

UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

ZAKLJUČNA STROKOVNA NALOGA VISOKE POSLOVNE ŠOLE

**NADZOR DELODAJALCA IN ZASEBNOST NA DELOVNEM
MESTU**

ERIK KONCUT

IZJAVA O AVTORSTVU

Podpisani Erik Koncut, študent/-ka Ekonomske fakultete Univerze v Ljubljani, predloženega dela z naslovom Nadzor delodajalca in zasebnost na delovnem mestu, pripravljenega v sodelovanju s svetovalko Nado Zupan

IZJAVLJAM

1. da sem predloženo delo pripravil/-a samostojno;
2. da je tiskana oblika predloženega dela istovetna njegovi elektronski obliki;
3. da je besedilo predloženega dela jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem poskrbel/-a, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam oziroma navajam v besedilu, citirana oziroma povzeta v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani;
4. da se zavedam, da je plagiatstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku Republike Slovenije;
5. da se zavedam posledic, ki bi jih na osnovi predloženega dela dokazano plagiatstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom;
6. da sem pridobil/-a vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označil/-a;
7. da sem pri pripravi predloženega dela ravnal/-a v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobil/-a soglasje etične komisije;
8. da soglašam, da se elektronska oblika predloženega dela uporabi za preverjanje podobnosti vsebine z drugimi deli s programsko opremo za preverjanje podobnosti vsebine, ki je povezana s študijskim informacijskim sistemom članice;
9. da na Univerzo v Ljubljani neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve predloženega dela v elektronski obliki, pravico reproduciranja ter pravico dajanja predloženega dela na voljo javnosti na svetovnem spletu preko Repozitorija Univerze v Ljubljani;
10. da hkrati z objavo predloženega dela dovoljujem objavo svojih osebnih podatkov, ki so navedeni v njem in v tej izjavi.

V Ljubljani, dne _____

Podpis študenta(-ke): _____

KAZALO

UVOD	1
1 ETIKA IN MORALA.....	2
2 DELOVNO OKOLJE	2
3 PRAVNA UREDITEV NA PODROČJU ZASEBNOSTI.....	3
3.1 Zakon o varstvu osebnih podatkov	4
3.2 Zakon o delovnih razmerjih	5
3.3 Zakon o elektronskih komunikacijah.....	5
3.4 Ustava Republike Slovenije	5
4 ZASEBNOST NA DELOVNEM MESTU.....	6
5 NADZOR NA DELOVNEM MESTU	7
5.1 Videonadzor na delovnem mestu.....	8
5.2 GPS nadzor	9
5.3 Beleženje prihodov in odhodov z delovnega mesta.....	9
5.4 Nadzor nad elektronsko pošto in telefonom	10
5.5 Testiranje s poligrafom	10
5.6 Biometrija	10
5.7 Detektivske agencije	11
5.8 Vgrajevanje čipov	12
6 SODBE EVROPSKEGA SODIŠČA ZA ČLOVEKOVE PRAVICE V POVEZAVI Z NADZOROM NA DELOVNEM MESTU.....	13
6.1 Primer Halford proti Združenemu kraljestvu.....	13
6.2 Primer Copland proti Združenemu kraljestvu	14
6.3 Primer I proti Finski.....	14
6.4 Primer Bogdana Barbulescuja	15
7 MOBING	15
8 POSLEDICE NADZORA NA DELOVNEM MESTU	17
8.1 Absentizem	18
8.2 Prezentizem.....	20
8.3 Fluktuacija	21
SKLEP	22
LITERATURA IN VIRI	24

UVOD

Ljudje skoraj tretjino svojega življenja preživimo na delovnem mestu, zato ni nepomembno, kako se tam počutimo. Kakovost opravljenega dela je odvisna od vsakodnevnih dogajanj na delovnem mestu. Medsebojni odnosi, način vodenja in motiviranja vplivajo na zaposlene. Delovno okolje tako na zaposlenega lahko vpliva pozitivno ali negativno. Dobro motivirani ljudje so pripravljeni vložiti več truda in energije, medtem ko so nezadovoljni delavci nemotivirani in manj učinkoviti. Kljub temu da smo v času gospodarske in finančne krize, bi bilo dobro, da se na zaposlene ne gleda samo kot na strošek, ampak kot na potencial, ki prinaša podjetju dodano vrednost.

Etiko potrebujemo zaradi splošnega sprejemanja in veljavnosti moralnih načel, ki presegajo posameznikova moralna načela in vrednote. Vrednote posameznika se razlikujejo, medtem ko so etična načela splošna, zato vrednote niso zadostno izhodišče za poslovodno odločanje, ampak so potrebna etična načela ravnanja. Zasebnost predstavlja pomembno vrednoto vsakega posameznika. Velik problem nastane, ko želimo določiti mejo med zasebnostjo in delom v odnosu delodajalec - zaposleni. Načini, s katerimi podjetje oziroma delodajalec posega v zasebnost, so pregledovanje elektronske pošte, nadzor v uporabi interneta, testiranje glede uporabe nedovoljenih substanc, prisluškovanje telefonom, videonadzor ipd. Na delovnem mestu ima vsak zaposleni pravico do zasebnosti. Zakonsko je urejeno, da mora delodajalec zaposlene pisno seznaniti, če se na delovnem mestu izvaja npr. videonadzor. Podjetja oziroma lastniki vedno bolj težijo k povečanju dobička, zaradi česar pa prihaja tudi do vse večjih pritiskov in posledično do nadziranja zaposlenih na delovnem mestu. Lastnik podjetja oziroma delodajalec neredko posega po takih ukrepih, ki so sicer zakoniti, z vidika morale in etike pa zelo sporni. Interes delodajalca je, da stremi k čim večji učinkovitosti in storilnosti na delovnem mestu, na drugi strani pa je interes zaposlenega čim večja zasebnost. Namen zaključne naloge je s pomočjo domače in tuje literature predstaviti ključne dileme nadziranja s strani delodajalca na delovnem mestu ter zasebnost, ki jo ima zaposleni na samem delovnem mestu. Zaključna naloga obravnava načine nadziranja na delovnem mestu s strani delodajalca in način poseganja v zasebnost vsakega posameznika ter posledice pretiranega nadzora na delovnem mestu. V nalogi je predstavljen tudi pravni vidik, ki natančno ureja, do kje sme delodajalec posegati v zasebnost zaposlenega.

Cilj zaključne naloge je podati nekaj predlogov, kako zmanjšati nadzor na delovnem mestu in poseganje v zasebnost zaposlenih na delovnem mestu ter na takšen način doseči nižje stroške za podjetja.

Zaključna naloga temelji na teoretičnem delu, torej je osnovana na študiju literature. V nalogi poskušam analizirati dosedanja spoznanja na področju zasebnosti in nadzora na delovnem mestu.

Hipoteza: Z razvojem modernejših oblik tehnologij se povečuje možnost zlorabe le-teh s strani delodajalca pri nadziranju zaposlenih.

1 ETIKA IN MORALA

Beseda **etika** izhaja iz grške besede *ethos*, kar pomeni dostojanstvo, značaj, način življenja. **Moralno** pa izhaja iz latinščine *moralis*, kar pomeni običaj, navado in označuje obliko človekovega odnosa do sveta. Etika in morala pomenita osnovni način ravnanja, ki ni samo običajen, pač pa tudi pravilen (Tschudin, 2004, str. 37).

Etika je kritična refleksija moralnega delovanja ter se kot praktična disciplina sklicuje na praktični razum. Etika je disciplina v filozofiji in si prizadeva opredeliti naravo in pomen različnih moral ter je študija o tem, kaj je prav in kaj narobe (Kocmur, 2006, str. 663–666). Etika pomeni tudi poštenost in odgovornost za prevzemanje stališč (Tschudin, 2004, str. 37).

Ravnanje, ki se sklada z zakoni v določeni družbi, imenujemo zakonito ravnanje. Običajno so zakonska pravila v skladu s prevladujočimi moralnimi pravili, vsebujejo pa tudi grožnje za posameznika, ki jih ne upošteva. Zakoni poskušajo slediti moralnim načelom (Kocmur, 2006, str. 663–666).

Etiko potrebujemo zaradi splošnega sprejemanja in veljavnosti moralnih načel, ki presegajo posameznikova moralna načela in vrednote. Vrednote posameznika se razlikujejo, medtem ko so etična načela splošna, zato vrednote niso zadostno izhodišče za poslovodno odločanje, ampak so potrebna etična načela ravnanja. Na relaciji družba - država - podjetje etika poleg državne regulacije prispeva h koristnim vzorcem obnašanja (Drnovšek & Prodan, 2005, str. 28).

Poslovna etika je uporaba etičnih pravil in načel, ko govorimo o poslovnih odločitvah. V poslovni etiki menedžer upošteva, da je sprejel odgovornosti do podjetja, na osebni ravni pa je odgovoren prijateljem in družini ter lokalni skupnosti (Drnovšek & Prodan, 2005, str. 29).

Zelo težko je v poslovnem svetu sprejemati etične odločitve. Ko smo postavljeni pred etično dilemo, je treba izbrati ustrezno strategijo presoje ter upoštevati izkušnje drugih. Upoštevanje etičnosti odločitve se mora zgoditi čim bolj zgodaj v procesu sprejemanja odločitve (Drnovšek & Prodan, 2005, str. 42).

2 DELOVNO OKOLJE

Pomemben dejavnik poslovanja predstavlja prav delovno okolje, še posebej tisti del, ki je tesno povezan z ljudmi. Delovno okolje je neločljivo povezano z učinkovitostjo in uspešnostjo, zato je proučevanje le-tega še posebej smiselno in potrebno. Vplivi, ki jih ima delovno okolje na posameznika oziroma vplivi, ki nastajajo v delovnem okolju, pomembno vplivajo na psihofizično stanje posameznika, kar pa lahko predstavlja tudi kopico zdravstvenih problemov. Vse naštetu pomembno vpliva na uspešnost in učinkovitost delovnega mesta, zato je pomembno, da organizacija posveča več pozornosti posamezniku oziroma sociokulturnemu okolju organizacije (Stare, 2012, str. 5).

Poslovno okolje podjetja v splošnem delimo na zunanje ter notranje okolje. Na zunanje okolje vplivajo spremenljivke zunaj podjetja, na katere podjetje na kratek rok nima vpliva. Med spremenljivke, ki vplivajo na podjetje iz zunanjega okolja, uvrščamo cene, dosegljivost posojil, bruto domači proizvod, zakonodajo, politično moč, inovacije ter invencije, tehnološki razvoj.

Spremenljivke, ki vplivajo na notranje okolje, so narava in organizacija, kultura podjetja, lastniki in vodstvo podjetja ter zaposleni (Jaklič, 2005, str. 2–3). Notranje okolje podjetja je v veliki meri določeno s specifikami zunanjega okolja delovanja podjetja, kar pomeni, da sta notranje in zunanje okolje podjetja v odnosu soodvisnosti oziroma se odnosi med seboj tesno prepletajo. Napačno bi bilo trditi, da so podjetja pri svoji organizaciji odvisna izključno od zunanjega okolja, v katerem delujejo. Notranje okolje podjetja oziroma silnice, ki delujejo med interesnimi skupinami v podjetju, se najpogosteje kažejo v kulturi podjetja. Kulturo podjetja bi lahko predstavili tudi z besedo skupnost. V skupnosti se vidijo odnosi med ljudmi. Ni pa vsaka kultura primerna za vsako organizacijo, kajti lahko se zgodi, da obstaja več kultur znotraj podjetja. Prav zaradi hitro spreminjajočega se zunanjega okolja so podjetja primorana, da spreminjajo svojo kulturo. Mnogokrat je kultura v podjetjih precej rigidna, kajti organizacije in ljudje stremijo k stabilnosti. Pravočasno in primerno spreminjanje kulture v organizaciji predstavlja eno najtežjih nalog sodobnega managerja. Manager mora v danih okoliščinah najbolje oceniti, katera kultura je najbolj ustrezna (Jaklič, 2005, str. 315–318).

Podjetja lahko veliko prispevajo k dobremu počutju zaposlenih na delovnem mestu tako, da pozornost namenijo prijetnemu delovnemu okolju. Raziskave so pokazale, da veliko različnih dejavnikov vpliva na dobro počutje, motivacijo in zadovoljstvo zaposlenih na delovnem mestu. Različni dejavniki, ki z majhnimi stroški pripomorejo, da se zaposleni na delovnem mestu počutijo bolje, so na primer (Društvo za vrednotenje dela, organizacijski in kadrovske razvoj, 2004, str. 84):

- primerna razsvetljava,
- vonjave,
- klimatizirani prostori,
- velikost prostorov,
- možnost skupnih prostorov,
- notranja ureditev delovnih prostorov.

3 PRAVNA UREDITEV NA PODROČJU ZASEBNOSTI

Ustava Republike Slovenije (v nadaljevanju Ustava RS) v 35. členu zagotavlja posamezniku varstvo pravic zasebnosti in osebnostnih pravic. 37. člen Ustave RS posamezniku zagotavlja tajnost pisem in drugih občil, to pomeni, da zagotavlja tudi tajnost elektronske pošte. Omenjeni 37. člen Ustave RS določa da, »samo zakon lahko predpiše, da se na podlagi odločbe sodišča za določen čas ne upošteva varstvo tajnosti pisem in drugih občil in

nedotakljivost človekove zasebnosti, če je to nujno za uvedbo ali potek kazenskega postopka ali za varnost države« (Ustava Republike Slovenije, Ur. l. RS 33/1991).

37. člen Ustave RS pravi, da delodajalec brez dovoljenja zaposlenega oziroma pošiljatelja ali prejemnika ne sme prebirati elektronskih sporočil. Komunikacijska zasebnost je v Sloveniji bolj zaščitena kot drugod po Evropi. Komunikacijska zasebnost ščiti vse vrste komunikacij. To pomeni, da ne samo vsebine, pač pa tudi podatke, ki so povezane s komunikacijo.

Delovnoppravna zakonodaja narekuje zaposlenemu, da opravlja delo po navodilih in pod nadzorom delodajalca, kar pomeni, da so delodajalci upravičeni nadzirati delavce, ampak morajo zaposlene vnaprej seznaniti s pravili (Zakon o varstvu osebnih podatkov, Ur. l. RS, št. 94/2007). Nadzor je torej popolnoma legalna in legitimna pravica delodajalca. Delodajalec mora vnaprej zaposlenega seznaniti s pravili o uporabi elektronske pošte in interneta ter uporabi telefona. Zaposleni mora biti seznanjen, kdaj in v kakšnih primerih ga delodajalec nadzira, delodajalec pa si ne more privoščiti pretiranega omejevanja pravic do zasebnosti in do komunikacije z zunanjim svetom. Zaposleni se mora z nadzorom strinjati. Delodajalec lahko nadzira oziroma ima pravico nadzirati elektronsko pošto, ki si jo izmenjujejo zaposleni znotraj podjetja, ne pa elektronske pošte, ki jo je v podjetje poslala tretja oseba.

V praksi delodajalec omejuje uporabo elektronske pošte tako, da je zaposlenim omogočen dostop do tistih strani, ki jih potrebujejo za nemoten delovni proces. To pomeni, da blokirajo dostop do določenih spletnih strani. Delodajalec ne sme ugotavljati, katere spletne strani je zaposleni obiskoval v preteklosti, komu je pošiljal elektronsko pošto ter kdo jo je pošiljal zaposlenemu (Havliček, 2012).

Zakon o varstvu osebnih podatkov, Zakon o elektronskih komunikacijah, Zakon o delovnih razmerjih, Kazenski zakonik in Ustava Republike Slovenije so predpisi, ki zajemajo določila in predpise na področju zakonodaje nadzora in zasebnosti na delovnem mestu. Krovna določila na področju človekovih pravic pa zajema Ustava RS.

3.1 Zakon o varstvu osebnih podatkov

Zakon o varstvu osebnih podatkov (v nadaljevanju ZVOP-1) zagotavlja varstvo osebnih podatkov. V 8. členu pravi, da se lahko osebni podatki obdelujejo le, če je za obdelavo osebnih podatkov podana osebna privolitve ali če obdelavo osebnih podatkov, ki se obdelujejo, določa zakon. V zakonu mora biti določen namen obdelave. V primeru, da se obdelujejo podatki na podlagi osebne privolitve, mora biti posameznik predhodno pisno ali na drug način seznanjen z namenom obdelave osebnih podatkov (Zakon o varstvu osebnih podatkov, Ur. l. RS, št. 86/04).

ZVOP-1 v 10. členu določa, da se lahko v zasebnem sektorju obdelujejo osebni podatki le, če je to nujno zaradi uresničevanja zakonitih interesov zasebnega sektorja ter ti interesi prevladujejo nad interesi posameznika, na katerega se nanašajo podatki (Zakon o varstvu osebnih podatkov, Ur. l. RS, št. 86/04).

ZVOP-1 zajema tudi področje videonadzora, in sicer v 74. členu, ki določa, da mora oseba javnega ali zasebnega sektorja, ki izvaja videonadzor, o tem objaviti obvestilo. Obvestilo mora zajemati naslednje informacije (Zakon o varstvu osebnih podatkov, Ur. l. RS, št. 86/04):

- naziv osebe javnega ali zasebnega sektorja, ki izvaja videonadzor,
- da se izvaja videonadzor,
- telefonsko številko za pridobitev informacije, kje in koliko časa se shranjujejo posnetki in videonadzornega sistema.

3.2 Zakon o delovnih razmerjih

Pravice delodajalca in delavca določa Zakon o delovnih razmerjih (v nadaljevanju ZDR-1). ZDR-1 v 46. členu pravi, da mora delodajalec varovati in spoštovati osebnost zaposlenih ter upoštevati in ščititi delavčevo zasebnost (Zakon o delovnih razmerjih, Ur. l. RS, št. 21/13).

48. člen ZDR-1 določa, da lahko delodajalec osebne podatke zaposlenih zbira, obdeluje ter posreduje tretjim osebam samo v primeru, če je to določeno s tem ali kakšnim drugim zakonom ali če je to potrebno zaradi uresničevanja pravic in obveznosti iz delovnega razmerja ali v zvezi z delovnim razmerjem.

Kazenski zakonik ščiti pravice tako delodajalcev kot delojemalcev. Zakon sankcionira delodajalca v primeru, če neupravičeno snema ali pa naredi slikovni posnetek brez njegovega soglasja ter na ta način občutno poseže v njegovo zasebnost (Kazenski zakonik, Ur. l. RS št. 55/08, 138. člen).

3.3 Zakon o elektronskih komunikacijah

Zakon o elektronskih komunikacijah (v nadaljevanju ZEKom-1) ureja pogoje za zagotavljanje elektronskih komunikacijskih omrežij in izvajanje elektronskih komunikacijskih storitev, ureja zagotavljanje univerzalne storitve ter zagotavljanje konkurence. Med drugim ureja tudi omejitve lastninske pravice ter varovanje pravice do komunikacijske zasebnosti uporabnikov javnih komunikacijskih storitev (Zakon o elektronskih komunikacijah, Ur. l. RS, št. 109/12).

ZEKom-1 zvišuje varstvo zasebnosti in osebnih podatkov končnih uporabnikov. To naj bi okrepilo zaupanje v uporabo elektronskih komunikacij. Zakon uvaja strožje pogoje za poseganje v terminalsko opremo naročnika ali uporabnika. V tem primeru gre za t. i. piškotke, katerih raba je bistveno omejena (Nov zakon o elektronskih komunikacijah, 2013).

Zakon določa, da se za elektronsko pošto šteje vsako slikovno, govorno ali besedilno sporočilo, poslano po komunikacijskem omrežju, ter se ga lahko shrani, dokler ga prevzemnik ne prevzame (Zakon o elektronskih komunikacijah, Ur. l. RS, št. 109/12, 3. člen).

3.4 Ustava Republike Slovenije

Ustava RS določa (Ustava RS, Ur. l. 33/1991):

35. člen

(varstvo pravic zasebnosti in osebnostnih pravic)

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

37. člen

(varstvo tajnosti pisem in drugih občil)

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

38. člen

(varstvo osebnih podatkov)

Zagotovljeno je varstvo osebnih podatkov. Prepovedana je uporaba osebnih podatkov v nasprotju z namenom njihovega zbiranja.

Zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa zakon.

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

4 ZASEBNOST NA DELOVNEM MESTU

Zasebnost predstavlja pomembno vrednoto velike večine ljudi. Velik problem nastane, ko želimo določiti mejo med zasebnostjo in delom v odnosu delodajalec - zaposleni. Delodajalci povsem legitimno zahtevajo uspešno opravljanje dela, vendar se pogosto dogaja, da posegajo v zasebnost zaposlenih. Načini, s katerimi delodajalec posega v zasebnost, so pregledovanje elektronske pošte, nadzor v uporabi interneta, testiranje glede uporabe nedovoljenih substanc, prisluškovanje telefonom, videonadzor ipd. Z razvojem informacijske tehnologije pa so se ti pristopi še spremenili. S pomočjo računalnikov lahko delodajalec zbere in hrani veliko podatkov, to pa pomeni, da zaposleni praktično nima več zasebnosti (Drnovšek & Prodan, 2005, str. 138–139).

V odnosu delodajalec - zaposleni velikokrat pride do konflikta interesov. Zaposleni ima pravico do zasebnosti, pravica delodajalca, ki jo ima kot lastnik komunikacijske opreme oziroma sredstev podjetja, pa je, da izvršuje lastninske pravice nad sredstvi ter da nadzira, ali je oprema, dana na razpolago zaposlenim, uporabljena skladno z namenom (Kovačič, 2010).

Zelo težko je najti ravnovesje med pravico zaposlenih in pravico delodajalca ter postaviti mejo, ki bi zadovoljila obe strani. Vsekakor pa mora delodajalec hraniti nekatere podatke zaposlenih, ki so potrebni za uspešno načrtovanje in izvajanje delovnega procesa. Izpostavil bi dejstvo, da se vsi sklicujemo na pravico do zasebnosti na delovnem mestu. Po drugi strani pa v domačem okolju vsi uporabljamo internet in drugo komunikacijsko opremo in prav nič se ne zgražamo, čeprav vemo, da smo prav tako pod nenehnim nadzorom različnih institucij; da ne govorimo o različnih socialnih omrežjih, kjer lahko posameznik vsak svoj korak, ki ga naredi, opiše in fotografira ter to tudi objavi. Paradoksalno se mi zdi, da imamo ljudje v različnih okoljih različne pravice in dolžnosti.

Na temo zasebnosti na delovnem mestu sta se v svetu uveljavila dva pristopa. Evropski pristop zaposlenega na delovnem mestu ne vidi samo kot delavca, pač pa tudi kot človeško bitje, ki ima kot tak človekove pravice. Drugi pristop je ameriški, ki zaposlenega vidi predvsem kot delojemalca, ki uporablja opremo v lasti delodajalca in zato službenih komunikacijskih sredstev ne sme uporabljati v zasebne namene (Kovačič, 2010).

Človekove pravice so najstarejše pravice, država pa jih ne more ne podeljevati ne pogojevati, kajti pripadajo človeku že zaradi dejstva, da je človek (Cvetko, 1999, str. 15). Pravna teorija označuje človekove pravice kot absolutne pravice, večkrat pa tudi kot univerzalne. Med človekove pravice spada tudi pravica do zasebnosti. Država je dolžna te pravice zavarovati.

V delovnem pravu je pravica do zasebnosti specifična pravica. Uveljavljanje pravic zasebnosti v delovnem razmerju se zaradi posebnosti delovnega razmerja nekoliko razlikuje, saj je le-ta zelo odvisna od delodajalčevega interesa. V Sloveniji je na ustavni ravni zasebnost dobro opredeljena ter tudi uspešno varovana, v delovnem pravu pa je pravica do zasebnosti slabše urejena. Očitno se tako delavci kot delodajalci ne zavedajo pomembnosti varovanja zasebnosti v delovnem pravu (Cvetko, 1999, str. 15–16).

5 NADZOR NA DELOVNEM MESTU

Na delovnem mestu ima vsak zaposleni pravico do zasebnosti. Zakonsko je urejeno, da mora delodajalec pisno seznaniti zaposlene, če se na delovnem mestu izvaja npr. videonadzor (ZVOP-1 74. člen). Videonadzor naj bi se nameščal na delovna mesta v izrednih primerih, če je to nujno potrebno za varstvo premoženja in oseb ali zaradi varovanja tajnih podatkov in poslovnih skrivnosti. Kamere nikakor ne smejo biti nameščene za nadzor storilnosti zaposlenih. Zakon za kršitve predvideva kazen od 4.000 do 13.000 evrov za pravne osebe in samostojne podjetnike ter od 1.000 do 2.000 evrov za odgovorne osebe (Nadzor nad zaposlenimi – podjetje korak v prednosti – da ali ne?, 2012).

Podjetja oziroma lastniki vedno bolj težijo k povečanju dobička, zaradi česar pa prihaja tudi do vse večjih pritiskov in posledično do nadziranja zaposlenih na delovnem mestu. Delodajalec neredko posega po takih ukrepih, ki so sicer zakoniti, z vidika morale in etike pa zelo sporni. Moje prepričanje je, da le zadovoljen delavec doprinese podjetju dodano vrednost. Pri nadzoru zaposlenih na delovnem mestu »trčita« dva pomembna interesa. Na eni

strani je interes delodajalca, ki stremi k čim večji učinkovitosti in storilnosti na delovnem mestu, na drugi strani pa interes zaposlenega, ki hoče čim večjo zasebnost. Interes zaposlenega je lahko tudi v tem, da je nagnjen k nedelu in uživanju in zaradi tega prihaja do velikih razhajanj med interesi delodajalca in interesi zaposlenega. Tehnologija v današnjem času omogoča delodajalcu popoln nadzor na delovnem mestu. Mnenja, koliko so ta dejanja sporna z vidika etike in morale, so različna.

Menim, da je elektronsko beleženje prihodov in odhodov na delovno mesto najbolj pogost in hkrati najmanj sporen način nadzora zaposlenih. V tem primeru so pravila igre oziroma predpisi znani. Bolj sporno se mi zdi nadziranje zaposlenih s kamerami oziroma tako imenovani videonadzor. Etično in moralno sporno je tudi nadziranje elektronske pošte zaposlenih. Elektronske komunikacije vnašajo nove pasti za delodajalce. Tako na primer nezadovoljen zaposleni lahko prek elektronske pošte pošilja zaupne podatke, strateške načrte in druge občutljive informacije osebam, ki lahko podjetju škodijo. Moje osebno mnenje je, da večanje nadzora na delovnem mestu ne pomeni tudi povečanja produktivnosti oziroma storilnosti delovnega mesta. Zna se zgoditi, da posameznik, ki je pod pretiranim nadzorom, dela slabše. Zaradi tega je zaposleni nenehno pod stresom, kar pa lahko pripelje do nesreč na delovnem mestu in posledično do bolniških odsotnosti. Moj predlog je, da bi bilo treba povečati zaupanje v odnosu med delodajalcem in zaposlenim. Nenehno nadziranje zaposlenih na delovnem mestu se mi zdi nesmiselno in nepotrebno. Delodajalec ima s tem tudi dodatne stroške. Če bi delodajalci bolj zaupali zaposlenim, bi bilo verjetno manj delovnih nesreč, manj bolniških odsotnosti in posledično manj stroškov. Motiviran zaposleni prinaša podjetju tudi višjo dodano vrednost, povečuje se tudi ugled podjetja. V očeh kupcev je podjetje, kjer so zaposleni tudi motivirani za delo, boljše oziroma ga višje vrednotijo.

Druga plat zgodbe pa je, da na delovnem mestu zaposleni potrebuje nadzor. Zaposlenim pomanjkanje nadzora preprečuje, da bi se uspešno spopadli s problemi, ki jih zaznavajo v delovnem okolju. Brez nadzora zaposleni ne morejo uresničevati svojih interesov z interesi podjetja. V primeru, ko zaposleni izgubi občutek, da njegovo početje ne prispeva k uspešnosti podjetja, izgubi voljo oziroma motivacijo (Maslach & Leiter, 2002, str. 11).

Rue in Byars (2004, str. 8) navajata pet značilnosti za uspešen nadzor na delovnem mestu. Tako naj bi bil uspešen nadzornik sposoben in pripravljen, da prenese razne spremembe na zaposlene, znal naj bi pravilno uporabiti moč oblasti, biti mora dober zgled za zaposlene, priznati mora spremenjeno vlogo v organizaciji ter imeti mora željo po novem delovnem mestu. Te značilnosti niso edine za uspešen nadzor na delovnem mestu, so pa med najpomembnejšimi.

5.1 Videonadzor na delovnem mestu

Informacijski pooblaščenec (Informacijski pooblaščenec, 2007a) ugotavlja, da se lahko videonadzor izvaja le v izjemnih primerih, ko je to nujno potrebno za varnost ljudi ali premoženja ali zaradi varovanja tajnih podatkov ter poslovnih skrivnosti. Videonadzor se

torej lahko izvaja le znotraj tistih prostorov, kjer je treba varovati prej navedene interese. Videonadzor je prepovedano izvajati v garderobah, sanitarijah in dvigalih.

74. člen ZVOP-1 določa, da mora oseba javnega ali zasebnega sektorja pred izvajanjem videonadzora objaviti obvestilo. Pred začetkom izvajanja videonadzora morajo biti zaposleni pisno obveščeni, delodajalec pa se mora pred samo izvedbo videonadzora posvetovati s sindikatom pri delodajalcu. Pisno obveščanje zaposlenih ter posvetovanja s sindikati pa niso potrebna na področju obrambe države, obveščevalno-varnostne službe ter na področju varovanja tajnih podatkov (Zakon o varstvu osebnih podatkov, Ur. l. RS, št. 94/2007).

5.2 GPS nadzor

Za sledenje službenih vozil se uporablja GPS tehnologija. Po mnenju informacijskega pooblaščenca (Informacijski pooblaščenec, 2010) je uporaba GPS nadzora za sledenje službenih vozil dopustna le v primeru, ko ni mogoče doseči istega namen z milejšimi ukrepi. Delodajalec je v primeru uvedbe GPS nadzora dolžan s sprejetjem notranjega akta zaposlene seznaniti s tem, da se v službenih vozilih za točno določen namen uporablja GPS tehnologija. Delodajalec je tudi dolžan zaposlene, ki uporabljajo službena vozila, seznaniti z načinom in delovanjem naprave, namenom namestitve naprave in za kakšne namene bodo podatki, ki so bili pridobljeni, tudi uporabljeni. Delodajalec mora v primeru, da se v službenih vozilih uporablja GPS tehnologija, poskrbeti za tehnični vidik zavarovanja zbirke osebnih podatkov, ki nastane na podlagi takšnega sledenja službenih vozil. Delodajalec je dolžan tudi pravno in tehnično urediti naslednja vprašanja: kdo ima dostop do zbirk podatkov, v kakšni obliki in koliko časa se podatki shranjujejo ipd.

5.3 Beleženje prihodov in odhodov z delovnega mesta

Beleženje prihodov in odhodov z delovnega mesta ne predstavlja nikakršnega posega v zasebnost zaposlenih oziroma služi predvsem za natančno beleženje prihodov oziroma odhodov zaposlenih z dela, trajanje odsotnosti z dela, koriščenje ur, dopustov ipd. Natančno beleženje v kombinaciji z odlično organizacijo dela pa lahko podjetju prinese večje prihranke, obenem pa tudi izboljša upravljanje s človeškimi viri (Registracija delovnega časa, 2015).

Ureditev vodenja evidenc o izrabi delovnega časa oziroma na področju evidenc beleženja prihodov in odhodov iz dela ureja Zakon o evidencah na področju dela in socialne varnosti (Ur. l. RS, št. 40/06; ZEPDSV). Evidenco beleženja prihodov in odhodov z dela vodijo delodajalci. Podatki, ki jih delodajalec dnevno beleži na področju registracije delovnega časa, so (Korošec, 2015):

- podatki o številu ur,
- skupno število opravljenih delovnih ur,
- nadurno delo,
- koriščenje dopusta,
- odsotnost z dela.

5.4 Nadzor nad elektronsko pošto in telefonom

S pomočjo elektronske pošte se je izjemno povečala komunikacija ljudi, tudi na delovnem mestu. Po nekaterih podatkih je leta 1996 v ZDA 42 % zaposlenih v velikih podjetjih uporabljalo elektronsko pošto za komuniciranje, danes pa lahko sklepamo, da se je število uporabnikov podvojilo (Drnovšek & Prodan, 2005 str. 139).

Pri zahtevi za pregledovanje elektronske pošte gre za navzkrižje interesov delodajalca, ki ima pravico, da nadzoruje, ali je službena oprema uporabljena skladno z namenom, za katerega je bila zaposlenemu predana v uporabo ter interesa zaposlenega, ki na delovnem mestu pričakuje določeno stopnjo zasebnosti. Delodajalec nima pravne podlage za vpogled v prometne podatke o elektronski pošti. Z vpogledom v te podatke je zaposlenemu kratena pravica do varstva osebnih podatkov, z vpogledom v vsebino pa je kratena tudi pravica do zasebnosti in pravica do tajnosti občil (Informacijski pooblaščenec 2007, str. 47).

Delodajalec lahko svojim zaposlenim blokira določene spletne strani, lahko pa se odloči za prost dostop do vseh internetnih strani. Delodajalci uporabljajo blokado neprimernih spletnih vsebin predvsem v primerih, ko gre za pornografske vsebine, za nakupovanje v spletnih trgovinah, dražbe, iskanje orožja, kockanje ali tistih spletnih strani, ki predstavljajo grožnjo okužbe z virusi (Kavran, 2004). Prisluskovanje telefonskim klicem in snemanje v Sloveniji ureja ZEKom. ZEKom v 5. odstavku 103. člena pravi, da so vse oblike nadzora ali prestrezanja, kot so poslušanje, prisluskovanje, snemanje, shranjevanje in posredovanje komunikacij prepovedane, razen če je to dovoljeno ali če je taka oblika nadzora ali prestrezanja potrebna za prenos sporočil (Zakon o elektronskih komunikacijah, 2004, 103. člen).

Sedmi odstavek istega člena pravi, da je dovoljeno snemanje komunikacij v okviru zakonite poslovne prakse z namenom, da se zagotovijo dokazi o tržni transakciji ali katerikoli drugi poslovni komunikaciji. Dovoljeno je tudi snemanje klicev v organizacijah, ki sprejemajo klice v sili (Zakon o elektronskih komunikacijah, 2004, 103. člen).

5.5 Testiranje s poligrafom

Številna podjetja so do leta 1989 uporabljala »detektor laži« za testiranje zaposlenih. To so bila predvsem podjetja v ZDA. Preverjali so predvsem kandidate za zaposlitev ter pri preiskavah tatvin v podjetjih oziroma na delovnih mestih. Številni raziskovalci in zdravstveno osebje so mnenja, da je uporaba poligrafa zelo sporna ter da lahko reagiranje posameznika zavaja oziroma pripelje do napačnih rezultatov in sklepov (Drnovšek & Prodan, 2005, str. 140).

5.6 Biometrija

Biometrija je veda »o načinih prepoznave ljudi na podlagi njihovih telesnih, fizioloških ter vedenjskih značilnostih, ki jih imajo vsi posamezniki, so edinstvene in stalne za vsakega

posameznika posebej in je možno z njimi določiti posameznika« (Informacijski pooblaščenec, 2007b).

Biometrija je en od načinov ugotavljanja oziroma preverjanja identitete, vendar je tudi najbolj učinkovit način, saj preverja tisto, kar oseba dejansko je. Največkrat se izvaja z uporabo prstnega odtisa, očesne mrežnice, šarenice, obraza, ušesa in DNK. Biometrične lastnosti posameznika se načeloma ne spreminjajo, se ne morejo izgubiti in skoraj nemogoče jih je posnemati ali reproducirati (Informacijski pooblaščenec, 2007b).

V slovenski zakonodaji je biometrija obravnavana v 78., 79., 80. in 81. členu ZVOP-1-a (Zakon o varstvu osebnih podatkov, 2007, 78.–81. člen). Zakon loči med preverjanjem identitete posameznika in med izvrševanjem identifikacije posameznika.

V omenjenem zakonu so biometrični ukrepi dovoljeni v javnem in zasebnem sektorju, in sicer v javnem sektorju le, če so določeni z zakonom in če so nujni za varnost ljudi ali premoženja ali za varovanje tajnih podatkov, za varovanje poslovnih skrivnosti in če jih ni možno doseči z milejšimi sredstvi. V zasebnem sektorju pa, če so nujno potrebni za opravljanje dejavnosti ali za varnost ljudi in premoženja ali za varovanje tajnih podatkov ali za varovanje poslovnih skrivnosti (Zakon o varstvu osebnih podatkov, 2007, 78.–81. člen). 80. člen tega zakona določa tudi, da lahko biometrične ukrepe delodajalec izvaja samo nad svojimi zaposlenimi, ki so bili o tem predhodno pisno obveščeni (Zakon o varstvu osebnih podatkov, 2007, 80. člen). Pred tem mora Informacijskemu pooblaščenecu tudi posredovati opis nameravanih ukrepov in vzroke za njihovo uvedbo. Informacijski pooblaščenec s svojo odločbo delodajalca obvesti o svoji odločitvi. Če se biometrične ukrepe izvaja brez dovoljenja Informacijskega pooblaščenca, gre v tem primeru za prekršek.

5.7 Detektivske agencije

Delodajalci vedno pogosteje najemajo zasebne detektivske agencije za nadzor zaposlenih v času bolniških odsotnosti. V takih primerih delodajalec preverja, če je njihov zaposleni res upravičen do bolniške odsotnosti ali pa v tem času počne kakšno drugo delo. Zasedil sem, da je delodajalec leta 2007 najel detektivsko agencijo, da bi nadzoroval tri zaposlene. Zasebni detektiv je vsem trem sledil ter jih fotografiral. Ugotovitve detektiva je delodajalec uporabil za izredno odpoved delovnega razmerja, vendar so vsi trije zaposleni na delovnem in socialnem sodišču dokazali, da so bile odpovedi nezakonite. Sodišče je v tem primeru menilo, da je delodajalec pri izrednih odpovedih uporabljal material detektiva, ker pa je bil pridobljen v nasprotju s takrat veljavno zakonodajo, je sodišče ugodilo delavcem. Okrajno sodišče v Kopru je v tem primeru presojalo o detektivovi kazenski odgovornosti. Zaradi neupravičenega slikovnega snemanja mu je sodišče prisodilo osem mesecev zapora, pogojno na dve leti. Koprsko okrajno sodišče je leta 2011 sporočilo, da je sodba še vedno na višjem sodišču (Detektiv nezakonito snemal osebe na bolniški, 2008).

Primer kaže, da je poseg v zasebnost zaposlenih, ko gre za slikovno snemanje, jasno začrtan. Detektiv lahko slikovno snema le na javnih krajih, javno dostopnih odprtih in zaprtih

prostorih ter krajih in prostorih, ki so vidni z javno dostopnega kraja in prostora. Detektiv lahko pridobi podatke tudi od zdravnika, ampak le glede bolniškega reda oziroma le to, koliko se sme bolnik gibati, kakšna rekreacija je bolniku dovoljena, ne sme pa poizvedovati o diagnozi in zdravilih bolnika. Zasebni detektivi so pri svojem delu omejeni s pravico posameznika do zasebnosti.

Zakon zasebnim detektivom dovoljuje, da preverjajo bolniški status tudi med tistimi, ki so zaposleni v javnem sektorju, vendar tam tovrstnega detektivskega nadzora skorajda ni. Javnega uslužbenca je treba z Zakonom o javnih uslužbencih obvestiti o tem, da ga bo delodajalec nadziral, zato je tak nadzor skoraj nesmiseln.

Delodajalec se takih praks največkrat poslužuje v primerih, ko je zaposleni večkrat v bolniškem staležu, ki se konča pred iztekom 30 dni. V takih primerih je nadomestilo plače zaposlenega breme delodajalca, po preteku 30 dnevnega roka pa je zaposleni v breme Zavoda za zdravstveno zavarovanje Slovenije (Repovž, 2015).

5.8 Vgrajevanje čipov

V Epicentru, enem od visoko tehnoloških razvitih švedskih podjetij, so približno 700 zaposlenim ponudili, da jim pod kožo vgradijo posebne čipe, ki bi nadomestili identifikacijske kartice. RFID čipi (angl. radio-frequency identification) so veliki kot riževo zrno in se vstavlja pod kožo na roki. Hannes Sjoblad, vodja projekta pravi, da je čipiranje delavcev prostovoljno, ampak tudi, da se brez čipa ne bo dalo vstopiti v objekt. S temi čipi je mogoče odpirati vrata, omogočajo dostop do fotokopirnega stroja, z njimi zaposleni lahko nakupujejo kavo in prigrizke v stavbi, pričakujejo pa tudi, da bodo čipi zamenjali gesla računalnikov (Pod kožo jim vgrajujejo čipe, 2015).

Čipi bi tako lahko v prihodnje postali pripomoček, s katerimi bi ljudje lahko plačevali hrano, menjali gesla in osebna gesla na službenih računalnikih. Mogoče jih je programirati, da komunicirajo z aplikacijami na pametnih telefonih (Pod kožo jim vgrajujejo čipe, 2015). V Ameriki naj bi imela čip vgrajena že ena od treh oseb. Barack Obama je v sklopu predloga zakona o zdravstveni zaščiti, znanem tudi kot Obamacare, napovedal za Američane tisto, kar je pred njim Ronald Reagan zavračal in zavrnil – obvezno čipiranje vsakega Američana. Predlog zakona o zdravstveni zaščiti je tako postal zakon, ki določa, da bo z letom 2017 čipiranje obvezno za vse Američane, vgrajevati pa jih bodo začeli že dojenčkom v porodnišnicah. Ta tehnologija bo tako nadomestila zdravstvene izkaznice, sam čip v človeškem telesu pa bo, prek čitalnika ali interneta, omogočal dostop do pacientovih zdravstvenih, medicinskih in identifikacijskih podatkov.

Potencial RFID čipa pa so zaznali tudi na Wall Streetu. Walmart in Procter & Gamble, dve največji ameriški družbi na področju proizvodnje in trgovine, sta v teh čipih razbrali konkurenčne prednosti za blagovne znamke in pridobivanja več informacij o potrošnikih. S pomočjo tega čipa zaposlenih v trgovinah praktično ne bi potrebovali več, vse delo bi opravil čip, ki bi ga obiskovalec oziroma kupec imel vgrajenega v sebi. Vstop v trgovino bi imel le

imetnik RFID čipa, tudi vsak izdelek na polici bi imel svoj čip. Po zaključku nakupa bi se ob izhodu natisnil račun, plačilo pa bi se avtomatsko izvedlo z računa kupca. V ZDA tudi že obstajajo določeni klubi za premožnejše sloje, v katere je vstop možen izključno z že vgrajenim mikročipom pod kožo (Pod kožo jim vgrajujejo čipe, 2015).

6 SODBE EVROPSKEGA SODIŠČA ZA ČLOVEKOVE PRAVICE V POVEZAVI Z NADZOROM NA DELOVNEM MESTU

Sodbe Evropskega sodišča za človekove pravice predstavljajo pomembne odločitve v zvezi z nadzorom na delovnem mestu. Sodobna tehnologija zaposlenim omogoča boljše ter hitreje opravljeno delo, na drugi strani pa delodajalcem z razmeroma majhnimi stroški omogoča popoln nadzor nad zaposlenimi. Delodajalce ne moti, če pozno v noč z zasebnega računalnika ali mobilnika zaposleni pošiljajo službene zadeve ali opravljajo službene naloge, ko pa zaposleni uporabljajo službene pripomočke v zasebne namene se slej ko prej zaposleni znajde v resnih težavah. Delodajalci pogosto uporabljajo videonadzor za zaščito svojih zaposlenih in premoženja, vendar se težko uprejo skušnjavi in nemalokrat opazujejo tudi zaposlene pri opravljanju vsakodnevnih službenih nalog. Čeprav obstajajo nekatere zakonske omejitve pri nadziranju zaposlenih, predstavlja neuporaba službenih pripomočkov v zasebne namene edino rešitev pred vdorom v zasebnost. Žal so delodajalci prepričani, da imajo pravico posegati v zasebnost zaposlenih, če le-ta uporabljajo službene pripomočke, ki so jim dani v uporabo. To pa ne glede na to, ali delovna sredstva uporabljajo v zasebne ali službene namene. Zaposleni imajo poleg temeljnih pravic tudi pravico do zasebnosti. Zaposlene ščiti zakon, ki pravi, da delodajalec lahko obdeluje samo osebne podatke, ki so potrebni in nujni za uresničevanje pravic in obveznosti v delovnem razmerju. Prav zato so še kako pomembne sodne odločitve, ki jih je Evropsko sodišče za človekove pravice prisodilo v korist tožnikom. Najpogosteje je težava v tem, da delodajalec zaposlene ne seznanja, kdaj in na kakšen način se izvaja nadzor nad njimi.

6.1 Primer Halford proti Združenemu kraljestvu

Alison Halford je bila namestnica načelnika merseysidske policije. Zaradi spolne diskriminacije je sprožila sodni postopek proti vladi Velike Britanije in proti svojim nadrejenim. Sodišče je odkrilo, da so njeni nadrejeni brez naloga prisluškovali telefonoma v njeni pisarni (Sodbe Evropskega sodišča za človekove pravice opr. št. 20605/92). Telefona sta bila del notranje telefonske mreže na merseysidski policiji, en od njiju je bil namenjen zasebnim klicem. Telekomunikacijski sistem je bil ločen od javne telefonske mreže. Alison Halford ni imela nobenih omejitev glede uporabe telefonov. Nadrejeni ji je dal izrecno dovolilo, da se o sodnem postopku pogovarja tudi med službenim časom. Na tak način so Halfordovi prisluškovali brez sodnega naloga ter pridobili informacije, ki so jih kasneje uporabili v sodnem postopku. Do tedaj je Velika Britanija kot nezakonito prepovedovala le prisluškovanje na javnih telekomunikacijskih mrežah, kar pa ni veljalo za notranje, interne komunikacijske mreže. V sodnem postopku je vlada menila, da Alison Halford ni mogla

pričakovati zasebnost teh klicev, saj naj bi delodajalec imel možnost nadzorovati klice brez vnaprejšnjega opozorila.

Leta 1997 je Evropsko sodišče za človekove pravice bilo mnenja, da je prišlo do kršitve 8. člena Evropske konvencije o človekovih pravicah. Halffordove ni nihče opozoril, da so njeni klici nadzorovani in zato je lahko razumno pričakovala zasebnost teh klicev.

6.2 Primer Copland proti Združenemu kraljestvu

Z Evropskega sodišča za človekove pravice leta 2007 izhaja še en primer posega v zasebnost na delovnem mestu, in sicer primer Copland proti Združenemu kraljestvu (opr. št. 62617/00). Primer Copland proti Združenemu kraljestvu temelji na pritožbi Lynette Copland, osebne asistentke predstojnika kolidža Carmarthenshire v Združenem kraljestvu. Asistentka Lynette Copland je trdila, da je namestnik predstojnika nadzoroval njene telefonske pogovore in njeno elektronsko pošto, da bi odkril, če je neprimerno uporabljala sredstva kolidža v zasebne namene. V zadevi Copland proti Združenemu kraljestvu je bilo to, da delavka ni bila vnaprej opozorjena, kdaj in v kakšnih primerih lahko delodajalec nadzira elektronsko pošto, ključni element sodbe (Sodbe Evropskega sodišča za človekove pravice, opr. št. 62617/00).

6.3 Primer I proti Finski

Evropsko sodišče za človekove pravice je tudi v primeru I proti Finski razsodilo v prid tožnici. Med letoma 1989 in 1994 je neimenovana oseba bila za določen čas zaposlena kot medicinska sestra v javni bolnišnici. V isti javni ustanovi, kjer je bila medicinska sestra zaposlena, so ji leta 1987 postavili diagnozo, da je HIV pozitivna. Primer se ukvarja s pritožničnimi navedbami, da je na podlagi posamičnih pripomb sodelavcev, ki so kazale na to, da so seznanjeni z njenim zdravstvenim stanjem, na začetku leta 1992 posumila, da so sodelavci nezakonito vpogledovali v njene zaupne zdravstvene podatke. Kasneje je medicinska sestra sume zaupala zdravniku, ta pa je poskrbel, da je do njene kartoteke imelo dostop le osebje na oddelku za infekcijske bolezni. Medicinski sestri so nato spremenili podatke ter ji dodelili novo številko zdravstvenega zavarovanja. Ko je tožnici prenehala veljati pogodba o zaposlitvi, ji le-te niso več podaljšali. Leta 1996 se je pritožila okrožni zdravstveni oblasti in jo pozvala, naj razišče, kdo je imel dostop do njenih podatkov. Okrožna zdravstvena oblast ni mogla ugotoviti, kdo je imel dostop do njenih zdravstvenih podatkov ter obenem ni zagotovila zadostnih varovalk proti nepooblaščenemu dostopu do zdravstvenih podatkov. Tožbo je vložila na podlagi 8. člena (pravica do spoštovanja osebnega življenja), na prvi odstavek 6. člena (pravica do poštene obravnave) in na 13. člen (pravica do učinkovitega pravnega sredstva). Evropsko sodišče za človekove pravice je ugotovilo, da je šlo nedvomno za kršitev 8. člena konvencije, ker ji zdravstvena oblast ni zavarovala osebnih zdravstvenih podatkov. Tožnici so prisodili odškodnino v višini 5.771,80 evrov za gmotno škodo, 8.000,00 € za nematerialno škodo in 20.000,00 € za stroške in izdatke (Sodbe Evropskega sodišča za človekove pravice, opr. št. 20511/03).

6.4 Primer Bogdana Barbulescuja

Romunski inženir Bogdan Barbulescu je bil leta 2007 odpuščen, potem ko so v njegovem podjetju ugotovili, da je v službi uporabljal Yahoo Messenger tudi za zasebni spletni klepet z bratom in zaročenko. Romunski inženir se je na Evropsko sodišče za človekove pravice obrnil potem, ko so proti njemu razsodili na romunskih sodiščih. Inženirjev bivši delodajalec je namreč zaposlenim prepovedal uporabo spletnih klepetalnic v zasebne namene. Evropsko sodišče za človekove pravice v Strasbourgu je presodilo, da so romunska sodišča ravnala pravilno. Evropsko sodišče je argument inženirja Barbulescuja zavrnilo, češ da gre za kršenje pravic do zaupnosti komunikacije. Sodišče je poudarilo, da »ni nerazumno, da delodajalec želi, da zaposleni med službenim časom opravljajo svoje službene naloge«. Obenem so dodali, da je podjetje podatke o pogovorih zaseglo v prepričanju, da gre za službeno komunikacijo. Evropsko sodišče za človekove pravice v Strasbourgu je presojalo le, ali je Romunija »v okviru svojih pozitivnih obveznosti po 8. členu EKČP ustrezno ravnala v sodnih postopkih pred delovnimi sodišči«. Dejanj delodajalca Evropsko sodišče ni presojalo (Delodajalec ima pravico brati vaša zasebna sporočila, 2016).

Informacijska pooblaščenka Mojca Prelesnik je opozorila, »da iz sodbe nikakor ne izhaja splošna pravica delodajalcev do nadzora zasebne spletne komunikacije zaposlenih in je vsakršno tovrstno posploševanje neprimerno«. Po mnenju Prelesnikove je sodišče »zamudilo odlično priložnost za razvoj prakse na področju pričakovane zasebnosti pri rabi službenih komunikacijskih sredstev«. Informacijska pooblaščenka dodaja, da »nikakor namreč ne gre prezreti, da so v Sloveniji pogoji za poseg v komunikacijsko zasebnost strožji že zaradi določb 37. člena ustave« (Prelesnik, 2016).

7 MOBING

Beseda **mobing** izhaja iz angleškega glagola *to mob*, kar pomeni napasti, lotiti se nekoga. Izraz mobing je skoval avstrijski etnolog Konrad Lorenz (Leyman v Brečko, 2014, str. 19). Do zanimivih ugotovitev je prišel pri opazovanju živali, kako preženejo vsiljivca ter kako pri tem živali sodelujejo. Lorenz je torej označeval z besedo mobing napad skupine živali na vsiljivca. Leta 1995 je delovni psiholog Heinz Leyman opazoval enak pojav na delovnem mestu. Leyman je prvi opredelil pojav: »Mobing v delovnem okolju vključuje sovražno in neetično komunikacijo enega ali več posameznikov, sistematično in najpogosteje usmerjeno k enemu posamezniku, ki je zaradi mobinga potisnjen v nemogoč položaj, kjer nima zaščite in tudi ostaja zaradi stalnih dejanj mobinga. Ta dejanja so pogosta, najmanj enkrat na teden in v daljšem časovnem obdobju, najmanj šestih mesecev. Zaradi pogostosti in trajanja sovražnega vedenja mobing vodi v duševne, psihosomatske in socialne težave.«

Munc (2010) v literaturi mobing označuje kot zelo razširjen pojav v slovenskih zasebnih podjetjih ter različnih organizacijah, tako vladnih kot nevladnih organizacijah. Avtor si je mnenje izoblikoval na podlagi različnih razgovorov v času sindikalnega udejstvovanja ter

kasneje, ko so v svetovalnico prihajali različni klienti s podobno problematiko. Pridobljeni vtisi kažejo tudi na to, da vodilni podrejene dojemajo kot lastnino, ki ima status potrošnega materiala. Omenjeno ponižujoče ravnanje do sodelavcev pripelje do katastrofalnih medsebojnih odnosov na delovnem mestu ter posledično tudi do slabših delovnih rezultatov. Stranska produkta mobinga sta absentizem in fluktuacija (Munc, 2010, str. 385–386).

Preprečevanje mobinga je vključeno v ZDR-1 (Uradni list, Ur. l. RS, št. 21/2013, z dne 13. 3. 2013). V tem zakonu najbolj izstopa 7. člen ZDR-1.

7. člen

(prepoved spolnega in drugega nadlegovanja ter trpinčenja na delovnem mestu)

Prepovedano je spolno in drugo nadlegovanje. Spolno nadlegovanje je kakršna koli oblika neželenega verbalnega, neverbalnega ali fizičnega ravnanja ali vedenja spolne narave z učinkom ali namenom prizadeti dostojanstvo osebe, zlasti kadar gre za ustvarjanje zastraševalnega, sovražnega, ponižujočega, sramotilnega ali žaljivega okolja. Nadlegovanje je vsako neželeno vedenje, povezano s katero koli osebno okoliščino, z učinkom ali namenom prizadeti dostojanstvo osebe ali ustvariti zastraševalno, sovražno, ponižujoče, sramotilno ali žaljivo okolje.

Spolno in drugo nadlegovanje iz prejšnjega odstavka se šteje za diskriminacijo po določbah tega zakona.

Odklonitev ravnanj iz prvega odstavka tega člena s strani prizadetega kandidata oziroma delavca ne sme biti razlog za diskriminacijo pri zaposlovanju in delu.

Prepovedano je trpinčenje na delovnem mestu. Trpinčenje na delovnem mestu je vsako ponavljajoče se ali sistematično, graje vredno ali očitno negativno in žaljivo ravnanje ali vedenje, usmerjeno proti posameznim delavcem na delovnem mestu ali v zvezi z delom.

Delavec, ki je žrtev trpinčenja, ne sme biti izpostavljen neugodnim posledicam zaradi ukrepanja, ki ima za cilj uveljavitev prepovedi trpinčenja na delovnem mestu (Zakon o delovnih razmerjih, 2013, 7. člen)

Mobing lahko označujemo kot posebno obliko šikane ter ga obravnavamo kot čustveno nasilje na delovnem mestu. Čustveno nasilje se lahko izrazi tako s psihičnim kot fizičnim posegom.

Leyman (v Brečko, 2014, str. 20) opredeljuje mobing kot konfliktov polno komunikacijo na delovnem mestu med sodelavci ali med podrejenimi in nadrejenimi, pri katerem je oseba v podrejenem položaju in sistematično izpostavljena dlje trajajočim napadom ene ali več oseb.

Vzroki za pojav mobinga so lahko različni ter jih ne moremo natančno opredeliti. Obstaja pa nekaj temeljnih vzrokov za pojav mobinga, ki so povezani z (Confidenti v Vidmar, 2013, str. 355):

- splošno etično klimo organizacije,
- osebnostnimi lastnostmi posameznika,
- nerazumevanjem med sodelavci,
- nesoglasji med zaposlenimi in vodstvom,
- krivičnim sistemom napredovanja,
- metodami vodenja in upravljanja s človeškimi viri.

Trpinčenje na delovnem se največkrat začne tako, da posameznik ali skupina sodelavcev začne zlorabljeni svojo moč nad zaposlenim. Oseba, izpostavljena zlorabi moči, lahko najde ustrezen način obrambe ter onemogoči zlorabo. V nasprotnem primeru, ko se oseba ne zna braniti in ostane pasivna, se zloraba moči razvije v trpinčenje (Povše-Pesrl in drugi v Vidmar, 2013, str. 358).

Pogosto so posledice mobinga zelo hude. Nasilje ne prizadene le žrtve, temveč tudi povzročitelje, delovno okolje in družino (Vidmar, 2013, str. 358). Na ta način se zmanjšajo volja do dela, delovna klima in medsebojni odnosi. Stres na delovnem mestu se povečuje, ljudje so manj ustvarjalni in produktivni ter se slabše počutijo. Raziskave so pokazale več psihičnih, fizičnih in psihosomatskih obolenj, kot so stres, depresija, slaba samopodoba, samoobtoževanje, različne fobije, motnje spanja ter tudi nagnjenost k samomoru. Žrtev mobinga se pogosto začne drugače vesti, lahko se zapre vase ali pa celo postane agresivna do sebe in drugih. Velikokrat žrtev mobinga postane pasivna, pogosto pije alkohol in kadi ali jemlje zdravila. Pogosto ima žrtev mobinga oslabilen imunski sistem, posledica tega je dojemljivost za različne bolezni. Literatura navaja tudi druge posledice mobinga, kot so: socialna osamitev, finančne težave in težave v družini. Finančne težave nastanejo predvsem zaradi odsotnosti z dela ali odpoved. Organizacije posledice mobinga občutijo predvsem v obliki večjega števila bolniške odsotnosti, večje fluktuacije delavcev ali manjšo učinkovitost na delovnem.

8 POSLEDICE NADZORA NA DELOVNEM MESTU

Kaj se lahko zgodi, če delodajalec preveč zagreto nadzira delojemalca? V očeh delodajalca je nadzor smiseln, češ delojemalec se boji za delovno mesto in bo svoje delo opravljal zelo zavzeto. Osebno menim, da pretiran nadzor pripelje do pomanjkanja motivacije, zavzetosti za delo ter manj kreativnosti. Na določeni točki se zaposleni ne poistoveti več s podjetjem, kar pa pripelje ravno do nasprotnega učinka, ki ga je delodajalec pričakoval oziroma do kontraproduktivnosti. Posledice pretiranega nadzora na delovnem mestu so mobing, prezentizem, absentizem in fluktuacija. Vse naštetu povzroča podjetju dodatne in nesmiselne stroške. Zakaj bi delodajalec pretirano nadziral zaposlene? Ali ni zaupanje v sodelavce ključno za uspešno in učinkovito poslovanje podjetja? Ali pretiran nadzor ne povzroča dodatnih stroškov podjetju? Šikaniranje na delovnem mestu vodi tudi do dodatnega stresa ter morebitnih kasnejših zdravstvenih težav zaposlenih. Prevelika pojavnost stresa povzroča težave in je vzrok številnih bolezni. Večina vzrokov stresa izvira ravno iz delovnega okolja. Zakaj se stres pojavi v delovnem okolju? Najpogosteje zaradi delovnih obremenitev,

prekomernega dela, slabe organizacije, klime ter organizacijske strukture in medsebojnih odnosov v organizaciji. Do česa lahko pripelje mobing na delovnem mestu? Podjetje s šikaniranjem na delovnem mestu povzroči začaran krog nezadovoljstva med zaposlenimi in nepotrebna trenja, kar pa privede do podobnih dogodkov, kot jih povzroči pretiran nadzor. Dogodek oziroma posledica mobinga je tudi absentizem.

8.1 Absentizem

Beseda **absentizem** izhaja iz latinske besede *absens*, ki pomeni odsotnost ali izostanek (Friedl, 1990, str. 134). Gre za pomanjkanje fizične prisotnosti na delu, ko zanjo obstajajo socialna pričakovanja. Nastanek absentizma nastane kot posledica širokega spektra dejavnikov. Med te dejavnike lahko uvrstimo bolezni, slabe navade, pomanjkanje motivacije, maksimizacije koristnosti zaposlenih, organizacijske kulture podjetja, navade delavcev ipd. (Božič, 2011, str. 20). Glavni vzrok za absentizem je največkrat bolezenska odsotnost. Pojav absentizma vpliva na ceno produkta in konkurenčno sposobnost podjetja na trgu prek več dejavnikov, npr. izguba trga, plačilo nadur za delavce, ki nadomeščajo odsotne, izplačila nadomestil pri bolniškem staležu, plačilo za začasno zaposlene, večji organizacijski napor ter večji stroški, slabša kakovost produktov in manjša produktivnost.

Absentizem negativno vpliva tudi na posameznika in ostale zaposlene (Božič, 2011, str. 21). Posameznik, ki je večkrat odsoten z dela, se mora sprijazniti z nižjo plačo, manjšimi možnostmi napredovanja in težavami pri povratku na delo. Odsotnost posameznika močno vpliva tudi na ostale sodelavce, ki so ga primorani nadomeščati ter so zato izpostavljeni večjim pritiskom na samem delovnem mestu, kar pa pripelje do trenj znotraj podjetja.

Izraz absentizem pomeni kakršnokoli odsotnost z delovnega mesta. Absentizem je v bistvu strokovni izraz za bolniško odsotnost (angl. *absense*) ter ga definiramo kot odsotnost z delovnega mesta (ZSSS, 2012, str. 8). Ko postanejo delovne obremenitve na delovnem mestu nevzdržne ali iz kakšnih drugih razlogov, se zaposleni pogosto odzovejo z umikom iz delovne situacije. Za večino podjetij bolniške odsotnosti predstavljajo velik problem. Izostanek z delovnega mesta vodi do nižje delovne uspešnosti, do motenj v delovnem procesu ter do povečanja delovnih obremenitev za zaposlene, ki ostajajo prisotni na delovnem mestu. Izostanki kažejo na to, da so zaposleni pod prekomernim stresom ter izčrpani in nimajo možnosti, da bi se primerno spočili od delovnih obremenitev. Pojav absentizma povzroča precejšno škodo družbi, organizacijam in ne nazadnje zaposlenim.

Statistični podatki kažejo na to, da v Sloveniji evidentiramo letno 10 do 11 milijonov izgubljenih delovni dni (desetletno povprečje). Podatek pomeni, da izostane iz dela zaradi bolezni in poškodb približno 38.500–39.000 ljudi dnevno. Po podatkih ZZZS se obseg in trajanje bolniških odsotnosti vztrajno povečujeta (ZSSS, 2012, str. 10). Z ekonomskega vidika imajo zaradi pojava absentizma škodo družba zdravstvene zavarovalnice ter delovne organizacije kot plačniki odsotnosti. Ker mora delodajalec zaposlenemu na bolniškemu staležu plačati nadomestilo ter nadure delavcem, ki delajo namesto odsotnih, to vpliva na ceno

izdelka ter na konkurenčno sposobnost na trgu. Vse naštetu močno vpliva na večje organizacijske napore in stroške podjetja. Posledice absentizma privedejo do nižje produktivnosti, nižja je kakovost produkta ter potencialna izguba trga. Absentizem negativno vpliva tudi na zaposlene, ki so zaradi bolezni ali poškodb odsotni z dela. Med negativne posledice lahko prištejemo konflikte s sodelavci in nadrejenimi, slabše plačilo za svoje delo ter manjša možnost napredovanj.

Zakon o varnosti in zdravju pri delu zavezuje državne organe, delodajalce, sindikate in zaposlene k zagotavljanju varnega dela in k skrbi za zdravje zaposlenih (ZSSS, 2012, str. 11). To pomeni, da je odgovornost tako na strani delodajalcev, ki morajo skrbeti za varno delovno okolje in osveščanje ter izobraževanje delavcev za bolj varno delo, kakor tudi na strani zaposlenih samih.

Delodajalci imajo možnost izbire med številnimi ukrepi za zmanjšanje pojava absentizma, ki pa morajo biti izbrani premišljeno ter ustrezno izvedeni. Praksa kaže na to, da se delodajalcu finančno vlaganje v preventivne ukrepe za obvladovanje absentizma povrne v doglednem času. Nižja stopnja absentizma zagotavlja tudi nižje stroške dela ter številne druge pozitivne učinke, kot so večja pripadnost podjetju, večje zadovoljstvo zaposlenih, večja motiviranost ter večja produktivnost zaposlenih (ZSSS, 2012, str. 8–11).

V splošnem lahko govorimo, da so vzroki za zdravstveni absentizem povezani z dejavniki delovnega okolja, dejavniki zunanjega okolja ter dejavniki, ki so povezani s posameznikom in njegove značilnosti ter njegovo gensko zasnovo. Raziskave kažejo, da je prav delovno okolje tisto, ki zaznamuje zdravje zaposlene populacije. Tudi ostale raziskave razkrivajo, da so dejavniki, povezani s psihosocialno dimenzijo delovnega okolja, »krivi« za večjo odsotnost z dela. Tu uvrščamo na primer delovne pogoje, sodelavce itd. Gre za dejavnike, ki oblikujejo posameznikove občutke in vplivajo na počutje ter zadovoljstvo na delovnem mestu (Stare et al., 2012, str. 21–23).

Finančna ter gospodarska kriza je državo in delodajalce spodbudila k še večji zainteresiranosti, da bi omejili oziroma znižali stroške, povezane z delovnim procesom. Absentizem oziroma stanje, ko so zaposleni odsotni z dela, povzroča pomembne stroške. Prav zaradi teh stroškov delodajalci ter država namenjajo vedno več pozornosti. Večja angažiranost deležnikov oziroma določeni ukrepi pomembno vplivajo na zmanjšanje odsotnosti z dela in posledično zmanjšanje stroškov, ki pri tem pojavu nastanejo. Zaposleni so lahko odsotni z dela iz več razlogov. To so na primer letni dopust, lastne zdravstvene težave, nega članov družine, izobraževanje itd. To kaže, da je absentizem večdimenzionalen segment, ki terja korektno in natančno obravnavo. Organizacije oziroma podjetja, ki želijo zmanjšati pojav absentizma, bi morala več storiti na področju zaupanja v njihove zaposlene. Žal se dogaja, da podjetja izberejo napačne ukrepe za zmanjšanje tega pojava. Največkrat posegajo v zasebnost zaposlenih pod krinko, da gre za njihovo varnost. Zaposleni na drugi strani pretiran nadzor na delovnem mestu vidijo kot pomanjkanje zaupanja v njih in njihovo delo. To pripelje do večjega stresa na delovnem mestu ter posledično tudi do kasnejših zdravstvenih težav.

Zdravstvene težave zaposlenih pomenijo večje stroške za podjetje zaradi bolniških odsotnosti. Primerno bi bilo, da bi podjetja vlagala v boljšo delovno klimo, kjer bi se zaposleni bolje počutili ter se s podjetjem poistovetili. Seveda bi to pripeljalo tudi do boljših poslovnih rezultatov podjetja. Obenem se mi poraja vprašanje, kako bo zaposleni zaupal delodajalcu, če pa delodajalec zaposlenemu ne zaupa.

8.2 Prezentizem

Zaposleni zaradi vseh trenj, ki jih doživlja na delovnem mestu, lahko zbolijo, kar pa povzroči podjetju stroške zaradi bolniških odsotnosti. Zakaj torej podjetje povzroča trenja na delovnem mestu, če pa ima zaradi tega nepotrebne stroške? Zakaj nekateri delodajalci zagovarjajo teorijo, kjer naj bi bili zaposleni med seboj skregani? Odgovor na to vprašanje ni enostaven in enoznačen. Žal sem taka trenja tudi sam občutil. Menim, da bi morala podjetja vzpostaviti prijazna delovna okolja, kjer bi se zaposleni dobro počutili in bi na delovna mesta prihajali z vso vnemo in motivacijo ter zadovoljstvom. Na tak način podjetje pride do konkurenčne prednosti. Kako lahko nezadovoljni zaposleni zagotavljajo dodano vrednost podjetja, če pa se s podjetjem ne poistovetijo? Seveda se s podjetjem niti ne morejo poistovetiti, če pa jih delodajalec šikanira oziroma ustvarja napete odnose med sodelavci. Ko se zaposleni boji za delovno mesto oziroma se boji za izgubo službe in je prisoten na delovnem mestu kljub temu, da ima zdravstvene težave, prihaja do nastanka prezentizma.

Prezentizem je vedenje, ko zaposleni prihajajo na delovna mesta kljub bolezni (Božič, 2012a, str. 23–26). Ker zaposleni prihajajo na delovna mesta z obolenji in niso popolnoma zdravi, lahko nalezejo svoje sodelavce ter zaradi bolezni ne morejo opravljati svojega dela stoodstotno oziroma dovolj učinkovito. Zelo pogosto se dogaja, da se zaposleni ne zaveda, da je takšno vedenje problematično ter ima škodljive učinke tako na delavca kot na podjetje. Med ljudmi prevladuje prepričanje, da je dober delavec tisti, ki ne zahaja v bolniški stalež. Problematično je tudi to, da podjetja spodbujajo takšno vedenje na račun zmanjševanja absentizma, namreč ponekod podjetja nagrajujejo zaposlene, ki v določenem časovnem obdobju niso bili v bolniškem staležu. Nekatere študije ugotavljajo, da je prezentizem posledica strahu delavca, da mu v delovnem okolju ne bodo verjeli, da je res bolan. Zato se tak zaposleni kljub bolezni odpravi v službo, da bodo v podjetju videli, da je zares bolan. Zaposleni, ki je bolan ali psihično obremenjen s problemi v zasebnem življenju, je bistveno manj sposoben in učinkovit na delu, posledice so pa vidne v podaljšanem času, ki ga porabimo za določeno delo, slabši kakovosti opravljenega dela, posledično se dogajajo tudi napake v delovnem procesu. Zaradi pojava prezentizma ima zaposleni tudi težave s koncentracijo, pozornostjo, slabim počutjem ter pomanjkanjem energije, zmanjša se sposobnost organiziranja dela. Prezentizem ima lahko za posledico poslabšanje zdravstvenega stanja, dolgotrajnejše okrevanje, širjenje bolezni med sodelavci, na dolgi rok pa povečanje bolniških odsotnosti zaposlenih, kar dolgoročno negativno vpliva na zdravje zaposlenih.

Zaposleni prihajajo na delo kljub bolezni zaradi več razlogov. Med te razloge lahko uvrstimo pridnost, lojalnost, občutek odgovornosti in nenadomestljivosti ali pa zaradi drugih razlogov,

kot je na primer pritisk nadrejenih (Božič, 2012b, str. 23–26). Študije kažejo, da je prezentizem bolj pogost med neproizvodnimi delavci ter zlasti med visoko strokovnim in izvršnim kadrom. Izrazito veliko prezentizma je v dejavnosti nege, v zdravstvu ter šolstvu. Pogosto je prezentizem prisoten med osebami z majhnimi otroki, slabo plačanimi delavci, to pa zaradi tega, ker si zaradi znižanja prihodkov ne morejo privoščiti bolniškega staleža. Pojav prezentizma je pogost tudi med delavci s kroničnimi boleznimi ali slabšim zdravstvenim stanjem. Stopnja prezentizma je večja med delavci, ki so zaposleni za določen čas. Ko so delovna mesta ogrožena, se stopnja prezentizma zvišuje, kajti zaposleni si skuša zmanjšati možnost izgube službe.

Razlogi, zakaj zaposleni kljub bolezni prihajajo na delovna mesta (Božič, 2012b, str. 23–26):

- občutek, da si ne more dovoliti dneva izostanka,
- strah pred izgubo zaposlitve,
- ker ne želi obremeniti sodelavcev,
- ob prihodu na delo ga čaka kup nerešenih zadev,
- zaposleni nima sodelavca, ki bi ga nadomestil oziroma prevzel njegove naloge.

Raziskave tudi kažejo na to, da je med osebami, ki so označeni kot deloholiki ter med osebami, ki gradijo lastno vrednost na dosežkih, visoka verjetnost prezentizma.

Ta pojav se je v zadnjih letih, ko je gospodarska rast negativna oziroma šibka ter je visoka brezposelnost, precej povečal. Žal dolgoročno pojav prezentizma na delovnem mestu privede do bolniških odsotnosti in drugih bolezni. Podjetja ta pojav tudi sama povečujejo tako, da nagrajujejo tiste zaposlene, ki ne gredo v tekočem letu skoraj nič na bolovanje oziroma niso skoraj nikoli na bolniški odsotnosti. In ponovno se podjetje znajde v začaranem krogu. Če zaposleni sprva vztraja na delovnem mestu kljub bolezni in delodajalec to dejanje finančno motivira na račun neizostankov z dela, pride do kasnejših in resnejših bolezenskih stanj, kar pa privede do absentizma. V takih primerih ima podjetje dvojne stroške. Delodajalci bi se morali vprašati, če je to smiselno in koristno za podjetja. Smiselno bi bilo, če bi podjetja zmanjšala delovne obremenitve na delu, stroške, ki nastanejo zaradi absentizma in prezentizma pa vlagala v zdravje in motiviranost zaposlenih. Na ta način bi na dolgi rok pozitivno vplivala na zaposlene ter posledično na izdatke podjetja zaradi bolniških odsotnosti.

8.3 Fluktuacija

Nenazadnje se podjetjem dogaja tudi to, da imajo težave s fluktuacijo. Kljub temu da je pozitivna fluktuacija za delodajalca zaželena, pride tudi do negativne fluktuacije, ki pa za delodajalca oziroma podjetje ni ravno dobrodošla. Seveda je razumljivo, da bo sposoben kader tudi poiskal sposobnega in spodobnega delodajalca, ki zna in hoče ustvariti pozitivno klimo v podjetju, ki je ključnega pomena za uspešno in učinkovito poslovanje podjetja. Tista podjetja, ki gradijo na medsebojnemu zaupanju in zagotavljajo dobro klimo na delovnem mestu, imajo veliko več možnosti, da ostanejo uspešna tudi v prihodnosti.

Slovar slovenskega knjižnega jezika definira fluktuacijo kot naraščanje in upadanje nečesa na določenem področju ter tudi kot pojav menjave zaposlitve (SSKJ, 2015). Beseda **fluktuacija** izvira iz besede *fluctuare* in je latinskega izvora, kar pa v prevodu pomeni valovanje. Fluktuacijo na splošno opredeljujemo kot odhajanje kadrov iz podjetja. Različni avtorji pojav fluktuacije definirajo na različne načine oziroma številčne dejavnike, oblike, vrste ter različne učinke na podjetja. Odhod kadrov vpliva na dinamiko procesov v podjetju. Za razvoj podjetja je spoznanje vrednosti ter pomen zadovoljnega zaposlenega ključnega pomena. Božič opredeljuje fluktuacijo kot normalen pojav oziroma proces, ki je potreben za vzdrževanje kadrovskega ravnovesja (Božič, 2012b, str. 15).

Pomemben dejavnik uspešnosti organizacije je v veliki meri odvisen od zmožnosti, da podjetje zadrži najboljše sodelavce ter da nadomesti slabše sodelavce z boljšimi. Podjetje, ki noče imeti težav z množičnim odhodom zaposlenih oziroma s fluktuacijo, mora predvsem zagotavljati dobro vzdušje na delovnem mestu, dobre delovne pogoje ter tudi ustrezno nagraditi sodelavce. Z odhodom najboljših sodelavcev lahko pripelje tudi do konca uspešne zgodbe podjetja. Na drugi strani pa se lahko zgodi tudi taka sprememba, ki bo dala nov zagon oziroma nov elan tistim, ki ostanejo v podjetju ter dobijo novo priložnost. Skratka fluktuacija je lahko v podjetju tudi zaželena. V času krize je fluktuacija dobila novo dimenzijo, in sicer zato, ker je fluktuacija bolj obvladljiva ter pogosteje zaželena (Stare et al., 2012, str. 57).

SKLEP

Zasebnost je človekova pravica, zagotovljena z ustavo. V današnjem času poostrelega nadzora in prevlade varnosti nad svobodo, ko je človek tako rekoč nadzorovan že skoraj na vsakem koraku, se je mogoče smiselno vprašati, ali se je vredno odpovedati svobodi za lažen občutek varnosti. In v tem primeru čigave varnosti – varnosti vseh ljudi ali varnosti tistih, ki ta nadzor uporabljajo?

Načini nadziranja so postali z leti vse bolj dostopni in nadzirani oziroma opazovani osebi skoraj nevidni. Zaposleni so v nekaterih primerih nadzirani s strani delodajalca ves čas delavnika, kar pa po navadi predstavlja več kot tretjino dela dneva. Le malo je takih delodajalcev, ki pomislijo tudi na to, kako (pretiran) nadzor vpliva na njihove zaposlene. Od vseh vrst nadziranja sta kartica za beleženje prihodov in odhodov z delovnega mesta in blokada nekaterih spletnih strani še najmanj invazivna. Najbolj zaskrbljujoča pa se mi zdita uporaba videokamer na vsakem koraku in biometrija. Zelo zaskrbljujoče pa je tudi razvijanje čipiranja ljudi. Delodajalci po teh načinih posegajo zaradi višanja stopnje varnosti, vendar bi se varnost lahko vzdrževalo tudi na drugačne, manj invazivne načine. Zakonodaja ščiti zasebnost in temeljne človekove pravice pred posegi delodajalcev, vendar ta področja ne ureja samo en zakon. V kolikor bi imeli en krovni zakon, ki bi ga ob razvoju novih tehnologij lahko po potrebi dopolnjevali in razširjali, bi bilo to področje mogoče bolje urejeno in bolj transparentno. Tehnologija je samo orodje, od nas posameznikov je odvisno, ali jo bomo uporabili v varovalne namene ali bomo pustili, da se jo izrablja za vedno večji nadzor posameznikov. S tem lahko potrdim svojo hipotezo, navedeno v uvodu.

Nadzor je na delovnem mestu potreben, vendar pa pretiran nadzor ne dosega pozitivnih učinkov, prej nasprotno. Med delodajalcem in zaposlenim je treba ustvarjati čim boljše sodelovanje, v podjetju se je treba truditi za dobro organizacijsko klimo, dobre medsebojne odnose in graditi na medsebojnem zaupanju. Posledice pretiranega nadzora na delovnem mestu so mobing, prezentizem, absentizem in fluktuacija. Dobro motiviran in zadovoljen zaposleni prinese podjetju dodano vrednost in konkurenčno prednost pred ostalimi podjetji.

LITERATURA IN VIRI

1. Božič J. (2011). *Psihosocialna tveganja na delovnih mestih: Izbor primerov dobre prakse v domačih in tujih podjetjih*. Ljubljana: Univerzitetni rehabilitacijski inštitut Republike Slovenije – Soča.
2. Božič J. (2012a). *Psihosocialna tveganja na delovnih mestih: gradivo za strokovne delavce v malih in srednje velikih podjetjih*. Ljubljana: Univerzitetni rehabilitacijski inštitut Republike Slovenije – Soča.
3. Božič J. (2012b). *Kako do boljšega počutja na delovnem mestu*. Ljubljana: Univerzitetni rehabilitacijski inštitut Republike Slovenije – Soča.
4. Brečko, D. (2014). *Recite mobingu ne. Preprečevanje psihičnega in čustvenega nasilja*. Ljubljana: Planet GV.
5. Cvetko, A. (1999). *Varovanje zasebnosti v delovnih razmerjih*. Ljubljana: Gospodarski vestnik.
6. Čipiranje ljudi – v ZDA obvezno, v EU dovoljeno. Najdeno 26. marca 2016 na spletnem naslovu <http://markom.watoc.org/2015/02/23/cipiranje-ljudi-v-zda-obvezno-v-eu-dovoljeno/>
7. *Delavec v zlati kletki zasebnosti ali delodajalec kot pravice ječar?* Najdeno 7. junija 2015 na spletnem naslovu <http://www.razgledi.net/2009/01/23/delavec-v-zlati-kletki-zasebnosti-ali-delodajalec-kot-pravice-jecar/>
8. *Delodajalec ima pravico brati vaša zasebna sporočila*. Najdeno 13. januarja 2015 na spletnem naslovu <http://www.rtv slo.si/evropska-unija/delodajalec-ima-pravico-brati-vasa-zasebna-sporocila/383314>
9. *Detektiv nezakonito snemal osebe na bolniški*. Najdeno 18. marca 2016 na spletnem naslovu <http://www.24ur.com/novice/slovenija/izolski-detektiv-osumljen-kaznivih-dejanj.html>
10. Drnovšek, M., & Prodan, I. (2005). *Poslovno okolje*. (Zapiski predavanj). Ljubljana: Ekonomska fakulteta v Ljubljani.
11. Društvo za vrednotenje dela, organizacijski in kadrovski razvoj. (2004). *Motivacija, kompetence in plače zaposlenih: zbornik referatov*. Kranj: Društvo za vrednotenje dela, organizacijski in kadrovski razvoj.
12. Friedl, A. (1990). *Absentizem: nastavek raziskave* (str. 333-343). Antropos.
13. Friedman, M. (2011). *Kapitalizem in svoboda*. Ljubljana: Soleco.
14. Havliček, M. (2012). *E-pošta in zasebnost na delovnem mestu*. Najdeno 10. januarja 2016 na spletnem naslovu <http://eudace.eu/knjiznica/clanki/2013021410315019/>

15. *Varstvo osebnih podatkov*. Najdeno 20. marca 2016 na spletnem naslovu https://www.ip-rs.si/vop/sledenje-sluzbenih-vozil-z-gps-1868/?tx_jzvopdecisions_pi1%5BhighlightWord%5D=gps%20tehnologija
16. Informacijski pooblaščenec, 2007a. *Letno poročilo Informacijskega pooblaščenca 2007*. Najdeno 15. marca 2016 na spletnem naslovu <https://www.ip-rs.si/o-pooblascencu/informacije-javnega-znacaja/letna-porocila/>
17. Informacijski pooblaščenec, 2007b. *Biometrija*. Najdeno 15. marca 2016 na spletnem naslovu <https://www.ip-rs.si/o-pooblascencu/informacije-javnega-znacaja/letna-porocila/>
18. Jaklič, M. (2005). *Poslovno okolje podjetja*. Ljubljana: Ekonomska fakulteta.
19. Kavran, D. (2004). Nadzor zaposlenih ali merjenje učinkovitosti. Najdeno 27. marca 2016 na spletnem naslovu http://www.finance.si/81648/Nadzor_zaposlenih_ali_merjenje_u%8inkovitosti?cctest&&cookie_time=1460446155
20. Kazenski zakonik. *Uradni list RS*, št. 55/08, 138. člen.
21. *Ko šef postane veliki brat*. Najdeno 3. junija 2015 na spletnem naslovu <http://www.zurnal24.si/ko-sef-postane-veliki-brat-clanek-212273>
22. Kocmur, M. (2006). *Pravica do zasebnosti bolnika in zdravnika – pogled zdravnika*. Ljubljana: Zdravniški vestnik.
23. *Komunikacijska zasebnost na delovnem mestu*. Najdeno 3. junija 2015 na spletnem naslovu <https://pravokator.si/index.php/2010/09/22/komunikacijska-zasebnost-na-delovnem-mestu/>
24. Korošec, B. (2015). Zaposleni morajo prevzeti odgovornost za svoj delovni čas. Najdeno 15. januarja 2016 na spletnem naslovu <http://registracijadelovnegacasablog.spica.si/2015/01/zaposleni-morajo-prevzeti-odgovornost.html#more>
25. Kovačič, M. (2006). *Nadzor in zasebnost v informacijski družbi*. Ljubljana: Fakulteta za družbene vede.
26. Kovačič, M. (2010). *Komunikacijska zasebnost na delovnem mestu*. Najdeno 20. novembra 2015 na spletnem naslovu <https://pravokator.si/index.php/2010/09/22/komunikacijska-zasebnost-na-delovnem-mestu/>
27. Kuhelj, A. (2004). *Varstvo pravice do zasebnosti, veroizpovedi in svobodnega izražanja v pravo Sveta Evrope*. Ljubljana: Fakulteta za upravo.
28. Maslach, C., & P. Leiter, M. (2002). *Resnica o izgorevanju na delovnem mestu*. Ljubljana: Educy

29. Munc, M. (2010). *Nemoč nasilja*. Maribor: De Vesta.
30. *Nadzor nad zaposlenimi – podjetje korak v prednosti – da ali ne?* Najdeno 3. junija 2015 na spletnem naslovu <http://delodajalci.mojedelo.com/novica/nadzor-nad-zaposlenimi-podjetje-korak-v-prednosti-da-ali-ne/d-2611>
31. *Nov zakon o elektronskih komunikacijah*. Najdeno 15. decembra 2015 na spletnem naslovu <http://data.si/blog/2013/01/15/nov-zakon-o-elektronskih-komunikacijah/>
32. *Obvladovanje psihosocialnih tveganj na delovnih mestih*. Najdeno 12. novembra na spletnem naslovu http://www.ir-rs.si/f/docs/Razvojni_projekti/Obvladovanje_psihosocialnih_tveganj_na_delovnih_mestih.pdf?irrs_admin=rasqkug2haca5b89m4kg1b1qi4
33. *Pod kožo jim vgrajujejo čipe*. Najdeno 26. marca 2016 na spletnem naslovu <http://www.slovenskenovice.si/novice/tehnovice/video-pod-kozo-jim-vgrajujejo-cipe>
34. Prelesnik, M. (2016). ESČP zamudilo odlično priložnost za razvoj prakse na področju pričakovane zasebnosti pri rabi službenih komunikacijskih sredstev. Najdeno na spletnem naslovu 15. januarja 2016 na spletnem naslovu <https://www.ip-rs.si/novice/escp-zamudilo-odlicno-priloznost-za-razvoj-prakse-na-podrocju-pricakovane-zasebnosti-pri-rabi-sluzbenih-komunikacijskih-sredste-1348/>
35. *Primer MMZ iz evropske perspektive*. Najdeno 5. junija 2015 na spletnem naslovu <http://www.razgledi.net/2008/03/03/primer-mzz-iz-evropske-perspektive/>
36. *Registracija delovnega časa*. Najdeno 16. januarja 2016 na spletnem naslovu <http://jantar.si/sl/resitve.html>
37. Repovž, E. (2015). Detektivi opravijo okrog 15 kontrol bolniških mesečno. Najdeno 16. 3. 2016 na spletnem naslovu <http://www.times.si/gospodarstvo/detektivi-opravijo-okrog-15-kontrol-bolniskih-mesecno--da3937fd5e1d16528d8fb6d5f50cfb7d3c7f0bff.html>
38. Rue, Leslie W., & Byars, Lloyd L. (2004). *Supervisor: key link to productivity*. New York: The McGraw- Hill/Irwin.
39. *Fluktuacija*. Najdeno 20. novembra 2015 na spletnem naslovu <http://bos.zrc-sazu.si/cgi/neva.exe?name=ssbsj&tch=14&expression=zs%3D15785>
40. *So zaposleni res na bolniški?*. Najdeno 26. marca 2016 na spletnem naslovu <http://www.times.si/gospodarstvo/gospodarstvo-z-vodjo-detektivske-agencije-o-nadzoru-delavcev--d750285e7a3a9e0d9be3d2706d6751e5f5484a1e.html>
41. *Sodbe Evropskega sodišča za človekove pravice opr. št. 20605/92*. Najdeno 16. januarja 2016 na spletnem naslovu <https://www.ip-rs.si/varstvo-osebni-podatkov/iskalnik-podlocbah-in-mnenjih/sodbe-mednarodnih-sodisc/povzetki-sodb/>

42. *Sodbe Evropskega sodišča za človekove pravice opr. št. 62617/00*. Najdeno 16. januarja 2016 na spletnem naslovu <https://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-podlocbah-in-mnenjih/sodbe-mednarodnih-sodisc/povzetki-sodb/>
43. *Sodbe Evropskega sodišča za človekove pravice, opr. št. 20511/03*. Najdeno 16. januarja 2016 na spletnem naslovu <https://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-podlocbah-in-mnenjih/sodbe-mednarodnih-sodisc/povzetki-sodb/>
44. Stare, J. (2012). *Izzivi in priložnosti zdravega delovnega okolja*. Ljubljana: Fakulteta za upravo.
45. Stare, J., Boštjančič E., Buzeti, J., Klun, M., Kozjek, T., & Tomažević, T. (2012). *Boljše delovno okolje za boljše sodelovanje*. Ljubljana: Fakulteta za upravo.
46. Inštitut za razvoj in inovacije. (2012). *Strokovna informativna skripta za delojemalce s področja obvladovanja stresa, absentizma, prezentizma, fluktuacije, izgorevanja ter usklajevanja poklicnega in družinskega življenja*. Ljubljana: Zveza svobodnih sindikatov Slovenije.
47. Tuschudin, V. (2004). *Etika v zdravstveni negi: razmerja skrbi*. Ljubljana: Educy.
48. Ustava RS. *Uradni list* 33/1991.
49. Vidmar, U. (2013). *Integriteta*. Ljubljana: Amalietti&Amalietti.
50. Zakon o delovnih razmerjih - ZDR-1. *Uradni list* RS, št. 21/2013.
51. *Zakon o elektronskih komunikacijah ZEKOM-1*. Najdeno 12. decembra 2015 na spletnem naslovu <http://www.saop.si/poslovne-informacije/novice/nova-zakonodaja/zakon-o-elektronskih-komunikacijah-zekom-1/>
52. Zakon o varstvu osebnih podatkov. *Uradni list* RS, št. 94/2007.
53. Zakon o elektronskih komunikacijah. *Uradni list* RS, št. 43/2004.
54. Zakon o elektronskih komunikacijah. *Uradni list* RS, št. 109/12.