UNIVERZA NA PRIMORSKEM
FAKULTETA ZA MANAGEMENT

DIPLOMSKA NALOGA

VIKTORIJA ARSOVSKA

KOPER, 2016

2016
DIPLOMSKA NALOGA
VIKTORIJA ARSOVSKA

UNIVERZA NA PRIMORSKEM
FAKULTETA ZA MANAGEMENT

Diplomska naloga

NADZOR ZAPOSLENIH IN ZASEBNOST NA DELOVNEM MESTU

Viktorija Arsovska

Koper, 2016

Mentor: izr. prof. dr. Viktorija Florjančič

POVZETEK

Razvoj informacijsko-komunikacijske tehnologije omogoča različne oblike nadzora nad lastnino delodajalca, sočasno pa odpira vprašanja o pravici do zasebnosti zaposlenih na delovnem mestu. Tako v diplomski nalogi obravnavamo načine in oblike nadzora dela na delovnem mestu ter stopnje zasebnosti. V teoretičnem delu naloge predstavljamo teoretične podlage nadzora dela na delovnem mestu, zakonska dovoljenja o nadzoru dela na delovnem mestu ter zakonske podlage o pravicah do zasebnosti na delovnem mestu. V nadaljevanju predstavljamo najpogostejše oblike nadzora na delovnem mestu. V empiričnem delu naloge predstavljamo rezultate raziskave, ki smo jo izvedli s pomočjo dveh spletnih anketnih vprašalnikov. Izpolnjevanje spletnih vprašalnikov je potekalo preko spletnega orodja 1KA. Z raziskavo je bilo ugotovljeno, da obstajajo razlike pri nadzoru dela na delovnem mestu med redno zaposlenimi in študenti.

Ključne besede: informacijsko-komunikacijska tehnologija, nadzor, zasebnost, zaposleni, študenti, načini nadzora.

SUMMARY

The development of information and communication technologies allows for various forms of control over the employer's property and consequently raises questions about the employee's right to privacy in the workplace. Therefore, the thesis discusses methods and forms of labor control in the workplace and the level of privacy. The theoretical part of the thesis presents a theoretical basis for supervising the work at the workplace, law regulations regarding labor supervision in the workplace, and the legal basis of the right to privacy in the workplace. The following chapter discusses the most common forms of supervision in the workplace. The empirical part of the thesis presents the results of the research, which was conducted using two online questionnaires on the survey tool 1ka.si. The research findings show that there are differences in the labor control in the workplace between regular employees and students.

Keywords: Information and communication technology, supervision, privacy, staff, students, methods of supervision.

UDK: 004.7:342.721(043.2)

VSEBINA

SLIKE

PREGLEDNICE

KRAJŠAVE

GPS	Global positioning system
IKT	Informacijsko komunikacijska tehnologija
IP naslov	Internet protocol
RS	Republika Slovenija
UP FM	Univezra na Primorskem, Fakulteta za management
Ur. l. RS	Uradni list Republike Slovenije
ZDR-1	Zakon o delovnih razmerjih
ZEKom-1	Zakon o elektronskih komunikacijah
ZEPDSV	Zakon o evidencah na področju dela in socialne varnosti
ZInfP	Zakon o informacijskem pooblaščencu
ZPLD-1-UPB4	Zakon o potnih listinah
ZVOP-1	Zakon o varstvu osebnih podatkov

1 UVOD

V tem poglavju smo opredelili problem in teoretična izhodišča pri diplomski nalogi. Nato smo zapisali namen in cilje ter predvidene metode, ki smo jih uporabili pri doseganju ciljev. Na koncu poglavja smo opredelili predpostavke in omejitve, pri pisanju diplomske naloge.

1.1 Opredelitev problema in teoretičnih izhodišč

Po Šprahu (2009) je zasebnost temeljna človekova pravica, s katero sta povezani človekova individualnost in svoboda.

Zasebnost posameznika na delovnem mestu je v Sloveniji določena z Ustavo RS. V 37. členu Ustave RS (Uradni list RS, št. 33/91-I, 42/97, 66/2000, 24/03 in 69/04) je zapisano: »Samo zakon lahko predpiše, da se na podlagi odločbe sodišča za določen čas ne upoštevata varstvo tajnosti pisem in drugih občil in nedotakljivost človekove zasebnosti, če je to nujno za uvedbo, ali potek kazenskega postopka ali za varnost države.«

Pojem zasebnosti različni slovarji različno opredeljujejo. V angleškem slovarju Oxford (2013) je zasebnost posameznika na splošno opredeljena kot stanje samote oziroma kot stanje brez navzočnosti javnosti. Slovar slovenskega knjižnega jezika (SSKJ 2005) pa zasebnost opredeljuje kot: »značilnost zasebnega: zasebnost premoženja / zasebnost izpovedi« in/ali kot »zasebno življenje, delovanje«. Slovenski informacijski slovar (Slovensko društvo Informatika 2013) zasebnost predstavlja kot lastnost, s katero je zagotovljen nadzor nad zbiranjem, razširjanjem in uporabno osebnih podatkov.

Kokemuller (2013) nadzor na delovnem mestu opredeljuje kot dejavnost, s katero vodja nadzira dejavnosti in odgovornosti delavcev, ki so v njegovi delovni skupini. Nadzor na delovnem mestu predstavlja pomembno delovno nalogo za vse vodje, in sicer na vseh ravneh vodenja. Vodja, ki izvaja nadzor na delovnem mestu, prevzame tudi odgovornost za razvoj, izobraževanje in usposabljanje zaposlenih (prav tam).

V današnji tehnološko razviti družbi obstaja veliko načinov in pripomočkov, s katerimi lahko delodajalci nadzorujejo delo svojih zaposlenih. Pri tem se postavlja vprašanje, ali delodajalci s tem ne posegajo v zasebnost zaposlenih. Na tem področju bi poudarili težavo neobveščenosti delavcev o nadzoru na delovnem mestu. Veliko delodajalcev seznanitvi zaposlenih o izvajanem nadzoru ne pripisuje velikega pomena, saj nadzor nad zaposlenimi jemljejo kot svojo dolžnost.

Delodajalci menijo, da je nadzor delavcev upravičen, saj so delavci za svoje delo plačani, delodajalci pa so lastniki opreme, s katero delavci opravljajo delo. Zato delavci v službi naj ne bi izkoriščali časa za svoje osebne interese, kot so osebni klici in, obiskovanje spletnih strani,

ki niso potrebni za delo ipd. V tem primeru pride do položaja, ko se izključujeta dve pravici, in sicer pravica delodajalca do varovanja lastnine (Ustava Republike Slovenije 67. člen, v Mišič 2013) in pravica delavca do zasebnosti, ki je prav tako opredeljena v Ustavi Republike Slovenije (Ustava Republike Slovenije od 35. člena dalje, v Mišič 2013). Vendar pa velja, da delodajalci nimajo pravice do nadzora delavcev, niti do prisluškovanja njihovim telefonskim pogovorom, če delodajalci ob začetku delovnega razmerja izrecno ne izrazijo, da so osebni klici v delovnem času prepovedani. Na spletni strani Informacijskega pooblaščenca (2012) je zapisano, da: »pridobitev izpiska klicev izhaja iz lastninske pravice delodajalca. A v trenutku, ko bi delodajalec začel ugotavljati, komu klicane številke pripadajo, to pomeni obdelavo osebnih podatkov. To je torej meja, do katere delodajalec obdeluje izpisek klicev«. Zato Informacijski pooblaščenec (2012) priporoča, da se pravila telefoniranja določijo že ob sklenitvi delovnega razmerja in s pisnim soglasjem posameznika.

Sodobna tehnologija omogoča še druge načine nadzora delavcev na delovnem mestu. Delodajalci najpogosteje preverjajo, katere spletne strani delavci med delovnim časom obiskujejo. Če delavec nameni veliko časa pregledovanju spletnih strani z neustrezno vsebino, ga delodajalec lahko obtoži neučinkovitosti na delovnem mestu. Vendar mora biti delavec o takšnem načinu nadzora predhodno obveščen. Delodajalci pogosto preverjajo e-pošto zaposlenih, če sumijo, da izkoriščajo službeno e-pošto za osebne namene in pišejo neprimerne vsebine, kot so pritožbe glede nadrejenih ipd. V 37. členu Ustave RS je jasno opredeljeno: »Zagotovljena je tajnost pisem in drugih občil. Samo zakon lahko predpiše, da se na podlagi odločbe sodišča za določen čas ne upoštevata varstvo tajnosti pisem in drugih občil in nedotakljivost človekove zasebnosti, če je to nujno za uvedbo, ali postopek kazenskega postopka ali za varnost države.«

Med nadzor na delovnem mestu spada tudi video nadzor zaposlenih. Taka oblika nadzora je na določenih delovnih mestih nujno potrebna za varnost delavcev in za varovanje delovne opreme. Vendar mora delodajalec tudi glede takega načina nadzora delavca obvestiti, slednji pa mora podpisati pisno soglasje, da se z video nadzorom strinja. Zakon o varstvu osebnih podatkov (ZVOP-1, Ur. l. RS, št. 86-3836/2004, 113-5005/20005, 4. odst. 77. člena) določa: »da morajo biti zaposleni pred začetkom izvajanja video nadzora po tem členu vnaprej pisno obveščeni o njegovem izvajanju.« Delodajalec nima pravice do pritožbe nad delavcem, da zanemarja svoje delo, če to opazi preko video nadzora, o katerem delavec predhodno ni bil obveščen. Video nadzor je kot oblika nadzora delavcev ena izmed najpogostejših načinov nadzora, zato je opredeljena tudi v Zakonu o varstvu osebnih podatkov (ZVOP-1) in v Zakonu o informacijskem pooblaščencu (ZInfP, Ur. l. RS. št. 113/2005, 001-22-132/05).

1.2 Namen in cilji diplomskega dela

Problem nadzora zaposlenih na delovnem mestu nas zanima iz lastnih delovnih izkušenj, saj se je avtorica naloge pri opravljanju različnega študentskega dela srečevala z različnimi

oblikami nadzora dela. V nekaterih primerih so bili zaposleni o tem obveščeni, v drugih pa ne. Zato nas zanima, ali so delodajalci s tem kršili pravico zaposlenih do zasebnosti. Zanima nas tudi, ali delodajalci delajo razlike pri nadzoru redno zaposlenih in zaposlenih, ki delo opravljajo preko študentske napotnice (študenti).

V nalogi zato želimo:
- opredeliti osnovne pojme s področja zasebnosti zaposlenih,
- pregledati zakonodajo, ki opredeljuje možnosti in omejitve za izvajanje nadzora zaposlenih na delovnem mestu,
- raziskati in predstaviti različne načine nadzora na delovnem mestu,
- predstaviti možnosti uporabe informacijske tehnologije za nadzor delavcev,
- raziskati in ugotoviti, ali delodajalci delajo razlike pri nadzoru, redno in začasno zaposlenih (npr. študenti),
- ugotoviti, ali delodajalci obveščajo delavce o nadzoru na delovnem mestu,
- ugotoviti, ali delodajalci spoštujejo zasebnost delavcev na delovnem mestu.

Z raziskavo, ki smo jo opravili med podjetji, ki zaposlujejo tudi študente in med študenti, ki so opravljali ali opravljajo študentsko delo, smo preverjali naslednje hipoteze:
- delodajalci pri nadzoru dela redno zaposlenih delavcev in študentov posegajo po različnih metodah,
- več kot tretjina anketiranih podjetij krši pravice o zasebnosti zaposlenih,
- več kot tretjina anketiranih podjetij delavce ne obvešča o nadzoru in delavcem ne da v podpis soglasje o nadzoru pri delu,
- učinkovitost delavcev pod nadzorom je slabša, ker so pod pritiskom.

Čeprav je bilo na to temo napisano že precej vsebin, smo tematiko raziskali in na podlagi ugotovitev raziskave predstavili današnje stanje v podjetjih na področju zasebnosti zaposlenih na delovnem mestu in o načinih nadzora zaposlenih na delovnem mestu.

1.3 Predvidene metode za doseganje ciljev

Diplomsko delo je razdeljeno na teoretični in empirični del. Teoretični del je bil napisan na podlagi preučene domače in tuje literature. S pomočjo literature smo določili tiste opredelitve o zasebnosti in nadzoru delavcev na delovnem mestu, ki so v današnjem času najbolj problematične. Pri tem smo porabili deskriptivno in primerjalno metodo.

Pri empiričnem delu naloge smo uporabili elektronski anketni vprašalnik, ki je vseboval vprašanja o nadzoru delavcev na delovnem mestu, načinih nadzora, s katerimi sredstvi delodajalci delavce nadzorujejo, načinom obveščanja delavcev in o spoštovanju zasebnosti delavcev. K anketiranju smo povabili podjetja in študente, ki med svojim prostim časom opravljajo različna študentska dela, ter na ta način zajeli mnenja delodajalcev in zaposlenih.

Vprašalnike smo posredovali na 60 naslovov izbranih podjetij. Izpolnjevala so jih podjetja različnih panog iz Obalno-kraške pokrajine. Prejeli smo 35 polno izpolnjenih vprašalnikov. Zbrane podatke smo obdelali s pomočjo MS Excela in uporabili metode opisne statistke. Rezultate ankete prikazujemo tabelarično, grafično in opisno.

V empiričnem delu naloge smo vključili tudi študente Fakultete za management, ki občasno opravljajo določena dela. V anketnem vprašalniku smo jih povprašali o tem, ali so se med delom srečali s kakšnimi težavami, kako so jih delodajalci nadzorovali, kakšne so bile sankcije ipd. Prejeli smo 72 polno izpolnjenih vprašalnikov.

Anketiranje podjetij in študentov je bilo anonimno.

1.4 Predpostavke in omejitve diplomskega dela

Predpostavljali smo, da delodajalci izvajajo nadzor delavcev na delovnem mestu in o tem ne obveščajo svojih zaposlenih.

Pri tistih delodajalcih, ki izvajajo nadzor na delovnem mestu, smo predpostavljali, da to izvajajo korektno in ne posegajo v zasebnost delavcev, kot bi bilo na primer nameščanje kamer za video nadzor v garderobah in toaletnih prostorih.

Omejitev pri izvajanju empiričnega dela naloge je bila neiskrenost delodajalcev pri izpolnjevanju vprašalnikov. Predvidevamo, da se niso hoteli negativno izpostavljati in posledično vprašalnikov niso izpolnjevali z resničnimi podatki.

Pri empiričnem delu raziskave smo se omejili na podjetja Obalno-kraške pokrajine.

2 ZASEBNOST

Današnja moderna družba dojema zasebnost kot ideal, za katerega se moramo boriti, saj nam omogoča dostojno življenje (Bien Karlovšek idr. 2008, 17-18). Zasebnost je za posameznika tudi vrednota, ki ga ščiti, mu zagotavlja samospoštovanje in pomaga pri oblikovanju lastne identitete. Zagotavljanje zasebnosti mora biti prosto kakršnekoli psihične in fizične prisile.

Cvetko (1999, 16) navaja, da bi pravica do zasebnosti vsakega posameznika morala biti tista pravica, ki bi kot pravica do osebnega življenja posamezniku omogočila razvoj osebnosti, ki si jo sam poljubno določi in jo varuje pred zlorabami.

Na delovnih mestih se vedno pogosteje e vse večji nadzor, ki odpira vprašanje o morebitnem kršenju pravic do zasebnosti. Da bi ugotovili, ali delodajalec krši našo pravico do zasebnosti, moramo poznati pravne pogoje, pod katerimi lahko delodajalec izvaja nadzor na delovnem mestu in načine, s katerimi ga lahko izvaja, ne da bi kršil pravice do zasebnosti zaposlenih.

Šprah (2009) svetuje, da bi se delodajalci, ki izvajajo nadzor nad zaposlenimi na delovnem mestu, morali zavedati, da je zasebnost ena izmed temeljnih človekovih pravic in da predstavlja človekovo individualnost in svobodo.

2.1 Splošno o zasebnosti

Pojem zasebnost je zelo obsežen in obširen pojem, ki obsega veliko opredelitev številnih avtorjev iz različnih strokovnih področij.

Zasebnost predstavlja temelj človekovega dostojanstva pravi Kovačič (2006, 46) in jo opredeljuje kot temeljno pravico, iz katere izhajajo vse ostale pravice v sodobni družbi.

Pravica do zasebnosti se povezuje z nekaj drugimi pravicami in sicer s pravico (Cate 1997, 21 v Kovačič 2006, 39):

- do zasebnega življenja,
- nadzorovati dostop in uporabo informacij o sebi,
- zmanjšati nadlegovanje na najmanjšo možno mero,
- pričakovati zaupnost,
- do uživanja osamljenosti in intimnosti, ter
- pravico do tajnosti idr.

Če razumemo vsebino vsake posamezne navedene pravice, lahko zasebnost opredelimo kot pravico, ki obsega vsebine vseh zgoraj navedenih pravic. Zato za varovanje naše zasebnosti ne sme biti kršena nobena od zgoraj navedenih pravic.

Pravica do zasebnosti je naša temeljna pravica, ki jo ščiti tudi mednarodna zakonodaja. Eden izmed zelo pomembnih in uveljavljenih mednarodnih aktov je Splošna deklaracija človekovih pravic, ki jo je 10. 12. 1948, sprejela Generalna skupščina združenih narodov. V njej je o zasebnosti zapisano (v Kovačič 2006, 73):

> Nikogar se ne sme nadlegovati s samovoljnim vmešavanjem v njegovo zasebno življenje, v njegovo družino, v njegovo stanovanje ali njegovo dopisovanje in tudi ne z napadi na njegovo čast in ugled. Vsakdo ima pravico do zakonskega varstva pred takšnim vmešavanjem ali takšnimi napadi.

Navedena opredelitev zasebnosti ne obsega vseh omejitev, ki bi jih sodobna družba morala spoštovati, med njimi tudi delodajalci.

Čebulj (1992, 7 v Kovačič 2003, 34) navaja tri sestavine zasebnosti:

- *zasebnost v prostoru*: predstavlja pravico oziroma možnost posameznika, da je sam, ko si to želi in ko to potrebuje;
- *zasebnost osebnosti:* opredeljuje svobodo misli, svobodo izražanja, svobodo političnih in verskih opredelitev;
- *informacijska zasebnost*: daje posamezniku možnost, da zadrži podatke in informacije o sebi, ker jih ne želi posredovati drugim in ne želi, da bi bili drugi seznanjeni z njimi.

Cvetko (1999, 61) pa našteva sestavine pravice do zasebnosti posameznika. Ta vključuje njegove osebne podatke, osebne razmere, osebno stanje, njegove dejavnosti in videz.

S pojavom interneta in razvojem svetovnega spleta se je problem zasebnosti še povečal. Zasebnost najbolj ogrožajo (Kovačič 2006, 29):

- *Globalizacija*, ki odstranjujejo geografske omejitve pri prenosu blaga in storitev, pa tudi pri pretoku podatkov,
- *Konvergenca med tehnologijami*: tehnologije postajajo vedno bolj povezane in med seboj operabilne,
- *Večpredstavnost*: ki omogoča, da se podatki predstavijo na različne načine in v različnih oblikah.

2.2 Zasebnost na delovnem mestu

Zasebnost želimo zavarovati v zasebnem življenju in tudi na delovnem mestu. Na delovnem mestu je zaradi izvajanja nadzora dela včasih težko ohraniti ustrezno raven zasebnosti.

Cvetko (1999, 25) pravi, da mora biti pravica delavca do zasebnosti varovana na enak način kot vse druge pravice, ki izhajajo iz delovnega razmerja. V nadaljevanju dodaja, da je v razviti družbi varovanje pravice do zasebnosti vrednota, za katero si moramo prizadevati. Da ne bi prihajalo do kršenja teh vrednot, je varstvo zasebnosti potrebno opredelit v delovnih razmerjih. Za to skrbijo zakoni in interni akti podjetij. Posledice kršitve pravice do zasebnosti

so za posameznika največkrat zelo hude, saj posegajo v človekove najgloblje občutke in ravnanje.

Zasebnost delavca na delovnem mestu je lahko kršena na različne načine. To je možno z nedovoljenim in nepravilnim nadzorom na delovnem mestu ali pa s posredovanjem podatkov o delavcu tretjim osebam. Zasebnost delavca na delovnem mestu je največkrat kršena z nadzorom, o katerem delavec ni obveščen. Če je delavčeva pravica do zasebnost na delovnem mestu kršena, se delavec počuti ogroženo, kar posledično vpliva na njegove zmožnosti pri opravljanju delovnega procesa.

Za lažje razumevanje zasebnosti bi se delodajalci morali vživeti v vlogo zaposlenega in razmisliti o nevarnostih, povezanih s kršenjem pravice do zasebnosti kot tudi o posledicah, ki so s tem povezane. Delodajalec se mora zavedati, da je v podjetju tudi sam in opravlja delovne naloge, zaradi česar je, če podatki niso ustrezno varovani, tudi sam izpostavljen istim nevarnostim. To je še dodaten razlog, da mora delodajalec poskrbeti za ustrezno zaščito osebnih podatkov in za zaščito zasebnosti.

Tehnološki razvoj je prisoten tudi na delovnih mestih. Na novo razvita IKT predstavlja grožnjo zasebnosti, ker omogoča nove in neznane posege v le-to. Po drugi strani pa je koristna, saj ima veliko prednosti v samem delovnem procesu. Delodajalci jo uporabljajo, da bi z njeno pomočjo pripomogli k boljšemu in kakovostnejšemu izkoriščanju delovne zmožnosti delavca ter k povečanju njegove storilnosti in produktivnosti. IKT delodajalcem pomaga pri varovanju lastnine in prispeva k boljši kakovosti dela, vendar ogroža zasebnost delavcev (Bien Karlovšek idr. 2008, 19). Če se delavci odrekajo zasebnosti na delovnem mestu, jih to vodi k pomanjkanju občutka svobode in k občutku nenehnega nadzora. Posledično pride tudi do upadanja kakovosti opravljanja dela, pomanjkanja ustvarjalnosti, motiviranosti za delo in občutka avtonomije.

Na delovno-pravnem področju se najpogosteje navaja stališče (Bien Karlovšek idr. 2008, 13): »Za številne anglosaške in francoske avtorje je pravica do zasebnega življenja pravica do zasebnosti, pravica do življenja, kakor si ga posameznik želi, zaščita pred publiciteto. ... Do neke stopnje se ta pravica nanaša tudi na pravico do vzpostavljanja in razvijanja razmerij z drugimi človeškimi bitji, predvsem na čustvenem področju za razvoj in izpolnitev posameznikove osebnosti.«

V Slovenski zakonodaji ne obstaja zakon, ki bi jasno urejal zasebnost delavca na delovnem mestu, kot tudi ne obstaja zakon, ki bi določal, v katerem obsegu lahko delodajalec dopustno nadzoruje delavca na delovnem mestu. Zupančič (2015, VI) opozarja na odločitev[1] Upravnega

[1] Upravno sodišče RS, sodba 702/99 z dne 21. marec 2000.

sodišča iz leta 1999 o opredelitvi zasebnosti komunikacijskih naprav na delovnem mestu. V tej sodbi je zapisano, da se pod pojmom zasebno življenje lahko razumejo zasebne in službene telefonske linije, ni pa pomembna pripadnost ali lastnina določenega komunikacijskega sredstva.

V času trajanja delovnega razmerja delodajalec nima pravice vpogleda v prosti čas delavca in njegovih dejavnosti zunaj dela, saj bi s tem kršil pravico do zasebnosti delavca. Delodajalec tudi nima pravice zahtevati podatkov o delavčevih aktivnostih v prostem času. V primeru, da se delavec in delodajalec poznata tudi v privatnem življenju in delodajalec pozna določene osebne podatke delavca, le-teh ne sme izkoriščati, da bi oškodoval delavca na delovnem mestu.

Delodajalec lahko krši zasebnost delavca tudi s pridobivanjem občutljivih osebnih podatkov o zdravstvenem stanju delavca. Informacijski pooblaščenec (2008b) dodaja, da delodajalec nima pravice zahtevati zdravniškega spričevala od zdravnika, h kateremu je bil zaposleni napoten na zdravniški pregled. Zadostuje že spričevalo o zdravstveni sposobnosti za delo.

Šprah (2009) navaja, da komunikacijska zasebnost »ščiti vse vrste komunikacij, s tem pa ne le njihove vsebine, ampak tudi podatke, povezane s komunikacijo.« Iz te trditve je razvidno, da imajo zaposleni na delovnem mestu pravico, da ohranjajo tajnost svojih sporočil in pravico do svobodne komunikacije. Komunikacijska zasebnost uporablja dvojno varstvo podatkov, to pomeni, da se zbrani podatki varujejo kot osebni podatki in kot pravica do komunikacijske zasebnosti.

Maltby (2013) podaja napotke, kako lahko delavci sami varujejo svojo komunikacijsko zasebnost na delovnem mestu, če uporabljajo mobilne telefone. Sodobni mobilni telefoni ne omogočajo le telefoniranja ali izmenjave kratkih sporočil (angl. Short Message Service – SMS) temveč tudi dostop do interneta in uporabo različnih spletnih storitev (e-pošte, spletno nakupovanje, izvajanje finančnih transakcij, sodelovanje na socialnih omrežjih ipd.). Uporaba mobilnega telefona na delovnem mestu delavcu omogoča, da internet in spletne storitve uporablja brez nadzora delodajalca.

Pri tem se mora delavec prepričati, če delodajalec dovoljuje uporabo mobilnih telefonov na delovnem mestu. Nekateri delodajalci takšno uporabo prepovedujejo, ker so lahko moteči za delavca med opravljanjem delovnega procesa.

2.3 Varstvo osebnih podatkov zaposlenih na delovnem mestu

ZVOP-1 v 6. členu opredeljuje osebni podatek kot »katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen«.

Torej lahko sklepamo, da je osebni podatek vsak podatek, iz katerega je možno ugotoviti identiteto posameznika, tudi če ni neposredna. »Najpogostejši osebni podatki so tako: osebno ime, naslov stalnega oziroma začasnega prebivališča, rojstni datum, rojstni kraj ter podatek o delovnem mestu in plačilnem razredu,« opisujejo Lampe idr. (2007).

Osebni podatki se zbirajo, še preden posameznik stopi v delovno razmerje. Posameznik osebne podatke navede že v prijavi na razpis za delovno mesto. Delodajalec je zavezan k varovanju takšnih podatkov kot tudi podatkov, ki izhajajo iz izbirnega postopka. Osebnih podatkov neizbranega kandidata delodajalec ne sme posredovati tretjim osebam in jih mora uničiti pravijo Bien Karlovšek idr. (2008, 49). Delodajalec mora na zahtevo neizbranega kandidata za delovno mesto vrniti vse njegove dokumente, ki jih je oseba predložila v postopku prijave na delovno mesto in so veljali kot dokaz za zahtevane pogoje (Zakon o delovnih razmerjih, ZDR-1, Ur.l. št. 21/2013, 003-02-3/2013-2, 30. člen). Osebne podatke izbranega kandidata pa delodajalec varuje še naprej v skladu z veljavno zakonodajo. V primeru zaposlitve izbranega kandidata delodajalec osebo prosi, da mu le-ta posreduje dodatne osebne podatke, vendar le tiste, ki so potrebne za zaposlitev in sklenitev pogodbe o zaposlitvi dodajajo Bien Karlovšek idr. (2008, 49).

V ZVOP-1 (11. člen) je zapisano, da lahko osebne podatke delavcev zbira delodajalec ali pa zunanji upravljavec osebnih podatkov, ki je pooblaščen s strani delodajalca. ZVOP-1 v 3. točki 6. člena obdelavo osebnih podatkov opredeli kot: »kakršnokoli delovanje ali niz delovanj, ki se izvaja v zvezi z osebnimi podatki, ki so avtomatizirano obdelani ali ki so pri ročni obdelavi del zbirke osebnih podatkov ali so namenjeni vključitvi v zbirko osebnih podatkov, zlasti zbiranje, pridobivanje, vpis, urejanje, shranjevanje, prilagajanje ali spreminjanje, priklicanje, vpogled, uporaba, razkritje s prenosom, sporočanje, širjenje ali drugo dajanje na razpolago, razvrstitev ali povezovanje, blokiranje, anonimiziranje, izbris ali uničenje.«

Obdelava osebnih podatkov delavcev ne sme biti obravnavana kot običajno poslovanje (Bien Karlovšek idr. 2008, 19), saj se z obdelavo osebnih podatkov posega v temeljno človekovo pravico.

Lampe idr. (2007, 6/1-2) opozarjajo, da morajo biti delodajalci pri upravljanju osebnih podatkov, pozorni na dejstvo, da podjetje razpolaga tudi z njihovimi osebnimi podatki. V primeru zlorabe osebnih podatkov so lahko žrtve tudi sami, ne samo delavci.

Vsi zaposleni, ki delajo in opravljajo naloge pri osebah, ki upravljajo z osebnimi podatki, so dolžni varovati njihovo tajnost. Vsak delodajalec se mora potruditi za ustrezno varovanje osebnih podatkov zaposlenih. Bien Karlovšek idr. (2008, 33-35) pravijo, da mora za namen varovanja delodajalec zagotoviti ustrezna tehnična sredstva, ustrezne postopke in ukrepe, s katerimi se lahko prepreči naključno ali namerno uničevanje podatkov, nepravilna sprememba ali izguba in seveda nepooblaščena obdelava osebnih podatkov. Pri osebnih podatkih, ki so

dostopni preko telekomunikacijskega sredstva oziroma omrežja, mora strojna, sistemska in programska oprema zagotoviti, da je obdelava podatkov le v mejah pooblastil, ki jih ima obdelovalec osebnih podatkov.

V prvem odstavku v 11. člena ZVOP1 je določeno, »da lahko upravljalec osebnih podatkov posamezna opravila v zvezi z obdelavo osebnih podatkov s pogodbo zaupa pogodbenemu obdelovalcu osebnih podatkov, ki je registriran za opravljanje take dejavnosti in zagotavlja ustrezne postopke in ukrepe iz 24. člena ZVOP-1.« Pavšič (2008, 18) pojasnjuje razliko med upravljalcem osebnih podatkov in pogodbenim obdelovalcem osebnih podatkov. Upravljalec osebnih podatkov je po 6. točki 6. člena ZVOP-1, lahko pravna ali fizična oseba oziroma druga oseba javnega ali zasebnega sektorja, ki določa namen in sredstva za obdelovanje osebnih podatkov. Upravljalec osebnih podatkov ima pravno podlago za obdelovanje osebnih podatkov po ZVOP-1 (8., 9. in 10. člen) ali osebno privolitev posameznika na katerega se osebni podatki nanašajo.

Pogodbeni obdelovalec osebnih podatkov pa je v ZVOP-1, v 7. točki 6. člena opredeljen kot »fizična ali pravna oseba, ki osebne podatke obdeluje v imenu in na račun upravljalca osebnih podatkov.« Pravno podlago za obdelovanje osebnih podatkov ima pogodbeni obdelovalec osebnih podatkov po pogodbi, ki jo sklene z upravljalcem osebnih podatkov. Glavna značilnost pogodbene obdelave osebnih podatkov je obstoj pravne podlage, ki je vedno v pisni obliki pogodbe med upravljalcem in obdelovalcem osebnih podatkov. Z njo upravljalec poveri določeno vrsto obdelave osebnih podatkov pogodbeni stranki, v tem primeru pogodbenemu obdelovalcu osebnih podatkov, ki storitev opravi na račun in v imenu upravljalca.

Pavšič (2008, 19) pojasnjuje eno izmed temeljnih pravil pri pogodbeni obdelavi osebnih podatkov. Upravljalec osebnih podatkov ne more prenesti načina obdelave osebnih podatkov na pogodbenega obdelovalca osebnih podatkov, katerega tudi sam ne sme izvajati.

Določene osebne podatke delavcev, kot so fotografije, službeni e-mail naslovi in službene telefonske številke, lahko delodajalec objavi brez privolitve delavca, če je to potrebno za opravljanje delovnega procesa. To je pogosto predvsem na takšnih delovnih mestih, kjer je veliko dela s strankami. Ti podatki so največkrat objavljeni na spletnih straneh podjetja oziroma jih delavci nosijo na priponki, ki jo imajo pripeto na delovni obleki. Če delodajalec želi objaviti fotografije zaposlenih in omenjen pogoj ni izpolnjen, mora prositi za soglasje delavca. Če delavec odkloni objavo fotografij, se njegov položaj pri delodajalcu zaradi tega ne sme poslabšati.

Ko se delovno razmerje konča, delodajalec še vedno razpolaga z osebnimi podatki delavca. Bien Karlovšek idr. (2008, 52) navajajo, da mora delodajalec ob koncu delovnega razmerja izbrisati oziroma uničiti vse osebne podatke delavca, ki niso pomembne zaradi morebitnih zastaralnih rokov sodnih postopkov. Nekateri dokumenti se lahko na podlagi zakona hranijo

trajno. Take dokumente je treba voditi v posebni arhivski zbirki nekdanjih zaposlenih, ki mora ustrezati vsem zahtevam ZVOP-a (prav tam).

Bien Karlovšek idr. (2008, 14) govorijo o posledicah, ki so nastale z razvojem IKT. IKT je vse bolj prisotna v organizacijah in podjetjih, posledično tudi na delovnih mestih. Razvoj IKT je poenostavil in pospešil zbiranje in obdelavo vseh podatkov, tudi osebnih podatkov. Zaradi tega se pričakuje tudi ustrezno bolj razvito varovanje zbranih osebnih podatkov in boljša raven zaščite.

Nekatere organizacije zelo spoštujejo varovanje podatkov in informacij Bien Karlovšek idr. (2008, 63) navajajo, da lahko podjetja pridobijo certifikat o varovanju informacij, in sicer po standardu ISO/IEC 27001:2005. Po tem standardu: »morajo tako pripraviti, uvesti, izvajati in nadzorovati sistem upravljanja in vodenja informacij.«

Informacijski pooblaščenec (2008b) navaja deset najpogostejših kršitev po ZVOP-1, do katerih prihaja v delovnih razmerjih:

1. Nadzor nad uporabo interneta in vpogled v vsebino elektronske pošte,
2. Vpogled v zdravstvene podatke zaposlenih,
3. Nedovoljen in nepravilen nadzor nad zaposlenega med bolniškim dopustom,
4. Video nadzor delovnih prostorov, brez utemeljenega razloga,
5. Ne obveščanje (pisno) zaposlenih o video nadzoru,
6. Neustrezno zavarovanje zbirk osebnih podatkov,
7. Neutemeljeno sledenje službenih vozil, mobilnih telefonov z uporabo GPSa,
8. Prisluškovanje telefonskim klicem zaposlenih brez utemeljitve,
9. Preprečitev delavcu, da se seznani z osebnimi podatki, ki jih delodajalec o njem ima,
10. Zbiranje osebnih podatkov zaposlenih preko dovoljene in potrebne meje.

Varstvo osebnih podatkov ima tudi pravno podlago. Zaradi občutljivosti področja je varovanje osebnih podatkov opredeljeno tudi v Ustavi RS, ki je najvišji pravni akt v Republiki Sloveniji in ga morajo spoštovati vsi državljani. Z Ustavo Republike Slovenije (38. člen) je prepovedana uporaba osebnih podatkov, če je le-ta v nasprotju z namenom za katerega so bili osebni podatki zbrani.

Iz Ustave RS izhaja tudi ZVOP-1, ki opredeljuje načine zbiranja, obdelovanja, uporabe, nadzora in varstva osebnih podatkov z upoštevanjem tajnosti. Če pride do zlorabe osebnih podatkov, ima vsak posameznik pravico do sodnega varstva.

ZVOP-1 je tisti zakon, po katerem se morajo ravnati oziroma ga morajo poznati vsi, ki delajo z osebnimi podatki. V ZVOP-1 so določene pravice, obveznost, načela in ukrepi, s katerimi je možno preprečiti nezakonite in neupravičene posege v zasebnost posameznika. V 4. členu ZVOP-1 je zapisano: »Varstvo osebnih podatkov je zagotovljeno vsakemu posamezniku ne glede na narodnost, raso, barvo, veroizpoved, etični pripadnosti, spol, jezik, politično ali

drugo prepričanje, spolno usmerjenost, premoženjsko stanje, rojstvo, izobrazbo, družbeni položaj, državljanstvo, kraj oziroma vrsto prebivališča ali katerikoli drugo osebno okoliščino.« ZVOP-1 velja za vse delodajalce, ki imajo sedež ali registrirano podjetje v Republiki Sloveniji in upravljajo z osebnimi podatki. Zakon velja tudi za vsa diplomatsko-konzularna in druga uradna predstavništva RS po svetu.

Za Slovenijo, kot članico Evropske unije, veljajo tudi listine Evropske unije. Listina Evropske unije o temeljnih pravicah (Ur. l. EU. 2010/C 83/02, 8. člen) navaja, da ima vsak posameznik pravico do varstva osebnih podatkov. V istem členu je tudi zapisano, da ima vsak delavec pravico dostopa do osebnih podatkov, ki jih o njem zbira delodajalec. Če delavec spremeni svoj stalni naslov oziroma se delavka poroči in spremeni priimek, jim mora delodajalec omogočiti spremembo osebnih podatkov.

Ker so osebni podatki del delovnega razmerja, obstaja zakon (ZDR-1), ki kot temeljni akt ureja področje delovnega razmerja. V zakonu sta še posebej dva člena osredotočena na varstvo osebnih podatkov. V drugem odstavku 48. člena ZDR-1 je zapisano sledeče: »Osebne podatke delavcev lahko zbira, obdeluje, uporablja in dostavlja tretjim osebam samo delodajalec ali delavec, ki ga delodajalec za to posebej pooblasti.« V prvem odstavku 48. člena ZDR-1 je zapisano tudi, da se osebni podatki delavca zbirajo in posredujejo tretjim osebam le zaradi uresničevanja obveznosti in pravic, ki izvirajo iz delovnega razmerja. Če za določene osebne podatke delavca prenehajo obstajati zakonske podlage za zbiranje in shranjevanje se morajo osebni podatki takoj prenehati uporabljati in izbrisati, navaja tretji odstavek 48. člena zakona (ZDR-1, 48. člen).

Prav tako obstaja zakon, ki posebej ureja področje varovanja osebnih podatkov v delovnem razmerju, in sicer Zakon o evidencah na področju dela in socialne varnosti (ZEPDSV, Ur. l. RS. št. 40/2006, 001-22-51/06, v 13. členu) so zapisani vsi podatki delavca, ki jih delodajalec lahko shranjuje. To so: ime, datum, kraj in država rojstva, EMŠO, davčno številko, državljanstvo, naslov stalnega in začasnega prebivališča, izobrazba in stanje delavca (invalid, delno invalid, upokojen, delno upokojen). Če delodajalec zaposluje tuje državljane, morajo ti delavci imeti delovno dovoljenje. V tem primeru delodajalec lahko zbira tudi podatke o vrsti delovnega dovoljenja, datumu izdaje in datumu izteka, številki delovnega dovoljenja in o odgovornem organu, ki je izdalo delovno dovoljenje. Ker ima delodajalec z vsakim delavcem sklenjeno pogodbo o zaposlitvi, hrani tudi podatke o vrsti in vsebini zaposlitve. To so podatki, ki izhajajo iz pogodbe o zaposlitvi, kot na primer: datum sklenitve pogodbe o zaposlitvi, datum nastopa dela, kraj dela in delovni čas, razlog za sklenitev, delavčev poklic in potrebna strokovna usposobljenost oziroma izobrazba za delovno mesto. Ko pogodba o delovnem razmerju preneha, delodajalec shrani tudi podatke o datumu in načinu prenehanja delovnega razmerja.

2.4 Informacijska in komunikacijska zasebnost

Wagner De Cew (1997, 75-78, v Kovačič 2006, 45) opredeljuje informacijsko zasebnost na naslednji način: »Informacijska zasebnost obsega varovanje informacij o posamezniku (t. i. osebne podatke), z njegovimi komunikacijami vred.«

Komunikacijska zasebnost je povezana z informacijsko zasebnostjo in Šprah (2009) jo opredeljuje kot zasebnost, kamor spadajo vsi podatki, pridobljeni preko vseh vrst komuniciranja, ki jih posameznik uporablja.

Na delovnem mestu z uporabo IKT komuniciramo z različnimi tehničnimi sredstvi. To zajema komuniciranje po telefonu, računalniku, e-pošti oziroma s pomočjo različnih informacijskih tehnologij. V spletnem slovarju TechTerms.com (2014) je zapisano, da se informacijske tehnologije nanašajo na vse, kar je povezano z računalniško tehnologijo in na ljudi, ki delajo s to tehnologijo.

Vsebine, o katerih se pogovarjamo po telefonu, pišemo po e-pošti in ki jih sporočamo preko drugih kanalov komuniciranja, so prometni podatki, ki so opredeljeni tudi kot osebni podatki. Ko delodajalec preverja našo e-pošto in prisluškuje telefonskim pogovorom, krši našo komunikacijsko zasebnost (Šelih 1979, 156 in 173, v Kovačič 2006, 53). Komunikacijska zasebnost je kršena že samo s tem, ko se delodajalec seznani z vsebino, ne da bi potem to uporabil proti delavcu.

Pirc Musarjeva (2008, 6) opozarja, da so prometni podatki osebni podatki, ki uživajo dvojno varstvo. Varstvo jim sledi po 38. členu Ustave in ZVOP in tudi po 37. členu, v katerem so določene meje posegov v komunikacijsko zasebnost. V nadaljevanju Pirc Musarjeva (2008, 6) opisuje dopustno zbiranje in obdelavo prometnih podatkov. Podatke o prometu morajo operaterji hraniti dve leti od dneva nastanka podatkov oziroma od dneva komunikacije. Operaterji so dolžni po Zakonu o elektronskih komunikacijah (ZEKom-1, Ur.l. RS. št. 109/2012, 00-02-10/2012-32, 107. člen) podatke posredovati po prejemu prepisa odredbe pristojnega organa, v katerem je zapisana navedba vseh potrebnih podatkov o obsegu dostopa. ZEKom v celoti sledi 37. členu Ustave, za rok hrambe in namen uporabe pa sledi Direktivi 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 ter spremembi Direktive 2002/58/ES. Sledi, da delodajalec lahko izvaja nadzor nad izpisom na posamezni telefonski številki, in sicer v primeru, da je prišlo do prekoračitve, ki je bila določena v internem pravilniku.

Če v podjetju pride do suma kaznivega dejanja in delodajalec želi preveriti prometne podatke zaposlenih, ki so nastali pri komuniciranju, se mora delodajalec omejiti na ozek krog ljudi, pri katerih je največja verjetnost, da so kaznivo dejanje storili. Pri iskanju kršitelja pravil oziroma storilca kaznivega dejanja nikakor ne sme preverjati vseh zaposlenih. Za vsak poseg in za

vsak prometni podatek mora obstajati zakonska podlaga in utemeljen razlog, ki pa mora biti v skladu z ustavnim načelom sorazmernosti, še dodaja Pirc Musarjeva (2008, 8).

Šelih (1979, 156 in 173, v Kovačič 2006, 53) razpravlja o posledicah poseganja v informacijsko in komunikacijsko zasebnost posameznika, ki so nastale po razvoju IKT. Tehnološka razvitost omogoča in prinaša nove oblike poseganja v zasebnost. S sodobno tehnologijo je omogočeno poseganje in kršitev zasebnosti posameznika brez vstopanja v njegov osebni prostor. Pred samim razvojem IKT je bil vpogled v pošto posameznika mogoč le tako, da je nekdo vstopil v hišo ter nato odprl in prebral pošto. Danes pa je z razvitostjo IKT to mogoče opraviti kjerkoli, kjer je mogoča povezava z internetom. Če kdo želi prebrati posameznikovo elektronsko pošto, lahko vstopi v njegov strežnik in to enostavno stori, ker se elektronska pošta shranjuje na spletnih strežnikih. Delodajalec lahko pregleda vsebino e-pošte zaposlenega tako, da se poveže na službeni strežnik. Na ta način delavec ne more vedeti, če je delodajalec to dejansko storil. Delavec to lahko ugotovi le v primeru, če ga delodajalec kaznuje za vsebino e-pošte (prav tam).

Z razvojem mikroprocesorskih tehnologij se je uporaba velikih računalniških sistemov ustavila opozarja Mayer-Schönberger (2001, 225, v Kovačič 2006, 75). To je omogočilo množično izdelovanje majhnih, ugodnih in zmogljivih računalnikov. Nadzor informacijske zasebnosti je postal otežen, saj je nadzor nove in razpršene tehnologije zahtevnejši od nadzora omejenega števila dragih in kompleksnih računalniških sistemov.

Schneier (2005, v Kovačič 2006, 54) na primeru telefonije predstavlja problem razvitosti IKT. »Pred desetimi leti je bila vaša glasovna pošta shranjena na telefonski tajnici v vaši hiši, zdaj je shranjena v računalniku telekomunikacijskega podjetja.« Tako je možno, da nekdo krši našo pravico do komunikacijske zasebnosti s tem, da prisluškuje našim telefonskim pogovorom, ne da bi vstopil v naš dom. Prisluškovanje telefonom je možno že tako, da se na zunanjih telefonskih žicah in kablih namesti prisluškovalna naprava.

Informacijsko samo odločanje je pomembno, saj se vsak posameznik odloča sam, v kolikšni meri bo svoje osebne podatke dal na razpolago tretjim osebam. Če bo objavil veliko osebnih podatkov, bo njegova zasebnost manjša in možnost kršitve zasebnosti večja. Če pa bo zavaroval svoje osebne podatke, je tveganje za kršitve njegove komunikacijske zasebnosti manjše. Vsak se odloči sam, koliko svojih podatkov bo navedel v spletni anketi, koliko podatkov bo zapisal na družabnih omrežjih in če, bo navedel resnične podatke. Do kršitve informacijske zasebnosti največkrat prihaja, ker so ljudje nepazljivi in svoje osebne podatke brez razmisleka zaupajo spletnim podjetjem.

Na delovnih mestih se o delavcih in tudi o delodajalcih zbirajo komunikacijski podatki, kot so zasebne in službene telefonske številke ter e-naslovi. Delavci morajo soglašati, da lahko delodajalec njihove službene komunikacijske podatke zbira v en imenik, ki se uporablja samo

za službene namene. Delodajalec tega imenika ne sme posredovati v uporabo in vpogled tretjim osebam.

Delodajalci niso edini, ki lahko kršijo informacijsko in komunikacijsko zasebnost delavca. Tudi država, državni organi in vojska zbirajo različne podatke o prebivalstvu, in sicer za njihovo zaščito. Z razvojem IKT imajo na voljo vedno boljša sredstva za zbiranje različnih podatkov o prebivalcih. Pri nepravilni uporabi IKT in tehnološko razvitih sredstev lahko pride do izdaje osebnih podatkov prebivalcev tretjim osebam, kar krši zasebnost prebivalcev in pravico do varstva osebnih podatkov po Ustavi in posledično tudi škoduje državi.

Po 37. členu Ustave RS je zagotovljena tajnost pisem in drugih občil. Vsebina tega člena določa dimenzijo zasebnosti, ki se nanaša na pravico do komunikacijske zasebnosti. Ta pravica obsega tajnost vseh občil in varuje komunikacije, ki so posredovane oziroma opravljene preko različnih komunikacijskih sredstev. To varstvo preprečuje seznanitev tretjih oseb z vsebino sporočila. S to pravico je tudi zagotovljena pravica posameznika pri njegovi svobodi komuniciranja. To pomeni, da posameznik izbira sam, komu in na kakšen način bo posredoval sporočilo. Določba zagotavlja nenadzorovano komunikacijo. Ustava RS pravi, da lahko edino zakon predpiše neupoštevanje varstva tajnosti pisem in drugih občil ter nedotakljivost človekove zasebnosti v primeru, da je to nujno za potek kazenskega postopka ali varnost države (Bien Karlovšek idr. 2008, 23-24).

Komunikacijska zasebnost je opredeljena v Evropski konvenciji o varstvu človekovih pravic in temeljnih svoboščin (EKČP, Ur. l. RS. št.7-41/1994, 33/1994, 8. člen, v Kovačič 2006, 81). Po tem členu je vsakemu posamezniku priznana tajnost pisem in drugih občil, tajnost telefonskih komunikacij, elektronske pošte, sporočil SMS in drugih. Francosko sodišče je leta 1998 v primeru Lambert proti Franciji[2] poudarilo, »da ni razlike med lastnim telefonskim priključkom in telefonskim priključkom tretje osebe«. Istega leta so v Švici v primeru Kopp proti Švici[3] dodali, da so zaščiteni tudi klici v in iz poslovnih prostorov. Seveda so pred posegi delodajalca zaščitena tudi komunikacijska sredstva, ki jih zaposleni uporabljajo na delovnem mestu.

V 8. členu Evropske konvencije o varstvu človekovih pravic in temeljnih svoboščin (v Kovačič 2006, 73) je dodano, da so posegi v pravico do zaščite doma, dopisovanja ter, zasebnega in družinskega življenja možni le, če je tako določeno z zakonom in če je to v demokratični družbi nujno zaradi državne ali javne varnosti, preprečitev zločina, varovanje zdravja ali pravic in svoboščin drugih ljudi.

---

[2] Lambert v. Francija, odločba z dne 24. 8. 1998.

[3] Kopp v. Švica, odločba z dne 25. 3. 1998.

Mayer-Schönberger (2001, 229 v Kovačič 2006, 77) opisuje pomembnega mejnika v razvoju informacijske zasebnosti. Izpostavlja načelo informacijskega samo-odločanja, kar pomeni, da je država dolžna pojasniti, zakaj potrebuje podatke in kaj bi pomenilo, če bi zavrnili oddajo osebnih podatkov. Z načelom informacijskega samoodločanja se razvila tudi pravica in možnost posameznikov, da se odločijo, kako bodo sodelovali v informacijski družbi.

V direktivi o zasebnosti in elektronskih komunikacijah (2002/58/EC) je zapisano: »komunikacij in z njim povezanih prometnih podatkov ni dovoljeno shranjevati brez soglasja uporabnika, razen za potrebe prenosa ali upravljanja prometa teh zaračunavanja storitev.« Kot izjema je zapisano shranjevanje komunikacij za potrebe dokazovanja komercialnih transakcij, vendar morajo biti uporabniki tudi pri tem obveščeni o shranjevanju, namenu in trajanju hranjenja. V 5. in 6. členu iste direktive je zapisano, da imajo pravico do obdelave komunikacijskih podatkov samo tisti, ki delajo za ponudnika storitev. Direktiva pravi, da obdelovanje podatkov, ki jih je zbral ponudnik preko javno dostopnih elektronsko komunikacijskih storitev za namene trženja brez uporabnikovega soglasja ni dovoljeno. Dolžnost ponudnikov storitev je redno obveščanje uporabnikov, čigar podatke obdelujejo, in sicer o namenu in obdobju shranjevanja podatkov. V direktivi je tudi zapisano, da morajo biti sistemi, ki zagotavljajo storitve, zasnovani tako, da je zbiranje osebnih podatkov čimbolj omejeno, oziroma da morajo biti zasnovani tako, da ščitijo zasebnost.

V 12. členu Splošne deklaracije o človekovih pravicah[4] (v Kovačič 2006, 73) je omenjena prepoved nadlegovanja: »… s samovoljnim vmešavanjem v njegovo zasebno življenje, v njegovo družino v njegovo stanovanje ali njegovo dopisovanje in tudi ne z napadi na njegovo čast in ugled«. V tem členu je tudi zapisano, da ima vsak posameznik v primeru kršitve vsebine iz tega člena pravico do pravnega varstva.

[4] Sprejela in razglasila jo je Generalna skupščina Združenih narodov 10. 12. 1948 z resolucijo št. 217 A (III).

3 NADZOR NA DELOVNEM MESTU

Kovačič (2006, 22) nadzor razume kot skupek dejanj oziroma orodje, ki omogoča zbiranje podatkov o posamezniku in s tem zakritje meje, ki pomagajo posamezniku, da loči svojo zasebnost od preostalega zunanjega sveta.

Beniger (1986, 7, v Kovačič 2006, 22) pa je nadzor opredelil kot: »usmerjen vpliv na zastavljen cilj«. V praksi se ta opredelitev kaže pri nadzoru, ki ga delodajalec izvaja nad delavci, da doseže zastavljeni cilj.

Brulc (2014, 12) nadzor razlaga kot sistematično in načrtno spremljavo dejavnosti in stanj delavca v času, ko opravlja delo z namenom, da zagotovi spoštovanje delovnopravnih obveznosti delavca in njegovih pravic.

Vsak zaposleni se srečuje z nadzorom dela na delovnem mestu (Kovačič 2003, 22). Delodajalci morajo pri tem spoštovati določena načela pri nadzoru delavcev. Nadzor dela zavzema vsa dejanja delodajalca, ki jih ta izvaja za doseganje svojih poslovnih ciljev. Zgodovinski začetek nadzora je povezan z vzpostavitvijo reda na delovnem mestu in utrjevanjem moči delodajalcev (prav tam).

Makarovič idr. (2001, 188-189, v Kovačič 2003, 24) izpostavljajo interese treh različnih osebkov, ki so prisotni pri nadzoru na delovnem mestu in jih je potrebno upoštevati. Prvi udeleženec je delodajalec, ki je lastnik delovne opreme, katero zaposleni uporabljajo. V interesu delodajalca je, da se delovna oprema uporablja v skladu z njenim namenom in da se preprečuje njena zloraba. Z namenom, da delavci ne bi oškodovali lastnika in uničili njegove opreme, delodajalec nad delavci izvaja nadzor. Interesi delavcev se razlikujejo od interesov delodajalca. Delavci pričakujejo, da bodo na delovnem mestu imeli določeno stopnjo zasebnosti, kar je povezano z nadzorom na delovnem mestu oziroma s seznanitvijo, da se nadzor izvaja. Tretji interes je interes tretjih oseb, ki komunicirajo z zaposlenimi preko komunikacijskih sredstev, kot je telefon in elektronska pošta, ne da bi vedeli, ali se pri tem uporablja službeno komunikacijsko sredstvo in/ali delodajalec izvaja nadzor uporabe komunikacijskih sredstev zaposlenih.

3.1 Vpliv nadzora na delovnem mestu na delavca

Nadzor na delovnem mestu lahko na delavca vpliva pozitivno ali negativno. Če se nadzor izvaja nepravilno in posega v delavčevo zasebnost, je delavec pod pritiskom, se na delovnem mestu počuti neprijetno, njegova delovna storilnost pa je zmanjšana. V primeru pravilnega izvajanja nadzora na delovnih mestih, kjer je to nujno potrebno (na primer v bankah in trgovinah) pa delavci ne čutijo nobenega pritiska, ker se zavedajo, da je to v skladu z načinom

poslovanja podjetja in naravo njihovega dela. Delodajalci predvidevajo, da bodo z izvajanjem nadzora povečali učinkovitost delavcev, zaščitili delovno opremo, preprečili krajo inventarja ipd.

Velikokrat se zgodi, da delodajalci zaradi teženj po večanju dobička in doseganju poslovnih ciljev uspešnosti posegajo po različnih ukrepih. Pri tem pa pozabijo na psihološke in sociološke dejavnike, ki so pri opravljanju delovnega procesa tudi pomembni. Če se zgodi, da delodajalec prekorači mejo razumnega, delavci postanejo nadzirani pri mnogih, če ne pri večini ravnanj. Njihova zasebnost na delovnem mestu tako postane omejena. Delavci zaradi različnih mehanizmov nadzora izgubijo zaupanje do delodajalcev, saj se bojijo sankcij in kazni, ki jim jih delodajalec lahko naloži. Na delovnem mestu občutijo pritisk in izgubljajo motivacijo za delo. Bien Karlovšek idr. (2008, 54) svetujejo delodajalcem, da morajo za dobro vzdušje na delovnem mestu in harmonične odnose med delodajalcem in delavci dopustiti dovolj svobode in zasebnosti. S tem delodajalec delavcem omogoča, da opravljajo svoje delo mirno in brez pritiska, njihova pravica do zasebnosti pa pri tem ni kršena. Tako so bolj motivirani za delo, kar se pozna tudi pri rezultatih poslovanja podjetja in v splošnem vzdušju delovnega okolja. Pri optimalni meri nadzora na delovnem mestu se delavci počutijo svobodno, vendar te svobode ne izrabljajo v slabe namene in ne škodijo delodajalcu.

Pri uporabi nadzora dela na delovnem mestu lahko pride do konfliktnih situacij. Lampe idr. (2007, 7/1-2) opisujejo štiri skupine konfliktnih situacij.

1. Uporaba video nadzora pri dostopu do poslovnih prostorov in na samem delovnem mestu.
2. Nadzor nad IKT opremo, ki je v lasti delodajalca.
3. Osebna preiskava delovnega mesta in delavčevih osebnih stvari (pisarna, predali, ipd).
4. Nadzor delavca izven delovnega časa s pomočjo detektivskih in varnostnih agencij.

Z nadzorom zaposlenih na delovnem mestu delodajalec zagotavlja in ohranja varno delovno okolje za svoje delavce. Oblika in količina nadzora se razlikujeta tudi v tem ali delodajalec nadzoruje izkušenega ali neizkušenega delavca. Pri nadzoru delavcev brez izkušenj je potreben višji nivo nadzora, in sicer vse do takrat, dokler delodajalec ni prepričan, da lahko delavec svoje delo opravlja samostojno. Takrat se nivo nadzora lahko zmanjša. Pri izkušenih delavcih, ki dlje časa opravljajo isto delo, pa je potreben nižji nivo in tudi drugačna oblika nadzora (Weeks 2013). Delavci po določenem času ponavljajočega se dela niso več tako dosledni, zato mora biti delodajalec pozoren tudi na take delavce. Ko med delavci opazi nedoslednost in površnost mora pri njih poseči po strožjem nadzoru dela, zlasti ko se uvaja nova delovna oprema, saj so izkušeni delavci običajno starejši in navajeni na starejšo opremo.

Bien Karlovšek idr. (2008, 62) navajajo, da nadzor na delovnem mestu: »... mora biti vsak nadzor v prvi vrsti zakonit in ustavno dopusten. Delodajalec ne sme pavšalno predpisovati oblik, načina in obsega nadzora z zanemarjanjem temeljnih določb o človekovih pravicah.« V nadaljevanju govori o internih aktih podjetja, v katerih delodajalec opredeli nadzor delavcev

na delovnem mestu. Pri tem mora biti zelo pazljiv, saj interni akti ne smejo biti v neskladju z veljavno zakonodajo in ustavnimi določili. Vsak ukrep, ki je določen v internih aktih delodajalca, mora biti ustavno in zakonito dopusten. Pri tem delodajalec ne sme kršiti zakonske in ustavne pravice posameznika do njegove informacijske in komunikacijske zasebnosti. Morebitni posegi v zasebnost posameznika morajo biti minimalni in dovoljeni oziroma potrebni za doseganje legitimnih, po zakonu in ustavi dopustnih ciljev (prav tam).

Delodajalec mora pri pripravi internih aktov upoštevati naslednja načela (Bien Karlovšek idr. 2008, 63):

- popolnost,
- preglednost,
- natančnost,
- nedvomnost,
- zakonitost in ustavno dopustnost.

3.2 Oblike nadzora na delovnem mestu

Glede na tehnološko razvitost današnje družbe se na delovnih mestih pojavlja vse več tehničnih pripomočkov, s katerimi je možno izvajati nadzor nad delavci in posegati v njihovo zasebnost, in sicer na popolnoma nove načine (Kovačič 2006, 30). Da bi z večjim nadzorom boljše zavarovali svojo lastnino in s povečanjem nadzora nad delavci povečali učinkovitost, delodajalci tehnične pripomočke za nadzor pogosto uporabljajo na nepravilen način. Nove elektronske nadzorne tehnologije so tako neopazne, da se jim posameznik ne more izogniti. Kovačič (2006, 30) ugotavlja, da je zaradi razvite tehnologije nadzor postal bolj obsežen, nezaznaven in instrumentaliziran. Posledično tak nadzor lahko spodkopava človekove pravice.

Na delovnem mestu se s pomočjo IKT največkrat nadzoruje (Bien Karlovšek idr. 2008, 56):

- IKT-oprema: računalniki, telefoni, dlančniki, diski (za zapisovanje podatkov),
- prihodi in odhodi z delovnega mesta s pomočjo evidenčnih kartic in biometrije,
- video nadzor nad delom in gibanjem delavca, nad poslovnimi prostori,
- nadzor nad uporabo interneta in vsebino elektronske pošte,
- GPS-nadzor pri uporabi službenih vozil ali službenih mobilnih telefonov.

Cvetko (1999, 47-78) govori o napravah na delovnem mestu, ki omogočajo zbiranje različnih podatkov o delavcih. Najpogosteje uporabljeni so telefoni, naprave za vodenje prisotnosti in kamere z vgrajenimi mikroprocesorji. Z njihovo pomočjo je mogoče preverjati delavčevo prisotnost, porabljen čas za odmor in malico, trajanje telefonskih pogovorov in naravo klicanih številk. Take oblike nadzora dela so dovoljene le v primeru, ko se predstavnik delavcev ali sindikat soglašata.

Nadzor na delovnem mestu se lahko izvaja z zgoraj omenjenimi sredstvi ali pa z osebnim nadzorom na delovnem mestu. To pomeni, da delodajalec določi delavca oziroma nadzornika, ki je odgovoren in nadzoruje zaposlene. Pri taki obliki nadzora je potrebno, da je nadzornik na delovnem mestu vedno prisoten. Pomanjkljivost te oblike nadzora pa je, da nadzornik ne more nadzirati vseh delavcev hkrati. Tak način nadzora pa omogoča še dodatna uporaba tehničnih sredstev.

Obstajajo tudi računalniški programi za popolni nadzor uporabe računalnikov zaposlenih. Pri tem se mora delodajalec zavedati, da z njegovo uporabo krši zakonsko in tudi ustavno varovane pravice zasebnosti zaposlenih in tretjih oseb, s katerimi zaposleni komunicirajo. Tovrstni programi se lahko na računalnike namestijo neopazno in tako omogočajo nadzor spletnih aktivnostih na internetu. Delodajalec lahko torej pregleda delavčevo prejeto in poslano e-pošto, program pa lahko prikazuje tudi oddaljen prikaz računalniškega zaslona zaposlenega (Bien Karlovšek idr. 2008, 55). Pri tem lahko delodajalec delavce spremlja med uporabo različnih programov ter nadzira programe, ki omogočajo neposredno komuniciranje. Z nekaterimi novejšimi različicami je mogoč tudi nadzor uporabe družabnih omrežij, kot so Facebook, Tweeter, My Space ipd.

Bien Karlovšek idr. (2008, 56) v nadaljevanju svetujejo delodajalcem, da morajo že ob začetku delovnega razmerja v internih aktih in pravilnikih opredeliti in zapisati, katere oblike nadzora, kako, v kolikšni meri in zakaj jih bodo uporabljali. Delodajalec mora opredeliti tudi, ali bodo delavcem na voljo službena sredstva zgolj v službene namene ali jih bodo lahko uporabljali pod določenimi pogoji tudi v zasebne namene.

3.2.1 Video nadzor

Video nadzor je eden izmed načinov nadzora delavcev na delovnem mestu in zbiranja osebnih podatkov delavcev na delovnem mestu. Video nadzor se lahko izvaja na dva načina: prvi način opredeljuje, da se spremlja gibanje oseb preko monitorjev in se posnetki ne shranjujejo, zato pri tem ne nastajajo zbirke osebnih podatkov in delodajalcu oziroma izvajalcu video nadzora ni treba slediti določilom ZVOP-1. Drugi način vključuje snemanje gibanja oseb, pri čemer se posnetki shranjujejo kot zbirke osebnih podatkov, delodajalec pa mora slediti določilom ZVOP-1, opisujejo Bien Karlovšek idr. (2008, 86).

Lampe idr. (2007, 7/2-1) opredeljujejo dve absolutni prepovedi video nadzora. Prvi je prikriti video nadzor, ki je prepovedan in predstavlja prekršek po ZVOP-1 in po 149. čl. Kazenskega zakonika. Druga prepoved je video nadzor, ki bi obsegal zvočno snemanje, saj tudi ta predstavlja »kaznivo dejanje neuporabnega prisluškovanja in zvočnega snemanja po 148. čl. Kazenskega zakonika.«.

V določbah ZVOP-1 (Informacijski pooblaščenec 2015a) je zapisano, da morajo vse osebe javnega ali zasebnega sektorja, ki izvajajo video nadzor, objaviti obvestilo o izvajanju video nadzora. Le-to mora biti razločno in javno dostopno posamezniku, da se seznani z video nadzorom, in sicer najkasneje takrat, ko se tovrsten nadzor nad njim začne izvajati. Obvestilo mora vsebovati stavek, da se video nadzor izvaja. Prav tako mora vsebovati tudi naziv osebe javnega ali zasebnega sektorja, ki video nadzor izvaja, in kontaktne podatke za pridobitev informacij, kje in koliko časa se posnetki hranijo.

Davies (idr. 2015, 315) pravi, da video nadzor omogoča stalen in takojšen nadzor nad potekom dela in varovanje infrastrukture podjetja. Incidenti ali nezgode se lahko na ta način hitreje preprečijo in tako terjajo manj posledic, saj imajo podjetja z video nadzorom tudi varnostnika oziroma nadzornika kamer, ki dogajanje preko ekranov stalno spremlja.

Delodajalec lahko za izvajanje video nadzora na delovnem mestu pogodbeno najame tudi podjetje, ki je registrirano za opravljanje take dejavnosti. V tem primeru pride do pogodbene obdelave osebnih podatkov. Delodajalec je upravljavec osebnih podatkov, podjetje s katerim je sklenil pogodbo za izvajanje video nadzora pa je pogodbeni obdelovalec. Njegova naloga je zbiranje posnetkov oseb v imenu delodajalca. Po ZVOPu je delodajalcu naložena dodatna zahteva, ki pravi, da mora delodajalec, ki s pogodbo zaupa obdelovanje osebnih podatkov, pogodbenemu obdelovalcu zagotoviti vse ustrezne tehnične in organizacijske postopke, za varovanje osebnih podatkov in za preprečevanje neustrezne uporabe osebnih podatkov (Bien Karlovšek idr. 2008, 87-88). Delodajalec mora skrbeti za preverjanje ustrezne stopnje varovanja osebnih podatkov.

Za vse nastale posnetke z video nadzorom je treba voditi ustrezno evidenco, iz katere mora biti razvidno, kdo in kdaj je dostopal do podatkov in zakaj so bili ti podatki uporabljeni (Bien Karlovšek idr. 2008, 88). Ker zakon posebej ne opredeljuje obdobja hrambe posnetkov video nazora, se v praksi uporablja čas hrambe osebnih podatkov »na splošno«. To pomeni, da se tudi posnetki video nadzora shranjujejo toliko časa, dokler je to potrebno za dosego namena, zaradi katerega se tudi video nadzor izvaja.

Video nadzor dostopa v uradnih poslovnih prostorih je urejen v 75. in 77. členu ZVOP-1. Po zakonskih določilih se video nadzor znotraj delovnih prostorov lahko izvaja le v primerih, ko je to nujno potrebno za zavarovanje premoženja, varnost zaposlenih ali varovanje tajnih podatkov in poslovne skrivnosti (Upravno sodišče Republike Slovenije 2014). Zakon še izrecno predpisuje (Bien Karlovšek idr. 2008 91), da je video nadzor dovoljen le, če namen ne more biti uresničen z milejšimi sredstvi nadzora. Seveda je pri izvajanju video nadzora pomembno, da delodajalec spoštuje in ne posega v zasebnost zaposlenih. Če želi delodajalec nadzorovati določen delovni stroj, mora biti kamera za video nadzor usmerjena le na delovni stroj, ne pa tudi na delavca, ki stroj upravlja.

Po zakonu je video nadzor izrecno prepovedan v tistih delovnih prostorih, kjer se izvaja poslovna dejavnost, vendar niso strogo določeni kot delovni prostori. Zato v teh prostorih zaposleni upravičeno pričakujejo visoko stopnjo zasebnosti (Bien Karlovšek idr. 2008 92). Videonadzor je prepovedan tudi v prostorih, ki so izven delovnega mesta. To so lahko garderobni prostori, prostori za malico ali odmor v delovnem času, dvigala in toaletni prostori.

Pri nadzoru dostopa do delovnih prostorov nastajajo zbirke posnetkov in osebnih podatkov. Tovrstni posnetki in podatki so lahko shranjeni največ eno leto po nastanku. Lampe idr. (2007, 7/2-8) pa svetujejo, da se v internih aktih, ki urejajo video nadzor določi krajši rok za brisanje nastalih posnetkov, tudi zaradi zmanjšanja stroškov nadzora.

V preteklosti je redko kateri delodajalec uporabljal video nadzor zaposlenih na delovnem mestu, danes pa je delovno mesto brez tovrstnega nadzora že prava rednost. Govorimo o različnih delovnih mestih, od blagajničarke do skladiščnika. Tukaj se lahko vprašamo, ali je tolikšna stopnja nadzora potrebna zaradi nezaupanja delodajalca v delavce ali zaradi same varnosti narave dela.

3.2.2 Nadzor uporabe interneta in svetovnega spleta

Internet predstavlja medij, ki deluje globalno in večpredstavnostno (Kovačič 2006, 29). Deluje tudi konvergentno, saj razvita IKT omogoča tudi povezavo interneta z drugimi tehnologijami, kot so telefoni, nadzornimi kamerami preko brezžične povezave in televizorji.

Internet je računalniško omrežje, ki povezuje več omrežij. »S pojmom internet si tako predstavljamo javno razpoložljiv in mednarodno povezan sistem računalnikov skupaj z informacijami in storitvami za uporabnike« (Bien Karlovšek idr. 2008, 57). Večina ljudi pojem internet napačno razume, saj si predstavlja le brskanje po spletnih straneh – Word Wide Web (angl) in elektronsko pošto. To sta samo dve storitvi interneta, dodajajo Bien Karlovšek idr. (2008, 57). Med drugimi storitvami so še videokonference, prenos datotek, klepetalnice, orodja za delo na daljavo ipd.

Bien Karlovšek idr. (2008, 58) v nadaljevanju opozarjajo na nevarnosti, ki nastanejo z uporabo interneta in njegovih storitev. Pri tem lahko delavci tretjim osebam posredujejo neprimerne in nedovoljene informacije o podjetju. Lahko si tudi ogledujejo neprimerne vsebine na spletnih straneh, prenašajo piratske kopije programov in s tem morda tudi viruse ipd. Največkrat delodajalci na službene računalnike naložijo računalniške programe, s katerimi je možno spremljati pogostost obiska spletnih strani. Računalniški programi za nadzor uporabe računalnikov in interneta največkrat kršijo pravico do zasebnosti zaposlenih in tudi zasebnosti tretjih oseb, s katerimi komunicirajo vsi zaposleni. Delodajalci se za nadzor uporabe interneta največkrat odločijo zaradi padca produktivnosti delavcev na delovnem mestu in zaradi večjih stroškov. Delavci, ki na svojem delovnem mestu obiskujejo spletne

strani zaradi osebnih interesov, pogosto ne izpolnjujejo norm, postanejo nedejavni, ne opravljajo naloženega dela, zamujajo roke ipd.

Delodajalec se lahko odloči, da bo nadzoroval uporabo interneta pri zaposlenih, tako da se zaščiti pred nelegalnim prenašanjem glasbe, video vsebin in drugih avtorskopravno zaščitenih vsebin, pravi Zupančič (2015, iii). Če se delavec odloči, da bo na delovnem mestu prenašal take vsebine, pri tem krši pravo intelektualne lastnine in ker to počne na delovnem mestu z opremo, ki je v lasti delodajalca, se prenese odgovornost za nelegalno početje tudi na delodajalca.

Internet ponuja tudi veliko odprto-kodnih programov, ki so primerni za osebno rabo, ne pa tudi za službeno rabo. Če želijo podjetja uporabljati tovrstne programe, morajo plačati licenčnino pravijo Bien Karlovšek idr. (2008, 60). Zato se je v podjetjih uveljavila praksa, da vsi zaposleni ne morejo namestiti takšnih programov. Da ne bi prišlo do težav, za izboljšavo in nadgradnjo informacijskega sistema v podjetjih skrbi služba, ki se ukvarja samo s tehnično podporo podjetja. Takšna služba skrbi tudi za informacijski sistem in ima pravico nameščanja novih programov ali nadgradnjo starih.

Ko smo na internetu, puščamo elektronske sledi, ki se shranjujejo pri našem ponudniku dostopa do interneta. V informacijskih sistemih, ki so tudi nameščeni na delovnih mestih, obstajajo datoteke dejavnosti, ki zapisujejo dejavnosti uporabnikov oziroma dejavnosti delavcev (Kovačič 2006, 30). Preko teh datotek lahko delodajalec odkrije, kdaj, zakaj in koliko časa je delavec namenil za uporabo interneta. Po drugi strani so datoteke aktivnosti tudi koristne, saj omogočajo odkrivanje in odpravljanje napak. V datotekah aktivnosti se pri uporabi interneta zapisujejo identifikacijski podatki o uporabniku, kot so: uporabniško ime, ki se lahko poveže z uporabnikovo identiteto, število IP-naslova, s katerega se je uporabnik povezal na internet, ter omrežje ali telefonska številka, preko katere je tudi mogoč dostop do interneta. Če se delodajalec poveže s ponudnikom interneta, lahko iz datotek aktivnosti pridobi vse podatke o gibanju zaposlenega na internetu.

Lampe s soavtorji (2007, 7/3-6) navajajo izjemo, ki ne predstavlja poseganja v zasebnost zaposlenega. To je v primeru blokiranja posameznih internetnih strani. Ko delodajalec zaposlenemu prepreči obisk določene spletne strani, npr. igranje spletnih igric, strani s pornografsko vsebino ipd., s tem ne posega in ne krši njegove zasebnosti. Zupančič (2015, iii) pa dodaja še en razlog, s katerim delodajalec lahko omeji delovanje zaposlenega na internetu in s tem ne posega v njegovo zasebnost, in sicer preprečitev prenosa večjih datotek na službeni računalnik, ne glede na vsebino.

3.2.3 Preverjanje e-pošte

V 8. točki 3. člena ZEKom-1 je e-pošta opredeljena na sledeči način: »Elektronska pošta pomeni vsako besedilno, govorno, zvočno ali slikovno sporočilo, poslano po javnem komunikacijskem omrežju, ki se lahko shrani v omrežju ali prejemnikovi terminalski opremi, dokler ga prejemnik ne prevzame.«

Elektronska pošta je storitev interneta, ki predstavlja eno izmed najhitrejših komunikacijskih sredstev v današnji informacijsko-komunikacijski družbi. Elektronsko pošto, krajše e-pošto, vsak posameznik uporablja za osebne in službene namene. Pri poslovanju v podjetju je le-ta zelo pomembna, saj omogoča obveščanje velikega števila zaposlenih na najhitrejši način in v kateremkoli času. Omogoča hitro, preprosto in skoraj brezplačno obveščanje poslovnih sodelavcev. Na nekaterih delovnih mestih imajo zaposleni službeni in zasebni e-poštni račun. Zasebnega e-naslova naj ne bi uporabljali v službi in preko njega tretjim osebam posredovali poslovnih informacij. Službeni e-naslov naj bi služil izključno službenim namenom in je najpogosteje prepovedan za uporabo pošiljanja osebnih vsebin. FindLaw (2014). Vsebina e-pošte je last delodajalca, če se uporablja preko računalniškega sistema, ki je v lasti delodajalca.

S pomočjo elektronske pošte je možno pošiljati tudi razne datoteke, slike, gradiva za sestanke, predstavitve ipd. Glede na njeno preprosto uporabo se je v praksi v podjetjih zelo dobro uveljavila. Veliko podjetij pošlje gradiva za sestanke, razna obvestila, račune kupcem in ostale poslovne dokumente po e-pošti. S tem prihrani stroške za tiskanje, pošiljanje in zamudo pošte. Če se en dan pred sestankom določi drugačen dnevni red ali pa je na voljo dodatno gradivo, je s pomočjo e-pošte te vsebine in informacije možno poslati takoj, tako da jih lahko vsi udeleženci prejmejo hitro in pravočasno.

V podjetjih delodajalci najpogosteje omejujejo uporabo zaradi možnega širjenja zlonamernih informacij, neprimernih vsebin, pošiljanja virusov in škodljive programske opreme. Nedovoljeno je tudi pošiljanje in prenašanje ne-licenčnih programov, nelegalno prenesene glasbene in video vsebine.

Perenič in Šalamon (2002, 148) podajata napotke za varno uporabo elektronske pošte. V primeru prejema pošte neznanega pošiljatelja prejemnik, v tem primeru delavec, ne sme odpirati pripete datoteke, saj lahko vsebujejo virusne datoteke. Tudi če je pošiljatelj znan, datotek ni priporočljivo odpirati, če je vsebina neznana. V primeru prejema verižnih in oglasnih sporočil jih je treba takoj izbrisati iz poštnega nabiralnika, da ne pride do zasičenja z elektronsko pošto.

Informacijski pooblaščenec (2010) pravi, da bi delodajalec lahko preverjal vsebino elektronske pošte zaposlenega, če bi vnaprej opredelil namene, primere in okoliščine, v katerih bi bila potrebna obdelava elektronskih sporočil, naslovljenih na zaposlenega. Delodajalec bi lahko to zapisal v določilu internih aktov podjetja. Določilo ne bi smelo

pomeniti generalnega pooblastila delodajalca, da bi lahko kadarkoli in brez nobene vednosti zaposlenega pregledoval njegovo pošto. Določilo bi bilo le obvestilo zaposlenega o možnosti pregleda elektronske pošte v primerih, ki bi bili vnaprej določeni in opravičeni. Po mnenju Informacijskega pooblaščena bi taki primeri bili izredni in redki. Delodajalec bi lahko opravičeno pregledal elektronsko pošto zaposlenega le, če bi grozila poslovna škoda zaradi pomanjkanja podatkov, ki bi jih imel dolgotrajno odsoten delavec. Če bi delodajalec sumil, da zaposleni izvršuje kaznivo dejanje preko elektronske pošte, je dolžan o tem obvestiti pristojne organe in jim prepustiti nadaljnje postopke. Kot vsa delovna sredstva in oprema je tudi elektronski naslov last delodajalca, zato lahko omeji delavčevo uporabo teh sredstev.

Elektronski naslov, ki je potreben za uporabo elektronske pošte, se smatra kot osebni podatek le v primeru, ko je preko njega mogoče ugotoviti identiteto lastnika elektronskega naslova (Informacijski pooblaščenec 2006). Da bi bila mogoča določljivost posameznika, ki je lastnik elektronskega naslova, mora le-ta vsebovati ime in priimek zaposlenega ter njegovo zaposlitev.

Delodajalec lahko omeji uporabo elektronske pošte na ta način, da omogoči pošiljanje samo na določene elektronske naslove oziroma samo na določene poslovne domene. Zupančič (2015, IV) dodaja, da delodajalec lahko tudi prepreči pošiljanje prilog in datotek, oziroma omeji pošiljanje le za določene formate datotek in določeno velikost prilog.

Rawlinson (2016) povzema odločbo Evropskega sodišča o človekovih pravicah z začetka januarja 2016, s katero so sodniki odločili, da ima delodajalec pravico vpogleda in branja zasebnih sporočil zaposlenih, ki so bila poslana preko spletnih klepetalnic, in e-mail naslovov med delovnim časom. V odločbi so na Evropskem sodišču o človekovih pravicah odločali o pritožbi romunskega inženirja, da je njegov delodajalec nedovoljeno prebral njegovo pošto, poslano preko Yahoojeve klepetalnice. Pritožba je bila zavrnjena z obrazložitvijo, da ima delodajalec pravico preverjanja, če zaposleni ne izpolnjujejo naloge med delovnim časom.

Po prenehanju delovnega razmerja lahko delavci še vedno razpolagajo s službenimi sredstvi, v tem primeru pa imajo tudi še vedno dostop do elektronske pošte. Priporočljivo bi bilo, da zaposleni po prenehanju delovnega razmerja iz službenega računa elektronske pošte izbrišejo ali prekopirajo vsa morebitna sporočila zasebne narave. Bien Karlovšek idr. (2008, 68-69) priporočajo, da delavec podpiše izjavo, da je iz službenega elektronskega poštnega računa izbrisal sporočila zasebne narave (odhodna in dohodna), in da izjavlja, da na tem računu ni več nobenih podatkov, ki bi pomenili kršitev njegove zasebnosti. S to izjavo bi delodajalec lahko arhiviral njegov službeni elektronski račun brez skrbi, da bi s tem posegal v delavčevo zasebnost. Arhiviranje lahko delodajalec zaupa osebi, ki je odgovorna za vzdrževanje informacijskega sistema ali v ta namen ustanovljeni komisiji (prav tam).

3.2.4 Nadzor telefonskih pogovorov

Za opravljanje telefonskih pogovorov je treba najprej vzpostaviti klic, ki pa je v 25. točki 3. člena v ZEKom-1 opredeljen tako: »Klic je zveza, vzpostavljena s pomočjo javno dostopne elektronske komunikacijske storitve, ki omogoča dvosmerno govorno komunikacijo.«

Telefonski podatki so tudi prometni telefonski podatki in spadajo v skupino osebnih podatkov, ker se nanašajo na fizične osebe. Iz njih pa je tudi razvidno, katere telefonske številke je posameznik klical iz dodeljenega fiksnega ali mobilnega telefona. Razvidno je tudi, kdaj in s katere telefonske številke je bil klic opravljen, katera telefonska številka je bila poklicana in čas trajanja klica. Če želi delodajalec preveriti, katere telefonske številke je delavec klical, lahko pri telefonskem operaterju naroči izstavitev razčlenjenega računa. Operater ne preverja, zakaj je naročnik naročil razčlenjen račun, ker je namen le-tega določen v 91. členu ZEKom in v Splošnem aktu o razčlenjenem računu (Bien Karlovšek idr. 2008, 106).

Delodajalec nima pravice, da iz seznama klicanih telefonskih številk ugotavlja, kdo je lastnik določene telefonske številke. Izjema tega je, če se vnaprej v pogodbi ali sporazumu o uporabi službenega telefona to določi drugače. Bien Karlovšek idr. (2008, 108) govorijo o dopustnem namenu, ki je določen tudi po Ustavi RS in zakonodaji, in sicer o obračunu porabe telefonskih impulzov. Delodajalec in delavec lahko določita znesek mesečne porabe telefonskih impulzov službenega telefona. Če pride do prekoračitve omejitve mesečnih impulzov in se delavec odloči, da prekoračitve ne bo plačal, ampak bo dokazoval, da so bili opravljeni klici v višini prekoračenih impulzov potrebni za opravljanje delovnih nalog, se lahko izstavi višja stopnja razčlenjenega računa. Vendar le v taki obliki, da ni mogoče razpoznati identitete klicanih številk. To mu dopušča izrecna določba 7. odstavka 91. člena ZEKom.

Eden izmed pogostih razlogov prisluškovanja oziroma nadzora telefonskih pogovorov zaposlenih je sum, da delavec izkorišča službeni telefon za zasebne namene, pravita Cassily in Draper (2002, 8). Po drugi strani pa lahko delodajalec telefonskim pogovorom prisluškuje tudi takrat, ko se delavec pogovarja s strankami, ker želi na tak način zagotoviti večjo kakovost storitve. Če se telefonski pogovor snema za zagotavljanje večje kakovosti storitve, je stranka s tem seznanjena še pred začetkom pogovora. Takrat lahko snemanje tudi odkloni ali pa nadaljuje s pogovorom.

Pri izpisu klicanih in kličočih telefonskih številk, ki se nanašajo na službeno telefonsko številko, gre za obdelavo osebnih podatkov in za obdelavo podatkov v elektronskem komunikacijskem omrežju. V tem primeru imajo ti podatki dvojno varstvo: »varstvo tajnosti pisem in drugih občil po 37. členu Ustave RS in tudi varstvo osebnih podatkov po 38. členu Ustave RS« (Informacijski pooblaščenec 2012).

Dejstvo, da je telekomunikacija oprema v lasti delodajalca, ne predstavlja možnosti neupravičenega nadzora delavca (Lampe idr. 2007, 7/3-5). Prikrit vdor v komunikacijsko

zasebnost delavca brez pravne podlage je protipraven in predstavlja kaznivo dejanje, ki je lahko zaradi posega v osebnostne pravice delavca tudi predmet odškodninske odgovornosti.

Če bi delodajalec nezakonito posegel v komunikacijsko zasebnost zaposlenih, bi posegel tudi v ustavno zagotovljeno pravico tajnosti občil in varstva osebnih podatkov zaposlenih. V teh primerih pride tudi v poseganje pravic posameznikov z drugih strani oziroma v poseganje pravic posameznikov, ki so komunicirali z zaposlenimi. Tukaj se pojavi kolateralna oziroma neizogibna škoda (Bien Karlovšek idr. 2008, 99). Tak poseg v zasebnost je sprejemljiv le takrat, če je v skladu z zakonskimi določili.

3.2.5 Sledenje lokaciji

Sledenje lokaciji je omogočeno s pomočjo tehnologije GPS (angl. Global Positioning System) ki lahko določa položaj posameznika ali predmeta na zemlji (Bien Karlovšek idr. 2008, 61).

Sistem GPS sestavlja vsaj 24 satelitov, ki delujejo na sončno energijo, medtem ko krožijo okoli zemlje (Informacijski pooblaščenec 2015b).

Tehnologija lahko med drugim delodajalcu natančno določi lokacijo službenega vozila, kar varuje uporabnika vozila in tovor, olajša pa tudi upravljanje in vodenje poslovnih procesov. Tovrstna tehnologija pa lahko omogoča tudi vdor v zasebnost zaposlenega. Zato je uporaba takšne oblike nadzora dopustna le v primeru, ko so porabniki službenih vozil z GPS-sledenjem predhodno obveščeni o uporabi te tehnologije in ko so seznanjeni tudi z namenom zbiranja in načinom hranjenja zbranih podatkov. Naprave z GPS-sledenje vozil se lahko namestijo le v primeru, ko je to nujno za zavarovanje in zaščito premoženja podjetja. Za zaščito osebnih podatkov, pridobljenih pri GPS-sledenju in varovanju zasebnosti zaposleni, mora podjetje slediti ZVOPu in jasno določiti primere uporabe GPS-sledenja v internih aktih podjetja. Havliček (2015) tako izpostavlja, da delodajalec nima pravice sledenja službenim vozilom, ki jih lahko zaposleni uporabljajo tudi v zasebne namene.

Zato mora biti zaposlenim, ki ta vozila uporabljajo, omogočen izklop GPS-sledenja, ko začnejo uporabljati vozilo v zasebne namene. Bien Karlovšek idr. (2008, 62, 70, 72) navajajo primer, da delodajalci izkoriščajo GPS-tehnologijo sledenja tudi za nadzor prisotnosti oziroma odsotnosti z delovnega mesta. Takšno vrsto nadzora omogoča sledenje časa mirovanja GPS-signala. Ko avto miruje, lahko delodajalec predpostavlja, da ga je delavec zapustil in odšel na malico ali drugi zasebni opravek. GPS-sledilna tehnologija se ne sme uporabljati za ustvarjanje evidence, s pomočjo katere bi se lahko v določenem trenutku lahko ugotovil položaj delavca.

Informacijski pooblaščenec (2015b) izpostavlja, da obdelava osebnih podatkov posameznika, pridobljenih z uporabo GPS, ni posebej zakonsko urejena, zato je treba smiselno uporabljati temeljna načela varstva osebnih podatkov.

GPS-sledenje je mogoče tudi preko sledenja službenih mobilnih telefonov (Lampe idr. 2007, 7/5-2). V tem primeru prihaja do večjega posega v zasebnost in lokacijski podatki, pridobljeni s takim nadzorom, spadajo v skupino prometnih podatkov elektronskih komunikacij, ki imajo podobno pravno varstvo, kot izpiski klicanih in sprejetih številk.

3.2.6 Nadzor z biometrijo

Informacijski pooblaščenec (2008a) razlaga biometrijo, kot vedo o načinih, ki omogočajo prepoznavanje ljudi na podlagi telesnih, fizioloških in vedenjskih značilnostih, ki pa so edinstveni za vsakega posameznika. Značilnosti posameznika, kot so prstni odtis, podoba obraza, šarenica, očesna mrežnica ipd., omogočajo določitev identitete posameznika. Le-to pa lahko določimo tudi preko vedenjskih značilnostih posameznika, na primer lastnoročnega podpisa, barve glasu, gibanja ipd. (prav tam).

Biometrični sistemi lahko s pomočjo posebnih čitalnikov zajemajo biometrične vzorce (Newman 2010, 423). Takšni čitalniki zajete vzorce nato vstavijo v bazo podatkov, ki jo hranijo za kasnejšo uporabo, ko posamezne vzorce med seboj primerjajo. Pri branju oziroma primerjavi se sistem odloči, v kolikšni meri se vzorci medsebojno ujemajo. Na ta način lahko potrdijo ali ovržejo identifikacijo osebe.

Identiteta posameznika se preverja tako (Informacijski pooblaščenec 2008a), da oseba najprej sistemu sporoči, za koga se izdaja. To lahko stori z uporabo kartice (»nekaj, kar ima«), vnosom osebnega gesla ali vnosom PIN številke (»nekaj, kar ve«) in/ali z oddajo prstnega odtisa (»nekaj, kar je«). Pri biometričnem sistemu se uporablja postopek prepoznavanja na osnovi osebnih biometričnih značilnosti. Sistem na osnovi zajetih podatkov naredi primerjavo ponujenih biometričnih značilnosti in že vnaprej shranjenih biometričnih podatkov, ki pripadajo osebi, za katero se posameznik izdaja. Nato lahko sistem identifikacijo potrdi ali ovrže.

Delodajalci uporabljajo nadzor z biometrijo na delovnem mestu zaradi ugotavljanja in beleženja prisotnosti in odsotnosti delavcev in tudi za varovanje premoženja in opravljanja dejavnosti. Ker je nadzor z biometrijo hud poseg v zasebnost posameznika Bien Karlovšek idr. (2008, 74) opozarjajo, da je za uporabo biometrije pri nadzoru dela potrebno pridobiti odločbo Informacijskega pooblaščenca, ki predstavlja državni nadzorni organ za varstvo osebnih podatkov. Za vstop v varovane oddelke podjetja lahko delodajalci uporabijo biometrični čitalnik, ki se lahko uporablja tudi kot nadomestilo za ključ (Bien Karlovšek idr. 2008, 75). To pomeni, da se v sistem čitalnika vnesejo prstni odtisi posameznikov, ki imajo pravico vstopa v določen prostor.

Če delodajalci uporabljajo biometrijo kot način evidentiranja vstopa in izstopa delavca v posamezne prostore, lahko od posameznika zahtevajo, da navede določene osebne podatke in razloge za vstop in izstop. V določenih primerih se lahko zahteva preverjanje podatkov osebnega dokumenta. Osebni podatki iz evidence vstopov in izstopov se lahko hranijo do treh let od datuma vpisa, nato pa morajo biti izbrisani ali uničeni na drug način opozarjajo Pirc Musarjeva idr. (2006b).

Biometrija je pri nas pravno urejena z ZVOP-1 (Informacijski pooblaščenec 2008a) in sicer od 78. do 81. člena, kjer so opredeljene posebne vrste obdelave osebnih podatkov. Po zakonu se uporaba biometrije razlikuje glede na sektor uporabe. V javnem sektorju je uporaba dovoljena s posameznimi zakoni, na primer z Zakonom o potnih listinah (ZPLD-1-UPB4, *Ur.l. RS,* št. 29/2011, 213-03/11-1/2). Izjema je opredeljena na podlagi posebnih zakonskih določil za vstop v stavbo ali dele stavb in za evidentiranje zaposlenih. V zasebnem sektorju se uporaba biometrije dovoli le, če je to nujno potrebno za: »opravljanje dejavnosti, varnosti ljudi ali premoženja, varovanje tajnih podatkov ali varovanje poslovne skrivnosti.«

Lampe idr. (2007, 8/3-2) kot tveganje uporabe biometrije omenjajo krajo identitete posameznika. V primeru kraje potnega lista se le-ta lahko prekliče, če pa nekdo posamezniku ukrade prstni odtis, preklic ni mogoč. Druga nevarnost je možnost okužbe z nalezljivimi boleznimi pri uporabi biometričnega čitalnika.

4 NADZOR ZAPOSLENIH IN ZASEBNOST – REZULTATI RAZISKAVE

Raziskavo o nadzoru zaposlenih in varovanju zasebnosti smo opravili med delodajalci in med študenti. Obe raziskavi smo opravili s pomočjo ankete, ki smo jo pripravili s pomočjo spletnega orodja 1KA.[5]

4.1 Potek raziskave in predstavitev vzorca raziskave

Zbiranje podatkov je potekalo preko spletnega vprašalnika. Pripravili smo dva različna vprašalnika in sicer za študente in za delodajalce. V prvi skupini smo se omejili na študente Univerze na Primorskem, Fakultete za management (UP FM), ki opravljajo ali so opravljali študentsko delo. V drugi skupini pa smo anketirali podjetja iz Obalno-kraške regije, ki poleg redno zaposlenih zaposlujejo tudi študente. Anketirancem smo povezavo do ankete posredovali preko elektronskih naslovov in družabnega omrežja Facebook.

4.1.1 Anketiranje študentov

Vprašalnik za študente (Priloga 1) je vseboval 22 vprašanj različnih tematskih sklopov. Vprašanja so bila razdeljena v naslednje kategorije: študentsko delo (sedem vprašanj), opravljanje dela (pet vprašanj) ter nadzor in zasebnost na delovnem mestu (sedem vprašanj). Ob zaključku ankete smo zbrali še nekaj osebnih podatkov (tri vprašanja).

Kot je že bilo omenjeno, so vprašalnike izpolnjevali študentje UP FM, ki so opravljali ali opravljajo študentsko delo. Anketiranje je potekalo od 15. 10. 2015 do 30. 11. 2015. V tem času smo zbrali 72 polno izpolnjenih vprašalnikov. Več kot polovico vprašalnikov so izpolnile ženske (57 %). Povprečna starost anketiranega študenta je bila 23,6 leta.

V anketi je sodelovalo največ študentov s statusom absolventa (46 %). Zastopanost študentov glede na letnik je razvidna iz preglednice 1.

[5] Http://www.1ka.si

Preglednica 1: Letnik študija anketiranih študentov

Letnik študija:	Število	Delež v %
1. letnik	3	4 %
2. letnik	17	23 %
3. letnik	19	26 %
Absolvent	33	46 %
Skupaj	72	100 %

4.1.2 Anketiranje delodajalcev

Vprašalnik za delodajalce je vseboval 15 vprašanj, različnih tematskih sklopov. Vprašanja so bila razdeljena v tri skupine: nadzor dela (sedem vprašanj), zasebnosti zaposlenih na delovnem mestu (eno vprašanje) in splošna vprašanja o delodajalcu (sedem vprašanj). Zbrali smo 35 polno izpolnjenih anketnih vprašalnikov.

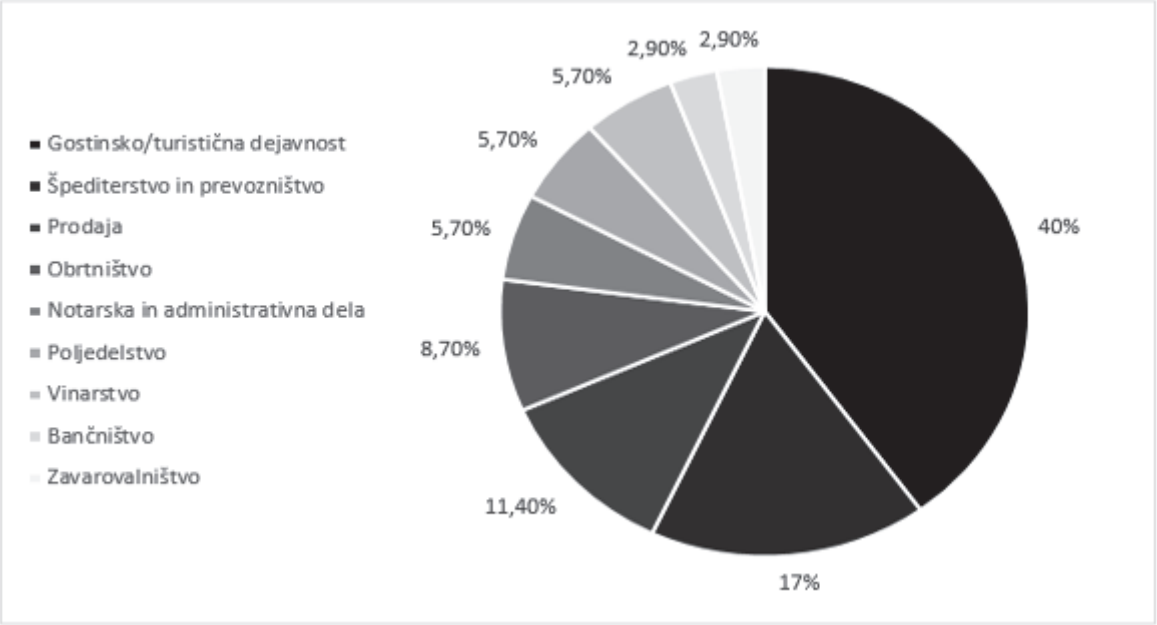
Anketiranje je potekalo od 15. 10. 2015 do 30. 11. 2015.

Povprečno število redno zaposlenih anketiranih podjetjih je 17,2. Med anketiranimi podjetji je največ redno zaposlenih imelo podjetje s 54 delavci, eno podjetje pa je redno zaposlovalo le enega delavca. Tako je bilo 60 % podjetij z med 10 in 20 redno zaposlenimi delavci.

Anketirana podjetja zaposlujejo različno število študentov. Povprečno število študentov v podjetjih je 2,6. Največ zaposlenih študentov v posameznem podjetju je bilo 18, najmanj pa eden zaposlen, in sicer v enem podjetju. Večina podjetij (68 %) zaposluje med 2 in 5 študentov.

Najstarejše anketirano podjetje je bilo ustanovljeno leta 1989, najmlajše pa leta 2014. Več kot polovica anketiranih podjetij (57 %) je bilo ustanovljenih med letoma 2000 in 2009.

Anketirana podjetja smo spraševali po dejavnostih, ki jo opravljajo. Največ anketiranih podjetij (40 %) se ukvarja z gostinsko/turistično dejavnostjo. Strukturo podjetij glede na dejavnost prikazujemo na sliki 1.



Slika 1: Dejavnosti anketiranih podjetij

4.2 Predstavitev rezultatov raziskave

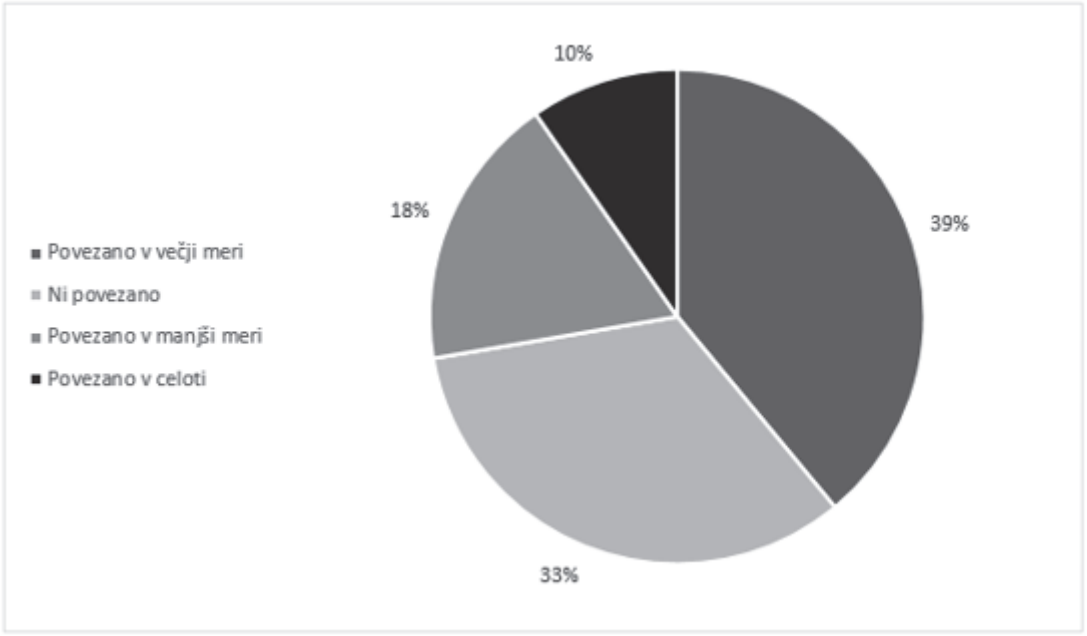
Rezultate raziskave predstavljamo ločeno, in sicer za študente in za delodajalce. V zaključnem delu naloge sledi analiza zbranih rezultatov in interpretacija ugotovitev.

4.2.1 Študentsko delo študentov

Najprej smo študente vprašali, kdaj so začeli opravljati študentsko delo. Največ anketiranih študentov (46 %) je delo preko študentskega servisa začelo opravljati med 16. in 17. letom, torej še v dijaških letih. Četrtina anketiranih študentov (25 %) je začela delo opravljati v prvem letniku fakultete, 11 % pa v drugem letniku fakultete. Slaba petina anketiranih študentov (18 %) je študentsko delo začela opravljati, ko so se odselili od staršev, kar lahko povežemo z začetkom študija in odhodom na fakulteto.

V nadaljevanju smo želeli izvedeti, kakšni so bili njihovi razlogi za začetek opravljanja študentskega dela. Velika večina (79,2 %) anketiranih študentov je študentsko delo začela opravljati iz finančnih razlogov. Anketirani študentje so želeli postati neodvisni (12,5 %) ali pa so hoteli svoj prosti čaj nameniti za koristno dejavnost (8,3 %).

Zanimalo nas je, ali je delo študentov povezano z njihovo izobrazbo oziroma z njihovim študijem. Tako je delo 39 % anketiranih študentov v večji meri povezano z njihovim študijem (Slika 2).



Slika 2: Povezava študija z izbranim študentskim delom

Študentje se za vrsto študentskega dela odločajo na osnovi različnih dejavnikov. Največ študentov (43 %) je študentsko delo, ki so ga opravljali v času anketiranja, izbralo, ker so v podjetju iskali študente in imeli za njih razpoložljiva delovna mesta. Naslednji najbolj zastopan dejavnik (34,8 %) za izbor študentskega dela so bili urna postavka, urnik dela in lokacija dela. Ostali študentje (22,2 %) so študentsko delo izbirali na osnovi želje po pridobivanju izkušenj na področju študija. Študentsko delo zaradi pridobivanja delovnih izkušenj v povezavi s študijem je torej šele na zadnjem mestu.

Anketirani študentje so do časa anketiranja opravljali različno število priložnostnih del. V povprečju je študent opravljal 6,2 različnih študentskih del. Več kot polovica anketiranih študentov (54,2 %) je opravljala od tri do šest različnih študentskih del.

Dobra polovica anketiranih študentov (56 %) je študentsko delo odpravljala tudi v času anketiranja, kar pomeni, da opravljanje študentskega dela ni vezano samo na čas študentskih počitnic.

V anketi smo zbrali tudi mnenja o počutju študentov pri opravljanju zadnjega študentskega dela. Večina anketiranih študentov (68 %) se je pri opravljanju zadnjega študentskega dela počutila odlično. Ostali študentje (32 %) se na delovnem mestu niso počutili dobro. Razlogi, ki so jih navedli za dobro oziroma slabo počutje so razvidni iz priloge 3.

V podjetjih lahko študentje opravljalo iste delovne naloge kot redno zaposleni ali pa jim delodajalci zaupajo manj zahtevna dela. Več kot polovica anketiranih študentov (67 %) je opravljala iste delovne naloge kot redno zaposleni, 14 % anketiranih študentov pa je opravljalo drugačna dela, kot jih opravljajo redno zaposleni. Slaba petina anketiranih študentov (19 %) pa ni vedela, če so opravljali iste delovne naloge kot redno zaposleni.

Če študentje niso opravljali istih delovnih nalog kot redno zaposleni delavci, so odgovorili še na vprašanje, ali so se pozanimali za razloge, zakaj jim delodajalci niso dodelili istih delovnih nalog, kot jih opravljajo redno zaposleni. Od vseh anketiranih študentov 14 % študentov ni zanimalo, zakaj prihaja do razlik.

Študentje običajno lahko opravljajo ista dela kot redno zaposleni delavci. Več kot četrtina anketirancev (26,4 %) ocenjuje, da trditev »študentje opravljajo ista dela kot redno zaposleni delavci« v večji meri drži, dodatnih 12,5 % pa ocenjuje, da trditev popolnoma drži. Strinjanje s trditvijo so anketiranci ocenili s povprečno oceno 3,0, kar predstavlja precej nevtralno oceno. Tudi če študentje in zaposleni opravljajo ista dela, to še ne predstavlja istih pravil za obe skupini. Zato smo v nadaljevanju ankete želeli izvedeti, če prihaja do razlik.

Največ (29,7 %) študentov je odgovorilo, da se pravila ne razlikujejo. Tudi pri tem vprašanju smo izračunali povprečno oceno strinjanja s trditvijo o enakosti pravil za redno zaposlene in študente, ki pa je nekoliko nižja (2,9), vendar še vedno dokaj nevtralna.

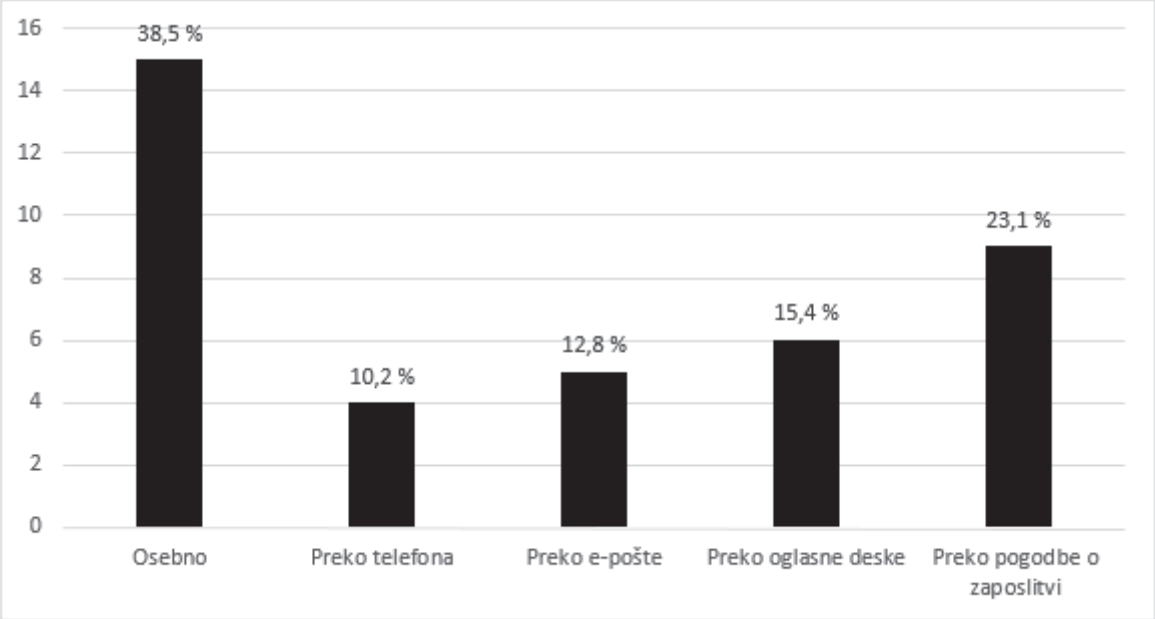
V naslednjem sklopu vprašanj so študentje odgovarjali na vprašanja o nadzoru na delovnem mestu. Najprej smo jih vprašali, če so bili obveščeni o nadzoru na delovnem mestu. Nekaj več kot polovica anketirancev (54 %) je bila o nadzoru na delovnem mestu obveščena, medtem, ko drugi (46 %) niso bili obveščeni ali pa nadzora na delovnem mestu ni bilo.

V nadaljevanju smo od študentov, ki so bili obveščeni o nadzoru dela na delovnem mestu, želeli izvedeti, kdaj so jih delodajalci o tem obvestili. Največ anketiranih študentov (51,3 %) je bilo o nadzoru na delovnem mestu obveščenih pred začetkom dela. Vrednosti ostalih odgovorov pa predstavljamo v preglednici 2.

Preglednica 2: Obveščanje študentov o nadzoru dela

Obvestilo o nadzoru	Število	Odstotek
Pred začetkom dela	20	51,3 %
Ob začetku dela	14	35,9 %
Med opravljanjem dela	5	12,8 %
Skupaj:	39	100 %

Tisti študentje, ki so bili obveščeni o nadzoru na delovnem mestu, so v naslednjem vprašanju odgovarjali o načinu obveščanja. Primerjava teh načinov obveščanja je prikazana na sliki 2. Največ anketiranih študentov (38,5 %) je bilo obveščenih osebno. Pri tem vprašanju so lahko anketirani študentje izbrali več različnih načinov obveščanja o nadzoru.



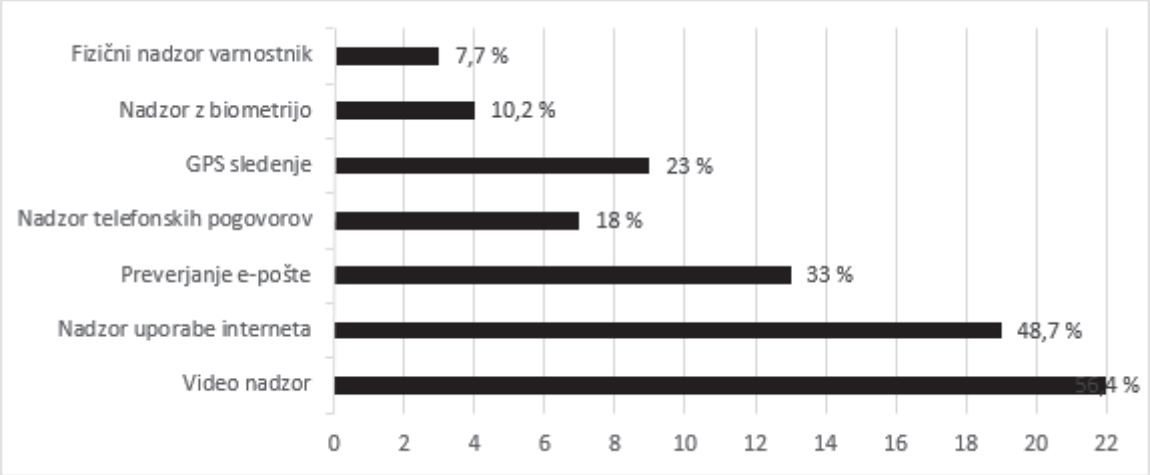
Slika 3: Načini obveščanja študentov o nadzoru dela

Zanimalo nas je, kaj menijo študentje o pravici delodajalca za nadzor delavcev med delom. Največ anketiranih študentov (41 %) ni prepričanih, da ima delodajalec pravico do tovrstnega nadzora. Samo dve odstotni točki manj (39 %) pa je odgovorilo, da ima delodajalec pravico do nadzora na delovnem mestu. Preostali anketirani študentje (20 %) pa menijo, da delodajalec zaposlenih ne sme nadzirati.

Nekatera delovna mesta zahtevajo nadzor dela, druga pa nadzora ne potrebujejo. Anketirani študentje so podali svoje mnenje o potrebnosti nadzora na delovnem mestu. Največ študentov (68 %) meni, da je nadzor dela odvisen od narave dela, medtem ko je 13 % anketiranih študentov mnenja, da nadzor na delovnem mestu ni potreben. Preostalih 19 % anketiranih študentov se je strinjalo, da je tovrsten nadzor potreben.

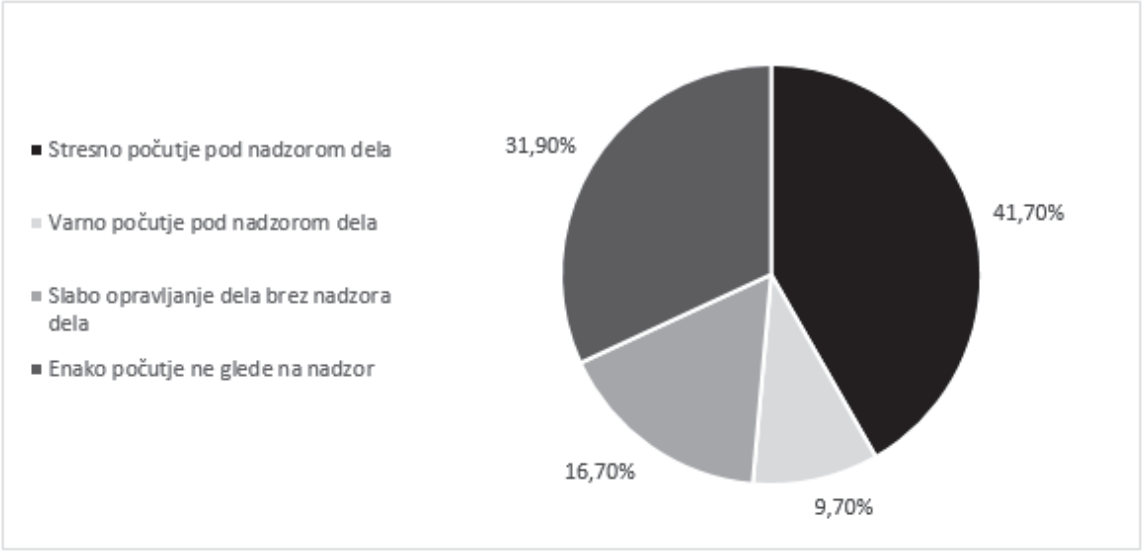
Glede na predvidevanja, da so se študentje pri svojem delu že srečali z nadzorom dela na delovnem mestu, nas je zanimala oblika nadzora, s katero so imeli izkušnje. Delodajalci anketiranih študentov, najpogosteje (56,4 %) zaposlene na delovnem mestu nadzorujejo z video nadzorom, najredkeje (7,7 %) pa z osebnim nadzorom oziroma fizičnim nadzorom varnostnika. Pri tem vprašanju so lahko anketirani študentje izbrali več različnih oblik

nadzora dela, če je njihov delodajalec uporabljal več kot eno omenjeno obliko. Kar tretjina (30,7 %) delodajalcev pri nadzoru dela uporablja tri različne načine nadzora, in sicer video nadzor ter nadzor uporabe interneta in elektronske pošte. Na sliki 4 prikazujemo zastopanost načinov nadzora dela.



Slika 4: Načini nadzora, s katerimi so se srečali študentje

Zadnje vprašanje je bilo namenjeno ugotavljanju počutja na delovnem mestu, na katerem so se študentje srečali z nadzorom dela, ter počutja na nenadzorovanem delovnem mestu. Največ študentov (41,7 %) nadzor dela povezuje s stresom. Tisti, ki so opravljali delo pod nadzorom, so se počutili nadzorovano, nelagodno in pod stresom. Drugi (9,7 %), ki so prav tako opravljali delo pod nadzorom, pa so se počutili varno, saj so opravljali nevarno delo in je narava dela zahtevala nadzor. V primerih, ko niso bili pod nadzorom, so nekateri študentje (16,7 %) zapisali, da so svoje delo opravljali slabše. Ker med delom ni bilo kontrole, je motivacija upadala, splošno počutje pa je bilo boljše. Skoraj tretjina anketiranih študentov (31,9 %) se je na delovnem mestu, ne glede na to, ali se je izvajal nadzor ali ne, počutila enako, saj so bili prepričani o svojih sposobnostih opravljanja zadanega dela.

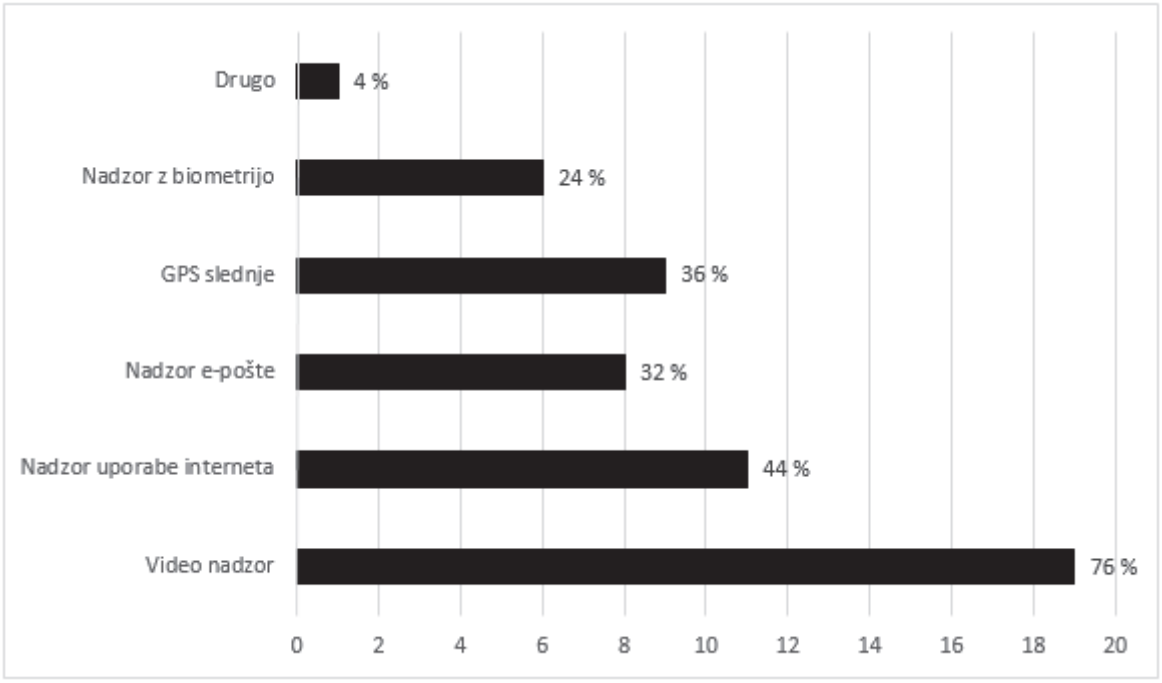


Slika 5: Ugotavljanje počutja na delovnem mestu pri delu nadzorovanem in nenadzorovanem delu

4.2.2 Anketirani delodajalci

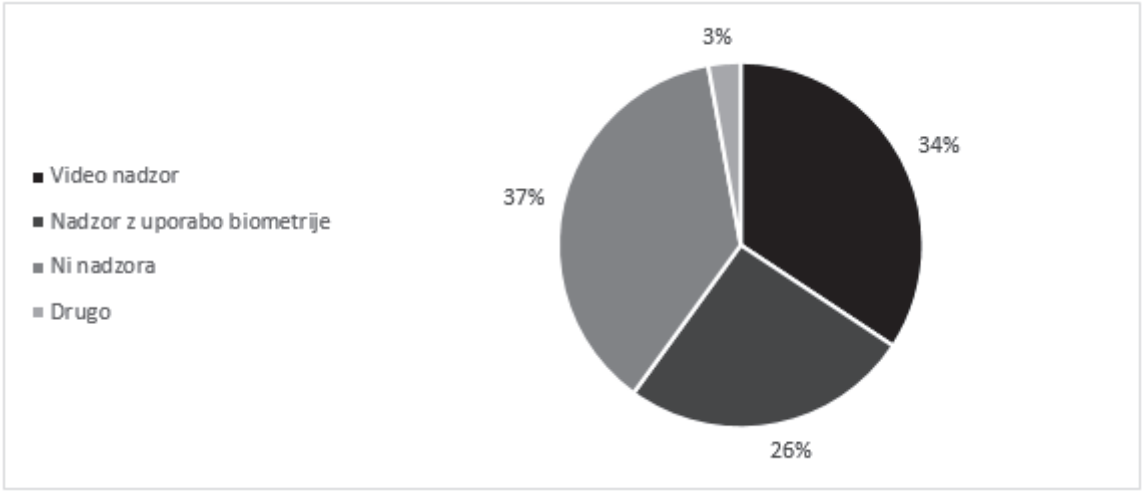
Kot smo že omenili, je v anketi sodelovalo 35 delodajalcev. 71,4 % anketiranih delodajalcev uporablja nadzor dela na delovnem mestu, 28,6 % anketiranih delodajalcev pa tovrstnega nadzora ne uporablja. Delodajalci nadzor uporabljajo za nadzor zaposlenih (nadzor dela) in za nadzor delovnih prostorov.

Delodajalce smo najprej vprašali, katere oblike nadzora dela uporabljajo. Odgovorili so, da je to najpogosteje video nadzor (76 %), najredkeje pa nadzor z biometrijo (24 %). 28 % anketiranih delodajalcev uporablja tri različne načine nadzora, in sicer video nadzor, nadzor uporabe interneta in nadzor e-pošte. Anketiranci so pri tem vprašanju lahko vpisali tudi obliko nadzora dela, ki je nismo predvideli. Samo eno podjetje je podalo odgovor na to vprašanje, in sicer, da za nadzor dela uporabljajo varnostnika. Na sliki 5 prikazujemo zastopanost načinov nadzora dela.



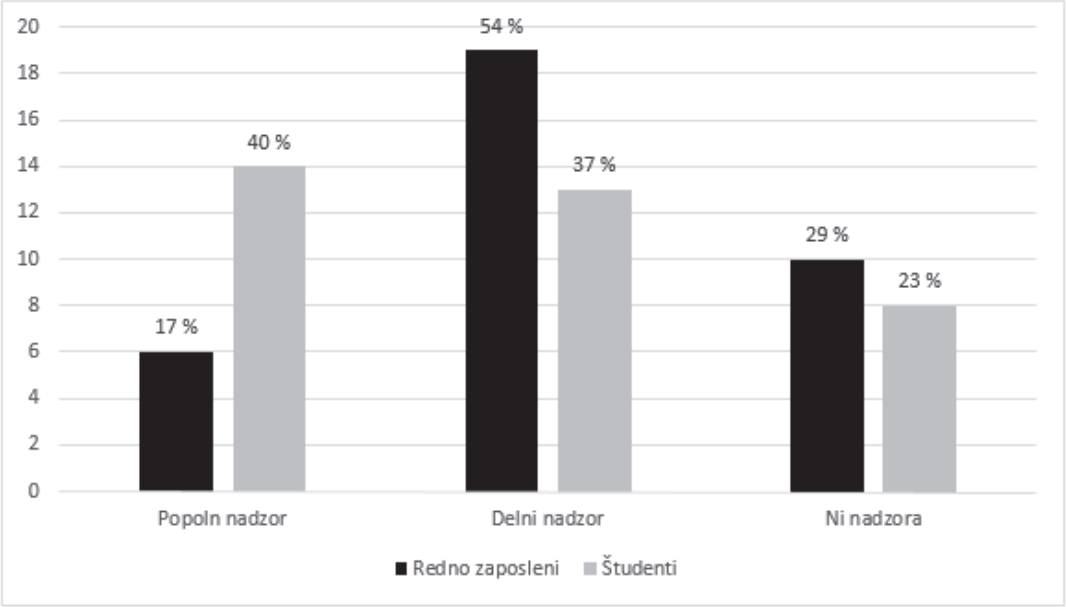
Slika 6: Načini nadzora dela

V nadaljevanju nas je zanimal še nadzor delovnih prostorov. Delovne prostore delodajalci največkrat nadzorujejo z video nadzorom (34 %) ali pa jih sploh ne nadzorujejo (37 %) (Slika 7).



Slika 7: Načini nadzora delovnih prostorov

V nadaljevanju nas je zanimalo, ali delodajalci pri nadzoru dela redno zaposlenih delavcev in študentov posegajo po različnih metodah. Kot je razvidno iz slike 6, več podjetij vrši več popolnega nadzora nad študenti (40 %), medtem ko je več delnega nadzora nad redno zaposlenimi (54 %).



Slika 8: Primerjava med nadzorom dela redno zaposlenih in študentov

Delavci morajo biti o nadzoru na delovnem mestu obveščeni, zato nas je zanimalo, kako in kdaj delodajalci zaposlene o tem obveščajo. 71,4 % anketiranih delodajalcev je zaposlene o nadzoru dela obveščajo, preostalih 28,6 % pa tega ni storilo.

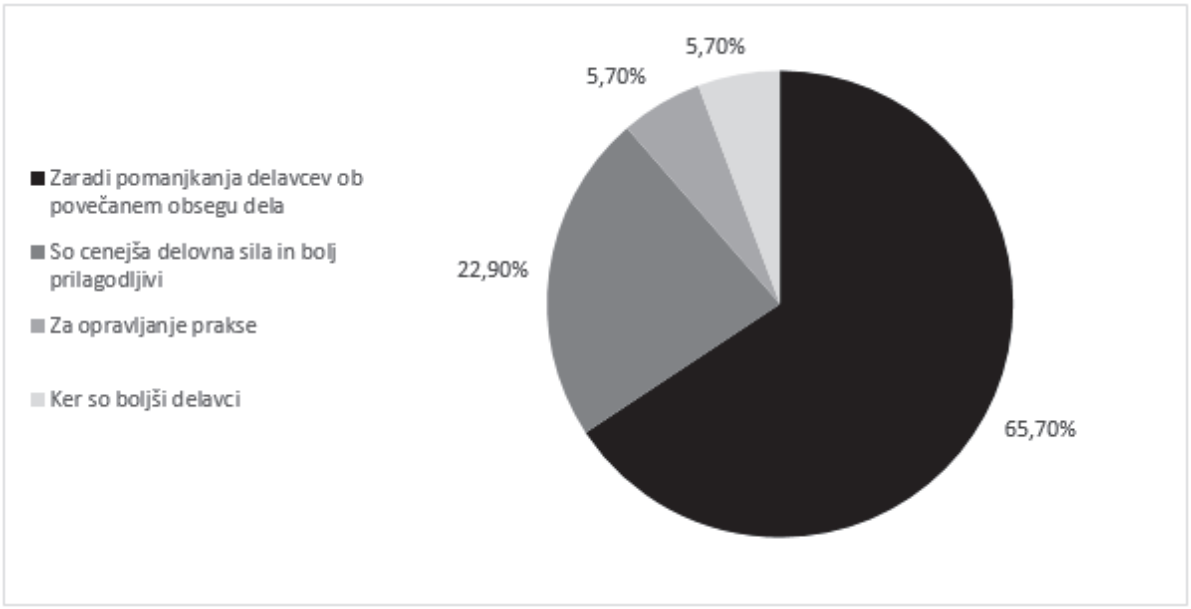
Zaposleni so o nadzoru dela najpogosteje (48 %) obveščeni pred začetkom opravljanja dela, sledi obveščanje (28 %) med opravljanjem dela in obveščanje takoj po začetku opravljanja dela (24 %).

Tisti delodajalci, ki so zaposlene obveščali o nadzoru dela na delovnem mestu, so odgovorili še na vprašanje o načinu obveščanja. Delavci so bili najpogosteje (76 %) obveščeni pisno preko pogodbe o zaposlitvi, sledijo osebno/ustno (60 %) obveščanje, obveščanje (16 %) preko oglasne deske in obveščanje (8 %) preko elektronske pošte. Malo manj kot polovica (48 %) delodajalcev hkrati uporablja dva načina za obveščanje, in sicer oseben način obveščanja in pisni način obveščanja preko pogodbe o zaposlitvi.

V nadaljevanju smo delodajalce vprašali za mnenje o zadovoljstvu delavcev z nadzorom dela. Po mnenju delodajalcev je tretjina zaposlenih (32 %) z nadzorom dela na delovnem mestu zadovoljna, medtem ko jih je petina (21 %) nezadovoljna. 26 % anketirancev je izrazilo neodločenost.

Čeprav je zasebnost na delovnem mestu opredeljena v zakonodaji, nas je zanimalo, kaj o tem mislijo delodajalci. Tri četrtine anketiranih delodajalcev (74 %) meni, da imajo njihovi zaposleni dovolj zasebnosti na delovnem mestu, medtem ko so drugi (26 %) podvomili o zadostni zasebnosti zaposlenih na delovnem mestu.

Delodajalci zaposlujejo študente ob različnih priložnostih. Anketirana podjetja so študente največkrat zaposlovala zaradi pomanjkanja delavcev ob povečanem obsegu dela (65, 7 %). Drugi najbolj pogost razlog (22,9 %) za zaposlovanje študentov pa je dejstvo, da so študentje cenejša delovna sila in da so glede delovnega urnika bolj prilagodljivi. Med anketiranimi podjetji 5,7 % študente zaposluje za potrebe opravljanja (obvezne) študentske prakse. Zanimiv je podatek, da 5,7 % anketiranih delodajalcev študente zaposluje zaradi prepričanja, da so študentje pri delu boljši od redno zaposlenih delavcev (Slika 9).



Slika 9: Razlogi za zaposlovanje študentov

Delodajalce smo nato še prosili, da opredelijo čas zaposlovanja študentov. 48,6 % anketiranih delodajalcev študente zaposluje po potrebi, in sicer v primeru povečanega obsega dela. 34,3 % anketiranih delodajalcev študente zaposluje skozi vse leto, medtem ko jih 17,1 % anketiranih delodajalcev zaposluje le v času letnih dopustov redno zaposlenih delavcev ali v primeru (daljše) bolniške odsotnosti redno zaposlenih delavcev.

Pri zadnjem vprašanju so se delodajalci opredelili glede zadovoljstva z zaposlenimi in študenti. Polovica anketiranih (51,4 %) je odgovorila, da so redno zaposleni boljši delavci, medtem ko je 34,3 % navedlo, da med redno zaposlenimi delavci in študenti ni razlik. Po mnenju 14,3 % anketirancev pa so študentje boljši delavci od redno zaposlenih.

4.3 Preverjanje hipotez

Hipoteza 1: Delodajalci pri nadzoru dela redno zaposlenih delavcev in študentov posegajo po različnih metodah.

To hipotezo smo preverjali s vprašanji o načinu nadzora dela za redno zaposlene delavce in za študente. Pri obeh vprašanjih so delodajalci navedli, če izvajajo popolni nadzor, delni nadzor oziroma nadzora ne uporabljajo. 51 % delodajalcev za obe skupini zaposlenih uporablja isti način nadzora dela, 49 % pa uporablja različne načine nadzora.

Posledično te hipoteze ne moremo potrditi, saj je večji delež (51 %) tistih delodajalcev, ki uporablja isti način nadzora dela za obe skupini delavcev.

Hipoteza 2: Več kot tretjina anketiranih podjetij krši pravice glede zasebnosti zaposlenih.

Zasebnost zaposlenih na delovnem mestu je lahko kršena v primerih, ko zaposleni niso obveščeni o nadzoru na delovnem mestu, ko delodajalec ne uporabi pravilnega načina obveščanja zaposlenih o nadzoru na delovnem mestu ter ko delodajalec izvaja nepravilen nadzor dela. To hipotezo smo preverjali z vprašanjem o zadovoljstvu zaposlenih z nadzorom dela. Tretjina (32 %) vseh anketiranih delodajalcev je odgovorila, da so zaposleni zadovoljni z nadzorom dela oziroma imajo do nadzora nevtralno stališče (26 %). Za potrjevanje te hipoteze smo delodajalce vprašali še, ali menijo, da je njihovim zaposlenim na delovnem mestu zagotovljeno dovolj zasebnosti. Kar 72 % vseh anketiranih je na to vprašanje odgovorilo pritrdilno.

Glede na zbrane odgovore te hipoteze ne moremo potrditi.

Hipoteza 3: Več kot tretjina anketiranih podjetij svojih delavcev ne obvešča o nadzoru in jim v podpis ne izroči soglasja o nadzoru pri delu.

To hipotezo smo preverjali z več vprašanji iz vprašalnika za delodajalce in iz vprašalnika za študente. Pri delodajalcih smo preverjali, kako in kdaj svoje zaposlene obveščajo o nadzoru dela. 28,6 % anketiranih delodajalcev zaposlenih o nadzoru dela ne obvešča, 71,4 % anketiranih delodajalcev pa zaposlene obvešča. Tisti delodajalci, ki obveščanje izvajajo, delavce (48 %) obvestijo pred začetkom dela, sledi (28 %) obveščanje med opravljanjem dela in obveščanje (24 %) po začetku opravljanja dela. V nadaljevanju so delodajalci odgovarjali na vprašanje o načinu obveščanja delavcev o nadzoru dela. 76 % anketiranih podjetij je odgovorilo, da zaposlene obveščajo preko pogodbe o zaposlitvi. Po zakonu ZDR (Zakon o delovnih razmerjih) bi delodajalci zaposlene z nadzorom dela morali seznaniti v pogodbi o zaposlitvi, ki jo podpišeta tako delodajalec kot zaposleni. Torej več kot večina (76 %) anketiranih delodajalcev dela po pravilih in spoštuje ZDR.

Hipotezo glede obveščanja o nadzoru na delovnem mestu smo preverjali tudi z odgovori na vprašanja iz vprašalnika za študente. Podani odgovori so bili skoraj enaki, saj je 55 % anketiranih študentov potrdilo, da so bili obveščeni o nadzoru na delovnem mestu, medtem ko jih 45 % ni bilo obveščenih. Študentje so odgovarjali tudi na vprašanje o načinu obveščanja delodajalca o nadzoru dela. Študentje, ki so bili obveščeni o nadzoru dela, so bili največkrat (38,5 %) obveščeni osebno. Predvidevamo, da pri tem v podpis niso dobili soglasja o nadzoru dela, saj so bili obveščeni samo osebno oziroma ustno. Malo več kot polovica (51,3 %) anketiranih študentov je bila o nadzoru na delovnem mestu obveščena pred začetkom opravljanja dela. Sledilo (35,9 %) je obveščanje ob začetku opravljanja dela in nato še obveščanje (12,8 %) med opravljanjem dela.

Glede na odgovore obeh vprašalnikov te hipoteze ne moremo potrditi, saj se mnenja študentov in delodajalcev razlikujejo.

Hipoteza 4: Učinkovitost nadzorovanih delavcev je slabša, saj so pod stresom.

To hipotezo smo preverjali z vprašanjem o splošnem počutju na zadnjem študentskem delu, na katerega je večina študentov (68 %) odgovorila, da je bilo počutje na študentskem delu odlično. Preostali anketirani študentje (32 %) pa so odgovorili, da je bilo počutje neznosno oziroma preveč nadzorovano. Primerjali smo tudi, če se počutje na delovnem mestu pri opravljanju dela pod nadzorom razlikuje od počutja pri opravljanju nenadzorovanega dela. Iz podanih odgovorov lahko razberemo, da so bili nadzorovani študentje pod stresom in so se počutili nadzorovane (41,7 %). Tretjina študentov (31,9 %) je bila glede nadzora na delovnem mestu neopredeljena, saj so bili prepričani v svoje sposobnosti opravljanja zadanega dela. Nenadzorovani študentje (16,7 %) so priznali, da so svoje delo opravljali slabše in nemotivirano, saj ni bilo kontrole. V primeru, da je narava dela zahtevala nadzor dela, so se študentje (9,7 %) počutili varno.

Glede na podane odgovore obeh vprašanj lahko hipotezo potrdimo.

5 SKLEP

IKT je orodje, ki pomaga pri doseganju poslovnih ciljev, pri izboljšanju poslovnih procesov ter pri izboljšanju kakovosti storitev in izdelkov. Razvita IKT pa lahko zaradi nepravilne rabe predstavlja tudi grožnjo posameznikom, podjetjem in družbi. Tako se neustrezna raba IKT kaže pri nepravilnem načinu nadzora delavcev ter pri izkoriščanju njene zmogljivosti za pridobivanje osebnih podatkov, ki niso ključni za poslovanje.

Z razvitostjo IKT se je povečalo število nedovoljenih in nepotrebnih posegov v zasebnost. Zasebnost je pomembna prvina človekovega življenja in predstavlja nekaj, kar je vsakemu posamezniku edinstveno. V zasebnem okolju lahko sami poskrbimo za svojo zaščito oziroma se sami odločimo, v kolikšni meri bomo IKT uporabljali za komunikacijo, posredovanje podatkov preko družabnih omrežij ipd.

Drugače pa je v službenem okolju, kjer zaradi velikega razvoja IKT obstaja več možnosti za nadzor dela in posledično za kršitev pravice do zasebnosti. Delodajalci stremijo k povečanju dobička in k učinkovitejšem izkoriščanju delovne sile. Pri tem morebiti začnejo nadzorovati delavce preko meje dovoljenega in s tem posegajo v njihovo zasebnost. Zaradi tega lahko delavci postanejo ranljivi, njihovo delo pa nazaduje.

V empiričnem delu naloge smo opravili raziskavo med podjetji iz Obalno-kraške regije in študenti UP FM. Podatke smo zbirali z uporabo anketnih vprašalnikov. Anketiranje je potekalo med 15. 10. 2015 in 30. 11. 2015. V anketo je bilo vključenih 35 različnih podjetij in 72 študentov.

Anketirani študentje se za delo preko študentske napotnice najpogosteje odločijo iz finančnih razlogov (79,2 % anketiranih študentov), delo pa začnejo opravljati takoj, ko je to dovoljeno oziroma, ko dopolnijo16 let (30 % anketiranih študentov).

Pri izbiri študentskega dela prevladuje višina urne postavke, urnik dela in lokacija (34,8 %) ter dejstvo, da številna podjetja za opravljanje različnih del pogosteje iščejo izključno študente. Študentska delovna sila je cenejša in bolj prilagodljiva, zlasti glede delovnega urnika (22,9 %). Nekaj več kot polovica anketiranih študentov (54,2 %) je opravljala že različna študentska dela, natančneje od treh do šest del.

Glede na to, da veliko študentov opravlja različna študentska dela in da razvoj IKT omogoča različne načine nadzora na delovnem mestu, nas je zanimalo, ali obstajajo razlike pri nadzoru redno zaposlenih in študentov.

Na osnovi analize zbranih odgovorov smo spoznali, da do takšnih razlikovanj dejansko prihaja. Iz analize je razvidno, da delodajalci za nadzor redno zaposlenih delavcev uporabljajo delni nadzor dela (54 %), za nadzor študentov pa popolni nadzor dela (40 %).

V zadnjih letih je bil nadzor dela pogosto tematiziran, zlasti nepravilen nadzor dela in kršitve pravice do zasebnosti zaposlenih na delovnem mestu. Raziskali smo, kako so se študentje počutili na nadzorovanem in nenadzorovanem delovnem mestu. Analiza podatkov je pokazala, da se je 41,7 % študentov, ki so bili pod nadzorom dela, počutilo nelagodno in stresno. Kljub temu se je 9,7 % anketiranih študentov počutilo varno, saj so menili, da sama narava njihovega dela zahteva nadzor. Primeri takih delovnih mest so banke, zavarovalnice, trgovine ipd.

Na nenadzorovanem delovnem mestu so se študentje počutili odlično, vzdušje pa je bilo bolj sproščeno (31,9 %). Po drugi strani pa so priznali, da so svoje delo opravljali malomarno, saj jih nobeden ni nadzoroval (16,7 %).

Z raziskavo smo tudi ugotavljali, kaj anketiranci menijo o zasebnosti na delovnem mestu. Na osnovi podatkov ugotavljamo, da je tretjina zaposlenih (32 %) zadovoljna s stopnjo zasebnosti, ki jo imajo na delovnem mestu, medtem ko je petina anketirancev (21 %) izrazila nezadovoljstvo. Preostali (26 %) pa so izrazili nevtralnost oziroma glede tega niso podali odgovora.

Ker ta tematika še ni dovolj raziskana, bi pri nadaljnji raziskavi vključila večje število udeležencev in tudi redno zaposlene delavce. Pri empiričnem delu bi opravljala tudi intervjuje, s katerimi bi lahko bolj poglobljeno analizirala raziskovalna vprašanja in tako pripomogla k razvoju novih spoznanj.

LITERATURA

Beniger, R. James. 1986, *The Control Revolution: technological and economic origins of the information society.* Cambridge, Massachusetts, London: Harvard University Press.

Bien, Karlovšek, Sonja, Alenka Jerše, Klemen Mišič, Nataša Pirc Musar, Jasna Rupnik in Andrej Tomšič. 2008. *Zasebnosti delavcev in interesi delodajalcev – kje so meje?*. Ljubljana: Uradni list Republike Slovenije.

Brulc, Urban. 2014. Meje varstva osebnih podatkov v delovnih razmerjih: nekatere vrste tehničnega nadzora. *HRM – strokovna revija za ravnanje z ljudmi pri delu.* 12 (60).

Cassilly, H. Lisa in Clare Draper. 2002. *Privacy in the Workplace: A Guide for Attorneys and HR Professionals.* Silver Spring, Maryland: Pike & Fisher. Inc.

Cate, H. Fred. 1997. *Privacy in the Information Age.* Washington: Brookings Institution Press.

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

Čebulj, Janez. 1992. *Varstvo informacijske zasebnosti v Evropi in Sloveniji.* Ljubljana: Inštitut za javno upravo pri Pravni fakulteti.

Davies, J. Sandi., Christopher A. Hertig in Brion P. Gilbride. 2015. *Security supervision and management – Theory and Practice of Asset Protection.* Waltham, USA: Elsvier Inc.

FindLaw. 2014. *Privacy in the Workplace: Overview.* Http://employment.findlaw.com/workplace-privacy/privacy-in-the-workplace-overview.html (13. 9. 2014).

Havliček, Mojca. 2015. *Gps sledenje službenim vozilom*. Http://www.pravo-kadri.si/arhiv-clankov/15-splosno/27-gps-sledenje-sluzbenim-vozilom (30. 12. 2015).

Informacijski pooblaščenec. 2006. *Delodajalčev nadzor elektronske pošte in dostopa do interneta zaposlenega.* Http://www.ip-rs.si/vop/delodajalcev-nadzor-elektronske-poste-in-dostopa-do-interneta-zaposlenega-215/?tx_jzvopdecisions_pi1%5BhighlightWord%5D=delodajal%C4%8Dev%20nadzor%20elektronske%20po%C5%A1te%20in%20dostopa%20do%20interneta%20zaposlenega (28. 1. 2014).

Informacijski pooblaščenec. 2008a. *Smernice glede uvedbe biometrijskih ukrepov.* Http://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Biometrija_-_smernice.pdf (29. 12. 2015).

Informacijski pooblaščenec. 2008b. *Zlata pravila zasebnosti na delovnem mestu.* Https://www.ip-rs.si/fileadmin/user_upload/Pdf/brosure/Zasebnost_na_delovnem_mestu.pdf. (22. 1. 2016).

Informacijski pooblaščenec. 2010. *Vpogled v elektronsko pošto zaposlenega*. Http://www.ip-rs.si/vop/vpogled-v-elektronsko-posto-zaposlenega-1865/?tx_jzvopdecisions_pi1%5BhighlightWord%5D=vpogled%20v%20elektronsko%20po%C5%A1to%20zaposlenega (28. 1. 2014).

Informacijski pooblaščenec. 2012. *Pravice delodajalca pri nadzoru službenih telefonov.* Http://www.ip-rs.si/vop/pravice-delodajalca-pri-nadzoru-sluzbenih-telefonov-2254/?tx_jzvopdecisions_pi1%5BhighlightWord%5D=pravice%20delodajalca%20pri%20nadzoru%20slu%C5%BEbenih%20telefonov (28. 1. 2014).

Informacijski pooblaščenec. 2013. *Pogosta vprašanja. Varstvo osebnih podatkov.* Https://www.ip-rs.si/pogosta-vprasanja/varstvo-osebnih-podatkov/#c303 (12. 9. 2013).

Informacijski pooblaščenec. 2015a. *Video nadzor-splošno.* Http://www.ip-rs.si/vop/video-nadzor-splosno-69/?tx_jzvopdecisions_pi1%5BhighlightWord%5D=informacijske%20tehnologije%20in%20osebni%20podatki%20-%20video%20nadzor (30. 12. 2015).

Informacijski pooblaščenec. 2015b. *Uporaba GPS sledilnih naprav in varstvo osebnih podatkov – smernice Informacijskega Pooblaščenca.* Https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/GPS_smernice_net.pdf. (01. 01. 2016).

Kokemuller, Neil. 2013. *About workplace supervision*. Http://smallbusiness.chron.com/workplace-supervision-42926.html (15. 8. 2013).

Kovačič, Matej. 2003. *Zasebnost na internetu.* Ljubljana: Mirovni inštitut, Inštitut za sodobne družbene in politične študije.

Kovačič, Matej. 2006. *Nadzor in zasebnost v informacijski družbi.* Ljubljana: Univerza v Ljubljani, Fakulteta za družbene vede v Ljubljani.

Lampe, Rok, Miro Cerar, Sonja Bien Karlovšek in Goran Klemenčič. 2007. *Zasebnost in varovanje osebnih podatkov na delovnem mestu – aktualna navodila in obrazci za pravno pravilno ravnanje delodajalec v odnosu do zasebnosti delavcev in varovanje osebnih podatkov – v priročniku in zgoščenk.* Maribor: Založba Forum Media.

Makarovič, Boštjan, Goran Klemenčič, Tomaž Klobučar, Maja Bogataj Jančič in David Pahor. 2001. *Internet in pravo: izbrane teme s komentarjem Zakona o elektronskem poslovanju in elektronskem podpisu,* ur. Matjaž Potrč, 188-189. Ljubljana: Pasadena.

Maltby, Lewis. 2013. Employment Privacy: Is There Anything Left? *Human Rights Magazine.* 39 (3).

Mayer-Schönberger, Viktor. 2001. General Development of Data Protection in Europe. V *Tehnology and Privacy: The New Landscape,* ur. Agre E. Philip in Marc Rotenberg, 219-241. Cambridge, Massachusetts, London, England: MIT Press.

Mišič, Klemen. 2013. *Sveti delavcev in varstvo osebnih podatkov. Zasebnost na delovnem mestu – pravica ali iluzija.* Http://www.delavska-participacija.com/clanki/ID070524.doc (12. 9. 2013).

Newman, Robert. 2010. *Security and access Control Using Biometric Technologies.* Course Technology Cengage Learning.

Oxford (*Advanced Learner's Dictionary*). 2013. Http://oald8.oxfordlearnersdictionaries.com/dictionary/privacy (14. 8. 2013).

Pavšič, Blaž. 2008. Pogodbena obdelava osebnih podatkov še vedno povzroča težave. *Pravna praksa* 27 (24/25): 18-21.

Perenič, Gorazd in Brane Šalamon. 2002. *Pojdite varno v svet.* Ljubljana: Perenič svetovanje.

Pirc, Musar, Nataša, Mojca Prelesnik in Sonja Bien. 2006a. *Predpisi s področja prava varstva osebnih podatkov in dostopa do informacij javnega značaja – uvodna pojasnila.* Ljubljana: GV Založba.

Pirc, Musar, Nataša, Mojca Prelesnik in Sonja Bien. 2006b. *Varstvo osebnih podatkov: vstop v zasebnost prepovedan!* Ljubljana: Informacijski pooblaščenec.

Pirc, Musar, Nataša. 2008. Neznosna lahkost kršitev zasebnosti. *Pravna praksa* 27(9): 6-8.

Ralph, Sarah in Adrian Wong. 2012. *Avstralija: Nadzor na delovnem mestu ali delodajalci gledajo na vse posledice?* Http://www.mondaq.com/australia/x/180198/Employee+Rights/Surveillance+in+the+Workplace+are+employers+looking+at+all+of+the+implications (28. 8. 2014).

Rawlinson, Kevin. 2016. *Private messages at work can be read by European employers.* Http://www.bbc.com/news/technology-35301148 (21. 1. 2016).

Schneier, Bruce. 2005. *T-Mobile Hack.* http://www.schneier.com/crypto-gram-0502.html (15. 2. 2005).

Slovensko društvo Informatika. 2013. *Slovar informatike.* Ljubljana: Slovensko društvo Informatika. Http://www.islovar.org/iskanje_enostavno.asp (15. 8. 2013).

SSKJ *(Slovar slovenskega knjižnega jezika).* 2005. Ljubljana: DZS.

Http://bos.zrc-sazu.si/cgi/a03.exe?name=sskj_testa&expression=zasebnost&hs=1 (14. 8. 2013).

Šelih, Alenka. 1979. Zasebnost in nove oblike njenega kazenskopravnega varstva. V *Zbornik znanstvenih razprav let. 39*, ur. Anton Perenič, 149-181. Ljubljana: Univerza v Ljubljani, Pravna Fakulteta.

Šprah, Franc. 2009. Kje so meje zasebnosti na delovnem mestu. V *FREM'09: Zbornik 6. študentske konference: Znanje: teorija in praksa.* CD-ROM (5. 09. 2013).

TechTerms.com. 2014. Http://www.techterms.com/definition/it (28. 8. 2014).

Zupančič, Lidija. 2015. Meje dopustnega nadzora uporabe interneta in elektronske pošte na delovnem mestu. *Pravna praksa* 34/1173(1).

Wagner DeCew, Judith. 1997. *In Pursuit of Privacy.* Ithaca, London: Cornell University Press.

Weeks, Joanna. 2013. *3 types of workers you need to supervise differently.* Http://www.healthandsafetyhandbook.com.au/3-types-of-workers-you-need-to-supervise-differently/ (7. 10. 2014).

PRAVNI VIRI

Ustava Republike Slovenije. *Uradni list RS*, št. 33/91-I, 42/97, 66/2000, 24/03 in 69/04.

Direktiva 2002/58/ES Evropskega parlamenta in Sveta o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij. *Uradni list EU*, št. L 201, str. 37-47.

Direktiva 2006/24/ES Evropskega parlamenta in Sveta o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij in spremembi Direktive 2002/58/ES. *Uradni list EU*, št. L 105/54.

Zakon o delovnih razmerjih (ZDR-1), *Uradni list RS*, št.21/2013, 003-02-3/2013-2

Zakon o elektronskih komunikacijah (ZEKom-1), *Uradni list RS*, št. 109/2012, 003-02-10/2012-32.

Zakon o evidencah na področju dela in socialne varnosti (ZEPDSV), *Uradni list RS*, št. 40/2006, 001-22-51/06.

Zakon o informacijskem pooblaščencu (ZInfP), *Uradni list RS*, št. 113/2005, 001-22-132/05.

Zakon o potnih listinah (ZPLD-1-UPB4), *Uradni list RS,* št. 29/2011, 213-03/11-1/2.

Zakon o varstvu osebnih podatkov (ZVOP-1), *Uradni list RS*, št. 86-3836/2004, 113-5005/20005.

Upravno sodišče Republike Slovenije. 2014. *UPRS sodba II U 195/2014.*

European Court of Human Rights. *Case of Barbulescu v. Romania.* Application no. 61496/08. Http://hudoc.echr.coe.int/eng?i=001-159906 (16. 1. 2016).

Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin (EKČP), *Uradni list RS,* št. 7-41/1994, 33/1994).

Varuh Republike Slovenije. 2010. *Uradni list Evropske unije. Listina Evropske unije o temeljnih pravicah,* št. 2010/C 83/02.

Generalna skupščina Združenih narodov. 1948. *Splošna deklaracija o človekovih pravicah (Universal Declaration of Human rights),* 10.12.1948.

PRILOGE

Priloga 1

VPRAŠALNIK ZA ŠTUDENTE

Pozdravljeni, sem Viktorija Arsovska, študentka 3. letnika univerzitetnega študijskega programa Management na Fakulteti za management v Kopru. Za potrebe diplomskega dela delam raziskavo na temo »Nadzor in zasebnost na delovnem mestu«. Z raziskavo želim ugotoviti ali delodajalci uporabljajo različne metode za nadzor na delovnem mestu med redno zaposlenimi in študenti ter kako spoštujejo zasebnost na delovnem mestu. Vsi odgovori so anonimni in se bodo uporabili izključno za izdelavo diplomske naloge.

Prosim, če lahko si vzamete pet minut časa in rešite anketo.

Hvala!

Študentsko delo

1. Kdaj ste prvič začeli delati kot študent?
- odprt odgovor

2. Zakaj ste začeli delati kot študent?
- odprt odgovor

3. Ali je vaše trenutno študentsko delo povezano z vašo izobrazbo?
- 1 ni povezano, 2 povezano v manjši meri, 3 povezano v večji meri, 4 v celoti povezano

4. Zakaj ste izbrali trenutno študentsko delo?
- odprt odgovor

5. Koliko različnih študentskih del ste opravljali do sedaj?
- odprt odgovor

6. Ali še vedno opravljate študentsko delo?
- da, ne

7. Kratko opišite splošno počutje na zadnjem študentskem delu.
- odprt odgovor

Opravljanje dela

8. Ali ste na trenutnem/zadnjem študentskem delu opravljali isto delo oziroma iste delovne naloge kot redno zaposleni delavci?
- da, ne, ne vem

Priloga 1

9. Če niste opravljali istega dela kot redno zaposleni delavci, ste se pozanimali, zakaj?
- odprt odgovor

10. Študenti vedno opravljajo ista dela kot redno zaposleni:
- 1 ne drži, 2 ne drži v manjši meri, 3 drži, 4 drži v večji meri, 5 popolnoma drži

11. Za študente in redno zaposlene veljajo ista pravila:
- 1 ne veljajo, 2 ne veljajo v manjši meri, 3 veljajo, 4 veljajo v večji meri, 5 veljajo popolnoma

12. Delodajalci študentom zaupajo enako kot redno zaposlenim:
- 1 se ne strinjam, 2 ne vem, 3 se strinjam

Nadzor in zasebnost na delovnem mestu

13. Ali ste bili obveščeni o nadzoru na delovnem mestu?
- da, ne

14. Kako vas je delodajalcev obvestil o nadzoru na delovnem mestu?
- osebno, preko telefona, preko e-pošte, preko oglasne deske, preko pogodbe o zaposlitvi, ni me obvestil, drugo.

15. Kdaj vas je delodajalec obvestil o nadzoru na delovnem mestu?
- pred začetkom dela, ob začetku dela, med opravljanjem dela, ni me obvestil

6. Ali mislite, da ima delodajalec pravico do nadzora delavcev?
- da, ne, ne vem

17. Ali mislite, da je nadzor na delovnem mestu potreben?
- nadzor na delovnem mestu je potreben, nadzor na delovnem mestu ni potreben, odvisno od narave dela.

18. S katerimi oblikami nadzora dela ste se srečali pri opravljanju študentskega dela?
- video nadzor, nadzor uporabe interneta in svetovnega spleta, preverjanje e-pošte, nadzor telefonskih pogovorov, GPS sledenje vozil, nadzor z biometrijo, nisem se še srečal z nadzorom na delovnem mestu, drugo.

19. Primer: pri opravljanju enega študentskega dela vas je delodajalec nadzoroval, pri drugem delu tovrstnega nadzora ni bilo. Bi lahko na kratko opisali splošno počutje na delovnem mestu?
- odprt odgovor

Osebni podatki

20. Spol
- M, Ž

21. Starost
Odprt odgovor

22. Letnik študija:
- 1 letnik, 2 letnik, 3 letnik, Absolvent.

Priloga 2

VPRAŠALNIK ZA DELODAJALCE

Pozdravljeni, sem Viktorija Arsovska, študentka 3. letnika univerzitetnega študijskega programa Management na Fakulteti za management v Kopru. Za potrebe diplomskega dela delam raziskavo na temo »Nadzor in zasebnost na delovnem mestu«. Z raziskavo želim ugotoviti ali delodajalci uporabljajo različne metode za nadzora na delovnem mestu za redno zaposlene in študente ter kako spoštujejo zasebnost na delovnem mestu. Vsi odgovori so anonimni in se bodo uporabili izključno za izdelavo diplomske naloge.

Prosim, če si lahko vzamete pet minut časa in rešite anketo.

Hvala!

Nadzor dela

1. Izberite oblike nadzora, ki jih uporabljate za nadzorovanje dela delavcev v vašem podjetju: video nadzor, nadzor uporabe interneta in svetovnega spleta, nadzor uporabe računalnika, nadzor telefonskih klicev, nadzor e-pošte, GPS sledenje službenih vozil, nadzor z biometrijo, ne uporabljamo nadzora dela delavcev, drugo.

2. Izberite oblike nadzora dela delovnih prostorov , ki jih uporabljate v vašem podjetju:
Video nadzor, nadzor z biometrijo, ne uporabljamo nadzora delovnih prostorov, drugo.

3. Nadzor dela redno zaposlenih delavcev je:
- 1 ni nadzora, 2 delni nadzor, 3 popolni nadzor

4. Nadzor dela študentov je:
- 1 ni nadzora, 2 delni nadzor, 3 popolni nadzor

5. O nadzoru so zaposleni obveščeni:
- pred začetkom dela, po začetku dela, med opravljanjem dela, niso obveščeni, drugo.

6. Na kateri način so zaposleni obveščeni o nadzoru dela?
- osebno, preko oglasne deske, preko e pošte, preko telefona, pisno- preko pogodbe o zaposlitvi, slišijo od sodelavcev, po končanem opravljanju dela, na redni sestankih, niso bili obveščeni, drugo.

7. Kako zadovoljni so zaposleni z nadzorom dela?
- 1 zelo nezadovoljni, 2 nezadovoljni, 3 nevtralni, 4 zadovoljni, 5 zelo zadovoljni

Priloga 2

Zasebnost na delovnem mestu

8. Ali menite, da imajo vaši zaposleni na delovnem mestu zagotovljeno dovolj zasebnosti?
- da, ne

Splošna vprašanja

9. Povprečno število študentov, ki letno dela v vašem podjetju:
- odprt odgovor

10. Zakaj zaposlujete študente?
- odprt odgovor

11. Kdaj zaposlujete študente?
- čez celo leto, samo v času dopustov, samo v času bolniške odsotnosti, po potrebi, ob povečanem obsegu dela, drugo.

12. Po vašem mnenju in vaših izkušnjah, kateri delavci svoje delo opravljajo bolje?
- redno zaposleni, študenti, ni razlik.

13. Dejavnost podjetja:
- odprt odgovor.

14. Leto ustanovitve podjetja:
- odprt odgovor.

15. Število zaposlenih v podjetju
- odprt odgovor

ODGOVORI ŠTUDENOTV NA VPRAŠANJE O POČUTJU NA DELOVNEM MESTU

V nadaljevanju so predstavljeni odgovori na vprašanje o počutju na zadnjem delovnem mestu, na katerem so študenti odgovarjali v anketnem vprašalniku.

Vprašanje 7 (Priloga 1): Kratko opišite splošno počutje na zadnjem delovnem mestu:

- prijetno zaradi strank, dober kolektiv
- ni bilo slabo ker sem delala z ljudmi ki sem jih poznala od prej
- stresno in naporno
- super
- dobro
- stresno, ker je količina dela prevelika samo za enega človeka
- zelo zadovoljna
- dobro ki ni bilo preveč stresno delo smo se dosti zafrkavali
- prevec dela
- malo neprijetno ker šefica je bila preveč nadzorovana
- dobro, zaradi samostojnosti in sproščenosti, ki mi jo je delo omogočalo
- sef je bil prevec nadzorovalen, sodelavci so bili super
- utrujajoce
- načeloma dobro, šef je bil zatezen ampak sodelavci super
- v celoti korektno, redna izplačila, možnost pogajanja, spoštljiv odnos
- slabo sodelavci so bili nesramni
- sefica je bila preveč nadzorovalna ni bilo pravega vzdusja
- naporno, dosti dela in šef je bil zatežen
- se je dalo it skozi, sem delal ker sem rabil denar
- ne prevec dobro pocutje sodelvci me niso spostovali
- dobro, delo je bilo super sodelavci pa ne prevec malo nelagodno je bilo
- odlicno sem tudi hitro napredovala
- super sem delala s kolegicami
- ne prevec prijetno ni bila prava ekipa
- nezadovoljna, sef me ni spostoval
- vedno so samo kritizirali nikoli niso dali pohvale
- dobro pocutje med opravljanjem dela
- srednja zalost
- se mi je zdelo da so mi dodelili prevec odgovornosti pa sem bil pod stresom
- na začetku je bilo vredu ampak potem je šef začel uveljavat neka svoja pravila in je postalo nerodno
- bedno, brezveze
- obupno. popolno izkoriščanje s strani delodajalca
- zelo dobro. delodajalec je bil pošten in plačilo primerno delu