B&B
VIŠJA STROKOVNA ŠOLA

Diplomsko delo višješolskega strokovnega študija
Program: Ekonomist
Modul: Organizator poslovanja

NADZOR NAD ZAPOSLENIMI NA DELOVNEM MESTU

Mentorica: mag. Alenka Bradač, univ. dipl. ekon.
Lektorica: Ana Peklenik, prof. slov.

Kandidat: Andrej Hribar

Kranj, junij 2014

ZAHVALA

Zahvaljujem se mentorici mag. Alenki Bradač, univ. dipl. ekon., za usmeritve pri izdelavi diplomske naloge.

Hvala g. Jožetu Bogataju, vodju nadzornikov v Uradu informacijskega pooblaščenca, za zbrane statistične podatke, uporabljene v diplomskem delu.

Zahvaljujem se tudi lektorici Ani Peklenik, ki je mojo diplomsko nalogo jezikovno in slovnično pregledala.

IZJAVA

»Študent Andrej Hribar izjavljam, da sem avtor tega diplomskega dela, ki sem ga napisal pod mentorstvom mag. Alenke Bradač, univ. dipl. ekon.«

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

Dne _____ Podpis: _____

POVZETEK

Pravico do varovanja premoženja delodajalcev in pravico delavcev do zasebnosti loči tanka meja. Slovenska zakonodaja določa pogoje uporabe moderne tehnologije in meje dopustne uporabe. Zlorabe se pojavljajo predvsem s pomočjo tehnologije na področju videonadzora, mobilne telefonije, sledenju vozil z GPS-napravami, nadzoru interneta in elektronske pošte ter uporabe biometrije. S tovrstno tematiko se v Sloveniji ukvarja predvsem Urad informacijskega pooblaščenca. Njegovo glavno vodilo je da se sme ukrepe za nadzor zaposlenih uporabiti samo v primeru, ko tega ni mogoče doseči z milejšimi ukrepi. Tovrstni prijemi delodajalca naletijo na buren odziv javnosti, vendar je treba poudariti, da so v Sloveniji, glede na število podjetij in zaposlenih, razmeroma redki. Zaposleni navadno postanejo pozorni šele takrat, ko pridejo v stik s tovrstnimi prijemi delodajalcev. Opravljena anketa izkazuje veliko mero zaupanja zaposlenih v delodajalce, kar lahko pripišemo strogi zakonodaji. Prav tako so zaposleni dobro seznanjeni s svojimi pravicami, saj tovrstne zlorabe pogosto pridejo v medije, nanje pa stalno opozarja tudi Urad informacijskega pooblaščenca.

KLJUČNE BESEDE

- videonadzor
- mobilna telefonija
- GPS-naprave
- elektronska pošta
- biometrija

ABSTRACT

The right to protection of property employers and workers' right to privacy separates fine line . Slovenian legislation lays down conditions for the use of modern technology and the limits of permissible use. Abuses occur mainly through technology in the field of video surveillance; mobile vehicle tracking with GPS devices, control of the internet and e-mail with this kind of topic in Slovenia is primarily engaged in the Office of the Information Commissioner. His main motto is to be measures to control employee use only in cases where this cannot be achieved by milder measures. These sorts of approaches employer encounter a hostile reaction from the public, but it should be noted that in Slovenia, regardless of the number of firms and employees are rare. Employees are aware of such approaches only when they come into contact with them. A survey showing a great deal of trust in employees, employers, which can be attributed to strict legislation and good to raise awareness and prevent undue control of the Office of the Information Commissioner.

KEYWORDS

- Video surveillance
- - Mobile telephony
- - GPS devices
- - E-mail
- - biometrics

KAZALO

1 UVOD

1.1 Predstavitev problema

Z razvojem informacijske tehnologije so delodajalci dobili nove možnosti za nadzor nad zaposlenimi na delovnem mestu. Obstaja zelo tanka meja med nadzorom zaposlenih in potrebi za zagotavljanje varnosti. Zastavlja se vprašanje, ali smo zaposleni z razvojem tehnologije izgubili zasebnost na delovnem mestu, kakšne so možnosti nadzora s strani delodajalca, ter kako lahko preprečimo nedovoljene posege v našo zasebnost, kako pogosto in na kakšen način delodajalci uporabljajo nedovoljene metode, ter ali smo zaposleni dovolj seznanjeni s svojimi pravicami.

1.2 Cilji naloge

Cilj naloge je oceniti spoštovanje zakonskih omejitev s strani delodajalcev in poznavanje lastnih pravic zaposlenih glede zasebnosti, preveriti ugotovitve informacijskega pooblaščenca na tem področju ter na podlagi opravljene ankete oceniti razsežnost obravnavanega problema.

1.3 Predstavitev okolja

Razvoj novih tehnologij je povzročil tudi sodobno informacijsko in tehnološko podprto delovno okolje, ki pa poleg večje učinkovitosti prinaša tudi možnost posega vdora v zasebnost zaposlenih. Težnje delodajalcev po varovanju premoženja, večji učinkovitosti poslovnega procesa in boljši izkoriščenosti zaposlenih pogosto privedejo v nedovoljene posege v zasebnost zaposlenih. Na to nas opozarjajo številni članki in poročila v medijih. Država se je spopadla s to nevarnostjo, zato je sprejela veliko število uredb in zakonov na tem področju ter s tem poskušala urediti obravnavano tematiko in definirati pogoje ter omejitve, predvsem pa zaščititi pravice šibkejših udeležencev poslovnih procesov.

1.4 Predpostavke in omejitve

V praksi smo pogosto priča številnim posegom delodajalcev v zasebnost zaposlenih. Na to nas opozarjajo številna poročila in članki v medijih, tudi poročila državnih organov, predvsem Urad informacijskega pooblaščenca. Zaposleni se pogosto ne zavedajo svojih pravic, saj niso dovolj pravno podkovani na tem področju, kar delodajalci pogosto izkoriščajo.

Nadzor nad zaposlenimi na delovnem mestu lahko obsega številna področja, zato bomo nalogo omejili zgolj na nadzor s pomočjo sodobne tehnike. Zakonodaja na

tem področju je zelo obsežna, zato bomo v teoretičnem delu naloge navedli predvsem tiste pomembne člene, ki se nanašajo na:

- videonadzor,
- uporabo interneta,
- zbiranje in obdelavo podatkov,
- elektronsko pošto,
- sledenje z GPS-napravami,
- spremljanje telefonskih pogovorov.

1.5 Metode dela

V teoretičnem delu bomo najprej s pomočjo opisne metode predstavili zakonske zahteve obravnavanega področja. V praktičnem delu bomo s pomočjo analitične metode analizirali ugotovitve Urada informacijskega pooblaščenca ter s pomočjo metode anketiranja ugotovili stanje poznavanja pravic in praktične izkušnje zaposlenih.

Pomembne predhodne raziskave se nanašajo predvsem na ugotovitve Urada informacijskega pooblaščenca, ki jih bomo uporabili v diplomski nalogi.

2 ZAKONSKE PODLAGE

Uvodoma smo omenili dilemo, ki jo je povzročil razvoj tehnologije. Vedno več modernih tehničnih in programskih orodij, poleg napredka na delovnem mestu, omogoča večji nadzor. Vse to pa je povzročilo tudi razvoj zakonodaje na tem področju, saj je bilo nujno urediti pravice delodajalcev pri varovanju premoženja in pravice delavcev pri varovanju njihove zasebnosti. Splošne zakonske pravice dobro ponazori mnenje informacijskega pooblaščenca, ki pravi (https://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/odlocbe-in-mnenja-varstvo-osebnih%20podatkov/?tx_jzvopdecisions_pi1%5BshowUid%5D=2046&cHash=484a541185a0b9224a452abf883028b9): »Kljub skrbi za zasebnost na delovnem mestu je določena stopnja nadzora s strani delodajalca zakonsko dopustna. Seveda pa je tak nadzor dopusten tedaj, ko se izvaja v okviru, ki ga določa ustava, zakonski predpisi in domača ali mednarodna sodna praksa. Razen tega mora biti dopusten nadzor oziroma poseg v zasebnost opredeljen v internih pravilnikih podjetja.«

Zakonodaja, ki zajema določila in predpise z vidika tehnološkega nadzora zaposlenih in varovanja zasebnosti delavcev, je zajeta v naslednjih predpisih:

- Ustava Republike Slovenije,
- Kazenski zakonik,

- Zakon o varstvu osebnih podatkov,
- Zakon o elektronskih komunikacijah,
- Zakon o delovnih razmerjih.

Ustava RS predstavlja krovna določila o človekovih pravicah. Člena, ki se nanašata na obravnavano področje, sta 37. in 38. člen. 37. člen zagotavlja varstvo tajnosti občil in drugih pisem, 38. člen pa zagotavlja varstvo osebnih podatkov. Podrobne določbe potem zagotavljajo in urejajo različni navedeni zakoni, katerih bistvena določila bomo predstavili v naslednjih podpoglavjih. Kazenski zakonik določa sankcije v primeru kršitev in ga bomo obravnavali v poglavju 2.2.

2.1 Določila po ZVOP-1 in ZEkom-1

Varstvo osebnih podatkov v Sloveniji zagotavlja Zakon o varstvu osebnih podatkov (ZVOP-1, Ur. l. RS št. 94/07), ki v svojem 8. členu pravi, da se osebni podatki lahko obdelujejo le, če to določa zakon, ali če je za obdelavo določenih osebnih podatkov podana osebna privolitev posameznika.

Zakon določa, da se lahko v zasebnem sektorju obdelujejo podatki, če je to nujno zaradi zakonitih interesov zasebnega sektorja in ti interesi očitno prevladujejo nad interesi posameznika, na katerega se nanašajo osebni podatki (Zakon o varstvu podatkov, Ur. l. RS št. 94/07, 10. člen).

Ureja tudi področje videonadzora, in sicer v svojem 74. členu predpisuje, da mora oseba javnega ali zasebnega sektorja o tem objaviti obvestilo. V nadaljevanju nato v svojem 77. členu določa, da se lahko uporablja znotraj delovnih prostorov le v izjemnih primerih, kadar je to nujno potrebno za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ter poslovne skrivnosti. Tega pa ni mogoče doseči z milejšimi ukrepi (Zakon o varstvu podatkov, Ur. l. RS št. 94/07, 74, 77. člen).

Navedenega 74. člena ZVOP-1 ne gre jemati zlahka, to so spoznali tudi na RTV Slovenija. Cerar (2006) v svojem članku, objavljenem v tedniku Mladina, opisuje poskus vodstva RTV Slovenija po ostrejšem varovanju. V ta namen so namestili dodatne varnostne kamere, ki so bile usmerjene tudi v notranjost prostorov in so snemale celo posamezne aparature. Zaposleni so obračali kamere in eden izmed njih je bil celo odpuščen. Na koncu je urad informacijskega pooblaščenca v skladu s 74. členom odločil, da morajo nadzor notranjih prostorov odpraviti ter ga nadomestiti z milejšim ukrepom, tj. poostrenim fizičnim varovanjem.

Posebno pozornost zakon namenja tudi biometriji in določa, da je potrebno pred tovrstnim zbiranjem podatkov obvestiti pristojni državni organ, ki mu je potrebno predložiti namen zbiranja in razloge za uvedbo. Tudi tukaj pa velja, da lahko oseba

javnega ali zasebnega sektorja zbira le tiste podatke, ki so nujno potrebni za opravljanje dejavnosti (Zakon o varstvu podatkov, Ur. l. RS št. 94/07, 80. člen).

Zakon o Elektronskih komunikacijah (ZEkom-1) določa, da se za elektronsko pošto šteje 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 (Zakon o elektronskih komunikacijah, Ur. l. RS št. 109/12, 3. člen).

V svojem 145. členu tudi predpisuje, da morajo ukrepi za zagotovitev varnosti ob upoštevanju tehnološkega razvoja zagotoviti takšno raven varnosti in zavarovanja, ki ustreza predvidenemu tveganju. Kot tveganje zakon izpostavlja predvsem vsako dejanje, storitev ali izdelek, ki posega v tajnost, zaupnost in varnost elektronskega komunikacijskega omrežja ali elektronske komunikacijske storitve, s tem ko spremeni dostopnost, vsebino, ceno ali kakovost storitve, in ki ga lahko operater sam ali skupaj z drugimi operaterji učinkovito onemogoči (Zakon o elektronskih komunikacijah, Ur. l. RS št. 109/12, 145. člen).

2.2 Določila po ZDR-1 in KZ-1

Zakon o delovnih razmerjih določa pravice delodajalca in delavca kot šibkejše stranke poslovnega procesa. Zato v svojem 46. členu poudarja, da mora delodajalec varovati, spoštovati delavčevo osebnost ter upoštevati in ščititi delavčevo zasebnost (Zakon o delavnih razmerjih, Ur. l. RS št. 21/13).

Za zaščito osebnih podatkov delavca v svojem 48. členu določa, da se osebni podatki delavcev lahko zbirajo, obdelujejo, uporabljajo in posredujejo tretjim osebam samo, če je to določeno s tem ali drugim zakonom ali če je to potrebno zaradi uresničevanja pravic in obveznosti delovnega razmerja ali v zvezi z delovnim razmerjem. Prav tako zakon pravi, da se morajo osebni podatki, za zbiranje katerih ne obstoji več zakonska podlaga, takoj zbrisati in prenehati uporabljati (Zakon o delovnih razmerjih, Ur. l. RS št. 21/13).

Tudi Kazenski zakonik je eden izmed zakonov, ki ščitijo pravice tako delodajalcev kot zaposlenih. Zanimivi s stališča diplomske naloge so predvsem členi, ki se nanašajo na videonadzor, zlorabo osebnih podatkov in tajnosti občil.

Zakon sankcionira tistega, ki neupravičeno snema ali naredi slikovni posnetek drugega ali njegovih prostorov brez njegovega soglasja in pri tem občutno poseže v njegovo zasebnost ali kdor tako snemanje neposredno prenaša tretji osebi oz. ji omogoči, da se z njim seznani (Kazenski zakonik, Ur. l. RS št. 55/08, 138. člen).

V nadaljevanju v svojem 143. členu KZ-1 predvideva sankcioniranje tistega, ki uporabi osebne podatke, ki se obdelujejo na podlagi zakona, v neskladju z namenom njihovega zbiranja ali brez osebne privolitve osebe, na katero se osebni podatki nanašajo (Kazenski zakonik, Ur. l. RS št. 55/08, 143. člen).

Sankcionira tudi nepravilnosti na področju tajnosti občil, zato v svojem 139. členu določa sankcije za tistega, ki se neupravičeno seznani z elektronskim sporočilom ali kakšnim drugim komunikacijskim sredstvom (Kazenski zakonik, Ur. l. RS št. 55/08, 139. člen).

2.3 Okviri dopustnosti nadzora

V prejšnjih podpoglavjih smo spoznali nekatere zakonske določbe, vendar moramo, če hočemo biti objektivni, predstaviti tudi drugo plat zgodbe. Pri iskanju in prebiranju literature le redko naletimo na takšno, ki bi upravičevala nadzor nad zaposlenimi. Vendar se morajo tudi zaposleni zavedati, da ima delodajalec v določenih primerih pravico opravljati nadzor. Dopustnost nadzora dobro povzame Hvaliček (2012), ki v svojem članku navaja delovno pravno zakonodajo, ki narekuje delavcu, da opravlja delo po navodilih in pod nazorom delodajalca. Tako so delodajalci upravičeni do nadzora nad delavci, vendar morajo biti delavci v naprej seznanjeni s pravili. Nadzor je torej popolnoma legalna in legitimna pravica delodajalca.

Hvaliček (2012) navaja, da je nadzor upravičen v primeru:

- kadar so zaposleni vnaprej seznanjeni s pravili uporabe telefona, elektronske pošte in interneta,
- kdaj in v kakšnih lahko nadzira komunikacijo zaposlenih,
- delodajalec si ne more privoščiti pretiranega omejevanja komunikacije z zunanjim svetom,
- zaposleni pod nadzorom se mora strinjati oz. mora biti nadzor objektivno opravičljiv in sorazmeren,
- uporabo interneta lahko delodajalci omejujejo le na način, da določijo dostop do strani, ki jih zaposleni potrebujejo za svoje delo.

Če povzamemo navedbe zakonskih določil iz poglavja 2.1. in 2.2., lahko zaključimo, da je videonadzor dopusten samo v primeru varovanja lastnine in je lahko usmerjen samo v dostopne točke poslopja in nikakor ne na področje delovnega mesta posameznega delavca.

V današnjih časih je zanimivo in vedno bolj razširjeno varovanje prostorov s pomočjo biometrije, vendar ZVOP-1 dovoljuje uporabo biometrije le v naslednjih primerih (http://www.e-tm.si/eTM_data/dokumenti/ZAKONODAJA_VIDEO NADZOR.pdf):

- za javni sektor, kadar tako določa zakon (npr. Zakon o potnih listinah), izjemoma na podlagi posebnih zakonskih določil tudi za vstop v stavbo ali dele stavbe in evidentiranje zaposlenih na delu,
- za zasebni sektor, le če je nujno potreben za:
  -opravljanje dejavnosti,
  -varnost ljudi ali premoženja,
  -varovanje tajnih podatkov ali
  -varovanje poslovne skrivnosti.

3 SANKCIJE ZOPER DELODAJALCE

Uvodoma smo zapisali omejitve diplomske naloge na obravnavana področja tehničnega nadzora nad zaposlenimi:

- videonadzora,
- uporabo interneta,
- zbiranje in obdelavo podatkov,
- elektronsko pošto,
- sledenje z GPS-napravami,
- spremljanje telefonskih pogovorov.

V drugem poglavju smo navedli glavno zakonodajo, ki ureja to področje, v tretjem poglavju pa želimo predstaviti sankcije v primeru kršitve nekaterih navedenih določil v drugem poglavju.

3.1 Sankcije po ZVOP-1

V tabeli 1 smo povzeli nekatere pomembnejše sankcije, ki jih predpisuje ZVOP-1 v primeru kršitve njegovih določb. Za kršitve 77. člena o videonadzoru je zagrožena kazen za podjetje 4170–12.510 evrov in globa za ogovorno osebo 1250–2080 evrov. Za kršitve 74. člena o videonadzoru je zagrožena globa za podjetje 4170–12.510 evrov in za odgovorno osebo 830–1250 evrov. Za kršitve, ki se nanašajo na 24. in 25. člen o varovanju osebnih podatkov, je zagrožena kazen za podjetje 4170–12.510 evrov in odgovorno osebo 830–1250 evrov. Za kršitve 80. člena, ki se nanaša na biometrijo, jo predpisana globa za podjetje 4170–12.510 evrov in 1250–2080 evrov za odgovorno osebo.

Kršitev člena	Podjetje	Ogovorna oseba
77. člen – videonadzor	globa 4170–12.510 €	globa 1250–2080 €
74. člen – videonadzor	globa 4170–12.510 €	globa 830–1250 €
24., 25. člen – varovanje osebnih podatkov	globa 4170–12.510 €	globa 830–1250 €
80. člen biometrija	globa 4170 do 12.510 €	globa 1250–2080 €

Tabela 1: Pregled nekaterih sankcij po ZVOP-1
(Vir: lasten povzetek ZVOP-1)

3.2 Sankcije po ZEkom-1 IN KZ-1

ZEkom-1 predpisuje predvsem visoke globe, in sicer smo v drugem poglavju podrobno spoznali določila 145. člena ZEkom-1, ki v primeru, da odgovorna javna ali zasebna oseba ne sprejme ustreznih ukrepov za varnost in zavarovanje, sorazmerno s pričakovanimi tveganji in stroški, ter v skladu s tehničnim in tehnološkim razvojem, predpisuje globo v višini od 50.000 do 400.000 €.

Drugi vidik sankcij predpisuje KZ-1, ki ne predpisuje samo globe, kot npr. ZVOP-1, ampak tudi zaporne kazni.

Kršitev člena	Zagrožena sankcija	Sankcije za uradne osebe
138. zloraba videonadzora	denarna kazen ali zapor do 1 leta	zapor od 3 mesecev do 5 let
143. zloraba osebnih podatkov	denarna kazen ali zapor do 1 leta	zapor do 5 let
139. tajnost občil	denarna kazen ali zapor do 6 mesecev	zapor od 3 mesecev do 5 let

Tabela 2: Pregled nekaterih sankcij po KZ-1
(Vir: lasten povzetek KZ-1)

V tabeli 2 prikazujemo sankcije. Najstrožja se nanaša na zlorabo osebnih podatkov v primeru kršitve 143. člena, saj predpisuje zaporno kazen do 5 let za uradno osebo, ki je storila omenjeni prekršek.

4 PREGLED UGOTOVITEV URADA INFORMACIJSKEGA POOBLAŠČENCA

Omenili smo, da v Sloveniji obravnavano tematiko spremlja Urad informacijskega pooblaščenca. Proučili smo objavljeno gradivo in v tem poglavju bomo predstavili njihove ključne ugotovitve. Poročilo o najpogostejših kršitvah delodajalcev v zvezi z nadzorom delavcev, ki ga je pripravil Urad informacijskega pooblaščenca, ugotavlja naslednjih 10 najpogostejših kršitev (https://www.iprs.si/fileadmin/user_upload/Pdf/brosure/Zasebnost_na_delovnem_mestu.pdf):

- vpogledi v elektronsko pošto zaposlenih,
- pridobivanje zdravstvenih podatkov zaposlenih,
- nepravilno izvajanje nadzora bolniškega staleža zaposlenih,
- neutemeljen videonadzor delovnih prostorov,
- delodajalci zaposlenih pisno ne obvestijo o izvajanju videonadzora,
- delodajalci ustrezno ne zavarujejo zbirk osebnih podatkov zaposlenih,
- neutemeljeno sledenje zaposlenim z GPS-napravami, mobilnimi telefoni ipd.,
- neutemeljen nadzor nad telefonskimi klici zaposlenih,
- delodajalci ne omogočijo delavcu, da se seznani z lastnimi osebnimi podatki,
- prekomerno zbiranje osebnih podatkov zaposlenih.

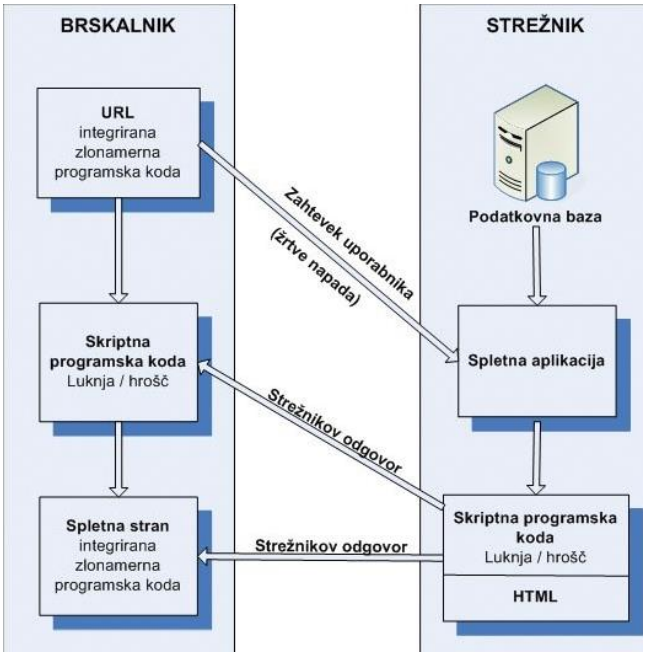
Iz objavljenega gradiva izhaja, da Urad informacijskega pooblaščenca ni samo neke vrste represivni organ, ampak tudi svetuje delodajalcem, kdaj je dopusten nadzor in kako se držati predpisanih pravil. V ta namen so izdali tudi smernice oziroma 5 zlatih pravil (https://www.iprs.si/fileadmin/user_upload/Pdf/brosure/Zasebnost_ na_ delovnem_mestu.pdf):

1. Delodajalec lahko od zaposlenega zbira in nadalje obdeluje le toliko osebnih podatkov, kolikor je to nujno zaradi izvrševanja pravic in dolžnosti iz delovnega razmerja in kar določa zakonodaja.
2. Delavec ima tudi na delovnem mestu pravico do zasebnosti, sorazmerno z zakonitim ciljem, ki mu delodajalec sledi.
3. Vsakršno obdelavo osebnih podatkov v okviru delovnega razmerja je potrebno izvrševati kar se da restriktivno, vendar je ni dopustno izsiliti.
4. Za osebne podatke, ki niso zajeti v 1. pravilu, je potrebno pridobiti osebno privolitev zaposlenega, vendar ne z izsiljevanjem.
5. Poseg v zasebnost delavca na delovnem mestu je mogoče izvesti le, ko pride do kolizije z neko drugo ustavno pravico in ta v konkretnem primeru prevlada.

V nadaljevanju naloge bomo podrobneje predstavili nekatere zgoraj navedene najpogostejše kršitve delodajalcev pri izvajanju nadzora.

4.1 Vpogledi v elektronsko pošto zaposlenih in nadzor interneta

Ravnanje z elektronsko pošto zaposlenih ureja ZEkom-1, katerega ključne člene smo navedli v teoretičnem delu naloge. Urad informacijskega pooblaščena tovrstne kršitve zaznava kot najpogostejše. Če povzamemo 5. pravilo, zapisano v brošuri Zlata pravila zasebnosti na delovnem mestu, je pravica delavca do varovanja zasebnosti pred pravico delodajalca, ki izhaja iz varovanja lastnine. Delodajalec lahko vpogleda v elektronsko pošto le v primeru, če je bil prej sklenjen dogovor med delodajalcem in zaposlenim, s katerim so bili natančno dogovorjeni pogoji uporabe in pogoji, pod katerimi lahko delodajalec vpogleda v službeno elektronsko pošto zaposlenega. Informacijski pooblaščenec priporoča, da se o tem sestavi pisni dogovor, tako da so pravila v naprej jasna. Seveda pa mora biti kljub vnaprejšnjemu dogovoru vpogled omejen in v skladu za načelom sorazmernosti, ki nam pomaga v določeni situaciji pretehtati, katera pravica je v določeni situaciji močnejša od druge (https://www.iprs.si/fileadmin/user_upload/Pdf/brosure/Zasebnost_na delovnem_ mestu.pdf).



*Slika 1: Prikaz možnega nadzora elektronske pošte, interneta (Vir: http://www.*monitor.*si/clanek/spletni-napadi/122720/)*

Sodobna tehnologija in razvoj programske opreme delodajalcu omogoča namestitev posebnih aplikacij, s pomočjo katerih ima možnost nadziranja elektronske pošte, interneta. Pogosto že ob nastanku določene programske opreme proizvajalec vgradi tovrstne aplikacije. Možen primer prestrezanja sporočil ponazarjamo na sliki 1.

4.2 Neutemeljen videonadzor delovnih prostorov

V poglavju 2 smo navedli, da to področje ureja predvsem ZVOP-1. Njegova določila praktično in na primeru izkušenj Urad informacijskega pooblaščenca pojasnjuje v smislu, da videonadzor zaposlenih lahko delodajalec uvede le v izjemnih primerih, kadar je to nujno pomembno za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ter poslovne skrivnosti, tega namena pa ni mogoče doseči z milejšimi ukrepi. Po izkušnjah Urada informacijskega pooblaščenca lahko delodajalec le redko upraviči takšen videonadzor, ki ne ustreza zakonskim zahtevam, pri tem pa ne pomislijo, kakšne posledice jih lahko doletijo. Kazen ni le globa pri informacijskem pooblaščencu, temveč tudi odškodninska tožba in v skrajnem primeru kazenska ovadba. Prav tako mora delodajalec pisno obvestiti delavca o uvedbi video nadzora (https://www.iprs.si/fileadmin/user_upload/Pdf/brosure/Zasebnost_na_delovnem_mestu.pdf).

Slika 2: Pogled video nadzorne kamere v podjetju
(Vir: http://www.zurnal24.si/ko-sef-postane-veliki-brat-clanek-212273)

Ugotovimo lahko, da število prijav sovpada z razvojem različne tehnologije na tem področju. Na slovenskem trgu je ogromno ponudnikov tovrstne opreme, ki svojim strankam zagotavljajo popoln nadzor nad objektom. Primer enega takih video nadzornih sistemov je Sistem S, ki zagotavlja uporabnikom (http://www.zaslon-telecom.si/product.php?id=15&detailId=-1):

- snemanje nadzorovane lokacije le ob dogodkih, s čimer se izognemo nepotrebnim in nekoristnim posnetkom;
- enostavno, hitro iskanje aktualnega dogodka/posnetka, saj je arhiv opremljen z datumom, časom in lokacijo;
- posamezni, poljubni ali istočasni pregled vseh lokacij v realnem času;
- 24-urno snemanje za lokacije, kjer nam ne sme uiti nobena podrobnost;

- opazovanje in pregled nadzorovanega področja iz oddaljene lokacije – pisarne, doma, video nadzornega centra preko interneta ali direktnega modemskega dostopa.

Pri tej obliki nadzora je potrebno tudi poudariti, da v nobenem primeru ni dovoljen nadzor v garderobah, dvigalih in sanitarnih prostorih (http://www.e-tm.si/eTM_data/dokumenti/ZAKONODAJA_VIDEONADZOR.pdf).

4.3 Neustrezno zavarovanje zbirk osebnih podatkov

V uvodu poglavja smo predstavili smernice Urada informacijskega pooblaščenca glede pridobivanja osebnih podatkov, v teoretičnem delu naloge pa zakonska določila, ki jih predpisuje ZVOP-1. Poleg navedenega Urad informacijskega pooblaščenca dodaja še, da morajo delodajalci voditi evidenco zbirk osebnih podatkov v skladu z Zakonom o evidencah na področju dela in socialne varnosti ter ZDR. Zbirke morajo ustrezno zaščititi pred nepooblaščenimi dostopi in zaposlenim, ki ravnajo s temi zbirkami, določiti jasne dostopne pravice (https://www.iprs.si/fileadmin/user_upload/Pdf/brosure/Zasebnost_na_delovnem_mestu.pdf).

Iz navedenega torej izhaja, da mora delodajalec poskrbeti za varovanje podatkov pred notranjimi in zunanjimi uporabniki. Na sliki 3 prikazujemo tudi ponazoritev pomembnosti varovanja osebnih podatkov, kot jih razlaga ustava.

Slika 3: Ponazoritev varstva osebnih podatkov
(Vir: http://www.us-rs.si/strip/)

Primer dobre prakse so v skladu z določili ZVOP-1 prikazali tudi v podjetju Lek d.d., kjer so v ta namen določili projektno skupino, ki se je ukvarjala z vprašanjem varovanja osebnih podatkov. V ta namen so določili internega skrbnika osebnih podatkov, katerega vloga je (www.delavska-participacija.com/priloge/ ID070822.doc):

- priprava in revizija internih aktov,
- nadzor nad izvajanjem določb Pravilnika,
- sodelovanje s pristojnimi državnimi nadzornimi organi,
- priprava katalogov zbirk osebnih podatkov na podlagi podatkov, ki so mu jih dolžne posredovati odgovorne osebe za posamezne zbirke osebnih podatkov,
- določitev oseb, ki so odgovorne za posamezne zbirke osebnih podatkov in
- vodenje postopkov v zvezi s pravicami posameznika.

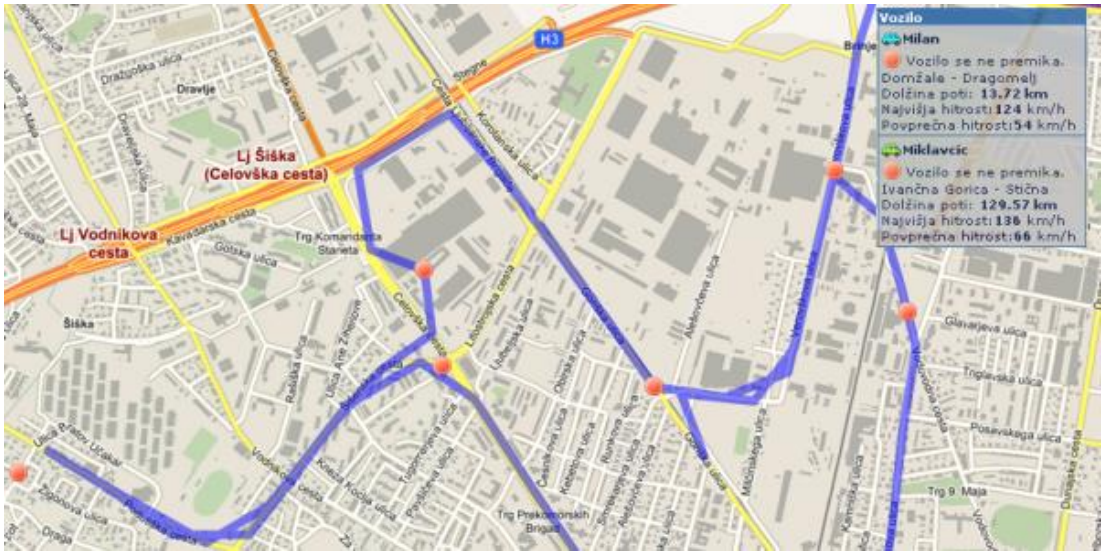
4.4 Sledenje zaposlenim z GPS-napravami

Prejete prijave na Urad informacijskega pooblaščenca so vodile k pojasnilu dovoljene uporabe GPS-tehnologije. Tako povzema stališče Evropskega sodišča za človekove pravice, ki je v svojih sodbah poudarilo pravico delavca do zasebnosti na delovnem mestu, na vsak nadzor (npr. nadzor nad telefonskimi klici, e-pošto, sledenje z GPS-napravami) pa je potrebno delavca vnaprej opozoriti in mu povedati, za kateri namen in v katerih primerih se nek ukrep lahko uporablja. Če se npr. službeni avto uporablja tudi za zasebno uporabo, je treba delavcu omogočiti izključitev naprave po koncu delovnega časa (https://www.iprs.si/fileadmin/user_ upload/Pdf/brosure/Zasebnost_na_delovnem_mestu.pdf).

Slika 4: Ročni GPS-sledilec
(Vir: *http://www.easytracker.si/si/resitve-sledenja/sledenje-in-nadzor-z-rocnim-gps-sledilcem.php*)

Razvoj tehnologije GPS je omogočil tudi delodajalcem varovanje vozil in nadzor zaposlenih, tako da vsakem trenutku preko posebne aplikacije vedo, kje se vozilo ali zaposleni nahaja. Tovrstne aplikacije lahko delodajalec izkoristi za nadzorovanje gibanja zaposlenih in lahko hitro pride v konflikt z določili ZVOP-1. Primer tovrstne opreme prikazujemo na sliki 4. Naprava je del ročnega GPS-sistema, imenovanega

Easytracker podjetja Bent Excellent d.o.o., ki je v prvi vrsti namenjena optimizaciji delovnega procesa terenskega delavca. Naprava omogoča, da delavec s preprostim pritiskom sporoča svojo lokacijo centrali in vnaprej določi lokacije, ki jih bo obiskal. V centrali pa imajo s pomočjo aplikacije na zemljevidu prikazano gibanje delavcev, kar prikazujemo na sliki 5.



Slika 5: Zemljevid gibanja zaposlenih – aplikacija Easytracker
(Vir: http://www.easytracker.si/si/resitve-sledenja/sledenje-in-nadzor-z-rocnim-gps-sledilcem.php)

Vsekakor lahko tovrstna tehnologija vodi v zlorabo in v uporabo za nedovoljene namene. Delavec se mora v prvi vrsti strinjati z njeno uporabo, kar smo spoznali v teoretičnem delu naloge, kjer smo navedli zakonske določbe, nikakor pa tehnologije delodajalec ne sme uporabiti za merjenje učinkovitosti delavca ali kakršenkoli drugačen nadzor, razen določenega s pogoji uporabe.

4.5 Nadzor nad telefonskimi klici

Glede nadzora nad telefonskimi klici pooblaščenec opozarja, da delodajalec ne sme kar prosto preko t. i. razčlenjenega računa preverjati, koga je zaposleni klical, pač pa mora dati zaposlenemu možnost pojasniti, koliko je bilo službenih in koliko zasebnih klicev, predvsem pa pred tem povedati, kakšen limit porabe ima delavec na konkretni telefonski številki. Najčistejša rešitev v takih primerih je, da delodajalec določi vsoto, do katere lahko zaposleni telefonira (enako velja tudi pri zaposlenih, ki uporabljajo službeni telefon za zasebno uporabo), presežek pa plača zaposleni, razen če se delodajalec ne strinja z delavčevo obrazložitvijo povečanega obsega klicev za službene namene (https://www.iprs.si/fileadmin/user_upload/Pdf/brosure/Zasebnost_na_delovnem_mestu.pdf).

Poudarja torej določila, navedena v teoretičnem delu naloge, predvsem ZVOP-1. Na sliki 6 prikazujemo primer telefonskega izpiska klicanih številk, ki ga lahko torej delodajalec pregleda samo v primeru, ko je delavcu predstavil pogoje uporabe mobilnega aparata in še to samo v primeru, ko gre za zlorabo s strani delavca.

25.02.2012	23:41:22	0:00:04	0	SVNSM-Si.mobil	38640222xxx	In
25.02.2012	23:43:21	0:00:02	0	SVNSM-Si.mobil	38640444xxx	In
25.02.2012	23:45:04	0:00:02	0	SVNSM-Si.mobil	38640666xxx	In
25.02.2012	23:46:37	0:00:02	0	SVNSM-Si.mobil	38640888xxx	In

Slika 6: Primer izpiska klicanih številk
(Vir: https://pravokator.si/index.php/2012/03/18/ko-poklicejo-hekerji-spreminjanje-klicne-identifikacije-telefonskih-klicev/)

4.6 Statistika prejetih prijav

Z analiziranjem letnih poročil Urada informacijskega pooblaščenca ter objavljenih vsebin nismo prišli do informacij o številu posameznih prejetih prijav v zvezi z nezakonitim nadzorovanjem zaposlenih. Vseeno pa smo za potrebe diplomskega dela želeli predstaviti tudi podrobnejše statistične podatke, zato smo se obrnili neposredno na Urad informacijskega pooblaščenca ter zaprosili za manjkajoče podatke.

V svojem odgovoru so nam pojasnili, da tovrstne statistike sicer ne vodijo, vendar so nam posredovali podatke, ročno pridobljene s pomočjo vnosa ključnih besed, zaradi česar obstaja verjetnost manjšega odstopanja od dejanskega števila prejetih prijav. V tabeli 3 povzemamo pridobljene podatke.

Prijava zoper/leto	2011	2012	2013	2014 (do 30. 4. 2014)	SKUPAJ
izvajanje videonadzora	26	21	20	4	71
neustrezno zavarovanje osebnih podatkov zaposlenih	8	10	11	3	32
poseg v elektronsko pošto	5	13	17	4	39
prijave zaradi nadzora interneta	1	1	1	1	4
sledenje zaposlenim s pomočjo GPS-naprav	1	2	3	0	6

Tabela 3: Število inšpekcijskih zadev v letih 2011, 2012, 2013, 2014
(Vir: lasten povzetek informacij Urad informacijskega pooblaščenca)

Iz tabele 3 lahko ugotovimo, da Urad informacijskega pooblaščenca na področju prijav zoper delodajalce, ki domnevno nezakonito izvajajo nadzor nad zaposlenimi s pomočjo tehnologije, prejmejo največ prijav v zvezi z izvajanjem videonadzora, sledijo prijave zoper nedovoljeni poseg v elektronsko pošto, takoj za njimi sledijo prijave zoper neustrezno zavarovanje osebnih podatkov zaposlenih. Najmanj prijav prejmejo zoper sledenje z GPS-napravami, prijave zaradi nadzora interneta pa so bile vsega skupaj 4 (Urad informacijskega pooblaščenca, 2014).

Ker ugotavljamo razsežnost obravnavanega pojava, sami predstavljeni podatki v tabeli 3 ne pokažejo razsežnosti problematike. Zato smo za primerjavo uporabili še podatke Statističnega urada RS, ki smo jih povzeli v tabeli 4. Objavili so, da je v Sloveniji v letu 2012 poslovalo 161.636 poslovnih subjektov, zato lahko sklepamo, da so prejete prijave v Uradu informacijskega pooblaščenca bolj izjemni primeri in ne nekakšen zelo razširjen pojav (https://www.stat.si/novica_prikazi.aspx?id=5900).

Leto 2012	Število podjetij	Osebe, ki delajo
Skupaj	161.636	817.801

Tabela 4: Število podjetij in zaposlenih v letu 2012
(Vir: https://www.stat.si/novica_prikazi.aspx?id=5900)

Vseeno se poraja vprašanje, ali ni vzrok majhnega števila prejetih prijav posledica nepoznavanja pravic med zaposlenimi. Podatki statističnega urada kažejo, da je bilo v letu 2012 817.801 ljudi, ki so delali. Zato bomo v nadaljevanju za potrebe diplomskega dela opravili anketo (http://www.stat.si/novica_prikazi.aspx?id=5900).

5 ANKETA O NADZORU NAD ZAPOSLENIMI NA DELOVNEM MESTU

V predhodnih poglavjih smo opisali pomembne zakonske določbe in predvidene sankcije ter navedli pomembne ugotovitve Urada informacijskega pooblaščenca. V tem poglavju pa bomo predstavili anketo, ki smo jo opravili za potrebe diplomskega dela.

Anketo smo izvedli s pomočjo spletnega anketiranja, privabiti smo želeli čim večji krog naključno izbranih sodelujočih, zato smo udeležence povabili preko socialnih in družbenih omrežij npr. Facebooka in Twitterja. Bistvo ankete je bilo spoznati zavedanje zaposlenih o zakonskih pravicah, navedenih v teoretičnem delu naloge, torej o svojih pravicah in ravnanju delodajalcev v njihovem primeru.

Zastavljena vprašanja smo razdelili po posameznih obravnavanih področjih, in sicer glede:

- videonadzora,
- varstva zbranih osebnih podatkov,
- sledenju z GPS-napravami,
- nadzoru elektronske pošte in interneta,
- uporabi biometrije.

Zavedamo se, da vsi anketiranci na svojem delovnem mestu nimajo stika z vsebino vprašanj, zato smo dopustili, da so lahko nekatera vprašanja pustili neizpolnjena. Čas izvedbe ankete je bil od 20. 5. 2014 do 25. 5. 2014, v njej je sodelovalo 30 anketirancev, od tega jih je anketo dokončalo 28. Na sliki 7 prikazujemo starostno skupino tistih anketirancev, ki so želeli odgovoriti na vprašanje. V največjem številu sta bili zastopani skupini od 36 do 50 let in več kot 50 let.

Slika 7: Predstavitev odgovorov na 18. vprašanje
(Vir: lasten povzetek po *https://www.1ka.si/a/42139*)

Odgovore na ostala demografska vprašanja predstavljamo v tabeli 5, iz katere je razvidno, da je v njej sodelovalo največ delovno aktivnih, več žensk kot moških, največ tistih, ki imajo srednješolsko izobrazbo, sledijo jim tisti z višjo in visokošolsko izobrazbo.

Vprašanje	Kakšen je vaš trenutni status?	
Odgovori	Število odgovorov	Odstotek odgovorov
Aktivni	23	88%
Neaktivni	1	4 %
Brezposelni	2	8 %
SKUPAJ	26	100 %
Vprašanje	Spol	
Odgovori	Število odgovorov	Odstotek odgovorov
Moški	10	40 %
Ženski	15	60 %
SKUPAJ	25	100 %
Vprašanje	Kakšna je vaša formalno dosežena izobrazba?	
Odgovori	Število odgovorov	Odstotek odgovorov
Osnovna šola	0	0 %
Srednja šola	12	48 %
Višja, visoka šola	11	44 %
Univerzitetna izobrazba in več	2	8 %
SKUPAJ	25	100 %

Tabela 5: Rezultati odgovorov na demografska vprašanja
(Vir: lasten povzetek po *https://www.1ka.si/a/42139*)

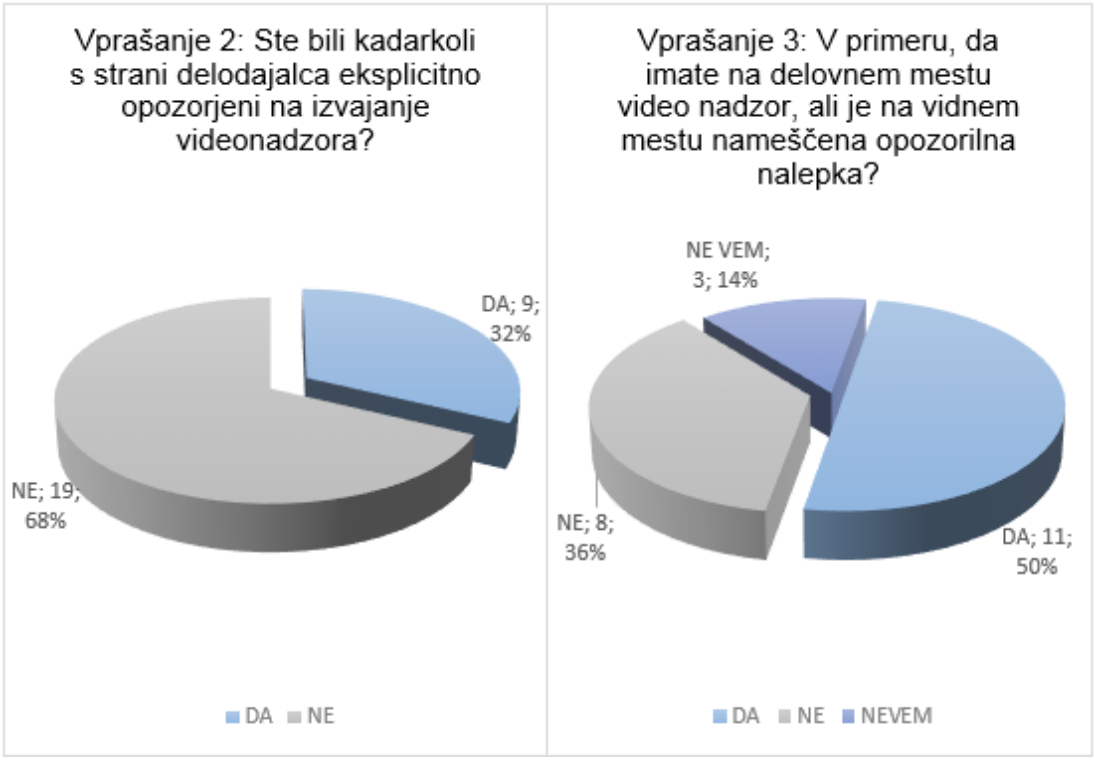
5.1 Analiza sklopa vprašanj o videonadzoru

V teoretičnem delu naloge smo navedli pomembnejša zakonska določila na področju videonadzora, predvsem navedbe 74. in 77. člena ZVOP-1. V analizi ugotovitev Urada informacijskega pooblaščenca smo tudi povzeli njihovo najpomembnejšo ugotovitev na tem področju, in sicer, da je videonadzor dopusten le v primeru, ko varovanja premoženja ni mogoče doseči z milejšimi ukrepi.

Vprašanje 1	Imate v prostorih vašega delovnega mesta nameščen video nadzorni sistem?	
Odgovori	Število odgovorov	Odstotek odgovorov
da	15	54 %
ne	13	46 %
Skupaj	28	100 %

Tabela 6: Odgovori na 1. anketno vprašanje
(Vir: lasten povzetek po https://www.1ka.si/a/42139)

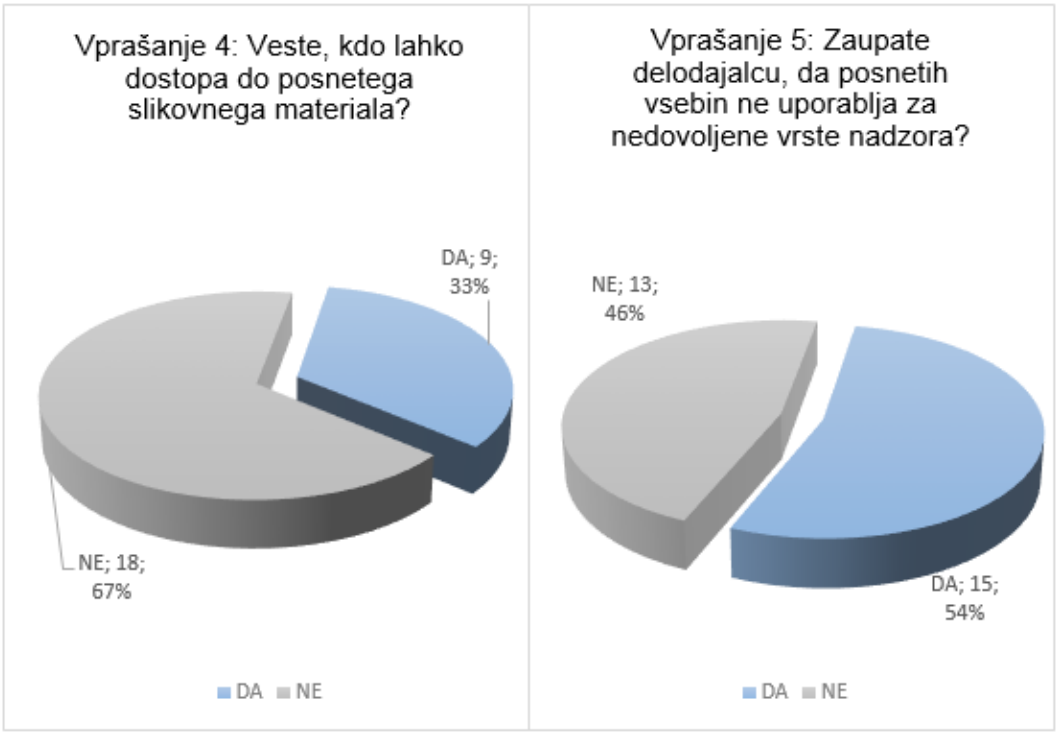
Z zastavljenimi vprašanji v anketi pa smo želeli ugotoviti najprej, koliko delovnih mest je opremljenih z videonadzorom, kar ponazarjamo v tabeli 6, kjer lahko ugotovimo, da ima več kot polovica anketirancev na svojem delovnem mestu nameščen video nadzorni sistem. Odgovorov nakazujejo, da delodajalci pogosto uporabljajo video nadzor za zaščito svoje lastnine.



Slika 8: Odgovori na anketni vprašanji 2 in 3
(Vir: lasten povzetek po https://www.1ka.si/a/42139)

Na sliki 8 so predstavljeni odgovori na vprašanja, kjer nas je zanimalo, koliko zaposlenih je delodajalec eksplicitno opozoril na izvajanje videonadzora, kot velevajo določila ZDR-1 oz. ostala zakonska določila. Iz odgovorov izhaja, da velika večina ni bila posebej opozorjena. Za prikaz rezultatov smo izbrali tortni diagram, pri vsakem kosu je navedeno število prejetih odgovorov in odstotek glede na skupno število prejetih odgovorov, tovrstno metodo ponazoritve rezultatov smo uporabili v vseh tortnih diagramih. Iz odgovorov na zastavljeno 3. vprašanje smo želeli ugotoviti, ali delodajalci spoštujejo določilo, da morajo v primeru videonadzora z nalepko opozarjati na tovrsten nadzor. Odgovori razkrivajo, da velika večina delodajalcev izobesi ustrezno nalepko, saj jo je opazilo več kot 50 % zaposlenih. Odstotek tistih, ki so odgovorili negativno, je sicer visok, kar 36 %, vendar to lahko pripišemo tudi njihovi nepozornosti. Z anketnim vprašanjem 4 smo želeli preveriti, ali zaposleni vedo, kdo lahko dostopa do posnetega slikovnega materiala, z vprašanjem 5 pa neko splošno zaupanje zaposlenih v tovrstni nadzor. Rezultate odgovorov podrobno prikazujemo na sliki 9. Ugotovimo lahko, da velika večina

anketirancev ne ve, kdo lahko dostopa do posnetega materiala, vseeno pa anketiranci zaupajo delodajalcem, da posnetih vsebin ne uporabljajo v nedovoljene namene.



Slika 9: Odgovori na anketni vprašanji 4 in 5
(Vir: lasten povzetek po https://www.1ka.si/a/42139)

5.2 Analiza sklopa vprašanj o varovanju baz osebnih podatkov

Sklop vprašanj se nanaša predvsem na poznavanje 46. in 48. člena ZDR-1, ki smo jih podrobneje opisali v teoretičnem delu naloge, med zaposlenimi. V tabeli 7 prikazujemo zbrane podatke, pridobljene z odgovori na 6. anketno vprašanje. Pri tem vprašanju smo poskušali ugotoviti, ali imajo v podjetju sistematiziran in natančno opredeljen dostop do zbirk osebnih podatkov zaposlenih. Od skupno 26 anketirancev jih je velika večina odgovorila pritrdilno.

Vprašanje 6	Imate v vašem podjetju opredeljene in sistematizirane pogoje dostopa do zbirke osebnih podatkov?	
Odgovori	Število odgovorov	Odstotek odgovorov
da	19	73 %
ne	3	12 %
ne vem	4	15 %
SKUPAJ	26	100 %

Tabela 7: Odgovori na anketno vprašanje 6
(Vir: lasten povzetek po https://www.1ka.si/a/42139)

Vprašanje 7	Ste mogoče že kdaj zahtevali vpogled v svoje zbrane podatke?	
Odgovori	Število odgovorov	Odstotek odgovorov
da	4	15 %
ne	22	85 %
SKUPAJ	26	100 %

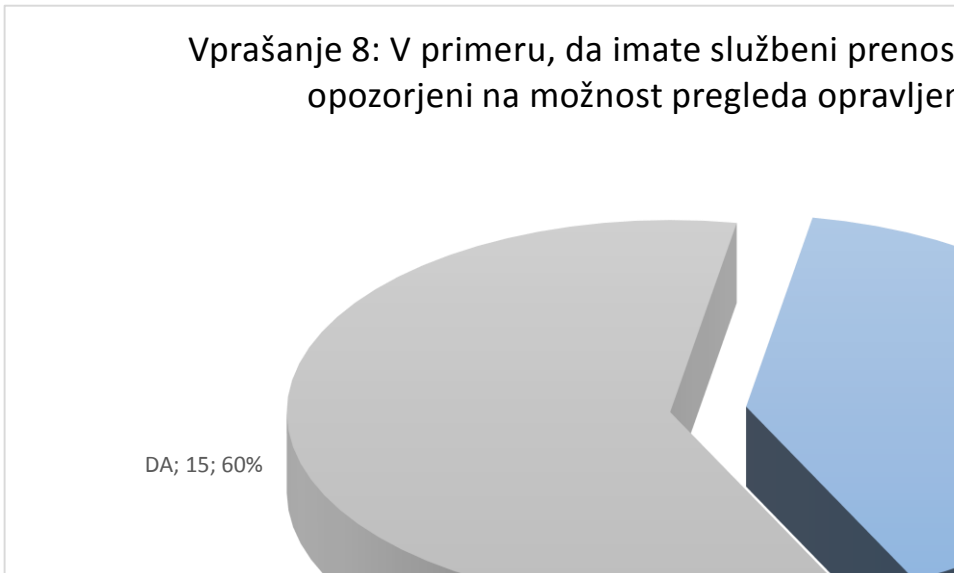
Tabela 8: Odgovori na anketno vprašanje 7
(Vir: lasten povzetek po https://www.1ka.si/a/42139*)*

Z vprašanjem 7 smo poskušali ugotoviti, koliko anketirancev je že zahtevalo vpogled v zbrane podatke, iz odgovorov pa lahko zaključimo, da velika večina anketirancev tega še nikoli ni storila. Podatke smo prikazali v tabeli 8.

5.3 Analiza sklopa vprašanj o nadzoru nad aparati mobilne telefonije

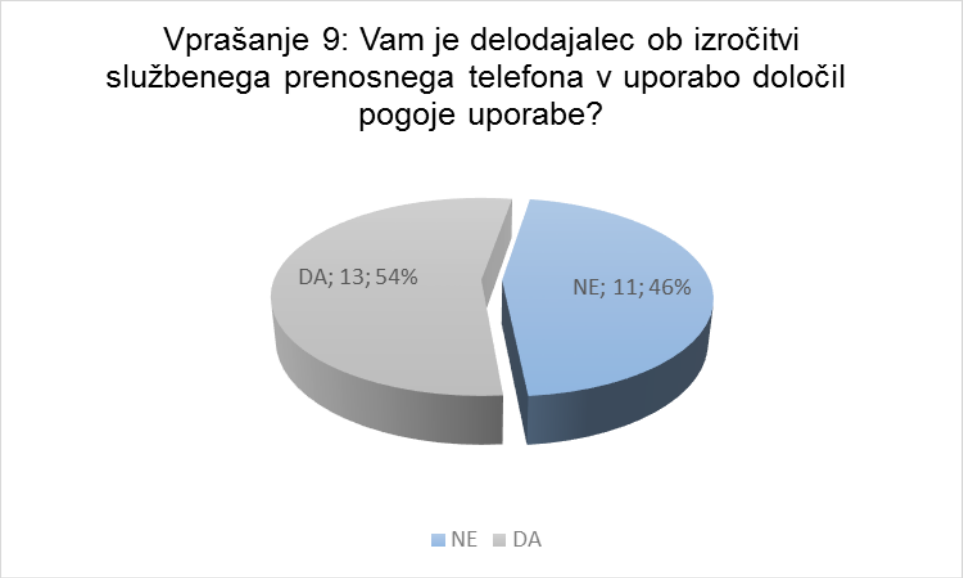
V tem sklopu smo želeli pri zaposlenih preveriti, kako ravnajo delodajalci, predvsem v smislu priporočil in obrazložitve te tematike Urada informacijskega pooblaščenca, navedenih v poglavju 4.6. Vprašanje 8 smo zastavili tako, da smo preverili predvsem to, ali delodajalci opozorijo na možnost, da v primeru zlorabe službenega telefona lahko pogledajo izpisek klicanih številk.

Večina anketirancev je odgovorila, da so bili na to možnost opozorjeni, podrobne rezultate odgovora prikazujemo na sliki 10.



Slika 10: Odgovori na 8. anketno vprašanje
(Vir: lasten povzetek po https://www.1ka.si/a/42139)

Iz odgovorov na 9 vprašanje, ki jih prikazujemo na sliki 11, smo poskušali preveriti, ali delodajalci zaposlenim pred uporabo mobilnega telefona določijo pogoje njegove uporabe. Odgovori nakazujejo, da v več kot polovici primerov delodajalci to storijo.



Slika 11: Odgovori na 9. anketno vprašanje
(Vir: lasten povzetek po https://www.1ka.si/a/42139*)*

5.4 Analiza sklopa vprašanj o nadzoru elektronske pošte in interneta

V tabeli 8 prikazujemo odgovore na vprašanja, ki se nanašajo na sklop o nadzoru elektronske pošte. Na ta zastavljena vprašanja je odgovorilo samo 10 anketirancev.

Vprašanje 10	Imate na delovnem mestu omejitve pri dostopu do spletnih strani in ali vam je delodajalec predstavil pogoje uporabe?	
Odgovori	Število odgovorov	Odstotek odgovorov
da	5	50 %
ne	5	50 %
SKUPAJ	10	100 %

Tabela 9: Predstavitev odgovorov na vprašanje 12
(Vir: lasten povzetek po https://www.1ka.si/a/42139*)*

Odgovori prikazujejo, da delodajalci zelo pogosto uporabljajo omejitve pri dostopu do spletnih strani, saj je polovica anketirancev odgovorila, da tovrstne omejitve imajo, ter da jim je delodajalec tudi predstavil pogoje uporabe. V nadaljevanju ankete nas je zanimalo tudi, koliko delodajalcev določi pogoje uporabe elektronske pošte in uporablja filtre (velikost datotek itd.). Odgovore prikazujemo v tabeli 9, iz katere izhaja, da 40 % zaposlenih nima tovrstnih omejitev elektronske pošte, 30 %

se s tovrstnimi vprašanji in tematiko še ni srečala, 30 % vprašanih pa je delodajalec predstavil pogoje uporabe elektronske pošte.

Vprašanje 11	Vam je delodajalec predstavil pogoje uporabe elektronske pošte in ali uporablja filtre (velikost datotek itd.) ter ali ste bili seznanjeni s pogoji uporabe?	
Odgovori	Število odgovorov	Odstotek odgovorov
Da, delodajalec mi je predstavil pogoje uporabe.	3	30 %
Ne, nimamo nobenih omejitev.	4	40 %
S tovrstno tematiko sploh nisem seznanjen.	3	30 %
SKUPAJ	10	100 %

Tabela 10: Predstavitev odgovorov na vprašanje 11
(Vir: lasten povzetek po https://www.1ka.si/a/42139)

5.5 Analiza sklopa vprašanj o biometriji

Uporaba biometričnih podatkov je pri nas zelo redka. To potrjujejo tudi odgovori na vprašanji 12 in 13, ki jih prikazujemo v tabeli 7. Z navedenimi vprašanji smo želeli preveriti upoštevanje v teoretičnem delu navedenih zakonskih določil s strani delodajalcev. Na 12. vprašanje je vseh 25 anketirancev odgovorilo, da delodajalec pri njih ne uporablja biometričnih podatkov. Na vprašanje 13, kjer nas je zanimalo, ali jim je delodajalec predstavil namen zbiranja biometričnih podatkov, so sicer 3 od 26 odgovorili z da, čeprav na predhodno vprašanje niso odgovorili pritrdilno.

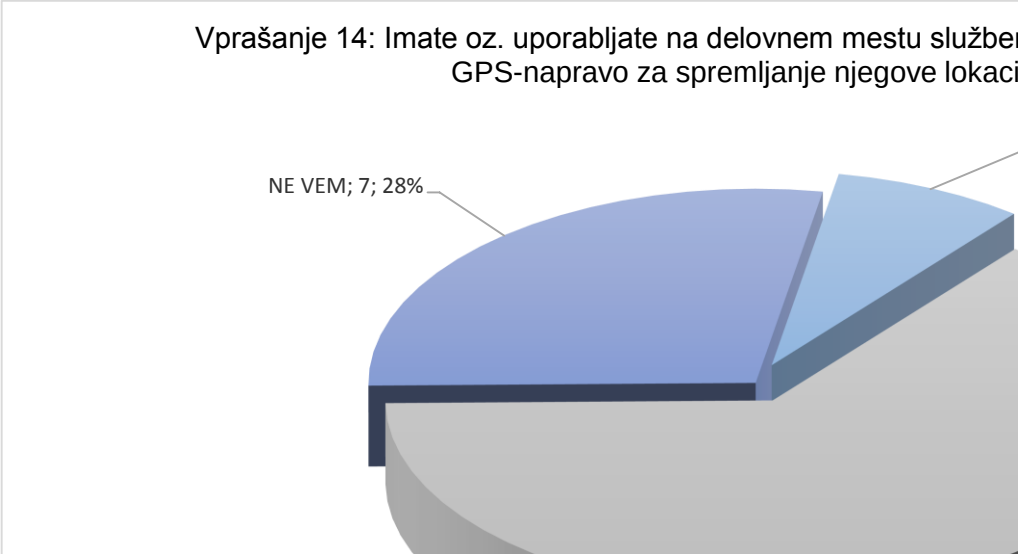
Vprašanje 12	Ali v vašem podjetju delodajalec uporablja vaše biometrične podatke za dostop do prostorov, podatkov itd. (npr. prstni odtis, mrežnica)	
Odgovori	Število odgovorov	Odstotek odgovorov
da	0	0 %
ne	25	100 %
SKUPAJ	25	100 %
Vprašanje 13	Vam je delodajalec predstavil namen zbiranja biometričnih podatkov?	
Odgovori	Število odgovorov	Odstotek odgovorov
da	3	12 %
ne	23	88 %
SKUPAJ	26	100 %

Tabela 11: Predstavitev odgovorov na vprašanji 12 in 13
(Vir: lasten povzetek po https://www.1ka.si/a/42139)

5.6 Analiza sklopa vprašanj o nadzoru z GPS-napravami

V analizi najpogostejših kršitev pri nadzoru nad zaposlenimi s strani delodajalcev se je pojavila tudi tehnika sledenja s GPS-napravami. Kako pri uporabi teh naprav v vozila, namenjena uporabi na delovnem mestu, ravnajo delodajalci, smo želeli preveriti v 14. in 15. vprašanju. S 14. vprašanjem smo želeli izvedeti, koliko delodajalcev uporablja GPS-naprave v vozilih.

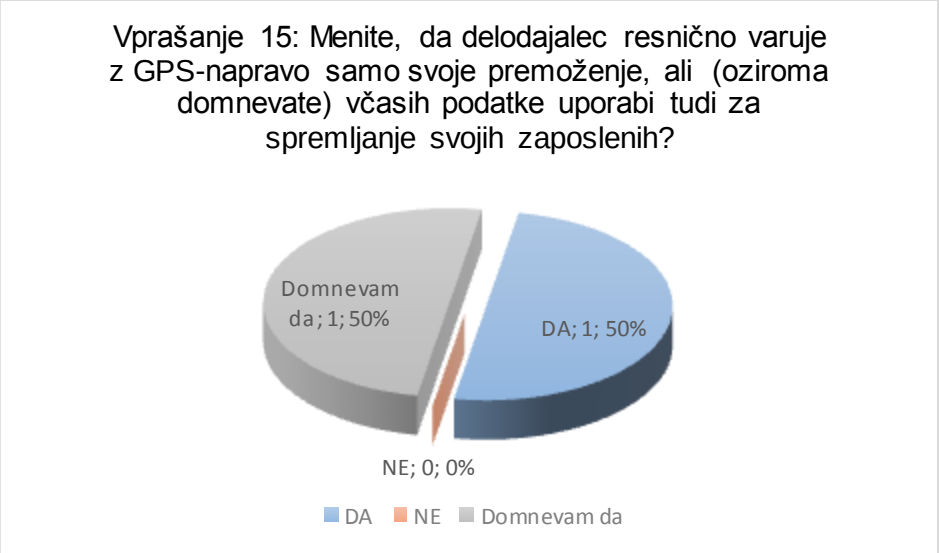
Na sliki 12 prikazujemo odgovore na 14. vprašanje, s katerim smo želeli preveriti razširjenost uporabe GPS-naprav za sledenje lokacije. Odgovori zaposlenih na vprašanje kažejo, da na splošno tovrstna oprema ni posebno razširjena, seveda se v anketi nismo omejili na ciljno skupino zaposlenih (kot so npr. varnostniki, pismonoše), kjer je uporaba tovrstna oprema pogostejša.



Slika 12: Odgovori na vprašanje 14
(Vir: lasten povzetek po https://www.1ka.si/a/42139)

Vseeno se moramo zavedati, da tovrstno opremo delodajalci lahko namestijo tako, da je zaposleni niti ne zaznajo. Posledica tega je lahko odgovor le dveh anketirancev, da imajo vozila opremljena s tovrstnimi napravami.

Na sliki 13 prikazujemo odgovore na vprašanja, ki smo jih zastavili le tistim anketirancem, ki so na prejšnje vprašanje odgovorili pritrdilno. Z njim smo želeli preveriti neko splošno zaupanje zaposlenih delodajalcu o pravilni uporabi tovrstnih naprav. Čeprav je ostal razmeroma majhen vzorec anketirancev, je vseeno iz odgovorov možno sklepati, da se zaposleni ob uporabi tovrstnih naprav s strani delodajalcev ne počutijo ravno lagodno.



Slika 13: Odgovori na vprašanje15
(Vir: lasten povzetek po https://www.1ka.si/a/42139*)*

5.7 Zaključki opravljene ankete

Anketo smo v diplomski nalogi uporabili kot orodje za ugotavljanje zavedanja zaposlenih o svojih pravicah in dejanskem ravnanju delodajalcev pri posameznih obravnavanih temah. Anketo smo opravili na naključnem, manjšem splošnem vzorcu zaposlenih, zato dobljenih podatkov ne moremo posplošiti na neko splošno sliko nadzora.

V sklopu vprašanj, ki se nanašajo na videonadzor, smo ugotovili, da je več kot 50 % delovnih mest opremljenih z videonadzorom, kar pomeni, da delodajalci tovrstno opremo pogosto uporabijo za zaščito premoženja. Prav tako ima večina delodajalcev nameščene ustrezne opozorilne nalepke. Zaposleni običajno ne vedo, kdo vse ima dostop do posnetih vsebin in načeloma zaupajo delodajalcu, da jih ne uporablja za nedovoljene namene.

Odgovori na anketna vprašanja o varstvu baz osebnih podatkov razkrivajo, da imajo delodajalci v veliki večini sistematiziran dostop do podatkov, vendar pa anketiranci možnosti vpogleda v zbrane podatke ne uporabijo pogosto. Iz odgovorov je prav tako možno zaključiti, da zaposleni zaupajo delodajalcem glede zbiranja obdelave in varstva osebnih podatkov.

Rezultati vprašanj o nadzoru mobilne telefonije razkrivajo, da delodajalci v veliki večini zaposlenim določijo pogoje uporabe službenega telefona in možnost pregleda klicanih številk v primeru zlorab. Zaposlenim tudi natančno predstavijo pogoje uporabe mobilnega aparata.

Odgovori na sklop vprašanj o nadzoru elektronske pošte in interneta razkrivajo, da delodajalci pogosto določijo namene uporabe elektronske pošte in interneta v službene namene, vendar s samimi omejitvami pogosto ne operirajo, saj 70 % anketirancev teh omejitev ne zazna.

Rezultati opravljene ankete bi nas lahko zavedli, da biometrija v slovenskem prostoru ni posebno razširjena, saj je ne uporabljajo niti pri enem anketirancu. Našo ugotovitev bi lahko povezali tudi s številom prejetih prijav, ki smo jih navedli v 4. poglavju naloge. Vendar je treba upoštevati, da smo anketo opravljali na nekem splošnem vzorcu anketirancev, kjer dopuščamo možnost, da med naključno anketiranimi ni bilo tistih zaposlenih, ki imajo izkušnjo z uporabo biometrije s strani delodajalcev.

Z vprašanji glede nadzora in razširjenosti GPS-naprav za spremljanje službenih vozil smo v pravi vrsti želeli preveriti razširjenost njihove uporabe. Pri interpretaciji rezultatov je treba poudariti, da je bila anketa opravljena na naključnem vzorcu zaposlenih in bi lahko s ciljno anketo prišli do drugačnih ugotovitev, pa vendar odgovori prikazujejo, da na splošno večina delodajalcev tovrstne zaščite ne uporablja oziroma je zaposleni niso zaznali, niso pa bili niti posebej opozorjeni.

6 ZAKLJUČEK

Uvodoma smo navedli, da razvoj tehnologije delodajalcem prinaša neslutene možnosti za nadzor zaposlenih ter da obstaja tanka meja med pravico delodajalca do varovanja premoženja in pravicami delavcev do zasebnosti. Cilj diplomske naloge je bilo raziskati spoštovanje zakonskih določb s strani delodajalcev, proučiti in navesti ugotovitve Urada informacijskega pooblaščenca ter ugotoviti, koliko se zaposleni zavedajo pravic do spoštovanja njihove zasebnosti.

Sodobna tehnologija ponuja neslutene možnosti za uporabo moderne programske in strojne opreme za uporabo v nedovoljene namene, zato smo nalogo omejili na področje:

- videonadzora,
- uporabe interneta,
- zbiranja in obdelave podatkov,
- elektronsko pošto,
- sledenje z GPS-napravami,
- spremljanjem telefonskim pogovorom.

V teoretičnem delu naloge smo navedli ključne določbe slovenske zakonodaje in predvidene sankcije, predpisane v primeru zlorab. Navedene teoretične osnove smo povezali z ugotovitvami Urada informacijskega pooblaščenca. Proučevanje njihovih

letnih poročil in objavljenih vsebin je vodilo v spoznanje, da delodajalci uporabljajo tovrstni nedovoljeni nadzor. Predstavili smo tudi njihova priporočila in smernice pri uporabi tehničnih pripomočkov. Njihova glavna smernica pravi, da lahko delodajalec uporabi tovrsten nadzor samo v primeru, ko zaščite pravic delodajalca ni mogoče doseči z milejšimi sredstvi.

Želeli smo oceniti razsežnosti tovrstnega pojava v Sloveniji, zato smo v diplomski nalogi uporabili tudi statistične podatke o prejetih prijavah na obravnavanih področjih. Prijazno so nam pripravili želene podatke, iz katerih izhaja, da prejmejo največ prijav zoper nedovoljen videonadzor na delovnem mestu, neustrezno zavarovanje osebnih podatkov, posege v elektronsko pošto. Pridobljene podatke smo tudi primerjali s podatki statističnega urada, kjer smo našli objavljene podatke o številu zaposlenih in podjetij za leto 2012. Primerjava pokaže, da glede na število poslovnih subjektov število prijav ni veliko. Ugotovitev nas je razveselila, saj pomeni, da so zagrožene sankcije v primeru zlorab, ki smo jih navedli v 3 poglavju, dovolj stroge, da večino delodajalcev odvrnejo od nezakonitega nadzora s pomočjo tehnologije.

Spoštovanje zakonskih določil smo želeli preveriti tudi sami, zato smo opravili anketo med zaposlenimi. Anketo smo opravili na manjšem, splošnem vzorcu naključno izbranih anketirancev, zato ne moremo posplošiti, da izkazuje neko splošno stanje nadzora. Iz prejetih odgovorov sledi, da večina delodajalcev spoštuje določila o videonadzoru, prav tako v večini primerov delodajalec poda pogoje uporabe službenega telefona. Ugotovitve, ki sledijo iz odgovorov o nadzoru elektronske pošte in interneta ter sledenja službenim vozilom, sicer ne dajejo nekega pravega odgovora, kar je moč pripisati dejstvu, da delavci težko zaznajo tovrstne nadzorne delodajalcev, vseeno pa delodajalci tudi v tem primeru določijo pogoje uporabe. Odgovori o razširjenosti uporabe biometrije razkrivajo, da v Sloveniji ni zelo razširjena.

Iz navedenega lahko sedaj podamo ugotovitve, ki smo jih navedli kot cilj naloge. Glede na primerjavo statističnih podatkov prejetih prijav Urada informacijskega pooblaščenca in objavljenih podatkov Statističnega urada RS, ki smo jih vzeli za primerjavo, sklepamo, da ne gre za zelo razsežen problem in da so tovrstni prijemi delodajalcev bolj izjema kot pravilo, kar potrjuje tudi opravljena anketa.

Analiza zakonodaje, vsebin objavljenih podatkov in poročil Urada informacijskega pooblaščenca nas lahko kot zaposlene pomirja. Zakonodaja je zastavljena dovolj restriktivno, imamo pa tudi Urad informacijskega pooblaščenca, ki ukrepa na področju zlorab, prav tako pa delodajalci iz njihovih priporočil in smernic dobijo vse potrebne podatke za uporabo tehnoloških nadzornih sistemov, da pri tem ne prestopijo zakonskih določil in naletijo na stroge sankcije.

LITERATURA IN VIRI

Knjige:

- Kazenski zakonik. *Uradni list Republike Slovenije*, št. 55/2008.
- Zakon o delovnih razmerjih. *Uradni list Republike Slovenije*, št. 21/2013.
- Zakon o elektronskih komunikacijah. *Uradni list Republike Slovenije*, št. 109/2012.
- Zakon o varstvu osebnih podatkov. *Uradni list Republike Slovenije*, št. 94/2007.

Spletne strani:

- *Bent Excellent d.o.o. Sledenje in nadzor z ročnim GPS sledilcem*. Pridobljeno dne 14. 6. 2014 z naslova http://www.easytracker.si/si/resitve-sledenja/sledenje-in-nadzor-z-rocnim-gps-sledilcem.php.
- *Biromatik NT d.o.o. Tehnični nadzor delovnih mest skozi pravico do zasebnosti.* Pridobljeno dne 14. 6. 2014 z naslova http://www.e-tm.si/eTM_data/dokumenti/ZAKONODAJA_VIDEONADZOR.pdf.
- Cerar, G. (21. 9. 2006). *Sindikat RTV preprečil videonadzor*. Mladina 38. Pridobljeno dne 5. 6. 2014 z naslova http://www.mladina.si/90490/uvo-manipulator--gregor_cerar-2/?utm_source=tednik%2F200638%2Fclanek%2Fuvo-manipulator--gregor_cerar-2%2F&utm_medium=web&utm_campaign=oldLink.
- Čepar, N. (15. 11. 2013). *Ko šef postane veliki brat*. Žurnal24. Pridobljeno dne 29. 5. 2014 z naslova http://www.zurnal24.si/ko-sef-postane-veliki-brat-clanek-212273.
- Hölbl, M. (30. 5. 2007). *Spletni napadi*. Monitor. Pridobljeno 29. 5. 2014 z naslova http://www.monitor.si/clanek/spletni-napadi/122720.
- Hvaliček, M. (1. 6. 2012). *E-pošta in zasebnost na delovnem mestu*. Eudace d.o.o. Pridobljeno 29. 5. 2014 z naslova http://www.eudace.eu/knjiznica/clanki/2013021410315019.
- Kovačič, M. (18. 3. 2012). *Ko pokličejo hekerji – spreminjanje klicne identifikacije telefonskih klicev.* Provokator. Pridobljeno 29. 5. 2014 z naslova https://pravokator.si/index.php/2012/03/18/ko-poklicejo-hekerji-spreminjanje-klicne-identifikacije-telefonskih-klicev.
- Statistični urad Republike Slovenije (2013). *Podjetja, Slovenija, 2012 – končni podatki.* Pridobljeno dne 29. 5. 2014 z naslova https://www.stat.si/novica_prikazi.aspx?id=5900.
- Urad informacijskega pooblaščenca (2011). *Pričakovana zasebnost na službenih računalnikih.* Pridobljeno 29. 5. 2014 z naslova https://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/odlocbe-in-mnenja-varstvo-osebnih-

podatkov/?tx_jzvopdecisions_pi1%5BshowUid%5D=2046&cHash=484a541185a0b9224a452abf883028b9.

- Urad informacijskega pooblaščenca (2014). *Zasebnost na delovnem mestu*. Pridobljeno 29. 5. 2014 z naslova https://www.iprs.si/fileadmin/user_upload/Pdf/brosure/Zasebnost_na_delovnem_mestu.pdf.
- Ustavno sodišče Republike Slovenije (2014). *Ilustrirana Ustava Republike Slovenije (v stripu)*. Pridobljeno 29. 5. 2014 z naslova http://www.us-rs.si/strip/.

Interni dokumenti:

- *Odgovor Urada informacijskega pooblaščenca* (2014). Ljubljana: Urad informacijskega pooblaščenca.

KAZALO SLIK

KAZALO TABEL

KRATICE IN AKRONIMI

RS:	Republika Slovenija
ZVOP-1:	Zakon o varstvu osebnih podatkov
ZEkom-1:	Zakon o elektronskih komunikacijah
ZDR-1:	Zakon o delovnih razmerjih
KZ-1:	Kazenski zakonik
GPS:	Global Positioning System: Globalni sistem pozicioniranja
€:	denarna valuta evro

PRILOGA 1: ANKETNI VPRAŠALNIK

Nadzor nad zaposlenimi

Q1 - Imate v prostorih vašega delovnega mesta nameščen video nadzorni sistem?

☐ da
☐ ne

Q2 - Ste bili kadarkoli s strani delodajalca eksplicitno opozorjeni na izvajanje video nadzora?

☐ da
☐ ne

Q3 - V primeru, da imate na delovnem mestu video nadzor, ali je na vidnem mestu nameščena opozorilna nalepka?

☐ da
☐ ne
☐ ne vem

Q4 – Veste, kdo lahko dostopa do posnetega slikovnega materiala?

◯ da
◯ ne

Q5 - Zaupate delodajalcu, da posnetih vsebin ne uporablja za nedovoljene vrste nadzora?

◯ da
◯ ne

Q6 - Imate v vašem podjetju opredeljene in sistematizirane pogoje dostopa do zbirke osebnih podatkov?

◯ da
◯ ne
◯ ne vem

Q7 - Ste mogoče že kdaj zahtevali vpogled v svoje zbrane podatke?
◯ da
◯ ne

Q8 - V primeru, da imate službeni prenosni telefon, ste bili opozorjeni na možnost pregleda opravljenih klicev?

☐ da
☐ ne

Q9 - Vam je delodajalec ob izročitvi službenega telefona v uporabo določil pogoje uporabe?

◯ da
◯ ne

Q10 - Imate na delovnem mestu omejitve pri dostopu do spletnih strani in ali vam je delodajalec predstavil pogoje uporabe?

◯ da
◯ ne

Q17 - Vam je delodajalec predstavil pogoje uporabe elektronske pošte in ali uporablja filtre (velikost datotek itd.), ter ali ste bili seznanjeni s pogoji uporabe?
Možnih je več odgovorov

☐ Da, delodajalec mi je predstavil pogoje uporabe
☐ Ne, nimamo nobenih omejitev
☐ S tovrstno tematiko sploh nisem seznanjen

Q12 - Ali v vašem podjetju delodajalec uporablja vaše biometrične podatke za dostop do prostorov, podatkov itd. (npr. prstni odtis, mrežnica)?

◯ da
◯ ne

Q13 - Vam je delodajalec predstavil namen zbiranja biometričnih podatkov?

☐ da
☐ Ne

Q14 - Imate oz. uporabljate na delovnem mestu službeno vozilo, opremljeno z GPS-napravo za spremljanje njegove lokacije?

◯ da
◯ ne
◯ ne vem

IF (2) Q14 = [1]
Q15 - Menite, da delodajalec resnično varuje z GPS-napravo samo svoje premoženje ali (oziroma domnevate) včasih podatke uporabi tudi za spremljanje svojih zaposlenih?

☐ da
☐ ne
☐ Domnevam, da včasih uporabi GPS informacije tudi za sledenje

Q16 - Kakšna je vaša formalno dosežena izobrazba?

◯ Osnovna šola
◯ Srednja šola
◯ Višja, visoka šola
◯ Univerzitetna izobrazba in več

XSPOL - Spol:

◯ Moški
◯ Ženski

XSTAR2a4 - V katero starostno skupino spadate?

◯ do 25 let
◯ 26–35 let
◯ 36–50 let
◯ več kot 50 let

XDS2a4 - Kakšen je vaš trenutni status?

◯ Aktivni
◯ Neaktivni
◯ Brezposelni

(vir: https://www.1ka.si/admin/survey/index.php?anketa=42139)