TALLINNA ÜLIKOOL

Informaatika Instituut

Timo Tarkmees

Töökoht kui oht töötaja privaatsusele

Magistritöö

Juhendaja: Aare Klooster

Tallinn 2014

Autorideklaratsioon

Deklareerin, et käesolev lõputöö on minu töö tulemus ja seda ei ole kellegi teise poolt varem kaitsmisele esitatud.

5. jaanuar 2015. a. …….

(lõputöö kaitsja allkiri)

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina _____ (sünnikuupäev: _____)
(*autori nimi*)

1. annan Tallinna Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose

   _____

   _____

   (*lõputöö pealkiri*)

   mille juhendaja on

   _____,
   (*juhendaja nimi*)

   säilitamiseks ja üldsusele kättesaadavaks tegemiseks Tallinna Ülikooli Akadeemilise Raamatukogu repositooriumis.
2. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.
3. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tallinnas _____
allkiri ja kuupäev

Sisukord

Sissejuhatus

Tänapäevases infoühiskonnas, kus andmed on muutunud suureks raha tegemise viisiks, tõstatub järjest teravamalt küsimus üksikisiku privaatsusest ning tema isikuandmete kaitsest. Tegemist on ühe kõige olulisema info- ja kommunikatsioonitehnoloogiaalase küsimusega koguni globaalselt tasemel. Näiteks erinevate (IT sektoris tegutsevate) ülemaailmsete korporatsioonide andmete töötlemise viisidele ning nende turvalisuse tagamisele pööratakse järjest suuremat tähelepanu. Käivad lõputud vaidlused selle üle, kus on piir lubatu ning lubamatu vahel. Selle kõige juures on aga kõige tähtsamaks see sama isik, kelle andmeid töödeldakse. Oht kahjustada saada on just temal. Üldiselt on levinud arusaam, et privaatsus on hüve, millele otsivad kaitset vaid kuulsad inimesed (Lisa 1, küsimus nr 3). Tegemist on väärarusaamaga, kuna õigus eraelule ei ole sugugi väljavalitute hüve. Tegemist on igaühe õigusega, mida on võib nõuda iga inimene, sõltumata tema ühiskondlikust, majanduslikust või muust kuuluvusest. Seega on üksikisiku privaatsuse ning tema isikuandmete töötlemise nõuetekohasuse tagamine üks ääretult oluline ning järjest enam päevakorda tõstatuv teema. Sellel põhjusel olen otsustanud seda probleemi ka antud töös käsitleda.

Üheks väga oluliseks kohaks nii inimese elus üldse, kui kindlasti ka tema privaatsuse vaatest on tema töökoht. Seal veedab ta väga suure osa oma ajast ning tegutseb teatud mõttes tööandja kontrolli all. Sellest aga tulenebki üks väga oluline probleem, milleks on töötaja privaatsus töösuhtes. Käesoleva magistritöö eesmärgiks ongi saada vastus küsimusele, kas töötaja privaatsus töösuhtes on hetkel kehtivate seaduste ning regulatsioonide kohaselt tagatud? Lisaks kontrollida hüpoteesi, et töötaja privaatsus töösuhtes ei ole hetkel tagatud, paika pidavust ning selle tõepärasuse korral pakkuda välja võimalikud lahendused olukorra parandamiseks. Peamised uurimisküsimused, mille kaudu töö eesmärki täidan ning hüpoteesi paikapidavust kontrollin, on järgmised:

- millisel määral toetab hetkel kehtiv regulatsioon töötajate privaatsuse tagamist?
- millised on peamised kitsaskohad tööandja poolse töötaja jälgimisega seoses?
- kui teadlikkud on inimesed oma õigustest seoses enda isikuandmete kaitse ja privaatsusega?

- milliste meetmetega on võimalik töötaja privaatsust senisest efektiivsemalt tagada?
- millisel juhul on tööandjal õigus töötajal eraellu sekkuda?
- kuidas toimib järelevalve töötaja privaatsuse tagamise üle?

Peamisteks töö eesmärgi saavutamiseks kasutatavateks meetoditeks on teaduslike (ning toetava materjalina vähesel määral ka mitteteaduslike) publikatsioonide ning ajakirjade analüüs. Lisaks töötajatele suunatud küsimustik ja intervjuud töötaja ning tööandja vahelise töösuhte õiguspärasuse ning töötaja privaatsuse üle järelevalvet teostavate riiklike institutsioonide esindajatega. Seega kasutan andmete kogumiseks peamiselt nö dokumendiuuringut, küsimustikku ning intervjuusid. Kasutan töös kvantitatiivset uurimisstrateegiat peamiselt just selle kaudu saadavate tulemuste usaldusväärsuse ning laiahaardelisuse tõttu.
Varasemalt on antud probleemi võrdlemisi põhjalikult uuritud USA-s. Ka seal esile kerkinud probleemistik on väga lähedane antud magistritöö raames uuritavale. Lisaks tasakaalu leidmisele tööandja vara ning töötaja privaatsuse kaitsmise vahel (Stanton & Stam, 2006) on seal suureks probleemiks ka pornograafia, mis on viinud olukorrani, kus tööandjad on hakanud tööarvutitesse installima tarkvara, mis võimaldab jälgida ning salvestada arvuti monitoril toimuvat (Lane, 2003). Eestisiseselt on antud probleemistikku analüüsitud peamiselt erinevas õigusalases kirjanduses (Kirst, 2012; Männiko, 2011). Üldiselt võib ütelda, et probleemid erinevates riikides on vägagi sarnased ning suurimaks nendest võib pidada liiga vähest riigi poolset sekkumist antud probleemi lahendamisesse. Üksikisiku privaatsus, mis on midagi väga vundamentaalset ja isiklikku ning mida ei ole õiguste mitte kellelgi rikkuda, on tänu tehnoloogia arengule saanud omale täiesti uue tähenduse. Ning kuna töösuhte puhul on igasuguste (info)tehnoloogiliste lahendustega seonduv otseselt IT juhi vastutusalas, siis on just sellel ametikohal töötaval isikul täita antud probleemi juures väga oluline roll.

1. Töötaja õigus privaatsusele

1.1. Privaatsuse olemus ja töötaja eraelu kaitse töösuhtes

Juba ammu enne tänapäevaste arusaamade tekkimist oli privaatsus inimeste elus olulisel kohal. Vanal ajal peeti eraelu kaitse all silmas ennekõike oma kodu kaitsmist võõraste pilkude eest kõrge aia ja tugeva luku abil. Ka tänapäeval takistavad teise inimese privaatsfääri tungimist lisaks seadustega sätestatud keeldudele mitmed ühiskonna moraalireeglid. Teise isiku kirjavahetust ei loeta ja telefonikõnesid ei kuulata pealt, sest nii ei ole tavaks ja nii ei ole viisakas. Võrreldes varasema ajaga, kui privaatsuse alla mõisteti peamiselt kõrgeid müüre ning tugevaid lukke, on tänapäeval tehnoloogia arenguga lisandunud väga palju võimalusi inimeste privaatsfääri tungimiseks. Tehnika areng on pannud inimesed olukorda, kus nad sageli ei oskagi enam oma privaatsust kaitsta, kuna nad lihtsalt ei tunne kõiki neid vahendeid ega tulegi nende viiside peale, kuidas tema privaatsust võidakse rikkuda. Kahtlemata on see suureks ohuks inimeste põhiõigustele ning tehnoloogia arenedes oht privaatsuse vähenemisele järjest kasvab.

Privaatsus on oma olemuselt isiku erasfäär. See on igaühe õigus enesemääratlemisele ning õigus elada oma soovide ja tahtmiste kohaselt minimaalse välise sekkumisega (Maruste, 2004). Oma eraelu sisustada on iga isiku õigus, mis seisneb isiku võimaluses ise määratleda, kes ta on ja milline on temast loodav kuvand teistele isikutele. Kui varasemalt oli eraelu olemus võrdlemisi üheselt mõistetav, siis seoses infotehnoloogia arenguga muutub privaatsuse defineerimine ning vastuse leidmine küsimusele, et kust läheb kaitstava eraelu piir, järjest keerulisemaks. Privaatsuse tagamisel on väga palju erinevaid komponente, kuid üheks peamisteks nendest on kahtlemata isikuandmete kaitse.

Isikuandmete kaitse eesmärgiks ei ole kaitsta andmeid, vaid kaitsta inimest, keda kaitstavad andmed identifitseerivad ja mille kaudu isik ennast teistele isikutele määratleb. Selle mõjualasse kuuluvad isiku kohta käivad andmed, mille alusel on isik tuvastatud või tuvastatav. Ehk isikuandmete hulka kuuluvad kõik isiku identifitseerimist võimaldavad andmed (Isikuandmete kaitse seaduse § 4 lg 1). Isikuandmete kaitse sisuks on isiku õigus informatsioonilisele enesemääratlusele. Selle sisuks on isiku põhiõigus ja -vabadus ise

otsustada, kellele ja milliseid andmeid ta enda kohta teada annab. Vajaduse isikuandmete kaitse järele tekitas infotehnoloogia ja andmete automatiseeritud kujul töötlemise ülikiire areng, millega seonduvalt muutus isiku identifitseerimine ja isikuandmete töötlemine nii lihtsaks, et tõi endaga kaasa otsese ohu informatsioonilisele enesemääratlusele ning sellega seonduvalt vajaduse õiguskaitse mehhanismide järele.

Ohtu inimeste võimalusele omada kontrolli nende kohta töödeldavate isikuandmete üle peamiselt just automatiseeritud võimaluste kiire arengu tõttu nähti juba 1981. aastal, mil võeti vastu isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon (edaspidi andmekaitse konventsioon). Tegu on rahvusvahelise instrumendiga, mille loomise tingis peamiselt kaks asjaolu. Esiteks nähti isikuandmete töötlemise lahendusi liikumas üha enam automatiseerituks ning selles osas oli vaja järele aidata ka kehtivat õigust. Teiseks osutus 4. novembril 1950. a Roomas vastu võetud Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni (edaspidi EIÕKonv) artikli 8 kohaldamisala praktikas oodatust märksa laiemaks. EIÕKonv-i artiklist 8 tulenevat privaatsusõiguse kaitset loetakse küll andmekaitsereeglite põhiliseks lähtekohaks, kuid kahjuks on privaatsuse mõiste osutunud ammendavalt defineerimatuks ning ka artikli 8 kohaldamise praktika näitab, et selle sätte sisu ei ole üheselt määratletav. On üldteada, et seda sätet on tõlgendatud suhteliselt laialt ning vastavalt ühiskonna arenedes tekkivatele vajadustele, mida EIÕKonv-i loomise ajal ei pruugitud ettegi näha (Bygrave, 1988, 225). Üheks selliseks valdkonnaks, mille kiiret arengut isikuandmete massilise ja automatiseeritult töötlemise suunas ei osatud konventsiooni loomisel ette näha, on kahtlemata ka isikuandmete kaitse ning nende töötlemine töösuhtes. Kuna mõisted nagu era- ja perekonnaelu, privaatsus ning privaatsfäär on väga laiali valguvad ja mitmeti tõlgendatavad, siis võimaldas see paigutada selle alla mitmeid huvisid, mis muidu oleksid jäänud kaitseta. See tekitas vajaduse andmekaitse konventsiooni järele, mis reguleerib isikuandmete kaitset võrreldes EIÕKonv-ga üksikasjalikumalt. Andmekaitse konventsioon aitas täita tühimikke, mida EIÕKonv-i koostamisel ei olnud võimalik prognoosida, kuid mis kerkisid esile selle praktilise rakendamise käigus. Enne andmekaitse direktiivi 95/46/EU (Euroopa Parlamendi ja EL Nõukogu direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta) vastuvõtmist oli andmekaitse konventsioon kahtlemata mõjukaimaks isikuandmete töötlemise printsiipe reguleerivaks dokumendiks. Eestis tagab

isikuõiguse privaatsusele EIÕKonv artikli 8 lõike 1 selgel eeskujul (E.-J. Truuväli et al., 2008, 278-279) Eesti Vabariigi Põhiseaduse (edaspidi PS) § 26, mille kohaselt on igaühel õigus perekonna- ja eraelu puutumatusele. Privaatsusõigus kui osa isiku enesemääratlusõigusest on kas eraldi põhiõigusena või kirjavahetuse ja kodu puutumatuse kaudu sisustatuna sätestatud enamike Euroopa riikide põhiseadustes. Näiteks Soome põhiseaduse artikkel 10, Kreeka põhiseaduse artikkel 9, Saksa põhiseaduse artiklid 10 ja 13. Eraelu ehk privaatsuse kaitsega on kahtlemata hõlmatud ka isikuandmete kaitse. Eesti esimene isikuandmete kaitse seadus (edaspidi IKS) võeti vastu 1996. aastal ning on alates sellest ajast olnud pidevas muutumises. Hoolimata regulatsiooni pikast ajaloost ning sagedasest muutmisest ei ole seni peetud vajalikuks selles reguleerida ka isikuandmete töötlemist töösuhtes.

Andmekaitse kaitseb isiku põhiõigust – õigust privaatsusele. Seega on andmete kaitse juures kõige olulisem termin andmesubjekt ehk füüsiline isik (Isikuandmete kaitse seaduse § 8), kelle isikuandmeid töödeldakse ning kelle õigused vajavad sellest tulenevalt kaitset. Töösuhtes on selleks isikuks töötaja. Iga töötaja, kelle kohta on olemas tema kohta käivat informatsiooni, mida teab, omab või kasutab mõni kolmas isik (näiteks tema tööandja), on andmesubjekt ja suure tõenäosusega ei ole võimalik leida mitte ühtegi töötajat, kes seda ei ole. Lisaks eelnevalt mainitud PS §-le 26 on asjakohaseks sätteks isikuandmete töötlemisel veel kahtlemata ka selle § 19. Selle sätte kohaselt on igaühel õigus vabale eneseteostusele ja igaüks peab oma õiguste ja vabaduste kasutamisel ning kohustuste täitmisel austama ja arvestama teiste inimeste õigusi ja vabadusi ning järgima seadust.

Andmed on informatsioon kellegi või millegi kohta (Eesti Keele Instituut, 2006). Andmed, mille alusel on võimalik isikut identifitseerida, on isikuandmed ehk teiste sõnadega on isikuandmed kõik isiku identifitseerimist võimaldavad andmed (Isikuandmete kaitse seaduse § 4 lg 1). Isikuandmed ilma nende andmetega seonduva identifitseeritava isikuta, kelle informatsiooniline enesemääratlusõigus vajab kaitset, ei ole iseseisev väärtus ega vaja seetõttu eraldi kaitset. Seega on õigusaktidega kaitstavad vaid need isiku kohta käivad andmed, mille alusel on füüsiline isik tuvastatud või tuvastatav. Üheselt ja selgelt piiritletud isikuandmete hulka kuuluvate andmeliikide kirja panemine on võimatu, kuna see vajab hinnangut igale konkreetsele juhtumile eraldi. Isikuandmete olemasolu iseenesest ei lisa ega võta aga ära kellegi põhiõigusi, seda võib teha isikuandmete töötlemine (Isikuandmete

kaitse seaduse § 5), mis on igasugune füüsilise isiku kohta käivate andmetega seonduv toiming või toimingute kogum, kui seda viib läbi kolmas isik. Isikuandmete kaitse mehhanismide loomise vajaduse peamiseks eelduseks on asjaolu, et isikuandmete töötlemine on vajalik. Olukorras, kus see nii ei oleks, saaks lihtsalt ütelda, et isikuandmete töötlemine on keelatud ja andmesubjekti õiguste ning nende riive küsimus olekski leidnud oma lahenduse. Töösuhte puhul see, tulenevalt selle iseloomust, nii lihtne kindlasti ei ole.
Et erinevaid andmeid kombineerides ei oleks võimalik luua pilti isiku omadustest, harjumustest, suhetest, varalisest seisust ja kõigest muust sarnasest, tuleb andmetöötlust piirata, et iga inimene saaks ise võimalikult palju otsustada, kui palju ta end oma tööandjale nähtavaks teeb. Töötaja, kellel on selge ülevaade sellest, et kui palju ning mis eesmärgil tööandja tema kohta käivaid andmeid töötleb, saab teadlikumalt oma käitumist juhtida ning oskab läbi selle paremini oma tööandjaga suhestuda. Kui ta ei pea korraldama oma elu üksnes subjektiivsete veendumuste põhjal selle järgi, mida tööandja võib temast teada, vaid ta on selgelt informeeritud sellest, et mida ja kui palju ta kohta teatakse, on tema õigused märksa paremini tagatud. Kui töötajal ei ole piisava kindlusega võimalik teada, millist tema kohta käivat informatsiooni tema tööandja omab ning ta ei oska ennustada, kellele seda informatsiooni veel võidakse edastada, on olulisel määral piiratud selle inimese vabadus oma tegevust planeerida, ilma et teda mõjutataks või talle survet avaldataks (Lisa 1, küsimus nr 6). Õigus informatsioonilisele enesemääratlusele välistab olukorra, kus töötaja enam ei tea, kes ja mida tema kohta teab. Teadmatus põhjustab ebakindlust ning seeläbi võivad saada kahjustada ka isiku muud õigused, näiteks õigus vabale eneseteostusele.
Üks privaatsusõiguse oluline komponent on kahtlemata inimese kodu. Üldjuhul eeldatakse, et eraelu toimub eraviisiliselt ning seetõttu peamisel kodus. Selline väide ei ole tõene. Kodu puutumatus on põhiõigusena Eesti põhiseadusega eraldi kaitstav, kuid inimese privaatsus peab olema võrdselt kaitstav ka muudes kohtades, milles isiku personaalne ruum on määratletav ning isikul on õiguspärane ootus eeldada, et ta viibib olukorras, kus tema privaatsus on kaitstud. Mh on isikul täielikult õiguspärane ootus privaatsusele ka näiteks tööl olles. Ka kaasuses Niemietz vs. Saksamaa (EIÕK lahend nr 13710/88, 1992) leidis Euroopa Inimõiguste Kohus (edaspidi EIÕK), et eraelu ei pea tingimata olema seotud ainult koduga ning et õigustamatu töökoha läbiotsimine või töötaja ülemäärane kontrollimine on samuti EIÕKonv artikliga 8 tagatud privaatsusõiguse rikkumised.

Sisustamist ning vastust vajab aga küsimus, et mida töötaja ülemäärane kontrollimine endast täpsemalt kujutab ning kas, kuidas, millisel juhul ning millises ulatuses on tööandjal õigus töötaja eraellu sekkuda?

Kui privaatsusele laiemalt loovad vundamendi EIÕKonv, andmekaitse konventsioon ning PS § 26 ja 19, siis kitsamalt töösuhtes on alusregulatsioonideks PS § 43, isikuandmete kaitse seadus, töölepingu seadus (edaspidi TLS) ning võlaõigusseadus (edaspidi VÕS). Kõikides nendes kirjeldatakse laialivalguvaid baaspõhimõtteid, milledest isikuandmete töötlemisel töösuhtes tuleb lähtuda, kuid üheselt selget ning ammendavat vastust nii tööandja, kui töötaja õigustele ei ole nendest kahjuks võimalik saada.

TLS § 1 järgi on töölepinguline suhe subordinatsioonisuhe, kus tööandjal on teatud võim töötaja üle. Sealhulgas õigus töötajat juhtida ja kontrollida. See tähendab muuhulgas õigust võtta vajalikke meetmeid, et selgitada välja töötaja poolt tehtava töö kvaliteet ja maht, samuti õigust jälgida, kas töötaja peab kinni tööaja ja -ohutuse nõuetest ning lojaalsuskohustusest. Tööandja puutubki töösuhte raames, eriti aga töötajat kontrollides, kas paratamatult või sihilikult kokku mitmesuguste töötaja kohta käivate andmetega ning see võib riivata töötaja õigust eraelu puutumatusele ja informatsioonilisele enesemääramisele. Arvestades, et TLS § 1 annab tööandjale sõnaselge volituse töötajat kontrollida ja selle kaudu töötaja kohta informatsiooni saada, võib siin täheldada teatavat tööandjasõbralikku lähenemist seadusandja poolt. Kahjuks puudub aga hetkel ühene arusaam tööandja poolse kontrolli piiride osas. See on aga otseseks ohuks töötaja privaatsusele.

Töösuhe, nagu iga teine alluvussuhe, on oma loomult konfliktne. Tööandja on huvitatud sellest, et töötaja teeks võimalikult väikese tasu eest võimalikult hästi ja palju. Töötaja seevastu soovib enamjaolt võimalikult vähese töö eest võimalikult suurt tasu.

Andmekaitsealane probleemistik töösuhetes on võrdlemisi uus nähtus ning on tingitud osaliselt ka sellest, et demokraatia ja ühiskonna areng on vähendanud olemuslikku lõhet töötaja ja tööandja vahel ning muutnud range alluvussuhte pigem partnerlussuhteks, kus pooltel on, või õigemini peaks olema võrdsed õigused ja kohustused. Andmekaitse töösuhetes on sarnaselt ülejäänud andmekaitse reeglitega välja arenenud privaatsusest ning inimeste õigusest sellele. Õigust privaatsusele on oma lahendites korduvalt kinnitanud EIÕK ka kaasuses Halford vs. UK (EIÕK lahend nr 20605/92, 1997) ja

Copland vs. UK (EIÕK lahend nr 62617/00, 2007). Mõlemas kaasuses on EIÕK leidnud, et kui töötajal on õiguspärane ootus privaatsusele töökohal, siis on privaatsusõiguse rikkumine vastuolus inimõiguste konventsiooni artikliga 8.

Töötajat kontrollides ning töötaja kohta käiva teabega muul viisil kokku puutudes (kui see teave on käsitletav isikuandmetena) peab tööandja arvestama andmekaitse reeglitega, mis on peamiselt sätestatud isikuandmete kaitse seaduses. Tööandjad peavad nende reeglitega arvestama eelkõige põhjusel, et IKS-i tuleb isikuandmetega seotud küsimustes pidada eriseaduseks TLS-i ja VÕS-i suhtes. Lisaks on oluline arvestada nõudega, et töötajat kontrollides on tööandja kohustatud austama töötaja privaatsust ning kontrollima töökohustuste toitmist viisil, mis ei riku töötaja põhiõigusi (Töölepingu seadus § 28 lg 2 p 11).

Kui tööandja töötleb töösuhte raames töötaja kohta käivaid andmeid ja teavet, mis ei mahu isikuandmete mõiste alla, siis ei ole tööandja ka sellise teabe töötlemisel täiesti vaba. Tööandja peab arvestama töötaja kohta käiva teabe töötlemisel näiteks ka VÕS § 6-st tuleneva hea usu põhimõttega. Hea usu põhimõte paneb lepingupooltele muuhulgas kohustuse arvestada vastastikuste õiguste ja huvidega, eriti põhiseaduslikult kaitstud õigustega ning hoiduda nende kahjustamisest. Seega, kui tööandja poolt töötaja kontrollimine ja selle käigus informatsiooni kogumine võib riivata mõnda töötaja põhiseaduslikult kaitstud õigust (nt õigust eraelu puutumatusele või informatsioonilisele enesemääramisele), siis peab tööandja töötaja asjakohaste õigustega arvestama ning hoiduma nende kahjustamisest. Hea usu põhimõtet kui küllalt abstraktset printsiipi, mida konkretiseerida edaspidi peab aitama kohtupraktika, tuleb siiski pidada filtri ülesannet täitvaks. See peab aitama ära hoida lepingupoolte õiguste rikkumise juhul, kui ükski teine õigusreegel ei ole seda enne teinud. Ka töösuhte poolte andmetega seotud huvide tasakaalustamise seisukohalt tuleb hea usu põhimõtet pidada subsidiaarseks. Seda muuhulgas seetõttu, et isikuandmete mõiste alla võib mahutada enamiku töötaja andmeid, millega tööandja töösuhte raames kokku puutub. Seetõttu tuleb esmatähtsaks pidada siiski töölepinguseaduses ja isikuandmete kaitse seaduses toodud reegleid ning alles siis, kui need ei taga poolte andmetega seotud põhiõiguste piisavat kaitset, tuleb kohaldada hea usu põhimõtet. Seega on oluline leida vastus küsimusele, kuivõrd piiravad isikuandmete töötlemise reeglid tööandja õigust saada töötaja kohta andmeid ning kas TLS ja IKS

regulatsioonid tasakaalustavad piisavalt täpselt poolte õigusi ja huvi andmetega seotud küsimustes.

Privaatsus on oma olemuselt väga tähenduslik ning kõikidel isikutel on kohustus teiste inimeste privaatsust austada. Ja seda kõikjal. Ka tööle asudes ei jäta töötaja oma privaatsust ukse taha, vaid see peab olema talle tagatud ka tema tööandja poolt. See, et töötaja kuulub tööandja isikkoosseisu ja peab täitma tööandja tööalaseid korraldusi ei tähenda, et tööandjal tekiks sellest automaatselt ka kontrollimatu võim töötaja (privaatsuse) üle. Kuna inimese privaatsfäär on väga lai, siis on väga raske ennustada tagajärgi, milliste töötaja õiguste rikkumise tööandja poolne õigusvastane töötaja isikuandmete töötlemine endaga kaasa võib tuua. Lisaks ohule eelpool mainitud töötaja vundamentaalsetele põhiõigustele ise otsustada, kui palju ta ennast teistele inimestele nähtavaks teeb, olla informeeritud mida ja kui palju tema kohta teatakse ning õigusele vabale eneseteostusele, võib töötaja andmete õigusvastane töötlemine viia ka töötaja maine, au, väärikuse ning muude mittemateriaalsete õiguste riivamise või näiteks ka delikaatsete isikuandmete töötlemiseni, mis oma olemuselt on juba väga tõsine töötaja õiguste riivamine.

1.2. Tööandja ärisaladuse kaitse vs töötaja privaatsus

1.2.1. Poolte vastanduvad huvid

Teatud ulatuses on töötaja õigus privaatsusele üldtunnustatud. Ilmselt ei vaidle keegi eriti selle üle, et töötajal on õigus ilma teiste juuresoleku või jälgimiseta kasutada tualettruumi ja duširuumi ning vahetada rõivaid. Kõige ülejäänu osas ei olda aga sugugi üksmeelel. Lisaks valmistab probleeme veel asjaolu, et igal inimesel on privaatsuse tunnetus erinev – mõned soovivad enda eraelu eksponeerida igal võimalikul ajal ja viisil, teised tunnetavad sügava riivena juba ainuüksi isikukoodi avaldamist. Oluline on seejuures mõista, et otsust eraelu tunnetatavate piiride kohta ei saa teha andmesubjekti eest keegi teine. Küll aga peab iga inimene arvestama sotsiaalseid suhteid luues, sh tööl käies, et eraelu ei ole eraldiseisev, muust täielikult eraldatav nähtus.

Kuigi tööandjad on selgelt kohustatud arvestama töötaja kontrollimisel tema privaatsusega, ei tähenda see kindlasti piiramatut keeldu tööandjal töötaja tegemisi kontrollida. Näiteks vältimaks, et töötaja tööandja valduses olevaid nii töötaja enda, kui ka teiste inimeste (klientide) andmeid kuritarvitab, peab olema võimalik rakendada mõistlikul tasemel kontrolli töötaja tegevuse üle. Lisaks on kõikides olukordades keeruline töötaja privaatsust tagada, sest see vastandub sageli näiteks üldisele tööandja infosüsteemide turvalisuse tagamisele. Oluline on küll tagada töötajale tema andmete puutumatus ja tegevuse privaatsus, kuid samal ajal on turvalisuse eesmärgil vaja sageli jälgida kasutajate tegevust infosüsteemis, jälgida protsesse ja tagada läbipaistvus. Tõenäoliselt on tööandja infosüsteemide ning erineva infotehnoloogilise infrastruktuuri töökindluse ning nende käideldavuse, tervikluse ja konfidentsiaalsuse tagamine üks ettevõtte jätkusuutlikkuse võtmeküsimus. Selle tagamiseks tuleb aga rakendada erinevaid turvameetmeid, mis võivad suure tõenäosusega olla mõningal määral seotud ka näiteks töötaja infosüsteemis tehtud tegevuste analüüsiga.

Tööandjate õigusi kaitseb eelkõige PS § 31, mis tagab ettevõtlusvabaduse. Arvestades, et ettevõtjad kasutavad oma tegevuses sageli teiste isikute, s.o. töötajate abi, siis on selge, et ettevõtlusega tegelejal, kes on ühtlasi ka tööandja, on vaja teatavat kontrolliõigust oma töötajate suhtes ning võimalust koguda nende kohta mitmesugust ettevõtluse toimimise tagamiseks vajalikku informatsiooni. Vastasel juhul puuduks ettevõtjal ülevaade oma tegevusest ning võimalus seda suunata, mistõttu ei saaks ettevõtja oma tegevuse eest vastutada. Tööandja põhiseaduslikult kaitstud õigused põrkuvad siin aga töötaja õigustega, sest igasugune töötaja kontrollimine ja tema kohta informatsiooni kogumine võivad riivata töötaja õigust eraelu puutumatusele. Samuti ja eriti võib töötaja kohta käivate andmete töötlemine riivata töötaja õigust informatsioonilisele enesemääramisele ehk isiku õigusele ise otsustada, kas, kui palju tema kohta informatsiooni kogub, salvestab ja edastab. Lisaks võib ennekõike töötajate e-kirjade jälgimine ning telefonikõnede pealtkuulamise puhul saada riivatud ka PS §-s 43 sätestatud õigus sõnumisaladusele.

Seega on töösuhte poolte põhiseaduslikult kaitstud õigused vastandlikud. PS § 19 lõike 2 järgi saavad pooled kasutada oma õigusi ja vabadusi niivõrd, kuivõrd nende kasutamine ei riiva põhjendamatult teiste isikute õigusi ja vabadusi. Sellele, et isikute õigused nende omavahelise suhtlemise käigus ei saaks põhjendamatult rikutud, peab PS §-st 13 (mis

sätestab, et igaühel on õigus riigi ja seaduse kaitsele) tulenevalt kaasa aitama ka seaduseandja. Selle sätte alusel on seadusandjal muuhulgas kohustus tasakaalustada töösuhte poolte põrkuvad põhiõiguslikud huvid andmete ja informatsiooniga seotud küsimustes, s.t. tagada, et ükski asjassepuutuv põhiõigus ei oleks ebaproportsionaalselt riivatud. Eestis ei ole eriseadust, mis käsitleks andmekaitset töösuhte raames. Samas on Euroopas mitmeid riike, kes on pidanud vajalikus reguleerida töösuhetes kerkivad andmekaitse küsimused eriseaduses. Näiteks Soome 2004 aastal jõustunud „Laki yksityisyyden suojasta työelämässä". Töösuhte poolte huvid on andmetega seotud küsimustes tasakaalustatud küll üldseadustes, peamiselt töölepinguseaduse, võlaõigusseaduse ja isikuandmete kaitse seaduse kaudu, kui ka nendes aktides on poolte õigused ja kohustused sõnastatud väga üldsõnaliselt, mis jätab väga suure tõlgendamisruumi.

1.2.2. Töö tegemiseks kasutatavad sidevahendid ning nende kaudu edastatud sõnumite saladus

Töötaja huvi on, et tööandja koguks tema kohta võimalikult vähe andmeid, teda minimaalselt kontrolliks ja jälgiks. Seda põhjusel, et töötaja seisukohalt on väga ebameeldiv, kui tööandja saab tema kohta teada isiklike ja võib olla isegi piinlikust tekitavaid asjaolusid. Häiriv on töötaja jaoks näiteks ka see, kui töötaja igal õhtul kontrollib, mida, mis kell ja kui palju töötaja täpselt tööpäeva jooksul tegi (Lisa1, küsimus nr 6). Tööandja on aga vastupidi oma õiguste ja huvide kaitsmiseks huvitatud töötaja kohta võimalikult suure hulga teabe saamisest. Nii on tööandjal huvi teada saada, kui kohusetundlikult ja millise kvaliteediga töötaja oma tööd teeb, kui lojaalne ta on (ennetamaks võimalikku ettevõttesisese informatsiooni lekkimist), millised on töötaja suhted kaaskolleegidega, kui säästlikult nad käivad ümber tööandja varaga, kas tööaja reeglitest peetakse kinni jne. Nagu näha, ei pruugi sidevahendite jälgimise vajadus olla seotud üksnes töötajate kontrollimisega, vaid teinekord on see otseselt vajalik ettevõtte või asutuse igapäevaste tööprotsesside normaalseks toimimiseks.

On üsna tavapärane, et inimesed kasutavad nii oma tööalaseks kui ka isiklikuks suhtlemiseks tööandjale kuuluvaid sidevahendeid. Olgu siis selleks töötelefon, -arvuti või

tööandjale kuuluv e-posti aadress. Sageli logitakse ka oma isiklikku e-posti kontosse või internetipanka sisse tööandjale kuuluvast arvutist, teadmata täpselt, kas sellega seatakse ohtu oma privaatsus või mitte. Tänapäeva veebilehitsejate funktsionaalsus võimaldab ka kõik paroolid otse veebilehitsejasse salvestada, et sisselogimist lihtsustada. Kuna see veebilehitseja on aga tööandja valduses, siis on need paroolid väga kergesti kättesaadavad ka tööandjale. Nimetatud programme kasutatakse ettevõtte infosüsteemis nii tööülesannete täitmiseks kui ka tihtipeale isiklikuks tarbeks. Seadus ei anna aga ühest vastust, mil määral on lubatud selle tööandja poolne jälgimine. Töölepingu seadus ütleb, et tööandja on kohustatud austama töötaja privaatsust ja kontrollima töökohustuste täitmist viisil, mis ei riku töötaja põhiõigusi. See on äga äärmiselt lai ning mitmeti tõlgendatav sõnastus, mis kindlasti ei tekita töötajas kindlust, et kõik tema õigused on kaitstud. Kuigi mingit otsest seadusest tulenevat õigust töötajatel selleks pole, siis paljud tööandjad ei ole sidevahendite kasutamist isiklikuks otstarbeks ka keelanud. Võib leida seisukoha, et tööandja isegi ei tohiks täielikult keelustada interneti ja e-posti kasutamist isiklikuks otstarbeks (Männiko, 2011, 146), kuid samas ei keela sellise piirangu kehtestamist sõnaselgelt ka ükski seadus. Seega on seisukohad väga erinevad, sageli vastanduvad ning ühene arusaam lubatust puudub.

Kõik ongi enamasti hästi seni, kuni kerkib esile mingi probleem või kahtlus näiteks seoses töötaja usaldusväärsusega. Sellisel juhul võib tööandja olla huvitatud töötaja kasutuses olevate sidevahendite kaudu edastatava või juba varem edastatud info teada saamisest. Siinkohal tekib küsimus, kuidas on selle juures kaitstud töötajate õigus privaatsusele ning sõnumisaladusele. Tulenevalt põhiseaduse §-st 43 on igaühel õigus tema poolt või temale posti, telefoni või muul üldkasutataval teel edastatavate sõnumite saladusele. Erandeid võib teha kohtu loal kuriteo tõkestamiseks või kriminaalmenetluses tõe väljaselgitamiseks seadusega sätestatud juhtudel ja korras. Nagu näha, on õigus sõnumisaladusele sätestatud Eesti põhiseaduse eraldiseisvas paragrahvis ning erandite tegemine on oluliselt piiratum, kui on lubatud PS §-s 26 eraelu riiveks. Eesti Põhiseaduses on õigus sõnumisaladusele sätestatud eraldiseisva põhiõigusena, kuigi sisuliselt on sõnumisaladus üks eraelu osa. Näiteks Euroopa Inimõiguste ja Põhivabaduste Kaitse Konventsioonis kaitstakse sõnumisaladust samas sättes (artikkel 8) eraelu ja kodu puutumatusega. Tähelepanelik tuleb nende õiguste kaitseala piiritlemisel olla seetõttu, et põhiseadus sätestab erinevad

tingimused sõnumisaladuse ja eraelu puutumatuse riivamiseks. Sõnumisaladust on lubatud riivata märksa piiratumatel juhtudel - ainult kohtu loal kuriteo tõkestamiseks või kriminaalmenetluses tõe väljaselgitamiseks, samas kui eraelu puutumatust võidakse seadusega piirata lisaks ka tervise, kõlbluse, avaliku korra või teiste inimeste õiguste ja vabaduste kaitseks. Probleem võib tekkida sõnumisaladuse kaitseala piiritlemisel, sest alati ei ole päris selge, milline töötaja sõnum peaks kuuluma tema isikliku sõnumi saladuse kaitse alla ning milline mitte. Samuti võib tekkida küsimus, kas pidada sõnumisaladusega hõlmatuks ka sõnumi liiklusandmed, mis teinekord paratamatult sõnumiga kaasas käivad ning võivad anda aimu suhtluse sisu või iseloomu kohta. Näiteks hilisõhtusel või öisel ajal sagedane helistamine ja sõnumite vahetamine viitab pigem isiklikule kui (üksnes) tööalasele läbikäimisele. Lihtne oleks väita, et tööalased sõnumid ei kuulu isiklike sõnumite kaitsealasse, kuid praktikas eeldaks selle üle otsustamine sõnumi sisuga tutvumist. Lisaks sellele võib üks sõnum sisaldada korraga nii tööalast kui ka isiklikku informatsiooni. See võib esineda näiteks nii tööalaselt kui ka eraelus lävivate isikute vahetatavate sõnumite puhul.

Kuigi tavapäraselt tuntakse sõnumisaladust osana isiku eraelust, siis ei tohiks märkimata jätta ka juriidiliste isikute õigust sõnumisaladuse kaitsele Nimelt on õigus sõnumi saladusele kõigi ja igaühe õigus, mis põhiseaduse § 9 järgi laieneb ka juriidilistele isikutele. Sellest võib teinekord sõltuda näiteks äri-, tootmis- ja riigisaladuse kaitse ning paljude ametite puhul ka ametisaladuse kaitse efektiivsus. Praktikas võib osutuda keeruliseks töötaja tööalase ja erasuhtluse piiritlemine eriti juhul, kui tööandja ei ole sidevahendite kasutamist ja selle suhtes teostatavat järelevalvet ise üldse reguleerinud. Kuna otsest kohustust seda teha ei ole, siis on riik taolise olukorra tekkimist ka igati soodustanud. Tekib küsimus, kuidas sellisel juhul toimima peaks? Või mida peaks tööandja tegema, kui tekib kahtlus, et töötaja lekitab mingit üksnes asutusesiseseks kasutamiseks mõeldud teavet isikliku e-posti aadressi kaudu või muidu „isiklike sõnumitena“? Kuna selge reeglistik puudub, siis on väga raske ütelda, et mis hetkel tekib tööandjal õigus mingi konkreetse meetme rakendamiseks ning mis hetkel saab tööandja viidata oma andmete kaitse vajadusele, riivates sellega töötaja privaatsust. Tegemist ei ole üksnes töötaja privaatsuse seisukohast oluliste küsimusega, vaid sellest sõltub hinnang ka tööandja

järelevalvetegevuse õiguspärasusele, ning mis seal salata, ka tema võimalik kriminaalvastutus liiga ulatusliku või ülemäära intensiivse jälgimise eest.

Töölepingu seaduse kohaselt allub töötaja tööandja juhtimisele ja kontrollile. Samal ajal sätestab seadus, et tööandja on kohustatud austama töötaja privaatsust ja kontrollima töökohustuste täitmist viisil, mis ei riku töötaja põhiõigusi. Seega võib tööandja küll töökohustuste täitmist kontrollida, kuid see õigus on piiratud. Samas seadus siin väga selgeid juhiseid ei anna. Eestis ei ole kujunenud ka arvestatavat kohtupraktikat, mis aitaks seda kohustust selgitada.

1.2.3. Vajadus töötaja kontrollimiseks

Põhjuseid, miks tööandja võib soovida töötajate kasutuses olevaid sidevahendeid ja nende kaudu edastatavat teavet jälgida, on mitmeid. Üheks põhjuseks on see, et sarnaselt muu vara kasutamisele kujutab ka sidevahendite kasutamine endast ressursside kulutamist, mistõttu peaks tööandjal olema õigus reguleerida ja vajadusel piirata enda poolt töötajate kasutusse antud sidevahendite kasutamist isiklikuks otstarbeks ning samas omama õigust ka kehtestatud reeglite järgimist vajadusel kontrollida. Põhjus on selleks lihtne: hoida kulud madalad. Kuna iga ettevõtte peamiseks eesmärgiks on teenida kasumit ning selle saavutamiseks on väga oluline hoida kulud võimalikult madalad, siis on tegemist aspektiga, millele iga professionaalne ettevõtja kindlasti tähelepanu pöörab. Lisaks sellele on tööandjad huvitatud töötajate lojaalsusest ja nende valduses oleva olulise teabe kaitsmisest. Samuti tuleb arvestada, et kõik töökohad ei ole käideldava informatsiooni konfidentsiaalsuse poolest ühesugused, mistõttu eksisteerib vajadus efektiivselt tagada äri, tootmis- ning teinekord ka riigisaladuse kaitse.

Tutvudes infoturbealase kirjandusega, võib ka ennast tehnikakaugeks inimeseks pidav isik üsna kiiresti saada piisava ettekujutuse arvutite, telefonide ning muude sidevahendite kasutamises peituvatest ohtudest oma privaatsusele, kuid ka finantsidele ja üldisele isiklikule turvalisusele (V. Hanson & M. Laur, 2009, 29-58). Ilmeka ülevaate ettevõtte infovarasid ohustada võivatest ohtudest annab näiteks ka Riigi Infosüsteemi Ameti poolt koostatud infosüsteemide kolmeastmelise etalonturbe süsteemi (ISKE) ohtude kataloog kus on võimalikke ohtusid loetletud lausa tuhandeid. Oluline on märkida, et tegemist ei ole

kindlasti ammendava loeteluga, kuid fakti, et ohtusid on palju ning nende hulk kasvab järjepidevalt, tõestuseks on see kindlasti. Tagamaks oma infosüsteemide käideldavus ning nendes töödeldavate andmete kaitse, on tööandja lausa kohustatud rakendama vastavaid turvameetmeid, mis vähendaks ohtusid nii süsteemidele, kui nendes töödeldavatele andmetele. Tõsiseks probleemiks on arvutiviiruste ja muu pahavara levik, kuid mitte ainult. Arvestades üha kasvavat eri riikide vahelist konkurentsi majanduses, on suundumus andmekaitse parendamisele ja töötajate põhjalikumale kontrollimisele pigem kasvav kui kahanev nähtus. Selle üheks põhjuseks on kasvav tööstusspionaaž, mis võib tekitada ettevõtjatele ning seeläbi ka riikide majandusele tõsist majanduslikku kahju. Ka Kaitsepolitseiamet tõdes juba oma 2009. aasta aastaraamatus (Kaitsepolitsei aastaraamat, 2009, 14-15), et Eesti ettevõtjad ei taju tööstusspionaaži ohtu piisavalt. Kaitsepolitseiameti hinnangul on probleemiks ettevõtjate vähene teadmine sellise ohu olemasolust, mistõttu võetakse riski maandamiseks harva midagi ette. Ameti hinnangul ei ole tegu ainult suurettevõtteid ja teadusasutusi puudutava probleemiga. Rünnaku objektiks võivad olla ka väiksemad ja keskmise suurusega ettevõtted. Eestis on küllaldaselt olulisi ettevõtteid, mille puhul on täiesti reaalne vajadus kehtestada nii töötajatele kui ka tööandjatele rangemad järelevalvemeetmed, kui seda näevad ette kehtivad seadused. Väidetavalt pakub välisriikide luurele enim huvi Eesti energeetika- ja transpordisektor. Mida olulisemaks muutub ettevõte riigi majanduse jaoks, seda tähtsamaks muutub ka personali usaldusväärsusega seonduv. Arvestades info-ja kommunikatsioonitehnoloogia sektori olulisust Eesti majandusele ning selle kasvupotensiaali, saab kahtlemata rääkida sellest, kui olulisest Eesti majanduse komponendist ning välisluure ründeobjektist. Oluline on märkida, et mainitud tööstusspionaaži kasv võib varem või hiljem hakata mõjutama igaühe õigust privaatsusele.

Lisaks eelnevale tekitab sageli vajaduse töötaja poolt kasutatavale sidevahendile ligipääsu saamiseks kliendikaebuste lahendamine. Tööandjad soovivad sageli kontrollida klienditeeninduse töö kvaliteeti ja kliendile antud lubadusi. Mõnikord on vaja pooleli olevate läbirääkimiste lõpetamiseks saada kätte kirjavahetus töölt lahkunud või puhkusel viibiva töötaja postkastist. Tegemist ei ole ammendava loeteluga, sest iga ettevõtte või asutuse töö spetsiifikast tulenevalt võib esineda ka mõni muu vajadus töötajate tegevuse kontrollimiseks ja nende kasutuses olevate sidevahendite jälgimiseks.

Seega eespool toodust tulenevalt võib tööandja soovida töötajate kasutuses olevate sidevahendite kasutamist jälgida peamiselt järgmistel põhjustel:

- töötaja lojaalsuse kontrollimine ning võimalike äri-, tootmis- või riigisaladuse lekete avastamine;
- tööandja vara ning tööaja otstarbekas kasutamine;
- andmeturberiskide maandamine ning pahavara leviku tõkestamine;
- klienditeeninduse kvaliteedi kontrollimine ning tõendusmaterjali kogumine võimalike kliendikaebuste lahendamiseks;
- puhkusel viibiva või töölt lahkunud töötaja postkasti saabunud olulise teabe kätte saamine.

2. Tehnoloogilised võimalused töötaja jälgimiseks

2.1. Kontrolli teostamise alused

2.1.1. Töötaja nõusolek, kui alus töötaja isikuandmete töötlemiseks

Kui tööandja töötleb töötaja isikuandmeid, siis peab tal olema selleks selge alus. Sageli võib kohata väärarusaama, et tööandjal on õigus töötaja isikuandmete töötlemiseks üksnes siis, kui tal on selleks töötaja luba (Lisa 1, küsimus nr 10). Tegelikult on kaheks peamiseks tööandja poolse töötaja isikuandmete töötlemise aluseks töösuhtes isikuandmete töötlemine andmesubjekti nõusolekul ning lisaks isikuandmete töötlemine lepingu täitmiseks. Nõusolek peab olema vaba, teadlik ja selge. Praktilises elus on peamiseks probleemiks see, et töötaja nõusolek ei ole sageli vaba. Nagu eelnevalt analüüsitud, allub töötaja tööandja juhtimisele ning kontrollile. Kuigi teoreetilises maailmas on töötajal vabadus oma isikuandmete töötlemisest keelduda, siis praktilises elus see paraku siiski nii lihtne ei ole. Sama asjaolu selgus ka töötajate seas läbi viidud küsitluse tulemusel (Lisa 1, küsimus nr 11). Tööandjal on mitmeid võimalusi oma isikuandmete töötlemisest keeldunud töötajat negatiivselt mõjutada ning teiseks töödelda tema isikuandmeid hoolimata keeldumisest, näiteks oma infosüsteemide ning andmete turvalisuse ettekäändel. Lisaks võib isikuandmete töötlemisel andmesubjekti nõusoleku alusel palju probleeme põhjustada töötaja õigus oma nõusolek igal ajal tagasi võtta. IKS näeb küll ette, et isikuandmeid võib töödelda isiku nõusoleku alusel, kuid samas sätestab IKS § 12 ka hulga tingimusi, millele nõusolek peab vastama. Lisaks sellele, et vastav nõusolek peab olema antud vabal tahtel ning isikul peab olema võimalus nõusolek igal ajal tagasi võtta, sätestab IKS § 12, et:

1) nõusolek peab olema kirjalikku taasesitamist võimaldavas vormis, välja arvatud juhul, kui vorminõude järgmine ei ole andmetöötluse erilise viisi tõttu võimalik. Delikaatsete isikuandmete töötlemiseks peab nõusolek olema igal juhul kirjalikku taasesitamist võimaldavas vormis;

2) nõusolekus peavad olema selgelt määratletud:

2.1 andmed, mille töötlemiseks luba antakse;

2.2 andmete töötlemise eesmärk;

2.3 isikud, kellele andmete edastamine on lubatud;

2.4 andmete kolmandatele isikutele edastamise tingimused;

2.5 andmesubjekti õigused tema isikuandmete edasise töötlemise osas;

3) kui nõusolek antakse koos teise tahteavaldusega, peab isiku nõusolek olema selgelt eristatav;

4) vaikimist või tegevusetust nõusolekuks ei loeta;

5) nõusolek võib olla osaline ja tingimuslik.

Vaidluse korral eeldatakse, et nõusolekut ei ole antud (Isikuandmete kaitse seaduse § 12 lg 8). Nõusoleku tõendamise kohustus on isikuandmete töötlejal (st tööandjal). Töötajal peab olema võimalik tõepoolest valida, kas ta soovib nõustuda isikuandmete töötlemisega või mitte. Kui nõusoleku mitteandmisega kaasnevad eelarvamused, hinnangud või sanktsioonid, ei saa rääkida vabal tahtel antavast nõusolekust. Töötaja nõusolekuga ei saa õigustada nende nõuete vastu eksimist. Nõusoleku alusel töötlemisest saab töösuhtes rääkida ainult juhul, kui töötaja on ka tegelikult vaba oma valikutes ning tal on igal hetkel tegelikult võimalus oma nõusolek tagasi võtta. IKS § 12 lõikest 7 lähtudes saab nõusoleku alusel töötlemine kõne alla vaid juhul, kui nõusoleku tagasivõtmise järgselt on töötlemine võimalik ka tegelikult ära lõpetada. Nõusoleku alusel töötaja isikuandmete töötlemine peab igal juhul olema kooskõlas ka hea usu põhimõttega, heade kommete ning avaliku korraga. Oluline on märkida, et nõusoleku saab anda vaid iseenda isikuandmete töötlemiseks. Teise inimese isikuandmete töötlemiseks saab tema eest nõusoleku anda vaid juhul, kui seadusest või tehingust tulenevalt on teise inimese esindamise õigus. Nii näiteks saab lapsevanem anda oma alaealise lapse andmete töötlemiseks nõusoleku. Küll aga ei saa töötaja anda tööandjale nõusolekut enda muude sugulaste (vanemad, abikaasa, õed-vennad) andmete töötlemiseks. Seega kaasneb töötaja nõusoleku alusel tema isikuandmete töötlemisega mitmeid nõudeid ning reegleid, millega tööandja on kohustatud arvestama. Arvestades nõusoleku alusel isikuandmete töötlemise keerukust ning nõuete rohkust, on tööandjal

mõistlikum kaaluda isikuandmete töötlemist teisel alusel – poolte vahel sõlmitud lepingu täitmiseks.

Nagu näitab ka töötajate seas läbi viidud uuring (Lisa 1), siis on töötajate privaatsuse tagamise juures väga suuri probleeme. Alustades juba töötajate hinnangust sellele, kui teadlikud nad enda õigustega oma isikuandmete kaitsel töösuhtes on (Lisa 1, küsimus nr 2) ning lõpetades asjaoluga, et 95% vastanutest ütlesid, et neil puudub ülevaade sellest, millisel määral neid oma töökohal tööandja poolt jälgitakse (Lisa 1, küsimus nr 5). Seega isegi olukorras, kus töötajad on nõusoleku oma isikuandmete töötlemiseks andnud, puudub neil sisuliselt ülevaade, millisel määral neid jälgitakse ning kas see jääb lubatu piiresse või mitte. Oluliseks probleemiks minu hinnangul on ka asjaolu, et hoolimata tehnoloogia äärmiselt kiirest arengust, mis on teinud ka töötajate jälgimise oluliselt lihtsamaks ning laiaulatsulikumaks, ei tunneta töötajad hetkel veel sellest tulenevaid ohte (Lisa 1, küsimus nr 4).

2.1.2. Tööleping, kui alus töötaja isikuandmete töötlemiseks

Kõige õigem ja esmane isikuandmete töötlemise alus peaks teoreetiliselt olema küll andmesubjekti nõusolek, kuid praktikas on väga sageli vastavaks aluseks siiski IKS § 14 lg 1 p 4 ehk isikuandmete töötlemine andmesubjektiga sõlmitud lepingu täitmiseks. Seega on tööandjal õigus töödelda töötaja kontrollimiseks tema isikuandmeid niivõrd, kuivõrd see on vajalik töötajaga sõlmitud töölepingu täitmiseks. Kui igasugune isikuandmete töötlemine tööandja poolt tugineks ainult töötaja nõusolekule, muutuks töölepingu jätkamine võimatuks, kui töötaja otsustaks näiteks võtta isikuandmete töötlemiseks antud nõusoleku tagasi. Seetõttu ongi IKS § 14 lg 1 punktis 4 sätestatud, et tööandjal on õigus töötaja isikuandmeid töötlemiseks temaga sõlmitud lepingu täitmiseks.

Oluline on märkida, et lepingu mõistet ei saa IKS § 14 lg 1 p 4 raames tõlgendada kitsalt, ainult töölepingu dokumendina. Leping hõlmab nii töölepingut kui selles viidatud dokumente, näiteks tööandja poolt kehtestatud reegleid töökorraldusele, ametijuhendit jms. Töösuhte reguleerimiseks võib olla sõlmitud üks või mitu lepingut, nt lisaks töölepingule ka materiaalse vastutuse leping ning kokkulepe saladuse hoidmise ning konkurentsipiirangu kohta. Lisaks ei pruugi kõik tingimused olla kirjas töölepingus: VÕS

§ 23 kohaselt võivad lepingupoolte kohustused lisaks lepingule ja seadusele tuleneda ka lepingu olemusest ja eesmärgist, lepingupoolte vahel välja kujunenud praktikast, lepingupoolte kutse- või tegevusalal kehtivatest tavadest ning hea usu ja mõistlikkuse põhimõttest. Lisaks sätestab VÕS § 27, et kui isegi olulised tingimused on jäänud kokku leppimata, siis võidakse kohaldada tingimust, mis on mõistlik asjaoludest, lepingupoolte tahtest, lepingu olemusest ja eesmärgist ning hea usu põhimõttest lähtudes. Ühelt poolt on küll positiivne, et töötaja kaitse on laiem, kui ainult lepingus reguleeritu, kuid teiselt poolt on ka kehtivad tavad, hea usu ning mõistlikkuse põhimõtted sarnaselt teistele töötaja privaatsust reguleerivatele punktidele äärmiselt laialt sisustatavad mõisted.

Tööandja poolse kontrollimise esemeks saavad olla vaid tööga seotud asjaolud. Töötaja töövälist tegevust võib tööandja kontrollida ainult töösuhtega seotud asjaoludel. Töövälise tegevuse kontrollimine võib kõne alla tulla näiteks seoses Töölepingu seaduse § 15 lg 2 p-s 9 sätestatud töötaja kohustusega hoiduda tegudest, mis kahjustavad tööandja mainet või põhjustavad klientide või partnerite usaldamatust tööandja vastu. Kõiki kontrollitavaid asjaolusid peab olema võimalik seostada töötaja töökohustustega, sest tööandja õigus kontrollida saab eksisteerida vaid juhul, kui töötajal on vastav kohustus. Kontrollimise lubatavuse hindamiseks tuleb seega välja selgitada töötaja kohustused. Primaarseks kohustuse allikaks on tööleping. Töölepingu kaudu seovad töötajat ka tööandja poolt kehtestatud reeglid töökorraldusele (Töölepingu seaduse § 5 lg 1 p 11). IKS § 14 lg 1 p 4 kohaselt ei või lepingu täitmise eesmärgil töödelda delikaatseid isikuandmeid. Seega delikaatseid isikuandmeid võib tööandja töötaja kontrollimise käigus töödelda juhul, kui selline õigus tuleneb tööandjale mingist seadusest või kui töötaja annab selleks nõusoleku. Siinkohal on oluline märkida, et taoline nõusolek peab kindlasti vastama eelmises alajaotuses kirjeldatud nõuetele. Suurimaks probleemiks on aga asjaolu, et praktikas ei ole võimalik delikaatsete isikuandmete töötlemist kontrollimise käigus täielikult välistada. Täpsemalt analüüsin seda probleemi järgnevates alajaotustes.

Juba töötaja välimus võib viidata tema rassilisele kuuluvusele või usulistele veendumustele. Sellistel puhkudel ei ole siiski mõeldav, et tööandjal ongi kontrollimine keelatud. Tööandjale juba ilmselgelt teadaolevate asjaolude täiendav ilmnemine kontrolli käigus ei saa olla kontrolli takistuseks. Sellisele järeldusele jõuab ka Euroopa andmekaitseasutuste töörühm oma dokumendi „Working document on the surveillance of

electronic communications in the workplace, 2002" punktis 3.1.4. Juhul, kui isikuandmete töötlemine töötaja nõusoleku alusel või lepingu täitmiseks on võimalik, siis tuleb silmas pidada, et ka sellisel juhul ei ole see kindlasti õigustatud piiramatul hulgal. Hoolimata aluse olemasolust tuleb isikuandmete töötlejal ikkagi järgida IKS-is sätestatud nõudeid, eeskätt IKS §-s 6 sisalduvaid põhimõtteid:

1) **seaduslikkuse põhimõte** – isikuandmeid võib koguda vaid ausal ja seaduslikul teel;
2) **eesmärgikohasuse põhimõte** – isikuandmeid võib koguda üksnes määratletud ja õiguspäraste eesmärkide saavutamiseks ning neid ei või töödelda viisil, mis ei ole andmetöötluse eesmärkidega kooskõlas;
3) **minimaalsuse põhimõte** – isikuandmeid võib koguda vaid ulatuses, mis on vajalik määratletud eesmärkide saavutamiseks;
4) **kasutuse piiramise põhimõte** – isikuandmeid võib muudel eesmärkidel kasutada üksnes andmesubjekti nõusolekul või selleks pädeva organi loal;
5) **andmete kvaliteedi põhimõte** – isikuandmed peavad olema ajakohased, täielikud ning vajalikud seatud andmetöötluse eesmärgi saavutamiseks;
6) **turvalisuse põhimõte** – isikuandmete kaitseks tuleb rakendada turvameetmeid, et kaitsta neid tahtmatu või volitamata töötlemise, avalikuks tuleku või hävimise eest.
7) **individuaalse 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.

Seega on töötaja kontrollimise reeglid väga detailirohked ning suurt tähelepanu vajavad. Peamisi tehnoloogilisi võimalusi tööandja poolseks töötaja jälgimiseks analüüsin põhjalikumalt järgnevates alajaotustes.

2.2. Töötaja tegevuse üle kontrolli teostamine

2.2.1. E-kirjad

Tööandja domeeniga e-postiaadress on tõenäoliselt üks peamisi tööandja poolt töötajale tööülesannete täitmiseks eraldatud sidevahendeid. Oluline on aga eristada ainult ühe töötaja kasutusse antud e-postiaadressi, nt eesnimi.perekonnanimi@firmanimi.ee (täisnime asemel kasutatakse sageli ka nimekombinatsioone, nt eesnime esitäht + perekonnanimi või ainult ees- või perekonnanime) ning üldisi e-postiaadresse, millele laekuvad kirjad edastatakse mitmele töötajale (näiteks info@firmanimi.ee, firmanimi@firmanimi.ee). Privaatsuse vaatest on nendel kahel võimalikul e-postiaadressi liigil väga suur erinevus, kuna e-kirja saatjal ei ole võimalik tuvastada, kes on nö üldisele e-postiaadressile saadetava e-kirja saajaks. E-postiaadressile kujul eesnimi.perekonnanimi@firmanimi.ee e-kirja saates võib eeldada, et tegemist on personaalses kasutuses oleva aadressiga (kuigi ka selles ei saa saatja täielikult kindel olla), kuid nö üldiste e-postiaadresside kasutamise puhul ei tea e-kirja saatja kunagi, kas see kiri jõuab näiteks paljude klienditeeninduse töötajate postkasti või on saajaks ainult üks inimene. Isegi juhul, kui saajaks on üks inimene, ei ole taolisel kujul e-postiaadresside puhul võimalik tuvastada, kes see isik on. See on aga e-postiaadressi, kui sidevahendiga seotud problemaatika ainult üks aspekt.

Lisaks eelnevalt kirjeldatule on suureks probleemiks näiteks ka tööandja poolne töötaja kirjade lugemine ning nende eristamine era- ning töökirjadeks. Kuna tööandjal puudub kohustus taolisi olukordi kirjeldavate sisemiste protseduuride kehtestamiseks, siis on sageli väga mitmeti tõlgendatav, et milliseid töötaja e-postiaadressile laekunud kirju tööandja lugeda ning muul viisil töödelda võib. Seega on privaatsuse vaatest e-kirja liiklus kahtlemata üks ebaturvaline ning palju tähelepanu vajav suhtlusviis. Kuna käesoleva töö fookuses on töötaja, kes saadab välja e-kirju tööandja domeenis olevast meiliserverist ning on üldjuhul kursis, milliselt e-postiaadressilt, siis käsitlen antud peatükis vaid personaalselt ühele töötajale eraldatud e-postiaadressiga seonduvat.

Eestis on praktikas kujunenud tavapäraseks, et töötajad kasutavad tööandja domeeniga e-postiaadresse muuhulgas ka oma erakirjade saatmiseks ja saamiseks. Paljudel juhtudel kasutavad töötajad töö e-posti isiklikuks otstarbeks mugavuse ja aja tõttu (töö e-posti

loetakse reeglina iga päev või lausa terve päeva jooksul, mistõttu pole vaja erapostkasti pidevalt sisse logida, et kontrollida, ega pole uusi kirju tulnud). Isikliku kirjavahetuse hulka tuleb arvata ka töötajate vaheline kirjavahetus, mis ei seondu tööülesannete täitmisega. Ka Euroopa andmekaitseasutuste töörühm märgib, et töötingimused on muutunud selliseks, et üha raskem on selgelt eristada töötunde eraelust. Paljudel juhtudel jätkub töö tegemine ka kodus. (Article 29 Data Protection Working Party, Working document on the surveillance and monitoring of electronic communications in the workplace, 2002). Ka EIÕK on märkinud kohtuasjas Nimeitz vs Saksamaa, et alati ei ole võimalik selgelt eristada, millised isiku tegevused moodustavad osa tema tööst ja millised mitte. Otseselt ei ole töötajal üldist õigust töö e-posti isiklikul eesmärgil kasutamiseks, kuid tööandjad peavad sellise väljakujunenud praktikaga ja sellest tuleneva töötaja õiguspärase ootusega privaatsusele arvestama seni, kuni nad pole ise kehtestanud teistsuguseid reegleid (ka Võlaõigusseaduse §-d 23 ja 25 sätestavad, et lepingupoolte kohustused võivad tuleneda ka väljakujunenud praktikast). Tööandjal on küll kohustus kehtestada sisemised reeglid töökorraldusele, kuid otsest kohustus, et need peavad sisaldama ka reegleid (töötajate) isikuandmete töötlemiseks, puudub (Töölepingu seaduse § 5 lg 1 p 11). Taoline regulatsioon annab tööandjale suurepärase võimaluse viidata selle kohustuse täitmisele näiteks sellega, et olemas on puhkuse võtmise kord, tuleohutusjuhend jms.

E-kirjad on paljudele inimestele elu igapäevane osa, osadele võib-olla isegi kõige ulatuslikum suhtlemisviis. Tihti ei mõelda sellele, kas keegi peale kirja adressaadi võib veel kirjavahetusest osa saada ning kui palju infot e-postkast kokkuvõttes inimese kohta sisaldab. Arvatavasti saab paljude inimeste puhul nende e-postkasti sisu analüüsides teada tohutu koguse informatsiooni. Ja seda mitte ainult töötaja enda, vaid ka paljude kolmandate isikute kohta. Näiteks kui üks kiri on saadetud korraga paljudele adressaatidele, on võimalik koosmõjus kirja sisuga teha mitmesuguseid järeldusi nii inimeste vaheliste seoste kui nende tegevuste kohta (nt tegemist on ühe sõpruskonnaga, sugulastega, sotsiaalse tugigrupiga, lastevanematega, mingit hobi või meelelahutust harrastavate inimestega).

Isegi juhul, kui tööandja on kehtestanud nõude (milleks tal tegelikult kohustust ei ole), et tööandja domeeniga e-postiaadressi ei või töötajad kasutada isiklike e-kirjade saatmiseks, ei ole ka siis kuidagi välistatud, et postkasti ei satu ühtegi töötaja erakirja. Kuivõrd just ees- ja perekonnanime sisaldavat e-postiaadressi on interneti otsingumootorite abil kõige

kergem leida ja isikuga seostada, tuleb arvestada, et töötajale võidakse kolmandate isikute poolt saata erakirju ilma, et ta selleks omalt poolt kuidagi kaasa aitaks. Näiteks leiab internetist e-posti aadressi ammune tuttav, kellega pole kaua suheldud ning kellel muid kontakte ei ole; keegi korraldab kooli või suguvõsa kokkutulekut ja otsib selleks internetist kontaktandmeid jne. Samuti ei pruugi ka domeeninime järgi olla alati võimalik kindlaks teha, et tegemist on tööandja domeeniga. Tüüpilisi 3-tähelisi domeeninimesid kasutavad näiteks nii e-postiteenuse pakkujad kui ka ametiasutused; kirja saatja ei pruugi teada, kas isik on ettevõttes vaid töötaja või on ta ise ettevõtja. Lõpuks tuleb arvestada veel ka sellega, et kirjad ei ole tihti üheselt ametialasteks või erakirjadeks liigitatavad. Näiteks töötaja suhtleb tööasjus tuttavaga, kes e-kirja lõpus teeb ühtlasi ettepaneku õhtul tema juures kokku saada; klient, kelle laps oli töötaja lapsega ühel ajal haiglas, pärib muuhulgas töötaja lapse tervise kohta; kolleeg teisest ettevõttest, kellega töötaja aeg-ajalt nõu peab, lisab kirjale lingi interneti meelelahutuslehele ning erinevate ettevõttesiseste regulatsioonide kehtestamisel puudub töötajal sageli sõnaõigus ning tööandjal on võimalus kehtestada reegleid nö jõupositsioonilt. Oluline on märkida, et eeskirjade kehtestamine ei vabasta tööandjat kindlasti IKS-is sätestatud kohustuste täitmisest ega võimalikust vastutusest ebaseadusliku tegevuse eest. Ka Euroopa andmekaitseasutuste töörühm märgib oma dokumendi „Working document on surveillance and monitoring of electronic communications in the workplace“ punktis 2.1, et eelnev hoiatamine ei ole piisav, et õigustada töötajate isikuandmete kaitse rikkumisi.

On selge, et tavaliselt loob tööandja töötajale tööandja domeeniga e-postiaadressi siiski tööülesannete täitmise jaoks ning ei saa kunagi täielikult välistada, et tööandjal võib ikkagi tekkida vajadus töötaja töö e-postkastist infot otsida ka muul põhjusel kui töötaja kontrollimiseks. Näiteks võib tööandjal olla vaja arvutisüsteemide tõrgeteta ja turvalise töökorra tagamiseks tuvastada suuremahulised ja ohtlikud (nt pahavaraga nakatunud) e-kirjad või lugeda töötaja puhkuse või äkilise haigestumise ajal saabunud arveid ja tellimusi. Probleemiks aga ongi selle kontrolli piirid. Põhiseadusest tulenev üldreegel ütleb, et tööandjal on õigus ettevõtlusvabadusele, mida ta võib teostada niivõrd, kuivõrd see ei riku töötajate ja kolmandate isikute põhiõigusi. Praktikas on palju küsimusi tekitanud just töötaja e-posti uurimine töö kontrollimise (ja tõendite hankimise) eesmärgil. Nagu punktides 2.1.1. ja 2.1.2 selgitatud, on isikuandmete töötlemine töötaja kontrollimise

käigus võimalik üldjuhul IKS § 14 lg 1 p 4 (töölepingu täitmiseks) või töötaja nõusoleku alusel. Tööandjal ei ole mingit takistust uurida töökohustuste täitmisega seotud e-kirju, sest need ei ole eelpoolkirjeldatud põhiõiguste kaitsealas. Kuivõrd kontrollida on tööandjal õigus vaid tööga seotud asjaolusid, ei peaks tööandjal reeglina üldse tekkima vajadust töötaja erakirju uurida. Praktilises elus on aga nende kahe eristamine sageli äärmiselt keeruline. Enamasti eksisteerib siiski oht, et töötaja eraelu puutumatust või sõnumisaladust rikutakse tahtmatult. Mida vähem on rakendatud preventiivseid meetmeid, seda suurem on tööandja risk töötaja ja töötajaga kirjavahetuses olevate kolmandate isikute isikuandmete töötlemiseks ja sõnumisaladuse rikkumiseks. Juba ainuüksi erakirjade saatmise-saamise kohta andmete vaatamine kujutab endast eraelu puutumatuse riivet. Kirja sisuga tutvumise juures on aga peamiseks probleemiks asjaolu, et sõnumi liigitamine era -või tööalaseks, eeldab selle sisuga tutvumist. Olukorras, kus tegemist oli eraviisilise kirjavahetusega, on tööandja rikkunud töötaja õigust sõnumisaladusele. Seega ei ole kunagi võimalik täielikult välistada, et tööandja ei loe töötaja e-postkastis olevaid erasõnumeid. Ka Euroopa andmekaitseasutuste töörühm märgib dokumendis „Working document on the surveillance and monitoring of electronic communications in the workplace“, et töötingimused on muutunud selliseks, et üha raskem on selgelt eristada töötunde eraelust. Paljudel juhtudel jätkub töö tegemine ka kodus. Ka EIÕK on märkinud kohtuasjas Nimeitz vs Saksamaa, et alati ei ole võimalik selgelt eristada, millised isiku tegevused moodustavad osa tema tööst ja millised mitte. Töötaja töö e-posti uurimisel eksisteerib ikkagi oht riivata sõnumisaladust ja eraelu puutumatust. Töötajal on küll võimalik vähendada riski, et tööandja tema erakirjavahetust loeb, näiteks kirju eraldi kaustadesse paigutades ning nimetades erakirju sisaldav kaust üheselt mõistetavalt erakirju sisaldavaks. Selle, kas taoline kirjade filtreerimine käsitsi (kuna kasutades automaatikat ei saa töötaja olla täielikult kindel, et see jaotab kirjad vastavalt tema soovidele) on mõistlik aja kulutamine, julgeksin aga isiklikult kahtluse alla seada. Ja ka selliste erakirjade olemasolu korral puudub töötajal täielik kindlus, et tööandja neid kirju ei loe. Tööandjal võib tekkida soov kontrollida töötaja erakirju näiteks ka konkurentsikeelu (Töölepingu seaduse § 23) ning konfidentsiaalsuskohustuse (Töölepingu seaduse § 22) rikkumise tuvastamiseks. Sellisel juhul peab töötaja olema teadlik, et töötaja poolt saadetud ja vastuvõetud e-kirjad salvestatakse ning neid võidakse uurida töökohustuste rikkumise korral.

2.2.2. Telefon

Lisaks e-postile on teiseks peamiseks sidevahendiks, mida töötajad töö tegemiseks kasutavad, (mobiil)telefon. Euroopa Inimõiguste Kohus on juba 1997. a selgelt välja öelnud, et telefonikõne tegemine ning vastuvõtmine kuulub EIÕKonv artikli 8 kaitsealasse nii eravalduses, äriühingus kui ka ametiasutuses (EIÕK lahend nr 20605/92, 1997) 2007. a kinnitas EIÕK seda seisukohta veelkord (EIÕK lahend nr 62617/00, 2007), lisades, et eraelu puutumatuse kaitse laieneb ka töötaja e-kirjadele (vt alajaotus 2.2.1) ja interneti kasutamisele (vt alajaotus 2.2.3). Telefonikõnede puhul on sarnaselt e-kirjadele jällegi äärmiselt oluline eristada töökõnesid ja erakõnesid. Nagu eespool selgitatud, siis tööalased sõnumid, sh telefonikõned ja andmed nende kohta, ei ole töötaja eraelu kaitsealas. Erakõnedega seotud andmete töötlemine võib aset leida näiteks juhul, kui töötajal on lubatud töötelefoni kasutada ka erakõnedeks ning hiljem nõutakse töötajalt erakõnede maksumuse hüvitamist. Lisaks saab tööandja võtta välja kõneeristuse või detailse arve ka selleks, et selgitada välja telefoniarve limiidi ületamise põhjus. Andmed töötaja erakõnede kohta (mis ajal ja kellele helistati, kui pikalt kõne kestis jms) on nn liiklusandmed, mis on aga töötaja eraelu puutumatuse kaitsealas. Siin on aga jällegi tegemist mitmeid probleemikohti sisaldava olukorraga.

Praktilises elu ei mõista tööandjad sageli, et miks neil puudub õigus täielikule ülevaatele talle kuuluva telefoninumbriga tehtud kõnede kohta. Tööandjate nägemus on sageli selline, et tegemist on tööülesannete täitmiseks eraldatud varaga ning kõik sellega tehtavad toimingud peavad olema tööandjale täielikult jälgitavad. Päris nii see aga siiski ei ole. Olukorras, kus ei ole kehtestatud selgeid sisemisi reegleid, mis seda lubavad, puudub tööandjal alus töötaja erakõnede kohta informatsiooni saamiseks. Erakõnede andmete uurimine on üldjuhul võimalik kas töölepingu täitmiseks (vt alajaotus 2.1.2) või töötaja nõusoleku alusel (vt alajaotus 2.1.1). Kui töölepingus on kokku lepitud töötaja õigus kasutada tööandja poolt antud mobiiltelefoni ka erakõnedeks, ei tähenda see, et tööandja võiks vabalt uurida töötaja poolt tehtud kõnede andmeid. Näiteks kui kokkuleppe kohaselt hüvitab telefoniarve limiiti ületava summa alati töötaja, ei ole tööandjal üldse mingit põhjust uurida, mis asjaoludel limiiti ületati. Õigustus selleks esineb vaid juhul, kui töötaja

väidab, et limiidi ületamise konkreetsel kuul põhjustas suurem tööalaste kõnede hulk. Sellisel juhul võib tööandja nõuda, et töötaja esitaks seda tõendavad andmed. See, et töötajal oleks võimalik taoline informatsiooni välja võtta, eeldab aga jällegi omakorda seda, et tööandja oleks (mobiilside)operaatori juures talle vastavad volitused andnud, kuna ametlikult on numbri kasutajaks tööandja. Seega omab tegelikku võimu telefoniga tehtud kõnede ning saadetud sõnumite üle siiski tööandja ise.

Oluliseks aspektiks telefoni kõneeristuse andmete uurimisel on veel asjaolu, et see võib sisaldada ka kolmandate isikute isikuandmeid. St sarnaselt e-kirjavahetusele võib töötaja privaatsuse küsimus väga kergesti jõuda ka kõikide temaga suhtlevate inimesteni ja sellisel juhul saab rääkida juba suuremast hulgast inimestest, kelle privaatsust on rikutud ning taoline olukord ei tohiks kindlasti olla aktsepteeritav.

Veel üks levinud telefonikõnede andmete töötlemise juhtum on kõnede salvestamine. Tihti tehakse seda „parema klienditeeninduse tagamiseks“. Ka parema klienditeeninduse tagamine on sisuliselt käsitletav töötajate kontrollimisena. Samas eeldusel, et tegemist on tõepoolest töökõnedega, ei kuulu need töötaja personaalse sõnumisaladuse ega ka eraelu puutumatuse kaitsealasse. Küll aga tuleb arvestada, et kõne on kaitstud kõne teiseks pooleks oleva isiku sõnumisaladusega. Kui lindistamise õigus ei tulene seadusest, peab kõne teist poolt lindistamisest hiljemalt kõne alguses selgelt teavitama ning olemas peab olema ka andmesubjekti nõusolek tema isikuandmete töötlemiseks (Isikuandmete kaitse seaduse § 10 lg 1). Kolmandate isikute jaoks peab nõusoleku andmise üle otsustamine olema reaalselt võimalik (näiteks monopoolse ettevõtte puhul, mille teenuste kasutamisest pole võimalik loobuda, peab kolmandal isikul olema võimalus valida suhtlemiseks muu kanal).

Sarnaselt e-kirjavahetusega, edastatakse telefoniga lisaks tööalasele informatsioonile ka eraviisilist informatsiooni. Töötaja eraviisilised kõned on kaitstud töötaja ja kõne teise osapoole sõnumisaladusega. Kui töötajad võivad töötelefoni kasutada ka isiklikuks otstarbeks, peaks töötajal olema võimalus erakõnede ajal salvestamine peatada või salvestis ise viivitamatult jäädavalt kustutada. Ka sellisel juhul on kõikide kõnede lindistamine siiski problemaatiline, sest üks kõne võib olla ka ainult osaliselt töökõne ning töötaja ei saa takistada sissetulevaid erakõnesid. Lisaks kujutab töötajale salvestiste kustutamise õiguse andmine tööandja vaatest ohtu nende ülemäärasele kustutamisele. Nagu e-kirjavahetuse

korral, nii kehtivad ka telefonisuhtluse puhul lisaks eelpool toodule kõik muud isikuandmete töötlemise nõuded, eeskätt eesmärgi selge määratlemise ning töötajate teavitamise nõue.

Rääkides telefonist, kui sideseadmest, ei saa jätta tähelepanuta, et seoses äärmiselt jõulise tehnoloogia ja nutiseadmete arenguga ei saa me tänasel päeval rääkida enam mobiiltelefonist, kui telefonist selle traditsioonilises mõttes. Tänapäevane nutitelefon sarnaneb juba oluliselt enam arvuti, kui telefoniga ning sellega on võimalik kasutada lugematul hulgal erinevaid teenuseid, mis muudavad inimeste elu mugavamaks ja lihtsamaks. Samal ajal on see aga ka tõsiseks ohuks selle kasutaja privaatsusele. Kui varasemal ajal räägiti olukorrast, kus mobiiltelefonside pealtkuulamine on tehniliselt võimalik üksnes sideoperaatoritel ning teatud riigivõimu esindajatel, siis tänaseks piisab üksnes ühe rakenduse laadimisest telefoni, mis näiteks salvestab kõik tehtud kõned või edastab muud informatsiooni seadme kasutamise kohta soovitud isikule. Seoses nutiseadmete laialdase levikuga on kasvanud ka oht nende pahavaraga nakatumisele, mis võib samuti viia väga kiiresti (tööandja) andmete lekkimise või rahalise kahjuni. Sisuliselt on kõik varasemalt ainult arvuti kasutamisega seonduv funktsioonid nüüdseks üle kandunud nii telefonidele, kui muudele nutiseadmetele.

See juhib meid aga omakorda järgmise probleemini. Nagu on viidanud ka üks maailma juhtivaid info- ja kommunikatsioonitehnoloogia uuringutega tegelev firma Gartner, siis enda isiklike seadmetega töö tegemine on selgelt kasvav trend ning aastaks 2017 võivad juba hinnanguliselt pooled töö tegemiseks kasutatavad seadmed kuuluda töötajatele endile (Gartner Predicts by 2017 - Half of Employers will Require Employees to Supply Their Own Device for Work Purposes). Ka töötajate sead läbi viidud uuring (Lisa 1, küsimus nr 15) kinnitab seda. See aga tähendab seda, et suur hulk tööandjale kuuluvaid andmeid asuvad seadmetes, mis tegelikult tööandjaile ei kuulu. Olukorras, kus failid asuvad seadmetel, mille üle tööandjal kontroll puudub, ei saa tal olla kindlust, et need on kaitstud nii hävimise, kaotsimineku, kui pahavaraga nakatumise eest. Sisuliselt vähendatakse sellega töötaja mugavuse arvelt tööandja kontrolli ning kindlust talle väga oluliste ning sageli äritegevuse aluseks olevate andmete nõuetekohase säilimise üle.

Lisaks seadmete kõvaketastel olevatele andmetele on olemas ka mitmeid muid (nii virtuaalseid, kui füüsilisi) andmekandjaid, millede kasutamise lubatavus töösuhtes ei ole

hetkel üheselt selge. Töötajal on võimalik kasutada andmekandjatena nii pilveteenuseid, kui mälupulki ning DVD plaate. See, milliseid andmeid millisele andmekandjale ning millisel juhul on lubatud salvestada, peab olema üheselt selge. Kohustus seda ettevõttesiselt reguleerida hetkel aga ei ole ning sellest võivad alguse saada mitmed arusaamatused.

2.2.3. Interneti kasutamine

Nagu teiste sidevahendite, nii ka töötaja interneti kasutamise jälgimisel, peab pöörama tähelepanu nõudele, et töötaja isikuandmete töötlemise lubatavuse mõõdupuuks on konkreetse töösuhte iseloom ning minimaalsuse printsiip. Peamisi põhjuseid, miks tööandjal võiks tekkida soov töötaja interneti kasutamise jälgimiseks on kaks: infosüsteemide turvalisuse (nende käideldavuse ning nendes töödeldavate andmete kaitse) tagamiseks ning töötaja kontrollimiseks. Peamisi põhjuseid, miks tööandja võiks soovida töötajat kontrollida, analüüsisin alajaotuses 1.2.3. Sarnaselt näiteks e-kirjavahetuse ning telefoni kasutamise kontrollimiseks on ka selle sidevahendi jälgimise puhul tõsine oht ülemäärasele isikuandmete töötlemisele, mis võib väga kergesti jõuda ka delikaatsete isikuandmete õigusvastase töötlemiseni ning sellisel juhul on töötaja eraelu riive juba väga ulatuslik. Seetõttu on ka interneti kasutamise jälgimine töösuhtes töötaja privaatsuse vaatest vägagi tundlik teema. Kuna tööarvutil olev internetiühendus on tänasel päeval lausa hädavajalik ning võrgust väljaspool olevaid arvuteid on näha väga harva, siis puudutab interneti kasutamine sisuliselt kõiki töö tegemiseks kasutatavaid arvuteid.

Kui töötajat kontrollitakse eesmärgiga, et teha kindlaks, ega töötajad ei külasta tööandja arvutit kasutades veebilehti, mille külastamine võib kahjustada tööandja mainet, peaks tööandja kirjeldama, millistele kriteeriumitele vastavate lehekülgede külastamine tööandja arvutit kasutades on keelatud. Taoline kirjeldus annaks töötajale endale selge võimaluse mitte külastada veebilehti, mille külastamist töötaja poolt tööandja ei soovi.

Et mitte riivata töötajate põhiõigusi ülemääraselt, tuleks enne töötaja internetikasutuse jälgimist väga hoolikalt kaaluda, kas selline jälgimine annab adekvaatset infot töötaja töökohustuste täitmise kohta. Kui töötaja kasutab internetti ka seoses tööülesannetega, võib olla keeruline eristada, milliseid lehti töötaja külastas tööülesannetega seoses ja milliseid erahuvides. Seejuures ei pruugi kõikide lehekülgede avamine olla tahtlik – näiteks töötaja

on eksinud aadressiga, link viib mittesoovitud lehele, lehe avamisel avanevad automaatselt muud lehed, link on eksitava pealkirjaga jpm. Eksitav võib olla ka internetis veedetud aja jälgimine – töötaja võib olla lehe hommikul avanud, kuid jätnud selle sulgemata.

Isegi kui töölepingust tulenevalt on tööandjal õigus töötaja internetikasutust arvutisüsteemi turvalisuse tagamiseks jälgida, tuleb hinnata, kas selline töötlemine on turvalisuse tagamiseks ka reaalselt vajalik. Turvalisuse tagamisel on märksa olulisem ennetamine, mistõttu on interneti kasutamise jälgimise asemel võimalik rakendada kohaseid arvutisüsteemi kaitsemeetmeid, vajadusel kuvades asjakohaseid automaatseid hoiatusi või blokeerides juurdepääsu ohtlikele lehtedele. Teiselt poolt tekib küsimus, kas taolise lubatud ja lubamatute lehtede haldamine ning hoiatusete reeglite loomine on mõistlik ning otstarbekas tegevus. Kuna uusi veebilehti on lugematu arv ning neid tekib järjepidevalt juurde, on taoliste õiguste ja reeglite haldamine ajamahukas töö ning tekib küsimus, kas tööandjal on mõistlik oma tööjõudu taolise tegevuse peale kulutada. Kuna ettevõttes võib olla väga erineva profiili ning andmevajadusega töökohti, võib kergesti jõuda olukorrani, kus osad veebilehed peaksid olema osadele töötajatele lubatud ning teistele mitte. Lisaks on teoreetiliselt võimalik kaaluda näiteks ajalise piirangu seadmist teatud veebilehtedele (näiteks sotsiaalmeedia keskkonnad). See aga suurendab taoliste õiguste haldusega tegelevate töötajate töökoormust veelgi ning suuremate organisatsioonide puhul saab taolise koormuse puhul rääkida ilmselt juba eraldi täiskoormusega ametikohast, kes taoliste küsimuste eest ettevõttes peaks vastutama.

Kui tööandja on aga otsustanud (kas siis õiguspäraselt või mitte) töötajate interneti kasutamist jälgima hakata, siis on see tema enda poolt hallatava arvuti (ja tegelikult ka kõikide muude sideseadmete ning jälgimisseadmete puhul) äärmiselt lihtne. Tööandjal on võimalik lasta paigaldada töötaja arvutisse täpselt selline tarkvara, nagu ta ise soovib ning saada selle abil soovitud informatsiooni. Töötaja tööarvuti on võimalik konfigureerida täpselt selliste õigustega nagu tööandja soovib ning töötaja võimalused sellesse sekkuda on praktilises elus võrdlemisi väikesed. See kinnitab veelkord fakti, et töötaja ning tema privaatsus väga suuresti tööandja kontrolli all ning taoline olukord vajaks kahtlemata täpsemat reguleerimist.

Tööandjate kasuks räägib asjaolu, et tänapäevases infoühiskonnas internetti kasutades ning näiteks kergekäeliselt kahtlastel veebilehtede linkidel klikkides on töötajal äärmiselt lihtne

nakatada pahavaraga nii tema poolt kasutatav tööandja arvuti, kui sealt edasi ka kõik muud tööandja võrgus olevad seadmed ning infosüsteemid. Olenevalt ettevõtte turvateadlikkusest on seal ilmselt küll rakendatud erinevaid turvameetmeid nii viirusetõrje, kui efektiivse, loogilise ning turvalise võrgutopoloogia näol, kuid kuna rakendatavad meetmed ei ole üheselt reguleeritud (ja praktikas see ei olekski võimalik), siis saame ikkagi rääkida suurest ohust tööandja infrastruktuurile. Taolise paari arvutihiire abil tehtud kliki võimalike tagajärgede nimistu on lõputu. Sellega võib töötaja seada ohtu nii enda, kui ka kõikide teiste töötajate privaatsuse ning kuna see võib viia ka näiteks kaastöötajate pangakoodide lekkimiseni, siis võib ohtu sattuda isegi nende majanduslik olukord. Rääkimata suurest ohust tööandja infosüsteemidele, mis võib väga sageli olla tööandja üheks kallimaks varaks ning kogu ettevõtluse tegevuse aluseks. Seega ei saa eitada, et ohud on suured, kuid ka üksikisiku privaatsus on midagi äärmiselt olulist, et mitte öelda ülimuslikku. Seetõttu ongi äärmiselt oluline saavutada ühine arusaam ning selgus tööandja õiguste üle töötaja jälgimisel. Olukorras, kus tööandjal on äärmiselt lihtne saada teada kõik töötaja paroolid, mida ta erinevatesse keskkondadesse sisenemiseks kasutab ning tutvuda ka näiteks (era)vestlustega, mida töötaja arvuti abil on pidanud, on ta tunginud väga tugevalt töötaja privaatsfääri.

2.2.4. Jälgimisseadmed

Jälgimisseadme täpne tähendus on reguleeritud turvaseaduses (Turvaseaduse § 11 lg 3) ning selle kohaselt on jälgimisseadmestik 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. Töösuhte vaatest saab peamisteks jälgimisseadmeteks pidada turvakaameraid, helisalvestusseadmeid ning asukohta tuvastada võimaldavaid seadmeid.
Võrreldes teiste töösuhtes sidevahendite abil isikuandmete kogumise viisidega, on jälgimisseadmete õigusvastane kasutamine tõenäoliselt kõige intensiivsem eraelu riive üldse. Seetõttu on ka sellega seotud õiguste ning kohustuste võimalikult täpne reguleerimine eriti oluline. Taoliste seadmete kasutamisel muudavad töötajad oma käitumist – enamik inimesi hakkavad enam kontrollima oma juttu ja käitumist, kui nad

teavad, et iga nende sõna ja liigutust jälgitakse. Lisaks sellele, et taoline teguviis võib väga kergesti minna vastuollu vundamentaalsete inimõigustega ning piirata inimeste väljendusvabadust, võib taolise jälgimise all töötamine viia ka meditsiiniliste tagajärgedeni (nt stress).

Iga jälgimisseadme kasutamisel peab olema eesmärk ning seda võib kasutada üksnes selle eesmärgi saavutamiseks. Juhul, kui tööandja kasutab valvekaamerat näiteks vara kaitseks, ei tohi see kahjustada ülemääraselt kaamera vaatevälja jäävate isikute (nt töötajate) huve. Näiteks olukorras, kus valvekaamera on paigaldatud töötaja selja taha ning suunatud konkreetselt ainult töötaja arvuti ekraanile, ei saa rääkida sellest valvekaamerast, kui jälgimisseadmest tööandja vara kaitseks. Taoline lahendus on kahtlemata ka töötajatele vägagi vastumeeldne (Lisa 1, küsimus nr 8). Töötaja regulaarne jälgimine kaamerate abil tema töö ajal peaks igal juhul olema välistatud (European Data Protection Supervisor, Video-surveillance Guidelines, 2010). Samuti tööandja ruumide sissepääsu juurde paigaldatud turvakaamera (mille eesmärk on ennetada ja avastada vargusi ja vandalismi) lindistusi ei või kasutada selleks, et kontrollida, kas töötajad peavad tööajast kinni. Kuigi tegemist on suurepärase võimalusega töötajate tööaja jälgimiseks ning seda tõenäoliselt laialdaselt kasutatakse, on tegemist selgelt seadusevastase tegevusega. Valvekaamerate paigaldamise eesmärk on turvaprobleemide lahendamine ning selle eesmärgi meelevaldne laiendamine töötaja kontrollimisega seonduvale ei ole kindlasti aktsepteeritav. Igasugune töötajate jälgimine peab olema adekvaatne ja proportsionaalne meede nende riskide suhtes, mis tööandjal on ning jälgimist tuleb teostada võimalikest leebemail viisil. Töötajate eraelu enam riivava tehnika kasutamist ei saa kindlasti õigustada ainult majanduslikud argumendid. Kas ja millisel viisil töötajate jälgimine on lubatud, tuleb hinnata igal konkreetsel juhul eraldi. Probleemiks ongi aga asjaolu, et suunised, millest taolise hinnangu andmisel lähtuda, sisuliselt puuduvad.

Jälgimisseadme kasutamise lubatavuse hindamisel tuleb hinnata näiteks seda, kas selle kasutamise eesmärk on piisavalt kaalukas (et sellega töötajate privaatsuse ohtu seadmine oleks põhjendatud), kas antud eesmärki oleks võimalik saavutada ka muude meetmetega, kas valvekaamera poolt kaetud ala on mõistlik ja proportsionaalne, kas valvekaamera suund on muudetav, kas see salvestab lisaks pildile ka heli jne. Taoliste seadmete kasutamine sisaldab endas suurel hulgal erinevaid nüansse ning võimalusi, mida on

tööandjal hetkel võimalik enda kasuks pöörata. Olen seisukohal, et riik ei tohiks taolist olukorda aktsepteerida.

Väga oluliseks asjaoluks töötaja jälgimisel tema isikuandmete kaitse vaatest on see, kas isik, kelle andmeid töödeldakse, on üheselt tuvastatav. Teatavasti hõlmab isikuandmete kaitse alane reeglistik üksnes isikuandmeid ning isikuandmete olemuse printsiibiks on isiku tuvastatavus. Kui andmete poolt kirjeldatav isik on tuvastatav, siis näiteks turvakaamerate salvestiste puhul ei omagi suurt tähtsust, kas salvestisi ka vaadatakse või mitte, isikuandmete töötlemisega on tegemist sellegi poolest. Lisaks sellele võib isikuandmeid töödelda ainult ulatuses, mis on vajalik eesmärgi saavutamiseks ning kogutud andmete töötlemine tuleb IKS § 24 p 1 kohaselt lõpetada kohe, kui eesmärgid on täidetud. Kui jälgimisseadmestikku kasutatakse näiteks varguste ja kallaletungide ennetamiseks ja tuvastamiseks, on põhjendatud vaid aset leidnud intsidente kajastavate salvestiste säilitamine. See asjaolu võib saada oluliseks näiteks olukorras, kus salvestisi on säilitatud kauem, kui nende kasutamise eesmärk eeldaks (näiteks töötajate jälgimiseks ning nende tegevuse tõendamiseks). Sellisel juhul peavad tööandjal olema adekvaatsed argumendid, mis tõendavad taoliste salvestiste säilitamise vajadust.

Jälgimisseadete alla ei liigitu aga kindlasti ainult valvekaameratega seonduv. Lisaks hõlmab see veel näiteks helisalvestite ning asukohta tuvastada võimaldavate seadmete abil kogutud informatsiooni. Tänapäevaste võimaluste juures ei olegi enam sisuliselt kohta, kus inimesed (töötajad) saaksid olla täielikult veendunud, et neid kuidagi ei jälgita („DIY stalker boxes spy on Wi-Fi users cheaply and with maximum creep value“). Ka töötaja kohta helisalvesti abil informatsiooni kogudes on tööandja kohustatud järgima kõiki nõudeid ning piiranguid, mis töötaja isikuandmete töötlemisele on kehtestatud. Näiteks ettevõtte esindustes töötaja ning klientide vahelist suhtlust salvestades on tööandja rangelt kohustatud mõlemaid vestluse osapooli sellest nõuetekohaselt teavitama. Lisaks sisaldab helisalvestise, kui isikuandmete töötlemine endas veel paljusid nüansse, mille kohta hetkel regulatsioon täielikult puudub. Hetkel puudub näiteks selge arusaam ruumidest ning keskkondadest, kus helisalvestise kasutamine on aktsepteeritav ning õigustatud.

Ka töötaja asukohta tuvastada võimaldavad sideseadmed on töötajale suureks ohuks. Näiteks on Eestis rakendatud GPS-jälgimissüsteemil põhinevat seadet ametiautode sõidupäeviku pidamiseks. Taoline süsteem suudab salvestab auto asukohaandmed

kellaajaliselt. Selline süsteem võimaldab täpselt tuvastada, kus, millal ja kaua on töötaja viibinud. Hetkel puudub aga ühene arusaam, et mida ja millisel juhul võib tööandja nende andmetega peale hakata? Kas tööandja võib jälgida taoliselt juhul auto asukohta 24 tundi ööpäevas ja 7 päeva nädalas või on jälgimine lubatud ainult konkreetsel ajavahemikul? Tänapäevases töökeskkonnas, kus soodustatakse järjest enam kaugtööd ja kus ajaraamid töö tegemiseks on järjest hägusemad, on väga keeruline töötaja töö tegemise ja eraelu aega omavahel eristada. Läbimõtlematu jälgimisseadmete kasutamine võib seega tööandjale kokkuvõttes tuua rohkem kahju kui kasu - seda eeskätt usaldamatuse õhkkonna loomise, stressi põhjustamise aga ka töötajate inimväärikuse alandamise kaudu. Lisaks peab tööandja arvestama, et igasugune filmimaterjal tekitab vägagi tihti soove selle väärkasutamiseks. See aga esitab omakorda kõrged nõudmised juba kogutud andmete nõuetekohaseks ning turvaliseks säilitamiseks. Seega on probleeme ning küsimusi, mis puudutavad töötaja jälgimist, väga palju. Järgnevas alajaotuses analüüsin selle kõige üle riikliku järelevalve teostamist.

2.3. Riiklik järelevalve

Ka töötaja isikuandmete õiguspärase töötlemise järelevalve analüüsi tuleb alustada tõdemusest, et suunised ja reeglid, milledele vastavust järelvalvet teostatavad institutsioonid peaksid kontrollima, sisuliselt puuduvad. See teeb aga järelevalve teostamise äärmiselt keeruliseks, kui mitte öelda võimatuks.

Kaks riigi institutsiooni, kelle vastutusalaga töötaja privaatsuse tagamise üle järelvalve teostamine haakub, on Tööinspektsioon (edaspidi TI) ja Andmekaitse Inspektsioon (edaspidi AKI). Esimene nendest tegeleb rohkem töötaja ja tööandja vahelise töösuhtega seonduvaga, teine aga andmekaitseliste ning otseselt töötaja privaatsusega seotud küsimustega. Üheks suureks probleemiks ongi aga nende kahe institutsiooni vastutusalade jaotumine (autori intervjuud Tööinspektsiooni ja Andmekaitse Inspektsiooni esindajatega). Kuna ka andmekaitsealane rikkumine töösuhtes on töösuhte reeglite rikkumine, siis peaks mõningate hinnangute kohaselt sellega tegelema TI. Teiselt on andmekaitsealane järelevalve väga üheselt AKI vastutada ning kuskil ei ole reguleeritud, et andmekaitsealane

järelevalve töösuhtes peaks olema selles suhtes erand. Seega hakkab järelevalvet puudutav probleemistik peale juba sellest, et ei ole üheselt selge, kes peaks taolises töötaja privaatsuse riive olukorras järelevalvet teostama ning nagu eelpool mainitud – puudub ka ühene regulatsioon, millele vastavust järelevalve peaks kontrollima. Tavaliselt nõuab töötaja privaatset töökeskkonda, tööandja seevastu õigust kontrollida töötaja tegevust, et kaitsta oma vara ja ärihuvisid. Konflikt eraelu puutumatuse ja ettevõtlusvabaduse vahel on vältimatu. Nagu eelnevalt analüüsitud - töökohustuste täitmise kontrollimise õigus ei anna tööandjale automaatselt õigust töötaja jälgimiseks kaamerast või jälgimisvõimalust andva arvutitarkvara kasutamiseks või telefoni pealtkuulamiseks, sest esiteks võib see riivata töötaja eraelu puutumatust ehk töökõnede vahele võivad sattuda ka isiklikud kõned, mille vastu tööandjal puudub õigustatud huvi, ning teiseks võib selline käitumine kahjustada kolmandate isikute huve. Näiteks helistab töötajale lähedane inimene, kes räägib talle oma terviseseisundist või analüüside tulemustest vms. Sõnumite jälgimiseks peab olema seaduslik alus – näiteks töötaja nõusolek. Samas peab sõnumi jälgimisest teadlik olema ka kolmas isik ehk see, kes sõnumi saatis või kellele sõnum saadeti. Ehk kui tööandja loeb töötaja tööpostkasti ja sellest saadetud e-kirju, siis tuleb sellest teavitada ka sõnumi saatjat või saajat, kuna see puudutab ka tema privaatsust. Praktikas ei ole aga selline lahendus kahjuks sageli mõeldav ja sellest tulenevalt tekib igati õigustatult kahtlus tööandja taolise tegevuse õiguspärasuses. Tööandja peab töötaja kohta andmete kogumisel ja säilitamisel lähtuma põhimõttest - koguda nii vähe kui võimalik ja nii palju kui vajalik, pidades seejuures silmas õigustatud huvi olemasolu kogutavate andmete suhtes.

Tänapäevases ülikiirelt arenevas infoühiskonnas (IT uudised: Nortal: IT-sektor on kasvanud kahe aastaga kolm korda), kus küberrünnakute tõttu võib olla häiritud isegi näiteks pakkide saatmine (Tarbija24: Post24 sattus küberrünnaku ohvriks), on kompetentse tööjõu leidmine info- ja kommunikatsioonisektorisse järjest keerulisem. Üha suureneva vajaduse info- ja kommunikatsioonitehnoloogia alase pädevuse järele on oma dokumendis „Eesti infoühiskonna arengukava 2020“ välja toonud ka Majandus- ja Kommunikatsiooniministeerium (Eesti infoühiskonna arengukava 2020).

Paraku on vastava kompetentsi puudumisega juba täna silmitsi ka töötaja privaatsuse üle järelevalvet teostavad institutsioonid. Nagu TI-s ja AKI-s läbi viidud intervjuudest selgus, ollakse väga suures hädas just tehnilisemate töötaja privaatsust kahjustada võivate

lahenduste kontrollimisega. Nii TI-s, kui AKI-s on pädevat IT-alast kompetentsi võrdlemisi tagasihoidlikult ning seetõttu on menetluste läbi viimine sageli raskendatud. AKI sõnul kasutavad nad aeg-ajalt sama ministeeriumi haldusalasse kuuluva Registrite ja Infosüsteemide Keskuse töötajate abi, kuid taoline lahendus ei ole esiteks kindlasti jätkusuutlik ning teiseks on taoline teise asutuse tööjõu kasutamine võimalik väga väikeses mahus. Seega on kindlasti tegemist küsimusega, millele Justiitsministeerium peaks tähelepanu pöörama ning kaaluma antud institutsiooni lisaressursside suunamist.

Seega samal ajal, kui puudub arusaam järelevalve teostajast, sellest, millele vastavust vastav institutsioon peaks järelevalvet teostama ning järelevalve teostajatel napib ka kompetentsed tööjõudu, on raske rääkida töötajate privaatsuse tagamisest ning efektiivsest järelevalvest selle tagamiseks. Mõnda aega tagasi meedias avaldatud juhtum, kus tööandja sisenes töötaja isiklikule meilikontole (IT uudised: Kuidas ettevõtja töötaja järele nuhkis?) on ilmekaks näiteks hetkel valitsevast olukorrast. Eelmisel aastal paljastunud luureskandaal (Eesti Päevaleht: Snowdeni aasta), mille kohta võib leida suure hulgal informatsiooni, on näide sellest, kus privaatsuse küsimus on üksiksiku tasemelt saanud väga aktuaalseks juba ka rahvusvahelisel tasemel. Ka intsident Eesti välisministriga annab kinnitust, et privaatsuse tagamisega on tõsiseid probleeme ka riigi kõrgeimatel isikutel (Delfi: Urmas Paeti kõnet EL välisteenistuse juhi Ashtoniga kuulati pealt).

Kokkuvõte

Antud magistritöö eesmärgiks oli saada vastus küsimusele, kas töötaja privaatsust töösuhtes on hetkel kehtivate seaduste ning regulatsioonide kohaselt tagatud, kontrollida hüpoteesi, et töötaja privaatsus töösuhtes ei ole hetkel tagatud paika pidavust ning selle tõepärasuse korral pakkuda välja võimalikud lahendused olukorra parandamiseks. Teostatud analüüsi tulemusena, kus analüüsisin eraldi alajaotustes põhjalikumalt ka peamisi töö tegemiseks kasutatavaid tehnoloogilisi lahendusi, mis võimaldavad eriti laialdaselt töötaja privaatsust riivata, võib selgelt ütelda, et töötaja isikuandmete kaitse ning privaatsus ei ole kindlasti tänasel päeval tagatud. Tööandjal on kahtlemata, tulenevalt juba töösuhte iseloomust, õigus töötajate kontrollimiseks, kuid taolisele tegevusele peavad olema kehtestatud selged piirid. Tänasel päeval võib selgelt väita, et tööandja poolse töötaja jälgimise küsimus on hetkel sisuliselt reguleerimata. Kehtivad küll väga üldsõnalised regulatsioonid, millest on tuletatavad baaspõhimõtted, mida tuleb töötaja jälgimisel silmas pidada, kuid need jätavad siiski äärmiselt palju tõlgendamisruumi ning väita, et töötaja võiks ennast privaatsuse vaatest töösuhtes turvaliselt tunda, on kindlasti väär. Antud seisukohta toetab selgelt ka töösuhtes olevate töötajate seas läbi viidud uurimus, kus koguni 91% vastanutest väitis, et tema tööandja ei ole kehtestanud arusaadavad sisemist reeglistiku töötajate isikuandmete kaitse ning privaatsuse tagamise kohta (Lisa 1, küsimus nr 9). Lisaks soovis koguni 98% vastanutest, et nende privaatsus töökohal oleks maksimaalsel võimalikul viisil tagatud (Lisa 1, küsimus nr 6).

Üheks peamiseks kitsaskohaks tööandja poolse töötaja jälgimisega seoses võibki pidada lubatu ning lubamatu piiri selgusetust. Tulenevalt asjaolust, et puudub selgus selle kohta, mis on lubatud ning mis mitte, ei ole võimalik teostada selle üle ka efektiivset järelevalvet, kuna puudub ühene regulatsioon, millele vastavust kontrollida. Nagu selgus intervjuudest nii Tööinspektsiooni, kui Andmekaitse Inspektsiooni esindajatega, on järelevalve juures lisaks probleemiks veel ka vastutusalade jaotus riigiasutuste vahel ning kompetentse tööjõu puudus.

Seega võib väga selgelt väita, et töötajate privaatsus ning isikuandmete kaitse töösuhtes on hetkel sisuliselt täielikult kaitsmata ning olukorra parandamiseks tuleks esimesel võimalusel asjakohased meetmed kasutusele võtta. Alustada tuleb selgete regulatsioonide

(seaduse) kehtestamisest, mis annaksid ühese selguse nii tööandjatele, kui ka töötajatele endile, et mis on tööandjale töötaja jälgimise juures lubatud ning mis mitte. Selleks tulenevalt tuleb lisada eraldi jaotus isikuandmete kaitse seadusesse ning teha sellest tulenevalt vajalikke muudatusi ka töölepingu seadusesse. Mh tuleks sätestada tööandjatele sisemiste töökorralduslike reeglite kehtestamise kohustus, kus oleks detailselt välja toodud kõik töötaja jälgimist ning tema privaatsuse tagamisega seonduvad asjaolud konkreetselt selle tööandja lahenduste ning võimaluste juures. Oluline selle juures on asjaolu, et seaduse tasemel ei oleks reguleeritud lihtsalt reeglite kehtestamise kohustus ise, vaid väga konkreetsed nõuded ka sellele, mida see endas peab täpsemalt sisaldama. Hoolimata asjaolust, et isikuandmete kaitse seadus on saanud juba 18 aastaseks, st selle esimene redaktsioon ilmus aastal 1996, ei ole seni peetud vajalikuks selles reguleerida isikuandmete töötlemist töösuhtes.

Järelevalve poole parandamiseks tuleb nii justiits-, kui sotsiaalministeeriumil, kelle haldusaladesse TI ja AKI kuuluvad, selgeks teha vastutusalade jaotus. Olukorras, kus pole üheselt selge, kus ühe riigiinstitutsiooni vastutusala lõppeb ning teise oma algab, on oht nn halli ala tekkeks ning suurimateks kannatajateks on lõpuks kõrgeima võimu kandjad ehk kodanikud ise. Lisaks tuleb neil institutsioonidel esimesel võimalusel leida lahendus ka kompetentse tööjõu probleemile. Järelevalve teostajal peab olema selgelt pädev ning kursis sellega, mille üle ta järelevalvet teostab. Olukorda, kus järelevalvet teostatavatel isikutel puudub piisav teadmine erinevatest tehnoloogilistest lahendustest, mille abil töötajat on võimalik järgida, ei saa rääkida efektiivsest ning toimivast järelevalvest niivõrd fundamentaalse asja üle, nagu seda on üksikisiku privaatsus.

Olukorras, kus Eestist räägitakse maailmas, kui info- ja kommunikatsioonitehnoloogia sektori ühest juhtriigist, peame me selle säilitamiseks pöörama erilist tähelepanu just selle valdkonna turvalisuse küsimustele. Seda tegemata ning veel enam, lastes erinevatel tehnoloogilistel lahendustel ning regulatsioonide puudumisel rikkuda inimeste põhiõigusi, võib Eesti e-riigi kuvand kiiresti kokku variseda. Selle vältimiseks tuleb käesoleva töö tulemuseks olevad ettepanekud võimalikult kiiresti realiseerida ning tagada inimestele nende õigused ja säilitada ka Eesti äärmiselt positiivne kuvand maailmas.

Kasutatud kirjandus

Raamatud

- Bygrave, L. A. (1988). Data protection Pursuant to the Right to Privacy in Human Rights Treaties. International Journal of Law and Information Technology, lk 255.
- Eesti Keele Instituut. (2006). Eesti keele sõnaraamat ÕS 2006. Tallinn: Eesti Keele Sihtasutus.
- Hanson, V., Laur, M. jt. (2009). Infosüsteemide turve I. Turvarisk. Tallinn: Cybernetica, lk 29–58 (ülevaade võimalikest ohtudest ja rünnakutest nii arvutitele kui ka mobiilsidele).
- Kaitsepolitsei aastaraamat. (2009), lk 14–15.
- Maruste, R (2004). Konstitutsionalism ning põhiõiguste ja vabaduste kaitse. Tallinn: Juura.
- Männiko, M. (2011). Õigus privaatsusele ja andmekaitsele. Tallinn: Juura, lk 146.
- Stanton, J., & Stam, K. (2006). The visible employee: using workplace monitoring and surveillance to protect information assets - without compromising employee privacy or trust. Medford, N.J.: Information Today
- Truuväli, E.-J., Aaviksoo B., Kask O., Lehis L., Madise L., Madise Ü., Merusk K., Mälksoo L., Narits R., Olle V., Pruks P. (2008). Eesti Vabariigi põhiseadus : kommenteeritud väljaanne. Tallinn: Juura, lk 278-279.

Akadeemilised veebiallikad

- „Eesti infoühiskonna arengukava 2020“. Arvutivõrgus kättesaadav: http://infoyhiskond.eesti.ee/files/Infoyhiskonna_arengukava_2020_f.pdf
- Eesti Vabariigi põhiseadus. 22.07.2011 – RT I, 27.04.2011, 2. Arvutivõrgus: https://www.riigiteataja.ee/akt/127042011002

- Euroopa andmekaitseasutuste töörühma dokument „Working document on the surveillance of electronic communications in the workplace", 2002. Arvutivõrgus kättesaadav: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp55_en.pdf
- Euroopa Parlamendi ja EL Nõukogu direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. EÜT L 281, 23.11.1995. Direktiivi on muudetud määrusega (EÜ) nr 1882/2003. ELT L 284, 31.10.2003. Arvutivõrgus: http://eur-lex.europa.eu/legal-content/ET/ALL/;ELX_SESSIONID=LxhGJWLQkvq2x5bHpq4XhvHf2LChzJpbQv1QykZ4RT5H85nMrr78!-844008730?uri=CELEX:31995L0046
- Inimõiguste ja põhivabaduste kaitse konventsioon. 16.04.1996 – RT II 1996, 11, 34. Arvutivõrgus: https://www.riigiteataja.ee/akt/13073654
- Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon. 01.03.2002 – RT II 2001, 1, 3. Arvutivõrgus: https://www.riigiteataja.ee/akt/78300
- Isikuandmete kaitse seadus. 01.01.2011 – RT I, 30.12.2010, 11. Arvutivõrgus: https://www.riigiteataja.ee/akt/78300
- Karistusseadustik. 01.04.2014 - RT I 2001, 61, 364. Arvutivõrgus: https://www.riigiteataja.ee/akt/121062014028
- Kirst, O. (2012, juuni). Sõnumisaladuse kaitse tööandja sidevahendi kasutamisel. Juridica. Arvutivõrgus: http://juridica.ee/juridica_et.php?document=et/articles/2012/6/215927.SUM.php
- Laki yksityisyyden suojasta työelämässä. Arvutivõrgus: http://www.finlex.fi/en/laki/kaannokset/2004/en20040759.pdf
- Lane, F (2003). The Naked Employee: How Technology Is Compromising Workplace Privacy. New York : AMACOM. Arvutivõrgus: http://books.google.se/books?id=bd2_Vn3jczYC&printsec=frontcover&hl=et#v=onepage&q&f=false
- Riigi Infosüsteemi Ameti ISKE ohtude kataloog ver. 7.00. Arvutivõrgus: https://www.ria.ee/iske-dokumendid

- Turvaseadus. 01.09.2013 - RT I, 11.07.2013, 17, §11 lg3. Arvutivõrgus: https://www.riigiteataja.ee/akt/129062014088
- Töölepingu seadus. 01.04.2013 – RT I, 22.12.2012, 30. Arvutivõrgus: https://www.riigiteataja.ee/akt/122122012030
- Võlaõigusseadus. 09.12.2013 - RT I, 29.11.2013, 4. Arvutivõrgus: https://www.riigiteataja.ee/akt/111042014013

Mitteakadeemilised veebiallikad

- „DIY stalker boxes spy on Wi-Fi users cheaply and with maximum creep value“ Arvutivõrgus: http://arstechnica.com/security/2013/08/diy-stalker-boxes-spy-on-wi-fi-users-cheaply-and-with-maximum-creep-value/ (wwwarstechnica.com, viimati vaadatud 14.12.2014)
- „Edward Snowden: ma ei taha elada ilmas, kus kõik mu tehtu ja öeldu talletatakse“ Arvutivõrgus: http://epl.delfi.ee/news/valismaa/edward-snowden-ma-ei-taha-elada-ilmas-kus-koik-mu-tehtu-ja-oeldu-talletatakse.d?id=66269340 (Eesti Päevaleht, viimati vaadatud 14.12.2014)
- „Gartner Predicts by 2017 - Half of Employers will Require Employees to Supply Their Own Device for Work Purposes“ Arvutivõrgus: http://www.gartner.com/newsroom/id/2466615 (Gartner, viimati vaadatud 14.12.2014)
- „Kuidas ettevõtja töötaja järele nuhkis?“ Arvutivõrgus: http://www.ituudised.ee/article/2013/11/22/kuidas-ettevotja-tootaja-jarele-nuhkis (IT Uudised, viimati vaadatud 14.12.2014)
- „Nortal: IT-sektor on kasvanud kahe aastaga kolm korda“ Arvutivõrgus: http://www.ituudised.ee/article/2013/11/21/nortal-it-sektor-on-kasvanud-kahe-aastaga-kolm-korda (IT Uudised, viimati vaadatud 14.12.2014)
- „NSA kuulas pealt 35 maailma riigijuhi telefonikõnesid“ Arvutivõrgus: http://www.delfi.ee/news/paevauudised/valismaa/nsa-kuulas-pealt-35-maailma-riigijuhi-telefonikonesid.d?id=66972608&utm_source=feedburner&utm_medium=feed

&utm_campaign=Feed%3A+delfiuudised+%28DELFI+%3E+K%C3%B5ik+uudised%29 (Delfi, viimati vaadatud 14.12.2014)

- „Nuhkimine tööpostil“ Arvutivõrgus: http://www.aripaev.ee/Default.aspx?PublicationId=299535a0-812e-45ea-9802-c98e8d9e8cc5 (Äripäev, viimati vaadatud 14.12.2014)
- „Post24 sattus küberrünnaku ohvriks“ Arvutivõrgus: http://tarbija24.postimees.ee/2731808/post24-sattus-kuberrunnaku-ohvriks (Tarbija24, viimati vaadatud 14.12.2014)
- „Snowdeni aasta“ Arvutivõrgus: http://epl.delfi.ee/news/valismaa/snowdeniaasta.d?id=67521064 (Eesti Päevaleht, viimati vaadatud 14.12.2014)
- „Urmas Paeti kõnet EL välisteenistuse juhi Ashtoniga kuulati pealt“ Arvutivõrgus: http://www.delfi.ee/news/paevauudised/eesti/urmas-paeti-konet-el-valisteenistuse-juhi-ashtoniga-kuulati-pealt.d?id=68176199 (Delfi, viimati vaadatud 14.12.2014)

Euroopa Inimõiguste Kohtu lahendid

- EIÕK 16.12.1992 nr 13710/88, Niemietz vs. Saksamaa. Arvutivõrgus: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57887#{"itemid":["001-57887"]}
- EIÕK 25.06.1997 nr 20605/92, Halford vs Ühendkuningriik. Arvutivõrgus: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58039#{"itemid":["001-58039"]}
- EIÕK 03.07.2007 nr 62617/00, Copland vs. UK. Arvutivõrgus: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-79996#{"itemid":["001-79996"]}

Resume in English

„Workplace as a Danger to Employee's Privacy"

The aim of the given thesis is to get answer to question that is employee's privacy at the moment ensured in the best possible way and if not, then propose solutions to make situation better. Info- and communication technology has been developed so fast that other world have had difficulties to stay on the board. There are lot of different solutions which enables employers to follow their employees and list of such solutions is getting longer basically every day. My hypothesis, that I checked, was that today we don't have clear understanding and regulations which are answering to question - what is allowed for employeers to check their employees and what is clearly prohibited? Is there a clear balance between employees and employers rights, obligations and interests? Can we say that employee's privacy is at the moment ensured on best possible way? Is there effective supervisioning about employee's privacy?

Through my analysis I became to conclusion that my hypthesis is true – there is no clear understanding and regulations about employees and employers rights and it can be almost said that employers can do with employees privacy and personal data what ever they want. Because there are no clear regualations, it is also almost impossible to supervise it by the state. And if we add here other problems (for example two state authorities doesn't have clear conclusion, who should supervise such cases), it can be said that there almost isn't such thing as employee's privacy in his workplace anymore. Technical solutions I analysed in my thesis are the biggest and main opportunities for empoyers to collect data about their employees, but there are also many others.

For conclusion it can be said that employee's privacy in his workplace is in a big danger at the moment and it isn't almost possible to talk about such thing. State should find a solution to this question on a first opportunitie. State have had Personal Data Act for 18 years now and during this period no regulation about employee's privacy hasn't regulated there. In my oppinnion it is latest time to do it now.

Lisad

Lisa 1

Juhusliku valimi alusel koostatud küsimustik, millele vastasid 117 hetkel töösuhtes olevat töötajat:

Nr	Küsimus	JAH	EI
1.	Kas Sa tead, mis on isikuandmed?	78%	22%
2.	Kas Sa tead hästi oma õigusi seoses enda isikuandmete kaitsega?	24%	76%
3.	Kas osadel inimestel (nt avaliku elu tegelastel) on suurem õigus oma isikuandmete ja privaatsuse kaitsele?	73%	27%
4.	Kas tunnetad, et tehnoloogia areng on ohtu sinu iskuandmete kaitsele ning privaatsusele töökohas vähendanud?	18%	82%
5.	Kas oled teadlik, millisel määral Sind töökohal jälgitakse?	5%	95%
6.	Kas sooviksid, et Sinu privaatsus töökohal oleks maksimaalsel võimalikul viisil tagatud ning tööandja kontrolliks Sind nii vähesel määral, kui võimalik?	98%	2%
7.	Kas privaatsus on seotud üksnes inimese koduga?	13%	87%
8.	Kas Sind häiriks, kui Sinu töökohale oleks suunatud kaamera või Sinu tööle tuleku ning lahkumise aega jälgitakse igapäevaselt?	2%	98%
9.	Kui Sinu tööandja on töötajate privaatsuse ning isikuandmete kaitseks kehtestanud reeglistiku, siis kas see annab Sulle piisavalt selge ülevaate lubatust ning lubamatust?	11%	89%
10.	Kas tööandjal peab töötaja isikuandmete töötlemiseks temalt alati luba küsima?	81%	19%
11.	Kas usud, et tööandjale oma isikuandmete töötlemiseks nõusoleku andmata jätmisel võid tunda ennast muretult hilisemate negatiivsete tagajärgede osas?	14%	86%
12.	Kas tööandjal on õigus töödelda töötaja isikuandmeid ka asjaoludel, mis ei ole töösuhtega seotud?	11%	89%
13.	Kas kasutad tööalast e-posti aadressi või telefoni ka eraelulistel eesmärkidel?	95%	5%
14.	Kas sinu jaoks on aktsepteeritav, kui tööandjal on ligipääs Sinu tööalasele e-kirjade postkastile ning Sinu töötelefonilt tehtud kõnesid salvestatakse?	43%	57%
15.	Kas sooviksid võimalusel töö tegemiseks kasutada isiklikku seadet (sülearvuti, mobiiltelefon)?	57%	43%