

TALLINNA TEHNIKAÜLIKOOL

Sotsiaalteaduskond

Tööstuspsühholoogia instituut

Kaire Saarep

JÄLGIMISSEADMETE KASUTAMINE TÖÖKOHAL JA TÖÖTAJA ÕIGUS

PRIVAATSUSELE

Magistritöö

Juhendajad: Aive Pevkur, PhD

Tallinn 2017

Deklareerin, et käesolev magistritöö,
mis on minu iseseisva töö tulemus,
on esitatud Tallinna Tehnikaülikooli
magistrikraadi taotlemiseks ja selle alusel
ei ole varem taotletud akadeemilist kraadi.

Autor Kaire Saarep

“21“ mai 2017

Töö vastab kehtivatele nõuetele

Juhendaja professor Aive Pevkur

“ “ 2017

LÜHIKOKKUVÕTE

JÄLGIMISSEADMETE KASUTAMINE TÖÖKOHAL JA TÖÖTAJA ÕIGUS

PRIVAATSUSELE

Kaire Saarep

Tehnoloogilised vahendid on töökohal tavapärased töökorraldamise ja monitoorimise vahendid. Igapäevased on erinevad online platvormid, mille kaudu töötajaid värvatakse, tehakse taustauuringuid, samuti erinevad programmid ja mobiilirakendused, mille abil koostatakse töögraafikuid, jagatakse ettevõtte sisest informatsiooni jne. Koos infotehnoloogiliste lahenduste arenguga käib paratamatult kaasas oht isikuandmete lekkimisest ning arutelu, mis on konfidentsiaalne info, mil määral, millist infot isikute kohta võib sotsiaalmeedias, ettevõtete kodulehel ja internetis laiemalt jagada.

Järjest enam on töökohtadel erinevatel eesmärkidel kasutusel ka turvakaamerad. Kasutades igapäevaselt nutiseadmeid, kus kaamerafunktsioon on tavapärane, siis selle valguses kipub töökohtadel kaamerate kasutamine ja privaatsuse küsimus jääma unarusse. Ei teadvustata, mis ohte võib privaatsuse küsimusega mitte tegelemine kaasa tuua, seda nii töötajale kui ettevõttele tervikuna. Sellest tulenevalt on tarvis uurida, kuidas tööandjad uue olukorraga kohanenud on.

Magistritöö eesmärk on välja selgitada, millistel eesmärkidel kasutavad tööandjad töökohal turvakaameraid, kas nende kasutamine on õiguspärane ning kas turvakaamerate kasutamisega rikutakse töötajate õiguseid.

Uuringu tulemustest selgub, et toitlustusettevõtetes ei ole turvakamarad paigaldatud läbimõeldult ja eesmärgipäraselt. Suures osas ei vasta turvakaamerate paigaldamise ja kasutamise eesmärgid seadusest tulenevatele nõuetele. Enamik tööandjaid ei ole töötajaid turvakaamerate olemasolust kirjalikult korrektselt teavitanud ega selgitanud nende kasutamise eesmärke ja isikuandmete töötlemise põhimõtteid. Töötajate õigus privaatsusele ei ole töökohal tagatud ning sellele ei pöörata ettevõttesiseselt erilist tähelepanu.

Võtmesõnad: privaatsus, jälgimisseadmed, turvakaamera, tagajärjed, eesmärgipärane kasutamine

ABSTRACT

USING SURVEILLANCE EQUIPMENT AT THE WORKPLACE AND THE EMPLOYEE'S RIGHT TO PRIVACY

Kaire Saarep

Technological tools are common means at the workplace for work organisation and monitoring. In daily use there are different online platforms that are used for personnel recruitment and carrying out background checks, also various programs and mobile applications that are used for drawing up work schedules, sharing enterprise's internal information, etc. The development of IT solutions is inevitably accompanied by the danger of leaking of personal data, and the discussion about the nature of confidential information, to what extent and which information may be shared about people on social media, on the company's website and the internet.

Also the usage of security cameras for different purposes at workplaces is becoming increasingly common. When using connected devices with the standard camera function daily, in the light of this the usage of cameras and the issue of privacy at the workplaces tend to remain neglected. There is a lack of awareness about the dangers that may arise when the issues of privacy are not dealt with, both for the employee and the company as a whole. Due to that it is necessary to research how the employers have adapted to the new situation.

The objective of the master thesis is to find out for what purposes do employers use security cameras at the workplace, is using the cameras lawful, and are the employees' rights being violated by using security cameras.

The results of the research suggest that in catering establishments the security cameras are not positioned reasonably and purposefully. The purposes of installing and using security cameras for the most part do not correspond to legal requirements. The majority of the employers have not notified the employees about the security cameras in written form, nor explained the purposes of using the cameras and the principles for processing personal data. The employees' right to privacy at the workplace is not guaranteed and not enough attention is turned to this issue within the enterprise.

Keywords: privacy, surveillance equipment, security camera, consequences, purposeful usage

SISUKORD

LÜHIKOKKUVÕTE	3
ABSTRACT	4
LÜHENDITE LOETELU	6
SISSEJUHATUS	7
1 JÄLGIMISSEADMETE PAIGALDAMINE JA KASUTAMINE.....	11
1.1 Jälgimine ja jälgimisseadmed	11
1.2 Jälgimisseadmete töökohal paigaldamise ja kasutamise põhjused	12
1.3 Jälgimisseadmete legaalne ja eesmärgipärane paigaldamine.....	15
1.4 Jälgimisseadmete töökohal kasutamise mõjud ja tagajärjed.....	17
1.5 Jälgimisseadmete paigaldamise ja kasutamise kaasneda võivate negatiivsete tagajärgede vähendamine või ära hoidmine	19
2 PRIVAATSUSÕIGUSE RAAMISTIK	23
2.1 Privaatsus- ja andmekaitseõiguse kujunemine.....	24
2.2 Privaatsus ja andmekaitseõigus Euroopa Liidus	25
2.3 Privaatsus ja andmekaitseõigus Eestis ja Eesti töösuhetes	27
2.3.1 Õigus isikuandmete kaitsele.....	27
2.3.2 Isikuandmete töötlemise õiguslikud alused	28
2.4 Jälgimisseadmete kasutamine töösuhetes	31
3 EMPIIRILINE UURIMUS	37
3.1 Uurimuse eesmärk.....	37
3.2 Uurimuse meetodika	37
3.3 Valim.....	38
3.4 Küsimustik	38
4 TULEMUSED	40
4.1 Jälgimisseadmete paigaldamine ja kasutamine.....	40
4.2 Jälgimisseadmetega kogutud info turvalisus.....	44
4.3 Jälgimisseadmetest teavitamine	45
4.4 Järeldused ja arutelu.....	47
4.4.1 Jälgimisseadmete paigaldamine ja kasutamine.....	47
4.4.2 Jälgimisseadmetega kogutud info turvalisus.....	49
4.4.3 Jälgimisseadmest teavitamine	50
KOKKUVÕTE.....	53
RESUME	56
VIIDATUD KIRJANDUS.....	59
LISA 1.....	65
LISA 2.....	67

LÜHENDITE LOETELU

andmekaitse direktiiv	direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta
EIK	Euroopa Inimõiguste Kohus
EIKo	Euroopa Inimõiguste Kohtu otsus
EIÕK	Euroopa inimõiguste ja põhivabaduste kaitse konventsioon
EL	Euroopa Liit
hart	Euroopa Liidu põhiõiguste hart
IKS	isikuandmete kaitse seadus
konventsioon nr 108	isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon
PS	põhiseadus
RKTKo	Riigikohtu tsiviilkolleegium otsus
TLS	töölepingu seadus
TVK	tõvaidluskomisjon

SISSEJUHATUS

Nutitelefonid ja kogu muu tehnoloogia, mis ülikiirelt areneb, on järjest enam tavapärase elu lahutamatu osa. Inimestes ei tekita enam suuri emotsioone kui poodidesse ilmub üha rohkem nutikassasid, restoranidesse tahvelarvuteid, kus saab teenindajatele tagasisidet jagada ja füüsilised kliendikaardid asenduvad rakendustega nutitelefonis. Personalijuhid on juba pikemat aega kasutanud Google'i otsimootorit ja sotsiaalmeediat, et tõhustada töötajate värbamist. Töö korraldamisel on abiks videokonverentside hõlbustamine ja isegi töögraafikute koostamiseks mõeldud mobiilirakendused. Väga kiirelt on töökohtade lahutamatuks osaks muutunud ka eri tüüpi monitoorimisvahendid, sealhulgas kiipkaartide või sõrmejäljelugerite kasutamine, mis registreerivad kõik hoonest, kabinetist või muust ruumist sisenemised ja väljumised ning turvakaamerad, mille abil on võimalik jäädvustada töötaja igat liigutust (Ciocchetti, 2011).

Kogu tehnoloogia võidukäigu juures kipub privaatsuse küsimus justkui tüütu pagasina kaasas käima. Sellest hoolimata on kõigil inimestel oma privaatsfäär, mille austamist teiste isikute poolt peavad nad loomulikuks. Häirituna tunneb inimene ennast siis, kui tema privaatsust ohustatakse. Selle ilmestamiseks on võimalik tuua analoogne näide tervise valdkonnast – nii kaua, kuni tervis on korras, ei mõelda aktiivselt selle hoidmisele; nii kaua, kuni ei ole isiklikult tajutud privaatsuse riivet, ei paista see olulise teemana, millega on tarvis tegeleda. Olgugi, et vajadus privaatsuse järele on inimestel erinev, siis teatav ootus privaatsusele säilib igas olukorras. Üldiselt on kodu kohaks, kus ootus privaatsusele on kõrgeim. Samas, arvestades, et töökohal veedetakse väga suur osa oma ajast, siis säilib teatav ootus privaatsusele ka siin. Mida madalam on töökohal privaatsuse tase (sh teiste töötajate sekkumine töösse, turvakaamerate abil töö tegemise jälgimine), seda enam kogevad töötajad emotsionaalset kurnatust ehk läbipõlemist (Laurence, Fried & Slowik, 2013). Tööandjate huvi on, et töötajad annaksid endast maksimaalse ettevõtte huve silmas pidades. Arvestades, et jälgimisseadmete, sh turvakaamerate kasutamine kujutab endast võrreldes teiste monitoorimismeetoditega kõige intensiivsemat privaatsuse riivet üldse (Andmekaitse Inspeksioon (edaspidi AKI), 2011a: 69), siis nende kasutamisega põrkuvad töötajate ootused privaatsusele ja tööandjate huvid kaitsta oma vara ja selle tarbeks kontrollida töötajaid. Personalijuht kui võtmeisik töötaja ja tööandja huvide vahel peab leidma tasakaalu tehnoloogiliste vahendite rakendamisel ja privaatsuse küsimustes. Kuna ettevõtete eesmärgiks on võimalikult suure kasumi saavutamine, siis on oluline teada, kuidas vältida kasvõi teadmatusel põhjustatud töötajate produktiivsuse langust. Seetõttu on tööandjate jaoks oluline teadvustada, et privaatsuse küsimusega tuleb tegeleda.

Seda, et Eestis pakub privaatsusõigus nii töötajate kui tööandjate seas kõneainet, sealhulgas see, kuidas on juriidiliselt korrektne kasutada jälgimisseadmeid töökohal ning mil viisil tohib isikuandmeid töösuhetes töödelda, näitab AKI poole pöördumise arv. Jälgimisseadmete kasutamisega kogutakse ja töödeltakse isikuandmeid. AKI on isikuandmete õiguspärase töötlemise järelevalveasutus. 2009. aastal seadis AKI sisse nõuandetelefoni. Alates 2013. aastast on AKI kategoriseerinud teemad, mille osas neile enim helistatakse. 2013. aastal helistati inspektsiooni nõuandetelefonile kokku 1134 korral (2014 - 1141 korral, 2015 - 1136 korral), millest 120 korral (2014 - 94 korral, 2015 - 108 korral) tunti huvi isikuandmete töötlemise kohta töösuhetes ja 94 korral (2014 - 72 korral, 2015 - 78 korral) jälgimisseadmete kasutamise kohta (AKI, 2014, 2015, 2016). Arvestades asjaolu, et AKI tööst moodustab isikuandmete töötlemine töökohal ja jälgimisseadmetega seonduv vaid väikese osa, on märkimisväärne, et kuni 19% kõikidest kõnedest puudutab just neid kahte valdkonda.

Privaatsuse küsimus on olnud päevakorral eelkõige ettevõtetes, kus tööandjad on pidanud otseselt kokku puutama tarbijatega, kes on iseenda privaatsuse riive korral nõudnud ettevõtetelt selle tagamist. Seetõttu, neis sektorites, kus on otsene kokkupuude klientidega (nt kaubandus, toidlustus jms) on privaatsuse küsimus olnud aktuaalne (Levin, Foster, Nicholson & Hernandez, 2006). On leitud, et kõige enam monitoorimismeetodeid, sh jälgimisseadmeid kasutatakse teenindussektoris, aga ka tootmises ja teistes primaartööstustes (Ball, 2010). Kui ametnikud raporteerivad rohkem internetikasutamise jälgimist, siis lihttöölised raporteerivad enam turvakaamerate abil nende töö tegemise jälgimist (Holland, Cooper & Hecker, 2015). Seda ilmestab ka Eesti töövaidluskomisjonide praktika (lisa 1). Vaidlused, kus üheks oluliseks komponendiks on turvakaamera olemasolu ja/või selle salvestis (nt tööandja süüdistab töötajat varguses või muus töökohustuste rikkumises ja tõendiks on turvakaamera salvestis või töötaja katab kaamera kinni, sest tunneb, et tema privaatsust on rikunud jms juhtumid), on toimunud kõikidel juhtudel primaarsektoris: 34,2% kordadest tootmises, 29,3% kaubanduses, 19,5% toidlustuses ja teeninduses, 14,6% transpordis, 2,44% puhastusteeninduses. Enamikel juhtudel on vaidluse üheks pooleks olnud lihttööline (92,7%) ning ainult kolmel korral (7,3% vaidlustest) on olnud vaidlus juhtivtöötaja ja tööandja vahel. Sarnane jaotumine sektorite vahel on välja joonistunud ka Hispaania kohtulahendite analüüsis. 22,8% vaidlustest toimus toidlustussektoris, 13,6% transpordi-, 13,6% tootmis-, 13,6% kaubandus-, 13,6% teenindus- ja 22,8% muus sektoris (Agustina & Coudert, 2013).

Võttes arvesse asjaolu, et suur hulk vaidluseid jälgimisseadmete kasutamises osas on toimunud toidlustussektoris, siis käesoleva magistr töö uurimus viiakse läbi Tallinnas asuvate

toitlustusettevõtete seas. Erinevates uurimustes on leitud, et jälgimisseadmete paigaldamise ebaselge eesmärk, mitte eesmärgipärane kasutamine ja riive privaatsusele võib põhjustada negatiivseid tagajärgi töökeskkonnas (Ciocchetti, 2011; Ball 2010). Eestis on jälgimisseadmete kasutamist töökohal uuritud pigem õigusteoreetilisest vaatekohast lähtuvalt. On leitud, et Eestis kehtiv õiguslik regulatsioon ja AKI koostatud juhend jälgimisseadmete paigaldamiseks töökohale ei ole piisav ning tarvis oleks eriseadust (Sits, 2014; Peeterson, 2012). Nimetatud tööd on õigusteaduskonna tööd, mistõttu on tegu seaduste analüüsiga. Autor leiab, et käesolev töö lisab seaduste analüüsile praktilisema väljundi, sest uurimus on suunatud tegeliku olukorra välja selgitamisele, sh sellele, kas AKI juhend on leidnud praktilist kasutamist. Varasemalt ei ole sarnast tööd kirjutatud, mistõttu puudub ülevaade, kas praktikas esineb murekohti jälgimisseadmete kasutamisel töösuhetes.

Käesoleva magistr töö eesmärk on välja selgitada, millistel eesmärkidel kasutavad tööandjad töökohal turvakaameraid, kas nende kasutamine on õiguspärane ning kas turvakaamerate kasutamisega rikutakse töötajate õiguseid. Magistr töö eesmärgi saavutamiseks leitakse vastused järgmistele uurimisküsimustele:

1. Millistel eesmärkidel on tööandjad ettevõttesse paigaldanud ja millistes eesmärkidel kasutatakse töökohtadel turvakaameraid?
2. Kas ja millised meetodid on tööandjad kasutusele võtnud, et minimeerida turvakaamerate kasutamisega kaasneva võivaid negatiivseid tagajärgi?
3. Kas ja kuidas on korraldatud töötajate teavitamine turvakaamerate olemasolust ja muust nendega seonduvast?

Magistr töö eesmärgi saavutamiseks ja uurimusküsimustele vastamiseks on autor püstitanud järgmised uurimisülesanded:

1. Anda kirjanduse põhjal ülevaade jälgimisseadmete kasutamisega kaasnevatest tagajärgedest töötajatele ja ettevõtetele.
2. Viia läbi empiiriline uurimus toitlustussektori tööandjate seas, et selgitada välja, kuidas on korraldatud jälgimisseadmete kasutamine ning kas see on seadusega kooskõlas.
3. Selgitada välja, kas tööandjad on pööranud tähelepanu võimaliku negatiivse mõju minimeerimisele.
4. Empiirilise uuringu tulemustest lähtuvalt teha ettepanekud andmekaitse inspeksioonile, kuidas jälgimisseadmete väärkasutamist vähendada.

Magistritöö koosneb neljast osast. Esimeses osas antakse teoreetiline ülevaade jälgimisseadmete kasutamise mõjudest töökohal. Samuti sellest, kuidas erinevad eeskirjad ja töötajate teavitamine ning selgitustöö jälgimisseadmete kasutamisega kaasneda võivaid negatiivseid tagajärgi vähendavad või lausa väldivad. Teises osas antakse ülevaade õiguslikust regulatsioonist. Kolmas osa moodustab autori poolt läbi viidud empiirilise uurimuse meetodite kirjeldusest ja kokkuvõttest. Neljandas osas arutleb autor uurimuse tulemuste üle ning teeb järeldused ja ettepanekud.

1 JÄLGIMISSEADMETE PAIGALDAMINE JA KASUTAMINE

Käesolevas peatükis antakse esmalt teoreetiline ülevaade põhjustest, miks tööandjad kasutavad töökohtadel töötajate jälgimiseks jälgimisseadmeid ning milliseid tagajärgi võib jälgimisseadmete kasutamine töötajatele ja ettevõtetele kaasa tuua. Seejärel kirjeldatakse, kuidas minimeerida või ära hoida jälgimisseadmetega kaasnevat võimalikke negatiivseid tagajärgi. Lisaks antakse ülevaade Eestis kehtivatest õigusaktidest, et luua õiguslik raamistik jälgimisseadmete korrektseks kasutamiseks.

1.1 Jälgimine ja jälgimisseadmed

Tänapäeval on veel väga suurel hulgal ettevõtteid, keda saab defineerida kui kontrollile orienteeritud ettevõtteid. Selliste ettevõtete üks ühine tunnus on see, et töötajate töö tegemist jälgitakse olulisel määral elektrooniliste vahenditega ning privaatsuse säilitamine nendes ettevõtetes on peaaegu võimatu (Chang, Liu & Lin, 2015). Lyon (2007: 14) on jälgimist defineerinud kui fokuseeritud, süstemaatilist ja rutiinset tähelepanu personaalsetele üksikdetailidele eesmärgiga mõjutada, juhtida, kaitsta või suunata. Seetõttu on jälgimine elektrooniliste vahenditega väga intensiivne ning näiteks võrreldes juhtidepoolse isikliku kontrollimisega väga kontrastne (Alder, 2001).

Ciocchetti (2011) on elektroonilised jälgimisseadmed liigitanud nelja kategooriasse. Need on järgmised: parimad praktikad – täidavad oma eesmärgi, kuid ei kahjusta liigselt töötaja privaatsust; riskantsed praktikad – sobivad üksnes ennetamise ja uurimise eesmärkidel, ei kahjusta liigselt töötaja privaatsust; väga riskantsed praktikad – täidavad oma eesmärgi, kuid kahjustavad liigselt töötaja privaatsust; kõlbmatud praktikad – sobivad teatud juhtudel üksnes uurimiseks, muid eesmärke ei täida ning kahjustavad liigselt töötaja privaatsust. Turvakaamerad on Ciocchetti paigutanud kõige viimasesse ehk kõlbmatute praktikate kategooriasse. Kuna turvakaamerate abil on võimalik töötajate töö tegemist väga detailselt jälgida, nende kasutamisega sekkutakse liigselt töötaja privaatsfääri ning ei täida üldjuhul seatud eesmärke on Ciocchetti nende kasutamist töökohal pidanud liiga invasiivseks. Seetõttu on nii töötajate kui tööandjate jaoks on jälgimisseadmete kasutamisel olulisemaks küsimuseks see, milline on ühisosa töötaja ootustel privaatsusele ja tööandja õigusel töötajat kontrollida (Sewell, Barker & Nyberg, 2012: 205).

Elektrooniliste jälgimisseadmete mõiste on laiem kui üksnes turvakaamerad. Töö teoreetilises osas kasutatud uurimustes on jälgimisseadmete käsitlemisel turvakaamerad olnud alati vaadeltavate hulgas. Seetõttu on edaspidises töös jälgimisseadmeid ja turvakaameraid kasutatud sünnunümidena.

1.2 Jälgimisseadmete töökohal paigaldamise ja kasutamise põhjused

Tänapäeva privaatsuse aruteludes on olulisel kohal see, mil määral peab töökohal olema tagatud privaatsus ja kuidas eristada töö- ja eraelu. Muutused elustiilis ja tehnika areng on jõudnud punktini, kus era- ja tööelu vahel selge piirjoone tõmbamine on hägustunud. On tavaline, et inimestel on samaaegselt mitu erinevat töökohta ja töökohtadel veedetakse pikki tunde. Selle tulemusena kasutavad töötajad tihti tööandja vahendeid ka isiklikuks otstarbeks, nt isiklike arvete tasumiseks, isiklike meilide saatmiseks jms. Ettevõtte huvidest lähtuvalt peaksid tööandjad nimetatud muutustele reageerima nii tehnoloogilisest, sotsiaalsest kui juriidilisest aspektist vaadatuna. Samas ei tohiks nad ülereageerida ega -reguleerida. Tööandjad peavad leidma tasakaalu ettevõtte varade kaitsmise ja töötajate privaatsuse vajaduste vahel (Miller & Wells, 2007: 316).

Daniel Slavíček (2012), kes on 17 aastat töötanud kahes teineteist vastandavas sektoris: juhina erafirmas, mis loob järelevalve tehnoloogiaid ning samal ajal tegutsenud akadeemikuna uurides järelevalve tehnoloogiate mõju, on leinud, et vastutus töötajate eest hoolitsemise ja nende järel kontrollimine on ühe mündi kaks erinevat poolt. Tööandjad soovivad saavutada maksimaalset kasumit ja kaitsta oma varasid, kuid samal ajal peavad nad vastutama töötajate tervise, heaolu ja ka turvatunde eest. Töötajate eest vastutamise ja kontrollimise vahel jookseb õhkõrn piir, kus on keeruline tuvastada, millal hoolimine ja vastutamine muutub kontrollimiseks ja millal kontrollimine muutub privaatsuse rikkumiseks.

Bentham (1995) on pidanud teiste jälgimist väga tõhusaks kui jälgitavad ei tea, millal neid täpselt vaadatakse. Ta leidis, et see paneb nad käituma kogu aeg nii nagu nad käituksid siis, kui neid vaadatakse. Bentham kujundas 18. sajandil ringikulise hoone idee, kus jälgitavad on ringikujuliselt hoone väliskülgedel ning töödejuhataja keskel. Seeläbi on töödejuhatajal hea ülevaade kõigist ning kuna töödejuhataja oleks hoone keskel tornis, siis töötajad ei tea kuna neid vaadatakse. Ta leidis, et ideed tuleks eelkõige rakendada vanglates kinnipeetavate kontrollimiseks, aga ka koolides, haiglates ja mujal. Ironilisel kombel sai idee alguse töökohalt, nimelt Venemaal asuvast tehasest, kus seda ka rakendati.

Ka tänapäeval on kontrollimine põhiline põhjus, mis jälgimisseadmeid rakendatakse. On üsna loomulik, et tööandjad on huvitatud töötajate töö tulemuslikkuse monitoorimisest, sest see aitab hinnata, kas töö eest makstav tasu on korrelatsioonis tehtava töö tulemuste ja kvaliteediga. Töötajate

kontrollimise põhjenduseks tuuakse enamasti vajadus kaitsta ettevõtte varasid ning seeläbi limiteerida võimalikke kulusid ja riske (Ball, 2010).

Ball (2010) toob välja kolm põhjust, miks tööandjad soovivad töötajate töö tegemist jälgida ja kontrollida. Need põhjused on järgmised:

1. Tööandjad soovivad jälgida ressursside kasutamist, et säilitada tootlikkust;
2. Tööandjad soovivad kaitsta ettevõtet ärisaladuste lekkimise ja edastamise eest andmete varguse, laimu ja sabotaaži näol. Selle ennetamiseks võetakse kasutusele e-kirjade ja interneti monitoorimine, kehtestatakse juurdepääsu piirangud;
3. Tööandjad soovivad kindlustada end töenditega võimalikeks õiguslikeks vaidlusteks.

Kõik Balli toodud põhjendused on seotud tööandja usaldusega või pigem usaldamatusega töötajate suhtes. Kuigi Ball toob välja monitoormispraktikate kasutamise põhjused üldiselt, kuuluvad sinna loetellu ka jälgimisseadmed. Jälgimisseadmete kasutamist põhjendatakse samuti ettevõtte huvide kaitsmisega. Agustina & Coudert (2013: 154) on selgitanud, et töötajate ja tööandjate vahelised suhted on võimusuhted, mistõttu ei saa nende vahel samal tasandil usaldust eksisteerida, nagu näiteks sõpruses. Töösuhted on liiga episoodilised selleks, et loota sajaprotsendilisele usaldusele. Jälgimisseadmete kasutamise põhjus on kartus saada petetud ehk põhjus peitub usaldamatuses. See on fundamentaalne vasturääkivus: jälgimise põhjuseks on hirm saada petetud ehk usaldamatus. Teisest küljest annab jälgimine signaali teisele osapoolle, et teda ei usaldata. Kuna usaldamatus tekitab hirmu saada petetud, siis tööandjate soov kasutada jälgimisseadmeid tuleneb soovist ennetada ja avastada rikkumisi. Allen, Coopman, Hart & Walker (2007) on leidnud, et 71% infotehnoloogia valdkonna töötajatest ja juhtidest peab järelevalve tehnikate kasutamise suurimaks põhjuseks töötajate ebaaususe tuvastamist. Kuigi tööandjad on öelnud, et nad kasutavad jälgimisseadmeid ohutuse ja turvalisuse eesmärkidel, siis on nad tunnistanud, et vajadusel kasutatakse neid ka töötajate poolt toime pandud varguste tuvastamiseks ja tõendite kogumiseks vaidluste tarbeks. Lisaks on tööandjad tunnistanud, et nad kasutanud ka varjatud turvakaameraid olukordades, kus neil on olnud kahtlus varguses osas, kuid konkreetsed tõendid on puudunud (Levin et al., 2006).

Turvakaamerad võib paigutada formaalsete järelevalve tehnikate hulka. Siia kuuluvad veel erinevad elektroonilised ligipääsu kontrollimeetodid, turvamehed jms. On olemas ka mitteformaalse järelevalve tehnikad, mille hulka kuuluvad näiteks töökultuuri ja töökeskkonna muutmine. Kõige lihtsam viis ebaaususe tuvastamiseks on formaalsete järelevalve tehnikate kasutamine (Kajalo & Lindblom, 2015). Kajalo & Lindblom (2015) viisid Soome toidukaupade jaeettevõtjate seas läbi

uuringu, mille valim hõlmas jaekaupmehi väikepoodnike omanikest kuni hüpermarketite juhtideni, kes omasid frantsiisi või olid seotud suure korporatsiooniga muul õiguslikul alusel, nt juhtisid tütarfirmat. Üks ühine tunnus kõigil küsitletutest oli see, et hoolimata seotusest suurema ettevõttega, olid nad vabad tegemaks otsuseid, mis puudutasid investeeringute tegemist turvalisuse ja järelevalve küsimustes. Uuringust selgus, et mida tugevamalt seostasid ettevõtjad turvalisusega seotud probleeme, sealhulgas inventari ja kassapuudujääkidega seotud probleeme, seda tugevam mõju oli sellel investeeringutesse formaalsesse järelevalvesse. Samas ei leitud statistilist seost investeeringutega mitteformaalsesse järelevalvesse. See tähendab seda, et tööandjatel on suurem usaldus formaalse järelevalve meetodite efektiivsusesse kui mitteformaalsete. Lisaks peegeldab see ka arvamust, et lihtsam viis turvalisusega, aga ka usaldusega seotud probleemidega tegelemiseks on formaalse järelevalve rakendamine, näiteks uue tehnoloogia paigaldamine ja tutvustamine. Tegevused, mis on seotud mitteformaalse järelevalve rakendamisega, näiteks töökultuuri ja töökeskkonna muutmine, ei ole kergesti kättesaadavad ja selle mõju võtab kauem aega ning vajab suuremat inimkapitali.

Sama on arvanud ka töötajad ise. Alstete (2006) viis läbi uuringu üliõpilaste seas, kellest enamik töötas täis- või osalis tööajaga väikestes ettevõtetes ja olid olnud tunnistajateks sellele, et töötajad on toime pannud varguseid. Neile esitati küsimus, kuidas peaksid väikeettevõtete juhid tuvastama ja ära hoidma töötajate varguseid. 42 % küsitletutest vastas, et tuleks kasutusele võtta või suurendada video järelevalvet, 24 % vastas, et tõhustada tuleks kontrollimise süsteeme (paremad süsteemid inventuuri tegemiseks, vara ja kauba arvestuse ülevaatlikum ja organiseeritum dokumentatsioon), 9 % leidis, et suurendada tuleks omaniku järelevalvet, s.t, et omanik viibiks füüsiliseks rohkem koha peal, 8 % leidis, et tõhustada tuleks töötajate värbamise protsessi, 8 % pakkus, et tuleks leida töötajate seast nn “nuhk”, kes abistab tööandjat varguste toimepanijate leidmisel, 4 % ütles, et tõsta tuleks töötasu ja 5 %, et töötajatele tuleks anda tasuta tooteid.

See ilmestab seda, et jälgimisseadmete kasutuselevõtt on nii öelda lihtsaim tee, mille rakendamine kerkib esimesena mõtteisse kui ettevõttes tekivad probleemid. Selle paigaldamine ja kasutamine ei nõua ka suurt pingutust, erialaseid teadmiseid ega pikka perioodi, et tulemusteni jõuda. Samuti pole tarvis hakata tegelema töötajate motiveerimisega, mis on võib tunduda keeruline ja aeganõudev. Lisaks fakt, et primaarsektoris on suur personalivoolavus, mida nähakse pigem paratamatusena kui probleemina, mida on võimalik leevendada. Slavíček (2012) on selgitanud, et jälgimisseadmete rakendamise õigustamiseks kasutatakse tihti põhjendust, et kunagi ei tea, mis võib juhtuda ehk neid

kasutatakse nii öelda igaks juhuks ning alati on lihtsam investeerida jälgimisseadmetesse, kui omada isiklikku vastutust.

Nii Ball (2010), Slavíček (2012) kui Kajalo & Lindblom (2015) leitud põhjused järelevalve rakendamiseks on seotud usaldamatusega ja sooviga ennetada võimalikke rikkumisi. Samal ajal tähendab see töötajate kahtlustamist ja tööandjate soovi omada kõigest ülevaadet. Seetõttu võib Jensen & Raveri (2012) arvates järelevalve tehnikate kasutamine osutada mikrotasandi juhtimise ja kontrollimise meetodiks, mille eesmärgiks saab töötajate käitumise piiramine.

1.3 Jälgimisseadmete legalne ja eesmärgipärane paigaldamine

Tööandjad on jälgimisseadmete kasutamiseks legaalseks hinnanud järgmised olukorrad:

- 1) töötajate ja klientide ohutus ning turvalisus;
- 2) töötajate poolt toime pandud varguste ennetamine ja avastamine;
- 3) tõendite kogumine töötajate poolt vägivaldsete tegude toimepanekul;
- 4) kaastöötajate ja tööandjate kiusamine ja solvamine (*offensive*) töötaja poolt;
- 5) tööandja vara kaitsmine;
- 6) tootlikkuse hindamine ja järelevalve

(Levin et al., 2006).

Samas mõistlikuks on tööandjad pidanud jälgimisseadmete paigaldamist pigem ohutuse ja turvalisuse kaalutlustel, sest nede soetamis-, paigaldamis- ja ülevalpidamiskulud on liiga kõrged, et neid kasutada produktiivsuse kontrollimise eesmärgil. Seda seetõttu, et jälgimisseadmetega saadud info on väga mahukas ja kogu info töötlemine ning vaatlemine on liiga ajakulukas ning lõppkokkuvõttes ei ole see majanduslikus mõttes piisavalt tasuv, sest kui töötajaid terve tööaja vältel jälgida, siis on see kallis, isegi siis kui avastada mõni viga töötajate produktiivsuses (Levin et al., 2006).

Tööandjate hinnangud ei kattu täielikult erinevate uuringute tulemustega. Ciocchetti (2011) toob välja, et jälgimisseadmete kasutamist võib pidada legaalseks ja õigustatuks ainult teatud juhtudel tööandja vara kaitsmise eesmärgil. Näiteks võib jälgimisseadmete kasutamine olla heaks vahendiks parkimisplatsil ja ettevõtte sisse- ning väljapääsude läheduses. Samuti ettevõtetes, kus on kõrgendatud turvalisuse ja ohutuse küsimus, nagu näiteks kasiinodes ja pankades (Jensen & Raver, 2012). Välistatud peaks olema kaamerate paigaldamine asukohtadesse, kus on kõrgendatud ootus privaatsusele, nt töötajate puhkeruumid ja tualetid (Agustina & Coudert, 2013: 148).

Ciocchetti (2011), kes on turvakaamerad paigutanud kõlbatute praktikate hulka (tabel 1), mille kasutamist töökohal ei pea ta üldjuhul õigustatuks. Sellega nõustuvad ka töötajad, kellest 56 % on täielikult vastu kaamerate kasutamisele töökohal kui töötajad jäävad kaamerate vaatevälja (Holland, Cooper & Hecker, 2012, Chang et al., 2015 kaudu). Ciocchetti (2011) on välja töötanud kontseptsiooni, mida ta kutsub privaatsuse hindamise reegliks (*Privacy Judgement Rule (PJR)*). Enne turvakaamerate kasutusele võttu peab tööandja saama “jah” vastuse privaatsuse hindamise reegli kolmele küsimusele, mis on järgmised:

- 1) Kas jälgimisseadmete kasutusele võtmine on seotud konkreetse eesmärgiga?
- 2) Kas jälgimisseadmete kasutusele võtmine on kõige vähen invasiivne meetod eesmärgi saavutamiseks?
- 3) Kas jälgimisseadmete kasutamine hõlmab minimaalsel hulgal ja määral töötajaid?

KATEGOORIA 1	KATEGOORIA 2	KATEGOORIA 3	KATEGOORIA 4
Parimad praktikad	Riskantsed praktikad	Väga riskantsed praktikad (<i>bordeline practice</i>)	Kõlbatud praktikad (<i>poor practice</i>)
<ul style="list-style-type: none"> • madal invasiivsus • kõrge kaitse/turvalisus • sobiv kõigis kategooriates 	<ul style="list-style-type: none"> • madal invasiivsus • madal kaitse/turvalisus • kohane ennatamiseks ja uurimiseks • peab läbima PJR äri eesmärkides 	<ul style="list-style-type: none"> • kõrge invasiivsus • kõrge kaitse/turvalisus • peab läbima PJR kõigis monitoorimise eesmärkides 	<ul style="list-style-type: none"> • kõrge invasiivsus • madal kaitse/turvalisus • sobiv ainult uurimiseks kui läbib PJRi
<ul style="list-style-type: none"> • elektroonilised sissepääsu paneelid • kohaloleku (tuleku ja mineku kellaegade) kontrollimine • automaatne hoiatus arvutiekraanil 	<ul style="list-style-type: none"> • filtrid ja tulemüürid internetikasutuses • Interneti kasutusajaloo jälgimine • sotsiaalmeedia jälgimine/kontroll 	<ul style="list-style-type: none"> • e-kirjade ja sõnumine kontroll • GPS (üleilme asukoha määramine) süsteemid • raadio sageduste jälgimine ja kuulamine • füüsilised läbiotsimised 	<ul style="list-style-type: none"> • arvuti kasutusajaloo jälgimine • klahvivajutuste ajaloo jälgimine • telefonikõnede reaajas või järelkuulamine • video järelevalve

Tabel 1 Enimkasutatavate monitoorimistehnikate jaotumine nende riskitaseme järgi töötajate privaatsusele (Ciocchetti, 2011: 356)

Seega enne jälgimisseadmete kasutusele võtmist peaks tööandja analüüsima, kas see on ainuvõimalik variant, et jõuda seatud eesmärkideni. Näiteks kui soovitakse vähendada töötajate poolt toime pandud varguste arvu, siis võib selleks olla ka muu vahend kui turvakaamerate paigaldamine. Heaks näiteks on siinkohal Queensi nätsuvabrik, kus oli suur probleem töötajate toime pandud vargustega. Näts on väike, mistõttu oli seda kerge varastada. Tööandja otsustas vabriku väljapääsude juurde panna kausid tasuta toodetega, mida töötajad said võtta nii palju kui soovisid. Varguste arv vähenes olematuseni, kuid ka tasuta tooteid praktiliselt ei võetud (Alstete, 2006). Seega antud näites leiti eesmärgi saavutamiseks tõhusam meetod kui turvakaamerate paigaldamine varguste ennetamiseks, vähendamiseks ja uurimiseks.

1.4 Jälgimisseadmete töökohal kasutamise mõjud ja tagajärjed

Jälgimisseadmete kasutamise töösuhetes toob teravalt esile privaatsuse ja usalduse küsimuse ning seob need omavahel (Chen & Park, 2005: 86). Üldiselt nõustuvad ka tööandjad, et töökohal peab olema teatud määral tagatud privaatsus, nn “personaalne ruum” või “eraelu”, et tagada probleemivaba ja funktsioneeriv ettevõtte (Levin et al., 2006). Privaatsuse säilitamise võimalus töökohal on üheks eelduseks usalduslike suhete tekkimisele töötaja ja tööandja vahel (Chang et al., 2015), sest austatakse üksteise privaatsfääri, mis on hea alus heade töösuhete, parema produktiivsuse ja tervislikuma atmosfääri loomiseks (Dowding, 2011: 60). Usalduse olemasolu ettevõttes suurendab tööga rahulolu ning valmidust ettevõtte heaks pühenduda (Agarwal, 2014).

Usalduse olemasolu saab suurendada muuhulgas sellega, et liigutakse eemale käsu-ja-kontrolli filosoofiast töötajate enesejuhtimise (*self-management*) lähenemise poole. Käsu-ja-kontrolli filosoofia seostub kõrge tööandja poolse kontrollimise ja järelevalvega. Enesejuhtimise lähenemises antakse töötajatele kontroll oma töökeskkonna üle ja samal ajal vastutus iseenda käitumise osas. Töötaja on kaasatud otsuste tegemisse ja töötaja otsuseid usaldatakse. See on üks osa ettevõtte juhtimistavadest ja -praktikatest. On leitud, et korrelatsioon enesejuhtimise ja tajutud usalduse vahel on positiivne kui töötajate järelevalve on madal (Jensen & Raver, 2012).

Seetõttu on privaatsusel ettevõtetes oluline koht. Muuhulgas on leitud, et mida madalam on töökohal privaatsuse tase (sh teiste töötajate sekkumine töösesse, jälgimisseadmetega töö tegemise jälgimine), seda enam kogevad töötajad emotsionaalset kurnatust ehk läbipõlemist (Laurence et al., 2013). Ainuüksi taju, et võidakse jälgida, isegi kui tegelikkuses seda ei esine, mõjutab töötaja õiglustunnet ja on tõsine oht jälgitavale (D’Urso, 2006). Töötajad on selgitanud, et pidev kontrollimine ja

tööandjapoolne jälgimine tekitab neis tunde nagu neid justkui ei usaldataks. Töötajad, kes peavad ennast ausateks töötajateks, kuid kes tunnevad, et ettevõtte ei usalda neid, neid kontrollitakse, siis põhjustab see võõrandumist töötaja ja tööandja vahel (Stanton & Weiss, 2003). Töötajad tunnevad ennast jälgitava rollis olles, et nad oleksid justkui süüalused, keda on tarvis igal ajahetkel kontrollida. Töötajad tunnetavad rahuololematust ning nad leiavad, et kaamerate kasutamine töökohal on üleliigne ja ebavajalik (Ball, Daniel & Stride, 2012). Mida enam takistusi usaldusele ehk mida enam ja mida intensiivsemalt elektroonilise järelevalve tehnikaid kasutatakse, seda vähem on töötajad valmis looma koostööd juhtidega. Põhjus seisneb selles, et tööandjad õõnestavad usaldust iseenda vastu kui nad ei usalda töötajaid. Usaldus on kahepoolne tunne. Töötajad usuvad, et tööandjate oskus võtta vastu asjatundlikke otsuseid ettevõtte arengu heaks, langeb märgatavalt mida enam ja intensiivsemalt elektroonilise järelevalve tehnikaid kasutatakse ning seda peetakse liigseks kontrollimiseks (Holland et al., 2015). Tugev kontroll töötajate üle välistab töötajate enesejuhtimise (*self-management*), sest temalt justkui võetakse vastutus ja kontroll iseenda tegude eest (Jensen & Raver, 2012).

Järelevalve süsteemide kasutamine alahindab töötajate motivatsiooni pühenduda ettevõttele. Süsteemid, mis peaksid suurendama ausameelse õhkkonna tekkimist, teevad hoopis vastupidist. Mida intensiivsemalt tajuvad töötajad töökohal jälgimisseadmete kasutamise määra, seda negatiivsemalt neisse suhtutakse (Martin, Wellen & Grimmer, 2016). Eraldi tasub märkimist, et lihttöölise seas on täheldatud tugevamat negatiivset korrelatsiooni usalduse ja elektroonilise järelevalve tehnikate kasutamise vahel. Lihttöölise usaldus ettevõtte juhatusse oli palju madalam võrreldes ametnikega sama arvu elektroonilise järelevalve tehnikate kasutamisel. Oluline fakt on ka see, et kui ametnikud raporteerisid rohkem internetikasutamise jälgimist, siis lihttöölised raporteerisid enam turvakaamerate abil nende töö tegemise jälgimist (Holland et al., 2015). Ausad töötajad tunnevad ennast jälgimise olukorras petetuna ning nende panus ja pühendumus ettevõtte hüvanguks väheneb (Kramer, 1999). Seetõttu võib jälgimisseadmete kasutamine iroonilisel kombel mõjutada inimesi tegema tegusid, mida jälgimissüsteem peaks ära hoidma. Eelkõige kannatavad töötajate ja tööandjate vahelised suhted (Holland et al., 2015), töötajates tekib trots ning motivatsioon pühenduda ettevõttele väheneb (Kramer, 1999). Tagajärjeks on vähem efektiivne tööpanus (*counterproductive work behaviour*), mille ilmingud töökohal on muuhulgas (pisi)varguste toimepanek, passiivne tegevus, nagu näiteks sihilik töö valesi tegemine ja juhiste mittetäitmine (Fox, Spector & Miles, 2001; Martinet et al., 2016). Lõpptulemuseks võib olla halvasti toimiv ja majanduslikult ebaefektiivne ettevõtte (Holland et al., 2015).

Seda, et tööandjad ei oska arvestada jälgimisseadmete kasutamise kaasneda võivaid probleeme, ilmestab see, et enamik tööandjatest usub, et töötajatel ei ole midagi selle vastu kui tööandja kasutab töökohal jälgimisseadmeid (Stanton & Weiss, 2003). Kõigest 1% juhtidest on leidnud, et elektrooniline jälgimine võib olla halb. Töötajatest leidis 13% vastanutest, et elektrooniline jälgimine on üdini halb (Allen et al., 2007).

Seega lõhe tegeliku olukorra ja tööandjate teadmiste vahel on üsna suur. Ciocchetti (2011), kes leiab, et turvakaamerad kuuluvad ebamõistlike järelevalve tehnikate hulka ning nende pidev kasutamine ei õigusta ennast, sest kättesaadavad on palju efektiivsemad ja vähem invasiivsed vahendid kaitsmaks samu tööandja huve, mida täidavad kaamerad, on leidnud ja toob kokkuvõtvalt välja ülemäärase ja ebamõistliku jälgimisseadmete kasutaminega kaasneda võivad tagajärjed. Need on järgmised:

- 1) see läheb vastuollu töötajate mõistliku ootusega privaatsusesse;
- 2) töötajad tunnevad, et on sunnitud vargsi, isegi salaja ringi käima ja mööda hiilima jälgimisseadmetest, et tegutseda tööajast isiklike asjadega;
- 3) töömoraal langeb;
- 4) töötajate rahulolematuse ja kurtumise suureneb ning võib kaasa tuua isegi töötajate lahkumise ettevõttest;
- 5) töötajatel tekib ebamõistlik hirm kasutamaks ükskõik milliseid elektroonilisi vahendeid, mida on võimalik teistel isikutel jälgida, isegi siis kui nende vahendite kasutamise soov on headel eesmärkidel.

1.5 Jälgimisseadmete paigaldamise ja kasutamise kaasneda võivate negatiivsete tagajärgede vähendamine või ära hoidmine

Kui tööandja on leidnud, et jälgimisseadmete paigaldamine soovitud eesmärgi saavutamiseks on ainuvõimalik variant, siis tuleb analüüsida, kuidas vältida võimalikke negatiivseid tagajärgi, mida jälgimisseadmete kasutusele võtmine endaga kaasa võib tuua. Järgnevalt on kirjeldatud erinevaid meetodeid ja tegevusjuhiseid, mida tööandjad peaksid arvesse võtma ja järgima.

Jälgimisseadmed peavad olema paigaldatud ja neid peab kasutama seaduslikel alustel, sest töötajate kognitiivne usaldus ettevõtte ja selle juhtide suhtes on tugevalt seotud ettevõtte juriidilise korrektsusega (Hon & Lu, 2010). Kui töötajad usuvad, et tööandjad on erinevad protseduuri reeglid ning eeskirjad koostanud seaduslikel alustel ning peavad nende täitmisest lugu, siis on töötajad suurema tõenäosusega valmis täitma ettevõtte nõudeid, sest nad tunnevad ennast kindlalt ning neil on

tööandja kui partneri vastu usaldus (Chang et al, 2015) ning protseduuriline korrektsus ühe lepingupartneri poolt stimuleerib õiglustunnet ja vabatahtlikku nõustumist teise lepingupartneri poolt (van Dijke & Verboon, 2010). Lisaks on tööandjate jaoks olulise tähtsusega see, et kui jälgimisseadmed on paigaldatud ja neid kasutatakse seaduslikel alustel, siis on võimalik kogutud salvestusmaterjali ehk tõendeid kasutada juriidilistes vaidlustes (Allen et al., 2007: 338).

Jälgimisseadmete paigaldamisel on olulise tähtsusega nende eesmärgid. Peab olema selge, milliseid ettevõtte jaoks oluliste probleemide lahendamist soovitakse nende rakendamisega saavutada. Jälgimisseadmete vajalikkus, eesmärgid ja meetodid peavad olema korrektselt ja selgelt sõnastatud, sest see aitab vältida töötajate vaenulikku reaktsiooni, saavutada töötajate tolerantsust ja positiivsemat suhtumist jälgimisseadmete osas (Mitrou & Karyda, 2006; Allen et al., 2007; Workman, 2009b). Ebaselgete ja vastuoluliste tehnoloogiate kasustusele võtmine, kus on ebaselge, kuidas on see seotud tööülesannetega, on vastuvõetamatu, kui sellel puudub mõistlik põhjendus (Stanton & Weiss, 2003).

Üldiselt on töötajad jälgimisseadmete suhtes toetavad kui seda tehakse isikute ja vara kaitsmise ning turvalisuse eesmärgil (Ball, 2010; Stanton & Weiss, 2000). Eesmärgipäraseks ei pea töötajad seda, kui tööandjate jaoks on liiga oluline töötaja tööaja detailne ajakasutamine ja järelevalvega seatakse ohtu töötaja autonoomsus (Ball, 2010).

Töötajad peab jälgimisseadmete kasutamisest teavitama. Aktsepteerimatu on töötajate seisukohalt salajane jälgimine (Allen et al., 2007). Ei saa eeldada, et töötajad oleksid alati kõigi seaduste ning tööandja poolt koostatud dokumentidega iseseisvalt kursis. Kui töötajad ei mõista ettevõtte eeskirjade ja praktikate vajalikkust, siis võib see lõpptulemusena viia vähem efektiivse tööpanuseni (*counterproductive work behaviour*) (Workman, 2009b). Seetõttu tuleb töötajatele selgitada jälgimisseadmetiku kasutamise eesmärgid ja protseduurireegleid, sest siis on nad suurema tõenäosusega nõus selle rakendamisega ettevõttes ning nende hoiakud on jälgimisseadmete suhtes toetavamad (Hsu & Kuo, 2003). Lisaks on leitud, et teavitamisel on väga suur roll sellel, kuidas töötajad hiljem ise jälgimisseadmete eesmärkidesse ja vajalikkuse suhtuvad. Allen et al. (2007) leidsid korrelatsiooni selle vahel, kuidas tööandjad töötajatele jälgimisseadmete kasutamise eesmärki tööle tulles selgitasid ja kuidas töötajad jälgimisseadmete olemasolu ettevõttes õigustasid. Kui tööandjad olid töötajatele tööle tulles selgitanud, et jälgimisseadmeid kasutatakse selleks, et tuvastada ebaausaid töötajaid, siis mainisid töötajad intervjuude käigus sama kui neilt küsiti, kuidas nad tunnevad ennast järelevalve suhtes. Kui tööandjad polnud seda töötajale öelnud, siis töötajad ise

sellist põhjendust ei toonud. Sama kehtis ka kõigi teiste põhjenduste, nt ohutuse ja turvalisuse otstarbel jms, kohta.

Asjakohase näite saab tuua ka Mason, Button, Lankshear, Coates & Sharrocki (2002) läbiviidud uuringust. Nimelt paigaldati turvakaamerad 24 tundi töötavasse elekrijaama. Töötajad reageerisid kaamerate paigaldamisele väga vaenulikult. Tööandja ei teavitanud töötajaid enne kaamerate paigaldamist ega ka vahetult peale seda. Teavitamine toimus oluliselt hiljem kui selgusid töötajate negatiivsed reageerinud. Tööandja teavitas ja selgitas seepeale töötajatele, et kaamerad on paigaldatud nende enda huvides. Nimelt pidi hooldustöötajatel olema ööpäevaringne juurdepääs varuosadele ja tööriistadele. Korrusel, kus vajalikud esemed asusid, ei olnud öösiti teisi töötajaid. Iga kord kui hooldustöötajad võtsid varuosi või tööriistu, pidid nad selle kirja panema. Praktikas töötajad selle aga unustasid ning selline süsteem ei toimunud. Invetuurides olid puudujäägid. Tööandja selgitas, et ta ei kahtlusta töötajate vargust ning kaamerad töötavad üksnes öösiti. Kaamerad fikseerivad selle kui töötajatel on tarvis midagi nimetatud korrusel võtta ning nad ei pea midagi kirja panema. Teavitus- ja selgitustööga kadusid ka töötajate hirmud ja mured.

Tööandjad peavad kinni pidama jälgimisseadmete kasutamise eesmärkidest, mida nad töötajatele tutvustanud on. Negatiivseid tagajärgi (rahuololematus, vastutöötamine jms) toob kaasa see kui jälgimisseadmetega kogutud andmeid kasutatakse muudel eesmärkidel kui algselt planeeritud. Kui töötajatele on tutvustatud ühte eesmärki, kuid tegelikkuses kasutatakse saadud infot muul eemärgil, siis tunnetavad töötajad, et jälgimine on liiga intensiivne ja rikub nende privaatsust (Ball, 2010).

Tööandjad peavad pöörama tähelepanu saadud andmete kaitsmisele ja turvalisusele. Kuna jälgimisseadmete kasutamisega kogutakse ühtlasi töötaja isikuandmeid, siis kõik tegevused töötaja isikuandmetega võivad ohtu seada töötaja privaatsusele. Töötajad avaldavad vastumeelsust siis kui ei ole teada, mida saadud andmetega tehakse, nende arvamus selle kohta, kas jälgimine on positiivne või negatiivne, on mõjutatud sellest, mida saadud andmete tehakse (Ball, 2010; Stanton & Weiss, 2000). Töötajate jaoks on oluline omada kontrolli iseenda andmete üle. Tööle tulles loovutavad töötajad teatud andmete osas kontrolli tööandjale, mistõttu on töötajate jaoks äärmiselt tähtis see, mida kogutud infoga tehakse. Teadmatus ja kontrolli kaotamine tekitab ebaõiglustunnet (Eddy, Stone & Stone-Romero, 1999). Seetõttu peavad tööandjad tegema kõik selleks, et kaitsta tööandjale teatavaks saanud informatsiooni töötajate kohta. Töötajad peavad teadma, et nende privaatsus on kaitstud. Kui töötajad tajuvad, et ettevaatusabinõud privaatsuse kaitsmiseks on efektiivsed, siis aktsepteerivad nad suurema tõenäosusega järelevalve eeskirju. Töötajatel peab olema kindlus, et

järelevalve protsessi käigus kogutud andmete kasutamine ja säilitamine toimub läbipaistvalt ning seadustega kooskõlas. Lisaks tuleb töötajatele selgitada, milliseid meetmeid kasutatakse, et kaitsta kogutud andmeid võimalike väärkasutuste eest (Thomas & Stoddard, 2004).

Tööandjad peavad koos töötajatega vaatama regulaarselt läbi järelevalve praktikaid, sealhulgas jälgimisseadmestiku kustamise põhjuseid, protseduurireegleid ja neist kinni pidamist. Arutlemine töötajatega aitab tööandjatel saada ülevaate selles osas, milline on töötajate meelestatus, kas kõiki koheldakse õiglaselt ning võrdselt. Töötajatel peab olema kindlus, et juhid ja isikud, kellel on ettevõttes suurem võimupositsioon, lähtuvad suuremast üldsuse huvist ning toetuvad üksnes objektiivsetele andmetele. On oluline, et võimupositsioonil olevad isikud ettevõttes ei kuritarvitaks on positsiooni, oleksid võimalikult erapooletud ning arvestaksid töötajate ettepanekutega. (Baldwin, Bommer & Rubin 2008, Workman, 2009a kaudu).

Tööandjad peavad tagama, et töötajatel oleks võimalus esitada kaebusi jälgimisseadmestiku väärkasutamise kohta. Töötajate jaoks on oluline, et nad saaksid kaasa rääkida otsustes, mis neid otseselt või kaudselt mõjutavad. Usalduslik õhkkond ning tunne õiglusest on saavutatud siis, kui töötajatele on tutvustatud kaebuste esitamise protsessi ning nad on kindlad selle toimimises reaalses probleemi situatsioonis. Töötajad peavad teadma milliseid meetmeid kaebuste saabumisel nende lahendamiseks rakendatakse. (Umpress, Labianca, Brass, Kass & Scholten, 2003). Töötajate õiglustunnet suurendab seegi kui nad kaasatakse järelevalve süsteemide, sealhulgas jälgimisseadmestiku protseduurireeglite ja eeskirjade väljatöötamisse (Alder, 2001).

Kokkuvõtvalt võib öelda, et kõige olulisem turvakaamerate paigaldamisel on see, et seda tehtaks seaduslikel alustel. Enne paigaldamist tuleb läbi mõelda, milliste probleemide lahendamist soovitakse nende kasutamisega lahendada. Seatud eesmärkidest tuleb kinni pidada, turvakaameraid ei või kasutada muudel eesmärkidel kui algselt plaanitud. Vältimaks töötajate pahameelt, tuleb neid turvakaamerate paigaldamisest teavitada, tuleb selgitada, milliseid eesmärke nendega soovitakse saavutada, kes ja kuidas neid kasutab, mida saadud salvestistega tehakse ning kuidas on tagatud kogutud andmete turvalisus.

2 PRIVAATSUSÕIGUSE RAAMISTIK

Privaatsusõiguse piiramise ja isikuandmete kaitse kohta eriseadus Eesti õiguses, mis käsitleks üksnes andmekaitset töösuhetes, puudub (Männiko, 2011: 152). Töötaja kui nõrgem pool töösuhetes vajab teatud kaitset tema kohta käiva info kuritarvitamise eest. Jälgimisseadmete kasutamisega on võimalik tungida isiku eraellu, mistõttu võib ta kaotada kontrolli iseeenda kohta käivate andmete üle. Võrreldes teiste isikuandmete kogumise viisidega kujutab jälgimisseadmete kasutamine endast kõige intensiivsemat privaatsuse ja eraelu riivet üldse (AKI, 2013b: 69). Õiguskirjanduses on eraelu defineeritud kui igapäevase õigust enesemääratlemisele ning õigust elada oma soovide ja tahtmiste kohaselt minimaalse välise sekkumiseta (Maruste, 2004: 429). Jälgimisseadmete kasutamine toob kaasa isikuandmete töötlemise kui isik on tuvastatav ehk pea igal juhul võib jälgimisseadmete kasutamine tuua kaasa sekkumise isiku eraellu. Isik on identifitseeritav ka siis, kui jälgimisseadmete abil pildilt ei nähtu tema nägu; isikut on võimalik identifitseerida tema muude tunnuste kaudu - nt kehakuju, riietus, kaasas oleva asjad jne (AKI, 2013b: 69). Jälgimisseadmete definitsioon on Eesti õiguses lahti mõtestatud turvaseaduses, mille kohaselt on see pilti või elektroonilist signaali edastavate ja salvestavate seadmete kogum, mis on ette nähtud territooriumi, inimese, eseme või protsessi jälgimiseks või territooriumi, inimese või eseme asukoha või protsessi toimumise koha kindlaksmääramiseks (Turvaseadus, 2015: § 11 lg 3). Autor käsitleb antud töös jälgimisseadmetena turvakaameraid, nii salvestavaid kui mittesalvestavaid. Kuna jälgimisseadmetega kogutakse ja töödeltakse töötaja isikuandmeid, sh võidakse rikkuda töötaja õigust privaatsusele, siis tuleb välja selgitada, milline on Eestis kehtiv õiguslik regulatsioon töötaja isikuandmete kogumiseks ja töötlemiseks töösuhetes, mistõttu tuleb vaadelda kogu õigusruumi, milles Eesti on, sh Euroopa Liidu õigusruumi.

Seetõttu keskendub töö autor selles peatükis privaatsus- ja andmekaitseõiguse tõlgendamisele ja sisutamisele nii Eestis kui Euroopas. Esmalt vaadeltakse privaatsusõiguse kujunemist, et anda ülevaade peamistest õigusaktidest, mis kehtivad Eesti töösuhetes. Sealhulgas kehtivad Eestis Euroopa Liidus vastuvõetud seadused, määrused ja direktiivid. Seejärel liigutakse konkreetsemalt jälgimisseadmete kohta käivatele õigusaktidele, millega tööandjad töösuhetes arvestama peavad.

2.1 Privaatsus- ja andmekaitseõiguse kujunemine

Privaatsus kui õiguhüve on tunnustamist leidnud juba üsna varases ajaloos. Juba 14. sajandil pöördusid inimesed kohtudesse põhjusel, et neid kuulati pealt või nende personaalseid kirju avati nende loata. Alates 19. sajandi lõpust on rõhk privaatsusel liikunud järjest enam indiviidide enda kohta käivate isikuandmete kaitsmise suunas (Holvast, 2008: 15). Avalikkuse tähelepanu alla sattus privaatsusõigus esmakordselt Ameerika Ühendriikides kui 1891. aastal kirjeldasid prominentsed advokaadid Samuel Warren ja Louis Brandeis oma kuulsas artiklis õigusest olla jäetud üksi (inglise keeles “*right to be left alone*”) (Holvast, 2008: 13) vastumeelsusest ajakirjanike liigsest sekkumisest inimeste eraellu (Stalla-Bourdillon, Phillips & Ryan, 2014: 6).

Esimene verstaapost inimõiguste ajaloos, kus esmakordselt sätestati privaatsusõigus kui inimõigus, on Ühinenud Rahvaste Organisatsiooni 1948. aasta Inimõiguste ülddeklaratsioon, mis on oluliselt mõjutanud teiste inimõigusi käsitlevate dokumentide väljatöötamist Euroopas (Euroopa Liidu Põhiõiguste Amet, 2015: 14). Euroopa riikide jaoks on esimene õiguslikult siduv akt 1950. aastal Euroopa Nõukogu poolt vastu võetud Euroopa inimõiguste ja põhivabaduste kaitse konventsioon (edaspidi EIÕK), mis jõustus 1953. aastal. EIÕK (2010; artikkel 8 lg-d 1 - 2) sätestab õiguse privaatsusle järgmiselt:

1. Igaühel on õigus sellele, et austataks tema era- ja perekonnaelu ja kodu ning sõnumite saladust.
2. Ametivõimud ei sekku selle õiguse kasutamisse muidu, kui kooskõlas seadusega ja kui see on demokraatlikus ühiskonnas vajalik riigi julgeoleku, ühiskondliku turvalisuse või riigi majandusliku heaolu huvides, korratuse või kuriteo ärahoidmiseks, tervise või kõlbluse või kaasinimeste õiguste ja vabaduste kaitseks.

EIÕKst tulenevate kohustuste täitmist kontrollib 1959. aastal asutatud Euroopa Inimõiguste Kohus (edaspidi EIK). Oma praktika jooksul on EIK hulganisti käsitlenud juhtumeid, milles on esile kerkinud andmekaitseküsimus, eeskätt teabevahetuse pealtkuulamine ja eri tüüpi jälgimine (Euroopa Liidu Põhiõiguste Amet, 2015: 14-15). Näiteks kaasuses *Niemietz vs Saksamaa* (1992; punkt 29) analüüsisk EIK EIÕK artikli 8 kohaldamist töösuhetes. EIKo leiti, et eraelu ei ole tingimata seotud ainult koduga. Lahendis märgitakse, et puudub põhjus, miks eraelu mõiste alt peaks välja jätma töölase tegevuse, kuna enamiku inimeste jaoks pakub tööl oldud aeg märkimisväärset, kui mitte suurimat, võimalust arendada suhteid välismaailmaga. Seda toetab asjaolu, et alati ei ole võimalik selgelt eristada, millised inimese tegevused kuuluvad tööellu ja millised mitte.

Vajadus privaatsuse järele on tihedalt seotud tehnoloogia arenguga, sest informatsioon inimeste kohta on läbi tehnoloogiliste vahendite üha kättesaadavam. Ühena esimestest defineeriti privaatsus läbi enesemääratlemise Alan Westini 1967. aastal ilmunud raamatus “Privaatsus ja vabadus” (inglise keeles “*Privacy and Freedom*”), kus on see sõnastatud järgmiselt: privaatsus on indiviidide, gruppide või institutsioonide õigus ise otsustada, kuna, kuidas ja mil määral jagavad nad enese kohta käivat informatsiooni teistega (Holvast, 2008: 13).

Esimene rahvusvaheliselt õiguslikult siduv dokument, mis käsitleb otseselt andmekaitset on isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon (edaspidi konventsioon nr 108), mis võeti Euroopa Nõukogu poolt vastu 1981. aastal. Konventsioon nr 108 eesmärk on isiku õigus säilitada privaatsus isikuandmete automatiseeritud töötlemisel ja eraelu kaitse tugevdamine digitaalajastul. Konventsioon nr 108 on ratifitseerinud kõik Euroopa Liidu liikmeriigid (Euroopa Liidu Põhiõiguste Amet, 2015: 14-17). Konventsioon nr 108 alusel on Euroopa Nõukogu Ministrite Komitee poolt 1989. aastal võetud vastu soovitus, mis puudutab otseselt tööseadusandlust. Selles sätestatakse töötajate eraelu puutumatus ja inimväärikuse austamine isikuandmete tööhõiveotstarbelisel kogumisel ja kasutamisel. Lisaks kohustus töötajaid täielikult teavitada selliste tehniliste vahendite kasutusele võtmisest, mis jälgivad töötajate liigutusi või tööviljakust (Euroopa Nõukogu Ministrite Komitee, 1989). Seega esmakordselt on mainitud jälgimisseadmete õigusliku rakendamise seotust tööõigusega Euroopa Liidu tasandil.

2.2 Privaatsus ja andmekaitseõigus Euroopa Liidus

Kuigi Euroopa Nõukogu poolt välja antud õigusaktid ei ole õiguslikult seotud Euroopa Liiduga, siis kõik EL liikmesriigid on ratifitseerinud nii konventsioon nr 108 kui EIÕK. Seetõttu on need saanud ka osaks siseriiklikest õigustest ning järelikult üldprintsipiideks Euroopa Liidu seadustes. Sama arutluskäiku on deklareerinud ka Euroopa Liidu kohus, kes rõhutab, et seetõttu on need on aluseks EL seadustele ja printsipiidele (Fink, 2014: 75).

Töösuhetes tekib tihti vaidlus, kumb on olulisem, kas tööandja õigus töötajat kontrollida või töötaja õigus privaatsusele. Tööandja omab vara ja vahendeid, millega tööd tehakse, mistõttu on tööandjal huvi neid kaitsta. Kuigi tegemist on põhimõttelise vaidlusega, siis Eesti koos Euroopaga on võtnud selge suuna. Euroopa on aluseks õiguste lähenemine (inglise keelest “*rights approach*”), mis tähendab seda, et igal inimesel on õigus väärikusele ja eraelule ning need õigused on võrdsed teiste õigustega. Võrdluseks, et Ameerika Ühendriikides on omandipõhine lähenemine (inglise keeles

“*property approach*”), mis tähendab seda, vara ja ressursside omajal on õigus omada kontrollivahendeid ja dikteerida reegleid, mis on talle soodsamad. (Levin et al., 2006). Privaatsusõigus Euroopas arenenud suhteliselt autonoomselt ja eraldi Ameerika Ühendriikidest EIK egiidi all (Stalla-Bourdillon et al., 2014: 6).

Donald Aplin, Bloomberg BNA Ameerika Ühendriikide ja rahvusvahelise privaatsusõiguse ja andmekaitse uudiste tegevtoimetaja (Bloomberg BNA, 2017), on võrrelnud Euroopa Liidu privaatsusõigust teiste riikide, sealhulgas Ameerika ja Aafrika riikide privaatsusregulatsioonidega ja lausunud järgmist:

“Euroopa Liidul on luksust mõelda asjadele nagu privaatsus, mis on Esimese Maailma probleem. Kõik suured Aafrika riigid saavad aru, et nad tõenäoliselt peaksid selle probleemiga tegelema, kuid nad peavad muretsema veel teedevõrgu ehitamise, telefonivõrkude, töödiguse ja looduskeskkonna murede pärast.” (Geller, 2016)

Euroopa Liidu liikmesriigid on omavahel kokku leppinud, et vajalik on ühtne euroopalik andmekaitse süsteem ja isiku eraelu ja privaatsuse puutumatus on põhiväärtus, milles järelandmisi ei tehta (Liivoja, 2015). See tähendab ka seda, et Euroopa Liidu siseselt võib isikuandmeid ühest riigist teise edastada, sest riikide turvanõuded privaatsusele ja andmekaitsele on ühtlustatud. Samas erineva lähenemise tõttu Euroopas ja Ameerikas on EL Ameerika Ühendriikide kohta teinud osalise piisavuse otsuse (s.t, et USAsse andmeid saata, tuleb täita lisanõuded), mis tähendab seda, et EL ei pea Ameerika Ühendriike piisavalt turvaliseks riigiks isikuandmete edastamisel (Euroopa Komisjon, 2017: 7).

Isikuandmete kaitse sai eraldi EL aluslepingutest põhiõiguseks alatest 2009. aastat, kui ratifitseeriti Euroopa Liidu põhiõiguste harta (edaspidi harta) (Fink, 2014: 75). Harta (2012; artikkel 7) sätestab privaatsusõiguse järgmiselt: Igaühel on õigus sellele, et austataks tema era- ja perekonnaelu, kodu ja edastatavate sõnumite saladust. Lisaks sätestab harta (2012; artikkel 8 lõiked 1-2), et õiguse isikuandmete kaitsele, eesmärgipärase töötlemise isiku nõusolekul või seaduses ettenähtud õiguslikul alusel ning igäihe õiguse tutvuda tema kohta kogutud andmetega.

Peamine EL andmekaitsealane õigusakt on Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (edaspidi andmekaitse direktiiv). Andmekaitse direktiivi eesmärk on täpsustada konventsioonis nr 108 juba sätestatud põhimõtteid eraelu puutumatus õiguse kohta ning laiendada

nende sisu. (Euroopa Liidu Põhiõiguste Amet, 2015: 18). Andmekaitse direktiivi (2003; punkt 28) üks olulisemaid põhimõtteid, mida tuleb jälgida jälgimisseadmete rakendamisel töösuhetes on see, et nende paigaldamiseks on tarvis seaduslikku alust, oluline on eesmärgipärane kasutamine ning nende abil kogutud info edasine kasutamine, mis ei või olla vastuolus esialgsete eesmärkidega. Kuna direktiiv ei ole otsekohalduv, siis on Eesti õiguses võetud selle sätteid aluseks isikuandmete kaitse seaduse (edaspidi IKS) väljatöötamisel.

Andmekaitse direktiivi alusel on Euroopa tasandil loodud ka Andmekaitseasutuste töörühm (ingl *Article 29 Data Protection Working Party*), kes on vastu võtnud mitmeid arvamusi ja soovitusi, mida on edaspidises töös kasutatud selgitamiseks Eestis kehtivaid sätteid jälgimisseadmete kasutamise kohta. Lisaks on kasutatud Euroopa Andmekaitse inspektori (ingl *European Data Protection Supervisor*) 2010. aasta arvamust (ingl *Video-surveillance Guidelines*).

2.3 Privaatsus ja andmekaitseõigus Eestis ja Eesti töösuhetes

2.3.1 Õigus isikuandmete kaitsele

Õiguse privaatsusele ja eraelu austamise kohustuse töökohal sätestab töölepingu seaduse (edaspidi TLS) (2017) § 28 lg 2 p 11, mille kohaselt on tööandjal kohustus austada töötaja privaatsust ja kontrollida töökohustuste täitmist viisil, mis ei riku töötaja põhiõigusi. Töötaja põhiõiguseid TLS täpsustavalt välja ei too. Õigus privaatsusele ja andmekaitsele on Eesti õiguses sätestatud EIÕK eeskujul erinevate paragrahvidega põhiseaduses (edaspidi PS) (PS, 2012: 26/p-d 2-3). PS (2015) § 18 kaitseb au ja head nime, § 19 õigust vabale eneseteostamisele, § 26 era- ja perekonnaelu puutumatust ja § 33 sõnumite saladust.

Töösuhete ja jälgimisseadmete vaates on neist kõige olulisemad § 19 ja § 26. PS § 19 hõlmab üldise isiksuspõhiõiguse enesemääramisõigusele, sh õiguse informatsioonilisele enesemääratlemisele. See tähendab igäühe õigust ise otsustada, kas ja kui palju tema kohta andmeid kogutakse ja salvestatakse (PS, 2012: 19/p 3.1.2.1). Riigikohtu tsiviilkolleegium (2010: p 11) leidis, et PS § 19-st tuleneb enesekujutamise õigus, mille all tuleb muu hulgas mõista õigust oma kujutisele. Õigus kujutisele hõlmab nii kujutise pildis kui ka liikuvus pildis.

Eraelu puutumatuse kui põhiõiguse kaitsealasse kuuluvad eelkõige isiku füüsiline ja vaimne puutumatuse, tema identiteet, isikuandmed, seksuaalsus ning õigus oma kujutisele. Isiku identiteet

hõlmab isiku nime, tema välimust, tundeid ja mõtteid, isiku minevikku, usutunnistust ja muid veendumusi (PS, 2012: 26/p-d 9.1-9.6).

Kuna jälgimisseadmete kasutamine on riive isiku enesemääramisõigusele ja tema identiteedile, siis tuleb neid õigusedi PS kohaselt kaitsta. Töösuhete kontekstis on Euroopa Andmekaitseasutuse töögrupp (2001: 19) on oma arvamuses nr 8/2001 märkinud, et töötajatel on tööl õigustatud ootus privaatsusele. Tööandjatel on küll legitiimne huvi töötaja isikuandmete vastu, kuid seda ainult selles ulatuses, mis on kookõlas seadusliku eesmärgiga ja on vajalik töösuhete normaaseteks igapäevasteks tegemisteks. Pilving (2005: 533) märgib, et eraelu tuleb mõista laialt, lisaks inimese intiim- ja sisemisele sfäärile laieneb kaitse ka suhetele teiste isikutega, samuti äriilistele ja sotsiaalsetele kontaktidele. Kuna töötajate jälgimine ja kontrollimine tööandja poolt kujutab endast isikuandmete töötlemist, siis tuleb antud küsimustes lähetuda üldisest isikuandmete töötlemise ja kaitse põhimõtetest, mis on sätestatud IKSis.

2.3.2 Isikuandmete töötlemise õiguslikud alused

Isikuandmeteks on mistahes andmed tuvastatud või tuvastatava füüsilise isiku kohta, sõltumata sellest, millisel kujul või vormis need on (IKS, 2016: § 4 lg 1). Isikuandmete töötlemine on iga isikuandmetega tehtav toiming, sealhulgas isikuandmete kogumine, salvestamine, korrastamine, säilitamine, muutmine ja avalikustamine, juurdepääsu võimaldamine isikuandmetele, päringute teostamine ja väljavõtete tegemine, isikuandmete kasutamine, edastamine, ristkasutamine, ühendamine, sulgemine, kustutamine või hävitamine, või mitu eelnimetatud toimingut, sõltumata toimingute teostamise viisist ja kasutatavatest vahenditest (AKI, 2013b: 12-13). Isikuandmete töötlemine kujutab endast vähemal või rohkemal määral ohtu töötaja privaatsusele. Seda on selgitanud ka EIK (2000: p 65) kaasuses *Amann vs Šveits*, et kuigi kuulati pealt äriküsimustega seotud telefonikõnet, siis telefonikõne kohta säilinud andmed olid seotud töötaja eraeluga. „Eraelu” mõiste hulgast ei tohiks välja jätta äritegevust, sest et pelk eraelu puudutavate andmete kogumine kujutab endast juba isiku privaatsusesse sekkumist ning kogutud isikuandmete edasisel kasutamisel ei ole siin mingisugust tähendust. Kohus tegi otsuse, et tegu oli EIÕK artikli 8 rikkumisega.

IKS (2016) §-de 10 lg 1 ja § 14 lg 1 kohaselt on isikuandmete töötlemine lubatud kahel peamisel juhul: admesubjekti nõusolekul ja seadusest tuleneval põhjusel. Töösuhetes on andmesubjektiks töötaja. Nõusolek isikuandmete töötlemiseks kehtib üksnes juhul, kui see tugineb töötaja vabal tahtel ja on tehtud kirjalikus vormis (IKS, 2016: § 12 lg-d 1-2, 4). Nõusolekus peavad olema selgelt

määratletud andmed, mille töötlemiseks luba antakse, andmete töötlemise eesmärk ning isikud, kellele andmete edastamine on lubatud, samuti andmete kolmandatele isikutele edastamise tingimused ning andmesubjekti õigused tema isikuandmete edasise töötlemise osas. Vaikimist või tegevusetust nõusolekuks ei loeta. Nõusolek võib olla osaline ja tingimuslik (andmekaitseinspektor, 2003: artikkel 2). Euroopa andmekaitseasutuste töörühm (2001:3) on märkinud, et kui isikuandmete töötlemine on töösuhete seisukohalt möödapääsmatult vajalik, siis nõusoleku küsimine töötajalt on eksitav. Nõusoleku küsimine peaks piirduma nende juhtudega, kus töötaja on päriselt vaba otsustamaks, kas soovib nõusolekut anda ning tal on hiljem võimalik nõusolek tagasi võtta kartmata negatiivseid tagajärgi. Olukorras, kus töötajal on küll teoreetiliselt õigus nõusolek tagasi võtta, kuid reaalseks tagajärjeks võib olla töökoha kaotus, siis sel juhul ei ole nõusolek antud vabatahtlikult ning seega see ei ole see kehtiv (Euroopa Andmekaitseasutuste töörühm, 2001: 23). AKI (2013b: 15) on seisukohal, et töötaja nõusolekut saab isikuandmete töötlemiseks küsida vaid juhul kui töötajal on tõepoolest võimalik otsustada, kas ta soovib anda nõusoleku ning tal on realselt võimalus ka nõusolek tagasi võtta. Seetõttu ei saa jälgimisseadmete abil kogutud isikuandmete töötlemine toimuda töötaja nõusolekul, sest tal puudub realselt võimalus paluda lõpetada tema jälgimine üks kõik mis ajal.

Seadusest tuleneval alusel andmesubjekti nõusolekuta võib töösuhetes isikuandmeid töödelda töötajaga sõlmitud lepingu täitmiseks (IKS, 2016: § 14 lg 1 p 4), töötaja elu, tervise või vabaduse kaitseks, kui temalt ei ole võimalik nõusolekut saada (IKS, 2016: § 14 lg 2 p 2) või isikute ja vara kaitseks kui sellega ei kahjustata ülemääraselt andmesubjekti õigustatud huve (IKS, 2016: § 14 lg 3).

AKI (2013b: 20) on seisukohal, et töösuhetes saab isikuandmete töötlemise aluseks olla üldjuhul ainult IKS (2016) § 14 lg 1 p 4 ehk selles ulatuses, mis on vajalik lepingu täitmiseks (nt on tööandjal tarvis teada töötaja isikukoodi, et kanda tema andmed töötajate registrisse) ja IKS (2016) § 10 lg 1 ehk töötaja nõusolekul (nt töötaja annab tööandjale teada, et talle on määratud osaline või puuduv töövõime, et saada pikendatud põhipuhkust).

AKI (2013b: 71) selgitab, et IKS (2016) § 14 lg 3 kohaselt võib turvakaameraid paigaldada isikute ja vara kaitseks, nt hoonete ja seadmete jälgimiseks, kuid need ei tohiks olla suunatud konkreetselt töötajate tegevuse jälgimisele. Töötajate kontrollimiseks nimetatud paragrahv ei kvalifitseeru. IKS (2016) § 14 lg 3 on sõnastatud järgmiselt: Isikute või vara kaitseks võib isikuandmeid edastavat või salvestavat jälgimisseadmetikku kasutada üksnes juhul, kui sellega ei kahjustata ülemääraselt andmesubjekti õigustatud huve ning kogutavaid andmeid kasutatakse ainult nende kogumise

eesmärgist lähtuvalt. Andmesubjekti nõusolekut asendab sellise andmetöötluse korral jälgimisseadmestiku kasutamise fakti ning andmete töötleva nime ja kontaktandmete piisavalt selge teatavakstegemine.

Seega turvakaameraid võib paigaldada isikute ja vara kaitseks, kuid peab jälgima, et kaamerad oleksid paigaldatud selliselt, et see ei kahjustaks liigselt töötajaid. Paratamatult jäävad kaamerate vaatevälja kohati ka töötajad, mistõttu tuleb mingil määral töötajate isikuandmeid siiski töödeldakse. Seetõttu peab turvakaamerate paigaldamisel arvestada IKS (2016) §-is 6 sätesatud põhimõtteid, mida on kirjeldatud järgnevalt.

Seaduslikkuse põhimõte – isikuandmeid võib koguda vaid ausal ja seaduslikul teel (IKS, 2016: § 6 p 1). Töösuhte puhul on seaduslikuks aluseks, mis annab tööandjale õiguse töötaja andmeid töödelda, töösuhe ise (Männiko, 2011: 143). Andmekaitse direktiiv (2003: artikkel 7 p b) sätestab, et isikuandmeid võib töödelda lepingu täitmiseks. Sisuliselt on tegemist IKS (2016) § 14 lg 1 p 4, mille kohaselt ei ole isiku nõusolekut tarvis, kui isikuandmeid töödeldakse lepingu isikuga seotud täitmiseks.

Eesmärgikohasuse põhimõte – isikuandmeid võib koguda üksnes määratletud ja õiguspäraste eesmärkide saavutamiseks ning neid ei või töödelda viisil, mis ei ole andmetöötluse eesmärkidega kooskõlas (IKS, 2016: § 6 p 2). See on kõige olulisem põhimõte. Kui eesmärk ei ole seaduslik, on igasugune järgnev töötlemine (peale kustutamise) ebaseaduslik. Eesmärk peab olema kindlaks määratud enne andmete kogumist. Eesmärgiks olla “isikuandmete töötlemine”. Isikuandmete töötlemine on vahend eesmärgi saavutamiseks, mitte eesmärk iseenesest (AKI, 2013b: 21). Hiljem ei või andmeid töödelda viisil, mis on vastuolus kõnealuste eesmärkidega (andmekaitse direktiiv, 2003: artikkel 6 lg 1 p b).

Minimaalsuse põhimõte – isikuandmeid võib koguda vaid ulatuses, mis on vajalik määratletud eesmärkide saavutamiseks (IKS, 2016: § 6 p 3). Ulatuses all tuleb mõelda ka ajalist ulatust – töötlemine tuleb lõpetada ja andmed kustutada või viia isikustamata kujule kohe kui on täidetud eesmärgid, milleks nad koguti (AKI, 2013b: 20). Sama põhimõte tuleneb ka IKS (2016) § 24 lg 1. Näiteks kui turvakaameraid kasutatakse varguste ja kallale tungide ennetamiseks ja tuvastamiseks, on põhjendatud vaid aset leidnud intsidente kajastavate salvestiste säilitamine (AKI, 2013b: 71). Euroopa Andmekaitseinspektori (2010: 33, p 7.1.2) hinnangul võib turva- ja sissepääsukaamerate salvestisi säilitada maksimaalselt ühe nädala – selle aja jooksul peaks olema võimalik otsustada, kas

mingit salvestist on vaja pikemalt säilitada intsidendi uurimiseks. Vastuolu tuleb siinkohal turvaseadusest (2015: § 11 lg 4), mille kohaselt säilitatakse salvestisi vähemalt üks kuu, kuid mitte kauem kui üks aasta.

Kasutuse piiramise põhimõte – isikuandmeid võib muudel eesmärkidel kasutada üksnes andmesubjekti nõusolekul või selleks pädeva organi loal (IKS, 2016: § 6 p 4).

Turvalisuse põhimõte – isikuandmete kaitseks tuleb rakendada turvameetmeid, et kaitsta neid tahtmatu või volitamata töötlemise, avalikuks tuleku või hävimise eest (IKS, 2016: § 6 p 6). Töötlemisel peab võtma arvesse tehnika taset (andmekaitse direktiiv, 2003: artikkel 17).

Individaalse osaluse põhimõte – andmesubjekti tuleb teavitada tema kohta kogutavatest andmetest, talle tuleb võimaldada juurdepääs tema kohta käivatele andmetele ja tal on õigus nõuda ebatäpsete või eksitavate andmete parandamist (IKS, 2016: § 6 p 7). Lisaks on töötajal õigus teada kellele tema isikuandmeid edastatakse (nt maksu- ja tolliamet, haigekassa) ning kes neid andmeid veel töötleb (nt ettevõtte juht, raamatupidaja) (IKS, 2016: §-id 15, 19).

2.4 Jälgimisseadmete kasutamine töösuhetes

Enne turvakaamerate paigaldamist ettevõttesse tuleb läbi mõelda, millistel eesmärkidel seda tehakse. IKS (2016) § 14 lg 3 kohaselt võib jälgimisseadmeid paigaldada üksnes isikute ja vara kaitseks. Eesmärk peab olema sõnastatud selgelt. Ebamäärane, mitmeti mõistetav või lihtsalt liiga üldine kirjeldus jälgimisseadmetiku paigaldamiseks ei ole piisav (Euroopa Andmekaitseinspektor, lk 17). Iga turvarisk peaks olema eraldi välja toodud, samuti see, kas turvakaamerate kasutamise eesmärk on konkreetse turvariski eenetamine või uurimine (Euroopa Andmekaitseinspektor, 2010: 20, p 5.7). Näiteks sissepääsu juurde paigaldatud turvakaamera (mille eesmärk on ennetada ja avastada varguseid ja vandalismi) lindistusi ei või kasutada selleks, et kontrollida, kas töötajad peavad tööajast kinni või kas konkreetne töötaja oli tööle tulles purjus (AKI, 2013b: 70). Euroopa Andmekaitseasutuste töörühm (2002: 22) on seisukohal, et distantsilt töötaja jälgimine tema töö kvaliteedi ja hulga kontrollimise eesmärgil ei ole lubatav. Ka Euroopa Andmekaitseinspektor (2010: 22, p 5.9) on seisukohal, et eesmärgid nagu tootlikkuse juhtimine, kvaliteedi tagamine, ettevõtte poliitika juurutamine või vaidluste puhuks tõendite kogumine, ei ole piisavad eesmärgid, et õigustada jälgimisseadmetiku kasutamist. Töötajate pidevat terve tööaja kestvat jälgimist tuleks igal võimalikul juhul vältida.

Turvakaamera salvestise kasutamine töösuhetes saab kõne alla tulla tõendinda, nt olukorras, kus eesmärgiks on konkreetse turvariski ennetamine või uurimine (Euroopa Andmekaiseinspektor, 2010: 21, p 5.8). EIK (2010: 11-12) leidis lahendis *Köpke vs Saksamaa*, et töötajat on lubatud kaamera abil jälgida üksnes tõsise ja põhjendatud kahtluse korral piiratud aja jooksul. Nimetatud lahendis tekkis tööandjal arvepidamise andmete analüüsimise põhjal tõsine kahtlus, et kassapidaja manipuleerib andmetega ja maksab taarapudeleid tagastades raha välja suuremas summas, kui on tagastatud pudelite väärtus. Tegemist oli põhjendatud kahtlusega, jälgiti ainult ühte konkreetset töötajat piiratud aja jooksul.

Kui eesmärk on paigas, siis tuleb turvakaamerate paigaldamisel arvestada minimaalsuse põhimõtet (IKS, 2016: § 6 p 3) ja seda, et ei kahjustataks ülemääraselt töötaja õigustatud huve (IKS, 2016: § 14 lg 3). Näiteks konkreetse töötaja ja tööandja vara klientide rünnakute (röövide) eest kaitsmiseks kasutatava kaamera peaks suunama selliselt, et vaatevälja jäävad ainult kliendid. Samuti võiks kaamera tööle rakenduda kliendi sisenemisel või töötaja poolt häire andmisel. Sissemurdumiste puhuks seatud kaamerad võiks tööle rakendada ainult töövälisel ajal. (AKI, 2013b: 70).

AKI on tõdenud, et Eesti töötajatele valmistab muret töötamine kaamerate vaateväljas. See näib olevat töökohtades töötajate kõige olulisem probleem. Seetõttu oli AKI 2010. aasta prioriteet isikuandmete temaatika. AKI infotelefonile helistajad on valdavalt töötajad, kes kurdavad ettevõttesse paigaldatud kaamerate üle (AKI, 2011). Ka AKI (2014, 2016) 2013. ja 2015. aasta kokkuvõttes nenditakse, et üha enam saabub pöördumisi töötajate jälgimise küsimustes ning see on üks enim küsitavaid küsimusi.

Kuigi isikute ja vara kaitseks paigaltavate turvakaamerate teavitamiskohustus on täidetud vastavate siltide panekuga ettevõtte ustele, siis töötajate hirmude hajutamiseks on mõistlik kasutada ulatuslikumalt teavitamist. Selleks on AKI 2011. aastal koostanud juhise “isikuandmete töötlemine töösuhetes” (edaspidi AKI juhise) (AKI, 2012). Juhises on välja töötatud soovituslik vorm, millega tuleks töötajaid jälgimisseadmete kaustamisest teavitada. Soovituslik juhenda peaks AKI (2013b: 72) hinnangul sisaldama järgmist:

- 1) jälgimisseadmete kasutamise eesmärk või eesmärgid (jälgimisseadmete ja eesmärkide paljususe korral tuleb täpsustada, milline seade milliseid eemärke teenib);
- 2) kas ja milliste töökohustuste rikkumiste menetlemiseks jälgimisseadmete salvestisi võidakse kasutada;

- 3) jälgitav ala;
- 4) jälgimise aeg;
- 5) jälgimise liik (reaalajas või salvestamisega);
- 6) jälgimisseadme üldine kirjeldus (statsionaarne, pööratav, suurendamisvõimalusega, koos helisalvestamisega jne);
- 7) jälgimisega kogutud andmete töötlejate andmed;
- 8) jälgimisega kogutud andmete kolmandatele isikutele edastamine;
- 9) jälgimisega kogutud andmete kaitse korraldus;
- 10) salvestiste säilitamise aeg;
- 11) salvestistega tutvumise kord.

AKI on turvakaamerate kasutamise osas töökohtadel läbi viinud mitu kontrolli. 2010. aastal kontrolliti 15 kaubandusettevõtet. Väga tõsiseid otseseid rikkumisi (näiteks riietusruumides, proovikabiinides ega tualettruumides kaamerate olemasolu) ei tuvastatud. Eksiti aga mitmete teiste nõuete vastu, näiteks sularaha seifi filmimisel jälgiti terves ruumis asuvaid töökohti, kaamera asus puhkeruumis selliselt, et töötajatel ei olnud võimalik puhkeruumis viibida kaamera vaateväljast väljaspool. Enamus tööandjatest ei olnud töötajaid teavitanud valvekaamerate kasutamisest. Inspektsiooni hinnangul tulenesid rikkumised teadmatusel (AKI, 2011: 41). 2013. aastal viis AKI koostöös Läti ja Leedu isikuandmete kaitse järelevalveasutustega kontrolli Balti riikide Radisson Blu Hotel kaubamärki kasutavas üheksas hotellis (neist kaks asub Eestis). Kontrolli käigus tuvastati puuduseid turvakaamerate teavitamisel. Hotellid olid küll võtnud kasutusele turvakaamerate kasutamisest teavitavad sildid, kuid need olid võrdlemisi väikeste mõõtmetega ning neil puudus andmetöötaja kohta käiv informatsioon. Kui kogu hoone üldkasutatavad alad on jälgimise all, siis peaks olema vastav märgistus ka sisealal, mitte vaid hotelli peasissekäigu juures. Rikkumised tulenesid AKI hinnangul teadmatusel (Liivrand, Balode & Šinkúniené, 2013).

Olgugi, et isikute ja vara kaitseks paigaltavate kaamerate puhul on tööandjate teavitamiskohustus kaamerate olemasolust töötajatele üsna minimaalne – piisab üksnes siltidest, siis sellegipoolest tuleb ette rikkumisi, seda ka suurtes ettevõtetes, kus üldjuhul on olemas personaliosakond või vähemalt personalijuht, kes peaks olema isikuandmete töötlisel töösuhetes piisavalt kompetentne.

2014. aastal sai AKI kaks vihjet kahe erineva ettevõtte kohta, mida ka kontrolliti. Kontrolliti turvakaamerate kasutamise eesmärgikohasuse, minimaalsuse ja kasutuse piiramise rakendamist. Esimesel juhul olid kaamerad paigutatud tootmisruumidesse. Videovalve kasutamisest teavitasid

ruumidesse sisenejaid ustel olevad sildid, millel oli ka viide kaamerate omanikule, vastutava isiku nimi ja telefoninumber. Kaamerate kasutamine oli reguleeritud töö sisekorraeskirjades, millega võib tutvuda tootmisruumi seinal oleval stendil. Jälgimissüsteemi kasutamise faktist, kohast ja eesmärgist teavitatakse töötajaid töölepingus ja selle lisaks olevas ametijuhendis. Kaamerate kasutamise eesmärgiks on isikute ja vara kaitse, tööohutuse, tööprotsessi katkematus ja tööaja optimaalse kasutamise jälgimine. Ligipääs salvestistele on kaitstud paroolidega ning salvestisi säilitatakse serveriteenust pakkivas ettevõttes. Kuna salvestiste hoidmise tähtaega ei olnud üheski dokumendis reguleeritud, soovitas AKI analüüsida, kui kaua on neid eesmärkide saavutamiseks vaja säilitada ning kehtestada konkreetset tähtajad. Kuna ettevõttes ei tuvastatud isikuandmete kaitse seaduse nõuete rikkumist, lõpetas inspeksioon riikliku järelevalvemenetluse. Teises ettevõttes olid kaamerad paigaldatud tehase tootmisruumidesse ja territooriumile eesmärgiga jälgida tööprotsessi ning isikute ja vara kaitseks. Kaamerate kasutamine oli reguleeritud töökorralduse eeskirjades, mida tutvustati töötajatele tööle asumisel. Lisaks sellele oli isikuandmete töötlemine reguleeritud töölepingu lisaks olevas isikuandmete töötlemise infolehes ja töötaja nõusolekus. Hoonesse sisenejat teavitas videojärelevalvest vastav silt uksele. Kaamerapilti ei jälgitud reaalselt, salvestisi vaadati ainult vajaduse tekkimisel (toodangu purunemise või õnnetuse põhjuste selgitamiseks). Salvestisi hoitakse serveris umbes kaks nädalat, misjärel need kirjutatakse uuesti üle. Kuna ettevõttes ei tuvastatud isikuandmete kaitse seaduse nõuete rikkumist, lõpetas inspeksioon riikliku järelevalvemenetluse. (AKI, 2015: 29-30).

Autor leiab, et kahe nimetatud juhtumi puhul on märkmisväärne asjaolu, et ettevõtteid kontrolliti vihjete alusel. Kummalgi ettevõttel ei olnud kasutusel AKI koostatud soovituslikku juhendit kaamerate paigaldamisest. Esimene ettevõtte oli märkinud, et üheks turvakaamerate kasutamise eesmärgiks on muuhulgas tööprotsessi katkematus ja tööaja optimaalse kasutamise jälgimine. Laskmata ennast eksitada sõnastusest tähendab tööaja optimaalse kasutamise jälgimine oma sisult töö tegemise jälgimist, mis läheb vastuollu nii Euroopa Andmekaitseinspektori kui Euroopa Andmekaitseasutuste tööühma arvamusega. Samal ajal tähendab see ka seda, et turvakaamerate eesmärk ei ole ainuüksi isikute ja vara kaitse ning vastuolla minnakse minimaalsuse põhimõttega. Töötaja optimaalset kasutamist on võimalik kontrollida nt kiipkaartide süsteemi rakendamisega, tükitöö eesmärkide seadmise ja juhi vahetu kontrolli jms. Kuna ettevõtteid kontrolliti vihjete alusel, siis võib eeldada, et vihjete tegija leidis, et turvakaamerate kasutamisel on rikutud mingisuguseid nõudeid või tundis ennast muul moel häirituna turvakaamerate olemasolust. Iga vihje ei pruugi loomulikult tähendada rikkumise asetleidmist. Vastus võib peituda hoopis selles, et töötajate privaatsusootused ei pruugi saada piisavalt tuge kehtivast seadusandlusest.

Seda, et töötajate ja tööandjate arusaamad privaatsuse õigustatud ootusest ei kattu tõendab ka töövaidluskomisjoni (edaspidi TVK) praktika. Vaidluses nr 4.1-2/128-2012 (TVKo, 2012) ütles tööandja töötajaga töölepingu üles muuhulgas seetõttu, et töötaja paigaldas turvakaamera ette papitüki. Tööandja rõhutas vaidluses, et tööandjal puudub seadusest tulenev kohutus teavitada eraldi kõiki töötajaid oma ettevõtte vara säilimise ja valve tõhustamise eesmärgil tehtavatest meetmetest. Ettevõtte ustel olid sildid, mis teavitasid turvakaamerate olemasolust. Töötaja leidis, et turvakaamera on häiriv ja sellega jälgitakse tema töö tegemist. Töövaidluskomisjon leidis, et kuna tööandja poolt on ustele pandud vastavad sildid, siis on tööandja teavitamiskohustus täidetud.

Sarnase sisuga kaasus on ka vaidluses nr 4-1/2633 (TVKo, 2016), kus tööandja ütles töötajaga töösuhte üles seetõttu, et töötaja ei usalda tööandjat. Usalduse puudumine seisnes tööandja väitel selles, et töötaja suunas turvakaamera käsitsi eemale ning esitas AKIle sellekohase kaebuse. Töötaja selgitas, et tundis ennast ahistatuna ning turvakaamerate paigaldamise kohta talle mingisugust infot ei jagatud. Tööandja rõhutas vaidluses, et tööandjal ei ole vaja saada töötaja nõusolekut kaamerate paigaldamiseks tööruumidesse. Tööandja oli seisukohal, et kui töötajal ei ole midagi varjata, siis ei ole tal ka tarvis teada, mida kaamera täpsemalt filmib ning tööülesannete täitmise salvestamise vastu ei peaks olema ükski vähemalt keskmise mõistlikkusega inimene. Olgugi, et tööandja mõõnis töötajate töö tegemise jälgimist turvakaamerate abil, selgitas TVK oma otsuses, et tööandja võib oma vara kaitseks kasutada turvakaameraid. Ei ole tõendatud, et turvakaamera paigutati töötaja valvamiseks.

Mõlemas vaidluses tuleb välja, et töötajal on praktiliselt võimatu tõendada, et turvakaameraid kasutati nende töö tegemise jälgimiseks. Praeguse regulatsiooni kohaselt on jälgimisseadmete olemasolu teavitavad sildid uksel sisuliselt piisavad, et anda töötajatele teada kaamerate olemasolust. AKI juhend kaamerate kasutamise kohta on üksnes soovituslik ja seetõttu ei saa AKI ega ka TVK üldjuhul tuvastada muud kui seda, kas kaamerate teavitavad sildid on ustel või ei ole. Ka AKI leiab, et kaebused, kus isikuandmete ebaseaduslikku töötlemist ei ole võimalik tõendada, on probleemsed. Sellegipoolest on inspeksioon seisukohal, et taolisi vaidlusi, kus ühe poole sõna on teise vastu (nt töötaja leiab, et kaameraid kasutatakse tema töö tegemise jälgimiseks ja tööandja väidab vastupidist), peaks lahendama tsiviilkohus (AKI, 2015).

Siit kerkibki esile kõige suurem vastuolo - juhul, kui tööandja on täitnud isikuandmete teavitamise ja säilitamisega seotud nõuded, siis kui tööandja kasutab kaameraid töötajate töö tegemise jälgimiseks, on töötajatel keeruline seda tõendada, s.t töötajatel puuduvad tõendid. Samal põhjusel ei minda ka

tsiviilkohtusse. Seetõttu leiab autor, et äärmiselt oluline on välja selgitada, milline on tegelik olukord turvakaamerate kasutamisel töökohtades ning vastavalt sellele teha järeldused ja ettepanekud.

3 EMPIIRILINE UURIMUS

3.1 Uurimuse eesmärk

Käesoleva magistritöö eesmärk on välja selgitada, kas tööandjad on kaamerate paigaldamisel ja kasutamisel lähtunud õiguslikest alustest ning kas tööandjad on teinud kõik vajaliku selleks, et minimeerida jälgimisseadmete võimalikku negatiivset mõju töökohal. Selleks on autor püstitanud järgmised uurimisülesanded:

1. Selgitada välja, kas tööandjad on jälgimisseadmete paigaldamisel lähtunud õiguslikest alustest, eelkõige minimaalsuse ja eesmärgipärasuse põhimõttest.
2. Selgitada välja, kas tööandjad on jälgimisseadmete kasutamisel lähtunud õiguslikest alustest, eelkõige minimaalsuse ja eesmärgipärasuse põhimõttest.
3. Selgitada välja, kas ja millised meetodid on tööandjad võtnud kasutusele, et tagada kogutud andmete turvalisus.
4. Selgitada välja, kas ja kuidas on tööandjad töötajaid jälgimisseadmete olemasolust ja nende kasutusviisidest teavitanud.

3.2 Uurimuse metoodika

Uuringu läbiviimisel on kasutatud kvantitatiivset uurimismeetodit. Käesolev uuring on läbiviidud 2017. aastal ajavahemikus 24.-30.04. Andmekogumismeetodiks on kasutatud veebiküsitlust struktureeritud küsimustega (Lisa 2). Küsitluse läbiviimiseks kasutati veebikeskkonda *FreeOnlineSurveys*. Küsitluse online aadress edastati ettevõtetele meili teel koos tutvustava kirjaga, mis koosnes adresseerija eesmärgist ja andmetest. Küsitluse täitmine oli anonüümne, millest teavitati nii e-kirja teel kui ka ankeedi sissejuhatavas osas. Küsimustikus on kasutatud nominaalskaalat ja binaarskaalat. Nominaalskaalat kasutati ettevõtte suuruse määramiseks, selleks, et välja selgitada iskuandmetega töötaja ettevõttes. Binaarskaala abil valisid vastajad, kas ettevõtte on Eesti või välismaa päritolu.

3.3 Valim

Uuring viidi läbi Tallinna toitlustusettevõtete seas. Statistikaameti kohaselt on populatsiooni kogusuurus ehk Eestis on kokku 1977 toitlustusettevõtetest, millest 946 asub Tallinnas, mis on ~ 48% kõikidest toitlustusettevõtetest (Statistikaamet, 2017). Valimi freimiks oli Veterinaar- ja Toiduameti kodulehekülje (2017) register toitlustusettevõtetest, kellel on tegevusluba toidukäitlemiseks. Kõikidel toitlustusettevõtetal peab seaduslikuks tegutsemiseks olema tegevusluba toidukäitlemiseks. Veterinaar- ja Toiduameti koduleheküljel on nimekiri kõikidest ettevõtetest, kellel on olemas tegevusluba toidukäitlemiseks, samuti oli kodulehel olemas sobiv otsingumootor, kus oli võimalik ettevõtteid otsida asukoha järgi. Veterinaar- ja toiduameti kodulehekülje otsingumootori kaudu leiti 1637 erinevat kirjet. Kirjete arv oli nii suur seetõttu, et kuvati kõik toitlustuskohad eraldi. See tähendab, et kuvati ühe ettevõtte kõik erinevad müügikohad, näiteks ühel ettevõttel võib olla mitu erinevat restorani ja baari. Kuna kogu nimekirja läbitöötamine oli ajamahukas, iga ettevõtte koduleheküljele tuli eraldi minna, et saada e-posti aadress, siis kasutati valimi moodustamiseks süstemaatilist juhuvalimit. Valiti nimekirjast iga kolmas ettevõtte ehk valimi moodustas 315 ettevõtet. Küsitlusele vastas 146 ettevõtet ehk 46,3 % valimist. 36 vastajat ehk ligikaudu 25 % kõigist vastajatest, kes vastasid “jah” neljandale küsimusele “Kas Teie ettevõtte territooriumile on paigaldatud turvakaamerad?” jättis küsitlusele vastamise seejärel pooleli. Seega korrektselt täidetud ankeete oli kokku 110, mis on 35 % valimist.

3.4 Küsimustik

Küsimustiku esimene osa koosnes kolmest küsimusest, mille abil grupeeriti ettevõtted erinevate tunnuste abil (ettevõtte suurus töötajate arvu järgi, personalitöötaja/personali osakonna olemasolu ettevõttes ja ettevõtte päritolu (Eesti või välismaa seostega ettevõtte)). Küsimustiku teine osa koosnes 16 küsimusest.

Küsimustiku esimeseks küsimuseks oli: “Kas Teie ettevõtte territooriumile on paigaldatud turvakaamerad. Eitava vastuse korral lõppes vastaja jaoks küsitlus. Jaatava vastuse andud ettevõtete jaoks küsitlus jätkus.

Küsimuste 3 - 7, mille eesmärk oli välja selgitada turvakaamerate eesmärgipärane pigaldamine ja kasutamine, koostamisel võeti aluseks AKI juhendmaterjal (2013b), Allen et al. (2007) uuringu küsimused, IKS (2016) § 6 põhimõtted ja Ball (2010).

Küsimuste 8 - 11, mille eesmärk oli välja selgitada, kas ja millised turvanõuded on tööandjad kasutusele võtnud jälgimisseadmetega kogutud andmete kaitsmiseks, koostamisel võeti aluseks AKI juhendmaterjal (2013b) ja IKS (2016) § 6 põhimõtted.

Küsimuste 12 - 14, mille eesmärk oli välja selgitada, kas ja kuidas töötajaid on turvakaamerate olemasolust teavitatud, koostamisel võeti aluseks AKI koostatud juhend töötajate teavitamiseks ja IKSist tulenevad nõuded.

Küsimuste 15 - 15, mille eesmärk oli välja selgitada, kas ettevõtetes on esinenud töötajate pahameelt ja kas on väljatöötatud kaebuste menetlemise süsteem, koostamisel lähtuti Umpress et al. (2003).

4 TULEMUSED

4.1 Jälgimisseadmete paigaldamine ja kasutamine

Küsitlusele vastas 146 ettevõtet, millest kaamerad olid kasutusel 118-s (81%). 28 (19%) ettevõtet vastas, et neil kaameraid kasutusel pole. 118-st ettevõttes, kes vastas, et neil on kasutusel kaamerad jättis järgnevatle küsimustele vastmata 36 ettevõtet, mis on ~ 25% kõigist vastanutest.

KAAMERATE OLEMASOLU							
JAH				EI			
Ettevõtete arv töötajate arvu järgi				Ettevõtete arv töötajate arvu järgi			
vähem kui 10	10-49	50-249	250 ja enam	vähem kui 10	10-49	50-249	250 ja enam
35	61	14	8	21	6	1	0
KOKKU: 118				KOKKU: 28			
Jätkas küsitlusele vastamist							
24	43	8	7				
KOKKU: 82							

Tabel 2 Kaamerate olemasolu ettevõtetes ettevõtete töötajate arvu järgi

Allikas: Autori koostatud

Ettevõtted, kellel polnud kasutusel kaameraid, neist suurem enamus ehk 21 (75%) olid mikroettevõtted, 6 (21%) väikese suurusega ettevõtted ja 1 (4%) keskmise suurusega ettevõtte. Ootuspäraselt polnud neis ettevõtetes üldjuhul personaliosakonda ega personalijuhti, kes privaatsuse küsimustega tegeleks. 24-s (86%) ettevõttes tegeles personaliküsimustega mõni töötaja teise töö kõrvalt (nt raamatupidaja, ettevõtte juht vms). Kaks ettevõtet, kellel polnud kaameraid ja kus oli olemas personaliosakond, neist üks oli väikese suurusega ettevõtte ja teine keskmise suurusega ettevõtte (tabel 3).

ETTEVÕTTED, KUS EI OLE KASUTUSEL KAAMERAID									
Ettevõtete arv töötajate arvu järgi									
vähem kui 10		10-49			50-249			250 ja enam	
21		6			1			0	
Personaliküsimustega tegeleb ...									
Person aliosakond	Person alijuht	Personaliküsimustega tegeleb ettevõttes töötaja, kellel on ka muid tööülesandeid	Person aliosakond	Person alijuht	Personaliküsimustega tegeleb ettevõttes töötaja, kellel on ka muid tööülesandeid	Person aliosakond	Person alijuht	Personaliküsimustega tegeleb ettevõttes töötaja, kellel on ka muid tööülesandeid	-
0	2	19	1		5	1			
Ettevõtte on ...									
Eesti ettevõtte		seotud välismaa ettevõttega		Eesti ettevõtte		seotud välismaa ettevõttega		-	
21		0		6		0			

Tabel 3 Ettevõtete, kellel polnud kasutusel turvakaameraid, jagunemine suuruse personaliküsimustega tegeleja ja päritolu järgi.

Allikas: autor koostatud

Vastanutest 118-1 (81%) olid kasutusel turvakaamerad. Neist 35 (30%) olid mikroettevõtted, 61 (52%) väike ettevõtteid, 14 (12%) keskmise suurused ettevõtteid ja 8 (7%) suured ettevõtteid. Enim jättis küsitluse pooleli väikese suurusega ettevõtteid (18), keda oli vastajate seas ka enim. Ettevõtteid, kus olid kasutusel turvakaamerad, neist jätkaks küsitlusele vastamist 82.

82 ettevõtet olid turvakaamerad suunatud järgmiselt: 35 – ettevõtte välialad (nt parkla), 61 – sisse- ja väljapääsud, 68 – klientide ala, 32 – töötsoon, kaamera suunatud inventarile, 60 – kaamera suunatud nii inventarile kui töötajatele, 7 – töötajate puhkeruum, 4 – töötajare riietusruum. Ükski ettevõtte ei olnud kaamerat suunatu tualetile ja riietusruumile. Kõik ettevõtteid, kus kaamera oli suunatud riietusruumile, neis tegeles personaliküsimustega töötaja, kellel oli ka muid tööülesandeid (nt raamatupidaja, ettevõtte juht vms). Kõigil neljal ettevõttel oli kaamera lisaks riietusruumile suunatud töötsoonis töötajatele ja kolmel neist ka töötajate puhkeruumile.

Erinevus joonistus välja Eesti ja välismaa päritolu ettevõtete vahel. Küsitlusele vastas 10 ettevõtet, kes olid seotud välismaa ettevõttega (frantsiis, tütarfirma vms). 10-st ettevõttest ühelgi ei olnud

kaamerad suunatud töötajate puhke- ja riietusruumile. Ainult kahel oli kaamera suunatud töötsoonis töötajatele. Kõigil 10-l olid kaamerad suunatud ettevõtte sisse- ja väljapääsude juurde.

Küsimuse “Millistel põhjustel on ettevõttesse paigaldatud turvakaamerad?” vastusevariandid on koostanud autor tuginedes Allen et al. (2007) küsimustikule. Valida sai nii mitu varianti kui vajalik. Kaamerate paigaldamise eesmärkidena joonistusid eelkõige välja turvalisuse, ohutuse ja vargustega seotud põhjused. 67 % ettevõtetest märkis, et kaamerate paigaldamise eesmärk on töötajate ausatena hoidmine (töötajate poolt toime pandud varguste toime panek jms), 77% töötajate ohutus ja turvalisus (kaitse agressiivsete klientide eest) ning klientide ohutus ja turvalisus (67%) ning tööandja vara kaitsmine klientide toime pandud varguste eest (74%).

KAAMERATE PAIGALDAMISE EESMÄRGID		
Põhjused, mis on seotud tööandja vajadusega kontrollida (<i>as coercive control</i>)	N	% vastajatest
hoiab töötajad ausad (ennetab töötajate poolt toime pandavaid varguseid, kindlustab, et töötajad järgivad ettevõtte eeskirju ja kasutavad ettevõtte vara üksnes selleks ettenähtud põhjustel)	55	67%
töötajate toime pandud varguste avastamine	38	46%
tootlikkuse tõhustamine ja hindamine (nt tööaja optimaalne kasutamine, materjalide mõistlik kasutamine), (teenindus)kvaliteedikontroll	34	41%
Põhjused, mis on seotud tööandja hoolivusega (<i>as caring</i>)		
töötajate ohutus ja turvalisus (tagab töötajatele turvatunde agressiivsete klientide ja võimalike rünnakute, nt varguste korral)	63	77%
töötajate kaitse (kaitseb töötajaid isiklike asjade varguste eest, tagab tõendid klientide/kaastöötajate valesüüdistuste, ähvarduste ja ahistamise korral)	39	48%
aitab tagada positiivse ja kiusamisvaba töökeskkonna	8	10%
Põhjused, mis on seotud ettevõtte huvidega (<i>benefits company</i>)		
tööandja vara kaitse (ennetab klientide toime pandud varguseid)	61	74%
klientide ohutus ja turvalisus	55	67%
aitab tagada tõendid õiguslike vaidluste korral (nt kohtus, politseis)	38	46%
on abivahend juhtidele võtmaks vastu otsuseid	24	29%

Tabel 4 Kaamerate paigaldamise ja kasutamise eesmärgid

Allikas: autori koostatud

Selgitamaks välja, kas tööandjad kasutavad kaameraid eesmärkidel, milleks need paigaldatud olid, paluti tööandjatelt järgmist: “Märkige, mis põhjustel on kaamerate kasutamine veel kasulikuks osutunud.” Vastusevariandid olid samad, mis küsimusel “Millistel põhjustel on ettevõttesse paigaldatud turvakaamerad?” (tabel 4). Lisaks neile oli üks veel üks vastusevariant – “ei ole kasutatud/ei ole plaanis kasutada muudel põhjustel kui esialgu planeeritud”. Selle vastusevariandi valis üksnes 16 (20%) ettevõtet.

Ülejäänud ettevõtted valisid neile kahele küsimusele enam kui pooltel kordadel ühesuguse vastusevariandi. Tööandjad, kes vastasid, et kaamerad on paigaldatud töötajate ohutuse ja turvalisuse eesmärkidel (63 tööandjat), neist 39 vastas küsimusele “Märkige, mis põhjusel on kaamerate kasutamine veel vajalikuks osutunud” samuti töötajate ohutus ja turvalisus. Sama oli ka teiste küsimustega. 38-st ettevõttest, kes märkis, et kaamerad on paigaldatud töötajate toime pandud varguste avastamiseks, vastas 23, et kaamerad on vajalikuks osutunud ka töötajate toime pandud varguste avastamiseks. 61-st ettevõttest, kes märkis, et kaamerad on paigaldatud tööandja vara kaitseks (klientide toime pandud varguste ennetamine), vastas 32, et kaamerad on vajalikuks osutunud ka tööandja vara kaitseks (klientide toime pandud varguste ennetamine) jne.

Ettevõtted ei ole üldjuhul kasutanud teisi lahendusi, et saavutada sama eesmärki, mida turvakaamerate kasutamisega saavutatakse. Üksnes 5 (6%) ettevõtet vastas jaatavalt. Need ettevõtted tõid teiste lahendustena välja järgmised vahendid ja meetmed: *“turvatöötajad”, “Elementaarsed tööohutus nõudmised. Kaamerad asuvad tegelikult kogu majas, kus restoran ruume rendib ja olid siin enne praegust juhtkonda. Kuuluvad terve maja turvasüsteemi juurde”, “tööajaarvestuse seade”, “töötajatega suhtlemine”, “Tegelik põhjus, miks kaameraid ettevõttes kasutame on see, et oleme paaril korral varguse ohviks langenud (tegemist ei ole olnud personali poolt toime pandud kuritegevusega). Kaamerad on suunatud meie kassadele, et hiljem oleks võimalik tuvastada sissemurdja ja varguse toimepanija. Raskendanud sissemurdmise võimalust”*.

50 (61%) ettevõtet vastas, et neil on turvakaamerate salvestisi olnud tarvis realselt kasutada. Vastused jagunesid üldjuhul kaheks. Ühelt poolt on tööandjad kaamera salvestisi kasutanud klientide poolt toime pandud kakluste ja varguste tõendamiseks ja süüdlase väljaselgitamiseks (sh külmarved, töötajate vara varastamine jms). Teine olukord, kus on kaamerate salvestisi kasutatud, on töötajate poolt toime pandud varguste tõendamiseks ja töötaja tööaja kontrollimiseks (sh lõunapauside pikkus, tööle tuleku ja mineku kellaajad).

4.2 Jälgimisseadmetega kogutud info turvalisus

Küsimuste 8 - 11 eesmärk oli teada saada, kuidas on tööandjad korraldanud jälgimisseadmete abil kogutud info turvalisuse. 10% ettevõtetest toimub jälgimine üksnes reaajas ning salvestisi ei säilitata. 90% ettevõtetest säilitab salvestisi teatud perioodi jooksul. Täpselt pooled ettevõtted on kasutanud kõige turvalisemat automaatset andmete kustutamise süsteemi. Salvestiste säilitamise aeg on väga erinev 24 tunnist kuni ühe aastani.

Andmete säilitamine	N	% vastajatest	Turvakaamera säilitamise aeg (ettevõtete arv)
jälgimine toimub üksnes reaajas, salvestisi ei säilitata	8	10%	-
vajaduse järgi, säilitamise aeg ei ole kindlaks määratud. Perioodi pikkuseks märkige, millal üldjuhul salvestised kustutatakse	24	29%	mõned päevad (1), 2 nädalat (1), 1 kuu (3), 2 kuud (3), 3 kuud (3), 4 kuud (2), 6 kuud (3), 1 aasta (3), ei tea (1), sisekaamerad hetkel ei toimi (1), jättis vastamata (3)
kindlaks on määratud periood, salvestised kustutatakse manuaalselt.	9	11%	1 kuu (3), 2 kuud (2), 3 kuud (2), 6 kuud (1)
kindlaks on määratud periood, salvestised kustuvad automaatselt.	41	50%	24 tundi (1), 1 nädal (2), 10 päeva (1), 12 päeva (1), 2 nädalat (11), 3 nädalat (1), 1 kuu (13), 2 kuud (3), 3 kuud (4), 4 kuud (1), 6 kuud (1), ei soovi avaldada (1), kahjuks ei oska täpselt vastata (1)

Tabel 5 Jälgimisseadmetega kogutud salvestiste säilitamise periood

Allikas: autori koostatud

Jälgimisseadmetega kogutud andmete töötlemise eest oli vastutaja määratud 36 (44 %) ettevõttes. Selleks oli märgitud juht, juhataja, juhatuse liige või juhiabi. Seitsmel korral oli selleks turvatöötaja, turvajuht, või IT tehnik ehk töötaja, kelle tööülesanded üldjuhul ei ole töötajate töö tegemise kontrollimine jms. Kahel juhul oli ligipääs ainult kolmanda ettevõtte ehk eraldi turvafirmal või majahaldaja firmal. Ettevõtetel, kellel oli kindlaks määratud kindel isik, kes andmete töötlemise eest vastutab, nendest 23 (64%) oli ka kindlaks määratud periood, mil andmed manuaalselt (2 ettevõtet ehk 6%) või automaatselt (21 ettevõtet ehk 58%) kustutatakse. Suurema tõenäosusega oli neil ettevõtetel ka salvestised paroolidega kaitstud (26 ettevõtet ehk 72%).

JÄLGIMISSEADMETEGA KOGUTUD SALVESTISTE KAITSMISE MEETMED	N	% vastajatest
salvestised on kaitstud paroolidega	53	65%
salvestisi saab vaadata ainult ettevõtte serverist	29	35%
salvestiste vaatamiseks on ette nähtud piiratud juurdepääsuga ruum	17	21%
salvestistele on ligipääs piiratud isikute ringil	64	78%
andmeid säilitatakse vaid teatud perioodi jooksul	45	55%
muu	2	2%

Tabel 6 Jälgimisseadmetega kogutud salvestiste kaitsmise meetmed

Allikas: autori koostatud

4.3 Jälgimisseadmetest teavitamine

Küsimuste 12 - 14 eesmärk oli välja selgitada, kas ja kuidas on tööandjad turvakaamerate olemasolust töötajaid teavitanud. Kirjalikult on teavitanud töötajaid kaamerate olemasolust ainult 12 (15%) ettevõtet. Töötajate teavitamist ei pea üldse vajalikuks 27 (33%) ettevõtet (valitud vastusevariandid “töötajaid ei teavitata turvakaamerate olemasolust, nad märkavad neid ise”, “töötajaid ei teavitata turvakaamerate olemasolust, see ei ole neile vajalik informatsioon” ja “muu”). Topelt vastuseid arvesse ei võetud, kontrolliti, mitu ettevõtet kokku neid kolme varianti valis. Ettevõtted, kes valisid vastuse variandiks “muu” täpsustasid seda järgnevalt: “Töötajad näevad ise turvakaameraid reaalajas” ja “Kaamerad on kõigile nähtavad”.

JÄLGIMISSEADMETEST TEAVITAMISE VIIS	N	% vastajatest
ettevõtte sissepääsude juures on turvakaamerate olemasolust teavitavad sildid	36	44%
ettevõtte siseterritooriumil on turvakaamerate olemasolust teavitavad sildid	22	27%
töötajaid teavitab turvakaamerate olemasolust suuliselt juht (nt personali juht vm juht)	44	54%
töötajaid teavitatakse kaudselt, s.t töötajal on võimalik info ise üles leida (nt infotahvel, siseveeb)	6	7%
töötajaid teavitatakse turvakaamerate olemasolust tööle asumisel kirjalikult (eraldi juhend, kirjaliku töölepingu osa või lisa vms)	12	15%
töötajaid ei teavitata turvakaamerate olemasolust, nad märkavad neid ise	23	28%
töötajaid ei teavitata turvakaamerate olemasolust, see ei ole neile vajalik informatsioon	3	4%
muu	2	2%

Tabel 7 Jälgimisseadmetest teavitamise viisid

Allikas: Autori koostatud

Kuigi küsimusele, kuidas teavitatakse töötajaid kaamerate olemasolust, vastas üksnes 12 ettevõtet, et töötajaid teavitatakse kirjalikult, siis küsimusele “Kui töötajaid teavitatakse turvakaamerate olemasolust kirjalikult, siis milline info sisaldub kirjalikus teavituses? (Vastake ainult siis, kui töötajaid on kirjalikult turvakaamerate olemasolust teavitatud)” vastas 14 ettevõtet. Mitte ühelgi ettevõttel ei olnud kirjalikus teavituses märgitud kõiki AKI poolt soovituslikus juhendis kirjas olevaid andmeid. Kõige rohkem infot oli kirjas ühel ettevõttes, kellel oli märgitud viis erinevat vastusevarianti, milleks olid turvakaamerate eesmärgid, olukordade ja protsesside kirjeldused, kuidas saadud andmeid kasutatakse, alade ja ruumide loetelu, kuhu kaamerad on suunatud, olukordade kirjeldused, millal turvakaamerate salvestisi võidakse edastada kolmandatele isikutele ja salvestiste säilitamise aeg.

JÄLGIMISSEADMETE KIRJALIKU TEAVITAMISE OSAD	N	% vastajatest (14 = 100%)
turvakaamerate eesmärk/eesmärgid	10	71%
olukordade ja protsesside kirjeldus, kuidas saadud andmeid kasutatakse	6	43%
alade ja ruumide loetelu, kuhu kaamera(d) on suunatud	7	50%
jälgimise aeg	3	21%
jälgimise liik (reaalajas või salvestamisega)	2	14%
turvakaamerate üldine kirjeldus (stационаarne, pööratav, suurendamisvõimalusega, koos helisalvestamisega jne)	2	14%
turvakaamerate salvestiste töötaja(te) nimed/ametikohad ja kontaktandmed	4	29%
olukordade kirjeldused, millal turvakaamerate salvestisi võidakse edastada kolmandatele isikutele	4	29%
kirjeldus meetmetest, millega tagatakse turvakaameratega kogutud salvestiste kaitsmine	0	0%
salvestiste säilitamise aeg	1	7%
salvestistega tutvumise kord	1	7%

Tabel 8 Jälgimisseadmete kirjaliku teavitamise osad

Allikas: Autori koostatud

Lisateavet töösuhte kestel ja/või turvakaamerae olemasolu üle on arutletud 7 (9%) ettevõttes. Täpsustavalt selgitati info jagamise kohta või viisi järgmiselt: “Koosolekul on teemat arutletud ja täpsustatud kõik põhjused”, “sisekorraeeskirjades”, “koosolekul”, “Räägime eesmärkidest, miks need on ettevõttes olemas”, “Räägitakse isikuga, kes kaameras pildile jäi ja mis valesti tehti”, “On tõstatud küsimus kaamerate vajalikkuse osas, kuid oleme need ära põhjendanud, sest ebaviisakaid

kliente on tõesti olnud arvestatavas koguses”, “Kui töötajatel on küsimus, miks või kellele on turvakaamera olemasolu vajalik vastatakse koheselt (otsene ülemus informeerib)”.

Küsimusele “Kas ettevõttes on esinenud olukordi, kus töötaja on avaldanud vastumeelsust kaamerate olemasolu üle?” vastas 14 (17%) ettevõtet, et töötajad on avaldanud vastumeelsust kaamerate olemasolu üle. Neist 10-l ettevõttel ei olnud välja töötatud kaebuste menetlemise korda. Ainult ühes ettevõttes, kus töötajad olid avaldanud vastumeelsust kaamerate olemasolu üle, oli töötajaid kaamerate kasutamisest kirjalikult teavitatud ja kahes ettevõttes on töösuhte kestel kaamerate kohta antud lisateavet. Ettevõtted, kus töötajad on avaldanud vastumeelsust kaamerate olemasolu üle, on töötajaid turvakaamerate olemasolust teavitatud minimaalselt või üldse mitte. Nimelt 7 (50%) ettevõtet vastas, et töötajaid on turvakaamerate olemasolust teavitanud üksnes siltidega sisse- ja väljapääsude juures ning 6 (43%) ettevõtet vastas, et töötajaid ei teavitata, sest nad märkavad neid ise.

4.4 Järeldused ja arutelu

Töö autor viis läbi uuringu Tallinna toitlustusettevõtete seas, et selgitada välja, millistel eesmärkidel on tööandjad turvakaamerad ettevõtetesse paigaldanud, millistel eesmärkidel neid kasutatakse, kas turvakaamerate kasutamine õiguspärane ning kas turvakaamerate kasutamisega rikutakse töötajate õiguseid. Töö tulemuste analüüsimisel selgus, et tööandjad ei ole kaamerate paigaldamisel lähtunud seaduslikest alustest ning AKI koostatud soovituslik juhend ei ole kasutust leidnud.

Antud uuringu tulemustes ei olnud suuri erinevusi ettevõtete vastustel tulenevalt ettevõtte suurusest, sellest, kas ettevõttel on eraldi personaliosakond või -töötaja ning ka sellest, kas tegemist on Eesti või välismaise päritolu ettevõttega.

4.4.1 Jälgimisseadmete paigaldamine ja kasutamine

Uurimuse tulemustes selgus, et ettevõtted ei ole kaamerate paigaldamist kasutanud n.ö viimase variandina. Seda tõendas see, et ainult 5 (6%) ettevõtetet kasutab ka muid võimalusi, et saavutada sama eesmärki, mida soovitakse turvakaamerate kasutamisega saavutada. Tööandjad tõid välja, et lisaks turvakaamerate kasutamisele on ettevõttes sama eesmärgi saavutamiseks tööl turvatöötajad, kasutatakse tööajaarvestuse seadet, suheldakse töötajatega ning rakendatakse elementaarseid tööohutuse nõudeid. Ciocchetti (2011) leiab, et arvestades sellega, et turvakaamerate näol on tegemist väga invasiivsete vahenditega, võiks neid kasutusele võtta üksnes siis kui muud vahendid ei aita sama

eesmärki täita ning eelkõige uurimise eesmärgil. Kajalo ja Lindblom (2015) on leidnud, et tööandjatel on suurem usaldus formaalse järelevalve meetodite efektiivsusesse kui mitteformaalsete. Tegevused, mis on seotud mitteformaalse järelevalve rakendamisega, näiteks töökultuuri ja töökeskkonna muutmine, ei ole kergesti kättesaadavad ja selle mõju võtab kauem aega ning vajab suuremat inimkapitali.

Autor leiab, et tööandjate vastused küsimusele, milliseid võimalusi kasutatakse lisaks turvakaameratele, et saavutada sama eesmärki, mida soovitakse turvakaamerate kasutamise saavutada tõendavad, et tööandjad leiavad, et turvakaamerate rakendamine on kõige lihtsam ja kiirem meetod eesmärgi saavutamiseks. Muid vahendeid ei kasutata põhjusel, et ei ole teadvustatud turvakaamerate kasutamise kaasna võivaid negatiivseid tagajärgi ning puuduvad teadmised mitteformaalsete meetodite rakendamiseks, nt parema töökultuuri loomine ettevõttes. Samuti ei ole kaalutud muid vähem invasiivseid vahendeid, et saavutada sama tulemust, mida turvakaameratega soovitakse saavutada.

IKS (2016) § 14 lg 3 kohaselt võib turvakaameraid kasutada üksnes isikute ja vara kaitseks. Ka töötajad ise peavad aktsepteeritavaks põhjuseks jälgimisseadmete paigaldamisel isikute ja vara kaitset (Ball, 2010; Stanton ja Weiss, 2000). Andmekaitseasutuste tööühm (2002: 22) on seisukohal, et distantsilt töötaja jälgimine tema töö kvaliteedi ja hulga kontrollimise eesmärgil ei ole lubatav. Ning Euroopa Andmekaitseinspektor (2010: p 5.9) on seisukohal, et eesmärgid nagu tootlikkuse juhtimine, kvaliteedi tagamine, ettevõtte poliitikate juurutamine või vaidluste puhuks tõendite kogumine, ei ole piisavad eesmärgid, et õigustada turvakaamerate kasutamist. 38 (46%) ettevõtet on turvakaamerad paigaldanud töötajate poolt toime pandud varguste avastamiseks, 34 (41%) tootlikkuse tõhustamiseks ja hindamiseks (nt töötaja optimaalne kasutamine, materjalide mõistlik kasutamine), (teenindus)kvaliteedikontroll. Nimetatud eesmärgid eeldavad töötajate töö tegemise pidevat jälgimist ning on seotud tööandjate usaldamatusega töötajate suhtes. Lisaks on tööandjad avatud küsimustes märkinud, et turvakaamera salvestisi on kasutatud töötajast kinnipidamise, tööle tuleku ja töölt mineku kellaaegade kontrollimiseks, samuti lõunapauside pikkuse ja toodete kasutamise hulga (nt kui palju kasutab kokk köögis toiduaineid) kontrollimiseks.

Ainult 16 (20%) ettevõtet vastas, et nad ei ole turvakaameraid kasutanud ega pole plaanis kasutada muudel põhjustel kui esialgselt planeeritud. IKS (2016) § 6 p 2 kohaselt võib isikuandmeid koguda üksnes määratletud ja õiguspäraste eesmärkide saavutamiseks ning neid ei või töödelda viisil, mis ei ole andmetöötuse eesmärkidega kooskõlas. Ülejäänud ettevõtted vastasid küsimustele, mis

eesmärkidel on kaamerad paigaldatud ja kas kaameraid on kasutatud ka muudel eesmärkidel kui esialgselt planeeritud üsna sarnaselt ehk planeeritud eesmärgid ja teisesed eesmärgid (olukorrad, mis on ette tulnud lisaks esialgselt määratud eesmärkidele) olid suures osas samad. Ball (2010) on leidnud, et negatiivseid tagajärgi (rahuololematus, vastutöötamine jms) toob kaasa see kui jälgimisseadmetega kogutud andmeid kasutatakse muudel eesmärkidel kui algselt planeeritud.

Autor leiab, et tööandjad ei ole mõistnud, et turvakaameraid võib paigaldada ja kasutada üksnes eesmärgipäraselt. Tööandjad on segamini ajanud turvakaamerate paigaldamise eesmärgid ja selle, milleks nad turvakaameraid realselt kasutavad. Põhjus võib peituda teadmatuses, aga ka selles, et tegelikkuses paigaldatakse turvakaamerad n.ö igaks juhuks. Toitlustussektoris on palju väikese suurusega ettevõtteid, kus puudub personalijuht või -osakond. Kuna personaliküsimustega tegeleb üldjuhul töötaja, kellel on ka muid ülesandeid (79%), siis puudub ettevõttes tõenäoliselt vastav pädevus. Teine põhjus turvakaamerate paigaldamiseks on tööandjate usaldamatus töötajate suhtes ja uskumus, et turvakaamerate abil on võimalik tõhustada töötajate töö tegemist ja vältida töötajate poolt toime pandud varguseid ja rikkumisi. Tööandjate vastused peegeldavad, et toitlustussektoris on väga palju kontrollile orienteeritud ettevõtteid, kes toimivad käsu-ja-kontrolli meetodil. Arvestades negatiivseid tagajärgi, mis võivad turvakaamerate ebaseadusliku paigaldamise ja kasutamise kaasneda (vähem efektiivne tööpanus (*counterproductive work behaviour*), (pisi)varguste toimepanek, passiivne tegevus, nagu näiteks sihilik töö valesti tegemine ja juhiste mittetäitmine (Fox et al., 2001; Martin et al., 2016)), võib järeldada, et toitlustussektoris on väga palju ettevõtteid, kus valitseb negatiivne töökeskkond, mittemotiveeritud töötajad, kes võivad ettevõttele lausa vastu töötada. Tööandjad omakorda proovivad tekkinud olukorda parandada kontrolli tõhustamisega ning töötajad vastavad sellele veel negatiivsemalt. Tegemist on lõpmatu negatiivse ringiga, kus lahenduse saab tuua üksnes tööandja olukorra teadvustamine ja uute juhtimisvõtete ja käitumiste rakendamine.

4.4.2 Jälgimisseadmetega kogutud info turvalisus

Kõik tööandjad säilitavad jälgimisseadmetega kogutud salvestisi turvaseaduses ettenähtud ajavahemiku jooksul ehk kuni ühe aasta jooksul. Üldjuhul rakendavad tööandjad siiski lühemat perioodi paarist nädalast paari kuuni.

41 (50%) ettevõtet on rakendanud ka andmete automaatset kustutamise süsteemi, mis on kõige turvalisem lahendus. Ligikaudu pooltes ettevõtetes (44%) on kindlaks määratud isik(ud), kes jälgimisseadmete abil kogutud salvestiste töötlemise eest vastutavad ning kõik ettevõtted olid

märkinud vähemalt ühe variandi, kuidas tagatakse turvakaamerate abil kogutud andmete turvalisus: 65% – andmed on kaitstud paroolidega, 35 % – salvestisi saab vaadata ainult ettevõtte serverist, 21% – salvestiste vaatamiseks on ettenähtud piiratud juurdepääsuga ruum, 78% – salvestistele on ligipääs piiratud isikute ringil, 55% – andmeid säilitatakse vaid teatud perioodi jooksul. Seega üldjoontes on tööandjad jälginud IKS (2016) § 6 p 6 sätestatud turvalisuse põhimõtet, mille kohaselt tuleb rakendada turvameetmeid, et kaitsta neid tahtmatu või volitamata töötlemise, avalikuks tuleku või hävimise eest. Kuna konkreetsed turvalisuse nõudeid ei ole välja seaduses toodud, siis peab tööandja ise otsustama, mis on parim viis tagamaks andmete turvalisust.

AKI (2011) on selgitanud, et turvakaamerate salvestisi võib säilitada üksnes mõistliku aja jooksul, mil see on vajalik püstitatud eesmärgi saavutamiseks. Eestis kehtivad õigusaktides ei ole määratlenud mõistliku aja kestust. Turvaseaduse kohaselt võib kogutud salvestisi säilitada kuni ühe aasta jooksul. Samas on turvaseadus üldseadus, mis ei arvesta töösuhete eripäraga. Kuna turvaseadus annab raamistiku turvakaamerate salvestiste säilitamiseks ja on n.ö tugevam kui AKI soovitus, siis ei saa antud küsimuses tulla ka kohtupraktikat, mis sisustaks mõistliku aja kestust. Kuigi tööandjad täidavad üldseadust, siis praktika on väga erinev. Salvestisi säilitatakse 24 tunnist kuni ühe aastani. Kuna antud küsimuses ei saa tulla ka vastavat kohtupraktikat, siis AKI soovitusest siinkohal ei ole kasu. Töötajatel ei ole võimalik õiguslikke vahendeid kasutades paluda tööandjal salvestis nt enne ühe aasta möödumist kustutada. Arvestades, et tööandjad ei ole toitlustussektoris kaameraid paigaldanud ja kasutanud üksnes seaduslikul alusel ja eesmärgipäraselt, siis antud juhul on siis väga suur riive oht töötaja privaatsusele.

4.4.3 Jälgimisseadmest teavitamine

IKS (2016) § 14 lg 3 kohaselt võib isikute või vara kaitse eesmärgil kasutada isikuandmeid salvestavat jälgimisseadmestikku ilma isiku nõusolekuta – andmesubjekti nõusolekut asendab sellise andmetöötluse korral jälgimisseadmestiku kasutamise fakti ning andmete töötleja nime ja kontaktandmete piisavalt selge teatavakstegemine. Seega sisuliselt on teavitamise nõue täidetud kui toitlustuskoha uksele on silt, et siin on kaamerad. Kokku vastas 50% ettevõtetest, et neil on ettevõtte sissepääsude juures või ettevõtte siseterritooriumil turvakaameratest teavitavad sildid. See tähendab, et pooled ettevõtted ei täida minimaalset nõuet teavitamisest. Juba 2010. aastal leidis AKI (2011) kaubandusettevõtteid kontrollides, et enamik tööandjaid ei olnud töötajaid valvekaamerate kasutamisest teavitanud. AKI leidis, et rikkumised tulenesid teadmatusest. Võrreldes 2010. aastaga, ei ole olukord paranenud.

Kirjalikku teavitamist töösisekorraeeskirjades, töölepingu osas vms kasutas üksnes 15% ettevõtetest ning mitte üheski ettevõttes ei olnud kasutusel täielikku AKI poolt väljatöötatud soovituslikku juhendit kaamerate teavitamise kohta. 10-l ettevõtetest olid kirjalikus teavituses üldiselt märgitud turvakaamerate kasutamise eesmärk ning mõnel üksikul ka muu info, nt kahel ettevõttel oli jälgimise liik kirjas, neljal turvakaamerate salvestiste töötajate nimed, ühel salvestamise aeg.

Teavitamine ja selgitamine jälgimisseadmete kasutamisel on üks olulisemaid viise, kuidas tööandja saab muuta töötajate suhtumist neisse ja seeläbi panusta tulemuslikumasse töösse. Aktsepteerimatu on töötajate seisukohalt salajane jälgimine (Allen et al., 2007). Lisaks ei saa eeldada, et töötajad oleksid alati kõigi seaduste ning tööandja poolt koostatud dokumentidega iseseisvalt kursis. Kui töötajad ei mõista jälgimisseadmete vajalikkust, siis võib see viia vähem efektiivse tööpanuseni (Workman, 2009b). Seetõttu tuleb töötajatele selgitada turvakaamerate kasutamise eesmärke ja protseduureegleid, sest siis on nad suurema tõenäosusega nõus selle rakendamisega ettevõttes ning nende hoiakud on jälgimisseadmete suhtes toetavamad (Hsu & Kuo, 2003). Lisaks on leitud, et sellel, kuidas tööandjad selgitavad, mis on jälgimisseadmete eesmärk, on väga oluline mõju sellele, kuidas töötajad neisse hiljem suhtuvad ja kuidas nad ise jälgimisseadmete olemasolu põhjendavad (Allen et al., 2007).

Autor leiab, et minimaalse teavitamiskohustuse tegemata jätmine viitab tööandjate teadmatusele. Võttes arvesse ka käesolevas uurimuses selgunud turvakaamerate paigaldamise eesmärgid ja olukorrad, mil kaameraid tegelikkuses kasutatakse, võib tegu olla mitte üksnes teadmatusena, vaid ka väheses suhtluses töötajatega üldiselt. Tööandjad soovivad töötajaid juhtida läbi käskude, mitte läbi arutelude ja koostöö. See on tõsine oht heale töökeskkonnale, töötajate vaimsele tervisele ja kokkuvõttes ka ettevõtte majanduslikele tulemustele.

Kuna puudub konkreetsete nõuetega eriseadus (või vastavad sätted TLSis või IKSis) turvakaamerate kohustusliku teavitamise, paigaldamise ja kasutamise osas ning AKI soovituslik juhend ei ole kasutust leidnud, siis leiab autor, et töötajatel on praktiliselt võimatu privaatsuse rikkumist esiteks tõendada ja teiseks nõuda tööandjalt rikkumise lõpetamist või isegi hüvitist rikkumise eest. Seda tõendavad ka TVK (2012, 2016) otsused, kus töötaja ja tööandjate selgitus olukorrast oli vastandlik. Töötaja tundis, et tema privaatsust on rikutud, tööandja selgitas, et tal on õigus kaameraid paigaldada vastavalt ettevõtte huvidele. Kuna mõlemal ettevõttel oli täidetud minimaalne teavitamise nõue – ettevõtte ustel olid kaamerate teavitavad sildid, siis leidis TVK, et privaatsust pole rikutud.

Samas ei tõenda kaamerateest teavitavad sildid ustel, et privaatsust pole rikutud. Sellega on täidetud üksnes seadusest tulenev minimaalne teavitamise nõue. Samas ei ole TVKI ühtegi seadusest tulenevat alust, et teha vastupidist otsust. Autor leiab, et see on turvakaamerate kasutamise kõige suurem vastuolu ja probleem. Tegu on väga invasiivsete vahenditega ja suure ohuga töötaja privaatsusele, kuid seadusest tulenev kaitse on minimaalne.

Lähtuvalt töö tulemustest teeb autor järgmise ettepaneku:

Reguleerida tööandja jälgimise ja kontrollimise õigused ja kohustused õiguaktide tasandil TLSis. Kuna tööandja on töösuhtes tugevam pool, siis ainuüksi AKI soovituslikust juhendist jääb väheks, mida tõendab see, et see pole rakendust leidnud. Töötajatel puudub õiguskindlus selles osas kui tööandja tungib liigselt töötaja privaatsfääri, ei ole konkreetseid sätteid, millele rikkumiste korral viidata. Hetkel puudub selge ja ühine arusaam, millal ja mis ulatuses tööandja võib töötajaid kontrollida. Ainuüksi viide privaatsuse austuse kohustusele TLSis ei taga töötajatele kindlust, et tööandja seda ei riku. Uus isikuandmete kaitse üldmääruse eelnõu annab liikmesriikidele volituse võtta vastu kooskõlas nimetatud määruse rakendumisega õigusakte reguleerimaks isikuandmete töötlemist töösuhetes. Mõistlik oleks koondada kõik konkeetselt töösuhteid puudutavad õigusaktid ühte seadusesse, mistõttu leiab töö autor, et TLSi, mis on nagoonii eriseadus töösuhetes, täiendamine annab nii töötajatele kui tööandjatele ülevaatlikuma regulatsiooni töösuhetes ühes kohas.

KOKKUVÕTE

Töökohtadel on järjest enam kasutusel erinevad tehnoloogilised vahendid igapäeva töö hõlbustamiseks. Kasutatakse erinevaid nutirakendusi nii klientikaartide kui klientide tagasiside tarbeks, samuti siseveebe ja sotsiaalmeedia gruppe, et operatiivselt olulisi uudiseid jagada, aga ka selleks, et tööd paremini korraldada. Töö tõhustamiseks on tööandjad kasutusele võtnud ka mitmeid monitoorimisevahendeid - kiipkaardid ja sõrmejäljelugerid, mille abil hoonesse ja/või erinevatesse ruumidesse siseneda; ülemaailmse asukoha määramise süsteemi, mille abil automaatselt pidada sõiduajaarvestust, aga ka kontrollida, kus töötaja on käinud; turvakaamerad nii isikute ja vara kaitseks kui ka töötajate töö tegemise kontrollimiseks jms. Kõigi nende vahendite kasutamisega käib alati kaasas oht privaatsusele ja isikuandmete väärkasutamiseks ning lekkimiseks.

Arvestades kõigi inimeste õigustatud ootust privaatsusele, siis ei saa seda unustada ka töökohtadel. Privaatsuse mitteastamine võib töökohal tuua kaasa negatiivseid tagajärgi. Seetõttu on tööandja jaoks oluline tagada töötajate heaolu, et oleks võimalik saavutada ettevõtte eesmärgid. Magistritöö eesmärk oli toitlustusettevõtete näitel välja selgitada, millistel eesmärkidel kasutavad tööandjad töökohal turvakaameraid, kas nende kasutamine on õiguspärane ning kas turvakaamerate kasutamisega rikutakse töötajate õiguseid.

Erinevad uurimused on välja toonud mitmeid olulisi nüansse, mida tööandjad turvakaamerate paigaldamisel silmas peaksid pidama. Turvakaameraid võib töökohal kasutada isikute ja vara kaitseks. Seejuures peab austama töötaja privaatsust. Kui töötajate jälgimine tehnoloogiliste vahendite abil ületab mõistlikkuse ja vajalikkuse piirid ning sekkub liigselt töötaja privaatsfääri, siis tekivad töötajate ja tööandjate vahel erimeelsuses ja süvened usaldamatus (Ball, 2010; Allen, Coopman, Hart & Walker, 2007). Mida madalam on töökohal privaatsuse tase (sh teiste töötajate sekkumine töösse, turvakaamerate abil töö tegemise jälgimine), seda enam kogevad töötajad emotsionaalset kurnatust ehk läbipõlemist (Laurence, Fried & Slowik, 2013). Privaatsuse säilitamise võimalus töökohal on üheks eelduseks usalduslike suhete tekkimisele töötaja ja tööandja vahel (Chang, Liu & Lin, 2015). Jälgimisseadmete töökohale paigaldamine võib õhnestada töötaja ja tööandja vahelist usaldust (Stanton & Weiss, 2003; Kramer, 1999; Holland, Cooper & Hecker, 2015). Töötajad on selgitanud, et pidev kontrollimine ja tööandjapoolne jälgimine tekitab neis tunde nagu neid justkui ei usaldataks (Stanton & Weiss, 2003). Selline usalduse langus tööandja suhtes tekitab töötajates trotsi, vähendab töötajate motivatsiooni pühenduda ettevõttele (Kramer, 1999) ning tagajärjeks on vähem efektiivne tööpanus (*counterproductive work behaviour*), mille ilmingud

töökohal on muuhulgas (pisi)varguste toimepanek, passiivne tegevus, nagu näiteks sihilik töö valesti tegemine ja juhiste mittetäitmine (Fox, Spector & Miles, 2001; Martin, Wellen & Grimmer, 2016). Lõpptulemuseks võib olla halvasti toimiv ja majanduslikult ebaefektiivne ettevõtte (Holland et al., 2015: 169). Kui töötajaid jälgimisseadmete kasutamisest teavitada, siis on nad suurema tõenäosusega nõus selle rakendamisega ettevõttes ning nende hoiakud on jälgimisseadmete suhtes toetavamad (Hsu & Kuo, 2003).

Isikuandmete kaitse seaduse (IKS) kohaselt on jälgimisseadmete paigaldamine ka kasutamine lubatud üksnes isikute ja vara kaitseks. Muuhulgas peab nende kasutamine olema eesmärgipärane ja minimaalne. See tähendab seda, et turvakaameraid ei või kasutada muul eesmärgil kui see algselt mõeldud oli ning nende vaatevälja ei tohi ülemääraselt jääda töötajad.

Empiiriline uurimus viidi läbi kvantitatiivset uurimismeetodit kasutades. Andmekogumismeetodiks kasutati veebiküsitlust struktureeritud küsimustega. Uurimus viidi läbi Tallinna toitlustusettevõtete seas. Küsitlus saadeti 315 Tallinna toitlustusettevõttele. Küsitlusele vastas korrektselt 118 Tallinna toitlustusettevõtet, mis on 34,29% valimist.

Töö tulemuste analüüsimisel selgus, et tööandjad ei ole kaamerate paigaldamisel lähtunud seaduslikest alustest, sh eesmärgipärasuse ja minimaalsuse põhimõtete silmas pidades ning andmekaitse inspeksiooni koostatud soovituslik juhend ei ole kasutust leidnud. Lisaks isikute ja vara kaitseks kasutati turvakaameraid ka töötajate töö tegemise järgimiseks. Euroopa andmekaitseasutuste töörihm on seisukohal, et distantsilt töötaja jälgimine tema töö kvaliteedi ja hulga kontrollimise eesmärgil ei ole lubatav. Selgus, et ettevõtted ei ole kaamerate paigaldamist kasutanud n.ö viimase variandina. Seda tõendas see, et ainult 5 (6%) ettevõtet kasutab ka muid võimalusi, et saavutada sama eesmärki, mida soovitakse turvakaamerate kasutamisega saavutada. Ciocchetti (2011) kohaselt võiks turvakaamerad kasutusele võtta üksnes siis kui muud vahendid ei aita sama eesmärki täita.

Ainult 16 (20%) ettevõtet vastas, et nad ei ole turvakaameraid kasutanud ega pole plaanis kasutada muudel põhjustel kui esialgselt planeeritud. Ball (2010) on leidnud, et negatiivseid tagajärgi (rahuololematust, vastutöötamine jms) toob kaasa see kui jälgimisseadmetega kogutud andmeid kasutatakse muudel eesmärkidel kui algselt planeeritud.

50% ettevõtetest ei täida minimaalset turvakaameratest teavitamise nõuet teavitamisest. Kirjalikku teavitamist kasutaks üksnes 15% ettevõtetest ning mitte üheski ettevõttes ei olnud kasutusel täielikku

AKI poolt väljatöötatud soovituslikku juhendit kaamerate teavitamise kohta. Turvakaamerate kasutamisest tuleb töötajaid teavitada, siis on nende hoiakud on jälgimisseadmete suhtes toetavamad (Hsu & Kuo, 2003).

Autor teeb lähtuvalt töö tulemustest reguleerida tööandja jälgimise ja kontrollimise õigused ja kohustused õiguaktide tasandil töölepingu seaduses. Kuna tööandja on töösuhtes tugevam pool, siis ainuüksi AKI soovituslikust juhendist jääb väheks ning puudub selge, ühine arusaam ja praktika, millal ja mis ulatuses tööandja võib töötajaid kontrollida. Ainuüksi viide privaatsuse austuse kohustusele TLSis ei taga töötajatele kindlust, et tööandja seda ei riku.

RESUME

Different technological tools are being used increasingly at workplaces to ease the daily work. Various smart applications are used for loyalty cards and feedback from customers, in addition internal websites and social media groups are used to promptly share important news, but also to arrange work better. To improve work efficiency the employers have adopted several monitoring devices: smart cards and fingerprint scanners for entering buildings and/or different rooms, global positioning system for automatic record keeping of vehicle driving time and to check where the employee has been, security cameras for protection of personnel and property and to check the working of employees, etc. Usage of all these devices is always accompanied by the danger to privacy and misuse and leaking of personal data.

Taking into account the reasonable expectation of all people to privacy, this also cannot be forgotten at the workplaces. Disrespecting privacy may have negative consequences at the workplace. To be able to reach the goals of the enterprise, it is therefore important for the employer to ensure the well-being of employees. The objective of the master thesis was to find out by the example of catering establishments for what purposes do employers use security cameras at the workplace, is using the cameras lawful, and are the employees' rights being violated by using security cameras.

Different researches have indicated several important nuances that the employers should take into consideration when installing security cameras. Security cameras may be used at the workplace for the protection of personnel and property. In doing so the privacy of the employer must still be respected. When monitoring the employees by technological means exceeds the limits of reason and necessity and intervenes excessively the private sphere of the employee, dissensions will emerge and distrust will deepen between the employers and employees (Ball, 2010; Allen, Coopman, Hart & Walker, 2007). The lower the level of privacy at workplace (including other employees intervening work, monitoring the working with security cameras), the more the employers experience emotional or burnout (Laurence, Fried & Slowik, 2013). The possibility to retain privacy at workplace is one of the prerequisites for the emerging of trustworthy relationships between the employee and employer (Chang, Liu & Lin, 2015). Installation of surveillance equipment to the workplace may undermine trust between the employee and employer (Stanton & Weiss, 2003; Kramer, 1999; Holland, Cooper & Hecker, 2015). The employees have explained that constant control and monitoring by the employer makes them feel as they are not being trusted (Stanton & Weiss, 2003). Such a drop in confidence towards the employer creates defiance among employees, reduces the employees'

motivation to dedicate to the company (Kramer, 1999) and the result is counterproductive work behaviour. It is manifested at work, among other things, as committing (small) thefts and passive activity, such as deliberately doing the work incorrectly and not following instructions (Fox, Spector & Miles, 2001; Martin, Wellen & Grimmer, 2016). The end result may be a poorly performing and economically inefficient company (Holland et al., 2015: 169). When the employees are notified about the usage of surveillance equipment, they are more likely to agree with it being used in the company and their attitudes towards the surveillance equipment are more supportive (Hsu & Kuo, 2003).

According to Estonian Personal Data Protection Act (PDPA) installing surveillance equipment is allowed only for the protection of personnel and property. Among other things the usage of such equipment must be purposeful and minimal. This means that security cameras may not be used for any other purpose than it was initially intended and there may not be an excessive number of employees within their field of view.

The empirical research was carried out using a quantitative research method. A web questionnaire containing structured questions was used as the method of data collection. The research was conducted among Tallinn's catering establishments. The questionnaire was sent to 315 catering establishments in Tallinn. 118 Tallinn's catering establishments replied correctly, which is 34.29% of the sample.

After analysing the results of the research, it was revealed that the employers have not based the installation of cameras on legal principles, including taking into account the principles of purposefulness and minimality, and the recommended guidelines composed by the Estonian Data Protection Inspectorate have not been used. In addition to protecting personnel and property the security cameras were being used to monitor employees doing work. The European Data Protection Working Party of the data protection authorities considers that monitoring the working of an employee from distance about the quality and quantity of his/her work is not permitted. It was revealed that the establishments have not used installing the cameras as "the last possible measure". This was evidenced by the fact that only 5 (6%) establishments are using other means to achieve the same objective that can be reached by using security cameras. According to Ciocchetti (2011) the security cameras could be used only when other means are not helping to fulfill the same purpose.

Only 16 (20%) establishments replied that they have not used security cameras and are not planning to use them for other purposes than previously planned. Ball (2010) has found that negative

consequences (dissatisfaction, counter-working, etc.) will be following when the data collected with surveillance equipment is used for other purposes than originally intended.

50% of the establishments do not meet the minimum requirement of notifying about the security cameras. Notification in writing was used only by 15% of the establishments and none of the enterprises had used the full recommended guidelines by the Estonian Data Protection Inspectorate of notifying about the cameras. Employees must be notified about the usage of security cameras, then their attitudes towards the surveillance equipment are more supportive (Hsu & Kuo, 2003).

Based on the results obtained by the research, the author proposes to regulate the rights and obligations of the employer for surveillance and control at legislative level in the Estonian Employment Contracts Act. Since the employer is the stronger partner in an employment relationship, the recommended guidelines of Estonian Data Protection Inspectorate are not sufficient enough, and there is no uniform understanding and practice about when and to what extent the employer may check over the employees. Only a reference to the obligation of respecting privacy in the Estonian Employment Contracts Act does not assure to the employees that the employer is not violating it.

VIIDATUD KIRJANDUS

- Agarwal, U.A. (2014). Linking justice, trust and innovative work behaviour to work engagement. *Personnel Review*, 44:1, 41-73.
- Agustina, J.R., Coudert, F. (2013). Limits and challenges of the expanding use of covert CCTV in the workplace in Spain – beyond jurisprudential analysis. *Innovation: The European Journal of Social Science Research*, 26:1-2, 145-160.
- Alder, G.S. (2001). Employee reactions to electronic performance monitoring: A consequence of organizational culture. *Journal of High Technology Management Research*, 12:2, 323-342.
- Allen, M.W., Coopman, S.J., Hart, J.L., Walker, K.L. (2007). Workplace Surveillance and Managing Privacy Boundaries. *Management, Communication Quarterly*, 21:2, 172-200.
- Alstete, J. (2006). Inside advice on educating managers for preventing employee theft. *International Journal of Retail & Distribution Management*, 34:11, 833-844.
- Andmekaitse Inspektsioon. (2011). *Avaliku teabe seaduse ja isikuandmete kaitse seaduse täitmisest aastal 2010. Soovitused aastaks 2011.*
- Andmekaitse Inspektsioon. (2012). *Avaliku teabe seaduse ja isikuandmete kaitse seaduse täitmisest aastal 2011. Soovitused aastaks 2012.*
- Andmekaitse Inspektsioon. (2013a). *Avaliku teabe seaduse ja isikuandmete kaitse seaduse täitmisest aastal 2012. Soovitused aastaks 2013.*
- Andmekaitse Inspektsioon. (2013b). *Isikuandmete töötlemine töösuhetes. Abistav juhendmaterjal.* Tallinn. Kasutatud: 01.03.2017
http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikuandmed%20t%C3%B6%20suhetes%20juhendmaterjal26%2005%202014_0.pdf
- Andmekaitse Inspektsioon. (2014). *Avaliku teabe seaduse ja isikuandmete kaitse seaduse täitmisest aastal 2013. Soovitused aastaks 2014.*
- Andmekaitse Inspektsioon. (2015). *Avaliku teabe seaduse ja isikuandmete kaitse seaduse täitmisest aastal 2014. Soovitused aastaks 2015.*
- Andmekaitse Inspektsioon. (2016). *Avaliku teabe seaduse ja isikuandmete kaitse seaduse täitmisest aastal 2015. Soovitused aastaks 2016.*
- Ball, K. (2010). Workplace surveillance: an overview. *Labor History*, 51:1, 87-106.
- Ball, K., Daniel, E.D., Stride, C. (2012). Dimensions of employee privacy: an empirical study. *Information Technology & People*, 25:4, 376 - 394.
- Bentham, J. (1995). *The panopticon writings*. London; New York: Verso.
- Bloomberg BNA *kodulehekülg*, Kasutatud 11.04.2017 <https://www.bna.com/donald-aplin-m17179894428/>

- Chang, S.E., Liu, A.Y., Lin, S. (2015). Exploring privacy and trust for employee monitoring. *Industrial Management & Data Systems*, 115:1, 88 - 106.
- Chen, J.V., Park, Y. (2005). The role of control and other factors in the electronic surveillance workplace. *Journal of Information, Communication and Ethics in Society*, 3:2, 79-91.
- Ciocchetti, C.A. (2011). The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring. *American Business Law Journal*, 48:2, 285–369.
- Dowding, M.R. (2011). *Privacy: Defending an Illusion*. Plymouth: Scarecrow Press.
- D’Urso, S.C. (2006). Who’s Watching Us at Work? Toward a Structural–Perceptual Model of Electronic Monitoring and Surveillance in Organizations. *Communication Theory*, 16:3, 281-303.
- Eddy, E.R., Stone, D.L., Stone-Romero, E.F. (1999). The effects of information management policies on reactions to human resource information systems: an integration of privacy and procedural justice perspectives. *Personnel Psychology*, 52:2, 335-358.
- Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. 3. väljaanne.* (2012). Tallinn: Juura.
- Euroopa Andmekaitseasutuste töörühm (ingl *Article 29 Data Protection Working Party*). (2001). *Opinion 8/2001 on the processing of personal data in the employment context*. Kasutatud 12.04.2017 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf
- Euroopa Andmekaitseasutuste töörühm (ingl *Article 29 Data Protection Working Party*). (2002). *Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance*. Kasutatud 12.04.2017 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2004/wp89_en.pdf
- Euroopa Andmekaitseinspektor (ingl *European Data Protection Supervisor*). (2010). *Video-surveillance Guidelines*, Kasutatud 12.04.2017 https://edps.europa.eu/sites/edp/files/publication/10-03-17_video-surveillance_guidelines_en.pdf
- Euroopa Komisjon. (2017). *Komisjoni teatis Euroopa Parlamendile ja Nõukogule. Isikuandmete vahetamine ja kaitsmine globaliseerunud maailmas*. Brüssel.
- Euroopa Liidu Põhiõiguste Amet. (2015). *Euroopa Andmekaitseõiguse käsiraamat*. Luxembourg: Euroopa Liidu Väljaannete Talitus.
- Euroopa Nõukogu Ministrite Komitee. (1989). *Soovitus nr R (89) 2 Liikmesriikidele tööhõiveotstarbel kasutatavate isikuandmete kaitse kohta*. Kasutatud 01.05.2017 <https://rm.coe.int/16804b8868>
- Fink, U. (2014). Protection of privacy in the EU, individual rights and legal instruments. N. Witzleb, D. Lindsay, M. Paterson, S. Rodrick (Toim), *Emerging Challenges in Privacy Law* (lk 75-91). United Kingdom: Cambridge University press.

- Fox, S., Spector, P.E., Miles, D. (2001). Counterproductive Work Behavior (CWB) in Response to Job Stressors and Organizational Justice: Some Mediator and Moderator Tests for Autonomy and Emotions. *Journal of Vocational Behavior*, 59:3, 291-309.
- Geller, T. (2016). In Privacy Law, It's the U.S. vs. the World. *Communications of the ACM*, 59:2, 21-23.
- Holland, P.J., Cooper, B., Hecker, R. (2015). Electronic monitoring and surveillance in the workplace: The effects on trust in management, and the moderating role of occupational type. *Personnel Review*, 44:1, 161 - 175.
- Holvast, J. (2008). *History of Privacy*. Berlin: Springer Heidelberg.
- Hon, A.H.Y., Lu, L. (2010). The mediating role of trust between expatriate procedural justice and employee outcomes in Chinese hotel industry. *International Journal of Hospitality Management*, 29:4, 669-676.
- Hsu, M.H., Kuo, F.Y. (2003). An investigation of volitional control in information ethics. *Behaviour & Information Technology*, 22:1, 53-62.
- Jensen, J.M., Raver, J.L. (2012). When self-management and surveillance collide: consequences for employees' organizational citizenship and counterproductive work behaviors. *Group and Organizational Management*, 37:3, 308-346.
- Kajalo, S., Lindblom, A. (2015). Creating a safe and pleasant shopping environment: a retailer's view. *Property Management*, 33:3, 275 - 286.
- Kramer, R. M. (1999). Trust and distrust in organizations: emerging perspectives, enduring questions. *Annual Review of Psychology*, 50, 569–598.
- Laurence, G.A., Fried, Y., Slowik, L.H. (2013). "My space": a moderated mediation model of the effect of architectural and experienced privacy and workspace personalization on emotional exhaustion at work. *Journal of Environmental Psychology*, 36, 144-152.
- Levin, A., Foster, M., Nicholson, M.J., Hernandez, T. (2006). Under the Radar? The Employer Perspective on Workplace Privacy. Office of the Privacy Commissioner. Toronto: Ryerson Centre for the Study of Commercial Activity. Canada.
- Liivrand, S., Balode, A. ja Šinkúniené, D. (2013). *Balti andmekaitsjed viisid läbi ühisjärelvalve Radisson Blu hotellides*. Kasutatud 10.04.2017 <http://www.aki.ee/et/news/balti-andmekaitsjed-viisid-labi-uhisjarelevalve-radisson-blu-hotellides>
- Liivoja, M. (2015). *Andmekaitse asjatundjad arutasid Euroopa Liidu andmekaitsereformiga seotud küsimusi*. Kasutatud 11.05.2017 <http://www.aki.ee/et/uudised/pressiteated/andmekaitse-asjatundjad-arutasid-euroopa-liidu-andmekaitsereformiga-seotud>
- Lyon, D. (2007). *Surveillance Studies: An Overview*. Cambridge: Polity Press.

- Martin, A.J., Wellen, J.M., Grimmer, M.R. (2016). An eye on your work: How empowerment affects the relationship between electronic surveillance and counterproductive work behaviours. *The International Journal of Human Resource Management*, 27:21, 2635-2651.
- Maruste, R. (2004). *Konstitutsionalism ning põhiõiguste ja -vabaduste kaitse*. Tallinn: Juura.
- Mason, D., Button, G., Lankshear, G., Coates, S., Sharrock, W. (2002). On the poverty of apriorism: Technology, surveillance in the workplace and employee responses. *Information, Communication & Society*, 5:4, 555-572.
- Miller, C., Wells, F.S. (2007). Balancing Security and Privacy in the Digital Workplace. *Journal of Change Management*, 7:3-4, 315-328.
- Mitrou, L., Karyda, M. (2006). Employees' privacy vs employers' security: can they be balanced? *Telematics and Informatics*, 23:3, 164-178.
- Männiko, M. (2011). *Õigus privaatsusele ja andmekaitse*. Tallinn: Juura.
- Peeterson, M. (2012). *Töötaja privaatsusõigus ja selle piiramine töösuhtes*. Magistritöö. Tartu Ülikool, õigusteaduskond.
- Pilving, I. (2005). Õigus isikuandmete kaitsele. *Juridica*, 7, 532-536.
- Sewell, G., Barker, J.R., Nyberg, D. (2012). Working under intensive surveillance: When does 'measuring everything that moves' become intolerable? *Human relations*, 65:2, 189-215.
- Sits, H. (2014). *Isikuandmete kaitse töösuhte vältel jälgimiseadmete kasutamisel*. Magistritöö. Tallinna Ülikool, õigusakadeemia.
- Slaviček, D. (2012). Surveillance at the workplace. *Central European Business Review*, 1:3, 55-56.
- Stalla-Bourdillon, S., Phillips, J., Ryan, M.D. (2014). *Privacy vs. Security*. London: Springer.
- Stanton, J.M., Weiss, E.M. (2000). Electronic monitoring in their own words: an exploratory study of employees' experiences with new types of surveillance. *Computers in Human Behavior*, 16:4, 423-440.
- Stanton, J.M., Weiss, E.M. (2003). Organisational databases of personnel information: contrasting the concerns of human resource managers and employees. *Behaviour & Information Technology*, 22:5, 291-304.
- Statistikaameti kodulehekül*, Kasutatud 15.03.2017 <http://pub.stat.ee/px-web.2001/dialog/statfile2.asp>
- Thomas, T., Stoddard, D. (2004). *Network Security First-Step*. Indianapolis: Cisco Press.
- Umphress, E.E., Labianca, G., Brass, D.J., Kass, E., Scholten, L. (2003). The role of instrumental and expressive social ties in employees' perceptions of organizational justice. *Organization Science*, 14, 738-53.

van Dijke, M., Verboon, P. (2010). Trust in authorities as a boundary condition to procedural fairness effects on tax compliance. *Journal of Economic Psychology*, 31:1, 80-91.

Veterinaar- ja Toiduameti kodulehekül, Kasutatud 15.03.2017
<https://jvis.agri.ee/jvis/avalik.html#/toitKaitlemisettevotedparing>

Workman, M. (2009a). How perceptions of justice affect security attitudes: suggestions for practitioners and researchers. *Information Management & Computer Security*, 17:4, 341-353.

Workman, M. (2009b). A field study of corporate employee monitoring: Attitudes, absenteeism, and the moderating influences of procedural justice perceptions. *Information and Organization*, 19:4, 218–232.

EESTI ÕIGUSAKTID

Isikuandmete kaitse seadus (RT I, 06.01.2016, 10) § 4 lõige 1, § 6 punktid 1 - 7, § 10 lõige 1, § 12 lõiked 1 - 2, 4, 7 - 8, § 14 lõige 1 punkt 4, § 14 lõige 2 punkt 2, § 14 lõige 3, § 15, § 19, § 24 lõige 1.

Põhiseadus (RT I, 15.05.2015, 2) § 18, § 19 lõige 1, § 26, § 33.

Turvaseadus (RT I, 30.12.2015, 54) § 11 lõiked 3-4.

Töölepingu seadus (RT I, 28.04.2017, 2) § 28 lõige 2 punkt 11.

EUROOPA LIIDU ÕIGUSAKTID

Euroopa Liidu põhiõiguste harta (ELT C 326/391, 26.10.2012) artikkel 7, artikkel 8 lõiked 1 - 2.

Euroopa Parlamendi ja Nõukogu direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (ELT L 284, 31.10.2003) punkt 28, artikkel 2, artikkel 7 punkt b, artikkel 6 lõige 1 punkt b, artikkel 17.

Inimõiguste ja põhivabaduste kaitse konventsioon (RT II 2010, 14, 54) artikkel 8 lõiked 1 - 2.

EESTI TÖÖVAIDLUSKOMISJONIDE LAHENDID JA RIIGIKOHTU KOHTULAHENDID

RKTKo 13.01.2010, 3-2-1-152-09, p 11

TVKo 22.02.2012, 4.1-2/128-2012

TVKo 04.02.2016, 4-1/2633

EUROOPA INIMÕIGUSTE KOHTU KOHTULAHENDID

EIKo 16.12.1992, 13710/88, Niemietz vs. Saksamaa.

EIKo 16.02.2000, 27798/95, Amann vs. Šveits.

EIKo 05.10.2010, 420/07, Köpke vs Saksamaa

LISA 1

TÖÖVAIDLUSKOMISJONIDE LAHENDID OTSINGUSÕNAGA SISUS “KAAMERA” JA
“TURVAKAAMERA” NUMBRITE JA AASTATE JÄRGI

	2016	2015	2014	2013	2012	2011
Transport	4-1/2549/16 bussijuht	4-1/76 bussijuht	4-1/307 laadija		4.4-2/1640 dokker	
KOKKU: 6	4-1/1457/16 bussijuht				4.3-2/528 bussijuht	
Tootmine	4-1/1629/16 metallitööline	4-1/1654 elektrimasinate mähkija	4-1/899 pingioperaator- tõstukijuht	4.3-1/1902 tõsteseadmete operaator	4.4-2/2340 tootmisjuht	4.4-2/1633 abitööline
KOKKU: 14	4-1/1525/16 klaasisulataja	4-1/1297 keevitaja			4.3-2/2259 käsielekter- keevitaja	
		4-1/551 puurpingi operaator			4.1-2/2132 tootmistööline	
		4-1/1436 lukksepp			4.1-2/128 plasma pingi operaator	
		4-1/1419 lukksepp				
Kaubandus	4-1/957/16 poemüüja	4-1/2633 klienditeenindaja	4-1/310 poemüüja	4.3-1/2970 müüja	4.4-2/835 kaupluse juhataja	4.3-2/2172 lemmiklooma- toidu pakkija
KOKKU: 12		4-1/2611 klienditeenindaja		4.2-1/2624 müügiesinduse juht		4.3-2/1946 poemüüja
		4-1/2583 müügikonsultant				
		4-1/2549 poemüüja				
		4-1/2403 poemüüja				
Toitlustus ja teenindus		4-1/1508 kokk	4-1/1980 klienditeenindaja		4.3-2/1840 administraator kasiinos	4.4-2/2239 klienditeenin- daja kasiinos
KOKKU: 8		4-1/1223 klienditeenindaja kardirajal	4-1/1071 klienditeenindaja			
		4-1/1644 toitlustuse abitööline	4-1/453 hasartmängu- diiler			
Puhastus- teenindus	4-1/160/16 puhastus- teenindaja					
KOKKU: 1						

KÕIK KOKKU: 41					
-----------------------	--	--	--	--	--

Allikas: autori koostatud

LISA 2

ETTEVÕTETELE VASTAMISEKS SAADETUD KÜSIMUSTIK

Hea vastaja!

Olen Tallinna Tehnikaülikooli tööstuspsühholoogia instituudi personalitöö ja -arenduse magistrant Kaire Saarep ja uurin oma magistritöös, kuidas on ettevõtetes reguleeritud turvakaamerate kasutamine.

Palun Teil leida kuni 10 minutit küsimustikule vastamiseks. Küsimustele palun ettevõtte nimel vastata personalijuhil või isikul, kes on vastutav (või seotud) isikuandmete töötlemise eest. Andmeid kogutakse anonüümselt, neid kasutatakse ainult magistriuurimuse teostamiseks ja üldistatud kujul.

Kui Teil tekib lisaküsimusi või kui soovite saada infot uuringu tulemuste kohta, siis palun kirjutage aadressil saarep@gmail.com või helistage numbril +372 5815 1561.

Vastuseid ootan hiljemalt 28. aprilliks.

Suur tänu abi eest!

Kaire Saarep

Üldised andmed

Mitu töötajat on Teie ettevõttes?

- a) vähem kui 10
- b) 10–49
- c) 50–249
- d) 250 ja enam

Kas ettevõttes on personaliosakond?

- a) jah
- b) ei, aga on personalijuht
- c) ei, personaliküsimustega tegeleb üks töötaja, kellel on ka muid ülesandeid (nt ettevõtte juht, raamatupidaja vms)

Ettevõtte on:

- a) Eesti ettevõtte
- b) seotud välismaa ettevõttega (nt tütarfirma, frantsiis vms)

Küsimustik

Kui on mitu sobivat vastusevarianti, siis palun märkige kõik sobivad.

1. Kas Teie ettevõtte territooriumile on paigaldatud turvakaamerad?

- jah ei

2. Mitu turvakaamerat on Teie ettevõtte territooriumile paigaldatud?

- 1-4
 5-14
 15-24
 25 ja enam

3. Millistele aladele ja/või ruumidele on turvakaamerad ettevõtte territooriumil suunatud?

- ettevõtte välialad (nt parkla)
 sisse- ja väljapääsud
 klientide ala
 töötsoon, kaamera suunatud inventarile
 töötsoon, kaamera suunatud nii inventarile kui ka töötajatele
 töötajate puhkeruum
 töötajate rietusruum
 tualett ja pesemisruum

4. Millistel põhjustel on ettevõttesse paigaldatud turvakaamerad?

- töötajate ohutus ja turvalisus (tagab töötajatele turvatunde agressiivsete klientide ja võimalike rünnakute, nt varguste korral)
 töötajate kaitse (kaitseb töötajaid isiklike asjade varguste eest, tagab tõendid klientide/kaastöötajate valesüüdistuste, ähvarduste ja ahistamise korral)
 aitab tagada positiivse ja kiusamisvaba töökeskkonna (nt ennetab seksuaalset ahistamist)
 klientide ohutus ja turvalisus

- hoiab töötajad ausad (ennetab töötajate poolt toime pandavaid varguseid, kindlustab, et töötajad järgivad ettevõtte eeskirju ja kasutavad ettevõtte vara üksnes selleks ettenähtud põhjustel)
- töötajate toime pandud varguste avastamine
- tööandja vara kaitse (ennetab klientide toime pandud varguseid)
- tootlikkuse tõhustamine ja hindamine (nt tööaja optimaalne kasutamine, materjalide mõistlik kasutamine), (teenindus)kvaliteedikontroll
- aitab tagada tõendid õiguslike vaidluste korral (nt töövaidluskomisjonis, kohtus, politseis)
- on abivahend juhtidele võtmaks vastu otsuseid

5. Kas olete ettevõttes kasutanud ka teisi lahendusi, et saavutada sama eesmärki, mida turvakaamerate kasutamisega saavutatakse? Palun täpsustage.

- jah,
- ei

6. Märkige, mis põhjustel on kaamerate kasutamine veel kasulikuks osutunud.

- töötajate ohutus ja turvalisus (tagab töötajatele turvatunde agressiivsete klientide ja võimalike rünnakute, nt varguste korral)
- töötajate kaitse (kaitseb töötajaid isiklike asjade varguste eest, tagab tõendid klientide/kaastöötajate valesüüdistuste, ähvarduste ja ahistamise korral)
- aitab tagada positiivse ja kiusamisvaba töökeskkonna (nt ennetab seksuaalset ahistamist)
- klientide ohutus ja turvalisus
- hoiab töötajad ausad (ennetab töötajate poolt toime pandavaid varguseid, kindlustab, et töötajad järgivad ettevõtte eeskirju ja kasutavad ettevõtte vara üksnes selleks ettenähtud põhjustel)
- töötajate toime pandud varguste avastamine
- tööandja vara kaitse (ennetab klientide toime pandud varguseid)
- tootlikkuse tõhustamine ja hindamine (nt tööaja optimaalne kasutamine, materjalide mõistlik kasutamine), (teenindus)kvaliteedikontroll
- aitab tagada tõendid õiguslike vaidluste korral (nt töövaidluskomisjonis, kohtus, politseis)
- on abivahend juhtidele võtmaks vastu otsuseid
- ei ole kasutatud/ei ole plaanis kasutada muudel põhjustel kui esialgu planeeritud

7. Kas ettevõttes on esinenud olukordi, kus turvakaamera salvestisi on olnud vaidluste/erimeelsuste/rikkumiste vms lahendamiseks/tõendamiseks tarvis kasutada? Palun täpsustage, millistes olukordades on neid kasutatud.

jah,

ei

8. Kui kaua säilitatakse turvakaamerate salvestisi? Valige üks vastus.

jälgimine toimub üksnes reaalajas, salvestisi ei säilitata

vajaduse järgi, säilitamise aeg ei ole kindlaks määratud. Palun märkige järgmise küsimuse vastuseks perioodi pikkus, millal üldjuhul salvestised kustutatakse

kindlaks on määratud periood, salvestised kustutatakse manuaalselt. Palun märkige järgmise küsimuse vastuseks perioodi pikkus.

kindlaks on määratud periood, salvestised kustuvad automaatselt. Palun märkige järgmise küsimuse vastuseks perioodi pikkus.

9. Kui valisite 8. küsimuse vastuseks 2.-4. variandi, siis palun märkige perioodi pikkus.

.....

10. Kas Teie ettevõttes on kindlaks määratud töötaja(d)/ametikoht(t/ad), kes turvakaamerate salvestiste töötlemise eest vastuta(b/vad)? Kui jah, siis palun märkige ametikoht.

jah,

ei

11. Kuidas on tagatud turvakaamerate abil kogutud andmete kaitsmine?

salvestised on kaitstud paroolidega

salvestisi saab vaadata ainult ettevõtte serverist

salvestiste vaatamiseks on ette nähtud piiratud juurdepääsuga ruum

salvestistele on ligipääs piiratud isikute ringil

andmeid säilitatakse vaid teatud perioodi jooksul

muu, täpsustage

.....

12. Kuidas on Teie ettevõttes töötajaid kaamerate olemasolust teavitatud?

ettevõtte sissepääsude juures on turvakaamerate olemasolust teavitavad sildid

ettevõtte siseterritooriumil on turvakaamerate olemasolust teavitavad sildid

töötajaid teavitab turvakaamerate olemasolust suuliselt juht (nt vahetu juht või personalijuht)

- töötajaid teavitatakse kaudselt, s.t töötajal on võimalik info ise üles leida (nt infotahvel, siseveeb)
- töötajaid teavitatakse turvakaamerate olemasolust tööle asumisel kirjalikult (eraldi juhend, kirjaliku töölepingu osa või lisa vms)
- töötajaid ei teavitata turvakaamerate olemasolust, nad märkavad neid ise
- töötajaid ei teavitata turvakaamerate olemasolust, see ei ole neile vajalik informatsioon
- muu

13. Kas Teie ettevõttes antakse lisateavet ja/või arutletakse turvakaamerate olemasolu (sh eesmärkide) üle ka töösuhte kestel (nt koosolekutel, tehakse lisakoolitusi ettevõtte sisekorrareeglite tutvustamiseks ja arutamiseks vms)? Kui vastus on „jah”, siis palun täpsustage, kuidas.

- jah,
- ei

14. Kui töötajaid teavitatakse turvakaamerate olemasolust kirjalikult, siis milline info sisaldub kirjalikus teavituses?

- turvakaamerate eesmärk/eesmärgid
- olukordade ja protsesside kirjeldus, kuidas saadud andmeid kasutatakse
- alade ja ruumide loetelu, kuhu kaamera(d) on suunatud
- jälgimise aeg
- jälgimise liik (reaalajas või salvestamisega)
- turvakaamerate üldine kirjeldus (statsionaarne, pööratav, suurendamisvõimalusega, koos helisalvestamisega jne)
- turvakaamerate salvestiste töötaja(te) nimed/ametikohad ja kontaktandmed
- olukordade kirjeldused, millal turvakaamerate salvestisi võidakse edastada kolmandatele isikutele
- kirjeldus meetmetest, millega tagatakse turvakaameratega kogutud salvestiste kaitsmine
- salvestiste säilitamise aeg
- salvestistega tutvumise kord

15. Kas ettevõttes on esinenud olukordi, kus töötaja on avaldanud vastumeelsust kaamerate olemasolu üle?

- jah
- ei

16. Kas ettevõttes on välja töötatud kaebuste menetlemise kord?

jah ei

Aitäh küsimustikule vastamast!

