



B&B  
VIŠJA STROKOVNA ŠOLA

Diplomsko delo višješolskega strokovnega študija  
Program: Komercialist  
Podjetniški modul

## **NADZOR NA DELOVNEM MESTU Z UPORABO INFORMACIJSKE TEHNOLOGIJE**

Mentor: mag. Alenka Bradač, univ. dipl. org.  
Lektor: Grega Rihtar

Kandidat: Sead Tugo Gavranović

Kranj, oktober 2009

## **ZAHVALA**

Zahvaljujem se mentorici, mag. Alenki Bradač, za strokovno in idejno pomoč pri izdelavi diplomskega dela.

Posebej bi se zahvalil ženi Editi in otrokom Katarini, Barbari in Filipu za potrpljenje in moralno podporo za ves čas študija.

Zahvaljujem se tudi lektorju Gregi Rihtarju, ki je lektoriral moje diplomsko delo.

## **IZJAVA**

»Študent Sead Tugo Gavranović izjavljam, da sem avtor tega diplomskega dela, ki sem ga napisal pod mentorstvom gospe mag. Alenke Bradač.«

»Skladno s 1. odstavkom 21. člena Zakona o avtorskih in sorodnih pravicah dovoljujem objavo tega diplomskega dela na spletni strani šole.«

Dne, 3. oktober 2009

Podpis: Sead Tugo Gavranović

## **POVZETEK**

Skozi celotno zgodovino človeštva in vse do danes se je človek trudil in razvijal različne stvari oziroma predmete, s katerimi si je olajšal marsikatero delo in s tem tudi življenje. Človek je s tem seveda korenito posegel v naravo in njeno okolje, prav tako pa tudi v družbo in njene medsebojne odnose.

V današnjem času si človek ne more predstavljati življenja brez uporabe moderne tehnologije in tehnoloških dosežkov sodobnega časa. Med novejšie tehnološke iznajdbe prištevamo informacijsko tehnologijo, ki jo danes množično uporabljamo na vseh ravneh družbenega življenja. Tudi v podjetjih se vse pogosteje odločajo uporabljati informacijsko tehnologijo za pomoč in olajšanje poteka različnih delovnih procesov. Z vse hitrejšim tehnološkim razvojem je postala informacijska tehnologija vse bolj uporabna in zanesljiva.

Zavedati pa se moramo, da informacijska tehnologija poleg prednosti prinaša tudi slabosti. Tako je na primer odvisna od: energetskih virov, strojne opreme v smislu stalnih nadgrajevanj, ki v veliko primerih ni kompatibilna z obstoječim sistemom, kar posledično pomeni, da hitro zastarajo in zahtevajo pogostejši nakup novih sistemov in naprav. Tudi programska oprema ni večna in včasih se pojavijo napake in pomanjkljivosti, zato potrebujemo za nemoten proces dela dobro servisno službo ali lasten strokovni kader. Ti pa morajo stalno slediti spremembam in novostim na trgu in se poleg tega tudi dodatno izobraževati. Vse to pa je povezano z dokaj velikimi stroški.

Največji problem pri uporabi informacijske tehnologije predstavlja varnost. Pri tem mislimo na nepooblaščen ali nekontrolirano uporabo ali vpogled v sisteme za obdelovanje in pretok različnih podatkov, ki so poslovno ali zasebno tajni oziroma zaupni. Tako stalno nastajajo nove oblike varnostnih programov, ki naj bi preprečevali nepooblaščenim osebam vstop v programe in na ta način vpogled v podatke, katere bi lahko zlorabili.

V tem diplomskem delu bomo podrobnejše predstavili problematiko nadzora in vdora v zasebnost z uporabo informacijske tehnologije. Največ bomo govorili o zlorabi informacij in kršenju pravic do zasebnosti pri izvajanju nadzora na delovnem mestu. Poskušali bomo določiti, kje je meja med javnim in zasebnim, dopustnim in nedopustnim nadzorom, upoštevajoč moralno-etične vrednote in načela v sedanji družbi.

## **KLJUČNE BESEDE:**

- ZASEBNOST
- NADZOR
- VAROVANJE
- INFORMATIKA
- ODNOSI

## **ZUSAMMENFASSUNG**

Seit dem Beginn der Menschheit bis zur heutigen Zeit, hat sich der Mensch viel Mühe gemacht und verschiedene Sachen bzw. Gegenstände entwickelt, die ihm so manch eine Arbeit und damit auch das ganze Leben erleichtert haben. Jedoch wurden dadurch radikale Eingriffe in die Natur und in die Umwelt gemacht, die auch ihre Auswirkungen in der Gesellschaft und in den zwischenmenschlichen Beziehungen haben.

Heutzutage kann man sich ein Leben ohne Nutzung moderner Technologien und technologischer Errungenschaften nicht mehr vorstellen. Zu den neueren technologischen Errungenschaften zählen wir auch die Informationstechnologie, die wir heutzutage massenhaft nutzen und das auf allen Ebenen des gesellschaftlichen Lebens. Auch Unternehmen entscheiden sich immer mehr für die Nutzung der Informationstechnologien und zwar zur Hilfe und Erleichterung verschiedener Arbeitsprozesse. Durch die immer schnelleren technologischen Entwicklungen erweiterte sich der Verwendungszweck der Informationstechnologie und gewann auch an Zuversicht.

Man muss sich aber auch bewusst werden, dass die Informationstechnologien, neben all ihren Vorzügen auch Nachteile bringen. So hängen sie von verschiedenen Faktoren ab: z.B. von den Energiequellen, der Hardware, im Sinne des ständigen Aufbaus, welcher jedoch in vielen Fällen mit dem bereits bestehenden System nicht kompatibel ist, was wiederum dazu führt, dass sie schnell veralten und deshalb öfters der Ankauf von neuen Systemen und Geräten erforderlich ist. Da jedoch die Hardware nicht für die Ewigkeit gemacht ist und sich auch öfters Fehler und Mangel zeigen können, brauchen wir, um den Arbeitsprozess so ungestört wie möglich durchzuführen, einen guten Servicedienst oder aber eigene Fachkräfte, die die ständigen Änderungen und Neuheiten auf dem Markt verfolgen müssen und sich ebenso ständig weiterbilden sollten. All dies ist jedoch mit ziemlich hohem Kostenaufwand verbunden.

In Verbindung mit der Informationstechnologie stellt das größte Problem die Sicherheitsfrage dar. Dabei denken wir an den unbefugten und nicht kontrollierten Gebrauch und die Einsicht in die Datenbearbeitungssysteme, die beruflich oder privat geheim bzw. vertraulich sind. Deshalb werden immer neue Formen von Sicherheitsprogrammen entwickelt, die unbefugten Personen den Eintritt und auf diese Weise auch den Einblick in Daten, verbieten, welche sie mißbrauchen könnten.

In dieser Diplomarbeit werden wir genauer die Problematik der Überwachung und den Eindrang in die Privatsphäre durch Gebrauch der Informationstechnologien erläutern. Am meisten werden wir über den Mißbrauch von Informationen und den Mißbrauch des Rechts auf Privatsphäre bei der Ausübung der Aufsicht auf dem Arbeitsplatz. Wir werden versuchen die Grenze zwischen öffentlichem und privatem und zwischen erlaubter und unerlaubter Aufsicht bzw. Überwachung zu setzen und werden dabei die moralisch-ethischen Werte und Grundsätze der heutigen Gesellschaft in Betracht nehmen.

## **SCHLÜSSELWORTE:**

- PRIVATSPHÄRE
- AUFSICHT
- SCHUTZ
- INFORMATIK

➤ BEZIEHUNGEN

## KAZALO

<b>1</b>	<b>UVOD</b>	<b>1</b>
1.1	PREDSTAVITEV PROBLEMA	1
1.2	PREDSTAVITEV OKOLJA	1
1.3	PREDPOSTAVKE IN OMEJITVE	1
1.4	METODE DELA	1
<b>2</b>	<b>ZASEBNOST</b>	<b>3</b>
2.1	OPREDELITEV ZASEBNOSTI	3
2.2	ZASEBNOST IN DRUŽBA	3
2.3	ZASEBNOST IN NJEN POMEN	4
2.4	ZASEBNOST IN INTERNET	5
2.5	ZASEBNOSTNA MEJA	5
<b>3</b>	<b>NADZOR</b>	<b>7</b>
3.1	NADZOR IN DRUŽBA	7
3.2	NADZOR KOT PANOPTIKON	8
3.3	VRSTE IN ZNAČILNOSTI NAZDORA	10
3.4	NADZOR IN INTERNET	10
3.5	SODOBNI NADZOR	11
3.5.1	GLAVNE ZNAČILNOSTI SODOBNEGA NADZORA	11
3.5.2	NADZOR V JAVNOSTI	12
3.5.3	NADZOR OSEBNIH PODATKOV	14
3.5.4	NADZOR KOT DRUŽBENO PROFILIRANJE	14
<b>4</b>	<b>SODOBNE TEHNOLOGIJE NADZORA</b>	<b>16</b>
4.1	VIDEONADZORNE NAPRAVE	16
4.2	NADZOROVANJE S POMOČJO BIOMETRIJE	17
4.3	NADZOR PRI UPORABI SPLETNE MREŽE	18
4.4	SATELITSKI NADZOR IN GPS	20
4.4.1	UPORABA GPS SISTEMOV NA VOZILIH	21
4.5	PRISLUŠKOVANJE IN OPAZOVANJE	22
4.5.1	PRISLUŠKOVANJE Z UPORABO TEHNOLOGIJE	23
4.5.2	NADZOROVANJE KOT OPAZOVANJE	23
4.6	NADZOR NA DELOVNEM MESTU	23
4.6.1	NADZOR NA DELOVNEM MESTU V ŠTEVILKAH	25
<b>5</b>	<b>PRAVNI RED IN KRŠITEV PRAVIC ZASEBNOSTI</b>	<b>26</b>
5.1	VARSTVO PRAVIC V SLOVENIJI	26
5.1.1	VARSTVO POSAMEZNIKA DO ZASEBNOSTI	26
5.2	ZAKON O VARSTVU OSEBNIH PODATKOV	27
5.2.1	INFORMACIJSKA POOBLAŠČENKA RS	27

5.2.2	ZAKON IN VIDEONADZOR NA DELOVNEM MESTU .....	28
5.2.3	NESPOŠTOVANJE ZAKONSKIH DOLOČIL .....	29
<b>6</b>	<b>MNENJE DELODAJALCA IN DELOJEMALCA O NADZORU NA DELOVNEM MESTU .....</b>	<b>31</b>
6.1	<i>INTERVJU Z DELODAJALCEM .....</i>	<i>31</i>
6.2	<i>INTERVJU Z UPORABNIKOM GPS-a V VOZILU.....</i>	<i>33</i>
6.3	<i>NADZOR NA DELOVNEM MESTU – »DA ali NE«? .....</i>	<i>35</i>
6.4	<i>TANKA MEJA MED ZASEBNIM IN SLUŽBENIM .....</i>	<i>36</i>
<b>7</b>	<b>ZAKLJUČEK .....</b>	<b>37</b>
	<i>LITERATURA IN VIRI .....</i>	<i>38</i>
	<i>KAZALO SLIK.....</i>	<i>39</i>
	<i>POJMOVNIK.....</i>	<i>39</i>
	<i>KRATICE IN AKRONIMI .....</i>	<i>39</i>

# 1 UVOD

## 1.1 PREDSTAVITEV PROBLEMA

V diplomskem delu bomo obravnavali uporabo informacijske tehnologije za nadzor na delovnem mestu in v povezavi s tem pojavljajoča se etična vprašanja, kot so: varstvo osebnih podatkov, možnost zlorabe in nekontroliranega vpogleda nepooblaščenim osebam, nadzor in s tem v zvezi kršenje pravice do zasebnosti.

Problem, ki ga bomo obravnavali, je nasprotovanje uporabe elektronskih naprav za nadziranje na delovnem mestu delodajalcev do zaposlenih. Prvi se vse bolj zavzemajo, da bi zaposleni imeli vse manj pravic pri odločanju, organizaciji in samem opravljanju dela. Tako bi pridobili boljši pregled nad procesi dela, povečali nadzor in vzpostavili večji vpliv na nemoten potek delovnega procesa in s tem povezano doseganje zastavljenih načrtov in ciljev, ki so potrebni za uresničevanje tekočega poslovanja in obstoj podjetja. Zaposleni pa se na drugi strani nenehno borijo za pravice in svoboščine, ki jim pripadajo pri opravljanju dela.

Vse prevečkrat se dogodi, da delodajalci izkoristijo nadrejeni položaj in prekoračijo pooblastila in s tem kršijo pravico do zasebnosti na delu zaposlenih.

## 1.2 PREDSTAVITEV OKOLJA

Za boljšo predstavo o problematiki nadzora na delovnem mestu smo izbrali podjetje, v katerem je osnovna dejavnost varovanje in nadzorovanje objektov, ljudi in premoženja. Podjetje deluje na območju Slovenije že več kot dvajset let. Prav zaradi večletnih lastnih izkušenj na omenjenih področjih dela so sledili tehnološkim spremembam na področju informacijske tehnologije in jo skladno z obstoječo zakonodajo uporabljajo za nadzor zaposlenih v svojem podjetju.

## 1.3 PREDPOSTAVKE IN OMEJITVE

V diplomskem delu kot predpostavko navajamo zlorabo varstva osebnih podatkov, nenapovedano opazovanje in nadzor gibanja, prisluškovanje telefonskim pogovorom, branje elektronske pošte in kršenje pravice do zasebnosti. Velik problem je, da zlorab v zvezi s tem ni lahko odkriti oziroma lahko traja dlje časa. Zato lahko pričakujemo, da se bodo tovrstna dejanja v prihodnosti še dogajala. V poslovnem in zasebnem življenju se vsak dan srečujemo z novimi oblikami zlorab, kot so ponarejanje bančnih kartic, vdor preko interneta v podatkovno bazo na vašem računalniku itd.

## 1.4 METODE DELA

Teoretična osnova v diplomskem delu so obstoječa zakonodaja v Sloveniji in Evropski uniji, moralno-etična načela, razni članki v informativnih medijih, internet in že dostopna literatura.

Za praktični del smo za metodo dela izbrali intervju, ki ga bomo opravili z direktorjem podjetja kot predstavnika delodajalca in zaposlenega delavca kot predstavnika delojemalca. Na ta način pridobljene odgovore in mnenja bomo med seboj primerjali in analizirali. Rezultati nam bodo vodilo za postavitve meje med še dopustnim službenim nadzorom in poseganjem v zasebnost zaposlenih na delovnem mestu.

## 2 ZASEBNOST

### 2.1 OPREDELITEV ZASEBNOSTI

Pravica do zasebnosti se je torej razvila z nastankom kapitalizma v 18. stoletju, najprej kot vrednota, in se od takrat dalje vse bolj uveljavljala. Zasebnost tako razumemo kot zaščito svobode posameznika in kot takšna ima tudi nasprotnike. Kot največjega akterja, ki ogroža posameznikovo zasebno svobodo, danes označujemo družbo in državo. Vendar se svoboda zasebnosti ne nanaša samo na politično oblast, ampak tudi na družbo. Tako se država pojavlja na eni strani kot kršitelj poseganja v zasebnost ljudi in omejevanje človekovih pravic, po drugi strani pa kot varuh pred vplivi družbe, ki ogrožajo zasebnost. Univerzalne definicije zasebnosti oziroma pravice do zasebnosti ni, ker je zasebnost relativna in subjektivna. Vsak ima drugačno mnenje in pričakovanja glede zasebnosti, ki se razlikujejo od družbene ravni. Tako nastane problem definicije zasebnosti, ker zasebnost ščiti svobodo posameznika. Individualna svoboda pa ne more biti napovedana in ne pogojena (Gutwirth v Kovačič, 2006), saj jo vsak vidi s svojimi očmi. Pravna teorija se zaradi tega izogiba natančnemu definiranju pravice do zasebnosti. Tako se zasebnost v sodni praksi ne nanaša le na pravico biti sam ter zaščito posameznika pred nepooblaščenim in neupravičenim nadzorovanjem, ampak tudi na pravico do svobode odločanja o rojstvu otrok, svobodno odločanje za različne spolne prakse. Sodišča so na podlagi pravice do zasebnosti posameznika zaščitila tudi pred škodljivimi vplivi iz okolja, kot je hrup, smrad, onesnaženje zraka in okolja. Zasebnost je svobodna volja posameznika do odločanja brez prisile in vmešavanja drugih. Prisila ni samo fizična, ki jo vidimo ali opazimo, ampak se kaže tudi v nevidni obliki, kot je izvajanje raznih manipulativnih oblik psihološkega pritiska na posameznika. Torej lahko rečemo, da so svoboda, avtonomija in samoodločanje bistvene prvine zasebnosti (Gutwirth v Kovačič, 2006).

### 2.2 ZASEBNOST IN DRUŽBA

Z naraščanjem prebivalstva se je oblikovala družina, ki je vse bolj postajala zasebna, delovno in organizacijsko okolje pa javno. Tako sta se oblikovali dve sferi družbenega življenja, zasebna ali intimna in javna ali socialna. To pomeni, da se delo vse bolj oddaljuje od zasebnega in prehaja v javno sfero, medtem ko se družina vse bolj umika v zasebno. Družina začne izgubljati tudi funkcijo vzgoje, varstva, oskrbe, pojavi se osebni in ne več družinski dohodek, oblikuje se razmejitev med prostim in delovnim časom, družina pa postaja porabnik prihodka in prostega časa. Intimna sfera se je tako zožila na območje ožje družinske porabniške skupnosti (Habermas v Kovačič, 2006). Del zasebne sfere se odcepi v socialno, del pa v intimno. Demokratične države v intimno sfero ne posegajo, kar pa ne moremo reči za javnost oziroma družbo. Prihod interneta je povečal problem zasebnosti tako, da je povečal možnosti zlorab zasebnosti. Pri razvoju interneta v svetu še vedno prevladuje ameriški pravni sistem in način obravnavanja zasebnosti. Uporabnik, ki vstopi v internet, je avtomatično prisoten v obeh sferah. Z razvojem multimedijske dejavnosti in razvojem sodobnega potrošništva to postane vse bolj očitno. Večkrat se dogaja, da postanejo osebne zgodbe ljudi tržno blago in se v javnosti objavljajo v

korist marketinških aktivnosti, po drugi strani pa postaja zasebnost ovira pri uresničevanju ekonomskih in političnih interesov. Nadzor vse bolj postaja orodje množičnega marketinga in upravljanja družbe (Habermas v Kovačič, 2006). V zvezi s tem Habermas pravi: "Nasploh se množični mediji priporočajo kot naslovniki za osebne stike in težave, kot avtoritete življenjske pomoči ...", ter "problematiko zasebne eksistence javnost delno vsrka: če je že ne razrešujejo pod vrhovnim nadzorom publicistične javnosti, jo pred njo vsaj prikazujejo" (Habermas v Kovačič, 2006).

Zanimivo je, da se je leta 2004 na internetu zelo razmahnilo pisanje tako imenovanih spletnih dnevnikov; blogov (izraz blog izhaja iz angleških besed web in log), v katerih posamezniki javno pišejo (oziroma objavljajo na spletni strani) svoj dnevnik. Posamezniki torej "na očeh javnosti" javno razgrinjajo svoja najbolj skrita razmišljanja, osebne probleme itd.

Lahko rečemo, da zasebna sfera lahko predstavlja zaščito in zavetje posameznika pred družbo, ki pripomore k razvoju svobodnega in avtonomnega človeka. Ker vdor v zasebnost lahko negativno vpliva na osebno avtonomijo, individualnost, dostojanstvo in neodvisnost posameznika, je zasebnost pomemben dejavnik, ki omogoča svobodo posameznika (Wagner DeCew v Kovačič, 2006). »Nekateri pravijo, da je zasebnost bistvena za biti človek, vendar je v resnici povsem mogoče biti človek brez zasebnosti. Bolj točno je reči, da je zasebnost nujna za biti svoboden človek.« (Sykes v Kovačič 2006).

### 2.3 ZASEBNOST IN NJEN POMEN

Zasebna sfera se je skozi zgodovinske dogodke zaradi življenjske nujnosti premaknila na območje svobode. Tako zasebnost ni več nujno zlo, temveč je postala vrednota, ki je predpogoj človekove svobode (Kovačič, 2006). Zasebnost je tudi območje, na katerem je človek varen in skrit pred svetom, in sicer na dva načina: pred vplivi iz sveta in pred tem, da posameznik postane viden v svetu. Arendtova namreč pravi, da so lastne štiri stene edini kraj, v katerega se lahko umaknemo pred svetom, ne samo pred tistim, kar se v njem stalno dogaja, temveč pred njegovo javnostjo, pred tem, da smo videni in slišani (Arendt v Kovačič, 2006). Zasebnost je torej meja med posameznikom in drugimi, meja, katere naloga je filtriranje pretoka informacij v obe smeri. Habermas in Arendtova izpostavljata dva zasebna vidika: osebni prostor, torej prostor intimne, in prostor, ki omogoča interesno združevanje, torej delovanje. Za delovanje, neodvisno od družbenih prisil, sta pomembna oba. Takšna delitev je opazna tudi v pravni kodifikaciji pravice do zasebnosti (8. člen Evropske konvencije o človekovih pravicah), kjer je pravica do zasebnosti klasificirana na podlagi štirih vidikov: zasebnega življenja, družinskega življenja, doma in dopisovanja. Arendtova ugotavlja, da ogrožanje svobode v moderni družbi ne prihaja od države, kot domneva liberalizem, temveč od družbe (Arendt v Kovačič 2006). Iz tega sledi, da državljske svoboščine lahko zagotavlja zgolj država nasproti družbi. Če se je torej zasebna sfera zožila na intimno in če je tudi intimno čedalje bolj na udaru sodobne družbe, potem se lahko zgodi, da je edini zasebni prostor, ki ostane posamezniku, njegova subjektivnost. Procesi čedalje obsežnejšega nadzorovanja pa zasebni prostor le še bolj ožijo (Arendt v Kovačič 2006).

## 2.4 ZASEBNOST IN INTERNET

Danes se vsak dan pojavlja mnogo novih tehnologij, ki tako ali drugače omogočajo ali onemogočajo zasebnost. Ne vemo pravzaprav, za kaj smo ljudje začeli najprej uporabljati sodobno tehnologijo, za zaščito zasebnosti ali za javno razkrivanje zasebnosti. V prvem primeru gre seveda za razne elektronske sisteme, ki preprečujejo vpogled nezaželenim v domače življenje drugih. To so na primer razni domofoni, videofoni, digitalni telefoni in telefonske tajnice, prenosni telefoni ter že malce zastareli, tako imenovani „pagerji“ (elektronska naprava, ki uporabniku prikaže na malem zaslonu telefonsko številko in čas kličočega). Vse te naprave namreč omogočajo komunikacijo le, če to sami želite oziroma, če ne želite, se preprosto potuhneta in videti bo, kot da vas ni doma oziroma ste nedosegljivi. Tudi spletno komuniciranje je postalo splošno vsakdanje opravilo slehernega človeka. Tako preko pisanja sporočil ali oddajanja mnenj na forumih, pisanja blogov, kot tudi na spletnih straneh Facebooka in MySpacea, kjer si sami oblikujemo svojo lastno podobo in podatke, ki so dostopni vsem uporabnikom. Seveda lahko s kodami zaščitimo te podatke in opredelimo, komu bodo dostopni za ogled in komunikacijo. Toda če to storimo, je vprašanje, zakaj smo potem sploh prisotni na teh forumih ali spletnih straneh.

## 2.5 ZASEBNOSTNA MEJA

Vsak človek ima pravico do zasebnosti. Družba pa je določila mejo med zasebnim in javnim, kar pomeni mejo, do koder lahko družba posega oziroma vdre v zasebno sfero ali življenje posameznika (Kovačič, 2006). Alan Westin (Lyon v Kovačič, 2006) pravico do zasebnosti definira sledeče: »Posamezniki, skupine in institucije imajo pravico kontrolirati, spreminjati, upravljati in brisati informacije o sebi in odločati kdaj, kako in v kakšnem obsegu so te informacije posredovane drugim«. Danes prevladuje mnenje, da vse bolj izgubljam zasebnost in trend kaže, da se bo to še nadaljevalo v naslednjih letih. Sodobna tehnologija je omogočila in pospešila zbiranje osebnih podatkov. Scott McNealy (Lyon v Kovačič, 2006) navaja: »Zasebnosti je konec, sprijaznite se!« (ang. Privacy is dead. Get over it!). Ljudi bo v prihodnosti vedno bolj skrbelo o njihovi zasebnosti in svobodi (Pečar v Kašnik 2006), saj je z razvojem sodobne informacijske tehnologije zasebnost bolj ogrožena kot kdaj koli prej! Zanimivo je, da je večina ljudi zaskrbljena o svoji zasebnosti, vendar pa v praksi malo poskrbijo za ustrezno zaščito ali varovanje. Mellros pravi, (v Kovačič, 2003) preventivo vidi v tem, da je pomembno, da oni (država) vedo o nas manj, da pa mi vemo o njih več.

Prav nasprotno meni Gary Rowden, ki je v devetdesetih letih prejšnjega stoletja sodeloval pri postavitvi videonadzora v Veliki Britaniji. V nekem intervjuju za Delo (Krašič v Kašnik, 2006) je dejal, da se miselnost ljudi spreminja. Ko so slišali za „Velikega Brata“, so mnogo let imeli pomisleke glede nezaželenega opazovanja s kamerami. Menili so, da je to nepošten vdor v zasebnost. Danes pa so mnenja, da jih „Veliki Brat“ ne le opazuje, ampak jim tudi pomaga. To zagovarjajo tisti, ki pravijo, da nimajo česa skrivati in se zato tudi nimajo česa bati. Posledice tako nosimo vsi, tako nedolžni kot krivi ali osumljeni kriminalnih dejanj (Lyon v Kovačič, 2006). Ali pa kot navaja Kovačič »nadzorovanje je dobilo hinavski obraz, saj je postalo neopazno, toda povsod prisotno, postalo je prijazno in prostovoljno«.

Torej ljudje danes menijo, da se meja zasebnosti vse bolj oži in zmanjšuje. Lahko pa poudarimo, da je zasebnost v Evropi dosti bolj varovana kot na primer v ZDA. To je zasluga ugodne zakonodaje na področju varstva osebnih podatkov. To potrjuje tudi intervju z informacijsko pooblaščenko za „Studio City“ (3. 7. 2006), kjer je povedala, da je Slovenija glede videonadzora še raj.

### 3 NADZOR

Pod besedo ali pojmom nadzor pojmujeemo sistematično pregledovanje, spremljanje poteka ali razvoja česa, zlasti določene dejavnosti.

Beseda nadzorovati pa pomeni sistematično pregledovati, spremljati potek ali razvoj česa, zlasti določene dejavnosti ali oseb: tudi nadzorovati delo, poslovanje; z opazovanjem, pregledovanjem ugotavljati položaj, stanje česa: prizadevati si skrbeti za pravilno ravnanje, vedenje, delo koga: Nadzorovati učence, uslužbence, ljudi (SSKJ, 2009).

#### 3.1 NADZOR IN DRUŽBA

Nadzorovanje v splošnem pomenu besede posameznikom omogoča delovanje, sodobna družba pa brez nadzorovanja ne more obstajati. Vendar pa je treba ločevati med nadzorom nad stvarmi in nadzorom nad ljudmi, pri čemer gre za vprašanje prisile in drugih oblik usmerjanja delovanja posameznikov (Kovačič, 2006).

V nadaljevanju se bomo opredelili zgolj na nadzorovanje ljudi. Nadzor je torej namenjen spoznavanju delovanja posameznikov in s tem povečanju nadrejenosti oziroma gospodovalnosti nad njimi. Nadzor se lahko pojavlja na več načinov: kot zbiranje informacij, sledenje ali zasledovanje, opazovanje itd. Država ali družba lahko nadzor uporabi proti posamezniku, hkrati pa lahko posameznik uporabi nadzor proti državi. Značilno za informacije javnega značaja je, da so lahko orodje v boju proti prikritemu nadzoru s strani države. Kljub temu, da je nadzor mogoče uporabiti v obe smeri, pa s sodobno tehnologijo lahko izvajamo nadzor le v eno smer. Obstaja seveda tudi tehnologija (kriptografija), katera omogoča izogibanje nadzoru, vendar je tudi to tehnologijo mogoče onesposobiti. Seveda ima nadzor ljudi še vedno negativen predznak, to pa zaradi tega, ker je postal bolj neopazen in kot takšnega ga jemljemo vse bolj prijaznega, čeprav hinavskega. Predvsem pa je postalo tako rekoč nujno za življenje v sodobni družbi. Slogan iz Orwellovega romana „Veliki brat te opazuje!“ se spreminja v „Veliki brat skrbi zate!“ (Whitaker v Kovačič 2006).

Življenje v sodobni družbi tako nujno zahteva pristanek na določeno stopnjo nadzora. In še več, če posameznik pristane na še večjo stopnjo nadzora, je deležen še dodatnih ugodnosti (Kovačič, 2006). Nadzor je sredstvo izvajanja moči!

Začenja se oblast nad življenjem, oblast, ki tokrat deluje tako, da okrog naključnosti namešča varnostne mehanizme (na primer socialna zavarovanja, spremljanje epidemij itd.), ki ne delujejo na ravni posameznika, temveč na ravni populacije. Zato je danes nadzorovanje posameznikov ne samo sredstvo disciplinskega nadzora, marveč tudi sredstvo za zagotavljanje pravic družbene participacije; posamezniki smo že s samo participacijo v družbi (uveljavljanje državljskih, zdravstvenih, zaposlitvenih in drugih pravic) izpostavljeni nadzoru, ta izpostavljenost pa je nujna za naše preživetje. „Moderna država blaginje brez računalnikov in zbirk podatkov, torej nadzora, ne more delovati“ (Mayer-Schönberger v Kovačič, 2006). S tem pa se spremeni tudi tehnologija kaznovanja - neprilagojenih posameznikov ni več potrebno kaznovati, dovolj je le, da jih izvržemo in pustimo umreti.

Prav zaradi hkratnega delovanja discipline in regulacije se nadzor danes pojavlja v obliki nadziranja ljudi, ki se ga v glavnem poslužujejo države in nosilci oblasti, ter v obliki zbiranja podatkov o ljudeh. Skratka, gre za družbo, v kateri nadzor v njenem

temelju ohranja ravnotežje (zaradi česar se sodobna družba boji odpraviti nadzorovanje in zaradi česar v tehtanju med pravico do zasebnosti in drugimi pravicami in ugodnostmi skoraj praviloma izgublja pravica do zasebnosti). Ta nadzor pa je močno odvisen od tehnologije. In to ne od katere koli tehnologije, temveč od informacijske tehnologije, zato Webster predlaga, da bi bilo morebiti namesto pojma informacijska družba boljše uporabljati pojem družba nadzora (Webster v Kovačič, 2006).

### 3.2 NADZOR KOT PANOPTIKON

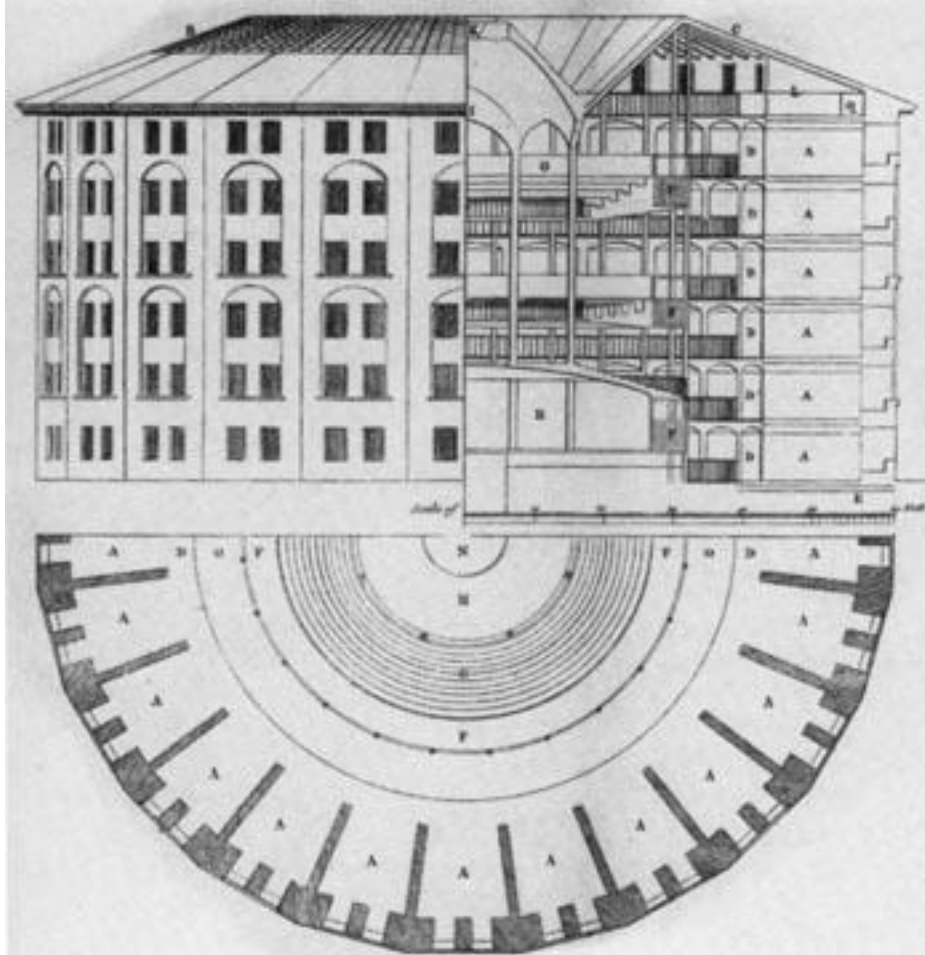
Konec 18. stoletja je angleški pravnik in filozof Jeremy Bentham predstavil načrt zapora, ki ga je poimenoval Panoptikon. Gre za zamisel, kako naj bi bil zgrajen zapor, ki bi omogočal nadzor nad zaporniki v vsakem trenutku. Zgrajen naj bi bil v obliki kroga, na obodu bi bile zaporniške celice, ki bi bile postavljene tako, da zaporniki med seboj ne bi mogli komunicirati. V središču zgradbe je prostor, namenjen nadzorniku, vmes pa je prazen prostor. Vsaka celica ima na zunanji strani okno, skozi katero pa ni moče videti ven, na notranji strani pa zamrežena vrata, skozi katera lahko nadzornik opazuje dogajanja v celicah. Od nadzornika do celic naj bi bile nameščene kositrne cevi, katere bi omogočale prisluškovanje zapornikom. Na takšen način zgrajen zapor omogoča, da nadzornik vidi in sliši zapornike, oni pa ne vidijo in ne slišijo njega. Po Benthamovi teoriji je pomembno, da morajo zaporniki vedno čutiti, da so nadzorovani. Poleg nadzornika je zapor odprt tudi za obiskovalce - ti nadzorujejo tako zapornike kot tudi nadzornike. Tako gre za nekakšen stroj, ki je bil v osnovi zamišljen tako, da je vsakdo pod nadzorom, da v bistvu temelji na nezaupanju. Panoptikon je torej stroj, v katerem vsakdo nadzoruje vsakogar glede na položaj, ki ga ima. To je aparat, v katerem ni absolutne točke, zato je v njem cirkulacija nezaupanja popolna. (Foucault, 1991). Vstop ali izstop je mogoč samo po eni poti.

Čeprav Panoptikon ni bil nikoli zgrajen in gre zgolj za utopijo, ki v realnosti ne bi nikoli delovala tako, kot je zamišljena, je Benthamova zamisel po svoje revolucionarna. Na podlagi Panoptikona se je porodila ideja o nadzoru kot tehnologiji oblasti. Tako je za Panoptikon značilno, da je v njegovem središču nadzornik, ki je neviden, vsi drugi pa so vidni. Revolucionarno v ideji Panoptikona je to, da je načelo grajskih celic obrnil na glavo. Ker so takrat zapornike metali v celice, ki so bile vsem skrite, tako rekoč v temo, se je Bentham domislil prav nasprotno in je zapornike izpostavil svetlobi. V Panoptikonu je mogoče vse preračunati, izmeriti vsak učinek in vzpostaviti polje popolne predvidljivosti. Po mnenju Foucaulta zato Panoptikon deluje kot nekakšen laboratorij oblasti.

To obvladovanje učinkov gre tako daleč, da skuša posameznika ne samo prisiliti, da se obnaša tako, kot je to od njega zahtevano, temveč mu celo želi odvzeti svobodno voljo, da ne bi sploh pomislil, da bi kaj storil narobe. Bentham je v svojem besedilu zelo jasno zapisal, kako pomembno je odvrčanje. Zelo važno je, da ima inšpektor zapornika neprestano na očeh, saj mu tako skorajda ne bo prišlo na misel, da bi storil kaj narobe. S tem smo se znašli v srcu revolucionarnih prizadevanj, kako preprečiti ljudem, da bi storili kaj narobe, kako izničiti njihovo željo, da bi grešili. Skratka, kako jim odvzeti zmožnost in voljo. (Foucault, 1991)

Benthamove zamisli o prosojnosti se niso ustavile samo pri zaporu, temveč je menil, da je mogoče z njegovim izumom izboljšati moralo, ohraniti zdravje, okrepiti

industrijo, utrditi ekonomijo in vse s preprosto idejo v arhitekturi, zato je predlagal, da bi njegov izum uporabili ne samo v zaporih, temveč tudi v bolnišnicah, norišnicah, šolah ter celo v politični skupščini. Oziroma kot ugotavlja Dolar v naslednjem koraku, kako čim boljše izpostaviti pogledu celoten družbeni prostor, ga napraviti preglednega in dostopnega kontroli. (Dolar v Kovačič, 2006). S tem Panoptikon postane šola človeštva (Miller, 1981) nadzorovanje pa postane orodje izvajanja oblasti.



Slika 1: Panoptikon (Jeremy Bentham 1791), vir: Wikipedia 2009

### 3.3 VRSTE IN ZNAČILNOSTI NAZDORA

Vsekakor velja, da je nadzor tesno povezan s tehnologijo, predvsem z informacijsko tehnologijo, ki je namenjena zbiranju in obdelavi vseh vrst podatkov in informacij, ter s komunikacijsko tehnologijo, ki je okužila vse vidike človeške komunikacije, saj posreduje skoraj vsako obliko človeških odnosov. Kot je razvidno že iz razvoja pravne zaščite zasebnosti, so prav tehnološke spremembe pomemben dejavnik, ki povečuje nadzor, in s tem tudi eden pglavitnih motivov za spremembo zakonodaje. Zaskrbljujoče je tudi to, da so se znanstvena tehnologija in klasične metode nadzorovanja združile. Zato so se tehnična sredstva za nadzorovanje izredno hitro izpopolnjevala in se še izpopolnjujejo.

Značilen zgled za to so telekomunikacijske tehnologije v ZDA in tehnologije, ki omogočajo avtomatsko obdelavo podatkov. Vendar pa sodobna računalniška tehnologija ni namenjena samo spremljanju posameznikovih dejavnosti, temveč lahko celo tehnično omeji določena ravnanja posameznikov in jim tako fizično omeji možnosti delovanja.

Ne gre za to, da bi oblast s prepovedjo, ukazom posamezniku omejila dostop, gre za to, da posameznika opremi z geslom, ki mu dostop omogoča ali pa ga zavrne. Računalnik oziroma informacijsko-komunikacijska tehnologija se torej vzpostavlja kot osrednja tehnologija nadzora, saj se s tem nadzorovanje pogloblja in krepi. Ne samo, da ga omogoča, temveč ga tudi olajšuje, saj je že v osnovi zasnovana za zbiranje in hranjenje podatkov. Zato ne preseneča, da je sistematičen in množičen nadzor, kakršnega poznamo v sodobni družbi, nastal obenem z nastankom in rastjo vojaške organizacije, industrijskih mest, vladne administracije in kapitalističnega podjetništva, predvsem pa z nastankom informacijskih in mikroprocesorskih tehnologij, ne preseneča pa niti, da je zasebnost posameznikov postala resen problem prav v 20. stoletju in da so se strahovi glede informacijske zasebnosti razvili kot neposreden odgovor na razvoj informacijske tehnologije.

### 3.4 NADZOR IN INTERNET

Nastanek interneta je probleme nadzorovanja in zasebnosti še okrepil.

**Po poročilu Privacy & Human Rights 1999 (v Kovačič, 2006) zasebnost ogrožajo trije pomembni pojavi:**

- **globalizacija** (odstranjuje geografske omejitve pri pretoku podatkov),
- **konvergenca** med tehnologijami (le-te so med seboj čedalje bolj povezljive in kompatibilne, medoperabilne – mogoče jih je prilagajati, dograjevati),
- **multimedialnost** (podatki v neki obliki se lahko hitro spremenijo v drugo obliko).

Za internet zagotovo velja, da predstavlja stično točko med temi tremi pojavi. Gre za medij, ki je globalen, multimedialen, na njem pa prihaja do konvergence med različnimi tehnologijami, saj se v internet danes ne povezujemo samo z računalniki, temveč tudi s prenosnimi telefoni in celo z drugimi napravami (nadzornimi kamerami, Wi-Fi kamere, televizorji). Ker se uporaba interneta hitro širi, je lahko ta

medij posredno velika grožnja zasebnosti. Večina današnjega nadzora se pojavlja na območju digitalnih signalov in prometnih podatkov, ki se zbirajo in shranjujejo samodejno in vsaj nekaj časa tudi hranijo. Zato so zbirke podatkov eno pglavitnih orodij množičnega nadzora.

**James Rule (Lyon v Kovačič 2006) ugotavlja, da predstavljajo omejitve sodobnih sistemov nadzora štirje dejavniki:**

- velikost datotek, ki jih sistem lahko shranjuje,
- stopnja, do katere so lahko ti sistemi centralizirani,
- hitrost pretoka podatkov in informacij med točkami v sistemu,
- število stičnih točk med sistemom in subjektom.

Po Benigerju se revolucija nadzora vzdržuje sama po sebi, kar pa omogočajo trije dejavniki: izraba energije, hitrost obdelovanja informacij in tehnologije nadzora sobivajo v pozitivni spirali (napredek enega dejavnika povzroči ali pa vsaj omogoči napredek preostalih). Tehnološki dosežki in inovacije pa sprožajo potrebe po novih in novih tehnoloških inovacijah (Beniger v Kovačič, 2006). Zgled so tehnologije zbiranja podatkov, ki so s seboj prinesle potrebo po novih tehnologijah shranjevanja podatkov, povečane zmogljivosti pomnilniških sistemov pa ustvarjajo možnosti za še bolj izpopolnjene in ekstenzivne metode zbiranja podatkov.

### **3.5 SODOBNI NADZOR**

Najprej se je sodobna tehnologija za nadzorovanje, bodisi za območje ali ljudi, razvijala v vojaške namene in pri policiji, šele nato so jo začele razvijati tudi večje organizacije in vladne službe, danes pa je dostopna tudi civilni družbi oziroma javnosti. Sodobna tehnologija se danes zelo hitro razvija, poleg tega pa v današnji družbi dobiva vse večjo veljavo.

Tako si danes brez računalnikov, prenosnih telefonov in drugih komunikacijskih naprav ne moremo več predstavljati normalnega življenja. Zanima me, kdo gre danes na dopust brez prenosnega telefona. Verjetno nihče. Za počitnice v hotelu izberemo takšnega, ki ima v sobah internetni priključek ali pa vsaj tako imenovano informacijsko sobo. Vendar to ni nič slabega in še zadovoljni smo, če imamo možnost koristiti prednosti, ki nam jih ponuja sodobna informacijska tehnologija.

#### **3.5.1 GLAVNE ZNAČILNOSTI SODOBNEGA NADZORA**

Gary T. Marx in Gordon (Kovačič, 2003) sta mnenja, da danes živimo pod nekakšnim elektronskim Panoptikonom. Pod občutkom, da nas stalno nekdo nadzoruje ali kot nekakšen „big brother“, lahko pa ta občutek opišemo kot nevidno, ampak vidno. Prav temu pa se danes težko izognemo, saj je opazovanje postalo neosebno in anonimno. Objekt nadzorovanja je postal subjekt, to je posameznikovo telo, njegovo gibanje, govor in obnašanje.

Torej, kako živi v vsakdanjem življenju, kako nakupuje, pri telefoniranju, na sprehodu itd. Kot pravi Lyon, (Kovačič, 2006) je večina današnjega nadzora nevidnega. Gary T. Marx (Kovačič, 2003) predlaga, da živimo v družbi nadzora. Osredotoča se na razlike med tradicionalnimi in novimi značilnostmi nadzora.

Tehnologija omogoča drugačen proces zbiranja in obdelovanja podatkov. Opozoriti velja, da tradicionalni način nadzora še ni izginil, temveč se dopolnjuje z novim.

#### **Značilnosti sodobnega nadzora so:**

- razširitev nadzora na uporabo vseh človeških čutil (videti ponoči, skozi stene, telesa, na ogromne razdalje),
- v večini primerov je neprosto voljen,
- zbiranje podatkov je postalo rutinsko,
- postalo je bolj manipulativno in je vsiljeno,
- zbiranje podatkov je avtomatsko (omogoča jo tehnologija),
- je relativno poceni (na enoto zbranega podatka),
- zbiranje podatkov se vrši na daljavo in neprestano,
- je uporaben za statistične primerjave,
- posameznik kot vir zbranih podatkov utegne postati objekt intervencije uradnih organov,
- čas od odkritja informacije do intervencije se je enormno skrajšal.

Hkrati je sistematično nadzorovanje postalo rutina in neizbežen del današnjega življenja. Hiter razvoj tehnologije v kombinaciji z vladnimi in komercialnimi strategijami vodi k novim načinom hitrega širjenja nadzorovanja, kateremu je težko slediti, še težje pa ga je regulirati. Vedno več naprav za nadzor je dostopnih tudi navadnim ljudem. Lyon navaja, da je nadzor, namenjen eni osebi, zanemarljiv proti institucionalnemu sistematičnemu nadzorovanju (Lyon v Kovačič, 2006). Slednji je avtomatski in je odvisen od moči računalniške tehnologije. Kovačič opozarja, da ni nujno nadzor v obliki velikega brata koncentriran na eno osebo ali mesto, temveč je nadzor razpršen. Lyon navaja, da so za sodobni nadzor značilni razpršenost, decentralizacija in globalizacija. Nadzor se danes širi z veliko hitrostjo.

#### **3.5.2 NADZOR V JAVNOSTI**

Nadzor v javnosti v veliki meri izvajata država in zasebni sektor, saj informacije o posameznikih zbirajo vladne službe in kapitalistične korporacije. (Kovačič, 2003) Prav tako Kovačič opisuje, da je v javnem in zasebnem življenju mogoče zaznati disciplinsko in regulacijsko funkcijo nadzora, ki jo je že opisal Foucault.

Država izvaja disciplinski nadzor s pomočjo vladnih represivnih organov, regulacijski nadzor pa preko državnega statističnega urada, davčne uprave itd. Zasebni sektor pa izvaja disciplinski nadzor preko nadzornih sistemov na delovnih mestih, regulacijski nadzor pa nad potrošniki s pomočjo marketinga. (Kovačič, 2006) Torej se nam dogaja nadzorovanje s strani države in zasebnega sektorja, kot posameznikom in kot potrošnikom. Ambicija države in zasebnega sektorja je nadzorovati vse in vsakogar, pri tem pa velja poudariti, da država preko vladnih organizacij v glavnem nadzoruje ljudi, njihovo gibanje, navade, običaje ... med tem pa zasebni sektor nadzoruje predvsem tako, da zbira podatke, ki predstavljajo tržno vrednost (Kovačič, 2003).

**Nadzor z uporabo policije kot represivnega organa in drugih javnih oblastnih organov delimo na naslednji način:**

- **Nadzor komunikacijskih podatkov**, kot so podatki, ki jih posredujejo telekomunikacijska podjetja in ponudniki internetnih storitev: ime, priimek, telefonska številka, IP naslov, področna lokacija kličočega. Poudariti moramo, da tovrstno nadzorovanje ne sme vsebovati prisluškovanja ali branja vsebine nadzorovanega, kajti za takšno vrsto nadzora je potrebno pridobiti sodno odobritev. Namenjena je predvsem zagotavljanju javne nacionalne varnosti in preprečevanju kriminala.
- **Usmerjeni nadzor** je oblika prikritega nadzora, kjer državni organi spremljajo in posnamejo posameznikovo gibanje. Tovrstno nadzorovanje se uporablja predvsem nad ljudmi, ki so osumljeni, da bodo storili kaznivo kriminalno dejanje.
- **Vsiljiv nadzor** je primer prikritega fizičnega nadzorovanja ali s podtaknjenimi nadzornimi napravami. Pri tem imamo v mislih sledenje osumljencem in prisluškovanje na domu, v avtomobilih in drugih osebnih prostorih.
- **Prestrezanje komunikacij**: tukaj gre za prestrezanje komunikacijskih podatkov, še preden informacije dosežejo namenski cilj. Za razliko od nadzora komunikacijskih podatkov tukaj nadzor obsega tudi komunikacijsko vsebino. Prestrezajo se lahko telefonski klici preko mobilnih, stacionarnih ali drugih govornih naprav, ter navadna in spletna pošta. Državni organi nadzora podatke prestrezajo samo v primeru ogrožanja nacionalne varnosti in suma storitve kriminalnih dejanj na podlagi in ob upoštevanju strogih zakonskih pooblastil.

Seveda pa ti načini nadzorovanja niso nujno rezervirani za uporabo samo državnih organov in oblasti. Na primer elektronsko pošto lahko prestreže vsak posameznik, ki boljše obvlada znanje iz računalništva, prav tako lahko podatke o uporabnikih interneta pregleduje operater internetnega strežnika. Kot opisuje Lyon (Kovačič, 2006), pričakuje v prihodnosti povečanje komercialnega nadzora oziroma nadzora, ki je značilen za zasebni sektor. To se že danes pogosto dogaja pri vsakodnevnem nakupovanju v trgovinah, pri telefoniranju, uporabi e-pošte in obiskih spletnih strani na internetu. Po teh podatkih velikokrat poseže tudi država. Danes se namreč vse vrti okrog individualnega obravnavanja potrošnikov (profiliranje), ki je navidezno namenjeno v korist potrošnikom. Vendar pa lahko na podlagi zbranih podatkov prihaja do njihove diskriminacije (Kovačič, 2003). Profiliranje je do posameznika na videz prijazno, saj potrošnika potiska, kamor si sam želi oziroma ga zalaga z dobrinami in vsebinami, ki ustrezajo njegovim potrebam in okusu (Kovačič, 2003). Velikokrat se takšni obliki nadzora niti ne moremo izogniti, na primer, če želimo pridobiti kartico ugodnosti trgovske organizacije. Na ta način pristopimo k nadzoru na nek način prostovoljno.

„Potrošniki in državljani živimo v svetu, v katerem se moramo nujno odpovedati delu svoje svobode in zasebnosti na račun večje funkcionalnosti in obvladovanja kompleksnosti življenja v sodobni družbi“ (Kovačič, 2006). Tako postaja zasebni sektor vedno večja grožnja zasebnosti, saj ima ta danes na „voljo vedno več sredstev za obdelavo osebnih podatkov kot država“ (Flaherty v Kovačič, 2006). In na koncu se po vsem tem lahko zamislimo in se vprašamo, kam vse to pelje oziroma kam bo vse to pripeljalo današnjo družbo. Pri tem mislim na medsebojne odnose.

### 3.5.3 NADZOR OSEBNIH PODATKOV

Današnja družba temelji na pridobivanju, obdelavi in shranjevanju podatkov. Poleg tega pa potrošniška aktivnost ljudi pospešuje nadzorovanje, opazovanje in uporabo osebnih podatkov v razne tržne in marketinške namene. Te podatke obdelujejo na različne načine razne agencije in organizacije za potrebe trženja, marketinga in politične namene. Za obdelavo teh podatkov nam je danes v veliko pomoč sodobna računalniška tehnologija in z raznimi programi, ki so dostopni na trgu, je obdelava le teh še toliko bolj preprosta. Prav zaradi tega se je v družbi pojavila potreba po nadzoru nad podatki. Osebnih podatki se pojavljajo danes že na vsakem koraku, od nakupov v trgovini, rezervacij počitnic pri turističnih agencijah, pri internetnih storitvah, mobilnih operaterjih ... skratka, povsod, kjer je mogoče zbirati podatke.

Tako zbrani podatki so prepuščeni prosti uporabi in seveda tudi izkoriščanju v nepošteno namene ali zlorabo (Lyon v Kovačič, 2006). Tako je marketing z milijonskimi podatki postal globalna multinacionalna sila, ki išče osebne podatke potrošnikov, njihove nakupovalne navade in s tem posledično trošenje denarja. Namen tega pa je profilirati ter zaslediti trenutnega in potencialnega potrošnika na različnih področjih življenja (Lyon v Kovačič, 2006). Najbolj zaskrbljujoči in tudi občutljivi glede varovanja pa so zdravstveni podatki posameznikov in možnosti zlorabe le-teh. Ti so na prvem mestu povpraševanja pri delodajalcih in zavarovalnicah. (Kovačič, 2006)

V Evropi je glede zaščite osebnih podatkov v veljavi dokaj obsežna in strogo naravnana sprejeta zakonodaja. Ta dovoljuje zbiranje in obdelovanje osebnih podatkov le ob predhodni privolitvi posameznika, na katerega se ti podatki nanašajo. Za te podatke pa je značilno, da jih ne smete posredovati drugi osebi (Marn v Kovačič, 2006), za razliko od ZDA, kjer prodajanje osebnih podatkov ni prepovedano in je običajno v praksi (Marn v Kovačič, 2006). Danes poznamo tehnologijo za zbiranje osebnih podatkov in informacij, ki prodira širše, bolj sofisticirano (učeno) in posamezniku prijazno kot tradicionalne metode. Moč nadzorovanja pa je v tem, da je zbrane podatke mogoče povezati in jih obdelati tako, da dobimo nove podatke, ki imajo novo vrednost in informacije. Takšni podatki so lahko v tem primeru nekomu škodljivi ali pa predstavljajo nevarnost (Čebulj, 1992).

#### **Pri zbiranju podatkov obstajajo tudi naslednje nevarnosti:**

- netočnost podatkov,
- nepopolnost podatkov,
- neažurnost podatkov.

Zato moramo podatke, ki so zbrani na takšen ali drugačen način, analizirati, popraviti napake in opredeliti verodostojnost (Lyon v Kovačič, 2006).

### 3.5.4 NADZOR KOT DRUŽBENO PROFILIRANJE

Že od davne preteklosti se v družbi pojavlja dejanje razvrščanja in profiliranja ljudi. To dejanje je v današnji družbi postalo neizogibno in je skoraj že rutinsko. Vse to se dela sistematično z uporabo sodobne računalniške tehnologije. Pri tem gre za dejanje, ki posameznike avtomatično uvrsti v neko kategorijo, kjer so si na podlagi

svojih karakteristik podobni ali enaki (Kovačič, 2003). Takšna klasifikacija je mogoče na prvi pogled zgleda nedolžna in koristna, vendar je lahko tudi nepravilna in nerealna (Lyon v Kovačič, 2006).

S pomočjo tako imenovane informacijsko-komunikacijske tehnologije (IKT) je razvrščanje ljudi v neke skupine (profiliranje) postalo preprosto. Marketinške tehnike in razne varnostne meritve uporabljajo IKT za identificiranje skupin ali posameznikov za interese naročnikov oziroma organizacij. Z zbiranjem podatkov o ljudeh in njihovih navadah lahko trgovci načrtujejo oglaševalne akcije. Uporaba osebnih podatkov za namene varnosti pa se prav tako poslužuje podobnih strategij za nadzorovanje osumljencev, ki so že bili identificirani ali pa samo ustrezajo profilu osumljenca (Lyon v Kovačič, 2006). Takšno nadzorovanje je usmerjeno v prihodnost in temelji na simulaciji in modeliranju situacij, ki se še niso zgodile, kar potrjuje, da brez podatkov, zbranih v nekem sistemu, ne more delovati (Lyon v Kovačič, 2006). Z različnimi podatki, kot so: video, avdio, besedilne datoteke, biometrični podatki, genske informacije ..., se manipulira za izdelavo profila in nevarnih kategorij posameznika.

Družbeno razvrščanje pa je najbolj občutljivo in nevarno v primeru, kadar organizacije, ki zbirajo takšne podatke, neposredno vplivajo na življenja teh ljudi (Lyon v Kovačič, 2006). Williams in Johnstone (Kovačič, 2006) navajata, da operaterji videonadzornega sistema selektivno nadzorujejo tiste družbene skupine, ki so bolj verjetno deviantne (ekstremne); predvsem mlade temnopolte moške. Za takšno dejanje se uporablja pojem „rasno profiliranje“. Torej se večinoma uporablja profiliranje na demografsko razvrščanje nadzorovanih oseb in zbiranje podatkov glede na to, kdo so. Družbeno razvrščanje oziroma profiliranje se je zelo povečalo v ZDA po znanih dogodkih 11. septembra 2001 (Lyon v Kovačič, 2006).

## 4 SODOBNE TEHNOLOGIJE NADZORA

Najrazličnejše naprave za nadzor so se razvijale najprej za državne varnostne službe, ki so jih preizkušale v vojaške namene, pozneje v policiji in ne nazadnje so se naprave za nadzor pojavile v civilni sferi (Lyon v Kovačič, 2006). Izredno hitro se razvija in izpopolnjuje sodobna tehnologija za nadzor. Tako je prisotna v današnji družbi že na vsakem koraku, kjer pa tudi dobiva vse večjo podporo in veljavo. Tako lahko vse več naprav kupimo v prosti prodaji v specializiranih prodajalnah ali pa jih naročimo preko spletnih strani, ki nam dostavijo naročeno blago po pošti na dom. Tako lahko kupimo različne videokamere, avdio prisluškovalne naprave, GPS naprave (naprava za določanje lokacije) itd. Torej je na trgu mogoče dobiti veliko naprav, ki omogočajo nadzor. V nadaljevanju bomo podrobno predstavili nekatere tehnologije za nadzor pri tem pa bi poudarili, da se vsak dan pojavljajo nove tehnologije in naprave, ki ponujajo boljše, preprostejše in učinkovitejše rešitve za uporabo.

### 4.1 VIDEONADZORNE NAPRAVE

Prvič so videonadzorni sistem uporabili v Angliji v šestdesetih letih prejšnjega stoletja in zaradi takratnega odobravanja javnosti so ga prevzeli tudi v ZDA (Surette, v Kovačič, 2006).

Prvo generacijo videonadzornega sistema predstavlja črno-bela kamera z nizko resolucijo slike, ki je bila z zaslonom povezana preko kableske povezave. Takšen sistem so uporabljali od leta 1950 pa do leta 1980. Takrat so se pojavili še videorekorderji in omrežna oprema. Seveda so ti prvi sistemi vsebovali določene pomanjkljivosti, kot na primer premajhna kakovost posnetkov, zapletena in draga namestitvev opreme, nezmožnost interaktivnega pregledovanja posnetega gradiva, omejen zorni kot snemanja, dolgotrajen proces dokumentiranja in shranjevanja posnetkov.

Hkrati s to tehnologijo so se pojavili prvi pomisleki in zaskrbljenost v javnosti zaradi izgube zasebnosti, nadzora posnetih video- in avdiomaterialov, možnosti zaščite oziroma zlorabe uporabe tehnologije za nadzor. Pojavilo se je tudi vprašanje razvrščanja državljanov glede na to, kdo bo nadzorovan (Surette v Kovačič, 2006). Prav zaradi pomanjkljivosti prvih sistemov za nadzorovanje so začeli izboljševati sistemsko tehnologijo. V devetdesetih letih prejšnjega stoletja so razvili digitalno tehniko in jo začeli uporabljati pri izdelavi kamer in videorekorderjev. To je pomenilo nastanek tako imenovanega digitalnega nadzorovanja. Tovrstna tehnologija je omogočala obdelavo večjih datotek, obdelavo slik z večjo slikovno ločljivostjo, s pomočjo novih programov so lahko obdelovali več stvari hkrati itd. Vendar pa je tudi ta oblika tehnike postala prepočasna in pretoga za vse večje potrebe po hitrejši obdelavi večjih količin podatkov in razvrščanje ljudi po demografski liniji.

Danes smo priča že tako imenovani tretji generaciji videonadzornega sistema, ki se imenuje IP sistem (internet protokol). IP je številka, ki natančno določa računalnik v omrežju interneta. Lahko bi jo primerjali z registrsko številko avtomobila. Ta sistem omogoča popolno digitalno povezavo z omrežjem, ki omogoča popolno kontrolo in upravljanje IP videonadzornih kamer preko LAN - (local area network) lokalno

krajevno omrežje in WAN - (wide area network) široko razsežno omrežje in interneta. Torej gre za digitalno snemanje, ki je hkrati odprto za povezavo v druga omrežja, kot sta internet in intranet. Torej omogoča daljinski nadzor ter spremljanje in nadzorovanje interaktivno preko interneta.

Glavne prednosti videonadzornega sistema tretje generacije so: oddaljeno opazovanje (dostop preko LAN omrežja, interneta ali intraneta, integracija ali kompatibilnost z ostalimi sistemi v omrežje (alarmi proti požaru ali vlomom, biometrične funkcije)), nizki stroški namestitve in vzdrževanja. S sodobno tehnologijo je mogoče v trenutku videoposnetke med seboj primerjati, jih analizirati, shranjevati in povezovati (Kovačič, 2003). Končni cilj videonadzornega sistema je ustvariti inteligentni decentraliziran sistem kamer, ki so sestavni del omrežja, hkrati pa bi vsaka kamera imela sposobnost samoanaliziranja (Surette v Kovačič, 2006).

Takšen videonadzorni sistem se lahko uporablja za odkrivanje kriminalnih dejanj in tudi za protiteroristična delovanja. V javnem oziroma civilnem življenju pa takšen sistem nadzora lahko uporabljamo pri reševanju nastalih problemov v prometu ali varovanju okolja pred onesnaževanjem. Omeniti velja tudi primer videonadzora podzemne železnice v Londonu (Anglija), kjer je bil postavljen z namenom preprečevanja kriminala in nadzora prometa. Po enem letu so ugotovili, da se je kriminal skoraj minimaliziral, toda po drugi strani se je stopnja kriminala povečala na področjih, kjer ni postavljenega sistema videonadzora (Surette v Kovačič, 2006). Pomembno pri tem je tudi to, da je za uporabo videonadzora v namene odkrivanja posameznikov, ki storijo kriminalna dejanja, nujno potrebno uskladiti zakonodajo in pristojnosti vladnih organov za pregon kriminalitete. K širitvi uporabe videonadzora pa močno vplivajo tudi komercialni in politični lobiji.

## 4.2 NADZOROVANJE S POMOČJO BIOMETRIJE

Biometrija sodi med najnovejše načine tehnologije za nadzor. Značilno za tovrstno metodo je, da uporablja telesne, biološke značilnosti za identifikacijo in nadzor oseb. Gre za proces zbiranja, analiziranja, shranjevanja podatkov o posameznikovih telesnih bioloških zdravstvenih lastnostih z namenom identifikacije (Kovačič, 2003). Biometrija omogoča identifikacijo skozi fizične značilnosti, kot so na primer barva glasu, oblika obraza, šarenice v očesu, prstni odtis, DNK itd. Ljudje se med seboj najbolj zanesljivo ločimo po DNK, šarenici, mrežnici in prstnih odtisih. Manj pa se razlikujemo po obliki obraza, dlani, govoru, pisavi, hoji itd. Zelo uspešno jo uporabljamo pri identifikaciji in verifikaciji oseb. Z biometričnimi metodami lahko zanesljivo ločimo osebe glede različnosti nekaterih organov, ki jih ima vsak človek enkratno.

### Tako ločimo osebe po:

- prstnem odtisu (znano je, da ima vsak človek enkratno prstni odtis na vsakem prstu posebej),
- obliki in značilnosti obraza,
- geometriji rok (oblika, velikosti prstov),
- šarenici (vsak človek ima enkratno vzorec in strukturo šarenice za vsako oko različno),
- mrežnici, ki sodi med najnatančnejši vir identifikacije,

- pisavi, ki nima velikega vpliva, saj je dostikrat odvisna od posameznikovega razpoloženja
- glasu, ki je odvisen od posameznikovega zdravja, prehlada, stresa itd.,
- infrardeči toplotni identifikaciji, ki tudi predstavlja značilnosti posameznika, vendar še ni popolnoma verodostojna in se še proučuje,
- gibanju (vsak človek ima svojevrsten način hoje in drže telesa),
- vonju telesa: vsak posameznik ima značilen vonj, vendar se lahko spreminja glede na zdravstveno stanje in razpoloženje,
- ušesu: biometrija ušesa velja za zanesljivo ločevanje glede na obliko in strukturo uhlja, vendar vsak posameznik nima enkratnega ušesa,
- DNK: je znanstveno potrjen kot najbolj verodostojen podatek, saj ima vsak posameznik enkratni DNK vzorec, razen enojajčnih dvojčkov.

Vsaka od zgoraj navedenih primerov za identifikacijo ima svoje prednosti in slabosti. Biometrija dlani se uporablja že vrsto let, vendar je za splošno rabo neprimerna, saj se dlani med seboj ne razlikujejo dovolj. Prav tako okrog 5 % ljudi nima čitljivega prstnega odtisa bodisi zaradi genskih napak, poškodb ali obrabe. Tudi prepoznavanje obraza, ki temelji na tridesetih točkah razpoznavanja, ni zanesljivo. Za prepoznavanje identitete posameznika je tako najbolj primeren način vzorec DNK, šarenice in mrežnice. Odčitavanje vzorca šarenice je najbolj primerno, ker je postopek hiter in ni potreben fizični dotik. Za večjo verjetnost pravilne identitete se uporablja kombinacija več načinov pregleda.

V Sloveniji smo sledili novostim sorazmerno hitro, saj smo med prvimi izdali biometrične potne liste. Seveda pa ne smemo pozabiti, da so tudi pri uporabi biometrije možne napake. Težave se pojavijo pri računalniškem odčitavanju biometričnih podatkov, zapisanih v dokumentih, ki se lahko v primerjavi s fizično izmerjenimi podatki razlikujejo ali pa jih nekdo namenoma zamenja. To pa predstavlja nevarnost, da bi lahko na primer policisti bolj verjeli računalniku kot lastni presoji in bi tako za krivega spoznali nedolžnega. Sporno pri tem je, da država ni zagotovila, da državni organi ne bodo povezovali podatkov v enotno bazo, kar pa bi pomenilo, da obstaja možnost spremljanja posameznika in s tem omejevanje in zlorabo pravice do zasebnosti.

### 4.3 NADZOR PRI UPORABI SPLETNE MREŽE

**Internet** uporabljamo že skoraj vsak dan. Je zelo razširjena oblika komuniciranja po celem svetu. Uporabljamo ga zaradi več razlogov. Lahko zaradi zabav, dopisovanj, obveščanj, iskanj različnih informacij. Uporabljamo ga tudi za različne vrste predstavitev, promocije, oglaševanje, izobraževanje, uradne storitve, bančništvo in tudi trženje. Zaradi obilo podatkov, ki jih internet ponuja, je kot takšen zelo uporaben in koristen, na drugi strani pa je podvržen v veliki meri zlorabi. Pri tem mislim seveda na nekontrolirano in nedovoljeno pregledovanje e-pošte, vsebin datotek, pa tudi prestrezanje podatkov in zlorabo le-teh.

Pri tako imenovanem „surfanju“ na internetu seveda uporabnik nevede pušča za seboj kar nekaj sledi, ki omogočajo vdor v osebne strani računalniško večšim nepridipravom. Tako lahko internetni ponudnik na strežniku ugotovi, kdaj in katere spletne strani in storitve je uporabnik uporabljal, iz katerega uporabniškega imena in preko katere IP številke, telefonske številke je dostopal (Kovačič, 2003). Ponudnik

strežnika ali operater, ki vam omogoča dostop na splet, lahko nevede zbira podatke in jih beleži ter jih obdela. Tako izdelava profiliranje in takšen podatek posreduje ali proda interesentom. Največkrat so to marketinška podjetja in agencije, ki informacije potrebujejo za svojo dejavnost. Nekateri spletni brskalniki lahko ugotovijo, kateri operacijski sistem uporabljate. Microsoftov Internet Explorer lahko odkrije celo, ali ima uporabnik nameščene programe Word, Excel in Power Point.

Ob obisku spletne strani se uporabniku dodeli tako imenovani „cookie“ ali piškotek, ki pri drugem obisku prepozna vaš računalnik. Na primer pri spletnem nakupovanju, kjer ste že enkrat morali vnesti različne podatke, si jih ta zapomni in vam jih v prihodnje ni več potrebno vnašati.

Velik problem okrog takšnega nadzora zbuja prav nadzorovanje na delovnem mestu. Pri nas takšen način nadzora ni dovoljen, razen če zaposleni niso o tem predhodno obveščeni. Velikokrat se dogaja zbiranje podatkov, kot so elektronski naslovi, preko podtaknjenih programov, ki jih ne opazimo in se jih težko znebimo. Takšni programi so znani kot računalniški virusi, črvi, pajki, roboti ... (Kovačič, 2003), Najpogosteje postanemo njihove žrtve, če se odzovemo na nagradne igre ali oglase.

Narazlične načine v računalniške sisteme nepooblaščno vstopajo računalniški pirati ali tako imenovani hekerji. To so osebe z veliko računalniškega znanja in to znanje zlorablja za napad na računalniške sisteme, z namenom onemogočiti delovanje le-tega oziroma ga uničiti. Za zdaj še nihče izmed njih ni uspel izsiliti večjo količino denarja za opustitev namere. Največkrat je nagrada za njihov „uspeh“ objava v medijih ali na naslovnica dnevnikov in tabloidov. Na ta način se lahko pohvalijo pred kolegi v svojih krogih.

Naj omenim še en primer vsiljive marketinške mreže, ki zna biti zelo nadležna. Gre za tako imenovane SPAM vsebine, ki sodijo med nezaželena oziroma nenaročena elektronska sporočila. Gre za oglasna elektronska sporočila. SPAM je eden izmed resnih problemov interneta, saj so raziskave pokazale, da se količina takšnih sporočil veča in je leta 2003 obsegala že več kot 50 % vseh sporočil. To bi celo utegnulo uničiti uporabnost elektronske pošte. SPAM je zaradi možnosti velikih zaslužkov tudi eden izmed pomembnih dejavnikov za razmah kiber kriminala. Omejen ni samo na elektronsko pošto, temveč so ga pošiljali tudi na interaktivne sisteme za klepet po internetu (MSN, ICQ ...). V zadnjem času je priljubljena posebna oblika SPAM-a, in sicer, da pošiljatelj dopisuje reklamne komentarje v tako imenovane spletne dnevnike (ang. Blog).

Čeprav SPAM ne pomeni neposrednega vdora v zasebnost v smislu nadzora, pa ga lahko štejemo za poseg v pravico biti puščen pri miru, skratka, v tisti del zasebnosti, ki posamezniku omogoča, da se umakne iz družbe.

Za vse naštet primere se lahko delno zaščitimo z vgradnjo zaščitnih sistemov, kot so požarni zid, protivirusni programi z vsakodnevnim osveževanjem, uporabljanjem alfanumeričnih kod - gesel. Danes se lahko pred dostopom v računalnik zaščitimo z uporabo prstnega odtisa kot kodo vstopa v sistem. Moramo pa se zavedati, da popolne zaščite ni. Zato nekatere pomembne podatke, kot so kode, PIN-i in drugi podatki, varno shranite v svojem pomnilniku v glavi.

## 4.4 SATELITSKI NADZOR IN GPS

GPS (global positioning system) je danes vse bolj razširjena tehnična metoda nadzora. Sistem obsega podatkovni nadzor s pomočjo uporabe satelita in naprave, nameščene na nadzorovanem objektu. Zadnje čase v uporabo vse bolj vstopa satelitski videonadzor. Uporabljamo ga za različne namene, kot spremljanje prometnih zastojev, poročanje s političnih kriznih področij, v vojaške namene, pogled na področja, ki so zaradi naravnih nesreč nedostopna, pri načrtovanju in gradnji infrastrukture (Kovačič, 2003). Ti sistemi so že tako izpopolnjeni, da je mogoče prepoznati predmete v velikosti manj kot en meter. Primer je satelitska slika, ki jo je mogoče spremljati preko Google Earth. Tam lahko pogledamo na vsak kotiček na svetu. Vendar je ločljivost odvisna od konkretnega primera. Sam sem si tako ogledal svojo hišo in naselje iz tako imenovane ptičje - satelitske perspektive. Zelo razločno lahko vidimo hiše, drevesa, ceste, vrtove, bazene, reke, potoke, jezera, morja itd

Satelitski nadzor s pomočjo GPS naprav je lahko bolj uporaben tudi za javne namene. Pri uporabi GPS kot sledilne naprave se uporablja satelit, s pomočjo katerega se ugotovi lokacija, kje se trenutno nahaja nadzorovan objekt. Čedalje bolj je v uporabi GPS sistem v motornih vozilih, saj je danes že cenovno prijaznejša za podjetja, tako da so se mnogi odločili za njegovo uporabo. V tujini se takšne naprave uporabljajo tudi za obveščanje o razmerah v prometu. GPS naprave vgrajujejo tudi v prenosne telefone. Tehnologija omogoča, da z nekajmetrsko natančnostjo ugotovimo, kje se nahaja oseba. To je primerno za nadzorovanje uslužbencev, saj lahko nadzorujemo osebo in ne več avtomobila. Obstajata dva načina ugotavljanja lokacije prenosnega telefona: to sta terminalski način, kjer lokacijo ugotovi preko omrežja telefonski aparat sam, ali omrežni način, kjer lokacijo prenosnega telefona ugotovi omrežje samo (Kovačič, 2003). Lokacijo lahko ugotovi tudi operater sam preko lastnih omrežnih usmerjevalcev signalov. Ta način večkrat uporabi tudi policija pri raziskovanju kriminalnih dejanj. V primeru sledenja je zlasti uporabno, da lahko locirajo, od kje je bil oddan zadnji signal ali klic na pomoč. Uporabni so še drugi sistemi lociranja uporabnikov prenosnih telefonov, kot je na primer LSP (Location Service Providers), ki starše preko prenosnih telefonov obvešča, kje se trenutno nahaja njihov otrok, vendar je v uporabi samo v nekaj zahodnoevropskih državah (Ahlert v Kovačič, 2006). V Sloveniji še ni takšne možnosti. Obveščanje omogoča v prenosni telefon vgrajena sledilna naprava, ki preko SMS-a ali e-pošte obvešča starše o trenutni lokaciji.



Slika 2: Ljubljana »Tromostovje«, vir: Google Earth 2009

#### 4.4.1 UPORABA GPS SISTEMOV NA VOZILIH

Tudi v avtomobil lahko namestijo poseben vmesnik, ki obvešča, kje se vozilo trenutno nahaja, torej lokacijo, koliko časa je vozilo peljalo, koliko časa je mirovalo, kako hitro se je peljalo (Lotrič v Kašnik, 2006). Zaradi takšnega nadzora se že pojavljajo forumi, ki ugotavljajo, v kolikšni meri je takšno nadzorovanje sporno z vidika zasebnosti.

**Danes vse več ponudnikov na trgu ponuja različne sledilne naprave, ki se preprosto montirajo na vozilo in omogočajo naslednje:**

- on-line sledenje in grafični prikaz realiziranih poti preko spleta,
- sledenje in grafični prikaz poročil v realnem času preko spleta,
- nadzor in prikaz prevoženih kilometrov, čas vožnje in postankov,
- sledenje vozila in prikaz na GSM aparatu,
- prikaz in arhiviranje poti neomejeno za nazaj.

Takšne storitve vam ponujajo že od 200 evrov mesečno dalje, odvisno od ponudbe in pogodbe. Nadzor vašega vozila lahko izvajate preko katerega koli računalnika ali dlančnika z internetno povezavo. Ponudbe vsebujejo grafični prikaz gibanja vozila na podlagi zemljevidov in kart držav v Evropi in svetu. Izdelajo vam lahko tudi podrobno analizo smotrnosti voženj in stroškov ter predlagajo optimalne rešitve. Podatke lahko prejimate tudi preko e-pošte dnevno, tedensko, mesečno, četrletno in letno. Za posredovanje podatkov uporabljajo GPS (global positioning system - sistem globalnega določanja položaja) in GPRS (general packet radio service, ki omogoča paketno namesto neprekinjeno pošiljanje podatkov) sistem za povezavo in so zanesljivi. Imajo dovoljenje za uporabo pristojnih vladnih služb. Sistem se zaradi

neprestanih sprememb infrastrukture cest, ulic, mostov, imen ulic in krajev, omejitev prometa interaktivno dopolnjuje.

**Takšen nadzorni sistem je primeren za podjetja, ki potrebujejo nadzor nad svojimi vozili, še zlasti tista podjetja, ki razpolagajo z več vozili v prometu, kot na primer:**

- komercialna vozila,
- servisna vozila,
- vozila za distribucijo,
- vozila za prevoz blaga in oseb,
- vozila, ki prevažajo material in delavce.

**Poglejmo si še prednosti, ki jih omogoča GPS sledilni sistem:**

- s sistemom lahko spremljate potovanja, postanke (minute, ure ...) in lokacije svojih avtomobilov od začetka do konca delovnega časa,
- vsak trenutek lahko spremljate, kje so vaša vozila, kar vam lahko poveča odzivni čas in zmanjša stroške,
- optimizirate dostavo, izboljšate izkoristek delovnega časa,
- predvidite morebitne zamude, obvestite stranko o razlogih zamude,
- nadziranje prihoda na delo, kjer se zaposleni vozijo na teren.

Poleg pozitivnih lastnosti uporabe GPS sledilnih naprav opazamo tudi negativne odzive uporabe takšnih sistemov.

S strani **najemnika** se to kaže predvsem v visokih stroških storitev, nakupa in servisiranja naprav.

S strani **uporabnikov** se pojavlja vprašanje z moralno-etičnega vidika kršenja pravice do zasebnosti zaposlenih.

Delodajalci na to vprašanje odgovarjajo, da z uvedbo sledilnih naprav v vozilih želijo zavarovati svojo lastnino pred zlorabo ali krajo.

Mi pa se sprašujemo, ali je bil prvotni namen namestitve sledilnih sistemov v službena vozila nadzor zaposlenih in šele drugega pomena zavarovanje lastnine.

## 4.5 PRISLUŠKOVANJE IN OPAZOVANJE

Že od nekdaj si človek želi ob določeni situaciji biti na tekočem in obveščen o dogajanju, ki ni povezano prav z njim. To je seveda prirojena lastnost človeka, zato si je skozi čas na različne načine prizadeval biti obveščen o dogajanjih okoli njega samega ali pa tudi o dogajanju v interesnem okolju. Tako so imeli že v davni preteklosti kralji, vladarji, cesarji, vojskovodje, politiki in drugi pomembni ljudje ovaduhe, vohune, agente oziroma osebe, ki so jim prinašale želene informacije. Včasih so bile vesti slabe, nepričakovane in boleče, nemalokrat jim niso hoteli verjeti, včasih so posumili v verodostojnost informacij.

V sodobnem času je vohune in tajne agente zelo uspešno nadomestila sodobna tehnologija. Na trgu obstaja veliko vrst prisluškovalnih in opazovalnih naprav, ki so se z leti razvile iz prvotno negativnih potreb po prisluškovanju in opazovanju do danes že v uporabi za koristne namene, kot na primer zaradi varovanja in varnosti.

#### 4.5.1 PRISLUŠKOVANJE Z UPORABO TEHNOLOGIJE

Prisluškovanje lahko razdelimo na dva načina. Prvo je telekomunikacijsko prisluškovanje, drugo pa prisluškovanje v prostoru (Kovačič, 2003). Za prisluškovanje obstaja cela vrsta elektronskih naprav. Banisar (v Kovačič, 2003) in drugi omenjajo, da nadzor komunikacijskih sredstev omogoča tako imenovano prijazno prisluškovanje, to je prijazno za prisluškovalca. Skoraj vsi smo že imeli priložnost videti in spoznati delovanje najpreprostejše naprave za prisluškovanje, tako imenovanega Babysitterja. Tudi prenosni telefon je lahko preprosta prisluškovalna naprava. S slednjim lahko prisluškovalec preprosto pokliče številko prenosnega telefona, prevzame klic in ga povezanega pusti v sobi, kjer je namen prisluškovanja. Tako brez ovir poslušaja pogovor v prostoru. Potem se vrne in ga preprosto poišče, kot da ga je pozabil. Dobijo se tudi preproste naprave, tako imenovani spyphon, ki navidezno izgleda kot prenosni telefon, vendar ko pokličemo njegovo številko, se avtomatično aktivira, ne zvonijo in tako poslušamo pogovor v prostoru. Ko je pogovor končan, preprosto prekinemo zvezo. Na internetu lahko takšen spyphon nabavite za dobrih 300 USD. Obstajajo pa seveda tudi bolj izpopolnjene naprave, pa vse do vrhunskih, ki jih uporabljajo tajne službe. Stanejo preko 300.000 evrov. Sem sodijo naprave, ki so preko satelitske zveze povezane z varnostnimi službami v posameznih državah, ki se samostojno aktivirajo ob določenih ukazih ali besednih zvezah, kot so na primer: terorist, orožje, bomba.

Kupiti prisluškovalno napravo je danes dokaj preprosto, saj na spletnih straneh najdete kar nekaj ponudnikov. Njena uporaba in namestitvev pa že zahteva nekaj tehničnega znanja in izkušenj.

V Sloveniji je nezakonita uporaba prisluškovalnih naprav v zasebnih prostorih prepovedana (Kovačič, 2003).

#### 4.5.2 NADZOROVANJE KOT OPAZOVANJE

Pri vsakdanjih življenjskih poteh, kot so nakupovanje, urejanje uradnih zadev, dvigu denarja v banki ali z bankomatov, obisku pošt, muzejev, športnih prireditev in vožnji po mestu ali avtocesti opazimo naprave za videonadzor. Tako nas včasih daje neugoden občutek, da nas nekdo opazuje in si nas ogleduje, se nam morda posmehuje ... Na vsakem koraku smo torej opazovani.

Kaj pa na delovnem mestu? Trgovke v trgovini, bančni, poštni, zavarovalniški uslužbenci ... Povsod so nameščene videokamere, ki prenašajo sliko v živo, neke tudi avdiosignal, ki omogoča prenos zvoka. In vse to nekdo spremlja, gleda, opazuje ali pa snema in posnetke nekam shranjuje.

Delodajalci se branijo z odgovorom, da vse to počnejo zaradi varnosti zaposlenih in premoženja. Mi pa se sprašujemo, ali je to z moralno-etičnega stališča sporno zoper varovanje zasebnosti.

### 4.6 NADZOR NA DELOVNEM MESTU

Sodobna informacijska tehnologija torej omogoča delodajalcem zmeraj bolj podroben nadzor nad zaposlenimi. Crossman and Lee-Kelley (Kašnik, 2006) opozarjata, da ima lahko nadzorovanje na delovnem mestu negativne učinke. Lahko se zgodi, da pade delovna motivacija. Tudi v Angliji so prišli do negativnega rezultata pri raziskavi mnenja o nadzoru na delovnem mestu, ki ga je izvedla vladna

komisija za delo. Ugotovili so, da povečan nadzor zmanjša produktivnost zaposlenih. S tem v zvezi se poveča stres kot posledica psihičnega pritiska in zmanjša se zmožnost učinkovitega organiziranja dela.

Z nadzorom na delovnem mestu želijo delodajalci zavarovati podjetje pred zlorabo informacij in tehnološkimi procesi ter zavarovati premoženje podjetja. Drugi motiv je vrednotenje posameznikove uspešnosti.

V Sloveniji je največ pritožb nadzora nad zaposlenimi zaradi ugotavljanja bolniške nesposobnosti za delo, uporabe alkotestov, videonadzora na delovnem mestu in nadzora (sledenja) poti s službenim vozilom (Kocmur, 2005). Državni nadzornik je ugotovil, da veliko delodajalcev zbira osebne podatke, kot so: ime očeta, podatke iz osebne izkaznice, zaposlitvah družinskih članov, socialnem stanu, članstvu v raznih društvih in političnih organizacijah, socialnih razmerah, hobijih, dejavnostih v prostem času (Bogataj, 2003).

Tudi v pravilniku Inštituta RS za varovanje zdravja ob prihodu takratnega direktorja Andreja Marušiča leta 2002, objavljeno v Nedelu (Kocmur, 2005), so zahtevana bolj stroga pravila in zahteva po navedbi več osebnih podatkov. Navedene so bile hujše kršitve zaposlenih, na primer prihod na delo pod vplivom alkohola (dovoljena meja je 0,0 promila), uživanje prepovedanih drog, kajenje na delovnem mestu in v okolici, nespoštovanje zdravnikovih navodil v času zdravljenja. Zagrožena je bila celo prekinitve pogodbe o zaposlitvi. Sicer pa zaposleni najprej dobijo pisno obvestilo (Kocmur, 2005). To bi bilo lahko vprašanje za varuha človekovih pravic, saj ni definirano, kaj je mišljeno pod besedo okolica. To je lahko že sosednji lokal. In tako rekoč bi pomenilo, da je tudi tam prepovedano kajenje. Prav tako pa lahko alkotest pokaže stopnjo alkohola v krvi več kot 0,0 promila že ob zaužitju kakšne hrane.

Svetovalka za pravne zadeve na IVZ – Inštitut za varovanje zdravja Zdenka Jakopanec meni, da spiti kozarec vina pri kosilu ni več zaželeno (Kašnik, 2006). Zaposleni, ki bi v nedeljo zvečer spili kozarček ali dva in bi v ponedeljek imeli v krvi še vedno sledi alkohola, pa naj vnaprej razmislijo o posledicah. Dodaja sicer, da bodo zares preganjali le „problematične pivce“. Glavni republiški inšpektor za delo, Borut Brezovar, je v dokumentu našel veliko pomanjkljivosti ali celo nezakonita določila. Vodilni sicer imajo pristojnost ukazati, da preverijo stopnjo alkoholiziranosti in omamljenosti zaposlenih, vendar le, če obstaja utemeljen sum kršitve, kar pa mora biti v pravilniku jasno napisano. Meni tudi, da je 0,0 promila alkohola v krvi vseh zaposlenih skrajno neživiljenjska meja in dodaja, da bi takšno mejo postavil le tistim, ki so z delom močno vezani na promet in kjer poklic zahteva popolno koncentracijo in sposobnosti. Prav tako pa ni dopustno pošiljati nadzornikov v kontrolo zaposlenih, ki so na bolniškem staležu (Kašnik, 2006). Spremljanje gibanja službenih vozil je dovoljeno le za nadzor nad stroški med delovnim časom, ne pa tudi za nadzorovanje zaposlenega med prostim časom.

Znan je primer videonadzora na delovnem mestu v podjetju Comet iz Zreč, kjer so zaposleni s stavko zahtevali odstranitev videonadzornih naprav (Repovž v Kašnik, 2006). Inšpektor je ugotovil, da so naprave postavljene v proizvodnih obratih v skladu s pravili, vendar mora uprava zaposlene o tem obvestiti trajno in na vidnem mestu. Videonadzor se sme v delovnih prostorih uporabljati le in izključno za varovanje ljudi in varovanje premoženja ob pogoju, da je to edini način, s katerim je mogoče zagotoviti varnost (Bogataj, 2003). Videonadzorne sisteme je prepovedano

namestiti v garderobah, dvigalih in sanitarijih. Zaposleni morajo biti o videonadzoru pisno obveščeni. Videonadzor se ne sme uporabljati za nadzor delovne discipline, postavljanje proizvodnih norm ali za prisluškovanje zaposlenim (Kocmur, 2005). Vodilni menedžerji v marsikaterem podjetju zagovarjajo medsebojno zaupanje med zaposlenimi in vodstvom, vendar se tega ne da zagotoviti z nadzorom, ampak z vse pogostejšo komunikacijo med njimi. Temu mnenju se pridružujejo tudi pri Mobitelu, čeprav zatrjujejo, da so ukrepi, ki jih izvajajo z videonadzornimi sistemi, potrebni zaradi lažjega, hitrejšega in varnejšega poslovanja, predvsem pa za varovanje zaposlenih in zaščito sredstev (Vovk v Kašnik 2006).

#### 4.6.1 NADZOR NA DELOVNEM MESTU V ŠTEVILKAH

Rezultati nekaterih agencij za javnomnenjske raziskave so potrdili negativno mnenje zaposlenih, s strani delodajalcev pa nasprotno pozitivno mnenje glede uporabe moderne informacijske tehnologije za nadzor na delovnem mestu.

**Raziskava American Management Association iz leta 2005 je za podjetja v ZDA pokazala naslednje :**

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

**Podjetja v ZDA kot razloge za nadzor navajajo:**

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

*vir: Matej Kovačič, Fakulteta za družbene vede, Univerza v Ljubljani*

Analiza raziskave organizacije The Privacy Foundation "The Extent of Systematic Monitoring of Employee e-mail and internet Use" iz leta 2001(Kovačič, 2006) je pokazala, da je glavni razlog za razmah nadzorovanja vse bolj cenovno dostopnejša tehnologija.

Za Evropo nismo zasledili statistične sheme podatkov glede vprašanj tehničnega nadzora na delovnem mestu.

## 5 PRAVNI RED IN KRŠITEV PRAVIC ZASEBNOSTI

V Sloveniji nadzor na delovnem mestu in uporabo nadzorne tehnologije in pravice do zasebnosti pravno ureja več zakonov in aktov, ki temeljijo na direktivah, uredbah in sklepih Evropskih komisij, parlamenta in organizacij in Ustave Republike Slovenije. Iz mednarodnega vidika je spoštovanje človekovih pravic opredeljeno v tako imenovani Dunajski deklaraciji o človekovih pravicah (UN) iz leta 1993.

Slovenija je Konvencijo skupaj s protokoli številka ena do sedem in devet do enajst ratificirala in sprejela Konvencijo o varstvu človekovih pravic in temeljnih svoboščin leta 1994, leto pozneje, kot je bila sprejeta v Svetu Evrope.

### 5.1 VARSTVO PRAVIC V SLOVENIJI

V Sloveniji se Konvencija uporablja neposredno. Vsi slovenski zakoni in predpisi morajo biti z njo usklajeni. V primeru neskladja z njo odloča Ustavno sodišče, ki lahko predpis tudi razveljavi. Evropska konvencija se sklicuje na Splošno deklaracijo človekovih pravic. Pomembna načela, kot so pravičnost, mir, politična demokracija, svoboda in pravna država, so izhodišča konvencije.

Evropska konvencija o varstvu človekovih pravic in mednarodnih svoboščin je bila spremenjena s protokoli 3, 5 in 8, ter dopolnjena s protokolom št. 2 ter njenimi protokoli 1, 4, 6, 7, 9, 10 in 11 (Convention on Human Rights and Fundamental Freedoms) z amandmaji, ki jo je sprejel Svet Evrope leta 1950. Konvencijo je Državni zbor Republike Slovenije ratificiral 13. 6. 1994, veljati pa je začela 28. 6. 1994. Zakon o varstvu osebnih podatkov, zakon o elektronskih komunikacijah, zakon o delovnih razmerjih, zakon o javnih uslužbencih, zakon o varstvu osebnih podatkov, kazenski zakonik in seveda Ustava Republike Slovenije.

#### 5.1.1 VARSTVO POSAMEZNIKA DO ZASEBNOSTI

Konvencija v prvem odstavku osmega člena določa opis in obseg pravice do spoštovanja zasebnega in družinskega življenja, doma in dopisovanja, medtem ko so v drugem odstavku naštetih pogoji in razlogi za možne omejitve pravice. Državna oblast torej lahko poseže v izvrševanje pravice samo v izrecno navedenih primerih.

To je v primerih, ko je ogrožena državna varnost, javna varnost ali ekonomska blaginja države, da se preprečijo nered ali kazniva dejanja, da se zavaruje zdravje ali morala, ali da se zavarujejo pravice in svoboščine drugih ljudi.

Pravica do zasebnosti se lahko razlikuje od posameznika, saj je potrebno upoštevati nekatere specifične poklice oziroma družbeno izpostavljenost tistih skupin posameznikov, ki so manj varovani pred posegom v zasebno sfero. Gre za politike, igralce, člane kraljevskih družin, skratka vse, ki jih upravičeno označimo za javne osebnosti.

#### **Tako posamezniku pravno priznavamo zaščito zoper:**

- napad na fizično in psihično integriteto ter moralno in intelektualno svobodo,
- napad na čast in ugled,
- nedovoljeno uporabo imena, identitete ali podobnosti,

- prisluškovanje, opazovanje in izsiljevanje,
- razkritje varovanih tajnosti in informacij.

## 5.2 ZAKON O VARSTVU OSEBNIH PODATKOV

Eden od pomembnejših zakonov s področja varovanja zasebnosti je Zakon o varstvu osebnih podatkov (ZVOP-1), ki velja od 1. 1. 2005. Zakon je v celoti usklajen z direktivo Evropske komisije o zaščiti posameznikov pri obdelavi osebnih podatkov in prostem pretoku teh podatkov. Posebnost je v tem, da so se po novem povečale pristojnosti Državnega nadzornega organa za varstvo osebnih podatkov. Dovoljuje uvedbo biometričnih ukrepov v zasebnem sektorju. Z zakonom je urejeno več področij, kot so direktni marketing in trženje, videonadzor, evidence vstopov in izstopov iz prostorov, uporaba javnih knjig; povezovanje, pregledovanje in zbiranje osebnih podatkov, uporaba osebnih podatkov, strokovnega nadzora itd.

### 5.2.1 INFORMACIJSKA POOBLAŠČENKA RS

V Sloveniji deluje urad Informacijske pooblaščenke, ki je nastal 1. 1. 2006 z združitvijo pooblaščenca/ke za dostop do informacij javnega značaja in Inšpektorata za varstvo osebnih podatkov. Sedaj urad vodi Nataša Pirc Musar. Urad je nevladna organizacija in je pooblaščen za nadzor na področju varstva osebnih podatkov. Sodeluje z drugimi državnimi organi, zavodi, združenji, nevladnimi organizacijami in tudi z mednarodnimi organizacijami pri EU. Opravlja preventivni inšpekcijski nadzor pri upravljalcih osebnih podatkov s področja javnega in zasebnega sektorja, vodi in vzdržuje register zbirk osebnih podatkov in skrbi, da je register ažuriran. Izvaja nadzor nad iznosom osebnih podatkov v tretje države.

6. člen zakona opredeljuje osebni podatek kot kateri koli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen. Potemtakem je na primer videoposnetek osebni podatek. Tudi če gre le za kratek čas, sodi v zbirko osebnih podatkov (Bogataj, 2003).

Najbolj občutljivi in značilni osebni podatki so identifikacijski podatki: ime in priimek, datum rojstva, prebivališče, EMŠO, davčna številka, prstni odtis, fotografija, izobrazba, zaposlitev, podatki o socialnem statusu, zdravstvenem stanju, ekonomskem položaju, družinskem statusu ipd. Med zelo občutljive podatke sodijo politična pripadnost, verska pripadnost, spolna usmerjenost, rasni izvor, kazenska preteklost, sindikalna aktivnost ... Ti podatki morajo biti še posebej varovani pred javnostjo. Zakon določa, da lahko te podatke obdeluje le pooblaščen oseba ali organizacija za določene namene, kot na primer za statistične, zgodovinske, zdravstvene, raziskovalne ipd.

V zasebnem sektorju se lahko obdelujejo osebni podatki tistih posameznikov, ki so sklenili kakšno pogodbo ali predpogodbo. Po zakonu je potrebno posameznike, o katerih se zbirajo podatki, obvestiti o namenu obdelave, torej kdo in zakaj jih uporablja. Podatki se lahko hranijo le toliko časa, kolikor so potrebni za doseganje namena, za katerega so bili pridobljeni. Po tem roku se morajo trajno izbrisati ali arhivirati na zakonsko določen način. Tisti, ki podatke obdelujejo, so dolžni varovati tajnost osebnih podatkov. Internetni ponudniki morajo IP številke uporabnikov zbirati in hraniti le, če te podatke potrebujejo za izpolnjevanje pogodb naročnikov. Lahko pa jih pridobijo s pisnim privoljenjem posameznikov.

Zakon ureja tudi neposredno trženje. Prepovedano je posredovanje elektronskih naslovov tretjim osebam, razen če posameznik to dovoljuje. Posamezniki lahko tudi v vsakem trenutku prepovedo nadaljnjo uporabo osebnih podatkov za neposredno trženje. Podjetja morajo elektronski naslov pridobiti na zakonit način.

**Za to obstajata dva načina:**

- posameznik zaupa svoj naslov sam,
- iz javno dostopnih virov, vendar mora posameznik dovoliti uporabo.

To je natančno opredeljeno v Zakonu o varstvu potrošnikov. Posameznik lahko uporabo svojih osebnih podatkov v namene neposrednega trženja kadar koli prekliče. Vsak posameznik ima pravico vpogleda v osebne podatke, ki se nanašajo nanj. To mu mora upravljavec omogočiti v 15 dneh. Omejitev pravic ima posameznik le v primeru evidenc policije, varnostnih državnih organov, Sove (Slovenska varnostno obveščevalna služba) in Urada za preprečevanje pranja denarja.

### **5.2.2 ZAKON IN VIDEONADZOR NA DELOVNEM MESTU**

V Zakonu o varstvu osebnih podatkov (ZVOP-1), Uradni list RS, št. 86/04 je zapisano naslednje:

#### **75. člen**

**Dostop v uradne službene oziroma poslovne prostore:**

- Javni in zasebni sektor lahko izvajata videonadzor dostopa v njihove uradne službene oziroma poslovne prostore, če je to potrebno za varnost ljudi ali premoženja, zaradi zagotavljanja nadzora vstopa ali izstopa v ali iz službenih oziroma poslovnih prostorov ali če zaradi narave dela obstaja možnost ogrožanja zaposlenih.
- Videonadzor se lahko izvaja le na takšen način, da se ne more izvajati niti snemanje notranjosti stanovanjskih stavb, ki nimajo vpliva na dostop do njihovih prostorov, niti snemanje vhodov v stanovanja.

#### **77. člen**

**Delovni prostori:**

- Izvajanje videonadzora znotraj delovnih prostorov se lahko 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.
- Prepovedano je izvajati videonadzor v delovnih prostorih izven delovnega mesta, zlasti v garderobah, dvigalih in sanitarnih prostorih.
- Zaposleni morajo biti pred začetkom izvajanja videonadzora po tem členu vnaprej pisno obveščeni o njegovem izvajanju.

### 5.2.3 NESPOŠTOVANJE ZAKONSKIH DOLOČIL

Kazenski zakonik (KZ), Uradni list RS, št. 63/94, 70/94-popr., 23/99-KZ-A, 110/02-ZDT-B, 40/04-KZ-B in 95/04-KZ-UPB1 opredeljujejo kaznovanje kršiteljev zoper kršenje pravic do zasebnosti v naslednjih členih:

#### 147. člen

##### Neupravičena osebna preiskava:

- Kdor neupravičeno preišče drugega ali stvari, ki jih ima ta na sebi ali s seboj, se kaznuje z denarno kaznijo ali zaporom do enega leta.

#### 148. člen

##### Neupravičeno prisluškovanje in zvočno snemanje:

- Kdor neupravičeno s posebnimi napravami prisluškuje pogovoru ali izjavi, ki mu nista namenjena, ali ju zvočno snema, ali kdor takšen pogovor ali takšno izjavo neposredno prenaša tretji osebi, ali takšen posnetek predvaja ali kako drugače omogoči, da se z njim neposredno seznanj, se kaznuje z denarno kaznijo ali z zaporom do enega leta.

#### 149. člen

##### Neupravičeno slikovno snemanje:

- Kdor neupravičeno slikovno snema ali naredi slikovni posnetek drugega ali njegovih prostorov brez njegove privolitve in pri tem občutno poseže v njegovo zasebnost, ali kdor takšno snemanje neposredno prenaša tretji osebi ali ji takšen posnetek prikazuje ali ji kako drugače omogoči, da se z njim neposredno seznanj, se kaznuje z denarno kaznijo ali z zaporom do enega leta.

#### 150. člen

##### Kršitev tajnosti občil:

- Kdor neupravičeno odpre tuje pismo, tujo brzojavko ali kakšno drugo tuje zaprto pisanje ali pošiljko, se kaznuje z denarno kaznijo ali z zaporom do šest mesecev.
- Kdor se z uporabo tehničnih sredstev neupravičeno seznanj s sporočilom, ki se prenaša po telefonu ali s katerim drugim telekomunikacijskim sredstvom, se kaznuje z denarno kaznijo ali z zaporom do enega leta. Prav tako se kaznuje z enako kaznijo, kdor s katerim izmed dejanj, ki so navedena v prvi in drugi alineji tega člena, omogoči drugemu, da se neposredno seznanj z vsebino sporočila ali pošiljke.

Tako so te stvari urejene v zakonu. Če zaupamo državi, smo zaščiteni pred nezakonitim nadzorovanjem in kršenjem pravic do zasebnosti.

Vendar pa ostane problem, kako dokazati kršenje pravic do zasebnosti in nezakonitega nadzorovanja?

Navedel bom zelo odmeven primer iz trgovine Emporium v Ljubljani pred nekaj leti. Ugotovljeno je bilo, da so videokamere nameščene v garderobah za pomerjanje

oblačil. Tako so »varnostniki« preko zaslonov v pisarni gledali in opazovali ljudi pri preoblačenju. Morda so to tudi posneli na prenosljiv medij in posredovali še komu tretjemu. Vemo, da se danes zelo preprosto objavi posnetek na spletnem portalu Youtube, ki je dostopen za ogled vsakomur, ki si to želi. Zelo sporno glede varovanja zasebnosti, kajne. Takoj, ko je prišlo to na dan, se je strogo odzval urad informacijske pooblaščenke in zadevo prijavil inšpekcijski službi.

To je samo en primer trgovine, ki je seveda odgovarjala na sodišču in plačala kazen. Koliko takšnih primerov ni nikoli odkritih. Sprašujem pa se, kaj so dobile žrtve, nad katerimi je bilo storjeno kaznivo dejanje. Verjetno nič, moralno pa so prizadete. Sprašujem se, kako se ti ljudje sedaj počutijo v kopalnici v kakšnem hotelu ipd.

Kot smo iz opisanega lahko izvedeli, nimamo dostopa do tehnologije in sistemov, ki so v lasti in upravljanju raznih agencij, služb, podjetij za varovanje in nadzor. Lahko prijavimo sum nezakonitega nadzora inšpekcijski službi. Upravljavci nadzornih sistemov lahko na zelo preprost način izbrišejo sporne posnetke. Tako nam preostane samo še sum, ki ga ne moremo dokazati.

## 6 MNENJE DELODAJALCA IN DELOJEMALCA O NADZORU NA DELOVNEM MESTU

Za lažje razumevanje oziroma predstavo uporabe moderne oziroma informacijske tehnologije za nadzor na delovnem mestu sem se odločil pridobiti mnenje neposredno od izvajalca in uporabnika. Tako sem izvedel intervju s predstavnikom delodajalca in osebo, ki opravlja poklic komercialista na terenu, ki uporablja sledilno nadzorno napravo.

Obe osebi sem seznanil z načinom izvedbe in namenom intervjuja, na katerega sta privolila, vendar pod pogojem, da ostaneta anonimna. Tako sem osebo, ki predstavlja delodajalca, poimenoval oseba »A« iz podjetja »X«, in osebo »B« iz podjetja »X« pa kot uporabnika. Tako sem jima zagotovil diskretnost in obljubil, da jima bom posredoval v branje diplomsko delo, v katerem bom uporabil njune odgovore.

### 6.1 INTERVJU Z DELODAJALCEM

Najprej vas lepo pozdravljam in se zahvaljujem, da ste se odločili sprejeti mojo prošnjo za intervju v zvezi z uporabo elektronskega sistema za nadzor zaposlenih na delovnem mestu. Pripravil sem dvanajst vprašanj, na katera mi prosim odgovorite čim bolj realno.

**Ali mi dovolite snemati ta razgovor, saj bi mi bilo v veliko pomoč pri poznejši obdelavi odgovorov? Seveda vam osebno jamčim diskretnost, da vašega imena in podjetja ne bom omenil v diplomskem delu.**

oseba A: Da

**Kako je vaše podjetje organizirano in koliko je vseh zaposlenih v podjetju?**

oseba A: Najprej bi vas rad seznanil, da je naše podjetje sestavljeno iz pet podjetij, ki so si po dejavnosti podobna in se ukvarjajo z varovanjem ljudi in premoženja ter drugimi storitvami. Na ravni skupine podjetja je okoli 1.200 zaposlenih. Na ravni podjetja, o katerem bova govorila, je okoli 700 zaposlenih.

**Ali nadzirate zaposlene na delovnem mestu in na kakšen način?**

oseba A: Da.

**Ali uporabljate informacijsko tehnologijo za nadzor na delovnem mestu?**

oseba A: Da, lahko naštejemo nekaj načinov: uporabljamo informacijsko tehnologijo, videonaprave, GPS za sledenje avtomobilov in s tem povezano prisotnost zaposlenih na različnih lokacijah. Pri tem bi poudaril, da je naša osnovna dejavnost varovanje ljudi in objektov oziroma premoženja. Pogodbeno smo zavezani z našim naročnikom za izvajanje varovanja in nadzora. Dolžni smo jih obveščati o poteku in izvajanju tega preko poročil. Tako smo na primer dolžni vsakodnevno beležiti vsa

dela, ki jih opravlja naš delavec v zvezi z izvajanjem varovanja. To je čas prihoda na lokacijo objekta, trajanje nadzora in ugotovitve dejanskega stanja.

### **Ali ste o izvajanju nadzora obvestili zaposlene in na kakšen način?**

oseba A: Da, imamo pravilnik o delovnih obveznostih zaposlenih v podjetju. Preko tega so vsi seznanjeni, da je stavba, v kateri delajo, pod videonadzorom in da so službeni avtomobili opremljeni z GPS nadzornim sistemom. Poudaril bi, da nadzor preko GPS sistemov in tudi drugih nadzornih sistemov opravljamo sami v podjetju, kjer imamo „varnostno nadzorni center“.

### **Ali menite, da je takšen način nadzora primeren?**

oseba A: Da, ker na ta način izpolnjujemo tudi merila, ki nam jih predpisuje zakonodaja. Naj povem primer, da mora biti vozilo pri prevozu denarja in vrednostnih papirjev nadzorovano 24 ur na dan. Moramo vedeti, kje se nahaja v delovnem času in tudi izven delovnega časa. Poleg tega sledimo našim avtomobilom zaradi narave dela, ki sem ga prej omenil. Seveda posredno sledimo kilometrino, porabo goriva, obenem pa poskušamo z analiziranjem poti tudi racionalizirati proces dela. Glede na dejavnost, ki jo opravljamo, pa se mi zdi takšen način nadzora ne samo primeren, ampak tudi zelo potreben.

### **Kakšni so stroški izvajanja takšnega nadzora na zaposlenega?**

oseba A: Težko bi opredelili strošek na zaposlenega. Sistem za nadzor je v naši lasti. Plačujemo pa najemnino za programsko opremo, ki nam jo posreduje podjetje, ki se ukvarja samo s tem. V Sloveniji imamo okoli 150 vozil pod GPS nadzorom in če stroške razdelimo na ta vozila, lahko povem, da znaša mesečni strošek okoli 13 evrov na avtomobil. Poudarjam pa, da je to samo strošek tehnike.

### **Kako ukrepite s kršitelji delovnih obveznosti, ugotovljenimi na takšen način?**

oseba A: Pred kratkim smo imeli primer kršitve delovne obveznosti enega zaposlenega, ki je uporabil službeno vozilo v druge namene, za kar ni imel dovoljenja nadrejene osebe. Poklicali smo ga na razgovor, kjer je dejanje priznal in smo sporazumno prekinili sodelovanje. V takšnih primerih postopamo skladno s pravili, ki jih opredeljujeta pravilnik o delovnih razmerjih in zakon o delovnih razmerjih, izvede se disciplinski postopek preko pravne službe, ki glede na ugotovitve stopnje kršitve povzročitelja primerno sankcionira. Na malenkosti običajno ne odreagiramo in jih prepustimo presoji nadrejenih. Ker so naši zaposleni uniformirani, avtomobili pa označeni z našim logotipom, smo v javnosti razpoznavni in zato moramo še posebej skrbeti za ugled naše firme, ki se nahaja oziroma deluje v zelo konkurenčnem področju.

### **Kaj storite z dokazi, pridobljenimi na ta način?**

oseba A: Z dokazi, pridobljenimi na takšen način, ravnamo po predpisih, ki jih opredeljuje zakon. Kadrovska pravna služba poskrbi za primerno hranjenje in zaščito pred morebitnim nepooblaščenim vpogledom in zlorabo ves čas, dokler traja

disciplinski postopek. Ko je postopek zaključen, dokazni material arhivira in po zakonsko določenem roku in postopku poskrbi za uničenje.

### **Ali upoštevate zakonodajo?**

oseba A: Da in to striktno do najmanjše vejice.

### **Ali upoštevate moralno-etična načela pri izvajanju nadzora?**

oseba A: Seveda, nekaj od tega že predpisuje zakon. Osebno se zavzemam za tako imenovani model življenjskosti, nikoli ne grem preko moralno-etičnih načel in ne dopuščam kakršnega koli medsebojnega obračunavanja. Zavedam se, da lahko pri tako veliki delovni organizaciji, kot je naša, prihaja do konfliktov, saj poznate tisti pregovor „sto ljudi, sto čudi“. Ko in če zaznamo kakršno koli osebno obračunavanje, to takoj prekinemo in ukrepamo tako, da se z osebo pogovorimo in skušamo preprečiti nadaljnje probleme. Če pa ugotovimo, da so medsebojna trenja prevelika, poskušamo s premestitvami ali prerazporeditvami preprečiti stik med konfliktnimi osebami. Nikogar še nismo odpustili zaradi kakšne neživljenjske, nemoralne ali neetične zadeve. Vsaj ne, odkar sem jaz v tem podjetju.

To bi bilo sedaj vse kar me je zanimalo, še enkrat se vam zahvaljujem za vašo pripravljenost, da ste odgovarjali na zastavljena vprašanja.

## **6.2 INTERVJU Z UPORABNIKOM GPS-A V VOZILU**

Najprej vas lepo pozdravljam in se zahvaljujem, da ste se odločili sprejeti mojo prošnjo za intervju v zvezi z uporabo elektronskega sistema za nadzor zaposlenih na delovnem mestu. Pripravil sem dvanajst vprašanj, na katera mi prosim odgovorite čim bolj realno. Najprej bi vas vprašal naslednje:

**Ali mi dovolite snemati ta razgovor, saj bi mi bilo v veliko pomoč pri poznejši obdelavi odgovorov? Seveda vam osebno jamčim diskretnost, da vašega imena in podjetja ne bom omenil v diplomskem delu.**

oseba B: Da.

### **Ali vas nadzorujejo na delovnem mestu in na kakšen način?**

oseba B: Da, nadzorujejo me na delovnem mestu preko GPS nadzornega sistema, ki je vgrajen v službeno vozilo, ki ga uporabljam. Moram povedati še to, da imam s podjetjem sklenjeno pogodbo o uporabi službenega vozila za zasebne namene izven delovnega časa, za kar plačujem dodatno boniteto.

### **Ali ste s strani delodajalca seznanjeni o načinu nadzora?**

oseba B: Da, delodajalec nas je seznanil na sestanku, na katerem so nam prikazali „demonstracijsko“ različico na primeru, kako sistem deluje.

**Ali ste seznanjeni, kako deluje sledilna naprava v vozilu, katerega uporabljate?**

oseba B: Da, strokovnjaki iz podjetja, pri katerem so naši ljudje naročili storitev sledenja, so nam na pilotskem primeru nazorno prikazali, kako sistem deluje. Preko računalnika lahko spremljajo vozilo, in sicer: kdaj greš na pot, kje se ustaviš, koliko časa stojiš, kako hitro voziš, kje se voziš, kraj, ulico, hišno številko ... skratka, vse.

**Ali se strinjate z izvajanjem nadzora na takšen način?**

oseba B: Ne, s tem se ne strinjam, ker nam je delodajalec obrazložil, da je to uvedel zaradi racionalizacije službenih poti in s tem pričakuje znižanje stroškov. Sam pa vem, da se zaradi tega nič manj ne vozim. Poti so okvirno znane že vnaprej in nemogoče je vsak mesec prevoziti enako število kilometrov, ker se vedno dogodi kaj nepredvidljivega. Včasih stranke ni tam in se moraš vrniti še enkrat. Tudi dela na cestnih odsekih včasih zahtevajo obvoze in se določene poti podaljšajo.

**Ali ste podpisali kakšen dokument v zvezi z izvajanjem sledenja vozil?**

oseba B: Da. Podpisali smo izjavo, da smo seznanjeni z izvajanjem sledenja na vozilih s strani podjetja. Doma hranim kopijo izjave.

**Ali vas takšen način nadzora pozitivno motivira oziroma ali zaradi tega bolj delate?**

oseba B: To je pa daleč od tega. Delam tako kot prej, ampak s to razliko, da sem vedno pod nekim pritiskom in poskušam na nek način odmisлити, da sem pod nadzorom. Skratka, nisem sproščen. Vest, da sem pod nadzorom, deluje name psihično obremenjujoče. Ne strinjam se s tezo, da me pozitivno motivira, prej nasprotno.

**Kako gledate na delodajalca zaradi tega?**

oseba B: Kot sem že rekel, je popolnoma nepotrebno izvajanje nadzora na takšen način. Občutim nezaupanje s strani delodajalca, saj nam je bilo predstavljeno, da je razlog uvedbe sledenja zmanjšanje prevoznih stroškov, v kar pa močno dvomim. Saj tudi nadziranje na ta način nekaj stane, mar ne. Mislim, da se je pojavilo nezaupanje tudi do delodajalca z moje strani, kajti ne vem, kdo vse ima vpogled v računalnik in s tem povezano upravičeno sumim v verodostojnost podatkov, pridobljenih na ta način. Sumim pa še na možnost zlorabe teh podatkov. Nekdo, ki spremlja moje poti, točno ve, kdaj grem od doma. To je zelo zaupen podatek, za vlomilce pa je lahko zelo dobrodošel.

**Ali menite, da je uvedba nadzora preko GPS-ja primerna metoda?**

oseba B: Ne. Obstaja veliko drugih načinov nadzora, ki so človeku bolj prijazni, humani. Lahko me preverijo preko vsakodnevnih poročil, s telefonskim preverjanjem, z uporabo žiga kupca na naročilih. Tudi osebna kontrola na poti je bolj prijazen način. Nekateri kupci imajo knjigo obiskovalcev, kjer se evidentirata datum in čas obiska.

**Ali ste na delovnem mestu zaradi tega bolj sproščeni?**

oseba B: Ne, prav nasprotno. To deluje zelo destimulativno in moteče. Od uvedbe sistema vse bolj razmišljam o tem, da bi zamenjal službo.

**Ali poznate zakonodajo v zvezi z nadzorom na delovnem mestu?**

oseba B: Nekaj mi je znano. Odkrito povedano sem se od trenutka, ko so mi vgradili sledilno napravo, začel zanimati o zakonski regulativi, ki ureja to področje. Kot je meni znano, je to dovoljeno in ni prepovedano, ker gre za zaščito zasebne lastnine. Ni pa opredeljeno z etičnega vidika in vidika zasebnosti.

**Kaj menite o stroških, ki nastanejo pri izvajanju nadzora z GPS sistemom?**

oseba B: Stroški so za moje pojme zelo visoki in nepotrebni, saj kot je meni znano stane sama naprava okoli 250 €, potem pa še vsak mesec okoli 60 € za naročnino. In iz tega razloga ne opravičujejo namena, zaradi česar so sistem nabavili. Naj vas spomnim, da nam je bilo rečeno, da zaradi znižanja prevoznih stroškov.

**Ali so medsebojni odnosi zaradi tega boljši?**

oseba B: Lahko rečem, da ne. Ne bom rekel, da so slabši, ampak da so na neki preizkušnji. Vsak ima svoje stališče glede tega. Za zdaj nas pustijo pri miru, saj še nihče ni bil klican na zagovor.

To bi bilo sedaj vse kar me je zanimalo, še enkrat se vam zahvaljujem za vašo pripravljenost, da ste odgovarjali na zastavljena vprašanja.

**6.3 NADZOR NA DELOVNEM MESTU – »DA ALI NE«?**

V današnjem času je torej še vedno dokaj pereče vprašanje: Nadzor na delovnem mestu: **Da ali Ne?** Evropska zakonodaja je načeloma bolj naklonjena pravici do zasebnosti posameznika na delovnem mestu kot na primer zakonodaja v ZDA.

Če „**DA**“, potem mora biti nadzor izveden zakonito, kar pomeni najmanj (pisno) soglasje zaposlenega. Nekatere vrste nadzora kljub pisnemu soglasju niso dovoljene. Potrebno je biti pozoren na pravice tretjih oseb. Nadzor mora biti transparenten. Zakaj se izvaja, kako se izvaja, kdo in v kakšnih primerih ima dostop do podatkov, koliko časa se podatki hranijo.

Potrebno je pretehtati, kakšna je pričakovana korist nadzora in kakšni so negativni učinki na klimo med zaposlenimi.

In še »**NE**«, ker škoduje oziroma izpostavlja problem dostojanstva in avtonomije posameznika na delovnem mestu. Povečevanje nadzora in nakup novih nadzornih tehnologij ima lahko negativne učinke. Tehnična zaščita ni vedno učinkovita, saj jo je mogoče zaobiti. Če bo nekdo od zaposlenih želel ukrasti informacije ali škodovati podjetju, lahko to stori kljub nadzorni tehnologiji.

Je pomembnejša motivacija in lojalnost zaposlenih ali povečan nadzor? (Kovačič, 2006)

**Največkrat se delodajalci branijo z naslednji izjavami oziroma navedbo razlogov, zaradi katerih zagovarjajo nadzor na delovnem mestu (Kovačič, 2006):**

- Podjetje je lastnik delovne opreme, svoje premoženje lahko nadzoruješ.
- Če zaposleni opremo podjetja uporablja v zasebne namene, s tem oškoduje podjetje, saj mu krade delovni čas in denar.
- Zaposleni je v službi zato, da dela.
- Naše podjetje je zaskrbljeno zaradi internih groženj, potencialni osumljenci so vsi zaposleni.
- Želimo se zaščititi pred krajo poslovnih skrivnosti.
- Želimo se zaščititi pred odškodninskimi tožbami zaradi neprimerne ravnanja zaposlenih (primer podjetja Chevron, ki je moralo štirim ženskam plačati 2,2 mio. USD odškodnine, ker jim je njihov zaposleni pošiljal elektronsko pošto z žaljivo vsebino (glej Kovačič 2006).

## **6.4 TANKA MEJA MED ZASEBNIM IN SLUŽBENIM**

Delodajalec, ki bere sporočila, ki jih zaposleni pošilja ali sprejema preko službenega računalnika, krši temeljne pravice delavca, kot jih določa 8. člen Evropske konvencije o človekovih pravicah. To velja, ne glede na to, ali je bil delavec vnaprej seznanjen, da službenega računalnika ne sme uporabljati v neslužbene namene. Podjetje ali druge ustanove ne smejo biti mesta, kjer bi delodajalci arbitrarno in brez omejitev izvajali svoje diskrecijske pravice; ne smejo postati okolja totalnega nadzora, kjer temeljne človekove pravice nimajo veljave ... Menimo, da je splošna popolna prepoved uporabe e-pošte v neslužbene namene nerealna in krši pravno načelo sorazmernosti. Prav tako je nesmiselno zahtevati od uporabnika službenega avtomobila, da ga uporablja striktno samo v službene namene. Saj bi že s tem, da bi zjutraj peljal ženo spotoma v službo ali otroka v šolo kršil pogodbeno pravila. Če bi službeni telefon uporabil za pogovor z ženo ali otrokom, bi seveda že kršil pogodbeno pravila.

Na drugi strani pa je država z obdavčitvijo uporabe službenega avtomobila v zasebne namene stvari še bolj zapletla in obremenila zaposlene.

## 7 ZAKLJUČEK

Danes se ljudje vse bolj zavedamo, da živimo v družbi nadzora, saj je vsak naš korak nadzorovan, če to želimo ali ne. V tem diplomskem delu smo predstavili koristi in pomanjkljivosti oziroma slabosti nadzorovanja s pomočjo informacijske tehnologije.

Teoretično smo podrobno opisali, kaj razumemo pod pojmi zasebnost, nadzorovanje in informacijska tehnologija sodobnega časa. Na nekaterih primerih iz prakse smo ugotovili, da se ti med seboj stalno prepletajo in so na nek način povezani.

Natančno določiti mejo med zasebnim in javnim se ne da, ker je zasebnost na nek način živa dimenzija, ki se sčasoma nenehno spreminja in se prilagaja glede na nova merila in standarde, ki jih določa družba v različnih geografskih, kulturnih, religioznih ali ekonomskih okoljih.

Ugotovili smo tudi, da je potrebno razmerja med delodajalci in zaposlenimi v zvezi z nadzorovanjem na delovnem mestu urediti ali dopolniti na področju zakonodaje. Pri tem imamo v mislih vprašanje: Kako dokazati kršenje pravic do zasebnosti? Odgovor na to vprašanje ostaja še vedno odprto.

Opozoriti moramo na to, da nadzorovanje oseb lahko v nekaterih primerih družbi koristi (dogodki 11. septembra 2001 v ZDA) in na drugi strani lahko škoduje (primer iz trgovine Emporium v Ljubljani).

Vse več naših osebnih podatkov je zapisanih v digitalni obliki v centralni podatkovni zbirki. Pridružujejo se jim tudi podatki o naših dnevni dejavnostih in aktivnostih. Verjetno je le še vprašanje časa, kdaj bodo vsi podatki o tem, kaj smo, kaj delamo, kje se nahajamo, s kom smo v stiku ... kot pravi zgodba v filmu *Zeitgeist* (neodvisna produkcija, ki je na voljo za brezplačen ogled na [Zeitgeistmovie.com](http://Zeitgeistmovie.com)), s kartic prenesena v miniaturne čipe RFID (radio-frekvenčna identifikacija), ki jih bomo imeli nameščene pod kožo. In vse naprave bodo ob katerem koli času vedele, kdo vstopa v njihovo območje dosega, kakšne navade imamo, kje živimo, kje kupujemo, kje se vozimo, katero politično stranko podpiramo, koliko denarja imamo na računu itd. Država, družba in ekonomija se ne bodo odrekli pravici do informacij zasebnega značaja, ki jih bodo zbirali, shranjevali in obdelovali na različne načine, ker je vsakomur kristalno jasno, da je imeti takšne informacije veliko bogastvo in moč. In ko bomo za oblast postali »neposlušen državljan«, bodo naš čip na daljavo preprosto izklopili. Vsi podatki o nas bodo izpuhteli in mi z njimi. In to ni najbolj pesimističen scenarij.

## LITERATURA IN VIRI

### Knjige:

- Bogataj, M. (2003). *Internet in pravo*. Ljubljana: Pravna fakulteta.
- Čebulj, J. (1992). *Varstvo informacijske zasebnosti v Evropi in Sloveniji*. Ljubljana: Inštitut za javno upravo pri Pravni fakulteti v Ljubljani.
- Foucault, Michael (1991). *Nadzorovanje in kaznovanje*. Ljubljana: Delavska enotnost.
- Kovačič, M. (2006). *Nadzor in zasebnost v informacijski družbi*. Ljubljana: FDV.
- Kovačič, M. (2003). *Zasebnost na internetu*. Ljubljana: Mirovni inštitut.
- Kuhelj, A. (2004). *Varstvo pravice do zasebnosti, veroizpovedi in svobodnega izražanja v pravu Sveta Evrope*. Ljubljana: Fakulteta za upravo.
- Mlinar, Z. (1994). *Individuacija in Globalizacija v prostoru*. Ljubljana: SAZU.
- Tomšič, A. (2009). *Zasebnost in varovanje osebnih podatkov na delovnem mestu*. Ljubljana: Forum Media.

### Članki:

- Kocmur, H. (2005). *Z alkotesti nad uradnike, z detektivi nad bolnike in doječe matere*. Nedelo 11. 9. 2005, dostopno na [http://www.delo.si/index.php?sv\\_path=43.50&src=mm](http://www.delo.si/index.php?sv_path=43.50&src=mm), 15.9.2009.
- Možina, D. (2002). *Se Evropa odreka zasebnosti v korist varnosti?* Informatika in pravo, Ljubljana: Pravna praksa št. 43. Gospodarski vestnik.

### Drugi viri:

- Kašnik, S. (2006). *Sodobne tehnologije nadzora v Sloveniji*. Diplomsko delo. Ljubljana: FDV.
- Miller, J.A. (1981). *Despotizem Koristnega*. Problemi razprave, št. 6-8, letnik XIX, strani 17–35. Ljubljana. Društvo za teoretsko psihoanalizo.

### Spletne strani

- Zasebnost in zaščita osebnih podatkov, <http://www.zps.si/aktualno/racunalniki-in-telefon/zasebnost-in-zascita-osebni-podatkov.html?Itemid=238>, dostop 24. 8. 2009.
- Zasebnost in nadzor v informacijski družbi, <http://www.ljudmila.org/matej/zasebnost/>, dostop 25. 7. 2009.
- Varnost in zasebnost, [http://www.informacijskadruzba.si/index.php?option=com\\_content&task=view&id=74&Itemid=85](http://www.informacijskadruzba.si/index.php?option=com_content&task=view&id=74&Itemid=85), dostop, 26. 7. 2009.
- Ministrstvo za finance, <http://www.unp.gov.si/>, dostop, 25. 5. 2009.
- Inšpekcijski nadzor, <http://www.ip-rs.si/varstvo-osebni-podatkov/inspekcijski-nadzor/> dostop, 25. 9. 2009.
- Nadzor nad zakonitostjo dela,

- [http://www.sova.gov.si/index93c5.html?sv\\_path=1102,1110](http://www.sova.gov.si/index93c5.html?sv_path=1102,1110), dostop 25. 5. 2009.
- Varuh človekovih pravic, <http://www.varuh-rs.si/>, dostop 26. 5. 2009.
  - Evropski varuh človekovih pravic, <http://www.ombudsman.europa.eu/home/sl/default.htm>, dostop 20. 5. 2009.
  - Zakon o varstvu osebnih podatkov, [http://zakonodaja.gov.si/rpsi/r06/predpis\\_ZAKO3906.html](http://zakonodaja.gov.si/rpsi/r06/predpis_ZAKO3906.html), dostop 25. 5. 2009.
  - Ustava Republike Slovenije, <http://www.dz-rs.si/?id=150>, dostop 20. 5. 2009.

## KAZALO SLIK

Slika 1: Panoptikon (Jeremy Bentham, 1791), vir: Wikipedia 2009.

Slika 2: Ljubljana »tromostovje«, vir: Google Earth 2009.

## POJMOVNIK

kodifikacija – združitev različnih zakonov, poenotenje

klasifikacija – razvrščanje

Facebook – spletna stran na internetu

Myspace – spletna stran na internetu

kriptografija – skrivnopoljsje

konvergenca – zmanjševanje razlik, zблиževanje

devianten – ekstremen, izstopajoč, neobičajen

multimedialnost – uporaben v drugih medijih, konvergenca med formati,

babysytter – naprava za prenos zvoka, za nadzor otrok iz drugih prostorov

biometrija – uporaba telesnih značilnosti za identifikacijo

## KRATICE IN AKRONIMI

SSKJ: slovar slovenskega knjižnega jezika

IP: internetni protokol (registrska številka internetnega priključka)

IKT: informacijsko-komunikacijska tehnologija

GPS: vseprostorski sistem določanja lokacije (global positioning system)

GPRS: prenos računalniških podatkov v paketni obliki

LAN: povezava preko vodnikov

WAN: brezžična povezava

DNK: genska identifikacija

SPAM: nezaželeno oglaševanje preko spletne mreže

UN: Organizacija združenih narodov

EMŠO: enotna matična številka občana

SOVA: Slovenska varnostno obveščevalna agencija

RFID: radio-frekvenčna identifikacija

ZVOP: Zakon o varstvu podatkov