prebira, telefonom se ne prisluškuje, prav tako se ne snema telefonskih pogovorov in tudi prihodov in odhodov zaposlenih se ne nadzira.

5.3.2.3 Ugotovitve

Po obisku in po pogovoru z zaposlenimi v organizaciji B sem dobila občutek, da elektronski nadzor zaposlenih ni pretiran, obratno: zelo je mil. Elektronski nadzor se izvaja predvsem v varovalne namene, njegovi rezultati se hranijo z ustreznimi ukrepi in ne predolgo (zakonsko določena meja). Vpogled v posnetke video nadzora imajo le pooblaščene osebe, dodatno varovalo je tudi evidenca dostopov do teh podatkov.

Nadaljnje dvome o postavitvi kamer v učilnicah in potencialno snemanje med predavanji ter med pisanjem izpitov brez soglasja študentov in zaposlenih, je razjasnil Informacijski pooblaščenec: snemanje je namreč dovoljeno,

> */.../ a le, če so izpolnjene vse obveznosti in pogoji iz 74.,[36] 75.[37] in / ali 77[38]. člena ZVOP-1. Glede na zgoraj navedene pogoje, ki morajo biti izpolnjeni za*

[36] Ta člen vsebuje določbo o obvestilu o izvajanju video nadzora.

[37] Ta člen govori o dovoljenem snemanju poslovnih prostorov zaradi varnosti ljudi ali premoženja; o pisni odločitvi o razlogih za nadzor; o obveščanju zaposlenih o nadzoru ter o času hrambe osebnih podatkov, pridobljenih z videonadzorom.

zakonito izvajanje videonadzora, Informacijski pooblaščenec zaključuje, da sme pravna ali fizična oseba izvajati videonadzor nad zaposlenimi /.../ in nad poslovnimi prostori (če učilnico smatramo kot poslovni prostor, v katerem je oprema, ki jo je potrebno varovati) samo v primerih in pod pogoji, ki jih določa ZVOP-1. V takšnem primeru bi bili pod videonadzorom tudi študentje, ki pa morajo biti obveščeni (obvestilo, skladno s 74. členom ZVOP-1), da vstopajo, v videonadzorovano območje. (Informacijski pooblaščenec 2008f, 14)

Pravi še, da razlog nadzorovanja študentov pri opravljanju izpitov ali študiju " /…/ pa sam po sebi ni zadosten za uvedbo videonadzora oziroma za tovrstno izvajanje videonadzora ni zakonske podlage." (Informacijski pooblaščenec 2008f, 14)

Video nadzor na hodniku brez soglasij dijakov/študentov ali njihovih zakonitih zastopnikov je po mnenju Informacijskega pooblaščenca tudi dovoljen,

/.../ vendar je potrebno kljub temu o uvedbi videonadzora obvestiti vse zaposlene, objaviti obvestilo iz 74. člena ZVOP-1 in določiti odgovorne osebe za zbirko videonadzornega sistema, saj vpogleda v posnetke videonadzora ne more imeti vsak profesor ob kateremkoli času. /.../ Pogoje, ki jih postavlja ZVOP-1 za uvedbo videonadzora v smislu 75. člena, je potrebno spoštovati tudi ob samem vpogledu v posnetke videonadzornega sistema. Ob upoštevanju načela sorazmernosti iz 3.[39] člena ZVOP-1 se lahko v posnetke videonadzora vpogleda zgolj, kadar pride do »dogodka«, ki ga opisujejo pogoji za uvedbo videonadzora dostopov v uradne službene oziroma poslovne prostore. V posnetke videonadzora lahko torej vpogleda le odgovorna oseba (npr. ravnatelj) v primerih, v okviru katerih varovane dobrine (npr. varnost ljudi ali premoženja) varuje 75. člena ZVOP-1. Poleg tega je potrebno vsak vpogled, kopiranje ali

[38] Ta člen govori o prepovedi izvajanja videonadzora v garderobah, dvigalih in sanitarijah; o posvetovanju delodajalca pred uvedbo videonadzora z reprezentativnim sindikatom in o izvajanju videonadzora za varovanje ljudi ali premoženja takrat, ko tega namena ni možno doseči z milejšimi ukrepi.

[39] "Osebni podatki, ki se obdelujejo, morajo biti ustrezni in po obsegu primerni glede na namene, za katere se zbirajo in nadalje obdelujejo" (ZVOP-1 2007, 3. člen).

posredovanje tretji osebi zabeležiti v dnevnik videonadzornega sistema. (Informacijski pooblaščenec 2008f, 9)

Drugih oblik elektronskega nadzora pa organizacija B ne uporablja, tako da o ostalih morebitnih kršitvah sploh ne more biti govora.

6 PREVERJANJE HIPOTEZ

Moji hipotezi sta bili:

- Elektronski nadzor zaposlenih je v teoriji z zakoni dovolj omejen, vendar se v praksi uporablja tudi nedovoljene oblike nadzora, ki jih država ne uspe pravočasno sankcionirati.
- Transparentnost nadzora zaposlenih se z uporabo modernih tehnologij zmanjšuje, možnost zlorabe pa se s strani delodajalca povečuje.

Po vsej prebrani literaturi in po opravljenih obiskih v organizacijah A in B lahko obe hipotezi potrdim.

Prvo hipotezo lahko potrdim, čeprav v nobeni od obiskanih organizacij nisem zasledila nepravilnosti ali kršitev. Potrdim pa jo lahko med drugim tudi na osnovi primera afere Ministrstva za zunanje zadeve (obravnavan je bil pri Vrstah elektronskega nadzora zaposlenih), ki bi kot državna institucija morala biti zgled ostalim delodajalcem v dobri, in ne v slabi praksi, kako se lotiti notranje preiskave ob curljanju zaupnih informacij v javnost. Kršili so določbe Zakona o elektronskih komunikacijah in Konvencije o varstvu človekovih pravic in temeljnih svoboščin zaradi notranje preiskave, čeprav bi se reševanja te težave lahko lotili drugače (na primer z dovoljenimi preiskovalnimi metodami) ali s pomočjo policije.

Prvo hipotezo lahko potrdim tudi po porastu pritožb pri Informacijskem pooblaščencu zaradi vdora v zasebnost zaposlenega na delovnem mestu, ki ga izvajajo delodajalci (še posebej na področju video nadzora in elektronske pošte). Z novimi tehnologijami lahko delodajalec dokaj neopazno vohuni za svojim zaposlenimi, ne da bi slednji to opazili. Zaradi vse večje previdnosti zaposlenih pa se zavedanje o vrednosti osebnih podatkov povečuje in s tem tudi skrb za lastno zasebnost na delovnem mestu.

Kljub potrditvi prve hipoteze pa nam primer pritožbe sindikata RTV Slovenije daje upanje, da zaposleni s pritožbo, ko delodajalec posega v njihovo zasebnost na delovnem mestu, lahko nedovoljen nadzor tudi odpravijo. Poleg tega lahko potrdim, da je zakonov in smernic na področju elektronskega nadzora zaposlenih dovolj (vsaj na področju video nadzora, biometrije, evidence prihodov in odhodov ter podatkov o lokaciji), vendar

njihovo izvajanje in preverjanje ni niti dovolj učinkovito niti dovolj hitro, vsaj sodeč po odločbah, mnenjih in poročilih Informacijskega pooblaščenca.

Drugo hipotezo lahko potrdim na osnovi primera Ministrstva za zunanje zadeve. Z napredkom tehnologije je težko vedeti, kako delodajalci uporabljajo podatke, pridobljene z elektronskim nadzorom. Potrebno je poudariti, da se dá, kljub ažurnim zakonom, z novimi tehnologijami elektronski nadzor zaposlenih tudi prikriti, kar bo še bolj očitno v prihodnosti. To na nek način potrjuje tudi primer organizacije A, ki z manipulacijo elektronskega nadzora zaposlenih izvaja tudi navidezni nadzor oziroma z drugimi besedami: del dejanskega video nadzora organizacija A ne opravlja s pravimi kamerami ampak uporabljajo lažne. Te imajo videz prave videokamere in dajejo zaposlenim občutek, da so opazovani. Lažne videokamere so tudi ena izmed modernih tehnologij, ki sicer v smislu zbiranja osebnih podatkov in vdiranja zasebnosti delavcu ne škoduje, ga pa zavaja in daje lažne podatke o njegovem delovnem okolju.

Elektronski nadzor zaposlenih se izvaja s pomočjo modernih tehnologij, ki se jim za sedaj do določene mere dá slediti. Ne smemo pa pozabiti na tiste profesionalce, vključno z delodajalci, ki znajo svoje sledi dobro prikriti in ki jih povprečen človek ne zna in ne zmore odkriti. Z znanjem se zaposleni sicer lahko do določene mere zaščitijo, vsekakor pa ni nobene potrebe, da bi delavci morali posegati po dodatnih varovalih , saj jim Zakon o delovnih razmerjih zagotavlja varne delovne razmere in varovanje delavčeve osebnosti.

Trenutno je na področju transparentnosti elektronskega nadzora zaposlenih bistveno, da se delodajalci držijo internih aktov o elektronskem nadzoru; da obveščajo zaposlene o elektronskem nadzoru, ki ga izvajajo, kot tudi o načinu hranjenja zbranih osebnih podatkov. Pomembno je, da ima vsak zaposleni vpogled v gradivo, ki je bilo o njem zbrano z elektronskim nadzorom in da ve, da to ne bo vplivalo na njegovo oceno uspešnosti. Za delodajalce pa je ključno zavedanje, da je najboljši delavec zadovoljen delavec.

7 ZAKLJUČEK

V modernem svetu, kjer tehnologija dnevno dosega nove presežke, je elektronski nadzor zaposlenih postal stalnica v našem življenju. Težnja delodajalcev je že od vedno bila želja po nadzoru zaposlenih, zaposleni pa so se vedno poskušali izogniti nadzoru svojih delodajalcev. Redki so taki delodajalci, ki pomislijo tudi na to, kako (pretiran) nadzor vpliva na njihove podrejene. Prava redkost je zato táko podjetje kot je organizacija B, kjer je elektronski nadzor zaposlenih omejen na video nadzor, pa še ta ima primarno funkcijo varovanja objekta.

V mojem diplomskem delu sem se v prvem, sociološkem delu posvetila teorijam, ki so večinoma znane širši javnosti; ugotovila sem, da imata Benthamov Panoptikon in Orwellov Veliki brat večji vpliv na realnost v okviru potenciala in izvedbe elektronskega nadzora tako zaposlenih kot ostalih ljudi, kot se mi je sprva zdelo.

Zanimivo je bilo opazovati, kako so teorije preraščale svoj prvotni okvir nadzora dela populacije in kako sta bila Bentham in Orwell daljnovidna. Njune vizije se tako ali drugače uresničujejo v vsakdanjem življenju.

Čeprav so videokamere (in pametne kartice) za zaposlene že del rutine delovnega dneva, se je med pogovori v organizaciji A pokazalo, da se zaposleni še kako zavedajo dejstva, da so nadzorovani. Kot je dejal varnostnik organizacije A: zaposleni so sproščeni in delovni, vendar se nekje globoko vseeno zavedajo tako kamer kot snemanja telefonskih pogovorov.

Organizacija A je bolj tipična predstavnica podjetij v Sloveniji in v Evropski Uniji. Varnost je postavljena na prvo mesto, šele na drugem mestu so zaposleni in njihovi rezultati. Kljub temu je dobro vedeti, da organizacija A kljub svojim možnostim večjega in bolj poostrenega (pa tudi nelegalnega) nadzora ne uporablja.

Od vseh vrst elektronskega nadzora se mi zdita pametna kartica (če je omejena le na evidenco prihodov in odhodov v organizaciji) in blokada nekaterih internetnih strani še najmanj invazivna. Najbolj zaskrbljujoča pa se mi zdita, poleg porasta uporabe videokamer na vsakem koraku, geolokalizacija in biometrija. Vem, da po njiju posegajo delodajalci zaradi višanja stopnje varnosti, vendar sem mnenja, da bi se dalo varnost vzdrževati tudi na obstoječe in manj invazivne načine.

S preučevanjem pravnih virov sem ugotovila, da je obseg zakonskih in podzakonskih aktov, ki urejajo področje elektronskega nadzora zaposlenih, dokaj obširen. V diplomskem delu sem izpostavila le tiste, za katere se mi je zdelo, da najbolje opredelijo in osvetlijo obravnavano področje nadzora. Pravilno je, da zakonodaja ščiti zasebnost in temeljne človekove pravice posameznika pred nedovoljenimi in invazivnimi posegi delodajalcev. Škoda je samo, da vsa ta pravna varovala niso nedvoumno zapisana v enem, krovnem zakonu, ki bi se po potrebi ob uvedbi in razvoju novih tehnologij nadzora lahko širil in dopolnjeval.

S skepso moramo spremljati napredek v tehnologiji in tehniki pri razvoju novih oblik nadzora in predvsem varovanja. Naivno bi bilo pričakovati tehnike nadzora, ki bi bile učinkovitejše in bi istočasno manj ali nič ne posegale v pravice do zasebnosti. Pri vsem tem pa ne smemo pozabiti, da je tehnologija nevtralna; od nas je odvisno, ali jo bomo uporabili zgolj za varovalne namene ali bomo pustili, da se izrablja za vedno večji (elektronski) nadzor posameznikov.

8 LITERATURA

Albreht, Mojca. 2008. *Nadzor nad zaposlenimi – podjetje korak v prednosti – da ali ne?* Dostopno prek: http://www.revija.mojedelo.com/hr/nadzor-nad-zaposlenimi-podjetje-korak-v-prednosti-da-ali-ne-865.aspx (29. april 2008).

ARTICLE 29 – Data Protection Working Party. 2001. *Opinion 8/2001 on the processing of personal data in the employment context*. Dostopno prek: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp48en.pdf (10. junij 2008).

--- 2002. *Working document on the surveillance of electronic communications in the workplace*. Dostopno prek: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp55_en.pdf (10. junij 2008).

--- 2003. *Working document on biometrics*. Dostopno prek: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/ 2003/wp80_en.pdf (10. junij 2008).

--- 2004. *Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance*. Dostopno prek: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp89_en.pdf (10. junij 2008).

Brennan, Shelley. 2001. *Cutting-edge biology: fingers and eyes fighting fraud*. Dostopno prek: http://www.galtglobalreview.com/newtech/biometrics.html (3. september 2008).

Bunc, Stanko. 1963. *Slovar tujk*. Maribor: Založba Obzorja.

Business Wire 2008. 2008. *2007 Electronic Monitoring & Surveillance Survey: Over Half of All Employers Combined…* Dostopno prek: http://www.reuters.com/article/pressRelease/idUS179098+28-Feb-2008+BW20080228 (4. september 2008).

Caf, Dušan. 2008. *Primer MZZ iz evropske perspektive*. Dostopno prek: http://razgledi.net/blog/2008/03/03/primer-mzz-iz-evropske-perspektive/ (4. september 2008).

Cerar, Gregor. 2006. Sindikat RTV SLO preprečil videonadzor. *Mladina* (2006/38/). Dostopno prek: http://www.mladina.si/tednik/200638/clanek/uvo-manipulator--gregor_cerar-2/ (4. september 2008).

Copans, Richard in Stan Neumann. 2007. *Programmation Antenne: La saline d'Arc et Senans*. Dostopno prek: http://www.arte.tv/fr/connaissance-decouverte/architectures-saline/778994.html (22. julij 2008).

Cvetko, Aleksej. 1999. *Varovanje zasebnosti v delovnih razmerjih*. Ljubljana: Gospodarski vestnik.

ČLEN 29 Delovna skupina za varstvo osebnih podatkov. 2005. *Mnenje 5/2005 delovne skupine iz člena 29 o uporabi podatkov o lokaciji z namenom opravljanja storitev z dodano vrednostjo*. Dostopno prek: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_sl.pdf (10. junij 2008).

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. Ur. l. L 281 , 23/11/1995, str. 0031 – 0050. Dostopno prek: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:SL:HTML (28. junij 2008).

Direktiva 2002/58/ES z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah). Ur. l. L 201, 31/07/2002, str. 0037 – 0047. Dostopno prek: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:SL:HTML (13. september 2008).

Dnevnik. 2008. *Afera prisluškovanje zaposlenim na MZZ: Minister Dimitrij Rupel osumljen prekrška*. Dostopno prek: http://www.preberi.si/content/view/545439/23/ (5. september 2008).

enaA.com. 2008. *Video nadzor – kamere*. Dostopno prek: http://www.enaa.com/oddelki/racunalniskiDodatki/dept.asp?dept_id=2006&sortField=stNakupov&sortType=desc (19. september 2008).

Engberg, David. 1996. *The Virtual Panopticon*. Dostopno prek: http://besser.tsoa.nyu.edu/impact/f96/Projects/dengberg/ (19. maj 2008).

Foucault, Michel. 2004. *Nadzorovanje in kaznovanje: nastanek zapora*. Ljubljana: Krtina.

Golob, Renato. 1997. *Sistemi zaščite in varovanja oseb in premoženja*. Ljubljana: samozaložba.

Informacijski pooblaščenec. 2007. *Letno poročilo Informacijskega pooblaščenca 2007*. Dostopno prek: http://www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/Letno_porocilo_2007.pdf (8. oktober 2008).

--- 2008a. *Biometrija*. Dostopno prek: http://www.ip-rs.si/varstvo-osebnih-podatkov/informacijske-tehnologije-in-osebni-podatki/biometrija/ (2. september 2008).

--- 2008b. *Odločbe in mnenja – Varstvo osebnih podatkov*. Dostopno prek: http://www.ip-rs.si/nc/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/odlocbe-in-mnenja-varstvo-osebnih-podatkov/ (3. september 2008).

--- 2008c. *Odločbe in mnenja – Varstvo osebnih podatkov*. Dostopno prek: http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/odlocbe-in-mnenja-varstvo-osebnih-podatkov/?tx_jzvopdecisions_pi1%5BshowUid%5D=1369&cHash=792a4525f0 (3. september 2008).

--- 2008č. *Odločbe in mnenja – Varstvo osebnih podatkov*. Dostopno prek: http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/odlocbe-in-mnenja-varstvo-osebnih-podatkov/?tx_jzvopdecisions_pi1%5BshowUid%5D=1384&cHash=08e98fd2ac (3. september 2008).

--- 2008d. *Odločbe in mnenja – Varstvo osebnih podatkov*. Dostopno prek: http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/odlocbe-in-mnenja-varstvo-osebnih-podatkov/?tx_jzvopdecisions_pi1%5BshowUid%5D=1529&cHash=581f01f5b3 (3. september 2008).

--- 2008e. *Odločbe in mnenja – Varstvo osebnih podatkov*. Dostopno prek: http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/odlocbe-in-mnenja-varstvo-osebnih-podatkov/?tx_jzvopdecisions_pi1%5BshowUid%5D=431&cHash=2b151bc3cc (3. september 2008).

--- 2008f. *Smernice za izvajanje videonadzora*. Dostopno prek: http://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_videonadzor2.pdf (28. avgust 2008).

Kadrovnica organizacije A. 2008. Intervju. Ljubljana, 1. september.

Kavran, Darko. 2004. *Nadzor zaposlenih ali merjenje učinkovitosti?* Dostopno prek: http://www.finance.si/81648/Nadzor_zaposlenih_ali_merjenje_u%E8inkovitosti (29. april 2008).

Kocjančič, Rudi, Ciril Ribičič, Franc Grad in Igor Kaučič. 1998. *Ustavno pravo Slovenije*. Ljubljana: Visoka upravna šola.

Konvencija o varstvu človekovih pravic in temeljnih svoboščin. Ur. l. RS (13.6.1994) MP, št. 7-41/1994 (RS 33/1994). Dostopno prek: http://www.varuh-rs.si/index.php?id=108 (28. junij 2008).

Konvencija o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov. Ur. l. RS (28. 2. 1994) MP, št. 3-18/1994 (RS 11/1994). Dostopno prek: http://www.ip-rs.si/zakonodaja/zakon-o-varstvu-osebnih-podatkov/konvencija-o-varstvu-posameznikov-glede-na-avtomatsko-obdelavo-osebnih-podatkov/ (21. julij 2008).

Kovačič, Matej. 2006. *Nadzor in zasebnost v informacijski družbi: filozofski, sociološki, pravni in tehnični vidiki nadzora in zasebnosti na internetu*. Ljubljana: Fakulteta za družbene vede. Dostopno prek: http://dk.fdv.uni-lj.si/eknjige/EK_Kovacic_2006_Nadzor.pdf (8. julij 2008).

Kresal, Barbara, Katarina Kresal Šoltes, Darja Senčur Peček. 2002. *Zakon o delovnih razmerjih s komentarjem in stvarnim kazalom*. Ljubljana: Primath.

Kuhelj, Alenka. 2004. *Varstvo pravice do zasebnosti, veroizpovedi in svobodnega izražanja v pravu Sveta Evrope*. Ljubljana: Fakulteta za upravo.

Orwell, George. 1967. *1984*. Ljubljana: Mladinska knjiga.

Pavšič, Blaž. 2008. Intervju. Ljubljana, 27. avgust.

Pirc Musar, Nataša, Sonja Bien, Jože Bogataj, Mojca Prelesnik, Alenka Žaucer. 2006. *Zakon o varstvu osebnih podatkov (ZVOP-1) s komentarjem*. Ljubljana: GV Založba.

Pirc Musar, Nataša. 2006a. *Odločbe in mnenja – Varstvo osebnih podatkov*. Dostopno prek: http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/odlocbe-in-mnenja-varstvo-osebnih-podatkov/?tx_jzvopdecisions_pi1%5BshowUid%5D=169&cHash=67d150443a (2. september 2008).

--- 2006b. *Odločbe in mnenja – Varstvo osebnih podatkov*. Dostopno prek: http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/odlocbe-in-mnenja-varstvo-osebnih-podatkov/?tx_jzvopdecisions_pi1%5BshowUid%5D=214&tx_jzvopdecisions_pi1%5BhighlightWord%5D=elektronska%20po%C5%A1ta& cHash=98c284e96b (5. september 2008).

--- 2006c. *Odločbe in mnenja – Varstvo osebnih podatkov*. Dostopno prek: http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/odlocbe-in-mnenja-varstvo-osebnih-podatkov/?tx_jzvopdecisions_pi1%5BshowUid%5D=502&cHash=f0a7d925e6 (2. september 2008).

--- 2007. *Odločbe in mnenja – Varstvo osebnih podatkov*. Dostopno prek: http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/odlocbe-in-mnenja-varstvo-osebnih-podatkov/?tx_jzvopdecisions_pi1%5BshowUid%5D=523&tx_jzvopdecisions_pi1%5BhighlightWord%5Dlokacija&cHash=ac65e95066 (4. september 2008).

--- 2008a. *Informacijski pooblaščenec izdal letno poročilo za leto 2007 in ga predal Državnemu zboru*. Dostopno prek: http://www.ip-rs.si/novice/detajl/informacijski-pooblascenec-izdal-letno-porocilo-za-leto-2007-in-ga-predal-drzavnemu-zboru/ (4. september 2008).

--- 2008b. Intervju. Ljubljana, 29. avgust.

Pravilnik o metodologiji vodenja registra zbirk osebnih podatkov. Ur. l. RS 28/2005. Dostopno prek: http://www.uradni-list.si/1/objava.jsp?urlid=200528&stevilka=955 (13. september 2008).

Pravnica organizacije A. 2008. Intervju. Ljubljana, 1. avgust.

Predstavnik organizacije B. 2008. Intervju. Ljubljana, 29. avgust.

Prijamovič, Tomislav. 2008. *Nadzorovanje v javnih prostorih – videonadzor*. Dostopno prek: www.varnost-solstva.com/doc/web-videonadzor.doc (3. september 2008).

Radiofrekvenčna identifikacija (RFID). 2008. Dostopno prek: http://www.spica.si/caseStudies/learn_rfid.aspx (4. september 2008).

Rettinger, Konstanca. 2008. Intervju. Domžale, 7. september.

RTVSLO.SI. 2008. *MZZ: Prisluškovanja ni bilo*. Dostopno prek: http://www.rtvslo.si/modload.php?&c_mod=rnews&op=sections&func=read&c_menu=1&c_id=164586 (5. september 2008).

Ustava Republike Slovenije (URS). Ur. l. RS 33I/1991-I. Dostopno prek: http://www.dz-rs.si/?id=150&docid=28&showdoc=1 (2. september 2008).

Varnostnik organizacije A. 2008. Intervju. Ljubljana, 1. september.

Videonadzori.net. 2008. *Kamere*. Dostopno prek: http://www.videonadzori.net/kamere.html (19. september 2008).

Vodja varnostnikov organizacije A. 2008. Intervju. Ljubljana, 1. avgust.

Zakon o dostopu do informacij javnega značaja (ZDIJZ-UPB2). Ur. l. RS 51/2006. Dostopno prek: http://www.uradni-list.si/1/objava.jsp?urlid=200651&stevilka=2180 (13. september 2008).

Zakon o elektronskih komunikacijah (ZEKom). Ur. l. RS 43/2004. Dostopno prek: http://www.uradni-list.si/1/objava.jsp?urlid=200443&stevilka=1925 (28. junij 2008).

Zakon o Informacijskem pooblaščencu (ZInfP). Ur. l. RS 113/2005. Dostopno prek: http://www.uradni-list.si/1/objava.jsp?urlid=2005113&stevilka=5005 (28. junij 2008).

Zakon o javnih uslužbencih (ZJU). Ur. l. RS 56/2002. Dostopno prek: http://www.uradni-list.si/1/objava.jsp?urlid=200256&stevilka=2759 (13. september 2008).

Zakon o varstvu osebnih podatkov (ZVOP-1-UPB1). Ur. l. RS 94/2007. Dostopno prek: http://www.uradni-list.si/1/objava.jsp?urlid=200794&stevilka=4690 (28. junij 2008).

Zakon o zasebnem varovanju (ZZasV). Ur. l. RS 126/2003. Dostopno prek: http://www.uradni-list.si/1/objava.jsp?urlid=2003126&stevilka=5385 (13. september 2008).

Zakonodaja.com. 2008. *106. člen - lokacijski podatki, ki niso hkrati podatki o prometu*. Dostopno prek: http://www.zakonodaja.com/zakoni/viii/4/zekom_upb1/cleni/106.clen/106.clen (4. september 2008).

Zaposleni v organizaciji B. 2008. Intervju. Ljubljana, 28. avgust.

Zgodbe uporabnikov. 2000-2006. Dostopno prek: http://www.sledenje.com/?m1=9&m2=2 (4. september 2008).

Wikipedia. 2008a. *Claude Nicolas Ledoux*. Dostopno prek: http://en.wikipedia.org/wiki/Claude_Nicolas_Ledoux#The_Royal_Saltworks_at_Arc-et-Senans_.281774-1779.29 (22. julij 2008).

--- 2008b. *George Orwell*. Dostopno prek: http://en.wikipedia.org/wiki/George_Orwell#Nineteen_Eighty-Four_and_final_years (29. avgust 2008).

--- 2008c. *Global Positioning System*. Dostopno prek: http://fr.wikipedia.org/wiki/Global_ Positioning_System#GPS_et_surveillance (4. september 2008).

--- 2008č. *Michel Foucault*. Dostopno prek: http://en.wikipedia.org/wiki/Michel_Foucault#Discipline_and_Punish (29. avgust 2008).

--- 2008d. *Pametna kartica*. Dostopno prek: http://sl.wikipedia.org/wiki/Pametna_kartica (4. september 2008).

--- 2008e. *Panopticon*. Dostopno prek: http://en.wikipedia.org/wiki/Panopticon (19. maj 2008).

9 PRILOGE

Priloga A: Elektronski intervju z Informacijsko pooblaščenko Natašo Pirc Musar

Ali se ime delovne skupine ARTICLE 29 - Data Protection Working Party pri citiranju obdrži v originalu ali se lahko sklicujem na slovensko ime skupine: Delovna skupina (člena) 29?

Lahko uporabljate slovensko ime, saj je Direktiva 95/46/ES, ki je uzakonila to skupino, prevedena tudi v slovenski jezik. Skupina se imenuje po členu iz omenjene direktive, namreč členu 29.

V kolikšni meri so ta mnenja in delovni dokumenti Delovne skupine 29 zavezujoči za članice EU in za Slovenijo oziroma za njeno pravo?

Niso zavezujoča, so le priporočila in neke vrste smernice, predvsem za delo Evropske komisije pri sprejemanju zakonodaje s teh področij.

Zanima me tudi, ali morda veste, če je katero slovensko podjetje že uvedlo biometrične ukrepe? In če da, katere?

Mnogo njih, odločbe najdete na internetu: http://www.ip-rs.si/nc/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/odlocbe-in-mnenja-varstvo-osebnih-podatkov/ kliknite okence odločbe in okence biometrija.

Ali obstaja tudi kakšno mnenje, priporočilo ali zakon, ki omenja telefonsko prisluškovanje s strani delodajalca?

Ne, ker je prisluškovanje zakonito le, če ga izvaja organ, ki ima izrecno pooblastilo v zakonu.

Ali imam vaše dovoljenje, da vaše odgovore citiram ali povzamem v diplomskem delu in vas navedem kot vir?

Seveda.

Priloga B: Elektronski intervju z vodjo varnostnikov (V) in pravnikom (P) organizacije A

Se zavedate elektronskega nadzora na svojem delovnem mestu?
NA DELOVNEM MESTU NI ELEKTRONSKEGA NADZORA.

Kakšen je elektronski nadzor na vašem delovnem mestu (videokamere, geolokalizacija, nadzor prihodov/odhodov)?
NA DELOVNEM MESTU NI ELEKTRONSKEGA NADZORA.

(P) Ali obstaja kak interni pravilnik ali obvestilo o izvedbi nadzora, njegovem obsegu, trajanju in o potencialnih sankcijah, če je prek nadzora ugotovljena kršitev delovnega razmerja ali če je nadzor neupravičen/prekoračen?
V SKLADU Z ZVOP JE UPRAVA PO PREDHODNEM MNENJU KONFERENCE SINDIKATOV SPREJELA PRAVILNIK O VARSTVU OSEBNIH PODATKOV, V KATEREM JE POSEBEJ OPREDELJEN VIDEONADZOR, EVIDENCA VSTOPOV IN IZSTOPOV IZ POSLOVNIH PROSTOROV TER DRUGE OBLIKE NADZORA. Z USTREZNIM SKLEPOM, NA KATEREGA JE PREDHODNO KONFERENCA SINDIKATOV DALA SVOJE MNENJE, JE UPRAVA V DRUŽBI UVEDLA IZVAJANJE VIDEONADZORA V OBJEKTIH IN PROSTORIH DRUŽBE. O TEM SO BILI DELAVCI PRAVOČASNO SEZNANJENI.

Načini elektronskega nadzora v vašem podjetju (filtriranje e-pošte, kamere, geolokalizacija, biometrija, pametne kartice, prisluškovanje ali snemanje telefonskih pogovorov, prebiranje e- pošte ipd.) in v kolikšni meri se izvaja?
VIDEO NADZOR, KONTROLA PRISTOPA (brezkontaktne kartice, biometrija).

(V) Je katera skupina zaposlenih pod večjim nadzorom? Če da, katera in zakaj?
NE.

Ste vi in ostali zaposleni dobili v podpis aneks k pogodbi ali obvestilo/okrožnico o izvajanju elektronskega nadzora na delovnem mestu?
PISNO OBVESTILO ZAPOSLENIM IN OBVESTILO PREKO INTRANETNIH STRANI.

Menite, da je ves ta elektronski nadzor v vašem podjetju pretiran (zanima me vaše osebno mnenje (zaposlenega) in mnenje z vidika pravnika/vodje varnostne službe?
SPLOH NI PRETIRAN.

Ali menite, da z vsem tem elektronskim nadzorom vaš delodajalec posega v vašo intimo, integriteto, pravico do zasebnosti (zanima me vaše osebno mnenje)?
NE.

Kdo vse ima vpogled v podatke, pridobljene z elektronskim nadzorom?
V SKLADU S PRAVILNIKOM POOBLAŠČENI DELAVCI DRUŽBE.

Koliko časa hranite zgoraj omenjene podatke?
V SKLADU Z ZVOP IN ZZasV (3 MESECE).

Ali je vaše podjetje elektronski nadzor uvedlo za zaščito oziroma varnost zaposlenih ali zaradi nadzora in varovanja organizacijske lastnine pred zaposlenimi in zunanjimi grožnjami oziroma zaradi varovanja osebnih podatkov, ki jih obdelujete?
NAMEN JE VAROVANJE LJUDI IN PREMOŽENJA DRUŽBE, /…/[40] , TER REDA V OBJEKTIH IN PROSTORIH DRUŽBE.

(P) Imate v splošni pogodbi o zaposlitvi člen, kjer se bodoči zaposleni strinja z avtomatizirano obdelavo podatkov za ovrednotenje njegove delovne uspešnosti?
SPLOŠNA POGODBA O ZAPOSLITVI NE OBSTAJA, AMPAK IMA VSAK DELAVEC Z DELODAJALCEM SKLENJENO "SVOJO" POGODBO O ZAPOSLITVI, V KATERI DELAVEC DOVOLJUJE DELODAJALCU, DA ZBIRA, OBDELUJE IN UPORABLJA NJEGOVE OSEBNE PODATKE, ČE JE TO POTREBNO ZARADI URESNIČEVANJA PRAVIC IN OBVEZNOSTI IZ DELOVNEGA RAZMERJA ALI V ZVEZI Z DELOVNIM RAZMERJEM. KER SE NE IZVAJA AVTOMATSKA OBDELAVA PODATKOV DELAVCA ZA VREDNOTENJE NJEGOVE DELOVNE USPEŠNOSTI, NI POTREBNA PREDMETNA DOLOČBA.

Kako varujete podatke, pridobljene z elektronskim nadzorom (fizično in ''virtualno''- s kakšno opremo ali požarnimi zidovi)? Če upoštevate varnostne standarde, prosim, navedite katere (interne, narejene po zakonu,…) in njihova osnovna načela.
V SKLADU Z VARNOSTNIMI STANDARDI. Zakoni: ZVOP-1-UPB1, ZZasV-A, standardi: BS 5979, ISO 17799, ISO 27001.

(V) Imate možnost vpogleda kdo, kdaj in komu je nekdo posredoval pridobljene osebne podatke ali podatke, pridobljene z elektronskim nadzorom?
ZAGOTOVLJENA JE REVIZIJSKA SLED V SKLADU Z VARNOSTNIMI STANDARDI V SISTEMIH, KJER SE HRANIJO OSEBNI PODATKI.

(V) Vršite del/celoto elektronskega nadzora sami ali imate za to najete zunanje izvajalce? In če da, za kater del elektronskega nadzora?
ELEKTRONSKI NADZOR IZVAJA DRUŽBA SAMA PREKO STROKOVNE SLUŽBE.

(V) Ali izvajate videonadzor tudi v dvigalih, garderobi ali toaleti?
NE, TO BI BILO V NASPROTJU Z ZAKONOM.

Kdo se je odločil za uvedbo elektronskega nadzora zaposlenih?
UPRAVA DRUŽBE.

Ali so se odgovorni za uvedbo elektronskega nadzora pred njegovo uvedbo posvetovali z reprezentativnim sindikatom, zaposlenimi, pravnim oddelkom ali s kom drugim?
DA, PRI SPREJETJU PRAVILNIKA O VARSTVU OSEBNIH PODATKOV IN SKLEPA UPRAVE O IZVAJANJU VIDEONADZORA V OBJEKTIH IN PROSTORIH DRUŽBE.

Ali izvajate tudi biometrične ukrepe?
DA. BIOMETRIJA JE BILA UVEDENA Z RAZLOGI POVIŠANJA STOPNJE VARNOSTI DRUŽBE S POSEBNIM POUDARKOM NA VARNOSTI /…/ SISTEMA. VSI ZAPOSLENI SO BILI OBVEŠČENI TER VSAK JE PODPISAL IZJAVO O STRINJANJU IZVAJANJA BIO. UKREPOV NAD NJIMI.

[40] Skrajšala sem tiste odgovore, ki vsebujejo del besedila, ki omogoča razpoznavo organizacij.

Če da, zakaj, katere in ali so vsi zaposleni o tem obveščeni?
Uporabljen je zajem prstnega vzorca. Uveden je bil z namenom povišanja stopnje varnosti družbe s posebnim poudarkom na varnosti /…/ sistema.

Ali imate evidenco vstopov in izstopov v zgradbo za zaposlene in obiskovalce?
DA.

Koliko časa jih hranite?
SE NE HRANIJO - DNEVNO SE UNIČUJEJO.

Ali lahko uporabljate e-pošto tudi za osebne/zasebne zadeve?
V skladu z internim aktom o uporabi elektronske pošte je osebna raba dovoljena v meri, ki ne vpliva na produktivnost delavca, ki ne vpliva na potek poslovnih procesov in ki ne povzroča neposredne ali posredne škode družbi. (11. točka)

Ali delodajalec dopušča uporabo osebne e-pošte prek službenega računalnike (gmail, yahoo in podobne)?
Uporaba osebne e-pošte preko spletnih vmesnikov ni posebej opredeljena, delavci pa morajo upoštevati določila internega akta o uporabi interneta.

Ali ima vaša e-pošta v službi posebna varovala (požarni zid), ki blokira nedovoljene ali vsebine, ki bi potencialno ogrožale vaš računalnik?
V vsej dohodni in odhodni elektronski pošti se preverja prisotnost kakršne koli zlonamerne kode.

Ali je delavcem dovoljena uporaba interneta za neslužbene namene? Če da: koliko časa?
Uporaba je dovoljena samo v skladu z določili internega akta o uporabi interneta.

Ali so katere spletne strani s strani delodajalca zablokirane ali imajo omejen dostop? Če da: katere (npr.: pornografija, strani z orožjem in igrami na srečo in podobno)?
Po potrebi se blokira dostop do naslovov, kjer se nahajajo vsebine katerih izključni cilj je povzročanje škode podjetju oz. delodajalcu.

(V) Vaše strokovno mnenje: Menite, da obstajajo alternativne metode nadzorovanja delavcev, ki bi bile bolj proporcionalne in bi opazovale le tisto, čemur so namenjene? Če da, katere?
Delavci so za svoje rezultate odgovorni sami. V kolikor se izkaže, da prihaja do kršitev pravilnikov, pa se ustrezno ukrepa.
Glede na sedanjo ponudbo tehničnih sredstev je težko govoriti še o kakšnih alternativnih metodah nadzora, ki bi bile izredno ozko usmerjene. Bolj je nadzor (tudi metoda) sofisticiran, bolj je posameznik nadzorovan. Vsak nadzor pomeni določen poseg v posameznikovo sfero in s tem se je treba sprijazniti do tiste meje, ki ne pomeni ogroženosti. Vsekakor pa obstoji "alternativna" metoda, ki sega verjetno v čas, ko se je pojavil homo sapiens sapiens, in sicer da je nekdo ves čas fizično navzoč in drugemu gleda pod prste.

Ali ima vsak zaposleni dostop do podatkov, ki se zbirajo o njem?
Da, V SKLADU Z ZAKONOM.

Ali ste bili že kdaj kaznovani zaradi kršitve Zakona o varstvu osebnih podatkov? (P) Če da, zaradi kršitve katerega člena in kdaj?

NE.

Katerega leta ste uvedli posamezne elemente el. nadzora?

KONTROLA PRISTOPA IN VIDEO NADZOR LETA 1996, KONTROLA PRISTOPA - BIOMETRIJO LETA 2007.

Priloga C: Elektronski intervju z odgovorno osebo v organizaciji B

Se zavedate elektronskega nadzora na svojem delovnem mestu?
Ne.

Kakšen je elektronski nadzor na vašem delovnem mestu (videokamere, geolokalizacija, nadzor prihodov/odhodov)?
Neposredna na delovnem mestu ni elektronskega nadzora, video kamere so v skupnih prostorih in pred vhodi.

Ali obstaja kak interni pravilnik ali obvestilo o izvedbi nadzora, njegovem obsegu, trajanju in o potencialnih sankcijah, če je prek nadzora ugotovljena kršitev delovnega razmerja ali če je nadzor neupravičen/prekoračen?
Vse sodelavce smo v začetku leta 2007 obvestili o načinu video nadzora, lokacijah kamer, času snemanja, kdo so odgovorne osebe, ki lahko pogledajo posnetke. O problematiki je razpravljal tudi senat /…/.

Načini elektronskega nadzora v vašem podjetju (filtriranje e-pošte, kamere, geolokalizacija, biometrija, pametne kartice, prisluškovanje ali snemanje telefonskih pogovorov, prebiranje e- pošte ipd.) in v kolikšni meri se izvaja?
Nobena od navedenih metod se pri nas ne izvaja.

Je katera skupina zaposlenih pod večjim nadzorom? Če da, katera in zakaj?
Ni.

Ste vi in ostali zaposleni dobili v podpis aneks k pogodbi ali obvestilo/okrožnico o izvajanju elektronskega nadzora na delovnem mestu?
Ne.

Menite, da je ves ta elektronski nadzor v vašem podjetju pretiran (zanima me vaše osebno mnenje (zaposlenega) in mnenje z vidika odgovornega v organizaciji?
Ne.

Ali menite, da z vsem tem elektronskim nadzorom vaš delodajalec posega v vašo intimo, integriteto, pravico do zasebnosti (zanima me vaše osebno mnenje)?
Ne.

Kdo vse ima vpogled v podatke, pridobljene z elektronskim nadzorom?
Posebej s strani vodstva določene pooblaščene osebe (varnostnik, računalniški center, vodstvo)

Koliko časa hranite zgoraj omenjene podatke?
3 mesece.

Ali je vaše podjetje elektronski nadzor uvedlo za zaščito oziroma varnost zaposlenih ali zaradi nadzora in varovanja organizacijske lastnine pred zaposlenimi in zunanjimi grožnjami oziroma zaradi varovanja osebnih podatkov, ki jih obdelujete?
Da, varovanje lastnine.

Imate v splošni pogodbi o zaposlitvi člen, kjer se bodoči zaposleni strinja z avtomatizirano obdelavo podatkov za ovrednotenje njegove delovne uspešnosti?
Izjavo posameznika, da se strinja, da se njegovi podatki uporabljajo za potrebe vezane nanj.

Kako varujete podatke, pridobljene z elektronskim nadzorom (fizično in ''virtualno''- s kakšno opremo ali požarnimi zidovi)? Če upoštevate varnostne standarde, prosim, navedite katere (interne, narejene po zakonu,…) in njihova osnovna načela.
Podatke se varuje z gesli, z vodenjem evidence dostopov do teh informacij in videokamerami.

Imate možnost vpogleda kdo, kdaj in komu je nekdo posredoval pridobljene osebne podatke ali podatke, pridobljene z elektronskim nadzorom?
Vodi se evidenca.

Vršite del/celoto el. nadzora sami ali imate za to najete zunanje izvajalce? In če da, za kater del el. nadzora?
Sodelovanje z zunanjim izvajalcem.

Ali izvajate videonadzor tudi v dvigalih, garderobi ali toaleti?
Ne.

Kdo se je odločil za uvedbo elektronskega nadzora zaposlenih?
Ob izgradnji novih prostorov v investicijskem načrtu.

Ali so se odgovorni za uvedbo elektronskega nadzora pred uvedbo elektronskega nadzora posvetovali z reprezentativnim sindikatom, zaposlenimi, pravnim oddelkom ali kom drugim?
Bili so seznanjeni.

Ali izvajate tudi biometrijske ukrepe?
Ne.

Ali imate evidenco vstopov in izstopov v zgradbo za zaposlene? Ali imate evidenco vstopov in izstopov v zgradbo za obiskovalce? Če da, koliko časa jih hranite?
Ne, razen pri receptorju.

Ali ste bili že kdaj kaznovani zaradi kršitve Zakona o varstvu osebnih podatkov? (P) Če da, zaradi kršitve katerega člena in kdaj?
Ne.

Katerega leta ste uvedli posamezne elemente elektronskega nadzora?
2005-06.

Priloga Č: Intervju z vodjo tržnega segmenta v NLB d.d. Konstanco Rettinger

Kaj je to debetna kartica?
Debetna kartica je kartica osebnega računa, ki omogoča tekoče opravljanje transakcij plačilnega prometa in dvig gotovine iz osebnega računa (TRR), pri čemer je osebni račun obremenjen z izvedeno transakcijo takoj, brez zamika plačila.

Kakšna je razlika med debetno in pametno kartico iz bančnega vidika?
Debetna kartica je lahko pametna kartica, vsaka pametna kartica pa ni nujno, da je tudi debetna kartica.

Kaj je to kreditna kartica?
Kreditna kartica je kartica, kjer se nakup v okviru odobrenega limita poravnava s časovnim zamikom v višini izbrane vrednosti 10, 20 ali 33 odstotkov v zaporednih mesečnih obrokih. To pomeni, da se mesečno poravnava le del obveznosti v izbranem deležu in ne celoten nakup.

Ali je pametna kartica lahko tudi kreditna kartica?
Pametna kartica je lahko tudi kreditna kartica, ja. Odvisno je namreč od zmogljivosti čipa na pametni kartici.

Ali imam vaše dovoljenje, da vaše odgovore citiram ali povzamem v diplomskem delu in vas navedem kot vir?
Ja.

Priloga D: Telefonski intervju z raziskovalcem pri Informacijskem pooblaščencu Blažem Pavšičem

Ali se pri zaznanih kršitvah tega zakona plača kazen za vsako zaznano kršitev posebej ali v enkratnem znesku? Primer: obstaja 10 istih kršitev. Ali se bo plačalo osnovno vsoto ali desetkratnik predpostavljene kazni?
Ja, kazni se seštevajo.

Če se ob izdaji zakona ne spremeni postopkov ali je to prekršek? Ali obstaja neko časovno okno ob izdaji zakona, ko se lahko postopki in nadzor spremenijo?
Spremembam zakonov je treba slediti; je pa ob izdaji zakona določen čas za pripravo, npr. 15 dni ali kakršen koli časovni okvir, ki je določen v prehodnih določbah.

Ali imajo podjetja ob zaznani kršitvi možnost popravka kršitev ali se jim že takoj predpiše kazen?
Odvisno je od okoliščin in od inšpektorja: lahko podjetje dobi globo, opomin ali pa se ga da v nadaljevalni prekršek. Opomin ali opozorilo se da, če ni škodljivih posledic; poleg tega obstaja čas za odpravo kršitev v inšpekcijskem postopku.

Ali je kršitev tudi to, če na primer delodajalec naknadno, po uvedbi elektronskega nadzora, pobere pristanke delavcev za nadzor ali skliče posvet s sindikatom le za videz in njihovih predlogov ne upošteva?
Je kršitev. Večja pa je kršitev, če se zaposlenih sploh ne obvesti, kot če se jih obvesti naknadno.

Koliko podjetij v Sloveniji že uporablja biometrične ukrepe?
Mislim, da se številka giblje okoli 10 odstotkov ali manj; rekel bi, da okoli 30 podjetij. Za bolj zanesljivo številko si oglejte našo spletno stran.

Kateri biometrični ukrepi so najpogostejši?
Večina podjetij uporablja preverjanje prstnih odtisov.

Ali se število pritožb čez delodajalce v primeru nadzorovanja in prebiranja elektronske pošte zaposlenih povečuje ali zmanjšuje?
Tega podatka trenutno nimam. Za statistične podatke o elektronski pošti raje poglejte v Letno poročilo Informacijskega pooblaščenca, ki je na naši spletni strani.

Po katerem zakonu se kaznuje vpogled v elektronsko pošto zaposlenega?
Nezakonita obdelava prometnih podatkov, ki se dojemajo kot osebni podatki, se obravnava in kaznuje po ZVOP-1. Pregledovanje in branje vsebine elektronske pošte pa spada pod širšo pravico varovanja zasebnosti, ki jo varuje Ustava.

Ali imam vaše dovoljenje, da vaše odgovore citiram ali povzamem v diplomskem delu in vas navedem kot vir?
Ja.