TARTU ÜLIKOOL

SOTSIAALTEADUSTE VALDKOND

ÕIGUSTEADUSKOND

Eraõiguse osakond

Katrin Kullamäe

TÖÖTAJA ISIKUANDMETE KAITSE TEHNOLOOGILISTE VAHENDITE ARENGU KONTEKSTIS

Magistritöö

Juhendaja

Prof. Merle Erikson

Tartu

2019

SISUKORD

SISSEJUHATUS **4**

1. ISIKUANDMETE TÖÖTLEMINE TÖÖSUHTES **8**

1.1. TÖÖANDJA ISIKUANDMETE TÖÖTLEJANA 8
1.2. TÖÖTAJA ISIKUANDMETE TÖÖTLEMISE ALUSED 10
1.3. TÖÖTAJA ISIKUANDMETE TÖÖTLEMISE PÕHIMÕTTED 13

2. PILTI, HELI VÕI SIGNAALI EDASTAVATE SEADMETE KAUDU KOGUTUD TÖÖTAJA ISIKUANDMETE TÖÖTLEMINE **16**

2.1. PILTI, HELI VÕI SIGNAALI EDASTAVATE SEADMED TÖÖKOHAL 16
2.2. KAAMERA 18
2.2.1. KAAMERA KASUTAMISE VÕIMALUSED TÖÖKOHAL 18
2.2.2. ÕIGUSLIK ALUS KAAMERA KASUTAMISEKS 19
2.2.3. KAAMERA KASUTAMISE PÕHIMÕTTED 23
2.3. ASUKOHA MÄÄRAMISE SEADE 27
2.3.1. ASUKOHA MÄÄRAMISE SEADME KASUTAMINE TÖÖSUHTE KONTEKSTIS 27
2.3.2. ÕIGUSLIK ALUS ASUKOHA MÄÄRAMISE SEADME KASUTAMISEKS 28
2.3.3. ASUKOHA MÄÄRAMISE SEADME KASUTAMISE PÕHIMÕTTED 30
2.4. RAADIOSAGEDUSTUVASTUSEL PÕHINEV IDENTIFITSEERIMISTEHNOLOOGIA 31
2.4.1. RAADIOSAGEDUSTUVASTUSEL PÕHINEVA TEHNOLOOGIA KASUTAMINE TÖÖSUHTE KONTEKSTIS 31
2.4.2. ÕIGUSLIK ALUS RAADIOSAGEDUSTUVASTUSEL PÕHINEVATE SEADMETE KASUTAMISEKS 32
2.4.3. RAADIOSAGEDUSTUVASTUSEL PÕHINEVATE SEADMETE KASUTAMISE PÕHIMÕTTED 33
2.5. KONTAKTIVABA LÄHIVÄLJA IDENTIFITSEERIMISTEHNOLOOGIA 34
2.5.1. KONTAKTIVABA LÄHIVÄLJA IDENTIFITSEERIMISTEHNOLOOGIA KASUTAMINE TÖÖSUHTE KONTEKSTIS 34
2.5.2. TÖÖTAJA BIOMEETRIAL PÕHINEVA IDENTIFITSEERIMISTEHNOLOOGIA KASUTAMISE VÕIMALUSED 34
2.5.3. ÕIGUSLIK ALUS BIOMEETRILISTE ISIKUANDMETE TÖÖTLEMISEKS 36
2.5.4. NAHAALUSTE KIIPIDE KASUTAMISE VÕIMALUSED 37
2.5.5. ÕIGUSLIK ALUS NAHAALUSTE KIIPIDE KASUTAMISEKS 38

3. INFO- JA KOMMUNIKATSIOONITEHNOLOOGIAVAHENDITE NING SOTSIAALMEEDIA KAUDU KOGUTUD ISIKUANDMETE TÖÖTLEMINE **41**

3.1. KOMMUNIKATSIOON KAASAEGSES TÖÖKESKKONNAS 41
3.2. TELEFON 42
3.2.1 ÕIGUSLIK ALUS TELEFONIKÕNEDE SALVESTAMISEKS 42
3.2.2. TELEFONIKÕNEDE SALVESTAMISE PÕHIMÕTTED 45
3.2.3. ÕIGUSLIK ALUS KÕNEERISTUSE ANLÜÜSIMISEKS 46
3.2.4. KÕNEERISTUSE ANALÜÜSIMISE PÕHIMÕTTED 48
3.3. ARVUTI 49
3.3.1. ARVUTIKASUTUSE JÄLGIMISE VÕIMALUSED 49
3.3.2. ARVUTIKASUTUSE JÄLGIMISE ÕIGUSLIK ALUS 51
3.3.3. ARVUTIKASUTUSE JÄLGIMISE PÕHIMÕTTED 54
3.4. INTERNETIKASUTUSE JÄLGIMINE 55
3.4.1. INTERNETIKASUTUSE JÄLGIMISE ÕIGUSLIK ALUS 55
3.4.2. INTERNETIKASUTUSE JÄLGIMISE ÜLDPÕHIMÕTTED 56
3.5. E-POSTI KASUTAMISE JÄLGIMINE 58
3.5.1. ÕIGUSLIK ALUS TÖÖTAJA E-POSTI JÄLGIMISEKS 59

3.5.2. E-POSTI JÄLGIMISE PÕHIMÕTTED 62
3.6. INFO JA KOMMUNIKATSIOONITEHNOLOOGIA VAHENDITE KASUTAMISE EESKIRJA KEHTESTAMISE VAJADUS 64
3.7. SOTSIAALMEEDIA JÄLGIMINE 67
3.7.1. ÕIGUSLIK ALUS TÖÖTAJA SOTSIAALMEEDIA JÄLGIMISEKS 67
3.7.2. TÖÖTAJA SOTSIAALMEEDIA JÄLGIMISE PÕHIMÕTTED 70
KOKKUVÕTE 72
SUMMARY 78
KASUTATUD LÜHENDID 84
KASUTATUD KIRJANDUS 85
KASUTATUD ÕIGUSAKTID 92
KASUTATUD KOHTULAHENDID 93

Sissejuhatus

Üha ulatuslikumaks muutuv isikuandmete kogumine ja töötlemine vähendab andmesubjekti kontrolli oma andmete käitlemise üle. Kuna info- ja kommunikatsioonitehnoloogia areng võimaldab isikuandmeid massiliselt koguda ja töödelda, kujutab seesugune tegevus ohtu üksikisiku eraelu puutumatusele ning üldisele isiksusõigusele: erinevad andmeid kombineerides on võimalik luua võrdlemisi terviklik pilt isiku omadustest, harjumustest, suhetest, varalisest seisust jms. ning seeläbi kaudselt inimest jälgida.[1] Tehnoloogia areng on tänasel päeval nii kaugel, et tööandjal on võimalik töötajaid pidevalt jälgida nii töökohas kui ka töötaja kodus mitmesuguste seadmete abil, nagu nutitelefonid, arvutid, tahvelarvutid, sõidukid jne. Seeläbi on tööandjal võimalik luua terviklik ettekujutus töötajast, mille saavutamine on reeglina võimalik üksnes privaatse elu tulemusena.[2] Isikuandmete töötlemine, mis väljendub töötaja või tema kasutuses olevate info- ja kommunikatsioonitehnoloogia (edaspidi IKT) vahendite jälgimises, kujutab endast fokusseeritud, süstemaatilist ja rutiinset tähelepanu isiku personaalsetele detailidele, mille eesmärgiks on mõjutamine, kontrollimine või suunamine.[3]

Tuginedes IBM-i (*International Business Machines corporation*) seisukohale, on viimase kahe aasta jooksul tekkinud rohkem andmeid, kui varasemate perioodide andmemaht kokku.[4] Just andmemahtude plahvatuslik kasv, informatsiooni väärtuse tõus ning üha enam võimalusi isikuandmete töötlemiseks on loonud vajaduse ja aluse isikuandmete töötlemise piirangutele. Olukorras, kus töötlemisreegleid pole või neid rakendatakse vääralt, võib töösuhte kontekstis tekkida olukord, kus inimene jääb heast tööpakkumisest ilma või kaotab oma töö. Kui isikuandmete töötlemise piiranguid ei oleks, võib esineda oht, et tööandjate õigustatud huvid tõhususe suurendamisel ja ettevõtte varade kaitsmisel muutuvad põhjendamatuks ja sekkuvaks jälgimiseks.

Isikuandmete töötlemisele kehtestatud reeglite eesmärk ei ole loomulikult üksnes andmete kaitse, vaid nende seostuvate isikute põhiõiguste- ja vabaduste kaitse. Isikuandmete töötlemise reeglite

[1] T. Ilus. Andmesubjekti osaluse põhimõte Euroopa Nõukogu konventsioonide ning Euroopa Inimõiguste kohtu lahendite valguses. Juridica VIII/2005, lk 522

[2] E. Palm. Privacy Expectations at Work – What is Reasonable and Why? - The Royal Institute of Technology Stockholm. Lk 10. Arvutivõrgus: https://ecpr.eu/Filestore/PaperProposal/f0449221-bc1a-46d7-98c0-fbff05c57826.pdf, (27.02.2019).

[3] D. Lyon. Surveillance Studies. An overview. Oxford. Polity Press. 2007 lk 471

[4] A. Hartshorn. Transparency and consent. Why data protection legislation is getting stricter? – Real business. 04/2017 Arvutivõrgus: https://realbusiness.co.uk/data-protection-legislation-getting-stricter/, (19.02.2019).

kaudu on võimalik tagada, et inimeste õiguseid ja vabadusi lubamatult ei riivataks.[5] Töötaja isikuandmete töötlemisel tuleb eelkõige arvestada selliste põhiõigustega nagu õigus eraelu puutumatusele, õigus sõnumisaladusele ning õigus vabale eneseteostusele. Põhiseaduse põhiõiguste kataloog ei sätesta eraldi õigust inimväärikusele, ent kuna see kujutab endast üht põhiseaduse aluspõhimõtetest[6], peab isikuandmete töötlemine olema sellega kooskõlas. Isikuandmete töötlemine, mis väljendub töötaja või tema kasutuses olevate IKT vahendite jälgimises, võib sõltuvalt jälgimisviisist olla inimväärikust alandav.[7]

Õigus eraelu puutumatusele, ei ole siiski absoluutne põhiõigus, mis tähendab seda, et õigusliku aluse olemasolul on selle riivamine lubatud.[8] Küll aga peab privaatsust riivav isikuandmete töötlemine olema põhjendatud, proportsionaalne ning riivama töötaja privaatsust minimaalselt. Tööandja peab arvestama, et eraelu kaitsega võib olla tagatud ka töökoht, sest eraelu hõlmab lisaks kõigele muule ka õigust luua ja arendada suhteid teistega. Ei ole mingit põhust, miks eraelu mõiste alt peaks välja jätma tööalase tegevuse, sest võimalus välismaailmaga suhteid arendada on märkimisväärne, kui mitte suurim, just tööelu raames.[9] Ka Euroopa andmekaitseasutuste töörühm on märkinud, et töötaja ei jäta oma eraelu ja privaatsust igal hommikul tööle tulles töökoha ukse taha, sest märkimisväärne osa inimese elust on just seotud töö ja töökohaga.[10]

Seoses IKT kiire arenguga on saanud võimalikuks ja sagenenud ulatuslikud tööandjapoolsed andmekaitse rikkumised, mistõttu on tööõigusliku isikuandmete kaitse muutumas üha olulisemaks ja aktuaalsemaks valdkonnaks. Tänapäevast infoühiskonda iseloomustab enim just informatsiooni rohkus ja selle kättesaadavus. Võrku on ühendatud nii töötajate arvutid ja autod, kasutusel on mitmesugused jälgimisseadmed ja tarkvarad, mille kaudu on tööandjal võimalik omandada suures koguses informatsiooni oma töötajate kohta jne. Teema aktuaalsust kinnitab ka 2018 aastal toimunud andmekaitseõiguse ühtlustamise eesmärgil ja privaatsuse kaitse tõhusamaks kaitseks

[5] K. Sarap. S. Kuusik. Kolm põhjust, miks me vajame nii karme andmekaitse reegleid. Arvutivõrgus: https://www.njordlaw.com/et/kolm-pohjust-miks-vajame-nii-karme-andmekaitse-reegleid/, (22.02.2019).
[6] Põhiseadus § 10. RT I, 15.05.2015, 2.
[7] Andmekaitse inspektsioon. Isikuandmete töötlemine töösuhtes. Abistav juhendmaterjal. Lk. 69. Arvutivõrgus: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikuandmed%20t%C3%B6%C3%B6suhetes%20juhendmaterjal26%2005%202014_0.pdf. (10.01.2019).
[8] M. Männiko. Õigus privaatsusele ja andmekaitse. Tallinn. Juura 2011, lk 34.
[9] Andmekaitse inspektsioon. Isikuandmete töötlemine töösuhtes. Abistav juhendmaterjal. Lk 8. Arvutivõrgus: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikuandmed%20t%C3%B6%C3%B6suhetes%20juhendmaterjal26%2005%202014_0.pdf. (10.01.2019).
[10] Article 29 Data Protection Working Party. Working document on the surveillance of electronic communications in the workplace, 29.05.2002, lk 4. Arvutivõrgus: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdf (14.02.2019).

toimunud andmekaitse reform, mille käigus kehtestati Euroopa Liidu liikmesriikidele otsekohalduv Euroopa Parlamendi ja nõukogu määrus füüsiliste isikute kaitse kohta isikuandmete töötlemisel.

Teema asjakohasust rõhutab autori hinnangul ka see, et käesoleval hetkel puudub konkreetne regulatsioon, mis annaks tööandjale selged juhtnöörid töötaja või tema kasutuses olevate IKT vahendite jälgimiseks. Vaatamata seesuguse andmetöötluse riskantsusele, lähtuvad tööandjad üldsõnalistest ja abstraktsetest õigusaktidest, Andmekaitse Inspektsiooni (edaspidi AKI) juhistest, vähemal määral ka Euroopa andmekaitse töörühma juhenditest ning kohtupraktikast. Kuigi nii AKI kui ka Euroopa andmekaitse inspektori juhendid on põhjalikud, on nad oma iseloomult üksnes soovituslikku laadi. Arvestades tehnoloogia arengut, teisenenud töökeskkonda ning toimunud andmekaitse reformi, on AKI 2011. aastal koostatud juhis autori hinnangul osaliselt vananenud ning vajab täiendamist. Sõnaselget sätet, mis annaks tööandjale õiguse või keelaks töötajate kaameraga filmimise, arvutikasutuse monitoorimise või kommunikatsioonivahendite kaudu edastatava info jälgimiseks või kontrollimiseks ei ole. Seetõttu on ka tööandjatel keeruline otsustada, millal on töötajate jälgimine õigustatud ning millal on tegemist õigusvastase tegevusega. Teema olulisust ja aktuaalsust kinnitab ka sage meediakajastus ja teemakohaste publikatsioonide arv.

Käesoleva magistritöö eesmärgiks on leida vastus küsimusele, kas tehnoloogiliste vahendite arengu kontekstis on töötajate isikuandmete kaitse tagatud andmekaitse üldreeglite alusel või on vajalik tööõigusliku eriregulatsiooni kehtestamine. Eesmärgi saavutamiseks analüüsib autor, kas olukorras, kus tehnoloogia kiire areng on toonud kaasa üha rohkem ja paremaid tehnoloogilisi võimalusi töötaja kontrollimiseks ja jälgimiseks, on tagatud töötaja isikuandmete kaitse või nende kasutamine riivab töötaja õigust isikuandmete kaitsele ning seeläbi ohustab töötaja privaatsust. Autor analüüsib töökeskkonnas levinud aga ka uuemaid tehnoloogilisi lahendusi, mille kaudu kogutud andmete abil on võimalik töötajate jälgimine, hinnates nende õiguslikku alust ja vastavust andmekaitse üldpõhimõtetele.

Magistritöö koosneb kolmest peatükist, mis jaotuvad omakorda alapeatükkideks ning milles antakse ülevaade isikuandmete töötlemise alustest ja üldpõhimõtetest; samuti on magistritöös välja toodud ja analüüsitud isikuandmete töötlemise õiguspärasust ja andmekaitse üldpõhimõtetele vastavust erinevate töötaja või tema kasutuses olevate IKT vahendite kaudu. Magistritöös käsitletakse lisaks klassikalistele jälgimisviisidele IKT arengu kontekstis ka uudseid ja vähem levinud võimalusi töötajate jälgimiseks.

Magistritöö esimeses peatükis antakse ülevaade isikuandmete töötlemise võimalikest õiguslikest alustest töösuhte kontekstis. Lisaks on analüüsitud andmekaitse üldpõhimõtteid tööõigusliku isikuandmete töötlemise vaatenurgast.

Magistritöö teises peatükis on välja toodud, millistel õiguslikel alustel on tööandjal lubatud töödelda erinevate jälgimisseadmete kaudu kogutud andmeid. Analüüsitavateks jälgimisseadmeteks on video- ja valvekaamerad, asukoha määramise ehk GPS seadmed (inglise keeles *Global Positioning System*), raadiosagedustuvastusel põhinev identifitseerimistehnoloogia (inglise keeles *radio frequency identification*) ning kontaktivaba lähivälja identifitseerimistehnoloogia (inglise keeles *near field communication*).

Käesoleva magistritöö viimases peatükis käsitletakse, millistel õiguslikel alustel on töötaja IKT vahendite ning sotsiaalmeedia kaudu kogutud isikuandmete töötlemine õiguspärane. Esimese IKT vahendina on käsitletud telefoni, mille kaudu saab isikuandmeid töödelda telefonikõnede salvestamise ja pealtkuulamise või kõneeristuse, ehk nn. liiklusandmete analüüsimise teel. Teiseks analüüsitavaks IKT vahendiks on arvuti: eraldiseisvalt on hinnatud arvutikasutuse, interneti kasutuse ning e-kirjade jälgimise kaudu kogutud isikuandmete õiguspärasust ja andmekaitse üldpõhimõtetele vastavust.

Autor toob välja peamiste lõputöö allikatena isikuandmete kaitse ja tööõiguse valdkondi reguleerivad rahvusvahelised ja siseriiklikud õigusaktid, eelkõige isikuandmete kaitse üldmäärus, isikuandmete kaitse seadus, isikuandmete kaitse rakendamise seadus ja töölepingu seadus. Samuti on allikatena kasutatud direktiivi 95/46/EÜ artikli 29 alusel asutatud andmekaitse töörühma suuniseid, Andmekaitse Inspektsiooni juhiseid ning Euroopa Inimõiguste Kohtu praktikat. Lisaks õigusteaduse erialakirjandusele ja asjakohastele teadusartiklitele, on töö kirjutamisel kasutatud ka IKT valdkonda puudutavat kirjandust.

Magistritöö autor avaldab tänu oma lõputöö juhendajale, Merle Eriksonile, kelle ideed ja ettepanekud ajendasid töös käsitletavat teemat laiemalt uurima ning kelle asjalikud soovitused ja parandused on väärtuslikuks abiks käesoleva töö kirjutamisel.

Magistritööd iseloomustavateks märksõnadeks on privaatsus, tehnoloogia areng, andmekaitse, isikuandmed.

1. Isikuandmete töötlemine töösuhtes

1.1. Tööandja isikuandmete töötlejana

Tööandja näol on tegemist alati isikuandmtete töötlejaga, sest ainuüksi töötaja nimi, isikukood, info elukoha kohta jms kujutavad endast isikuandmeid. Isikuandmete töötleja staatuse omandab tööandja enne töösuhte vormistamist töötajate värbamise protsessis, samuti jätkub isikuandmte töötlemine töölepingu lõppemise järgselt.

Isikuandmete töötlemist töösuhtes iseloomustavad vastandlikud huvid ja põhiõigused, kõrge abstraktsusega õigusnormid, era ja avaliku õiguse segunemine.[11] Töölepinguline suhe töötaja ja tööandja vahel on olemuselt keeruline, ning omavahel võivad põrkuda eelkõige ühe poole põhiõigused- ja vabadused ning teise poole majanduslikud huvid. Kuigi lepinguõiguslikust vaatepunktist on töösuhte pooled võrdsed, iseloomustab traditsioonilist töötaja ja tööandja vahelist suhet pigem (range) alluvussuhe, kus tööandjal on õigus anda korraldusi, kontrollida tööd ning töötaja on kohustatud alluma tööandja korraldustele ja juhistele.[12] Töösuhet iseloomustab ühelt poolt tööandja huvi saada töötajalt minimaalsete vahenditega maksimaalne tulu ning seisukoht, et töötaja on tööandjaga võrreldes nõrgemas positsioonis. Õigusteoorias ollakse veendumusel, et tööandjapoolse kontrollfunktsiooni teostamisel kollideeruvad tööandja ettevõtlusvabadus ning töötaja eraelu kaitse ja enesemääramisõigus.[13]

Töösuhetes vastanduvad üha enam töötajate ja tööandjate huvid seoses andmete ja informatsiooniga seotud valdkondades. Kõige laiemas tähenduses võib töötaja peamiseks huviks pidada võimalikult vähest andmetöötlust tööandja poolt (s.h. minimaalne kontrollimine, jälgimine). Isikuandmete kaitse reeglid ongi suunatud privaatsuse kaitsele. Privaatsus kõige laiemal tasandil on soov olla rahule jäätud, olla vaba ning omaette – loomulikult, sundimatult ning jälgimata.[14] Tööandja vastupidiselt on huvitatud oma töötaja kogemuste, teadmiste aga ka harjumuste kohta võimalikult suurel määral teabe saamisest. Reeglina ei ole tööandja eesmärgiks

---

[11] Andmekaitse inspektsioon. Isikuandmete töötlemine töösuhtes. Abistav juhendmaterjal. Arvutivõrgus: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikuandmed%20t%C3%B6%C3%B6suhetes%20juhendmaterjal26%2005%202014_0.pdf, (10.01.2019).

[12] Riigikohtu tsiviilkolleegiumi 31. märts 2008 a. Otsus tsiviilasjas nr. 3-2-1-13-08.

[13] K. Randveer. Isikuandmete kaitse töötaja värbamisprotsessis – väljakutse tööandjale. Lk 19. Magistritöö. Tallinn 2011. Arvutivõrgus: https://www.toooigusabi.ee/failid/Upload/tooted_failid/MAG_TOO_Isikuandmete_kaitse_tootaja_varbamisprotsessis_Kadri_Randveer.pdf , (15.02.2019).

[14] R. Wacks. Privacy. A Very Short Introduction. Oxford University Press, 2010, Lk. 30

seejuures kahjustada töötaja õigust privaatsusele, vaid pigem on tööandjal siiras soov luua motiveeritud, pädev ja lojaalne meeskond. Kuna aga tööandja jaoks oluline informatsioon võib paratamatult seostuda isikute eraeluga, on konflikt sageli vältimatu. Ehk isikuandmete töötlemisel töösuhte kontekstis on olemuselt tihedalt seotud privaatsusõigusega. On selge, et isikuandmete kogumine, säilitamine, kasutamine ja avalikustamine võib kaasa tuua otseseid või kaudseid tagajärgi eraelu puutumatusele.[15] Teatud ulatuses peavad töötajad oma ootuseid privaatsusõigusele töösuhtes vähendama, sest teatavat isiklikku informatsiooni peavad nad tööandjaga jagama. Näiteks töötaja nimi ja isikukood on vajalikud töölepingu sõlmimiseks ning töötaja riiklikusse töötajate andmebaasi (MTA töötajate register) kandmiseks. Töötaja pangakonto number on seevastu vajalik raamatupidamisele töötasu ja muude tasude maksmiseks jne. Ka meedias palju kajastatud informatsioon laste olemasolu ja sünniaegade kohta võib tööandja jaoks vajalikuks osutada, eelkõige TLS-I täitmisest tulenevate otsuste langetamisel. Ehk kokkuvõtvalt võib öelda, et isikuandmeid töötlevad enamik ettevõtjatest – kui mitte põhitegevuse raames, siis kindlasti seoses tööõigusega.[16]

Vaatamata sellele, et andmekaitsest kõneldes rõhutatakse valdavalt just piiranguid ja keelde, mis ei luba isikuandmeid vabalt töödelda, tuleb isikuandmete töötlemise piiramisele suunatud andmekaitsereeglitest rääkides lähtuda siiski eeldusest, et isikuandmete töötlemine on vajalik. Vastasel juhul ei oleks andmekaitse põhimõtteid vajagi, vaid piisaks ainsast ühemõttelisest reeglist: isikuandmete töötlemine on keelatud.[17] Nagu eelpool mainitud, siis peavad tööandjad arvestama, et mitmete rutiinsete tegevustega töösuhtes kaasneb isikuandmete töötlemine, mõnel juhul ka eriliiki isikuandmete töötlemine,[18] mis kinnitab, et kuigi andmed on kaitstud põhiõigustega, ei tähenda see veel andmete töötlemise keeldu.[19] Töösuhet, millega ei kaasne isikuandmete töötlust ei ole tänases ühiskonnas võimalik ette kujutada Liigne andmetöötlus tööandja poolt pole samuti kooskõlas tänaste väärtustega, mistõttu on oluline rääkida andmetöötluse võimalustest ja piirangutest.

[15] L. Wildhaber. O. Diggelmann. Euroopa inimõiguste konventsioon ja eraelu kaitse. Uuemad arengusuunad. – Juridica 01/2007. Lk 5

[16] Seletuskiri isikuandmete kaitse seaduse juurde. Lk 55. Arvutivõrgus: https://www.koda.ee/sites/default/files/content-type/content/2018-05/Seletuskiri%20%282%29.pdf, (25.02.2019).

[17] T. Ilus. Andmesubjekti osaluse põhimõte Euroopa Nõukogu konventsioonide ning Euroopa Inimõiguste Kohtu lahendite valguses. – Juridica 2005/8. Lk 522.

[18] Article 29 Data Protection Working Party. Opinion 8/2001 on the processing of personal data in the employment context, lk 19. Arvutivõrgus. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf (20.02.2019).

[19] I. Pilving. Õigus isikuandmete kaitsele. – Juridica VIII/2005. Lk. 536

Töölepinguseaduse § 41 lg 2 kohaselt peab tööandja tagama töötaja isikuandmete töötlemise vastavalt õigusaktides sätestatule. Alates 25. maist 2018 reguleerib isikuandmete kaitse valdkonda Euroopa Parlamendi ja nõukogu otsekohalduv määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (edaspidi üldmäärus), millel on keskne roll Euroopa andmekaitse õiguses. Kuigi üldmäärus on EL-i liikmesriikide jaoks otsekohalduv, jätab see teatud küsimustes liikmesriikidele kaalutlusõiguse riigisiseselt täpsustada, kehtestada ja säilitada üldmääruses sätestatud isikuandmete töötlemisega seotud tingimusi.[20]

Üldmääruse eesmärk on aidata kaasa vabadusel, turvalisusel ja õigusel põhineva majandusliidu saavutamisele, majanduslikule ja sotsiaalsele arengule, Euroopa Liidu majanduse tugevdamisele ja lähendamisele ning füüsiliste isikute heaolule.[21] Andmekaitse üldmäärust kritiseeritakse peamiselt seetõttu, et selle üldsõnalisus võib kaasa tuua õigusliku ebakindluse. Samuti on kriitika osaliseks langenud üldmäärusest tulenev liikmesriikidele jäetud otsustamisruum, millel on artiklist 88 tulenevalt otsene mõju tööõiguslikule isikuandmete töötlemisele. Paindlikkusklauslite olemasolu kasuks räägib aga asjaolu, et õiguslik reguleerimine võib olla riigiti väga erinev. Näiteks tööõiguse valdkond on Euroopa Liidus riigiti erinevalt reguleeritud ja nüansse, mis tööelu korraldust puudutavates seadustes ja määrustes erinevad, on palju. Kuna tööõigus ja sellega seotud harjumuspärased tavad riigiti erinevad, on mõistlik, et üldmääruses on jäetud liikmesriikidele võimalus töösuhte kontekstis andmete töötlemise osas täpsemad reeglid kehtestada.[22]

1.2. Töötaja isikuandmete töötlemise alused

TLS § 41 lg 2 kohaselt peab tööandja tagama töötaja isikuandmete töötlemise vastavalt õigusaktides sätestatule. Tegemist on üldise viitega kohustusele, et isikuandmete töötlemine peab olema vastavuses õigusaktides sätestatule. Autori hinnangul on tegemist väga abstraktse ja üldise sättega, mistõttu võib tööandjatel praktikas olla keeruline otsustada, kas töötaja isikuandmete töötlemine konkreetses kontekstis on õiguspärane või mitte.

[20] Seletuskiri isikuandmete kaitse seaduse juurde. Lk 1. Arvutivõrgus: https://www.koda.ee/sites/default/files/content-type/content/2018-05/Seletuskiri%20%282%29.pdf, (25.02.2019).
[21] Samas. Lk 2.
[22] M. Iro. Isikuandmed töösuhtes. Mida peab teadma uuest isikuanmdete. Personaliuudised. 18.05.2018. Arvutivõrgus: https://www.personaliuudised.ee/uudised/2018/04/18/isikuandmed-toosuhetes-mida-peab-teadma-uuest-isikuandmete-kaitse-uldmaarusest, (27.04.2019).

Kuna kehtiv IKS ei sätesta täpsemaid nõudeid seoses töötajate isikuandmete töötlemisega töösuhte kontekstis, tuleb andmetöötluse aluste leidmiseks pöörduda üldmääruse poole. Käesolevas alapeatükis antakse ülevaade, millistel alustel tööandja töötaja isikuandmeid töödelda võib. Autor rõhutab, et isikuandmete töötlemiseks tuleb lugeda iga isikuandmetega seotud toiming ning töötajat, kelle andmeid töödeldakse, nimetatakse seejuures andmesubjektiks. Töötaja või tema kasutuses olevate info- ja kommunikatsioonitehnoloogia vahendite kontrollimine kujutab endast samuti üht isikuandmete töötlemise liiki.

Igasugune isikuandmete töötlemine peab olema seaduslik. Üldmääruse art. 6 sätestab, et isikuandmete töötlemine on seaduslik ainult juhul, kui on täidetud vähemalt üks kõnealuses artiklis nimetatud tingimustest. Ka töösuhte kontekstis isikuandmeid töödeldes, peab olema täidetud vähemalt üks üldmääruse artiklis 6 sätestatud alustest. Autor rõhutab, et artikkel 6 loetleb isikuandmete töölemise õigusliku alused ammendavalt, mistõttu ei ole neid lubatud kitsendada. Artiklis 10 sätestatud eriliiki isikuandmete (rassiline või etniline päritolu, poliitilised vaated, geneetilised või biomeetrilised andmed jms) töötlemine töösuhtes reeglina lubatud ei ole. Järgnevalt on analüüsitud üldmääruse art. 6 tulenevaid andmetöötluse aluseid:

- Andmesubjekti nõusolek: Üldreeglina võib igasugune andmetöötlus leida aset üksnes andmesubjekti nõusolekul. Nõusolekuks üldmääruse kontekstis loetakse vabatahtlikku, konkreetset ja teadlikku tahteavaldust, millega andmesubjekt annab nõusoleku töödelda tema kohta käivaid andmeid.[23] Andmetöötlus töötaja nõusoleku alusel võib teatud juhtudel olla võimalik, ent sellisel juhul peab töötajal olema võimalik ilma kahjulike tagajärgedeta nõusoleku andmisest keelduda või seda töösuhte kestel tagasi võtta. Praktikas on keeruline ette kujutada olukorda, kus töötaja annab vabatahtliku nõusoleku iseenda käitumise jälgimiseks. Töösuhte kontekstis loetakse selline nõusolek kehtetuks, sest võib olla tõenäoline, et see ei ole antud vabatahtlikult. Lisaks arvestades töötaja ja tööandja alluvussuhet, on väga ebatõenäoline olukord, kus töötajal on võimalik vabatahtlikult nõusoleku andmisest keelduda või see tagasi võtta. Illustreeriva näitena võib tuua olukorra, kus tööandja paigaldab töö tulemuslikkuse tõstmise eesmärgil tööruumidesse valvekaamerad ja võtab töötajatelt kirjaliku nõusoleku selle kohta, et oleks võimalik jälgida töötajate liikumist ja töökohalt eemal veedetud aega. Kuna töötaja on paratamatult

[23]Article 29 Data protection Working Party. Opinion 2/2017 on data processing at work. Lk. 6. Arvutivõrgus: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169. (20.01.2019).

nõrgemas positsioonis, siis ei ole loeta töötaja antud nõusolekut õiguspäraseks ja kehtivaks aluseks isikuandmete töötlemiseks ning tööandjal ei ole lubatud sellele toetudes valvekaameraid paigaldada.[24] Üldmäärus rõhutab, et olukorras, kus tööandja omab jõupositsiooni, ei saa andmetöötluse aluseks olla töötaja nõusolek.[25] Eelnevale tuginedes võib öelda, et töötaja nõusoleku alusel isikuandmete töötlemine on pigem väga erandlik ning tööandja peab tuginema mõnele muule õiguslikule alusele.

- Lepingu täitmine: Reeglina põhineb töösuhe töötaja ja tööandja vahelisel töölepingul, mistõttu võib andmetöötluse tuleneda kõnealuse lepingu täitmisest. Töötajale töötasu maksmise kohustus on reguleeritud töölepingus, mistõttu on tööandja kohustatud töötajale tasu makstes töötlema selliseid isikuandmeid nagu töötaja pangakonto number, isikukood jms. Viidates lepingu täitmisele kui isikuandmete töötlemise õiguslikule alusele, peab tööandja järgima põhimõtet, et koguda võib andmeid minimaalselt, s.t. üksnes andmeid, mis on hädavajalikud lepingu täitmiseks.
- Juriidilised kohustused: On üsna tavaline, et tööõigusega kehtestatakse tööandjale seadusjärgsed kohustused, mis toovad kaasa isikuandmete töötlemise vajaduse (näiteks maksude arvutamise ja töötasu haldamise eesmärgil).[26]
- Tööandja õigustatud huvi: Tegemist on andmetöötluse alusega, millele tööandjad töötajaid jälgides reeglina tugineda saavad, tõendades, et nende õigustatud huvi töötajate isikuandmete töötlemise kontekstis kaalub üles töötajate õiguse privaatsusele. Kahtlemata on tegemist väga laiaulatusliku põhimõttega, mis vajab täpsemat sisustamist ning tõlgendamist.[27] Kui tööandja soovib õigusliku aluse puhul tugineda õigustatud huvile, siis peab töötlemise eesmärk olema õiguspärane ning valitud meetod või konkreetne tehnoloogia, millega töötlemine toimub, peab olema tööandja õigustatud huvi jaoks vajalik. Töötlemine peab olema ka proportsionaalne ärivajadustega, s.t. eesmärgiga, mida sellega soovitakse saavutada. Andmetöötlus töökohal peab toimuma kõige vähem sekkuval viisil, mis on võimalik, ning olema suunatud konkreetsele riskivaldkonnale. Tuginedes töötajaid

[24] Euroopa komisjon. Kas mu tööandja saab mind sundida nõustuma minu isikuandmete kasutamisega? Arvutivõrgus: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/can-my-employer-require-me-give-my-consent-use-my-personal-data_et (15.02.2019).
[25] A. Bevitt. Employee „consent“ under the GDPR. Arvutivõrgus: http://in-houseblog.practicallaw.com/employee-consent-under-the-gdpr/ (20.02.2019).
[26] Article 29 Data protection Working Party. Opinion 2/2017 on data processing at work. Lk. 7. Arvutivõrgus: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169. (20.01.2019).
[27] A. Bevitt. Employee „consent“ under the GDPR. Arvutivõrgus: http://in-houseblog.practicallaw.com/employee-consent-under-the-gdpr/ (20.02.2019).

jälgides õigusliku alusena õigustatud huvile, on oluline, et kehtiksid konkreetsed leevendusmeetmed, et tagada nõuetekohane tasakaal tööandja õigustatud huvi ning töötajate põhiõiguste ja vabaduste vahel. Need meetmed peaksid (olenevalt jälgimise viisist) hõlmama jälgimise ja kontrollimise piiranguid, tagamaks, et töötaja eraelu puutumatust ei rikuta. Sellised piirangud võivad olla näiteks geograafilised, mille kohaselt on töötaja jälgimine lubatav üksnes konkreetsetes kohtases ning tundlikes alades (pesu- ja tualettruumid, religioossed paigad jms) peaks jälgimine olema keelatud; andmete põhised, ehk isiklikke elektroonilisi faile ja teabevahetust ei tohiks jälgida ning ajapõhised, kus töötajaid jälgitakse ajalise valimi alusel, mitte aga pidevalt.[28] Praktiline näide, kus tööandja õigustatud huvi on piiratud: tööandja võib paigaldada serveriruumile (alternatiivselt arhiivile füüsilisel kujul), kus hoiustatakse ärisaladust puudutavaid andmeid, töötajate isikuandmeid, klientide andmeid jms. jälgimissüsteemi, mis salvestab töötaja sisenemise ja väljumise ruumist, eeldusel, et täidetud on üldmääruse art. 5 nimetatud andmekaitse üldpõhimõtted.[29]

1.3. Töötaja isikuandmete töötlemise põhimõtted

Lisaks õigusliku aluse olemasolule, peab töötajate isikuandmete töötlemine vastama üldmääruse artiklis 5 nimetatud isikuandmete töötlemise põhimõtetele. Tööandja, kes töötleb töötaja isikuandmeid, on alati kohustatud järgima isikuandmete töötlemise põhimõtteid.

Üldmääruse art. 5(1) a sätestab, et isikuandmete töötlus peab olema seaduslik (inglise keeles *lawful*), õiglane (inglise keeles *fair*) ja läbipaistev (inglise keeles *transparent*).[30] Tööandja peab töötaja isikuandmete töötlemisel tagama, et nende isikuandmetega seotud teave on lihtsalt kättesaadav, arusaadav ning selgelt ja lihtsalt sõnastatud. Andmetöötluse läbipaistvus tagatakse töösuhtes eelkõige teavitamise teel: töötajat peab enne andmetöötluse algust teavitama töötlemise eesmärkidest, töötleja identiteedist ja muudest olulistest andmetöötlusega seotud asjaoludest. Andmetöötlusest tuleb töötajat teavitada nii juhtudel, kui ta avaldab enda kohta käivaid andmeid

[28] Article 29 Data protection Working Party. Opinion 2/2017 on data processing at work. Lk. 7-8. Arvutivõrgus: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169. (20.01.2019).
[29] A. Bevitt. Employee „consent“ under the GDPR. Arvutivõrgus: http://in-houseblog.practicallaw.com/employee-consent-under-the-gdpr/(20.02.2019).
[30] Euroopa parlamendi ja nõukogu määrus (EL) 2016/679, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta.

tööandjale ise, aga ka olukordades, kus tööandja kogub töötaja andmeid vahendatult, näiteks jälgimissüsteemide kaudu.[31] Tööandja peab töötajaid jälgides tagama tõhusa teavitamise mehhanismid.

Üldmääruse art. 5(1)b kohaselt võib isikuandmeid koguda üksnes täpselt ja selgelt kindlaks määratud ning õiguspärastel eesmärkidel. Sama sätte teine lause lisab, et andmeid ei ole lubatud töödelda hiljem viisil, mis on nende eesmärkidega vastuolus (inglise keeles *purpose limitation*). Ehk tööandja peab kindlaks määrama isikuandmete töötlemise selged, konkreetsed ja õiguspärased eesmärgid, millest tulenevalt on töötaja isikuandmete töötlemine lubatav üksnes juhul, kui see täidab andmete kogumisele sätestatud eesmärki. Lubamatu on töötaja isikuandmete töötlemine "muudel eesmärkidel", mis võivad tekkida andmetöötluse kestel, v.a. juhtudel, mil uus eesmärk ühildub esialgsega.[32]

Ühtlasi peavad tööandja järgima üldmääruse artiklis 5(1) c nimetatud võimalikult vähese andmete kogumise põhimõtet (inglise keeles *data minimation*). Kogutavad isikuandmed peavad olema asjakohased, olulised ja piiratud sellega, mis on vajalik nende töötlemise eesmärgi seisukohalt. Tööandja peab kindlustama, et andmeid kogutakse, s.h. jälgimise teel vaid ulatuses, mis on vajalik seatud eesmärgi saavutamiseks. Vältida tuleks olukorda, kus töötajate isikuandmeid kogutakse "igaks juhuks" põhimõttel. Tööandja peaks enne isikuandmete kogumise või töötlemise alustamist kaardistama ära, milliseid isikuandmeid vaja läheb ja piirduma rangelt selle vajalikuga.[33]

Üldmääruse art 5(1) d kohaselt peavad isikuandmed olema õiged ja vajaduse korral ajakohastatud (inglise keeles *accuracy*). Tööandja peab isikuandmeid kogudes või töödeldes võtma kasutusele kõik mõistlikud meetmed, et töötlemise eesmärgi seisukohast ebaõiged andmed kustutataks või parandataks. Töösuhte kontekstis kogutud isikuandmed peavad olema adekvaatsed ning asjakohased. Kui kogutud isikuandmeid pole enam vaja, peab tööandja need kustutama. Tööandjal on lubatud kogutud teavet hoiustada nii vähese aja jooksul, kui võimalik ning kui teavet ei ole enam vaja, tuleb see kustutada. Õigsuse ja ajakohastuse põhimõte eeldab tööandjalt regulaarset andmebaaside ülevaatust ja kontrolli, eesmärgiga eemaldada ebavajalik teave.

[31] D. Heywood. Lawful processing og HR data under the GDPR. – Global data hub. Arvutivõrgus: https://globaldatahub.taylorwessing.com/article/lawful-processing-of-hr-data-under-the-gdpr. (20.02.2019).
[32] Samas.
[33] K. Salumaa. Isikuandmete töötlemise põhimõtted ja seaduslikkus ehk õiguslikud alused. 24.11.2017. Arvutivõrgus: https://www.just.ee/sites/www.just.ee/files/24.11.17_kart_salumaa.pdf

Üldmääruse art 5(1) e sätestab, et isikuandmeid säilitatakse kujul, mis võimaldab andmesubjekte tuvastada ainult seni, kuni see on vajalik selle eesmärgi täitmiseks, milleks isikuandmeid töödeldakse (inglise keeles *storage limitation*). Säilitamise piirangu põhimõtte kohaselt ei tohi tööandja säilitada isikuandmeid kauem, kui on vajalik töötlemiseesmärgi saavutamiseks. Näiteks ei tohiks tööandja säilitada konkursil osalenud ent valituks mitte osutunud kandidaatide andmeid.

Isikuandmete töötlemine peab vastama usaldusväärsuse (inglise keeles *integrity*) ja konfidentsiaalsuse (inglise keeles *confidentiality*) põhimõtetele: üldmääruse art 5(1) f kohaselt võib isikuandmeid töödelda viisil, mis tagab isikuandmete asjakohase turvalisuse, s.h. kaitseb loata või ebaseadusliku töötlemise eest ning juhusliku kaotamise, hävimise või kahjustumise eest, kasutades asjakohaseid tehnilisi või korralduslikke meetmeid. Magistritöö autor on seisukohal, et tegemist on ühe olulisima põhimõttega, mille üldmäärus andmetöötlusele sätestab. Tööandja, kui vastutav töötleja, on kohustatud võtma kasutusele asjakohaseid tehnilisi ja korralduslikke meetmeid andmete turvalisuse tagamiseks. Ehk tööandjal tuleb rakendada isikuandmete töötlemiseks sobivaid organisatsioonilisi, füüsilisi ja infotehnoloogilisi turvameetmeid. Lisaks elementaarsetele meetoditele, näiteks personaalsed kasutajatunnused ja paroolid arvutivõrku sisenemiseks ning ekraanilukustamine töökohalt eemalviibimise ajaks[34], peab tööandja teaduse ja tehnoloogia arengu tõttu vajadusel kasutusele võtma ka seni vähem levinud turvameetmeid, näiteks isikuandmete pseudonümiseerimine ja krüpteerimine, isikuandmeid töötlevate süsteemide konfidentsiaalsus ja vastupidavus, tehniliste ja korralduslike meetmete tõhususe korrapärane testimine jms.[35]

Üldmäärus nimetab artiklis 25 ka kaks uudset põhimõtet, milleks on vaikimisi ja lõimitud andmekaitse, mille kohaselt isikuandme kaitsega peab arvestama koheselt ja riske ennetama, mitte ootama nende realiseerumiseni.[36] Üldmäärusele on omane lähtumine põhimõttest, et kõik elu- ja tegevusvaldkonnad on seotud infotehnoloogiaga ning infotehnoloogia on omakorda kasutajatele ning regulatiivsetele asutustele läbipaistmatu. Praktikas tähendab see seda, et andmekaitse asutustel ei ole võimekust efektiivselt ja süstemaatiliselt uurida ning karistada rikkumisi. Selle „nõrkuse“ tasakaalustamiseks on rõhk ennetamisel.[37]

[34] Andmakaitse inspektsioon. Isikuandmete töötlemine töösuhtes. Abistav juhendmaterjal. Lk 61
[35] Andmekaitse üldmäärus art. 32. Töötlemise turvalisus.
[36] K. Salumaa. Isikuandmete töötlemise põhimõtted ja seaduslikkus ehk õiguslikud alused. 24.11.2017. Arvutivõrgus: https://www.just.ee/sites/www.just.ee/files/24.11.17_kart_salumaa.pdf
[37] K. Turk. Andmekaitse üldmääruse TOP 10: Uudsed andmekaitse põhimõtted. 19.10.2016. Arvutivõrgus: https://triniti.ee/andmekaitsemaaruse-joustumiseelsete-tegevuste-top-10-4-uudsed-andmekaitse-pohimotted/

2. Pilti, heli või signaali edastavate seadmete kaudu kogutud töötaja isikuandmete töötlemine

2.1. Pilti, heli või signaali edastavate seadmed töökohal

Töötaja kontrollimine on töösuhtele omane nähtus, sest tulenevalt TLS § 1 lõikest 1 allub töötaja tööandja juhtimisele ja kontrollile. Küll aga on tööandja töötajat kontrollides kohustatud austama töötaja privaatsust ning kontrollima töökohustuste täitmist selliste viisidega, mis ei riiva töötaja põhiõigusi. Kõige vähem riivavad töötaja põhiõigusi sellised meetmed, mille puhul tööandja omandab konkreetsete asjaolude kontrollimiseks vajaliku informatsiooni töötajalt endalt, paludes neil hinnata töö tulemuslikkust, võimet tulla toime tööülesannete täitmisega jms. Vastupidiselt kõige enam riivavad töötaja privaatsust sellised kontrollimise viisid, mis seisnevad töötaja jälgimises, töötaja enda, tema isiklike asjade või tema töökoha läbiotsimises ja telefoni pealtkuulamises.[38] Ka AKI on selgelt väljendanud, et võrreldes teiste isikuandmete kogumise viisidega, kujutab just käesolevas magistritöös käsitletav valdkond, ehk töötajate jälgimine mitmesuguste elektrooniliste vahendite kaudu, kõige intensiivsemat eraelu riivet üldse, sest selliste seadmete kasutamine võib olla inimväärikust alandav.[39] Töötaja, kelle iga liigutust, sõna ja näoilmet pidevalt jälgitakse, muudab ja kontrollib oma käitumist. Lisaks sellele, et jälgimine võib riivata töötaja põhiõiguseid, võib pikaaegne jälgimine kaasa tuua ka stressi ja töövõime langust. Läbimõtlematu jälgimisseadmete kasutamine võib seega tööandjale kokkuvõttes tuua rohkem kahju kui kasu – seda eeskätt usaldamatu õhkkonna loomise, stressi põhjustamise aga ka töötajate inimväärikuse alandamise kaudu.[40] Käesoleval hetkel selgesõnaliselt ükski seadus ei sätesta, mil viisil võib tööandja töökohustuste täitmist kontrollida. Üks tingimus, mis piirab tööandja kontrolli teostamise õigust on, et kontrollida võib üksnes töökohustustega seotud asjaolusid. Ehk kontrollitavad asjaolud peavad tulenema töösuhte aluseks olevatest dokumentidest, näiteks töölepingust, ametijuhendist, töökorralduse eeskirjadest ning seadustest.

[38] E. Käärats jt. Töölepingu seadus. Selgitused töölepingu seaduse juurde. Lk. 68.
[39] Andmekaitse inspektsioon.. Isikuandmete töötlemine töösuhtes. Abistav juhendmaterjal. Lk. 66. Arvutivõrgus: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikuandmed%20t%C3%B6%C3%B6suhetes%20juhendmaterjal26%2005%202014_0.pdf. (10.01.2019).
[40] Andmekaitse inspektsioon. Juhis personalitöötajale: Isikuandmed töösuhtes. Lk. 16. Arvutivõrgus: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikuandmed%20t%C3%B6%C3%B6suhetes%20juhis%20personalit%C3%B6%C3%B6tajale.pdf. (22.02.2019).

Tänapäeva infoühiskonda iseloomustab enim uudse ja laiaulatuslike kasutusvõimalustega tehnoloogia kasutuselevõtt ning areng. Uued tehnoloogilised võimalused töösuhte kontekstis võivad üheaegselt kujutada endast suurt edasiminekut ja lihtsustada oluliselt töötegemist, ent teisalt võivad need kaasa tuua ka palju negatiivset. USA õigusteadlane Corey A. Ciccoletti on uusi tehnoloogiaid töösuhetes nimetanud üheaegselt lausa õnnistuseks ja needuseks.[41] Tõenäoliselt nähakse jälgimisseadmetes üheaegselt positiivset ja negatiivset külge eelkõige seetõttu, et ühelt poolt on tööandjal võimalik nende abil kerge vaevaga koguda suurel määral informatsiooni töötajate kohta, ent teisalt põhjustavad jälgimisseadmed töötajates ebamugavust, hirmu ja kahtlusi.[42] Lihtsustatult saab tõesti väita, et jälgimisseadmete kasutamine on kas positiivne või negatiivne, ent selline vahettegu ei olegi probleemi lahendamisel kõige olulisem: tõeline väljakutse on määrata kindlaks jälgimisseadmete kasutamise lubatavuse ulatus ja kontekst, kus neid kasutatakse.[43]

Töötajate jälgimisel kasutatavate seadmete defineerimiseks tuleb pöörduda Turvaseaduse § 11 lg 3 juurde, mis sätestab, et jälgimisseadmestik on pilti või elektroolilist signaali edastavate ja salvestavate seadmete kogum.[44] Töökohal kasutatavad jälgimisseadmed edastavad ja salvestavad pilti reeglina selleks, et jälgida mingit territooriumi, inimesi, eset või protsessi. Lisaks videopilti salvestatavatele seadmetele kujutavad endast jälgimisseadmeid ka GPS-seadmed, mis võimaldavad kindlaks määrata inimese või eseme (töösuhte kontekstis eelkõige sõiduki) asukohta[45] ning kõikvõimalikud kiipkaardisüsteemid, mille abil on võimalik kindlaks teha töötajate liikumist ettevõtte ruumides.

Põhjused, miks tööandjad soovivad kasutada jälgimisseadmeid, on mitmeid. Valdavalt põhjendavad tööandjad jälgimisseadmete kasutust järgmiste ärihuvi teenivate põhjendustega:

1. Jälgimisseadmeid paigaldatakse töötaja produktiivuse hindamiseks;
2. Töötaja produktiivse arvutikasutuse maksimeerimise eesmärgil;

---

[41] C. A. Ciccoletti. The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring. - American Business Law journal. Vol 48. Issue 2. 2011

[42] Andmekaitse inspektsioon. Isikuandmete töötlemine töösuhtes. Lk. 66. Arvutivõrgus: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikuandmed%20t%C3%B6%C3%B6suhetes%20juhendmaterjal26%2005%202014_0.pdf. (10.01.2019).

[43] S. Lohr. Unblinking Eyes Track Employees. – New York Times. Arvutivõrgus: https://www.nytimes.com/2014/06/22/technology/workplace-surveillance-sees-good-and-bad.html?action=click&module=RelatedCoverage&pgtype=Article&region=Footer, (14.03.2019).

[44] Turvaseadus. - RT I, 03.03.2017, 27.

[45] Tööinspektsioon. Isikuandmed töösuhetes ja reeglid töökorraldusele.Lk. 7

3. Jälgitakse, kas töötaja lähtub oma töös ettevõttes kehtestatud töökorralduslikest reeglitest;
4. Tõendite kogumiseks (näiteks töölepingust tuleneva vaidluse korral);
5. Tööstusspionaaži, ärisaladuste ja muude intellektuaalset omandit puudutavate õiguste kaitseks ja rikkumiste avastamiseks;
6. Volitamata isikute, s.h. häkkerite (inglise keeles *hacker*) arvutisüsteemidele ligipääsu takistamiseks ja avastamiseks.[46]

2.2. Kaamera

2.2.1. Kaamera kasutamise võimalused töökohal

Töötajate jälgimine kaamera kaudu ei ole iseenesest just kuigi uudne tehnoloogiline jälgimisviis ning küsimused ja probleemid seoses töötajate eraelu puutumusega on jäänud samaks. Siiski saab seoses IKT arenguga täheldada mõningaid olulisi muudatusi ja edasiminekuid, mis on seotud videoseire ja -valve kohaldamisega töösuhte kontekstis.

Klassikalised proleemid, mis kaasnevad videoseire ja -valve kasutamisega on seotud töötajate eraelu puutumatusega: võimalus salvestada pidevalt töötaja käitumist. Kõige olulisemad muudatused seoses selle tehnoloogia kohaldamisega töösuhete kontekstis on võimalus kogutud andmetele lihtsasti kaugteel (näiteks nutitelefoni kaudu) juurde pääseda; kaamera suuruse vähenemine koos võimaluste suurenemisega, (näiteks kõrgresolutsioon) võimaldab tööruumidesse paigaldatud kaameratel jääda märkamatuks, lisaks on võimalik töötajaid jälgida uudse videoanalüüsi abil.[47] Videoanalüüs kujutab endast võimalust jälgida töötaja näoilmeid, eesmärgiga teha kindlaks kõrvalekaldeid eelnevalt kindlaks määratud liikumismustritest, näiteks tehase vm. tootmisüksuse kontekstis.[48] Magistritöö autor on seisukohal, et selline automatiseeritud jälgimine on töötajate õiguste ja vabadustega ebaproportsionaalne ning seetõttu lubamatu.

Tänu tehnoloogia arengule ja privaatsusõiguse olulisusele on infoturbe spetsialistid koostöös juristidega asutud välja töötama ja rakendama nn. Targa kaamera süsteeme (inglise keeles

[46] G. Lasprogata jt. Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada. – Stanford Technology Law Review. 2004/04. Lk 2.
[47] Article 29 Data protection Working Party. Opinion 2/2017 on data processing at work. Lk 20. Arvutivõrgus: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169. (20.01.2019).
[48] Samas. Lk 20.

intelligent video surveillance). Arendustöö põhjuseks on selliste jälgimissüsteemide vähendamine, mis võivad kahjustada töötajate põhiõiguseid. Ainuüksi kaamera olemasolu (isegi kui see ei salvesta) töökohal mõjutab töötaja käitumist ning tänases ühiskonnas ei saa seda aktsepteerida. Eelnevale tuginedes on loodud süsteem, mis on võimeline eraldama videovoost konkreetseid elemente. Näiteks saab süsteemile programmeerida korralduse tunda ära ettevõtte töötajad ning privaatsuse eesmärgil nad videol hägustada (inglise keeles *blurring*). Nii on võimalik oluliselt vähendada riivet töötaja privaatsusele ametikohal, millega kaasneb tööpäevaringne jälgimine.[49] Magistritöö autor toob siinkohal näitena välja lennujaama töötajad, keda tööandja küll usaldab, ent üldise julgeoleku huvides on siiski õigustatud videovalve kasutamine. Targa kaamera süsteem suudab rakendada privaatsust tagavaid mehhanisme, eristades videosalvestistel lennujaama töötajaid reisijatest. Oluline on töötajad videovoost eraldada nii, et neid pole enam võimalik identifitseerida. Ainuüksi näo hägustamisest seetõttu ei piisa, sest töötajat on võimalik identifitseerida ka muude tunnuste kaudu – näiteks keha kuju, riietus, kaasasolevad seemed jms.[50]

2.2.2. Õiguslik alus kaamera kasutamiseks

Õiguslik alus kaamera kasutamiseks tööruumides on seotud tööandja õigustatud huviga. Tööandja on kohustatud enne kaamerasüsteemide kasutuselevõttu veenduma, et tema õigustatud huvi on selline, mis kaalub üles töötaja õiguse eraelule ja isikuandmete kaitsele. Tööandjad põhjendavad sageli oma õigustatud huvi varguste ennetamise, töötajate ja klientide turvalisuse, töötervishoiu- ja ohutuse tagamise ning tootlikkuse hindamise vajadusega. Tööandjad eksivadki üldjuhul selle vastu, et põhjendavad oma õigustatud huvi väga üldistatult, kuid üldmääruse kohaselt peab see olema selge ja ühemõtteline. Seetõttu enne videoseire ja -valve süsteemide rakendamist töökohal, peaks tööandja hoolega kaaluma, kas see on ilmtingimata vajalik ning kaardistama jälgimistegevuse eesmärgid. Euroopa andmekaitseinspektor on märkinud, et töötajate produktiivsuse, kvaliteedikontrolli või vaidluste lahendamiseks tõendite kogumine ei saa olla

[49] P. Birnstill jt. Privacy-preserving surveillance: an interdisciplinary approach. – International Data Privacy Law. Oxford academic. 04/2015. Lk 299. Arvutivõrgus: https://www.researchgate.net/publication/282349311_Privacy-preserving_surveillance_an_interdisciplinary_approach (17.03.2019).

[50] Andmekaitse inspektsioon. Juhis personalitootajale: isikuandmed töösuhtes. Lk. 14. Arvutivõrgus: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikuandmed%20t%C3%B6%C3%B6suhetes%20juhis%20personalit%C3%B6%C3%B6tajale.pdf. (22.02.2019).

jälgimistegevuse eesmärkideks.[51] Sellest tulenevalt langevad ära mitmed levinud õigustatud huvi põhjendused ning tööandjal ei ole lubatud kasutada kaameraid nimetatud eesmärkidel.

Õigustatud huvi kaamera kasutamiseks ei tohiks tööandja põhjendada ka üldsõnalise viitega turvariskidele või rikkumiste, mis võivad ettevõttes aset leida. Turvariskide vähendamine võib endast kujutada tööandja õigustatud huvi kaamerate kasutamiseks ja olla eesmärgipärane üksnes siis, kui tööandja määratleb iga turvariski eraldiseisvalt ja detailselt, tuginedes andmetele, mis kinnitavad reaalselt riski esinemist: spetsiifiline oht, näiteks lubamatu sissepääs ruumi, kus paiknevad ettevõtte jaoks kriitilise tähtsusega IT infrastruktuurid või muu oluline teave; kuritegevuse kõrge tase, sel juhul on õigustatud kaamerate paigaldamine näiteks parklasse, vältimaks vargusi ja vandalismi jne. Pelgalt hirm, spekulatsioonid või ebapiisav tõendus ei ole piisavad, et õigustada video- või valvekaamerate kasutamist.[52] Tööandja on kohustatud austama töötaja privaatsust ja kontrollima töökohustuste täitmist viisil, mis ei riku töötaja põhiõigusi – sellest põhimõttest tulenevalt peaks tööandja loobuma kergekäelisuset kaamerate kasutamisel. Hindamaks, kas tööandjal on õigustatud huvi kaamerate kasutamiseks töökohal, peaks tööandja arvesse võtma järgmisi asjaolusid:

- Milline on kaamerate kasutamisest saadav kasu ning kas see kaalub üles jälgimisega kaasnevad negatiivsed mõjud?
- Kas jälgimisseadmete kasutamise eesmärk on selgelt määratletud, ühemõtteline ja selge ning õiguspärane? Kas jälgimist toetab seaduslik alus?
- Kas jälgimisseadme kasutamine on ilmtingimata vajalik? Kas tegemist on efektiivse meetmega või on olemas teisi, töötaja privaatsust vähem riivavaid alternatiive jälimisseadmetele?[53]

Praktikas on jälgimisseadmete kasutamine aktuaalne olnud eelkõige töötajate puhul, kes puutuvad kokku rahaga selle füüsilisel kujul, näiteks kassapidajad, kohviku teenindajad jms. Euroopa andmekaitseinspektor pigem eitab tööandja õigustatud huvi kassapidajate järjepidevaks jälgimiseks, sest jälgimine terve tööaja vältel riivab liigselt töötaja privaatsust, mistõttu tuleks seda vältida.[54] Euroopa inimõiguste kohus on lahendis *Lopez Ribalda and others vs. Spain* tunnistanud

[51] European data protection supervisor. The EDPS video-surveillance guidelines. 2010. Lk. 22. Arvutivõrgus: https://edps.europa.eu/sites/edp/files/publication/10-03-17_video-surveillance_guidelines_en.pdf (27.02.2019).
[52] European data protection supervisor. The EDPS video-surveillance guidelines. 2010. Lk. 20. Arvutivõrgus: https://edps.europa.eu/sites/edp/files/publication/10-03-17_video-surveillance_guidelines_en.pdf (27.02.2019).
[53] Samas. Lk.17
[54] Samas. Lk. 23

lubamatuks kassapidajate varjatud jälgimise olukorras, kus tööandja kahtlustas kaupluse töötajaid järjepidevas varguses. Tööandja põhjendas oma õigustatud huvi kaamerate paigaldamiseks üldsõnalise viitega turvariskide vähendamiseks, ning paigaldas tööruumidesse kaamerad, mis olid töötajatele nähtavad. Samuti selgitas tööandja kaamerate kasutamise eesmärke ning Euroopa Inimõiguste kohtu hinnangul teavitas töötajaid nõuetekohaselt. Konkreetsete vargusjuhtumite tuvastamiseks kasutas tööandja aga ka kaamerat, mis jäi töötajatele varjatuks. Vaatamata asjaolule, et varjatud kaamera abil tuvastas tööandja varguse toimepanijad, leidis Euroopa Inimõiguste kohus, et seesugune varjatud jälgimine riivas Euroopa inimõiguste ja põhivabaduste konventsiooni artiklist 8 tulenevat õigust era- ja perekonnaelu puutumatusele.[55] Magistritöö autor järeldab, et tööandjal ei saa olla õigustatud huvi töötajate varjatud jälgimiseks. Teatud juhtudel võib töötajate varjatud jälgimine olla kriminaliseeritud karistusseadustiku § 137 kohaselt eraviisilise jälitustegevusena.[56]

Analüüsides Euroopa Inimõiguste kohtu praktikat, on võimalik järeldada, et töötaja õigustatud ootus privaatsusele töökohal on ajas muutunud. Varasemalt on Euroopa Inimõiguste kohus oma lahendis 420/07 *Köpke vs. Germany* lubatavaks tunnistanud kassapidaja jälgimise situatsioonis, kus tööandjal oli tekkinud raamatupidamise andmete ja inventuuri dokumentide analüüsimise põhjal kahtlus, et kassapidaja manipuleerib andmetega ja maksab kassast välja suurema summa raha kui tagastatud taarapudelite väärtus tegelikult on. Vaatamata asjaolule, et tegemist oli varjatud jälgimisega, leidis kohus, et tööandja jälgis kaamera abil üksnes konkreetset kassapidajat, piiratud aja jooksul, mistõttu leidis kohus, et jälgimine on õigus- ja eesmärgipärane ning proportsionaalne. Tööandja põhjendas oma õigustatud huvi jälgimisseadme kasutamiseks ka asjaoluga, et puudusid teised, töötaja privaatsust vähem riivavad meetodid järjepideva varguse tuvastamiseks.[57] AKI on tööandja õigustatud huvi eitanud ning kaamera paigutamise lubamatuks tunnistanud ja töötajate privaatsuse riivet kinnitanud järgmises situatsioonis: Kaamera paigaldamist ruumi, kus paikneb sularaha šeif, eesmärgiga jälgida sularaha liikumist, võib pidada õiguspäraseks. Lubamatu on aga

[55] EIKo lahend. 1874/13 ja 8567/13. 09.01.2018. Lopez Ribalda and others vs Hispaania.
[56] Andmekaitse inspektsioon. Tööandja ei tohi töötajaid varjatult kaamerate abil ja telefonikõnede salvestamisega jälgida. Arvutivõrgus: https://www.aki.ee/et/tooandja-ei-tohi-tootajaid-varjatult-kaamerate-abil-ja-telefonikonede-salvestamisega-jalgida (26.02.2019).
[57] EIKo lahend 420/07. 05.10.2010. Köpke vs Saksamaa.

kaamera paigutamine viisil, kus kaamera salvestab kogu ruumi, s.h. töötajaid kogu tööpäeva jooksul, kes samas ruumis töötavad.[58]

Lahendis Antonovic & Mirkovic vs Montenegro leidis EIK, et tööandjal ei ole õigustatud huvi kaamera paigaldamiseks ülikooli auditooriumisse. Kõnealuse kaasuse puhul paigaldas Montenegro Ülikool kaamerad haridusasutuse ruumidesse, kus toimuvad loengud, põhjendades oma õigustatud huvi eesmärgiga kaitsta oma vara ning jälgida õppejõude. Kohus leidis, et privaatne elu hõlmab m.h tööalaste ülesannete täitmist avalikus kohas, antud juhul auditooriumis ning kaamerad riivavad töötajate privaatsust liigselt. Samuti viitas kohus asjaolule, et tööandja põhjendused õigustatud huvi esinemisele olid liiga üldsõnalised ja ebapiisavad.[59] Magistritöö autor järeldab Euroopa Inimõiguste kohtu praktikat analüüsides, et tööandja õigustatud huvi kaamerate kasutamiseks peab olema väga selgelt ja ühemõtteliselt määratletud ning tuvastatav ning pelk hirm oma vara pärast ei saa olla õigustuseks kaamerate kasutamiseks.

Samuti puudub tööandjal õigustatud huvi video- või valvekaamerate paigaldamiseks ruumidesse, kus töötajal on õigustatud ootus täielikule privaatsusele. Euroopa Andmekaitseinspektori seisukoha kohaselt on keelatud jälgida ruume, mis ei ole mõeldud töötajate poolt tööülesannete täitmiseks, vaid töötajatele eraviisiliseks käsutamiseks - näiteks tualett- ja duširuumid, riietusruumid, töötajate puhkeala. Sarnaselt nimetatud aladele, on töötajal kõrgendatud ootus privaatsusele ka oma kabinetis. Kusjuures andmekaitseinspektor rõhutab, et kabinetiks tuleb lugeda ka ruum, mida jagavad mitu töötajat ning nn. avatud kontorid. Ühtlasi pole lubatud kaamera kasutamine ruumides, mille jälgimisega kaasneb delikaatsete isikuandmete töötlemine. Andmekaitseinspektor nimetab sellistena näiteks ametiühingule eraldatud ruumi, palvetamisruumi, meditsiinitöötaja kabineti, s.h. selle ooteruumi ja sissepääsu. [60]

[58] A. Ojaver. Valvekaamerate kasutamine töökohtadel ja kaubanduspindadel – kontrollide sõnaline kokkuvõte. 24.10.2010. Arvutivõrgus: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Valvekaamerate%20seire.pdf, (14.03.2019).
[59] EIKo lahend. 70838/13. 28.11.2017. Antonovic & Mirkovic vs Montenegro.
[60] European data protection supervisor. The EDPS video-surveillance guidelines. 2010. Lk. 29. Arvutivõrgus: https://edps.europa.eu/sites/edp/files/publication/10-03-17_video-surveillance_guidelines_en.pdf (27.02.2019).

2.2.3. Kaamera kasutamise põhimõtted

Jälgimisseadmete kasutamine töökohal peab olema proportsionaalne kaasnevate riskide suhtes. Proportsionaalsuse hindamiseks tuleb omavahel kaaluda töötaja privaatsuse riivet ning tööandja õigustatud huvi jälgimisseadme kasutamiseks tuleb ning juhul kui riive on proportsionaalne, on ta ka õigustatud.[61] Jälgimist võib pidada proportsionaalseks siis, kui see on püstitatud eesmärgi saavutamiseks sobiv, vajalik ja mõõdukas. Privaatsusõiguse kontekstis tasub eelkõige kindlaks teha jälgimise vajalikkus ning veenduda, et eesmärgi saavutamiseks puuduvad teised, töötajat eraelu puutumatust vähem riivavad abinõud.

Artikli 29 alusel asutatud andmekaitse töörühm on m.h. ebaproportsionaalseks tunnistanud sõidukisse paigaldatud videokaamera, mis teeb heli- ja videosalvestisi, eesmärgiga parandada töötajate sõiduoskusi ja kaitsta oma töötajate ning teiste liiklejate ohutust. Töörühm rõhutas, et vastavaid kaameraid paigaldades ei ole ettevõtte õigustatud huvi jälgida juhte olulisem kui nende juhtide isikuandmete kaitse õigus. Seda isegi siis, kui kaamerad konfigureeritakse selliselt, et need säilitavad salvestise üksnes siis, kui toimub teatav vahejuhtum, näiteks järsk pidurdus või suunamuutus. Töötajate pidev jälgimine selliste kaameratega toob kaasa ulatusliku sekkumise nende õigusesse eraelu puutumatusele. Töörühm lisas, et on olemas muid meetodeid (nt mobiiltelefonide kasutamist takistava seadme paigaldamine), samuti muid ohutussüsteeme, nagu kõrgetasemeline hädapidurdussüsteem või sõidurajalt kõrvalekaldumise hoiatussüsteem, mida võib kasutada sõidukite õnnetusjuhtumite ärahoidmiseks ja mis võivad olla asjakohasemad. Peale selle esineb suur tõenäosus, et selline video toob kaasa kolmandate isikute (näiteks jalakäijate) isikuandmete töötlemise, ning nimetatud kolmandate isikute isikuandmete töötlemiseks tööandjal õigustatud huvi olla ei saa.[62]

Autori sõnul on praktikas tihti probleemseks see, et tööandjad isegi ei kaalu proportsionaalsemaid ja vähem invasiivseid vahendeid, saavutamaks jälgimistegevusele seatud eesmärki. 2017. Aastal Tööisnpektsiooni juristi Kaie Saarepi läbiviidud uuringust selgub, et vaid 6% tööandjatest on kaalunud ja kasutusele võtnud muid lahendusi alternatiivina turvakaameratele, nagu näiteks turvatöötajaid, tööajaarvestuse seadmeid või lihtsalt elementaarset suhtlemist töötajatega.

[61] M. Ernits. PS § 12 kommentaar 4.2. Madise jt (toim). Eesti Vabariigi põhiseadus. Komm vlj. 3. vlj. Tallinn: Juura 2012

[62] Article 29 Data protection Working Party. Opinion 2/2017 on data processing at work. Lk 20
Lk. 21. Arvutivõrgus: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169. (20.01.2019).

Tööandjate seisukohad töötajate kaameraga jälgimist puudutavas küsimuses peegeldavad teadmatust, millised ohud kaasnevad turvakaamerate kasutamisega. Ühtlasi puuduvad tööandjatel piisavad teadmised proportsionaalsemate mitteformaalsete meetodite rakendamiseks, nt organisatsioonikultuuri arendamine.[63]

Tööandja peab kaameraid kasutades lähtuma ka minimaalsuse põhimõttest, mille kohaselt tuleb neid rakendada kõige vähem sekkuval viisil, mis on võimalik ning kaameraid võib kasutada üksnes selles ulatuses, mis on vajalik jälgimisele seatud eesmärgi täitmiseks. Magistritöö autor on seisukohal, et töötaja jälgimine terve tööaja vältel või tema näo salvestamine lähivaates on üldjuhul vastuolus minimaalsuse põhimõttega. Näiteks juhtudel, mil tööandjal on õigustatud huvi sularaha liikumise jälgimiseks kaamerast, võib tekkida õiguslik küsimus, kas minimaalsuse põhimõtet arvestades on töötaja nägu asjassepuutuv? Ehk minimaalsuse põhimõtte kohaselt tuleks kaamerad seadistada selliselt, et jälgitakse üksnes seda ala, mis on kaetud tööandja õigustatud huvi ja jälgimise eesmärgiga. Minimaalse jälgimise põhimõtte kohaselt peab tööandja suutma tõendada, et rakendatud on asjakohased meetmed, et tagada tasakaal töötajate põhiõiguste ja vabaduste vahel.[64]

Läbipaistvuse tagamise eesmärgil peab tööandja jälgimisseadmete kasutamisest töötajaid alati teavitama. Magistritöö autor on seisukohal, et teavitamise protsessis ei tohi näha pelgalt formaalsust: reeglina teavitatakse töötajaid video- ja valvekaamerate kasutamisest töökohal kas töölepingus või fikseeritakse see ettevõttesiseses töökorralduse eeskirjas. Autor arvab, et läbipaistvuse põhimõttega võib vastuolus olla olukord, kus teavitamine kujutab endast üksnes töötaja allkirja andmist juhendile või eeskirjale. Läbipastvuse põhimõtet arvesse võttes ja et teavitamine täidaks oma eesmärki, peaks töötaja selgelt aru saama andmetöötluse vajadusest, ulatusest, põhimõtetest ja protsessidest. Igasugune jälgimistegevus eeldab töötajate eelnevat teavitamist ning õiguspärast jälgimist käsitlevad põhimõtted ja eeskirjad peavad olema selged ja lihtsasti juurdepääsetavad.[65] Seoses üldmääruse artiklist 32 tuleneva kohustusega tagada töötajate

[63] K. Saarep. Kaameraid kasutatakse töökohtadel tihti valedel eesmärkidel - Tööelu 01/18
[64] Article 29 Data protection Working Party. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7(f) of Directive 95/46/EC. Arvutivõrgus: https://ec.europa.eu/justice/article-29/press-material/public-consultation/notion-legitimate-interests/files/20141126_overview_relating_to_consultation_on_opinion_legitimate_interest_.pdf (14.03.2019).
[65] Article 29 Data protection Working Party. Opinion 2/2017 on data processing at work. Lk. 23. Arvutivõrgus: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169. (20.01.2019).

andmete turvalisus, on oluline töötajaid teavitada ka sellest, kuidas töötaja isikuanmdeid organisatsioonis kaitstakse.

Praktikas on just läbipaistvuse põhimõttega arvestamine ja sellest tulenev töötajate nõuetekohane teavitamine osutunud probleemiks. Ehk situatsioonides, kus tööandjal on olemas õigustatud huvi kaamerate kasutamiseks, ei ole sageli täidetud läbipaistvuse põhimõte - tööandjad ei teavitata oma töötajaid kaamerate kasutamisest korrektselt. Tööandjate seas on levinud ka arusaam, et kaamerad on iseenesestmõistetavad ning nende kasutamisest ei olegi vaja töötajaid teavitada ega jälgimise eesmärke selgitada. Tööandjad põhjendavad töötajate mitte-teavitamist näiteks väitega, et kaamerad on ju kõigile nähtavad.[66] Autor on seisukohal, et pelk asjaolu, et jälgimisseade ei ole varjatud ja on töötajale silmaga nähtav, ei saa mingil juhul olla piisavaks "selgituseks". Töötajale peab olema teada, mis eesmärgil jälgimisseadet kasutatakse, mis ajal ja mille alusel see töötaja tegevust salvestab, kui laiaulatuslik on jälgitav ala, millised on jälgimisseadme tehnilised näitajad (heli-, pildi ja logifailide salvestamise võimalus, objektiivi pööramis ja suurendamisvõimalus) jms. Samuti on töötaja jaoks olulise tähtsusega teave, kellel on võimalik pilti edastava seadme kaudu kogutud andmeid töödelda, kuidas on tema kohta käivad andmed kaitstud kolmandate isikute eest, millise aja jooksul salvestisi säilitatakse jms.

Video- ja valvekaamerate kasutamisel soovitab AKI kasutada kombineeritud teavitamissüsteemi, kus lisaks töötajate eelnevale põhjalikule teavitamisele, mis mh. kirjeldab jälgimisseadmete kasutamise eesmärki; jälgitavat ala; jälgimise aega ja -liiki; jälgimisseadme tehnilist kirjeldust; jälgimisega kogutud andmete töötlejate andmed; andmete kaitse mehhanismid; salvestiste säilitamise aeg; salvestistega tutvumise kord, paigutatakse jälgimisalasse arusaadavad märgistused.[67]

Läbipaistvuse põhimõtte kohaselt peab töötajale olema tagatud lisaks õigus tutvuda video- või valvekaamerate kaudu tema kohta kogutud teabega[68], s.h. salvestistega[69]. Võimaluse korral peaks vastutav töötleja saama anda juurdepääsu turvalisele süsteemile, kus andmesubjekt saab otse

[66] K. Saarep. Kaameraid kasutatakse töökohtadel tihti valedel eesmärkidel - Tööelu 01/18

[67] Andmekaitse inspektsioon. Juhis personalitootajale: isikuandmed töösuhtes. Lk. 16. Arvutivõrgus: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikuandmed%20t%C3%B6%C3%B6suhetes%20juhis%20personalit%C3%B6%C3%B6tajale.pdf. (22.02.2019).

[68] Andmekaitse üldmäärus art. 15. Andmesubjekti õigus tutvuda andmetega.

[69] Andmekaitse inspektsioon. Juhis personalitootajale: isikuandmed töösuhtes. Lk. 16. Arvutivõrgus: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikuandmed%20t%C3%B6%C3%B6suhetes%20juhis%20personalit%C3%B6%C3%B6tajale.pdf. (22.02.2019).

tutvuda oma isikuandmetega. Tööandja võib juurdepääsu andmisest keelduda juhul, kui see võib kahjustada kolmandate isikute õigusi ja vabadusi, näiteks sisaldab ka isikuandmeid teiste töötajate kohta. Magistritöö autor toob välja mõistliku lahendusena üldmääruse valguses töötajaportaali loomise, kus töötaja ise näeb enda kohta kogutud andmeid. Teisalt autor nendib, et sellise keskkonna loomine ja haldamine võib olla tööandja jaoks kulukas.

Kaameraid kasutades tuleb olulist tähelepanu pöörata ka isikuandmete töötlemise turvalisuse põhimõttele. Just igasugune filmi ja videomaterjal võib tekitada tihti soove selle väärkasutamiseks.[70] Kasutades töötajate jälgimiseks kaameraid peavad olema rakendatud nii füüsilised ja infotehnoloogilised turvanõuded, mis tagavad kogutud isikuandmete turvalisuse. Turvalisuse põhimõttest lähtudes peab olema ettevõttes selgelt kindlaks määratud isikute ring, kellel on õigus kaamerapildile ja -valvestisele juurde pääseda ning võetud kasutusele asja- ja ajakohased infotehnoloogilised meetmed välistamaks volitamata isikute juurdepääsu töötajate isikuandmetele. Kui ettevõttesiseselt ei ole kindlaks määratud, millistel töötajatel on õigus kaamera kaudu kogutud isikuandmeid töödelda, võib tekkida olukord, kus isikuandmete lekke või kaotsimineku korral ei ole võimalik kindlaks teha, kes ja mis põhjustel informatsiooni lekitas või selle kustutas.[71]

Tööelu praktikast nähtub, et tööandjad suhtuvad jälgimisseadmete kasutamisesse pigem kergekäeliselt ega suuda selgelt põhjendada oma õigustatud huvi kaamerate kasutamiseks. Samuti eksitakse sageli andmekaitse üldpõhimõtete vastu ning isegi ei kaaluta teisi meetodeid jälgimistegevusele seatud eesmärkide saavutamiseks. Autor on arvamusel, et olukorra parandamiseks ei ole ilmtingimata vajadust reguleerida kaamerate kasutamist seaduse tasandil, ent kindlasti on vaja korrastada ja täiendada AKI juhist. Varasem IKS lubas tööandjal kaameraid kasutada näiteks vara ja isikute kaitseks – seda põhimõtet on sisustatud ka AKI juhendis. Käesoleval hetkel kehtivad isikuandmete kaitset reguleerivad õigusaktid sellist alust ette ei näe. Autori hinnangul ei ole tööandja poolne õigustatud huvi tõendamine üldsõnalise viitega vara kaitsmisele ka piisav. Autor on seisukohal, et vaatamata isikuandmete kaitse üldmääruse sätete abstraktsusele, seavad need pigem kitsad võimalused töötajate jälgimiseks kaamerast. Eelkõige

[70] Andmekaitse inspektsioon. Isikuandmete töötlemine töösuhtes. Abistav juhendmaterjal. Lk 69. Arvutivõrgus: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikuandmed%20t%C3%B6%C3%B6suhetes%20juhendmaterjal26%2005%202014_0.pdf. (10.01.2019).

[71] A. Ojaver. Valvekaamerate kasutamine töökohtadel ja kaubanduspindadel – kontrollide sõnaline kokkuvõte. 24.10.2010. Arvutivõrgus: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Valvekaamerate%20seire.pdf, (14.03.2019).

seetõttu, et õigustatud huvi kaamera kasutamiseks töökohal tuleb põhjendada selgelt ja ühemõtteliselt.

Autor on seisukohal, et video- ja valvekaamerate kasutamise valdkokonnaga tuleb aktiivselt tegeleda: kuna tegelik tööelu näitab, et tööandjad suhtuvad kaamerate kasutamisesse pigem kergekäeliselt, on oluline võtta suund pigem tööandjate teadlikkuse tõstmisele. Täiendava tööõigusliku eriregulatsiooni loomiseks ei näe autor käesoleva hetkel vajadust, sest isikuandmete kaitse üldmäärus seab kaamerate kasutamisele suhteliselt kitsad piirid. Lisaks ei ole autori hinnangul võimalik anda ammendavat loetelu olukordadest, kus kaamerate kasutamine on/ei ole lubatud – tööelu ei ole alati must-valge, mistõttu tuleb igas konkreetses situatsioonis kaaluda ja hinnata õigustatud huvi olemasolu. Kahtlemata vajab aga kaasajastamist AKI isikuandmete töötlemise juhis ning seda üldmääruse ja sellest tulenevate õiguslike aluste ja põhimõtete valguses.

2.3. Asukoha määramise seade

2.3.1. Asukoha määramise seadme kasutamine töösuhte kontekstis

Jälgimisseadmeteks loetakse ka globaalse asukoha määramise seadmeid (inglise keeles *Global positioning system*, edaspidi GPS seadmed), mis võimaldavad tööandjal kindlaks määrata inimese või eseme, näiteks sõiduki asukoha.[72]

Reeglina kasutavad GPS seadmeid need ettevõtted, kellel on märkimisväärne sõidukipark või ettevõtted, kelle tegevusvaldkond hõlmab kaupade või inimeste vedu. Varasema põlvkonna GPS seadmed võimaldasid tööandjal kindlaks määrata üksnes sõiduki asukohta, ent tänased seadmed, sõltuvalt tehnoloogiast, edastavad tööandjale oluliselt rohkem teavet. Näiteks edastavad uuemad seadmed informatsiooni sõitja isiku, kiiruse ja sõidustiili kohta. Mõned GPS seadmed on varustatud ka kaameraga, mis võimaldavad salvestada või reaalajas jälgida sõiduki juhti ja/või teekonda. Samuti on valdav osa tänastest nutiseadmetest varustatud positsioneerimistarkvaraga, mistõttu on töötaja asukoha kindlakstegemine muutunud tööandja jaoks äärmiselt lihtsaks. Igasugune teave, mis saab tööandjale teatavaks positsioneerimist võimaldavate seadmete abil,

[72] Tööinspektsioon. Isikuandmed töösuhtes ja reeglid töökorraldusele. Lk 7. Arvutivõrgus: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikuandmed-toosuhetes_ja_reeglid_tookorraldusele_1.pdf

kujutab endast töötaja isikuandmeid, mistõttu peab sellise informatsiooni töötlemine vastama õigusaktidele.

2.3.2. Õiguslik alus asukoha määramise seadme kasutamiseks

Töötaja või tema sõiduki asukoha jälgimiseks või kindlakstegemiseks peab olema tööandjal selge õigustatud huvi. Tööandja õigustatud huvi sõiduki asukoha kindlaks määramiseks võib olla seotud sõidukite varguste tuvastamise ja lahendamisega. Kahtlemata aitab positsioneerimisfunktsioon kaasa sõidukite varguste avastamisele ja parimal juhul ka lahendamisele.[73] Võttes arvesse üldmäärusest tulenevat nõuet, mille kohaselt tööandja peab formuleerima oma õigustatud huvi konkreetselt ja ühemõtteliselt, leiab autor, et pelk hirm oma vara varguste suhtes ei pruugi olla piisav.

Samuti võib tööandja õigustatud huvi võib olla seotud äriliste eesmärkidega. Eelkõige inimesi, aga ka mitmesugust kaupa vedavate sõidukite puhul on õigeaegselt asukohta jõudmine äärmiselt oluline. Sellisel juhul on tööandjal õigustatud huvi GPS seadmete paigaldamiseks ja sõiduki viibimise korral selle asukoha ja selle liikumist takistavate põhjuste väljaselgitamiseks töödelda asukohaandmeid. Magistritöö autor on seisukohal, et õigustatud huvi hindamisel tuleb siiski igal juhul kaaluda ja hinnata, kas GPS seadme kasutamiseks on konkreetne ja ühemõtteline õigustatud huvi ning kas esineb reaalne jälgimisseamdete rakendamise vajadus. Isegi kui ettevõtte põhitegevuseks on kaupade või inimeste vedu, võib töötajate asukohaandmete töötlemine ületada lubatud piire. Seda näiteks olukorras, kus töökorraldus näeb ette, et töötajad organiseerivad oma reise iseseisvalt.[74]

Tööandja õigustatud huvi GPS seadmete paigaldamiseks võib olla seotud ka ametiautode sõidupäeviku pidamisega. Eestis on GPS jälgimissüsteem laialt kasutusel sõidupäeviku pidamise abivahendina.[75] Autor on seisukohal, et sellisel juhul ei saa tööandja tegevust samastada

[73] Fact sheet privacy and monitoring at work under the GDPR. – Legal ICT Amsterdam. Lk. 5. Arvutivõrgus: https://legalict.com/content/uploads/sites/2/2017/07/Fact-sheet-Privacy-and-monitoring-at-work-under-the-GDPR-Legal-ICT.pdf (22.02.2019).
[74] Article 29 Data protection Working Party. Opinion 2/2017 on data processing at work. Lk 20. Arvutivõrgus: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169. (20.01.2019).
[75] Andmekaitse inspektsioon. Isikuandmete töötlemine töösuhtes. Abistav juhendmaterjal. Lk 73. Arvutivõrgus: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikuandmed%20t%C3%B6%C3%B6suhetes%20juhendmaterjal26%2005%202014_0.pdf. (10.01.2019).

jälgimisega. Vaatamata sellele, et tööandjal on õigustatud huvi GPS seadme kasutamiseks, peab see olema eesmärgipärane. Tööandjal ei ole õigustatud huvi andmetöötlusele seatud eesmärgist ehk sõidupäeviku pidamisest, kõrvale kalduvateks tegevusteks, näiteks töötaja asukoha pisteliseks kontrolliks.

Üldjuhul ei saa tööandjal olla õigustatud huvi töötaja jälgimiseks GPS seadme abil reaalajas.[76] Töötaja reaalajas jälgimise lubatavus võib kõne alla tulla üksnes väga erandlikel juhtudel, näiteks olukorras, kus sõiduk on varastatud või kui teel olev saadetis hilineb ning sõiduki asukoha kindlakstegemiseks teised võimalused puuduvad.[77]

Mitmetel juhtudel teenib aga GPS seadmete kasutamine nii töötaja kui ka tööandja huve, näiteks võimaldab jälgimistehnoloogia tagada sõidukit juhtiva töötaja ohutust liiklusavarii korral, kus on töötaja asukoha kiire tuvastamine eluliselt tähtis. Ka sõiduki tehnilise rikke korral on oluline töötaja asukoht operatiivselt kindlaks teha. Sellisel juhul on tuvastatav tööandja õigustatud huvi sõiduki asukoha kindlaksmääramiseks.

Nii nagu video- ja valvekaamerate puhul, ei ole tööandjal lubatud GPS-seadmete abil kontrollida töötajate töö kvaliteeti ja hulka. Ka töötajate pisteline seire ei ole reeglina lubatud, kui seireks on teisi, töötaja privaatsust vähem riivavaid võimalusi.

Autor leiab, et kõige probleemsemad situatsioonid praktikas on kahtlemata sellised, kus töösõidukit on lubatud kasutada ka isiklikuks otstarbeks või väljaspool tööaega. Arvestades asukohaandmete tundlikkust, on vähetõenäoline, et tööandjal esineb õigustatud huvi töötajate sõidukite asukoha jälgimiseks väljaspool tööaega[78] või TLS § 42 sätestatud töötajale ettenähtud vabal ajal. Nimetatud säte võimaldab töötajal külastada tööaja siseselt näiteks arsti või teha muid isiklikke toiminguid, mistõttu kujutavad asukohaandmed sellises kontekstis töötaja privaatseid andmeid ja jälgimistegevus on seetõttu keelatud.

[76] Tööinspetsioon. Isikuandmed töösuhtes ja reeglid töökorraldusele. Lk 7.
[77] Fact sheet privacy and monitoring at work under the GDPR. – Legal ICT Amsterdam. Lk. 5. Arvutivõrgus: https://legalict.com/content/uploads/sites/2/2017/07/Fact-sheet-Privacy-and-monitoring-at-work-under-the-GDPR-Legal-ICT.pdf (22.02.2019).
[78] Article 29 Data protection Working Party. Opinion 2/2017 on data processing at work. Lk 20. Arvutivõrgus: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169. (20.01.2019).

2.3.3. Asukoha määramise seadme kasutamise põhimõtted

GPS seadmete kasutamisel peab tööandja lisaks oma õigustatud huvi tõendamisele lähtuma ka andmekaitse üldpõhimõtetest. GPS-seadmete kaudu kogutud isikuandmete töötlemine peab olema proportsionaalne ning kui andmetöötlusele seatud eesmärke on võimalik saavutada töötaja privaatsust vähem riivavate meetmetega, tuleks eelistada neid. Üheks proportsionaalsemaks meetodiks on autori hinnangul seada töötajale nõue aruandluse esitamiseks töösõitude kohta.

Olukorras, kus töösõidukit kasutatakse ka isiklikuks otstarbeks, on proportsionaalne kasutada sellist GPS-seadet, millel on võimalus asukoha jälgimise funktsioon ajutiselt välja lülitada kui teatavad asjaolud, näiteks arstivisiit, põhjendavad sellist väljalülitamist.[79] Varguste tuvastamiseks on mõistlik kasutada seadet, mis on võimeline tuvastama ja märku andma sõiduki väljumist selle tavapärasest ja kokkulepitud tööpiirkonnast. Olenevalt ettevõtte tegevuspiirkonna suurusest võib ee olla määratletud linna, maakonna või riigi täpsusega. Nii ei piirata liigselt autot juhtiva töötaja privaatsust, ent siiski on võimalik tööandjal kaitsta oma vara.

Töötajat tuleks jälgida minimaalselt ehk üksnes ulatuses, mis on eesmärgi saavutamiseks vältimatult vajalik. Üldjuhul ei ole minimaalsuse põhimõtte ga kooskõlas ega proportsionaalne töötaja asukoha pidev jälgimine.

Nii nagu kõigi teiste jälgimisviiside kasutamisega, tuleb töötajat GPS seadmete kasutamisest selgesõnaliselt teavitada. Töötaja peab olema teadlik, et töösõidukile, millega ta sõidab, on paigaldatud jälgimisseade ning tema liikumisi salvestatakse. GPS seadmete puhul oleks lisaks mõistlik vastav teave kuvada igas jälgitavas autos märgatavalt ja juhi jaoks nähtavas kohas.[80]

Jälgimine peab olema seotud konkreetse ja ühemõttelise eesmärgiga. Eesmärgipärasuse tagamiseks ei ole lubatud GPS seadmeid, mis on paigaldatud sõidukitesse tööandja vara (sõiduki) või töötaja ohutuse tagamiseks, kasutada ka töökohustuste rikkumise tõendamiseks.[81]

Magistritöö autor toob välja tõenäoliselt olulisima põhimõtte, millest tuleb GPS jälgimisseadmeid kasutades lähtuda. Artikli 29 alusel asutatud andmekaitse töörühm on oma arvamuses 13/2011 märkinud järgmist: *GPS seadmed, mida kasutatakse sõidukite jälgimiseks, ei ole mõeldud töötajate jälgimiseks. Seadmete ülesandeks on jälgida üksnes sõidukit, kuhu nad on paigaldatud. Tööandjad*

[79] Samas. Lk 20
[80] Samas. Lk 20
[81] Tööinspetsioon. Isikuandmed töösuhtes ja reeglid töökorraldusele. Lk 7.

ei tohi kõnealuseid jälgimisseadmeid kasutada autojuhtide või teiste töötajate asukoha kindlakstegemiseks või käitumise jälgimiseks.[82]

Eelnevale tuginedes järeldab autor, et GPS seadmete kasutamise õiguslik alus on pigem piiratud, olles seotud tihedalt ettevõtte tegevusvaldkonnaga. Vaatamata sellele, et tööandja õigustatud huvi mõiste on lai, on sellele tuginemine GPS seadmete kasutamisel suhteliselt kitsas. Seetõttu julgeb autor väita, et ka töötaja õigus isikuandmete kaitsele on hästi tagatud. Praktilise probleemina toob autor välja, et isikuandmete kaitse ulatus sõltub paljugi sellest, kui hästi tööandja isikuandmete kaitse üldmääruses kehtestatud põhimõtteid järgib. Tööõigusliku eriregulatsiooni kehtestamisega ei ole autori hinnangul mõistlik GPS seadmete kasutamist reguleerida, sest nagu ka kaamerate puhul, ei ole võimalik andma ühtset loetelu lubatud kasutusvõimaluste kohta.

2.4. Raadiosagedustuvastusel põhinev identifitseerimistehnoloogia

2.4.1. Raadiosagedustuvastusel põhineva tehnoloogia kasutamine töösuhte kontekstis

Laialt kasutusel tehnoloogiline abivahend, mis esmapilgul ei viita jälgimistegevusele, ent mille kaudu on võimalik tööandjal koguda suurel määral informatsiooni töötajate kohta, on raadiosagedustuvastuse identifitseerimistehnoloogial (inglise keeles *radio-frequency identification*, edaspidi RFID-identifitseerimistehnoloogia) põhinev kiipkaardi süsteem. Töötajale väljastatud kiibi lugemisel toimub töötaja identifitseerimine süsteemi kesksеadmes, mis kas lubab või keelab töötajal soovitud ruumi või alale pääsemist. Kusjuures kogu informatsioon töötajate liikumiste kohta salvestub kesksüsteemi andmebaasi. RFID tehnoloogia kasutamine iseenesest ei riiva töötaja õigust privaatsusele, küll aga on praktikas leitud süsteemile eesmärgist kõrvalekalduvaid kasutusviise, mis kindlasti pole kooskõlas privaatsuse ja andmekaitse reeglitega.[83] Eesmärgipärane kasutus aitab tagada kõrvaliste, volitamata isikute sattumist ettevõtte

[82] Article 29 Data protection Working Party. Opinion 13/2011 on Geolocation services on smart mobile devices. 05/2011. Lk. 14. Arvutivõrgus: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf (15.03.2019).
[83] C. Russell. The use of RFID in the workplace sparks privacy concerns. Blogi Olender Feldman – Attorneys at law. Arvutivõrgus: https://www.olenderfeldman.com/rfid-and-workplace-privacy/, (11.03.2019).

ruumidesse – see ühelt poolt tagab töötajatele suurema turvatunde, teisalt on tööandja vara paremini kaitstud.

2.4.2. Õiguslik alus raadiosagedustuvastusel põhinevate seadmete kasutamiseks

Iga kiipkaardi lugemine registreeritakse ning vastav info salvestub omakorda andmebaasi. Seni, kuni kiipkaarti kasutatakse üksnes töötaja identifitseerimiseks ja läbipääsu võimaldamiseks, ei kujuta tegevust ohtu töötaja privaatsusele. Kuna tööruumidesse sisenemise, korruste vahel liikumise ja ettevõttest väljumise info salvestub andmebaasi, on võimalik tööandjal sealseid andmeid töödelda nii, et teha kindlaks töötaja liikumine mingi perioodi, näiteks tööpäeva jooksul või jälgida töötaja tööle tuleku ning lahkumise aega. Tööandjal võib olla õigustatud huvi tööle tuleku ja töölt lahkumise aja jälgimiseks olukorras, kus tööaja arvestus toimub kiipkaardi registreerimise alusel. Kui tööaja arvestus on ettevõtte sisekorraeeskirjade või töölepinguga kokku lepitud teiste meetoditega, ei saa tööandjal olla õigustatud huvi töökohale saabumise ja sealt lahkumise andmete töötlemiseks.

Kirjanduse ja meediaväljaannete põhjal ei ole võimalik leida näiteid töötajate jälgimisest RFID süsteemide abil Euroopas, küll aga USA-s. Magistritöö autor möönab, et kuigi näited Euroopa Liidu kohta puuduvad, ei saa siiski väita, et tööandjad RFID süsteeme töötajate jälgimiseks ei kasuta. Kuna andmed töötaja liikumise kohta paiknevad tööandja infosüsteemides, on viimasel võimalik teostada jälgimistegevust varjatult ja töötaja ei pruugi oma jälgimisest üldse teadlik olla. Andmekaitsereegleid silmas pidades ei saa tööandjal olla aga õigustatud huvi töötajate asukoha varjatud jälgimiseks. Teema tõsidust rõhutab autor näitega USA praktikast, kus töötaja asukoha jälgimine ei riivanud mitte üksnes töötaja privaatsust, vaid ka inimväärikust. USA ettevõte *WaterSaver Faucet Co.* paigaldas kiipkaardi lugeja tootmishoones paiknevatele tualettidele, jälgimaks, et töötajad seal liiga kaua ei viibiks. Jälgimistegevuse tulemusel väljastas tööandja mitmele töötajale hoiatuse, mille kohaselt on töötajal lubatud ühe tööpäeva jooksul viibida tualetis maksimaalselt 6 minutit. Reegli mittejärgimisel kaasneks juba vastav distsiplinaarkaristus.[84] Tualetis viibimise aja jälgimise näiteid saab tuua ka Hiina, Jaapani ja Korea tootmisettevõte

[84] S. Kim. Company Limits Worker Bathroom Use to 6 Minutes a day, Union claims. – ABC News. 16.07.2014. Arvutivõrgus: https://abcnews.go.com/Business/regulate-bathroom-work/story?id=24581940, (14.03.2019).

põhjal.[85] Autor on seisukohal, et tööandjal ei saa olla mingil juhul õigustatud huvi andmete töötlemiseks tualetis veedetud aja kohta.

Autor toob näite, et töötaja asukoha jälgimiseks võib tööandjal olla õigustatud huvi ka siis, kui töötamine eeldab viibimist ekstreemsetes või kõrge turvariskiga oludes (tehas, vangla jms), kus on ohu korral oluline kiire reageerimine. Sellisel juhul on õigustatud huvi seotud töötajate ohutuse tagamisega on oluline ja nende liikumise tuvastamine on oluline eelkõige töötaja enda turvalisuse tagamiseks.

2.4.3. Raadiosagedustuvastusel põhinevate seadmete kasutamise põhimõtted

Eeldusel, et tööandjal on õigustatud huvi RFID seadmete kaudu kogutud isikuandmete töötlemiseks, peavad olema lisaks täidetud kõik andmekaitse üldpõhimõtted. Näiteks olukorras, kus tööandja töötleb RFID seadmete kaudu kogutud andmeid eesmärgiga pidada tööaja arvestust, tuleb töötajaid sellest selgelt ja arusaadavalt teavitada. Töötajad peavad olema teadlikud sellest, et nende tööle tuleku ja lahkumise aeg fikseeritakse ning selle alusel arvestatakse tööaega. Autori arvates oleks mõistlik kindlaks määrata lisaks reeglid selle kohta, millised on protseduurireeglid olukorras, kus töötaja unustab oma kiibi koju või kui mitu töötajat sisenevad üheaegselt.

Magistritöö autor leiab, et ettevõtetes, kus turvariskid on pigem madalad ning uksekaardisüsteem on paigaldatud üksnes kolmandate isikute juurdepääsu piiramiseks, oleks minimaalsuse ning proportsionaalsuse põhimõtetega ja mõistlik kooskõlas kasutada selliseid tehnoloogilisi lahendusi, mis küll võimaldavad kontrollida ja piirata sissepääsuõigust, ent ei võimalda jälgida isiku liikumist. Nii ei teki tööandjal probleemide ilmnemisel, pistelise kontrolli teostamise või tööajast kinnipidamise kontrollimise eesmärgil "ahvatlust" töötajate liikumist jälgida.

RFID tehnoloogial põhinevate seadmete kaudu isikuandmete töötlemine võib autori arvates kahtlemata ohustada töötaja õigust isikuandmete kaitsele ja seeläbi privaatsusele, kuid arvestades isikuandmete kaitse üldmäärusest tulenevaid nõudeid on praktikas kõnealuste seadmete kaudu isikuandmete töötlemine lubatud üksnes äärmiselt piiratud olukordades. Sellele tugindedes on autor seisukohal, et kuna andmekaitse üldreeglid ei võimalda töötajaid RFID tehnoloogial põhinevate seadmete kaudu jälgida, on nende isikuandmete kaitse tagatud piisavalt. Tõenäoliselt

[85] Chinese workers hold managers hostage after toilet break changes. – The Guardian. 22.01.2013. Arvutivõrgus: https://www.theguardian.com/world/2013/jan/22/chinese-managers-hostage-toilet-breaks (14.03.2019).

jääb praktikas puudu tööandjate teadlikkusest kõnealuse tehnoloogia rakendamisel ja selle kaudu kogutud andmete töötlemisel, mistõttu on oluline tegeleda tööandjate teadlikkuse kasvatamisega.

2.5. Kontaktivaba lähivälja identifitseerimistehnoloogia

2.5.1. Kontaktivaba lähivälja identifitseerimistehnoloogia kasutamine töösuhte kontekstis

Kontaktivaba lähivälja identifitseerimistehnoloogia (inglise keeles *Near Field Communication*, edaspidi NFC) võimaldab sarnaselt RFID tehnoloogiale raadiosageduse kaudu informatsiooni vahetada. Põhimõtteline ja olulisim erinevus kahe tehnoloogia vahel on, et NFC signaaliedastus ja seeläbi töötaja identifitseerimine on kontaktivaba ning toimub väiksema vahemaa tagant. Tegemist on käesoleval hetkel paljulubava ning väga mitmeid kasutusvõimalusi pakkuva tehnoloogiaga – lisaks isikute tuvastamisele kasutatakse NFC tehnoloogiaga kiipe laialdaselt mobiiltelefonides, ühistranspordi sõidukaartides ning viipemakse võimalusega pangakaartides.

NFC tehnoloogiat kasutatakse seadmetes, mis töötlevad isiku tuvastamiseks biomeetrilisi isikuandmeid, näiteks sõrmejälje lugeja (inglise keeles *fingerprint scanner*), näotuvastus (inglise keeles *facial recognition*) või silma sõrkkesta skänner (inglise keeles *iris scanner*). Ehk NFC tehnoloogial põhineva sikutuvastussüsteemi puhul ei pea töötaja identifitseerimiseks kaasas kandma kiipi, vaid töötajaid tuvastatakse nende biomeetriliste andmete põhjal. Uueks suunaks seoses NFC tehnoloogiaga on aga töötajate "kiibistamine", mis hõlmab pisikese kiibi sisestamist inimese kätte, mille abil on edaspidi võimalik ettevõtte hoones ringi liikudes ilma füüsilist kiipkaarti kaasas kandmata uksi avada või kohvi võtta.[86]

2.5.2. Töötaja biomeetrial põhineva identifitseerimistehnoloogia kasutamise võimalused

Kaasaegsetes kontorites ja tootmisettevõtetes on tavapäraseks kujunenud RFID identifiteerimistehnoloogial põhineva kiipaardisüsteemi kasutamine, seda nii ettevõtte välisuksest

[86] K. Kook. Tallinna ettevõte kiibistab töötajaid. – Digigeenius. 18.04.2017. Arvutivõrgus: https://digi.geenius.ee/rubriik/uudis/tallinna-ettevote-kiibistab-enda-tootajaid/, (17.03.2019)

sisenemiseks, aga ka eri ruumide või korruste vahel liikumiseks. RFID kiipkaardisüsteem on küll efektiivne, ent tihtipeale tülikas – kiipkaardi koju unustamisel ei ole töötajal võimalik ettevõttesse siseneda. Samuti kaasneb füüsilisel kujul kiibiga alati oht selle kaotamiseks või kuritarvitamiseks. Seetõttu on üha enam hakatud arendama ja tootma isikutuvastussüsteeme, mis põhinevad töötaja biomeetrial. Ehk isikutuvastussüsteem on lahendatud selliselt, et töötajate tööle tulek, tööruumides liikumine ning vajadusel ka tööaja registreerimine toimub ilma lisavahendeid, s.t. kiipi kasutamata. Ehk sisuliselt pole ettevõtte ruumidesse sisenedes või ringi liikudes enam kiipkaarti vaja ning läbipääsuks piisab sõrmejälje (või muu biomeetrilist informatsiooni kandva jäljendi või omaduse) registreerimist läbipääsuseadmel, mis isikutuvastuse õnnestumisel võimaldab töötajale soovitud läbipääsu. Kõnealuse tehnoloogia suurimaks miinuseks on selle tänane ebatäpsus – sageli tuleb töötajal registreerida oma sõrmejälg mitmel järjestikkusel korral, enne, kui süsteem ta tuvastab.

Töötajate tööle saabumise ja sealt lahkumise aega ning ettevõtte ruumides või territooriumil liikumise kohta käivaid andmeid võimaldavad töödleda ka seadmed, mis kasutavad identifitseerimiseks töötaja biomeetrilisi isikuandmeid. Käesoleval hetkel on biomeetrilist informatsiooni (mitmesugused bioloogilised, füüsilised, psühholoogilised, käitumislikud või sarnased omadused, mida kasutatakse isiku või isikusamasuse tuvastamisel)[87] töötlevad seadmed kasutusel piiripunktides, ent Eesti ettevõtetes leiavad need pigem vähem kasutust. Siiski on võimalik leida näiteid ettevõtete ja asutuste kohta, kus maja-, territooriumi- või võrgusisene liikumine on piiratud ning füüsilisse ruumi või küberruumi sisenemiseks on vajalik skanneerida sõrmejälg. Arvestades suuri andmelekkeid ning küberrünnakute kasvu, on mitmed suured ettevõtted nagu *Microsoft* ja *Facebook* kasutusele võtnud biomeetrilise autentimise võimalused, mis tuvastab töötaja tema näoilme, sõrmejälje või silma võrkkesta alusel.[88] Biomeetriline autentimine võimaldab töötajatel logida arvutisse, telefoni jt. seadmetesse ning pääseda juurde mitmesugustele andmekogude, kas füüsiliselt arhiivis või elektrooniliselt serveris. Magistritöö autorile ei ole teada, kas ja millistel eesmärkidel kasutavad tänased Eesti tööandjad biomeetrilisi isikutuvastusvahendeid, kuid tõenäoliselt leiavad need käesoleval hetkel kasutust pigem vähe. Teisalt erinevad uuringud näitavad, et aastaks 2020 läheb ligi 90% IT valdkonna ettevõtetest klassikalistelt tuvastusmeetmetelt (salasõna, kiipkaart jms) üle biomeetriliste

[87] Andmekaitse inspektsioon. Isikuandmete töötlemine töösuhtes. Abistav juhendmaterjal. Lk 54. Arvutivõrgus: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikuandmed%20t%C3%B6%C3%B6suhetes%20juhendmaterjal26%2005%202014_0.pdf, (10.01.2019).

[88] S. Larson. Beyond passwords. Cpompanies use fingerprints and digital behaviour to ID employees. – CNN Business. Arvutivõrgus: https://money.cnn.com/2018/03/18/technology/biometrics-workplace/index.html, (14.02.2019)

isikutuvastusvahenditele. Mitmesugused uuringud kinnitavad, et juba käesoleval hetkel on IT sektoris biomeetrilise autentimise kasutusele võtnud ca 62% ettevõtetest.[89] Eelnevale tuginedes võib järeldada, et tehnoloogia arenedes ja küberturvalisuse huvides võivad tänased isikutuvastuse seadmed asenduda üsna pea biomeetrilist informatsiooni töötlevate seadmetega.

2.5.3. Õiguslik alus biomeetriliste isikuandmete töötlemiseks

Kasutades töötaja biomeetrial põhinevaid isikutuvastussüsteeme tuleb arvestada, et igasugune biomeetriline materjal ja jäljendid kujutavad endast eriliiki isikuandmeid (varasema sõnastuse järgi delikaatsed isikuandmed) mille töötlemisõigus on väga piiratud. Üldmääruse art. 9 (1) kohaselt ei ole eriliiki isikuandmete, s.h. biomeetriliste isikuandmete töötlemine üldjuhul lubatud ja tööandjal puudub selliste andmete töötlemiseks õigustatud huvi. Eriliiki andmete töötlemisega seonduvat on lubatud liikmesriikidel üldmääruse art 9 (4) kohaselt täiendavalt reguleerida, s.h. täiendada piiranguid seoses geneetiliste, biomeetriliste või terviseandmete töötlemisega. Erandid eriliiki isikuandmete töötlemise üldisest keelust peaksid olema liikmesriigi õigusega sõnaselgelt ja ühemõtteliselt sätestatud. Tänane eriliiki isikuandmete regulatsioon on töötajate jälgimise ja kontrollimisega seonduvalt autori arvates võrdlemisi üldsõnaline. Arvestadae, et tööandjad rakendavad üha enam töötaja biomeetrilisi isikuandmeid töötlevaid isikutuvastusseadmeid, võib tulevikus olla vajalik eriliiki andmete töötlemise osas regulatsiooni täpsustada. Autor on seisukohal, et vaatamata oma abstraktsusele, kaitseb tänane isikuandmete üldmäärusest tulenev regulatsioon eriliiki isikuandmete töötlemise olukorras pigem töötajat, mistõttu ei ole ka töötaja privaatsuse riive tõenäoline.

Arvestades eriliiki isikuandmete töötlemise piiratust, arendatakse intensiivselt tulevikutehnoloogiaid, mille abil on võimalik vältida töötaja biomeetriliste andmete töötlemist, luues universaalseid tehislikke biomeetrilisi markereid ning mille abil on tuvastamine kiirem, kindlam ja usaldusväärsem.[90] Sisuliselt luuakse sellise tehnoloogia puhul töötaja biomeetria abil unikaalne kood, kuid biomeetrilisi andmeid eraldi ei töödelda. Selline tehnoloogia vähendab ka

[89] P. Tsai. Data snapshot: Biometrics in the workplace commonplace, but are they secure? – Spiceworks. Arvutivõrgus: https://community.spiceworks.com/security/articles/2952-data-snapshot-biometrics-in-the-workplace-commonplace-but-are-they-secure, (15.03.2019).

[90] R. Süld. Biomeetrilise isikutuvastuse levik muudab kogu ühiskonda. Postimees. 03.06.2016. Arvutivõrgus: https://arvamus.postimees.ee/3719871/rein-suld-biomeetrilise-isikutuvastuse-levik-muudab-kogu-uhiskonda (15.03.2019).

töötajate jälgimise riski, sest biomeetrial põhineva koodi alusel ei ole võimalik identifitseerida töötaja isikut. Autorile teadaolevalt on uuemates seadmetes biomeetriline algoritm, nii näotuvastuse, sõrmejäljelugeja kui silma võrkkesta tuvastuse puhul loodud selliselt, et seadme kasutaja nägu, sõlmejälge või vikerkesta jäljendit ei salvestata tervikuna mingil moel seadme andmebaasi, vaid isikutuvastuse seade võrdleb üksikuid krüpteeritud punkte. Ehk töödeldav informatsioon on anonüümne ning seda ei ole võimalik töötajatega seostada.

2.5.4. Nahaaluste kiipide kasutamise võimalused

Mitmed tööandjad üle maailma on asunud oma töötajaid kiibistama, eesmärgiga esialgu asendada üksnes uksekaart, ent tulevikulahendusena soovitakse kiibi kasutusvaldkonda oluliselt laiendada. Tehnoloogiliselt on nahaaluseke kiibile võimalik programmeerida hulk funktsioone, alates kohvimasina ja printeri kasutamise võimaldamisest lõpetades töötaja kodu ukseluku avamise ja sõiduki käivitamiseni. Lisaks on kiipe võimalik eri moel personaliseerida, näiteks programmeerida kiip selliselt, et kohviautomaadi juurde minnes teab kiip, millised on töötaja joogieelistused. Mitmed töötajate kiibistamist pooldavad tööandjad on väljendanud, et kaugemas tulevikus võiks nahaalune kiip asendada lisaks ka pangakaarti ning lausa ID-kaarti, mistõttu puuduks inimesel vajadus kaasas kanda võtmeid, rahakotti ning isikut tõendavat dokumenti.[91]

Eestis on oma töötajatele kiibid paigaldanud autorile teadaolevalt neli ettevõtet, kelle kontorid paiknevad Ülemiste City innovaatilises ärilinnakus. Linnakut arendava Mainor Ülemiste meeskonnas on kiibid juba enam kui pooltel töötajatel.[92] Vaatamata sellele, et kiipide kasutamine on invasiivne ning valus, põhjendavad nii tööandjad kui ka kiibistatud töötajad nende kasutamist eelkõige mugavusega.

Töötajate kiibistamisega seonduvalt on aga tõusetunud ka mitmeid probleeme. Vaatamata asjaolule, et nahaaluste kiipide eesmärk on uste avamine, printeri aktiveerimine jms, on võimalik

[91] The office of the future: microchipped employees. – Business World. 26.09.2018. Arvutivõrgus. https://businessworld-usa.com/office-future-microchipped-employees/ (17.03.2019).
[92] L. Kanarbik. Võtmed naha alla ehk miks Ülemiste linnaku töötajad end kiibistada lasevad. – Eesti Päevaleht. 11.10.2018. Arvutivõrgus. https://epl.delfi.ee/eesti/votmed-naha-all-ehk-miks-ulemiste-linnaku-tootajad-end-kiibistada-lasevad?id=83959080, (17.03.2019).

seda tehnoloogiat kasutada töötajate jälgimiseks. Selline laiaulatuslik kontroll tõstatab paratamatult küsimusi seoses töötajate inimväärikuse, privaatsuse, eetika ja tervisega seonduvalt.[93] Autori hinnangul saab nahaalust kiipi käsitleda püsiva jälitusseadmena, mille eemaldamine töötajal endal on keeruline. Nii nagu RFID kiipide puhul, on tööandjal võimalik jälgida tööle tulemise, lahkumise ja töökohalt eemaloleku aega ning ettevõtte ruumides liikumist. Käesoleval hetkel on nahaalune kiip seotud üksnes tööruumidesse sissepääsu ja mõnedel juhtudel kontoritehnika aktiveerimiseks. Võttes arvesse tööandjate ideid tulevikulahendusteks, kus nahaalune kiip sisaldab suures koguses isikuandmeid (pangarekvisiidid, juhiluba, id-kaart, tervise digilugu jms), muutub kiipide kasutus autori hinnangul komplitseerituks ja isegi ohtlikuks. Niivõrd suure hulga isiklike andmete hoiustamine nahalustel kiibil toob kaasa vajaduse arendada märkimisväärselt kõnealuse tehnoloogia turvalisust.

Kuna töötajatel kasutatavad kiibid ei ole läbinud ühtegi riiklikult tunnustatud testi ning ei ole sertifitseeritud[94], ei saa autori hinnangul välistada ka ohtu töötaja tervisele. Samuti on autor arvamusel, et kiibistamise eesmärgi täitmiseks ei ole vaja ilmtingimata paigaldada kiipe töötajat vigastades naha alla - NFC tehnoloogial põhineva kiibi võib paigaldada näiteks nutiseadmele, käekellale või muule esemele, mis on töötajal alati kaasas.

2.5.5. Õiguslik alus nahaaluste kiipide kasutamiseks

Kui teised käesolevas magistritöös käsitletavad tehnoloogilised vahendid eeldavad kasutamiseks tööandja õigustatud huvi olemasolu, siis nahaaluste kiipide paigaldamiseks tööandjal õigustatud huvi mingil juhul olla ei saa. Kui tööandja soovib välistada kolmandate isikute juurdepääsu ettevõtte ruumidele, siis saab jaatada tema õigustatud huvi uksekaardi süsteemi paigaldamiskes, ent kindlasti mitte nahaaluste kiipide paigaldamiseks.

[93] S. Firfiray. Microchip implants are threating worker's rights. 26.11.2018. Arvutivõrgus: https://phys.org/news/2018-11-microchip-implants-threatening-workers-rights.html, (17.03.2019).
[94] A. Pau. Tele2 paneb töötajatele naha alla riskantse kiibi. – Postimees. 11.10.2018. Arvutivõrgus: https://tehnika.postimees.ee/6426622/video-tele2-paneb-tootajatele-naha-alla-riskantse-kiibi, (17.03.2019).

Nahaaluste kiipide paigaldamine saab toimuda üksnes töötaja nõusolekul. Kusjuures töötaja nõusoleks loetakse kehtivaks vaid juhul, kui see vastab üldmäärusest tulenevatele standarditele. Töötaja nõusolek nahaaluse kiibi paigaldamiseks peab olema antud vabatahtlikult, konkreetselt, teadlikult ja ühemõtteliselt.[95] Vabatahtlik nõusolek tähendab seda, et töötajal peab olema võimalik keelduda nõusoleku andmisest nii, et sellega ei kaasneks tööta jaoks kahjulikke tagajärgi. Nõusolek hõlmab üksnes andmetöötlusele seatud eesmärki ning sellest kõrvalekalduvate eesmärkide korral tuleb töötajat teavitada ning hankida uus nõusolek. Toetudes nahaaluste kiipide kasutamisel töötaja nõusolekul põhinevale õiguslikule alusele, peavad olema täidetud järgmised nõuded:

- Nõusolek peab olema konkreetne ja teadlik, sisaldades teavet nõusoleku tagasivõtmise kohta.
- Nõusolek peab olema rangelt vabatahtlik.
- Nõusolek peab olema ühemõtteline ja selgesõnaline.[96]

Kui nahaaluse kiibi paigaldamises lepivad töötaja ja tööandja kokku dokumendis, mis sisaldab ka muud informatsiooni, näiteks töölepingus või töösisekorraeeskirjas, peab nõusolek olema:

- Esitatud viisil, mis on selgelt eristatav teistest lepingus või dokumendis sisalduvatest küsimustest.
- Esitatud arusaadavalt ja selgelt ning töötaja jaoks lihtsas keelekasutuses.[97]

Nimetatud nõuete mittetäitmise kujutab endast andmekaitse nõuete rikkumist, mis võib tööandjale kaasa tuua ulatuslikke kahjunõudeid töötajate poolt. Autor rõhutab, et kui kiibi paigaldamise õiguslikuks aluseks saab olla üksnes töötaja vabatahtlik nõusolek, siis edasine andmetöötlus, näiteks informatsiooni salvestamine, saab toimuda siis, kui tööandjal on selleks õigustatud huvi. Ehk ettevõttes, kus tööaja arvestus toimub kiibi registreerimise alusel, võib tööandjal olla õigustatud huvi vastava teabe töötlemiseks. Autor leiab, et sel juhul on mõistlik juba enne kiibi paigaldamist teavitada töötajaid kiibi kaudu kogutud andmete töötlemisest, pidades silmas kõiki üldmäärusest tulenevaid andmekaitse üldpõhimõtteid. Kui tööandja soovib töötajaid kiibistada eesmärgiga jälgida aega, millal töötajad ettevõttesse sisenevad ja sealt lahkuvad või näiteks

[95] Üldmäärus art 4 p. 11.
[96] Euroopa parlament. Tööhõive ja sotsiaalvaldkonna komisjon. The Use of Chip Implants for workers. Lk. 20. Arvutivõrgus: http://www.europarl.europa.eu/RegData/etudes/STUD/2018/614209/IPOL_STU(2018)614209_EN.pdf, (17.03.2019)
[97] Samas. Lk 20.

arvutisse sisse logivad, peab ta seda selgelt põhjendama. Autor arvab, et õigustatud huvi tõendamisel võib tööandja jaoks vähemalt käesoleval hetkel probleemiks kujuneda see, kuidas ta on suuteline põhjendama, miks on töötajate jälgimiseks ilmtingimata vaja neid kiibistada kui sama eesmärgi saab täita traditsiooniliste süsteemidega, nagu uksekaardi- või pin-koodi süsteemid.

Autor leiab, et tööandjad peavad enne töötajate kiibistamist andmekaitse reegleid hindama koostoimes tööõiguse ja põhi- ning inimõigusi sisaldavate normidega. Tänasel päeval ei ole võimalik anda selget vastust küsimusele, kas töötajate kiipimine on ebaseaduslik, riivates töötaja inimõigusi. Sõltuvalt olukorrast tuleb omavahel kaaluda võimalikke kahjusid, mis töötajale kiibi paigaldamisega võivad kaasneda töötaja õiguspäraste majanduslike huvidega.

3. Info- ja kommunikatsioonitehnoloogiavahendite ning sotsiaalmeedia kaudu kogutud isikuandmete töötlemine

3.1. Kommunikatsioon kaasaegses töökeskkonnas

Kaasaegses töökeskkonnas toimub valdav osa suhtlusest kas vahetu vestluse või kommunikatsioonivahendite kaudu. Kommunikatsioonivahenditest olulisim on kahtlemata tööandja domeeniga e-posti aadress. Tööaja säästmise eesmärgil kasutavad paljud ettevõtted majasisese suhtluse puhul töövahendina ka mitmesuguseid veebipõhiseid suhtluskanaleid nagu *messenger*, *Skype*, *WhatsApp* jne.

Samuti on levinud tendents, et töötajad kasutavad nii oma tööalaseks kui ka isiklikuks suhtluseks tööandjale kuuluvaid sidevahendeid. Töötelefoni ja tööandja domeeniga e-posti kasutatakse eravestluste pidamiseks ning sageli logitakse ka oma isiklikku e-posti kontosse või internetipanka sisse tööandjale kuuluvast arvutist, teadmata täpselt, kas sellega seatakse ohtu oma privaatsus või mitte. 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 teadasaamisest.[98]

Töötajad peavad arvestama, et kõik tööülesannete täitmiseks vajalike infotehnoloogiliste vahendite kasutamisel jätavad nad endast tööandja seadmetesse maha digitaalse jälje – olgu selleks siis arvuti nimi, IP aadress, võrgulehtede kasutamise ajalugu võrguserveri logis või töötajate tarbimisharjumuste ja -eelistuste profiili andmed otsingu- ja sotsiaalmeediateenuseid pakkuvate organisatsioonide andmebaasides.[99] Võib isegi öelda, et iga töötaja liigutuse tuvastamine on tänaseid tehnoloogilisi võimalusi arvestades reaalne, alustades interneti kasutusajaloo jälgimisest lõpetades teabega, mitu hiireklikki töötaja ühe tunni jooksul tegi jne.

Just elektroonilise teabevahetuse, näiteks telefoni, internetikasutuse ajaloo, e-posti, suhtlusplatvormide jms. jälgimist töökohal peetakse peamiseks ohuks töötaja eraelu puutumatusele.[100] Tehnoloogia areng on kaasa toonud elektrooniliste suhtlusviiside ja -kanalite

[98] O. Kirst. Sõnumisaladuse kaitse tööandja sidevahendite kasutamisel. VI/2012. Lk 421

[99] Andmekaitse inspektsioon. Töötajate arvutikasutuse privaatsus. Arvutivõrgus: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/T%C3%B6%C3%B6tajate%20arvutikasutuse%20privaatsus_.pdf (10.01.2019).

[100] Article 29 Data protection Working Party. Opinion 2/2017 on data processing at work. Lk 12. Arvutivõrgus: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169. (20.01.2019).

osakaalu suurenemise igapäevases tööelus, mistõttu on oluline pöörata tähelepanu ka privaatsusega seotud küsimustele. Tehnoloogia areng on ühelt poolt kahtlemata kaasa toonud uusi võimalusi jälgimiseks, ent arvestades privaatsuse tähtsust töökohal, on mitmed uued jälgimisviisid vähem sekkuvad. Teisalt on tööandjale kerge vaevaga kättesaadavad ka nn. kõik-ühes jälgimislahendused, näiteks turvapaketid, mis võimaldavad tööandjal jälgida kogu IKT kasutust töökohal, selle asemel, et jälgida üksnes e-posti ja/või külastatud veebisaitide ajalugu.[101] Ekslik on arvamus, et e-posti lugemine või telefonside pealtkuulamine on tehniliselt võimalik üksnes sideoperaatoritel või teatud riigivõimu esindajatel. Ainuüksi otsinguga Internetis võib kiiresti leida erinevaid tarkvara- ja muid tehnilisi lahendusi nii oma laste, truudusetu abikaasa kui soovi korral kas või töötajate arvuti- ja telefonikasutuse või muu tegevuse jälgimiseks.[102] Põhjuseid, miks tööandja otsustab töötaja sidevahendite kasutamist jälgida on mitmeid. Kuna sidevahendite kasutamine kujutab endast ressursside kulutamist, võiks ja peaks tööandjal olema õigus reguleerida ja vajadusel piirata enda poolt töötajate kasutusse antud sidevahendite kasutamist isiklikuks otstarbeks ning samuti omama õigust ka kehtestatud reeglite järgimist vajadusel kontrollida. Esiteks on nii võimalik optimeerida ettevõtte kulusid, samuti on tööandja huvitatud töötajate lojaalsusest, nende valduses oleva teabe kaitsmisest, raha ja muude resssursside sihipärasest ning mõistlikust kasutamisest ning sõltuvalt ettevõtte iseloomust ja tegevusvaldkonnast ka äri-, tootmis ning isegi riigisaladuse kaitse tagamisest.[103]

3.2. Telefon

3.2.1 Õiguslik alus telefonikõnede salvestamiseks

Oluline ja üks vanemaid kommunikatsioonivahendeid, mida töövahendina kasutatakse, on kahtlemata telefon. Jälgimistegevuse võimalused on ajas muutunud ja edasi arenenud seoses kommunikatsioonivahendi enda arenguga. Tänaseks töövahendiks ei ole ammu enam üksnes lauatelefon, vaid tööks kasutatakse ka mobiil- ja nutitelefone. Kusjuures viimane kujutab endast

[101] Samas. Lk 13
[102] O. Kirst. Sõnumisaladuse kaitse tööandja sidevahendi kasutamisel. – Juridica IV/2012. Lk 424
[103] Samas. Lk. 421.

tehniliselt pigem arvutit, kuhu on kerge vaevaga võimalik installeerida tarkvara, mis salvestab tehtud ja vastuvõetud kõnesid või edastab mud informatsiooni seadme kasutamise kohta

EIK on lahendis *Halford vs. United Kingdom* öelnud, et lisaks kodus tehtud ja vastuvõetud kõnedele kuuluvad eraelu puutumatuse ja sõnumisaladuse kaitsealasse ka töökohal tehtud kõned.[104] Sama seisukohta on EIK väljendanud ka hilisemas lahendis *Copland vs United Kingdom.*[105] Sõnumisaladus tähendab seda, et sõnumi sisu on mõeldud üksnes neile, kes sõnumi vastuvõtmises osalevad.[106] Sõnumi sisu võib sisaldada teavet töötaja mõtete, veendumuste, arvamuste, kavatsuste, sündmuste kirjelduste ja muu kohta, mida ta soovib jagada vaid valitud suhtluskaaslastega.[107] Sõnumisaladuse ja eraelu kaitsealasse kaitsealasse kuuluvad lisaks laua- või mobiiltelefoni teel tehtud või vastuvõetud kõnedele ka muud, tänasel päeval tööalases kasutuses laialt levinud suhtluskanalite, nagu *Skype*, *WhatsApp*, *Viber* jne. vahendusel sooritatud kõned. Suhtlemine ja vaba teabevahetus (kommunikatsioon) on osa isikuvabadusest, mistõttu on õigusriigis igaühel põhjust eeldada oma suhtluse privaatsust ning seda, et sõnumite saladuse õigust ei riivata.[108]

Töösuhtele omasest alluvusvahekorrast tulenevalt saab töötaja personaalsesse sõnumisaladuse kaitsealasse kuuluvaks lugeda mõistagi vaid töötaja erakõned. Tööalased kõned teebki töötaja tööandja nimel ja tööandja jaoks.[109] Vaatamata sellele, et töökõned ei kuulu eraelu puutumatuse ja sõnumisaladuse kaitsealasse, peab tööandja arvestama, et need kõned on kaitstud kõne teiseks pooleks oleva isiku sõnumisaladusega.[110]

Õiguslik alus telefonikõnede lindistamiseks on seotud tööandja õigustatud huviga. Ehk kui tööandjdal on selge ja tuvastatav õigustatud huvi telefonikõnede salvestamiseks, siis on see üldjuhul lubatud. Töökõnede salvestamist rakendatakse käesoleval hetkel eelkõige "parema klienditeeninduse tagamise" eesmärgil. Tööandja põhjendab oma õigustatud huvi telefonikõnede salvestamiseks sellega, et tagada parem teenindus, mis autori hinnangul kujutab oma olemuselt

[104] EIKo lahend. 20605/92. 25.06.1997. Halford vs Ühendkuningriik
[105] EIK lahend. 62617/00. 03.05.2007. Copland vs Ühendkuningriik
[106] R. Maruste. Konstitutsionalism ning põhiõiguste ja vabaduste kaitse. Tallinn: Juura 2004. Lk 532
[107] S. Laos. H. Sepp. Põhiseaduse § 43 kommentaar, komm. 2. - Ü. Madise jt (toim). Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. 4., täiend. vlj. Tallinn: Juura, 2017
[108] S. Laos. H. Sepp. Põhiseaduse § 43 kommentaar, komm. 1. - Ü. Madise jt (toim). Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. 4., täiend. vlj. Tallinn: Juura, 2017
[109] Andmekaitse inspektsioon. Isikuandmete töötlemine töösuhtes. Abistav juhendmaterjal. Lk 10. Arvutivõrgus: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikuandmed%20t%C3%B6%C3%B6suhetes%20juhendmaterjal26%2005%202014_0.pdf. (10.01.2019).
[110] Andmekaitse inspektsioon. Isikuandmete töötlemine töösuhtes. Abistav juhendmaterjal. Lk. 67. Arvutivõrgus: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikuandmed%20t%C3%B6%C3%B6suhetes%20juhendmaterjal26%2005%202014_0.pdf. (10.01.2019).

töötaja tööülesannete täitmise kvaliteedi kontrollimist. Ka AKI on väljendanud, et parema klienditeeninduse tagamine on sisuliselt käsitletav töötajate kontrollimisena.[111] Tööandja õigustatud huvi peab olema seotud kindla eesmärgi saavutamisega ehk tööandja peab määratlema selged ja konkreetsed eesmärgid, mille täitmiseks on telefonikõnede salvestamine vajalik.[112] Eeldusel, et kõnede salvestamise eesmärk peab olema piisavalt konkreetne, on magistritöö autor seisukohal, et töötajate kõnede salvestamine "parema klienditeeninduse huvides" on liiga üldine. Autor rõhutab, et tööalaste kõnede salvestamine ei ole keelatud, aga tööandjal peaks olema selliseks tegevuseks konkreetne ja äratuntav õigustatud huvi. Ehk ka töökõnede salvestamisel peab olema väga selge eesmärk, mille täitmiseks esineb just kõnede salvestamise vajadus. Põhjendades oma õigustatud huvi "parema klienditeeninduse tagamisega", ei võimalda tegelikult just kuigi palju hinnata salvestamise eesmärke. Autor toob näite, et töökõnede salvestamiseks võib olla tööandjal õigustatud huvi näiteks siis, kui salvestamise eesmärgiks on seatud ettevõttesse pöördumise levinumate põhjuste kaardistamine. Enne telefonikõnede salvestamise rakendamist tuleks tööandjal hinnata salvestamise eesmärke ning võimalusi ja praktilist vajadust.

Kahtlemata on tehnoloogia areng avardanud võimalusi töötajate kõnede salvestamiseks. Tööandjal on võimalik paigaldada märkamatuks jäävaid seadmeid töötaja kabinetti, arvutile, telefonile, sõidukisse või isegi magistritöö peatükis 2.5. käsitletud kiipkaardile (*identification badge*).[113] Selliseks varjatud jälgimiseks ei ole aga tööandjal õigustatud huvi, mistõttu ei ole see lubatud. Ühtlasi puudub tööandjal õigustatud huvi töötaja erakõnede pealtkuulamiseks kõne toimumise ajal. Üks ulatuslikumaid töötajate telefonikõnede varjatud pealtkuulamise ja salvestamisega seotud juhtumeid on seotud Saksamaa suurima telekommunikatsiooni ettevõttega *Deutsche Telekom*, kes kuulas kahe aasta vältel pealt juhtkonna liikmete ning teiste kõrgetel positsioonidel töötavate isikute kõnesid seoses ajakirjanikega suhtlemisega, et leida võimalikke infolekitajaid. Jälgimistegevust teostas tööandja vahendatult, palgates ettevõtte, kes järjepidevalt töötajate kõnesid monitooris. Tööandjal puudus õigustatud huvi seesuguseks varjatud jälgimistegevuseks. Lisaks toob autor välja, et kõnealuse juhtumi puhul oli töötajatel lubatud töötelefoni kasutada m.h.

[111] Samas. Lk 67.
[112] Andmekaitse inspektsioon. Telefonikõnede salvestamise lubatavuse juhend. Lk 1. Arvutivõrgus: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Telefonik%C3%B5nede%20salvestamise%20lubatavuse%20juhend.pdf. (22.03.2019).
[113] C. A. Ciccoletti. The Eavesdropping Employer: A Twenfy-first Century Framework for Employee Monitoring. – The American business Law Journal. Lk 58.

erakõnedeks, mistõttu kuulati pealt ka eravestlusi, riivates nii töötajate õigust elaelu puutumatusele kui ka õigust sõnumisaladusele.[114]

Praktikas tekitab probleeme kõige enam olukord, kus tööandjal on selge ja tuvastatav õigustatud huvi töökõnede salvestamiseks, ent töötajal on lubatud telefoni kasutada ka erakõnede tegemiseks ja vastuvõtmiseks. Vältimaks erakõnede salvestamist ja sellega kaasnevat eraelu puutumatuse ja sõnumisaladuse riivet, on mõistlik kasutusele võtta tehniline lahendus, mis võimaldab töötajal salvestamise funktsiooni ajutiselt välja lülitada. Magistritöö autor nendib, et sellise võimaluse olemasolu annab töötajale potenttsiaalse võimaluse salvestamist vältida ka töökõnede puhul. Andmekaitse inspektsioon pakub lahendusena ka võimalust salvestis töötajal kustutada, ent ka sellisel juhul on töötajal põhimõtteline võimalus kustutada lisaks ka tööga seotud kõnesid.[115]

3.2.2. Telefonikõnede salvestamise põhimõtted

Tööandja peab enne telefonikõnede salvestamist hindama, kas tegemist on proportsionaalse meetmega, või on olemas ka teisi efektiivseid meetmeid. Peatükis 3.2.1. toodud näite puhul, mille kohaselt tööandja põhjendab oma õigustatud huvi telefonikõnede salvestamiseks ettevõttesse pöördumise põhjuste väljaselgitamiseks, võiks proportsionaalsemaks, ent sama efektiivseks lahenduseks olla autori arvates kord, mille kohaselt töötajad märgivad kirjalikult üles sissetulnud kõnede põhjused. Sellisel juhul puuduks vajadus töökõnede salvestamiseks.

Kui tööandjal on tuvastatud õigustatud huvi telefonikõnede salvestamiseks ja muud alternatiivid eesmärgi saavutamiseks puuduvad, peab töötajaid korrektselt ja selgelt salvestamisest teavitama. Jälgimistegevuse läbipaistvuse tagamiseks tuleb töötajaid salvestamisest teavitada ning see peab toimuma enne tööülesannete täitma asumist. Töötajale tuleb seejuures tutvustada ka salvestamisele seatud eesmärke. Samuti peab töötajale olema teada, kellel on õigus telefonikõnede salvestamise teel kogutud andmeid töödelda ning millise aja jooksul neid säilitatakse.

Salvestiste säilitamine on selgelt seotud minimaalsuse põhimõttega, mille kohaselt peab olema kindlaks määratud salvestiste säilitamise tähtaeg. Autor rõhutab, et tööandja peab tähtaega

[114] EDRi – Protecting digital freedom. Deutsche Telecom under investigation for spying its employees. Arvutivõrgus: https://edri.org/edrigramnumber6-11deutsche-telekom-spying-employees/ (15.03.2019).
[115] Andmekaitse inspektsioon. Isikuandmete töötlemine töösuhtes. Abistav juhendmaterjal. Lk 68. Arvutivõrgus: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikuandmed%20t%C3%B6%C3%B6suhetes%20juhendmaterjal26%2005%202014_0.pdf. (10.01.2019).

määrates arvestama, et salvestisi säilitatakse üksnes sellise aja jooksul, mis on vältimatult vajalik. Sõltuvalt ettevõtte tegevusvaldkonnast on autor seisukohal, et üldjuhul ei tohiks mõistlik tähtaeg ületada paari kuu pikkust perioodi. Minimaalsuse põhimõttest lähtudes peaks tööandja töökõnesid salvestama üksnes mahus, mis on eesmärgi saavutamiseks tingimata vajalik. Autori hinnangul võib minimaalsuse põhimõttega vastuolus olla kõikide töökõnede salvestamine. Soovides hinnata töötaja töökohustuste täitmise kvaliteeti on üldjuhul piisav ka kõnede osaline või pisteline salvestamine.

Tööandja peab tagama, et salvestistele ei pääseks ligi isikud, kellel ei ole õigust salvestistele juurde pääseda ning võtma vajadusel kasutusele vastavad infotehnoloogilised turvameetmed. Turvalisuse põhimõtte kohaselt peab tööandja või tema poolt volitatud isikuandmete töötleja tagama salvestiste töötlemisel ja käitlemisel nende konfidentsiaalsuse, terviklikkuse ja päritolu õigsuse.

Töötajale, kelle kohta on telefonikõnede salvestamise teel kogutud isikuandmeid, peab olema tagatud ligipääs salvestistele. Tööandja võib keelduda juurdepääsu võimaldamisest siis, kui töötajale ei ole võimalik tema kohta kogutud andmeid esitada nii, et sellega ei kaasneks kolmandate isikute isikuandmete töötlemist.

Eelnevale tuginedes on autor arvamusel, et isikuandmete kaitse üldmääruse valguses on isikuandmete töötlemine telefonikõnede salvestamise kaudu lubatud pigem varva. Tööandjal on autori hinnangul keeruline põhjendada oma õigustatud huvi selliseks tegevuseks, ning isegi kui see õnnestub, võib õiguslik alus ära langeda andmekaitse üldpõhimõtete tõttu. Sellest tulenevalt võib öelda, et töötajate isikuandme kaitse on vaatamata telefoni kasutusvõimaluste arengule pigem hästi tagatud.

3.2.3. Õiguslik alus kõneeristuse anlüüsimiseks

Lisaks telefonikõnede salvestamisele võib töötaja isikuandmete töötlemine väljenduda ka kõneeristuse analüüsimises. Nn. liiklusandmed ei kuulu sõnumisaladuse kaitsealasse, vaid on PS § 26 eraelu puutumatuse kaitsealas. Sellisteks liiklusandmeteks on andmed telefonikõne fakti,

kestuse, viisi ja vormi ning edastaja või vastuvõtja isikuandmete ja asukoha kohta.[116] Ka nende andmete põhjal on tööandjal võimalik saada olulist infot töötaja tegevuse kohta.

Kõige tõenäolisemalt töödeldakse telefonikõnede andmeid telefoniarvete puhul.[117] EIK märkis lahendis Copland vs United Kingdom, et töötaja kõnede pikkuse, telefoninumbrite, millele on helistatud ja telefoninumbrid, millelt on helistatud töötajale uurimine tööandja poolt, eesmärgiga selgitada välja tööandja vara ülemäärast kasutamist, ei ole lubatud. Sellele tuginedes saab väita, et tööandja ei saa oma õigustatud huvi põhjendada viitega oma vara otstarbekale kasutamisele.

Probleeme võib tekitada olukord, kus tööandja lubab töötelefoni kasutada ka erakõnedeks. Ka sellisel juhul ei ole tööandjal ilmtingimata õigustatud huvi kõneeristuse analüüsimiseks, eesmärgiga eristada erakõned tööalastest. Isegi olukorras, kus töötaja ja tööandja on kokku leppinud, et töötelefoni võib lisaks töökõnede tegemisele kasutada ka erakõnedeks, ent need tuleb töötajal hüvitada, ei ole tööandjal õigustatud huvi liiklusandmete töötlemiseks. AKI hinnangul peaks sellise telefoni kasutamise korra puhul töötaja ise esitama andmed selle kohta, millise summa eest ta erakõnesid tegi. Kusjuures loetakse tööandja poolt ülemääraseks nõuda erakõnede eristamist iga kuu kõneeristuses eraldi.[118]

Kui töötaja ja tööandja on kokku leppinud, et telefoni kasutamise limiiti ületava osa tasub töötaja, ei ole tööandjal õigustatud huvi kõneeristuse analüüsimiseks, eesmärgiga selgitada välja limiidi ületamise põhjused. Tööandja õigustatud huvi on tuvastatav üksnes siis, kui töötaja ise väidab, et limiidi ületamise konkreetsel kuul põhjustas suurem tööalaste kõnede hulk. AKI hinnangul võib tööandja sellisel juhul eelkõige nõuda, et töötaja esitaks ise tööalaste kõnede suurt hulka tõendavad andmed.[119] Magistritöö autor näeb aga siinkohal praktilist probleemi: üldjuhul ei ole töötajal volitust kõneeristuse väljavõtte saamiseks, sest sideoperaatori jaoks kuulub telefoni number tööandjale. Ehk liiklusandmetele juurdepääsu õigus kuulub reeglina üksnes tööandjale või tema poolt volitatud isikutele.

Autor on seisukohal, et tööandjal on üldjuhul väga piiratud võimalused kõneeristuses sisalduvate andmete töötlemiseks. Õigustatud huvi olemasolu võiks jaatada näiteks tööstusspionaaži kahtluse

[116]AKI. Isikuandmete töötlemine töösuhtes. Abistav juhendmaterjal. Lk 10. Arvutivõrgus: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikuandmed%20t%C3%B6%C3%B6suhetes%20juhendmaterjal26%2005%202014_0.pdf. (10.01.2019).
[117] Samas. Lk 66.
[118] Samas. Lk 67
[119] Samas. Lk 67.

korral, kui on reaalne võimalus, et töötaja on äri- või tootmissaladusi edastanud tööandja konkurendile. AKI hinnangul pole tööandjal õigus kõnede eristusest nähtuvaid telefoninumbreid tuvastada, mistõttu peaks reaalse konkurentsikeelu või tööstusspionaaži kahtluse korral küsima lisaselgitusi töötaja enda käest.

Tõenäoline põhjus, miks tööandjal üldjuhul ei ole õigustatud huvi kõneeristuses sisalduvate andmete töötlemiseks on autori hinnangul seotud järgmise asjaoluga: vaatamata sellele, et tööandjale ei saa teatavaks kõne sisu, kuuluvad ka nn. liiklusandmed (telefoninumber, kõne kestvus jms) eraelu puutumatuse kaitsealasse ning nende andmete analüüs võimaldab samal määral töötaja eraellu sekkumist ja tema elu ning käitumisharjumuste üksikasjalikku jälgimist.[120]

3.2.4. Kõneeristuse analüüsimise põhimõtted

Lisaks sellele, et tööandjal on üldjuhul väga piiratud võimalused töötaja kõnede eristuse analüüsimiseks, kitsendavad seda ka andmekaitse üldpõhimõtted. Olukorras, kus tööandjal on õigustatud huvi kõnede eristuse kontrollimiseks, on oluline lähtuda minimaalsuse põhimõttest. Kõnede eristuse uurimisel peaks piirduma võimalikult üldiste andmetega – näiteks telefoninumbrite esinemissagedus, väga pikad kõned jms. Viimase puhul peaks tööandja küsima lisaselgitusi töötajalt endalt.

Kõnede eristuses sisalduvate andmete töötlemine peab olema läbipaistev ehk töötaja peab olema sellest teadlik. Kui kõnede eristuse jälgimine toimub töötaja teadmata, kujutab see endast eraelu riivet.[121]

Proportsionaalsema lahendusena sama eesmärgi saavutamiseks pakub autor välja teabe küsimist töötaja enda käest. Kahtlemata ei suuda töötaja anda detailset informatsiooni oma möödunud kuu telefonikõnede kohta, ent kindlasti suudab töötaja meenutada tavapärasest pikemaid kõnesid, kõige enam valitud ja samuti ebaharilikke kontakte.

[120] Article 29 Data protection Working Party. Opinion 2/2017 on data processing at work. Lk 10. Arvutivõrgus: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169. (20.01.2019).
[121] EIKo lahend. 62617/00. 03.05.2007. Copland vs Ühendkuningriik

3.3. Arvuti

3.3.1. Arvutikasutuse jälgimise võimalused

Töötaja isikuandmete töötlemine, mis väljendub töötaja arvutikasutuse jälgimises, on AKI hinnangul Eestis pigem uudne ning pole teada, kas ja kui mitmed ettevõtted seda tänasel päeval rakendavad. Samuti puudub Eesti osas kohtupraktika, ent Euroopa kohta saab tuua mitmeid näiteid. AKI sõnul on tõenäoliselt aja küsimus, millal kõnealune probleem ka Eestis kohtulaua taha jõuab.[122] Magistritöö autor lisab, et kuna tegemist on vastuolulise ja vastumeelse teemaga, siis üldjuhul tööandjad väldivad kommentaaride andmist teemal kas ja kuidas töötaja arvutikasutust kontrollitakse. Vaatamata asjaolule, et tänasel päeval puuduvad Eesti kohtupraktikas näited selle kohta, kus tööandja on mõistetud süüdi töötajate arvutikasutuse ebaseaduslikus jälgimises, ei kinnita see fakti, et tööandjad lubatud jälgimise piire ei ületa. Nimelt vastavasisulise kohtupraktika puudumine ei peegelda tegelikku olukorda juba seetõttu, et töötajatel on reeglina raske nende suhtes teostatud ebaseaduslikku jälgimist avastada, rääkimata selle hilisemast tõendamisest. Kõik vajalikud logid ja muud jäljed asuvad tööandja ning selle IT-personali poolt ligipääsevates kohtades.[123] Hinnates teiste EL liikmesriikide kohtupraktikat, saab aga välja tuua väga suuri privaatsusõigugse riivega seotud kohtuasju, mis kinnitab, et problem on reaalne ja vajab tähelepanu. Autor on seisukohal, et paljudel juhtudel ei pruugi töötajad arvutikasutuse jälgimisest üleüldse teadlikud olla, sest seda on lihtne teostada varjatult.

Peamised põhjused, miks tööandjdad otsustavad töötajate arvutikasutast jälgida, on seotud arvutikasutuse turvalisuse tagamisega ja töötajate kontrollimisega. Tehnoloogia areng on kaasa toonud palju uusi võimalusi töötajate arvutikasutuse jälgimiseks.

Arvutikasutuse jälgimisega seonduvalt saab välja tuua olulise erinevuse Euroopa ja Ameerika Ühendriikide töökultuuri vahel. Nimelt Euroopas hinnatakse töötajate eraelu puutumatust ja privaatsust töökohal pigem kõrgelt, seevastu USA-s on arvuti ja muude töövahendite kontrollimine selgelt seotud kõnealuste töövahendite omandiga. Töötaja privaatsuse teemal on Euroopa Liit võtnud suuna inimeste õiguste kaitseks (inglise keeles "*Right approach*"), mis tähendab seda, et igal inimesel on õigus eraelule ja väärikusele ning need õigused on võrdsed tööandja õigustega.

[122] Andmekaitse inspektsioon. Spioon töötaja arvutis. Arvutivõrgus: https://www.aki.ee/et/uudised/meediakajastus/spioon-tootaja-arvutis. (15.03.2019).
[123] O. Kirst. Sõnumisaladuse kaitse tööandja sidevahendi kasutamisel. – Juridica IV/2012. Lk 428

USA-s, vastupidiselt on levinud omandipõhine lähenemine (inglise keeles *"property approach"*), mis tähendab seda, et vara ja ressursside omajal on õigus omada kontrollivahendeid ja dikteerida reegleid, mis on talle soodsamad.[124]

Käesoleval hetkel ei reguleeri ükski õigusakt selgesõnaliselt, kas, milliste vahenditega ja millises ulatuses on tööandjal õigus töötaja arvutikasutust jälgida. Töötaja arvutikasutust jälgiva tarkvara müük igal juhul Eestis keelatud ei ole ning teenusepakkujaid on turul palju.

Enamlevinud jälgimisviisideks on näiteks ekraani jälgivad programmid (inglise keeles *desktop monitoring programs*); internetikasutust jälgivad programmid (inglise keeles *internet monitoring*); klahvilugejad (inglese keeles *keystroke logging*) jms. Uuemate tehniliste lahendustena, mis mõnel juhul on vähem sekkuvad, saab välja tuua järgmised jälgimisviisid:

1. Lekketõrjevahendid, millega jälgitakse tööarvutite kaudu jälgitavat teavet, eesmärgiga tuvastada võimalikud andmetega seotud rikkumised;
2. Uue põlvkonna tulemüürid ja ohuhalduse süsteemid, mis võimaldavad kasutada mitmesuguseid jälgimistehnoloogiaid, s.h. pakettide süvakontrolli (inglise keeles *deep packet inspection*) ehk edastatavate pakettide infosisu analüüsimist, infopüüki (inglise keeles *interception)*, veebisaitide filtreerimist, sisu filtreerimist jne;
3. Turvarakendused ja -meetmed, mis hõlmavad tööandja IKT süsteemidesse sisenemise logimist;
4. E-tõendamise tehnoloogia, mis otsib arvutist elektroonilisi andmeid eesmärgiga kasutada neid tõendina;
5. Rakenduste ja seadmete kasutamise jälgimine nähtamatu tartkavara kaudu;
6. Pilveteenusena pakutavate kontorirakenduste abil töötaja tegevuse jälgimine;
7. Isiklike seadmete, näiteks nutitelefonide ja tahvelarvutite jälgimine;
8. Ihuarvutite (inglise keeles *wearable computer*), näiteks nutikella kasutamise jälgimine.[125]

Tarkvara, mille kaudu on võimalik jälgida arvuti ekraani, võimaldab tööandjal salvestada, kopeerida ja reaalajas jälgida töötaja arvutikasutust, mis aitab tööandjal saada informatsiooni m.h. selle kohta:

[124] K. Saarep. Kaameraid kasutatakse töökohal tihti valedel eesmärkidel. 17.05.2018. Arvutivõrgus: http://www.tooelu.ee/et/uudised&nID=1963, (15.02.2019)
[125] Article 29 Data protection Working Party. Opinion 2/2017 on data processing at work. Lk 12-13. Arvutivõrgus: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169. (20.01.2019).

- Milliseid programme töötaja kasutab (inglise keeles *application tracking*);
- Millised dokumendid arvutis paiknevad (*document tracking*);
- Töötaja kalendri ja tööülesannete täitmise jälgimine (*events timeline tracking*);
- Arvutisse ja programmidesse sisenemise jälgimine (*log-on tracking*);
- Salasõnade jälgimine (*password tracking*);
- Kuvatõmmiste tegemine igal ajahetkel (*screenshot capture*);
- Tarkvara allalaadimiste jälgimine (*software installation*);
- Veebis avatud rakenduste jälgimine (*window tracking*).[126]

3.3.2. Arvutikasutuse jälgimise õiguslik alus

Töötaja arvutikasutuse jälgimiseks peab tööandjal olema selge eesmärk ja õigustatud huvi. Autor on seisukohal, et õigustatud huvi põhjendamine üldise viitega töötaja või tema töökohustuste kontrollimisele ei ole piisav. Tegemist on liiga laialivalguva põhjendusega ning kontrollimise eesmärk peaks olema määratletud kitsamalt. Arvestades küberturvalisuse olulisust kaasaegses töökeskkonnas, leiab autor, et tööandja võib oma õigustatud huvi töötajate arvutikasutuse jälgimiseks põhjendada infoturbe tagamisega. Loomulikult tuleb silmas pidada ettevõtte tegevusvaldkonda ja reaalseid ohte küberturvalisusele. Ehk pelk hirm infoturbega seotud riskide vastu ei saa samuti olla piisavaks põhjenduseks. Autor nõustub seisukohaga, et kui tööandja ei suuda selgelt ja ühemõtteliselt oma õigustatud huvi ja reaalset vajadust töötaja arvutikasutuse jälgimiseks põhjendada, siis suure tõenäosusega neid lihtsalt ei olegi.[127]

EIK on seisukohal, et tööandjal ei ole mingil juhul õigust kasutada varjatud nuhkimistarkvara (inglise keeles *spyware*) jälgimaks arvutikasutuse ajalugu, kontrollimaks tööaja kasutust jms. Tööandja peab arvestama, et vaatamata faktile, et selliseid programme on palju, et ole tal nende paigaldamiseks õigustatud huvi. Samuti tasuks loobuda sellistest jälgimisviisidest, mida pole võimalik hiljem tuvastada, näiteks füüsiline nuhkimine töötaja arvutis.[128]

[126] C. A. Ciccoletti. The Eavesdropping Employer: A Twenfy-first Century Framework for Employee Monitoring. – The American business Law Journal.
[127] Global data hub. Employee monitoring update. Arvutivõrgus: https://globaldatahub.taylorwessing.com/article/employee-monitoring-update (11.02.2019).
[128] EIKo lahend. 61496/08. 12.01.2016. Bărbulescu vs Rumeenia.

Ka töötaja arvuti ekraani jälgivate seadmete kasutamine on pigem komplitseeritud, sest reeglina puudub tööandjal selleks õigustatud huvi. Kui tööandja soovib sellist programmi kasutada, peab ta oma õigustatud huvi väga selgelt ja ühemõtteliselt põhjendama. Üldjuhul ei võimalda ekraani jälgiv programm tuvastada ka turvariske, mistõttu on nende kasutamine seotud eesmärgiga jälgida töötajate tööaja kasutust. Üksnes viide töötaja produktiivsuse kontrollimisele on aga liiga üldine.

Ka klahvilogerite, mis jälgivad ja salvestavad arvutihiire ja -kvaviatuurivajutusi, kasutamine töökohal on pigem riskantne ning õigustatud huvi tõendamine sellise jälgimisviisi kasutamiseks on keeruline. Sellise tarkvara abil on võimalik salvestada töötaja töö- ja erakirjavahetust, sotsiaalmeediasse tehtavaid postitusi või tuvastada asjaolu, et töötaja kasutab tööajal arvutit töövahendina liiga vähe. Tänasel päeval on kõnealuse jälgimisviisi kasutamisest pigem loobutud, sest töötaja produktiivsuse hindamiseks on ka teisi, töötaja privaatsust vähem riivavaid meetmeid. Saksamaa föderaalne töökohus (inglise keeles *german federal labor court*) kinnitas oma hiljutises lahendis, et klahvilogerite paigaldamine töötajate arvutitele riivas nende privaatsust ning tööandjal puudus selliseks jälgimistegevuseks õigustatud huvi. Kõnealuse kaasuse puhul paigaldas tööandja vastava tarkvara varjatult, ega teavitanud töötajaid, mistõttu oli töötajate privaatsusõiguse riive eriti suur.[129] Varasemalt on tööandjad jälgimisviisina kasutanud ka tarkvara, mis teatud aja tagant pildistab töötajat arvutil oleva veebikaamera abil, veendumaks töötaja kohalolus.[130] Tänaseid andmekaitse reegleid arvestades, ei saa aga ka sellist tegevust tööandja poolt lubatavaks pidada – on äärmiselt ebatõenäoline, et tööandja suudab nimetatud jälgimisviiside kasutamiseks ära tõendada oma õigustatud huvi.

Autorile teadaolevalt on töötaja arvutikasutuse jälgimine praktikas probleemseks osutunud sageli kaugtöötajate puhul. Kaugtöö mõiste on sätestatud TLS § 6 lõikes 4: kui töötaja ja tööandja lepivad kokku, et töötaja teeb tööd, mida tavapäraselt tehakse tööandja ettevõttes, väljaspool töö tegemise kohta, s.h. töötaja elukohas, on tegemist kaugtööga. Võttes arvesse tehnoloogia arengut, õigustab kaugtöö end mitmetel erialadel – näiteks infotehnoloogid, raamatupidajad jm. Kontrori töötajad ei pea ilmtingimata täitma tööülesandeid tööandja asukohas, vaid võivad teha tööd ringi liikudes või kodukontroist. Kaugtöö võimaluse olemasolu on keskne tegur, mis on tinginud töökoha ja kodu väiksema eristamise. Põhimõtteliselt tähendab kaugtöö olukorda, kus tööandja annab töötajate kasutusse IKT seadmed või tarkvara, mis nende töö- või isiklikele seadmetele paigaldatuna

[129] Saksamaa föderaalse töökohtu lahend 27.07.2017, 2 AZR 681/16.
[130] Employee monitoring technologies: gone too far? – GDPR informer. 12/2018. Arvutivõrgus: https://gdprinformer.com/gdpr-articles/employee-monitoring-gone-far (16.03.2019).

võimaldavad neil olenevalt rakendamisest omandada samal tasemel juurdepääsu tööandja võrgule, süsteemidele ja ressurssidele, mis neil oleks juhul kui nad töötaksid tööandja asukohas.[131] Kaugtöö positiivne külg on kahtlemata seotud kulude vähenemisega, sest mida vähem on kontoris töötajaid, seda vähem tekib kontoriga seotud kulusid. Töötajatele võimaldab kaugtöö kindlasti suuremat paindlikkust ja üldjuhul ka vabadust valida enda jaoks sobiv tööaeg. Ehkki kaugtöö on töökultuuri positiivne edasiareng, võib sellega kaasneda ka hulk probleeme. Oluline küsimus, mis seoses kaugtööga tõusetub, on järelevalve ja kontrolli teostamise võimalused ja ulatus. Näiteks ei ole tööandjal õigust minna füüsiliselt kontrollima tööülesannete täitmist töötaja kodukontorisse, mistõttu vahetu kontroll kaugtöötaja üle on pigem piiratud. Riski maandamise eesmärgil leiavad paljud tööandjad, et kaugtöötajate kontrollimiseks on põhjendatud mitmesuguste jälgimisrakenduste kasutamine, mis salvestavad klahvivajutusi ja hiireklikke, teha suvalistel ajahetkedel kuvatõmmiseid töötaja arvutiekraanist, logida kasutatavaid rakendusi ning jälgida millise aja jooksul neid kasutati või võimaldada tööandja võrku ühendatud seadmetel kasutada veebikaamerat ja hoida nende salvestisi.[132] Kaugtöötaja kontrollimist võimaldavaid seadmeid ja jälgimist võimaldavaid pilveteenuseid on turul hulgaliselt ning neid on võimalik väga lihtsalt töötaja arvutile paigaldada. Euroopa andmekaitse töörühm kinnitab, et selliste tehnoloogiatega kaugtöötaja isikuandmete töötlemine ei ole õiguspärane ning on väga ebatõenäoline, et tööandjal on õigustatud huvile vastav õiguslik alus näiteks kaugtöötaja klahvivajutuste ja hiireklikkide salvestamiseks. Töörühm rõhutab, et oluline on käsitleda kodu- ja kaugtööga kaasnevaid riske proportsionaalselt ja mitte ülemääraselt.[133] Autor on seisukohal, et tööandja peab kaugtööd lubades arvestama, et tema kontrollimis- ja jälgimisvõimalused on raskendatud, mistõttu esmajoones peab olema poolte vahel vastastikkune usaldus. Vaatamata kaugtöö kõikidele positiivsetele külgedele, nõuab see kindlasti rohkem enesedistsipliini ning paljudele töötajatele ning tööanjdatele ei pruugi selline paindlik töökorraldus üleüldse sobida. Kui tööandja ei usalda oma töötajaid piisavalt, andmaks neile vabadust olla n.ö oma aja peremees, on mõistlik eelistada klassikalist töökorraldust.

[131] Article 29 Data Protection Working party. Opinion 2/2017 on data processing at work. Lk 16. Arvutivõrgus: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169. (20.01.2019).
[132] Samas. Lk 16.
[133] Samas. Lk 16.

3.3.3. Arvutikasutuse jälgimise põhimõtted

Töötaja arvutikasutust jälgides tuleb eelkõige lähtuda proportsionaalsuse, läbipaistvuse ja minimaalsuse põhimõtetest. Kui lisaks arvutikasutuse jälgimisele on olemas teisi, töötaja privaatsust vähem riivavaid kontrollimismeetmeid, siis tuleks eelistada neid. Üldjuhul ei saa proportsionaalseks pidada ekraani jälgivaid seadmeid, mille abil on võimalik jälgida töötaja arvutikasutust terve tööaja vältel. Kui infoturbega seotud riske on võimalik vältida viirusetõrje tarkvara või tulemüüridega, ei saa samuti arvutikasutuse jälgimist pidada proportsionaalseks. Autor soovitab tööandjatel arvutikasutuse jälgimisse suhtuda ettevaatlikult ning kaaluda võimalusel teisi, töötaja privaatsust vähem riivavaid abinõusid.

Töötajate arvutikasutuse jälgimine peab olema minimaalne - on oluline, et tööandjad kohtleksid töötajaid austusega ning ei jälgiks nende arvutikasutust rohkem, kui riskide vältimiseks vajalik on. Kahtlemata on töötaja ja tööandja huvide vahel tasakaalu leidmine keeruline, mistõttu peab jälgimine olema läbipaistev ja konkreetne.

Tööandja peab töötajaid läbipaistvuse tagamiseks arvutikasutuse jälgimisest teavitama. Tööandja peaks selgelt töökorralduslike eeskirjade kaudu kindlaks määrama arvuti kasutamisega seotud reeglid. Näiteks võib tööandja keelata temale kuuluvate seadmete kasutamise tööga mitteseotud tegevusteks. Kõik arvuti kasutamise ja võimaliku tööandjapoolse jälgimisega seotud reeglid peavad aga olema eelnevalt paika pandud ning nende vajalikkust töötajale läbipaistvalt selgitatud. Autori hinnangul on mõistlik läbipaistvuse tagamiseks kasutada lisaks ka elektroonilist teavitussüsteemi, mis töötajat arvutisse sisse logides informeerib võimalikust jälgimisest ja selle eesmärkidest.

Kaugtöötaja kontrollimiseks on üldjuhul proportsionaalsemaid alternative kui arvutikasutust jälgivad seadmed, mistõttu selliste tehnoloogiatega kaugtöötaja isikuandmete töötlemine on reeglina ebaproportsionaalne. Autori hinnangul peegeldab töötaja produktiivsust töö tulemus, mille kaudu saab kaudselt kaugtöö tegijat kontrollida. Samuti võib kehtestada kaugtöötajale nõude esitada vastav aruanne, mis kajastab kindlaks määratud perioodil täidetud tööülesandeid. Tõenäoliselt võib proportsionaalseks pidada kaugtöötajate puhul tööaja arvestuse programmide kasutust, kus töötaja märgib ära, mis ajal ta tööd alustab ning millal lõpetab. Sisuliselt saab kaugtöötaja ise valida, millal tööülesandeid täita, mis mõnel juhul võib viia töödistsipliini kadumise ja tööaja reeglite mittejärgimiseni. Kuna kaugtöö korral pole tööandjal reaalset kontrolli

tööaja üle, siis on mõistlik täpselt kokku leppida, kuidas toimub tööaja arvestus.[134] Eelkõige on tööaja-arvestust jälgivad programmid mõistlikud ja proportsionaalsed kontekstis, kus töö tasustamine toimub tunnipõhiselt.

3.4. Internetikasutuse jälgimine

3.4.1. Internetikasutuse jälgimise õiguslik alus

Kindlustamaks, et töötaja täidab tööajal oma töökohustusi, ega viida aega ebasobivatel või tööga mitteseotud veebilehtedel, võib tööandja soovida jälgida nende internetikasutust. Töötaja internetikasutuse jälgimine tööandja poolt võib kõne alla tulla siis, kui tööandjal on selleks konkreetne eesmärk ja selgelt määratletud õigustatud huvi. Pelgalt töötajate kontrollimine või töökohustuste täitmise kontrollimine ei ole üldmääruse valguses piisav. Magistritöö autor toob välja, et internetikasutuse jälgimise vastu võiks huvi olla sellistel ettevõtetel, kus kohaldatakse kõrgendatud hoolsus- ja turvalisuse tagamise kohustust, näiteks erinevatel finantsasutustel. Kuid ka sel juhul peab internetikasutuse jälgimine olema põhjendatud. Üldine viide kõrgendatud turvariskidele ei ole üldjuhul piisav ning tööandja peab formuleerima jälgimistegevusele seatud selged eesmärgid. Autor on arvamusel, et mõõdukas internetikasutuse kontroll või piiramine on mõistlik, sest arvestades tänast infohulka internetis, on töötajatel võimalus otsida sisuliselt kõike ning ilma piisava kontrollita võib kaasneda palju võimalusi interneti sobimatuks või isegi kriminaalseks kasutamiseks.[135]

Tööandjate õigustatud huvi külastatud veebisaitide jälgimiseks võib olla seotud eesmärgiga tagada ressursside otstarbekas kasutamine. Mõnes ettevõttes võib õigustatud huvi tulenedada ka infoturbe kindlustamise vajadusest. Tööandja peaks oma õigustatud huvi selgelt põhjendama – autor toob välja, et õigustatud huvi võib väljenduda võrgu ja selles hoitavate töötajate ja klientide andmete, ärisaladuse ja intellektuaalse omandi kaitsmise vajaduses. Võrgu kaitsmise eesmärgil võib tööandja rakendada sellist jälgimisena käsitletavat tegevust nagu infopüük. Euroopa andmekaitse töörühm on seisukohal, et täielik infopüük ei saa praktikas olla vajalik ning tööandjal ei ole niivõrd

[134] M. Liiv. M. Miidla-Vanatalu. Kaugtöö ja paindliku töösuhte probleemid. – Personaliuudised. 16.05.2017. Arvutisõrgus: https://www.personaliuudised.ee/uudised/2017/05/16/kaugtoo-ja-paindliku-toosuhte-probleemid, (28.03.2019).
[135] N. Lugaresi. Electronic Privacy at the workplace: Transparency and Responsibility. – International review of Law, Computers & Technology 24/2010. Lk 165.

ulatuslikku õigustatud huvi. Samuti puudub tööandjal õigustatud huvi töötaja isikliku internetikasutuse vastu. Ehk kui Kui tööandjal on põhjendatult õigustatud huvi andmevoogude kaitsmiseks infopüügi abil, tuleks see konfigureerida selliselt, et ära hoida töötaja tegevuse pidev jälgimine. Näiteks isiklikel eesmärkidel veebis paikneva e-postkasti kasutamine ja internetipanga ja tervishoiusaitide külastamine peaksid jääma infopüügist välja.[136] Kuna töötaja isikliku veebikasutuse jälgimiseks ei ole tööandjal õigustatud huvi, võiks tööandja leevendusmeetmena pakkuda töötajatele alternatiivset, jälgimata juurdepääsu internetile. See võib seisneda tasuta *WiFi* võrgus või autonoomsete seadmete võimaldamises, mille abil saavad töötajad kasutada töövahendeid teatavatel isiklikel eesmärkidel.

3.4.2. Internetikasutuse jälgimise üldpõhimõtted

Kui tööandjal on õigustatud huvi interneti kasutamise jälgimiseks, peab ta hindama, kas see on kooskõlas isikuandmete kaitse üldpõhimõtetega. Proportsionaalsuse põhimõttest lähtudes on internetikasutusega seotud probleemide lahendamiseks kõige tõhusam ja lihtsam variant internetiühenduse puudumine tööarvutis. Kui töötajal puudub võimalus interneti kasutamiseks, kaob ära ka tööandja vajadus selle jälgimiseks. Magistritöö autor on aga seisukohal, et tegemist on suhteliselt äärmusliku vahendiga ning tänasel infoajastul tuleks internetti näha pigem abistava töövahendina kui segajana. Tõenäoliselt enamik arvutiga töötavatest inimestest vajavad tööülesannete täitmiseks aeg-ajalt internetti. Ka Euroopa andmekaitse töörühm on märkinud, et internetikasutuse täielik keelustamine on ebapraktiline ja isegi ebareaalne, sest internet kujutab endast olulist ja abistavat töövahendit.[137] Tegemist on aga üksnes soovitusega ning kui tööandja soovib interneti kasutamise täielikku keelustamist, siis on ta selleks õigustatud.[138]

Vältimaks töötaja privaatsuse riivet, on tööandjal lubatud keelustada interneti kasutamine isiklikul otstarbel. Magistritöö autor on seisukohal, et tööandja poolt ei ole mõistlik keelustada interneti kasutamist isiklikul otstarbel täielikult, sest tõenäoliselt ei tekita see mingeid probleeme, ega turvariske, kui töötaja loeb lõunapausi ajal ajalehe veebiväljaannet, külastab isiklikku e-postkasti

[136] Article 29 Data protection Working Party. Opinion 2/2017 on data processing at work. Lk. 13-14. Arvutivõrgus: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169. (20.01.2019).
[137] Article 29 Data Protection Working Party. Working document on the surveillance of electronic communications in the workplace. Lk. 24. Arvutivõrgus: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdf , (14.02.2019).
[138] M. Johnson. Employee Use of IT. – Rocket lawyer. Arvutivõrgus: https://www.rocketlawyer.co.uk/article/employee-use-of-it.rl (11.02.2019).

jms. Pigem aitab see töötajal hetkeks mõtted tööst mujale viia, et pärast pausi taas värskena tööülesannete täitmist jätkata. Töötajad ise on välja toonud järgmisi põjuseid, miks tööga mitteseotud veebilehti ja suhtlusvõrgustikke külastatakse:

- Vaimselt keerulisest tööst puhkepausi tegemiseks;
- Sõprade või perekonnaga suhtlemiseks;
- Kolleegidega suhtlemiseks, eesmärgiga suurendada avatud õhkkonda;
- Uute teadmiste omandamiseks;
- Suhtlemiseks inimestega samal tegevus- või kutsealal jms.[139]

Ka EIK on oma lahendis *Barbulescu vs. Romania* leidnud, et tööandja ei tohiks oma nõuete, sisekorraeeskirjade ja instruktsioonidega minna liialt karmiks ning redutseerida töötaja privaatset sotsiaalset elu töökohal nullini.[140] Vältimaks olukorda, kus jälgimise alla satub töötaja isiklik veebikasutus, võiks tööanjda piirata internetikasutust teatud kellaaegadel.[141]

Olukorras, kus tööandjal on õigustatud huvi internetikasutuse jälgimiseks eesmärgiga tuvastada selle väärkasutus, ei ole üldjuhul proportsionaalsuse põhimõttega kooskõlas kogu internetikasutuse jälgimine. Samuti kui interneti väärkasutust saab tuvastada muude vahenditega, vältides veebisaidi sisu analüüsimist, näiteks veebifiltrite kasutamise teel, on üldine internetikasutuse jälgimine ebaproprtsionaalne.[142] Magistritöö autor on arvamusel, et just mitmesugused veebifiltrid ja tulemüürid võimaldavad tööandjal vältida töötajate jälgimist, saavutades efektiivselt õigustatud huvile vastav eesmärk. Need tehnilised lahendused üksnes ei vähenda küberrünnakute riske, vaid võimaldavad blokeerida veebisaidid, mis pole tööga seotud ja mille kasutamine tööarvutis lubatud ei ole. USA-s kasutab veebisaitide filtreerimist hinnanguliselt 65% tööandjatest.[143] Reeglina on blokeeritud sellised veebisaidid, mille sisu on pornograafiline. Samuti ei luba paljud tööandjad tööarvutites külastada arvutimängude, sotsiaalmeedia ja e-poodide veebilehti.[144] Näiteks Politsei- ja Piirivalveametis on ressursside otstarbeka kasutamise huvides teatud internet lehekülgedele,

[139]C. Lampe. Social media and the workplace. – Pew Reseach Center, Internet & Technology. 22.06.2017. Arvutivõrgus: https://www.pewinternet.org/2016/06/22/social-media-and-the-workplace/, (14.03.2019).
[140] EIKo lahend. 61496/08. 12.01.2016. Bărbulescu vs Rumeenia
[141] M. Johnson. Employee Use of IT. – Rocket lawyer. Arvutivõrgus: https://www.rocketlawyer.co.uk/article/employee-use-of-it.rl, (11.02.2019).
[142] Article 29 Data protection Working Party. Opinion 2/2017 on data processing at work. Lk. 7-8 lk 23. Arvutivõrgus: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169. (20.01.2019).
[143] AMA/ePolicy Institute research. Electronic monitoring and surveillance survey. Arvutivõrgus: http://www.plattgroupllc.com/jun08/2007ElectronicMonitoringSurveillanceSurvey.pdf (16.03.2019).
[144] C. A. Ciccoletti. The Eavesdropping Employer: A Twenfy-first Century Framework for Employee Monitoring. – The American business Law Journal.

milleks on teadaolevad piraattarkvara lehed, mängude lehed, pornograafilist materjali sisaldavad lehed jms, juurdepääs infotehnoloogiliselt blokeeritud.[145] Magistritöö autor nendib, et kuna valdaval osal töötajatest on olemas nutiseade, mis võimaldab nimetatud veebilehekülgi külastada, ei saa tööandja kindel olla, et tööaja kasutus on otstarbekas.

Et töötaja ja tööandja huvid ning õigused oleksid tasakaalus, tuleks internetikasutust jälgides lähtuda minimaalse jälgimise põhimõttest. Minimaalne jälgimine võiks seisneda selles, et tööandja kogub küll andmeid töötajate internetikasutuse kohta, ent see ei ole personaliseeritud.[146] Saadud informatsiooni tulemusel on võimalik tööandjal saavutada jälgimise eesmärk ehk välja selgitada, kas on veebilehti, mis pole tööga seotud ja mida külastatakse tööajal liiga palju. Selle alusel on võimalik privaatsuspoliitikat muuta selliselt, et veebilehed, mis kulutavad tööaega ja juhivad tähelepanu töötegemisest kõrvale, kas blokeeritakse veebifiltrite abil või keelatakse nende kasutamine tööarvutis.

Läbipaistvuse põhimõtte kohaselt peab töötaja olema teadlik isikuandmete töötlemisest ja selle eesmärkidest. Talle peab olema tutvustatud turvanõudeid ning samuti peab töötajale olema teada, kellel on õigus tema internetikasutust jälgida. Autor on seisukohal, et nii nagu arvutikasutuse jälgimisel, oleks otstarbekas ka veebi jälgimisel läbipaistvuse tagamise eesmärgil kasutada kahekordset teavitamist. Ehk lisaks tööandja info- ja kommunikatsioonitehnoloogia vahendite kasutamise reeglite tutvustamisele, võiks ettevõtte IT-süsteem töötajaid arvutisse sisenedes teavitada, et tema veebikasutust võidakse kontrollida.

3.5. E-posti kasutamise jälgimine

E-kirjade jälgimine on õigusteadlaste, IT-spetsialistide, töötajate ja tööandjate poolt enim analüüsitud valdkond, mis puudutab privaatsust töökohal.[147] On tavapärane, et töötaja kasutab tööülesannete täitmiseks ettevõtte nimega e-posti aadressi. Probleemseks muudab aga valdkonna eelkõige asjaolu, et töötajad kasutavad tööandjale kuuluvat e-posti aadressi ka isikliku kirjavahetuse pidamiseks. Tõenäoliselt kasutavad töötajad tööalast e-posti ka erakirjade saatmiseks

[145] O. Kirst. Sõnumisaladuse kaitse tööandja sidevahendi kasutamisel. – Juridica IV/2012. Lk 428
[146] C. A. Ciccoletti. The Eavesdropping Employer: A Twenfy-first Century Framework for Employee Monitoring. – The American business Law Journal.
[147] C. A. Ciccoletti. The Eavesdropping Employer: A Twenfy-first Century Framework for Employee Monitoring. – The American business Law Journal.

seetõttu, et nii jõuavad kirjad kõige operatiivsemalt nendeni. Tööalane e-postkast on reeglina terve tööpäeva vältel avatud, mistõttu puudub vajadus veebirakenduse või isikliku seadme kaudu privaatsesse e-postkasti sisse logimiseks, selle jälgimiseks jne. Kuigi töö- ja isiklike e-kirjade haldamine ühes ja samas postkastis täidab kahtlemata mugavuse eesmärki, kaasneb sellega oht, et privaatsed kirjad ning nende sisu võivad tahtlikult või kogemata jõuda ka tööandjani. Kuna tööandja väljastab ettevõtte domeeniga e-posti aadressi tööülesannete täitmise eesmärgil, võib tööandjal tekkida aeg-ajalt vajadus töötaja postkastist informatsiooni otsimiseks.

Arvestades tööalase e-posti kontrollimisega seotud küsimuste rohkust ja aktuaalsust, nõustub autor AKI seisukohaga, mille kohaselt esmajoones peaks oma eraelu kaitsma iga inimene ise. Ehk töötajad peaksid eelkõige ise meeles pidama ja rakendama oma eraelu ja sõnumine saladuse kaitseks kõiki võimalikke meetmeid.[148] Kõige lihtsamaks mooduseks on isiklike kirjade kustutamine tööandjale kuuluvast postkastist. See ei pruugi olla igal juhul efektiivne meede, sest autorile teadaolevalt rakendavad paljud tööandjaid käesoleval hetkel e-posti varundamist, mis tähendab seda, et isiklikud kirjad paiknevad ka pärast kustutamist mingi kindla aja jooksul tööandja serveris. Igal juhul on selge, et töötaja ei saa eeldada, et tööandja poolt tagatud e-posti ja teisi sidevahendeid kasutades on talle garanteeritud absoluutne diskreetsus ning isikliku ja tööalase suhtluse vahele saab tõmmata selge piiri.[149]

3.5.1. Õiguslik alus töötaja e-posti jälgimiseks

Tööandja õigustatud huvi töötaja e-postkasti jälgimiseks ja e-kirjade lugemiseks võib olla olukorrast sõltuvalt väga erinev. Näiteks võib tööandjal olla vaja arvutisüsteemide tõrgeteta ja turvalise töökorra tagamiseks tuvastada suuremahulised ja ohtlikud e-kirjad või lugeda töötaja puhkuse või äkilise haigestumise ajal saabunud arveid ja tellimusi.[150] Töötaja tööalaste e-kirjade lugemine kontrollimise või töö korraldamise eesmärgil ei kujuta endast ohtu töötaja privaatsusele ja on seetõttu lubatud. Töötaja postkasti või konkreetseid e-kirju uurides on tööandjal aga risk

[148] Andmekaitse inspektsioon. Isikuandmete töötlemine töösuhtes. Abistav juhendmaterjal. Lk 61. Arvutivõrgus: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikuandmed%20t%C3%B6%C3%B6suhetes%20juhendmaterjal26%2005%202014_0.pdf. (10.01.2019).
[149] A. Nõmper. K. Michelson. Kas tööandja saab sidevahendite kasutamist kontrollida? Arvutivõrgus: https://majandus24.postimees.ee/240487/kas-tooandja-saab-sidevahendite-kasutamist-kontrollida, (11.02.2019).
[150] G. Sibold. Tööandja võib lugeda ka su isiklikke e-kirju, aga väga hea põhjusega. – Digigeenius. Arvutivõrgus: https://digi.geenius.ee/rubriik/uudis/tooandja-voib-lugeda-ka-su-isiklikke-e-kirju-aga-vaid-vaga-hea-pohjusega/, (16.03.2019).

sattuda peale töötaja erakirjadele. Erakirjadeks on kusjuures ka kolleegide omavaheline, tööga mitteseotud suhtlus ning juba ainuüksi erakirja liiklusandmete nägemine kujutab endast töötaja privaatsusõiguse riivet.[151]

Töötaja erakirjad, s.h. nende liiklusandmed kuuluvad eraelu kaitsealasse ning õigus sõnumite saladusele peab olema tagatud nii eravalduses, äriühingus kui ka ametiasutuses ehk nii kodus kui ka isiku töö- või ametikohal.[152] Seetõttu ei saa tööandjal üldjuhul olla õigustatud huvi töötaja erakirjade lugemiseks ega nende saatmise või vastuvõtmise fakti tuvastamiseks. EIK on lahendis *Copland vs. United Kingdom* kinnitanud, et töökohalt isiklikel eesmärkidel saadetud e-kirjade jälgimisega riivatakse eraelu ja sõnumisaladuse puutumatust.[153] Lahendis *Barbulescu vs. Romania* andis EIK konkreetseid juhiseid selle kohta, millistel juhtudel ja ulatuses on tööandjal lubatud töötajate kirjavahetust jälgida. Kõnealuse kaasuse puhul lõpetati töötajaga töösuhe põhjendusega, et töötaja on rikkunud ettevõtte sisekorraeeskirjas kehtestatud reegleid, mille kohaselt ei ole lubatud töövahendite, s.h. e-maili ja tööandja loodud *Yahoo Messenger'i* isiklikul otstarbel kasutamine. Tööandja luges enne töölepingu ülesütlemist töötaja eravestlusi *Yahoo messenger*-is, s.h. tegi nendest koopiad, eesmärgiga tõendada töötaja poolset töökorralduse reeglite rikkumist. Euroopa Inimõiguste kohus leidis oma lahendis, et tööandjal puudus õigustatud huvi erakirjade lugemiseks ning kopeerimiseks ja selline tegevus riivas töötaja õigust privaatsusele.[154] Vastukaaluks eelnevale saab välja tuua Inglismaa kõrgema astme kohtu lahendi *EWHC 376 (CB) Williams vs Leeds United Football club.* Kõnealuse juhtumi puhul otsis tööandja aktiivselt tõendeid töölepingu ülesütlemiseks töötajaga. Muuhulgas hõlmas tõendite otsimine e-posti jälgimist. Jälgimistegevuse tulemusena leidis tööandja töötaja postkastist ebasobiva sisuga e-kirja, mis oli viis aastat tagasi saadetud samas ettevõttes töötavale naiskolleegile. Töötaja vaidlustas töölepingu ülesütlemise, ent kohus kinnitas, et tööandjal oli õigus töötaja erakirjas sisaldvat informatsiooni kasutada, vaatamata asjaolule, et kirja saatmisest oli möödunud juba viis aastat.[155] Kaasuse muudab erakordseks ka see, et kinnitust leidis fakt, mille kohaselt tööandja otsis aktiivselt tõendeid töölepingu rikkumise kohta, eesmärgiga lõpetada tööleping ennetähtaegselt ja vältida lepingus

[151] A. Sander. Töötaja kontrollimine ja isikuandmete kaitse. Kas ja kuidas võib tööandja töötajat kontrollida? Arvutivõrgus: http://www.tarkgruntesutkiene.lv/uudised/kasulik/toeoetaja-kontrollimine-ja-isikuandmete-kaitse-kas-ja-kuidas-voib-toeoeandja-toeoetajat-kontrollida, (20.03.2019).
[152] S. Laos. H. Sepp. Põhiseaduse § 43 kommentaar, komm. 11. - Ü. Madise jt (toim). Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. 4., täiend. vlj. Tallinn: Juura, 2017
[153] EIKo lahend.. 62617/00. 03.05.2007. Copland vs Ühendkuningriik
[154] EIKo lahend. 61496/08. 12.01.2016. Bărbulescu vs Rumeenia
[155] Inglismaa kõrgema astme kohtu lahend. 2015 E*WHC 376 (CB) Williams vs Leeds United Football club.*

kokku lepitud tasu maksmist. Magistritöö autor on seisukohal, et kuigi kõnealuse juhtumi puhul oli ettevõttes kord, mis keelas töö e-posti kasutamise isiklikel eesmärkidel, oleks käesoleval hetkel üldmääruse valguses keeruline tõendada tööandja õigustatud huvi töötaja e-kirjade uurimiseks samadel asjaoludel.

Kindlasti ei saa tööandja põhjendada oma õigustatud huvi sellega, et e-posti aadress kuulub talle. Üksnes asjaolu, et ettevõtte domeeniga e-posti aadress kuulub tööandjale, et tähenda seda, et ka sealsed e-kirjad kuuluvad talle, või et neid võib lugeda.[156] USA-s vastupidiselt on töötaja õiguspärane ootus privaatsusele ja sõnumisaladusele väiksem põhjendusega, et e-posti aadress ja töövahendid kuuluvad tööandjale. Prantsusmaal seevastu on töötajate ootus privatsusele töökohal väga kõrge ning tööandjad ei tohi lugeda töötajate e-kirju ka siis, kui neile on seatud keeld isiklike meilide saatmiseks.[157]

Harvadel juhtudel ei pruugi olla välistatud ka olukord, kus tööandjal on õigustatud huvi töötaja erakirjade jälgimiseks. Praktikas on erakirjade õigustatud jälgimise juhtumid seotud teadus- või tööstusspionaaži, töötaja konfidentsiaalsuskohustuse või konkurentsikeelu rikkumisega. Päris ilma põhjuseta tööandja töötajate lojaalsust ja konfidentsiaalsust kontrollida ei tohi, vaid tal peab olema põhjendatud kahtlus, et töötaja on rikkumise toime pannud. Ehk tööandja ei tohiks erakirjadena identifitseeritavaid kirju avada ja lugeda, kui ei ole reaalset ning tõsist riski ettevõtlusele või ärisaladusele. Soovitatav on töötajat enne erakirjade kontrollimist informeerida.[158]

Arvestades üha kasvavat eri riikide vahelist konkurentsi majanduses, on suundumus töötajate sidevahendite, s.h. kõige levinuma kommunikatsioonivahendi ehk e-posti põjalikumale kontrollimisele pigem kasvav kui kahanev nähtus. Selle üheks põhjuseks ongi eelnevalt välja toodud teadus- ja tööstusspionaaži kasv, mis tekitab ettevõtjatele ning seeläbi ka riikide majandusele tõsist majanduslikku kahju.[159] Kinnitust on leidnud asjaolu, et tõendid tööstusspionaaži, konkurentsikeelu rikkumise või ärisaladuse hoidmise keelu mittejärgimine kohta ilmnevad valdavalt just erasuhtluses.[160] Autor leiab, et sellises olukorras ei ole tööandja õigustatud

[156] N. Lugaresi. Electronic privacy in the workplace: Transparency and responsibility. – International review of Law, Computers & Technology. 24/2010. Lk 168
[157] A. Jõks. Eraelu kaitse töösuhtes – väljakutsed tööandjale. Arvutivõrgus: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Allar%20J%C3%B5ks%202010.pdf, (07.03.2019).
[158] S. Thompson. Can employers legally monitor employees' e-mails at work? - GDPR report. 11/2017. Arvutivõrgus: https://gdpr.report/news/2017/11/17/5383/, (19.03.2019).
[159] O. Kirst. Sõnumisaladuse kaitse tööandja sidevahendi kasutamisel. – Juridica IV/2012. Lk 428
[160] A. Nõmper. K. Michelson. Kas tööandja saab sidevahendite kasutamist kontrollida? Arvutivõrgus: https://majandus24.postimees.ee/240487/kas-tooandja-saab-sidevahendite-kasutamist-kontrollida, (11.02.2019).

huvi e-posti jälgimiseks seotud töötaja kontrollimisega, vaid eesmärgiga vältida ulatuslikke kahjusid ja tagada ettevõtte normaalne funktsioneerimine. Tuntuim näide on kahtlemata Soome telefonitootja *Nokia* ja Hiina telekommunikatsioonivõtte *Huawei* juhtum, mille puhul kahtlustas esimene, et *Huawei* on e-posti teel omandanud *Nokia* ärisaladusi. Nimelt märkasid *Nokia* töötajad tehnikamessil osaledes, et *Huawei* toodang sarnaneb kahtlaselt toodetega, mida Nokia kavatses messil esmakordselt esitleda. Tuvastamaks ärisaladuse lekitajat, hakkas *Nokia* oma töötajate e-posti uurima. Jälgimistegevuse tulemusena leidis *Nokia* ühe oma töötaja kasutuses olevast e-postkastist jäljed vähemalt 69 kontakti kohta *Huaweiga*.[161] Paljude Soome juristide arvates oleks aga selle juhtumi puhul tulnud alustada uurimist *Nokia* juhtkonna enda tegevusest, sest väidetavalt ületati sel hetkel kehtinud seadustest tulenevaid volitusi.[162] Autori arvates on ka tänaseid andmekaitsereegleid silmas pidades pigem ebatõenäoline, et tööandjal on sellises olukorras õigustatud huvi kõikide oma töötajate e-postkastide seireks. Kahtluse olemasolul oleks mõistlik kõigepealt kindlaks määrata töötaja või töötajate ring, keda kahtlustatakse ärisaladuse lekitamises. Sarnaselt on oma töötajate e-posti jälginud Saksamaa suurim telekommunikatsiooni ettevõte *Deutshe Telekom*, eesmärgiga tuvastada kontaktid ajakirjanikega. Seesugune jälgimistegevus tunnistati Saksamaa õigusteadlaste ja üldsuse poolt lubamatuks, kuid ettevõtte tippjuhtide suhtes algatatud kriminaalasi kohtuni ei jõudnud ja lõpetati seoses tõendite ebapiisavusega. Küll aga esitati süüdistus ettevõtte turvajuhile ning mitmele äriturvalisuse eest vastutavale töötajale, kes olid kaasatud jälgimistegevusesse.[163] Ka magistritöö autor on seisukohal, et tööandjal puudub õigustatud huvi erakirjade lugemiseks ajakirjanikega suhtluse tuvastamise eesmärgil. Võimalike kontaktide väljaselgitamist võib pidada põhjendatuks olukorras, kus suhtlemine on seotud näiteks ärisaladuse hoidmise kohustusega.

3.5.2. E-posti jälgimise põhimõtted

Probleemne on ka see, et kolleegide omavaheline suhtlus võib üheaegselt hõlmata nii era- kui ka tööalast suhtlust, mistõttu ei saa tööandja alati kirja saatja või saaja järgi otsustada, kas avada kiri või mitte. Magistritöö autor on seisukohal, et tööandja peaks otsustama töötaja postkasti ja kirjade

[161] P. Sajari. Nokia jatkoi työntekijöidensä viestiliikenteen urkintaa. – Helsingin Sanomat. 09.06.2008
[162] O. Kirst. Sõnumisaladuse kaitse tööandja sidevahendi kasutamisel. – Juridica IV/2012. Lk 429
[163] O. Kirst. Sõnumisaladuse kaitse tööandja sidevahendi kasutamisel. – Juridica IV/2012. Lk 429

uurimise kasuks üksnes siis, kui alternatiivsed meetmed ei anna soovitud tulemust. Näiteks võiks enne postkasti uurimist paluda töötajal endal edastada või näidata soovitud kirjavahetust.

Eestis on praktikas kujunenud tavapäraseks, et töötajad kasutavad tööandja domeeniga e-posti aadresse m.h. ka oma erakirjade saatmiseks ja vastuvõtmiseks, kui tööandja pole kehtestanud muid reegleid töökorraldusele. Igal juhul on tööandjal õigus kehtestada vastav nõue, et tööandja domeeniga e-posti ei ole lubatud kasutada isiklike e-kirjade saatmiseks. Kui tööandja ei näe vajadust kõnealuse keelu rakendamiseks, peaks ta vähemalt kehtestama reegli, et erakirjad tuleb postkastist kustutada või tõsta spetsiaalselt loodud alamkausta, mis oleks tööandja jaoks selgelt eristatava pealkirjaga, näiteks "isiklik".[164]

Läbipaistvuse tagamiseks peavad e-posti haldusega seonduvad küsimused ja reeglid olema hästi läbimõeldud ning töötajatele töökorralduse reeglite kaudu teatavaks tehtud. Näiteks peaks töötajale olema teada, kellel ja milliste tööülesannete täitmiseks, on juurdepääs tema e-postkastile, kuidas käituda e-postkasti suunamisega puhkuse või töövõimetuse ajal, kas postkasti koopia (inglise keeles *back up*) asub tööandja serveris jne. Kui tööandja vastavaid e-posti kasutamise reegleid ei kehtesta ja töötajatele teatavaks ei tee, on töötajal õiguspärane ootus privaatsusele ja sõnumisaladusele ning tööandja peab arvestama asjaoluga, et e-postkastis võib olla ka töötaja isiklikke kirju.

Isegi kui tööandja lubab kasutada e-posti ka isiklikul otstarbel, oleks mõistlik kindlaks määrata reeglid selle kohta, et tööprotsesside normaalseks toimimiseks vajaminev info on kättesaadav ka siis, kui töötaja on kontorist eemal. Näiteks võib praktikas tekkida olukord, kus koosoleku läbiviimiseks olulised materjalid ja dokumendid asuvad haigestunud töötaja e-postkastis. Läbipaistvuse tagamiseks peab sellisel juhul info otsimine haigestunud töötaja postkastist toimuma eelnevalt kindlaks määratud protseduurireegleid järgides. Töötaja peab olema teadlik kellel ja millistel asjaoludel on tema eemaloleku ajal ligipääs postkastis olevale teabele.[165]

EIK leidis lahendis *Barbulescu vs. Romania*, et tööandja rikkus läbipaistvuse põhimõtet, mis seisnes selles, et töötaja ei olnud sidevahendite jälgimisest teadlik ning lisaks ei olnud töötajale teada asjaolu, et tööandjal on ligipääs tema kasutuses olevale kontole *Yahoo* keskkonnas. Samuti

[164] Andmekaitse inspektsioon. Kas tööandjal on õigus lugeda minu e-kirju? Arvutivõrgus: https://www.aki.ee/et/kas-tooandjal-oigus-lugeda-minu-e-kirju. (22.02.2019).
[165] Euroopa andmekaitse inspektor. Access to e-communications data when an employee is absent. Arvutivõrgus: https://edps.europa.eu/data-protection/data-protection/reference-library/access-ecommunications-data-when-employee-absent_en (07.03.2019).

viitas kohus asjaolule, et tööandja poolne jälgimine kõnealuses situatsioonis ei ole proportsionaalne ning eesmärgi saavutamiseks oleks ka teisi, töötaja privaatsust vähem riivavaid meetmeid.[166]

3.6. Info ja kommunikatsioonitehnoloogia vahendite kasutamise eeskirja kehtestamise vajadus

Vaatamata faktile, et võimalusi töötaja arvuti- interneti- ja e-posti jälgimiseks on seoses tehnoloogia arenguga tekkinud väga palju, nii tarkvaraliste lahendustena kui pilveteenustena, on nende kasutamine üsna piiratud. Olenemata tehnoloogia uudsusest või intensiivsusest, allub nende kasutamine ühtsele isikuandmete kaitse regulatsioonile. Üksnes asjaolu, et potentsiaalsed tehnoloogilised võimalused töötaja jälgimiseks on suurenenud, ei tähenda seda, et nende kasutamine on lubatud. IKT vahendite kaudu kogutud isikuandmete töötlemist ei ole autori hinnangul vajalik reguleerida seaduse tasandil, sest õigustatud huvi nõue seab juba praegu piisavalt range piirangu.

Autor näeb aga enim probleeme läbipaistvuse põhimõtte mittejärgimises, ehk töötajate ebapiisavas teavitamises IKT vahendite kaudu kogutud andmete töötlemise kohta. Kuna ka praktikas on suur osa vaidlustest seotud just töötajate ebapiisava teavitamisega, siis lisaks tule- ja tööohutuse ning töötervishoiunõuete tutvustamise nõudele võiks tööandja jaoks kohustulikuks muuta ka tööandjale kuuluvate IKT vahendite kasutamise eeskirja kehtestamise. Käesoleval hetkel ei ole tööandjal kohustust IKT vahendite kasutamise ja nende kaudu kogutud isikuandmete töötlemise eeskirja kehtestamiseks, kuid autori arvates täidaks just asjaomane eeskiri, mis on töötajatele teatavaks tehtud ja millega on võimalik ka hiljem tutvuda läbipaisvuse põhimõtte eesmärki. Siseriikliku õigusega on võimalik töötaja IKT vahendite kasutamise eeskirja nõue mõistlikult ja efektiivselt reguleerida. See muudaks ühelt poolt tööandjate tegevuse palju läbipaistvamaks ning töötajate isikuandmete kaitse oleks paremini tagatud. Vastav regulatsioon võiks sisalduda autori hinnangul töölepinguseaduses tööandja kohustuste all.

Vältimaks andmekaitse ja privaatsuse rikkumisi töökohal, on autor arvamusel, et tööandjad peaksid pöörama tähelepanu tööaja väärkasutuse ennetamisele ning üksnes vajaduse korral tuvastamisele. Autor leiab, et võimalike kohtuvaidluste või andmekaitse rikkumisega seotud sanktsioonide

[166] EIKo lahend. 61496/08. 12.01.2016. Bărbulescu vs Rumeenia

vältimiseks on mõistlik koostada töökorralduse eeskiri, mis sisaldab m.h. konkreetseid ja arusaadavaid elektrooniliste töövahendite kasutamise reegleid ning teavet tööandja poolt jälgitavate seadmete ja jälgimisviiside kohta.

Kui varasemalt olid trahvid andmekaitse rikkumiste eest pigem marginaalsed, siis käesoleval hetkel võib andmetöötluse nõuete ja üldpõhimõtete rikkumise korral järgneda tööandjale karm sanktsioon. Tööandjad, eelkõige suurkorporatsioonid, peavad võtma andmekaitse valdkonda väga tõsiselt, sest viimase aasta praktika näitab, et andmekaitseasutused püüavad trahvide määramisel näidata, et seadusandjal on üldmäärusega n.ö tõsi taga.[167] Konkreetsete ja üheselt mõistetavate kommunikatsioonivahendite kasutamise reeglite kehtestamine on mõistlik nii tööandja kui ka töötajate huvides, sest kui reegleid pole, on töötajal õigustatud ootus privaatsusele. Üldmääruse kohaselt peab andmesubjekt minimaalselt olema teadlik andmetöötluse eesmärkidest ja vahenditest.[168] Kusjuures iga üksiku andmetöötluse võimaluse puhul peavad need eesmärgid olema eraldi välja toodud ning vältida tuleks üldist ja abstraktset sõnastust. Autor toob välja, et kõnealused reeglid peaksid sisaldama teavet selle kohta, kas tööandja IKT vahendeid on lubatud kasutada isiklikuks otstarbeks või mitte; milliseid IKT vahendeid tööandja jälgib ning milliseid isikuandmeid ja milliste konkreetsete jälgimisviisidega töödeldakse; millise reegli järgi kogutud andmeid hoitakse; kellel on kogutud andmetele juurdepääs ja millised õigused on töötajal, kelle kohta need andmed käivad. Sisuliselt tähendab see seda, et tööandja peab protsessiliselt lahti kirjeldama, mida ja millisel eesmärgil kogutakse ja töödeldakse.[169] Autor rõhutab, et kindlasti peaks eeskiri sisaldama teavet võrgu ja töövahendite lubatud ja lubamatu kasutamise kohta. Nagu eelnevalt kirjas, ei ole tõenäoliselt mõistlik keelata ära tööandjale kuuluvate IKT vahendite täielik kasutamine isiklikul otstarbel. Seetõttu peaks vastav eeskiri sisaldama detailset teavet m.h. selle kohta, milliste internetisaitide külastamine on tööandja jaoks aktsepteeritav; kas ja millist tarkvara võib töötaja oma tööarvutile paigaldada; kas tööandja domeeniga e-posti kasutamine on lubatud; kas erakõned tööandja telefonilt on lubatud jne. See võimaldab töötajatel kohanda oma käitumist, vältimaks tööandjapoolset jälgimist, eeldusel, et nad kasutavad töövahendeid õiguspäraselt. Samuti tuleks eeskirjas kindlaks määrata, millistel ettevõtte töötajatel on juurdepääs kogutud teabele. Oluline on, et need töötajad oleksid kursis andmekaitse ja küberturvalisusega ning läbiksid

[167] T. Kookmaa. Kaks soovitust andmekaitse trahvide vältimiseks. – Äripäev. Arvutivõrgus: https://www.aripaev.ee/uudised/2019/02/19/kaks-soovitust-andmekaitse-trahvi-valtimiseks, (20.02.2019).
[168] Andmekaitse üldmäärus. Art 4 p 7. Mõisted.
[169] M. Jalakas. Andmekaitse uue määruse valguses. – IT ja andmekaitse – Mart Jalakas. Arvutivõrgus: https://mtjholding.ee/andmekaitse-uue-maaruse-valguses/, (20.03.2019).

regulaarselt valdkonnaspetsiifilisi koolitusi. Kommunikatsioon, mis on selgelt identifitseeritav privaatsena, ei tohiks kuuluda jälgimisalasse. [170]

Eestis on lubatud tööandjal koostada kommunikatsioonivahendite kasutamise eeskiri iseseisvalt, ent on ka riike, kus kõnealused reeglid peavad saama heakskiidu töötajate esindusorgani poolt. Euroopa Liidu liikmesriikidest on üheks näiteks Prantsusmaa, kus töötajate õigustatud ootus privaatsusele on kõrge ning siseriiklikud seadused kaitsevad privaatsuse küsimustes pigem töötajat.[171] Olenevalt ettevõtte suurusest, näeb prantsuse töökoodeks (prantsuse keeles *code du travail*) ette töötajate delegatsiooni (prantsuse keeles *délégués du personnel*) või töötajate nõukogu (prantsuse keeles *comité d'entreprise*) olemasoluks. Needsamad töötajate esinduskogud omavad olulist rolli mitmesuguste töökorralduslike eeskirjade kehtestamisel ja muutmisel, samuti peab esinduskoguga olema kooskõlastatud jälgimisseadmete kasutamine. Näiteks on tööandjal keelatud enne esinduskoguga konsulteerimist lugeda tööandja serveris paiknevaid e-kirju isegi siis, kui need on tööga seotud.[172]

Magistritöö autor on seisukohal, et praktikas tuleks vältida olukorda, kus IKT vahendite kasutamist puudutava eeskirja loomisel konsulteeritakse üksnes infotehnoloogidega. Mõistlik on kombineerida IT valdkonna spetsialiste, juriste ning töötajate esindajaid, sest üksnes nii on võimalik koostada eeskiri, mis keskendub ühelt poolt turvalisusele, teisalt peab aga silmas ka töötajate huve ja õigust privaatsusele.

Euroopa andmekaitse töörühm möönab, et töökorralduse reegleid tuleks hinnata vähemalt kord aastas, et teha kindlaks, kas valitud jälgimislahendus tagab soovitud tulemused ning kas tehnoloogia areng on kaasa toonud uusi, proportsionaalsemaid vahendeid, et saavutada sama eesmärk. Hea tavana tuleks enne mistahes jälgimistehnoloogia kasutuselevõttu läbi viia andmekaitsealane mõjuhinnang (inglise keeles *PIA privacy impact assessment*).[173] Töötajate jälgimine kujutab endast kõrge riskiga andmetöötlust, mistõttu on soovitatav läbi viia detailne ja jälgimisseadmete kasutamise eesmärke ning töötajate privaatsusõigust arvestav andmekaitse

[170] Global data hub. Employee monitoring update. Arvutivõrgus: https://globaldatahub.taylorwessing.com/article/employee-monitoring-update, (11.02.2019).
[171] M. Lane. Monitoring employee emails in the UK, France, Singapore and Germany. CMS Law now. Arvutivõrgus: http://www.cms-lawnow.com/ealerts/2016/02/monitoring-employee-emails-in-the-uk-france-singapore-and-germany?cc_lang=en, (20.03.2019).
[172] L. Joncour. Ten things to know about labour and employment law in France. – Norton Rose Fulbrright. Arvutivõrgus: https://www.nortonrosefulbright.com/en/knowledge/publications/f1d8c939/ten-things-to-know-about-labour-and-employment-law-in-france, (11.02.1019).
[173] Article 29 Data protection Working Party. Opinion 2/2017 on data processing at work. Lk 14. Arvutivõrgus: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169. (20.01.2019).

mõjuhinnang. Juhtudel, mil mõjuhinnagu tulemusel selgub, et jälgimisseadmete kasutamine kujutab potentsiaalset riski töötajate privaatsusele, on lisaks soovitatav konsulteerida riikliku andmekaitseasutusega.[174]

Eelneva põhjal ei saa siiski järeldada, et info- ja kommunikatsioonitehnoloogia vahendite jälgimine on tööandja jaoks raskendatud või isegi välistatud. Autor rõhutab, et kommunikatsioonivahendite jälgimine on üks osa töötajate kontrollist, ent tööandja peab rangelt järgima, et seejuures oleksid täidetud kõik isikuandmete kaitsele kehtestatud nõuded. Just läbipaistvuse huvides peaks olema kehtestatud ja töötajatele teatavaks tehtud kommunikatsioonivahendite kasutamise kord ning kui tööandjal on õigustatud huvi nende jälgimiseks, siis tuleb töötajatele teatavaks teha ka jälgimise viisid ja eesmärgid.

3.7. Sotsiaalmeedia jälgimine

3.7.1. Õiguslik alus töötaja sotsiaalmeedia jälgimiseks

Praktikas on sotsiaalmeediasse tehtud postituste jälgimisega seotud problemaatika tõusetunud eelkõige tööle kandideerivate isikute puhul, mille käigus tööandja teostab kandidaadi sotsiaalmeedia abil n.ö taustakontrolli. Kuna sinna üles laetud postitused peegeldavad suuresti inimese iseloomu, harjumusi, hoiakuid ja põhimõtteid, võib see kahtlemata vähendada konkursil valituks osutumise võimalusi. Vähem tähelepanu pälvinud teema on aga ka see, et tööandja võib tunda huvi ka selle vastu, mida tema olemasolevad töötajad on internetti postitanud. Juhtudel, mil töötaja on ise otsustanud enda kohta avalikult midagi jagada, olgu siis sotsiaalmeedias, blogis, internetikommentaarides või traditsioonilises meedias, ei saa AKI sõnul mitte kellelegi pahaks panna selle infoga tutvumist.[175] Vaatamata sellele, peavad tööandjad aga arvestama, et töötaja sotsiaalmeedia jälgimine ärilisel eesmärgil, kujutab endast isikuandmete töötlemist mistõttu peab jälgimine toimuma vastavalt andmekaitse reeglitele. Üksnes asjaolu, et töötaja sotsiaalmeedia profiil on avalik, ei anna tööandjale õigust sealseid andmeid enda huvides töödelda. Tööandja peab

[174] Global data hub. Employee monitoring update. Arvutivõrgus: https://globaldatahub.taylorwessing.com/article/employee-monitoring-update (11.02.2019).
[175] G. Sibold. Millistel juhtudel võib tööandja uurida, mida sa sotsiaalmeedias teed? – Digigeenius. 19.10.2017. Arvutivõrgus: https://digi.geenius.ee/rubriik/uudis/millistel-juhtudel-voib-tooandja-uurida-mida-sa-sotsiaalmeedias-teed/, (16.03.2019).

arvestama, et ta ei kogu andmeid reeglina lihtsalt huvist, vaid andmete kogumisel võivad olla profiili kasutajale tagajärjed, näiteks töölepingu ülesütlemine.[176] Teoreetiliselt seni, kuni sotsiaalmeedia kaudu teatavaks saanud info töösuhet kuidagi ei mõjuta võib tööandja avalikult jagatud postitusi lugeda ilma, et sellega kaasneks isikuandmete töötlemine.

Õiguslik alus töötaja sotsiaalmeedia jälgimiseks ei saa olla seotud töötaja nõusolekuga, vaid tööandja peab tõendama õigustatud huvi olemasolu. Tööandjad reeglina põhjendavad töötaja sotsiaalmeedia jälgimist sellega, et soovitakse olla kindel, et töötajate tehtavad postitused ei kahjusta tööandja mainet. Paratamatult kõik see, mida töötaja tööandja kohta sotsiaalmeediasse või laiemalt internetti postitab, peegeldab organisatsiooni ja brändi.[177] Tehnoloogia arengut silmas pidades, on informatsiooni jagamine muutunud äärmiselt lihtsaks ning konfliktsituatsioonid töötaja ja tööandja vahel kerged ilmnema. Tööandja jaoks on oluline kindlaks teha, et tema töötajad on lojaalsed ka väljaspool tööaega ning seetõttu võib kõne alla tulla justnimelt sotsiaalmeedia monitoorimine, eesmärgiga leida ettevõtte mainet kahjustavaid kommentaare või postitusi. Üldmäärust silmas pidades Euroopa andmekaitse töörühm seisukohal, et õigustatud huvi ja jälgimise eesmärk peab alati olema seotud mingi konkreetse juhtumiga.[178] Näiteks juhtudel, mil tööandja tähelepanu juhitakse asjaolule, et tema töötaja avaldab ettevõtte ärisaladusega seotud postitusi, saab jaatada tööandja õigustatud huvi ning jälgimisel on selge ning ühemõtteline eesmärk.[179] Küll aga ei tööandjal õigustatud huvile vastavat õiguslikku alust suvaliseks töötajate profiilide kontrollimiseks, eesmärgiga leida ebasobivat sisu või kommentaare. Euroopa andmekaitse töörühm soovitab tööandjatel töötajate sotsiaalmeediat võimalusel üldse mitte jälgida, sest tänu sealsetele profiilidele ja uudsete analüüsitehnoloogiate arengule on tööandjatel tehniline suutlikkus teha pidevat töötajate taustakontrolli, kogudes teavet nende sõprade, arvamuste, veendumuste, huvide, kommete, asukoha, seisukohtade ja käitumise kohta, kogudes seega andmeid, s.h. töötaja era- ja perekonnaeluga seotud eriliiki isikuandmeid.[180] Kahtlemata võivad töötajate negatiivsed kommentaarid ja postitused mingis ulatuses kahtlustada tööandja mainet, ent

[176] S. Suder. Tööandja, ära konda Facebookis! – Personaliuudised. 22.08.2017. Arvutivõrgus: https://www.personaliuudised.ee/uudised/2017/08/22/tooandja-ara-konda-facebookis, (29.03.2019).
[177] G. Dietrich. Social media polocy: When are Your owm opinions not okay? Arvutivõrgus: https://spinsucks.com/social-media/social-media-policy-when-are-your-own-opinions-not-okay/ (29.03.2019).
[178] Article 29 Data Protection Working party. Opinion 2/2017 on data processing at work. Lk 12. Arvutivõrgus: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169. (20.01.2019).
[179] L. Irwin. EU regulators to curb employers searching social media. – IT governance European blog. Arvutivõrgus: https://www.itgovernance.eu/blog/en/eu-regulators-to-curb-employers-searching-social-media (25.03.2019).
[180] Article 29 Data Protection Working party. Opinion 2/2017 on data processing at work. Lk 12. Arvutivõrgus: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169. (20.01.2019).

siiski nõustub magistritöö autor andmekaitse töörühma seisukohaga, et võimalusel tuleks töötajate sotsiaalmeedia monitoorimist vältida. Vastasel juhul on reaalne oht, et töötajad võivad karistada saada ka selliste postituste eest, mis tööandjale lihtsalt ei meeldi. Samuti peab tööandja arvestama, et sõna- ja väljendusvabadus hõlmab m.h. avaldusi, mis on solvavad, shokeerivad või häirivad ning pole mingit põhjust, miks see põhimõte ei peaks kehtima tööalases kontekstis.[181] Samas spontaanne ja triviaalne kõne ei ole reeglina kaitsmist väärt.

Kindlasti ei ole tööandjal õigustatud huvile vastavat õiguslikku alust nõuda, et töötaja lisaks tööandja oma era-sotsiaalmeedia kontolt sõbraks. AKI seisukoha kohaselt on selline nõue sisuliselt võrreldav tööandja nõudega käia töötajal kodus külas. Töötaja eraelu, mille hulka tänasel päeval saab arvata ka privaatse sotsiaalmeedia konto, on esmajoones puutumatud ning asjaolu keda töötaja oma sotsiaalmeedia kontaktide hulka lisab ja milliseid privaatsussätteid kasutab, on igaühe enda otsustada.[182] Autor on arvamusel, et töötajad peaksid ka ise esmajoones kaaluma, kas lubada tööandja esindaja oma kontaktide hulka või mitte. Konflikt võib seisneda selles, et tööandja omab sel juhul kahte väga vastandlikku rolli olles üheaegselt nii "sõber" kui ka tööandja. Samuti rõhutab autor, et iga sotsiaalmeediasse loodav postitus peaks sündima läbimõeldud ja kaalutletud otsuse tagajärjel, sest postituses olev informatsioon on kergesti kopeeritav, mistõttu on lihtne info konteksti muuta ja originaalpostitust seeläbi osavalt moonutada.

Paljudele tööandjatele ja personalitöötajatele on oluliseks abivahendiks saanud sotsiaalmeedia platvorm *LinkedIn*, kuhu inimesed on konto loonud töö leidmise või professionaalsete kontaktide loomise eesmärgil. Näiteks saab tööandja õigustatud huvi ja jälgimise eesmärgipärasust jaatada olukorras, kus tööandja jälgib selliste endiste töötajate *LinkedIn*i profiile, kelle suhtes kehtib konkurentsipiirang. Tööandja peab arvestama, et jälgimistegevus saab hõlmata üksnes konkurentsipiiranguga seotud endisi töötajaid.

[181] EIKo lahend 5493/72. 07.12.1976. Handyside vs. Ühendkuningriik
[182]G. Sibold. Millistel juhtudel võib tööandja uurida, mida sa sotsiaalmeedias teed? – Digigeenius. 19.10.2017. Arvutivõrgus: https://digi.geenius.ee/rubriik/uudis/millistel-juhtudel-voib-tooandja-uurida-mida-sa-sotsiaalmeedias-teed/, (16.03.2019).

3.7.2. Töötaja sotsiaalmeedia jälgimise põhimõtted

Nii nagu eelnevate jälgimisviiside puhul, kehtivad ka sotsiaalmeedia monitoorimisele kõik andmekaitse üldpõhimõtted.

Et sotsiaalmeedia kaudu kogutud isikuandmete töötlemine oleks läbipaistev, tuleb jälgitavaid töötajaid nende avaliku sotsiaalmeedia profiili jälgimisest teavitada.[183] Ehk kui tööandjal on õigustatud huvile vastav õiguslik alus töötaja sotsiaalmeedia jälgimiseks, peab ta neid eelnevalt teavitama. Kuna sotsiaalmeedia jälgimine peab olema seotud konkreetse juhtumiga, näiteks ohuga ärisaladuse avalikustamisele, ei saa pidada õiguspäraseks töötaja teavitamist töökorralduslike reeglite või käesoleva magistritöö peatükis 3.5. kirjeldatud eeskirja kaudu. Töötaja teavitamine tema sotsiaalmeedia jälgimisest peaks toimuma selle aluseks oleva asjaolu ilmnemisel. Kõikide ettevõtte töötajate teavitamine viitega, et nende sotsiaalmeedia kasutust võidake jälgida ärisaladuse hoidmise kohustuse rikkumise korral ei ole küll välistatud, ent autori hinnangul on praktikas otstarekam teavitada konkreetset töötajat konkreetse rikkumise korral.

Magistritöö autor leiab, et nii tööandjad kui ka töötajad peaksid suhtuma sotsiaalmeedia kasutamisesse ettevaatlikult. Töötajad võivad kogemata jagada konfidentsiaalset informatsiooni või oma postitustega kahjustada tööandja mainet. Seesuguse sotsiaalmeedia väärkasutuse riski maandamiseks võiks tööandja proportsionaalne meetmena kehtestada ettevõttesisese poliitika, mis sätestab suunised sotsiaalmeedia sobivaks ja sobimatuks kasutamiseks.[184] Loomulikult ei saa tööandja piirata töötajate sõna- ja väljendusvabadust, ent läbi vastavate juhiste saab tööandja töötajale teatavaks teha organisatsiooni jaoks olulised väärtused ning käitumisnormid. Tööandja ei saa kujundada ega muuta töötajate arusaama moraalist, nende poliitilisi vaateid või eelistusi. Tööandja peab mõistma, et sotsiaalmeedia platvormid on olulised kommunikatsioonivahendid, mille abil inimesed saavad kuuluda teatavatesse kogukondadesse, mis on omakorda oluline inimese identiteedi ja autonoomia jaoks. Sotsiaalmeedia aitab hoida ja luua sidemeid, võimaldab arvamuste

[183] Article 29 Data Protection Working party. Opinion 2/2017 on data processing at work. Lk 12. Arvutivõrgus: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169, (20.01.2019).
[184] R. Weihermann. Social media in the employment context and the nw EU General Data Protection regulation (GDPR). – Employment Germany blog. 27.06.2016. Arvutivõrgus: https://blogs.dlapiper.com/employmentgermany/2016/06/27/social-media-in-the-employment-context-and-the-new-eu-general-data-protection-regulation-gdpr/, (24.03.2019).

ja vaadete avaldamist laiale auditooriumile, kuuluda gruppidesse, kus inimesed jagavad sarnaseid vaateid jne.[185]

Isikuandmete kaitse üldmääruse valguses on töötaja sotsiaalmeedia kaudu kogutud isikuandmete töötlemise aluseks oleva õigustatud huvi tõendamine tööandja jaoks keeruline. Isikuandmete kaitse üldmäärusest tulenv nõue määratleda selge ja põhjendatud õigustatud huvi töötaja sotsiaalmeedia jälgimiseks, seab sellisele isikuandmete töötlemise võimalusele praktikas väga kitsad piirid. Seega kuna tööandjal ei ole reeglina lubatud töötaja sotsiaalmeedia kasutust jälgida, on töötaja isikuandmete kaitse tagatud. Autori hinnangul on tegemist eelkõige praktilise probleemiga, sest vaatamata andmekaitse üldmääruse seatud piirangutele, ilmneb mitmesugustest uuringutest ja meediaväljaannetest, et tööandjad jälgivad oma töötajate või tööle kandideerijate sotsiaalmeedia kasutust. Kuna sotsiaalmeedia kaudu kogutud isikuandmete töötlemine üha süveneb, on vaja teemat tõsiselt käsitleda ning selgitada tööandjatele sellise tegevuse lubatavust praktiliste näidete kaudu. Arvestades kõnealuse probleemi aktuaalsust, tuleks ka sotsiaalmeedia kaudu kogutud isikuandmete töötlemise valdkonda käsitleda AKI juhendis.

[185] V. Mantouvalou. I Lost my Job Over a Facebook Post: Was that Fair? – UK Labour Law. 21.06.2018. Arvutivõrgus: https://uklabourlawblog.com/2018/06/22/i-lost-my-job-over-a-facebook-post-was-that-fair/, (26.03.2019).

Kokkuvõte

Tänases ühiskonnas puudutab töötamine valdavat osa tööealisest elanikkonnast. Sellest tulenevalt ei saa eraelu puutumatust ja ootust privaatsusele seostada üksnes töötaja koduse keskkonnaga, vaid töötajal on õigustatud ootus sellele, et tema priaatsusesse liigselt ei sekkuta, ka töökohal. Privaatsus töökohal on peamiselt seotud informatsioonilise enesemääramisõigusega, ehk vabadusega otsustada, kas ja kui palju isik lubab enda kohta andmeid koguda, salvestada ja avaldada. Selline isikuandmete töötlemine mitmesuguste tehnoloogiliste vahendite või töötaja kasutuses olevate IKT vahendite kaudu võib juhtudel, mil andmekaitse reegleid ei järgita, riivata töötaja privaatsust. Kuna õigus privaatsusele ei ole absoluutne, siis on õigusliku aluse olemasolul selle piiramine töösuhtes lubatud. Magistritöö eesmärgiks oli leida vastus küsimusele, kas kiire tehnoloogilise arengu kontekstis on töötajate isikuandmete kaitse tagatud andmekaitse üldreeglite alusel või on vajalik tööõigusliku eriregulatsiooni kehtestamine.

Töötaja isikuandmete töötlemiseks peab olema täidetud vähemalt üks üldmääruse artiklis 6 sätestatud alustest. Töötaja isikuandmete töötlemine, mis väljendub teabe kogumises jälgimisseadmete või töötaja kasutuses olevate IKT vahendite kaudu, ei saa toimuda töötaja nõusoleku alusel. Töösuhte kontekstis pole töötajal reeglina võimalik vabatahtlikult nõusoleku andmisest keelduda või seda tagasi võtta. Kõige levinum õiguslik alus seesuguseks isikuandmete töötlemiseks on seotud tööandja õigustatud huviga. Kuna tegemist on väga laiaulatusliku põhimõttega, tuleb seda iga üksikjuhtumi puhul konkreetselt sisustada. Kui tööandja tugineb õigusliku aluse puhul õigustatud huvile, peab jälgimisseadmete kasutamise eesmärk olema õiguspärane ning valitud meetod või konkreetne tehnoloogia, millega töötajaid jälgitakse olema vajalik.

Lisaks õigusliku aluse olemasolule, peab töötajate isikuandmete töötlemine vastama üldmääruse artiklis 5 nimetatud isikuandmete töötlemise põhimõtetele. Tööõiguslik isikuandmete töötlemine peab olema proportsionaalne ärivajadustega, s.t. eesmärgiga, mida sellega soovitakse saavutada. Lisaks peab tööõiguslik isikuandmete töötlemine olema seaduslik, õiglane, läbipaistev, eesmärgipärane ja minimaalne. Andmed peavad töötlemise käigus olema vajadusel ajakohastatud ning lähtuda tuleb andmete säilitamise piirangu, usaldusväärsuse ja konfidentsiaalsuse põhimõtetest. Vaikimisi ja lõimunud andmekaitse põhimõtete kohaselt on oluline isikuandmete kaitsega arvestada koheselt ja võimalikke riske ennetada, mitte oodata nende realiseerumist.

Järgnevalt on välja toodud olulisimad järeldused, millal on töötaja isikuandmete töötlemine pilti, heli või signaali edastavate seadmete või tööandjale kuuluvate IKT vahendite kaudu õiguspärane ning millisel juhul ei ole tööandjal õigustatud huvi tuvastatav.

Õigustatud huvi kaamerate kasutamiseks peab olema selge ja ühemõtteline, ent tihtipeale põhjendavad tööandjad kaamerate kasutamist üldsõnalise viitega turvariskidele või rikkumistele, mis võivad ettevõttes aset leida. Kui tööandja põhjendab oma õigustatud huvi turvariskide vähendamisega, peab iga risk olema eraldiseisvalt ja detailselt kaardistatud – pelk hirm ei õigusta valvekaamerate kasutamist. Töötajate varjatud jälgimiseks või kaamerate paigaldamiseks ruumidesse, kus töötajal on täielik ootus privaatsusele (tualett- ja duširuumid jms) tööandjal õigustatud huvi ei ole. Samuti ei ole kaamerate kaudu kogutud andmete alusel lubatud kontrollida töötaja töö kvaliteeti ja hulka. Üldjuhul ei ole ka lubatav töötaja jälgimine terve tööpäeva vältel. Kaamerate kasutamine peab olema kooskõlas andmekaitse üldmäärusest tulenevate põhimõtetega. Töötaja isikuandmete kaitset mõjutab praktikas enim asjaolu, et töötajad üldjuhul ei kaalu proportsionaalsemaid ja vähem intensiivseid vahendeid, saavutamaks jälgimisele seatud eesmärke. Ka läbipaistvuse põhimõttega mittearvestamine on praktikas osutunud probleemiks, mistõttu võib töötaja isikuandmete kaitse ulatus vähendeda. Autori hinnangul on kaamerate kasutamisega seonduv võimalik mõistlikult ja efektiivselt lahendada AKI juhendi kaasajastamise ja tööandjate teadlikkuse tõstmisele suunatud tegevustega. Täiendava tööõigusliku eriregulatsiooni loomiseks ei näe autor käesoleval hetkel vajadust, sest isikuandmete kaitse üldmäärus seab kaamerate kasutamisele suhteliselt kitsad piirid. Lisaks ei ole autori hinnangul võimalik anda ammendavat loetelu olukordadest, kus kaamerate kasutamine on/ei ole lubatud – tööelu ei ole alati must-valge, mistõttu tuleb igas konkreetses situatsioonis kaaluda ja hinnata õigustatud huvi olemasolu.

Isikuandmete töötlemine võib väljenduda ka asukoha määramise seadmete ehk GPS seadmete kasutamises. Tööandjal on õigustatud huvi GPS seadmete kasutamiseks üldjuhul inimesi või kaupa vedavate sõidukite puhul. Siiski tuleb iga üksikjuhtumi puhul hinnata konteksti – isegi kui ettevõtte põhitegevuseks on inimeste või kauba vedu, võib õigustatud huvi GPS seadme paigaldamiseks olla küsitav olukorras, kus ettevõtte töökorraldus näeb ette, et töötajad organiseerivad oma reise iseseisvalt. Töösõiduki reaalajas jälgimiseks tööandjal õigustatud huvi reeglina ei ole, erandiks võib olla sõiduki vargus. Töötaja produktiivsuse kontrollimiseks GPS seadmetega tööandjal õigustatud huvi ei ole. Autori hinnangul on GPS seadmete kasutamise õiguslik alus pigem piiratud, olles seotud tihedalt ettevõtte tegevusvaldkonnaga. Vaatamata sellele, et tööandja õigustatud huvi mõiste on lai, on sellele tuginemine GPS seadmete kasutamisel suhteliselt kitsas. Seetõttu julgeb

autor väita, et ka töötaja õigus isikuandmete kaitsele on hästi tagatud. Praktilise probleemina toob autor välja, et isikuandmete kaitse ulatus GPS seadmete kasutamisel sõltub paljugi sellest, kui hästi tööandja isikuandmete kaitse üldmääruses kehtestatud põhimõtteid järgib.

Raadiosagedustuvastusel põhinev identifitseerimistehnoloogia ehk RFID on kasutuses mitmesugustes kiipkaardi lugemise süsteemides, töökeskkonnas levinumaks kasutusviisiks on näiteks uksekaardi lugemise süsteem. Üldjuhul ei ole võimalik tuvastada tööandja õigustatud huvi töötaja tööle tuleku ja lahkumise, töökohalt eemaloleku aja või korruste vahel liikumise jälgimiseks. Erandiks on olukord, kus tööaja arvestus toimub kiipkaardi registreerimise põhiselt või kui töökeskkonnas on kõrgendatud turvarisk, näiteks tehas, vangla jms. Eeldusel, et tööandjal on õigustatud huvi RFID seadme abil kogutud andmete töötlemiseks, peavad lisaks olema täidetud kõik andmekaitse üldpõhimõtted. RFID tehnoloogial põhinevate seadmete kaudu isikuandmete töötlemine võib autori arvates kahtlemata ohustada töötaja õigust isikuandmete kaitsele ja seeläbi privaatsusele, kuid arvestades isikuandmete kaitse üldmäärusest tulenevaid nõudeid on praktikas kõnealuste seadmete kaudu isikuandmete töötlemine lubatud üksnes äärmiselt piiratud olukordades. Sellele tugindedes on autor seisukohal, et kuna andmekaitse üldreeglid ei võimalda üldjuhul töötajaid RFID tehnoloogial põhinevate seadmete kaudu jälgida, on nende isikuandmete kaitse tagatud piisavalt. Tõenäoliselt jääb praktikas puudu tööandjate teadlikkusest kõnealuse tehnoloogia rakendamisel ja selle kaudu kogutud andmete töötlemisel, mistõttu on oluline tegeleda tööandjate teadlikkuse kasvatamisega.

Lisaks RFID tehnoloogiale leiavad üha enam kasutust isikutuvastussüsteemid, mis põhinevad töötaja biomeetrial. Töötaja biomeetrilised isikuandmed kujutavad endast eriliiki isikuandmeid, mille töötlemisõigus on väga piiratud. Üldjuhul ei ole ka tööandjal töösuhte kontekstis õigustatud huvi töötaja biomeetriliste isikuandmete töötlemiseks. Eriliiki isikuandmete töötlemist on lubatud liikmesriikidel täiendavalt reguleerida. Autori hinnangul on tänane eriliiki isikuandmete töötlemise regulatsioon võrdlemisi üldsõnaline, eelkõige just töötaja jälgimise ja kontrollimisega seonduvas. Arvestades, et tööandjad rakendavad üha enam töötaja biomeetrilisi andmeid töötlevaid isikutuvastusseadmeid, võib ühel hetkel eriliiki isikuandmete regulatsiooni vajaduse järele muutuda päevakohaseks. Kuna aga tänased Eesti tööandjad rakendavad töötaja biomeetrial põhinevaid isikutuvastussüsteeme vähe ning eriliiki isikuandmete töötlemist puudutav regulatsioon kaitseb selgelt andmesubjekti ehk töötaja huve, siis on töötajate isikuandmete kaitse tagatud üldmäärusest tuleneva range regulatsiooniga.

Suhteliselt uudse ja vähelevinud võimalusena analüüsis autor ka isikuandmete töötlemist, mis väljendub töötajate kiibistamises. Vastupidiselt teistele isikuandmete töötlemise võimalustele saab töötajate kiibistamine toimuda üksnes töötaja vabatahtlikul, konkreetsel, teadlikul, ühemõttelisel ja selgesõnalisel nõusolekul. Õigustatud huvi kiibi paigaldamiseks töötaja naha alla tööandjal mingil juhul olla ei saa. Edasine kiibi kasutamisega seotud isikuandmete töötlemine, näiteks informatsiooni salvestamine, võib toimuda üksnes siis, kui tööandjal on selleks õigustatud huvi. Käesoleval hetkel võib tööandja õigustatud huvi nahaaluse kiibi kaudu kogutud andmete töötlemiseks olla raskendatud, sest sama eermärgi saavutamiseks on olemas mitmeid "klassikalisi" alternatiive.

Töötaja IKT vahendite jälgimiseks peab tööandjal olema õigustatud huvi. Tööandja õigustatud huvi telefonikõnede salvestamiseks või kõnede eristuse analüüsimiseks on pigem keeruline põhjendada ning isegi kui see õnnestub, on üldjuhul olemas proportsionaalsemaid lahendusi jälgimisele seatud eesmärgi saavutamiseks.

Isikuandmete töötlemine, mis seisneb arvutikasutuse jälgimises, võib väljenduda mitmel eri viisil: töötaja arvutikasutuse, s.t. arvuti ekraanil toimuva jälgimine; töötaja külastatud interneti lehekülgede ajaloo jälgimine ning tööandja domeeniga e-posti jälgimine. Kõigi nimetatud jälgimisviiside rakendamiseks peab tööandjal olema selge õigustatud huvi. Üldjuhul ei ole tööandjal õigustatud huvi ekraani jälgivate seadmete, klahvilogerite ning nuhkvara kasutamiseks. Arvutikasutuse jälgimist võib tööandja põhjendada infoturbe tagamisega, kuid ka sel juhul peavad konkreetsed riskid olema selgelt väljendatud. Praktikas on töötaja arvuti kaudu kogutud isikuandmete töötlemine vaidlusi tekitanud eelkõige kaugtöötajate puhul. Vaatamata tööandja piiratud kontrollile kaugtöötaja üle, ei ole üldjuhul ka siis töötaja arvutile jälgimist võimaldavate seadmete paigaldamine või –pilveteenuste kasutamine lubatud.

Internetikasutuse jälgimise õiguslik alus on üldjuhul seotud võrgu kaitsmise vajadusega. Isikuandmete töötlemine internetikasutuse jälgimise teel on seega seotud eesmärgiga tagada võrgu ja selles hoitavate töötajate- ja klentide andmete, ärisaladuse ja intellektuaalse omandi kaitse. Ühdjuhul ei ole proportsionaalne kogu internetikasutuse jälgimine ning kui internet väärkasutust saab tuvastada muude vahenditega, ei ole üldine internetikasutuse jälgimine lubatud. Käesoleval hetkel on võimalik töötaja isikuaandmete töötlemist vältida ja saavutada õigustatud huvile vastav eesmärk selliste tehnoloogiliste vahendite kasutusele võtmisega nagu veebifiltrid, tulemüürid, viirusetõrje tarkvara jms.

Tööandja õigustatud huvi töötaja e-psti jälgimise ja e-kirjade lugemise teel kogutud andmete töötlemiseks võib olla seotud arvutisüüsteemide tõrgeteta ja turvalise töökorra tagamisega või vajadusega lugeda olulisi kirju töötaja eemaloleku ajal. Ka tööalaste e-kirjade lugemine on õiguspärane ega riiva töötaja privaatsust. Töötaja isiklike kirjade, s.h. nende liiklusandmete töötlemiseks tööandjal üldjuhul õigustatud huvi ei ole. Harvadel juhtudel ei ole siiski välistatud ka töötaja isiklike kirjade jälgimine, näiteks konfidentsiaalsuskohustuse, kokurentsikeelu rikkumise või tööstusspionaaži korral.

Vaatamata faktile, et võimalusi töötaja arvuti- interneti- ja e-posti jälgimiseks on seoses tehnoloogia arenguga tekkinud väga palju, nii tarkvaraliste lahendustena kui pilveteenustena, on nende kasutamine üsna piiratud. Olenemata tehnoloogia uudsusest või intensiivsusest, allub nende kasutamine ühtsele isikuandmete kaitse regulatsioonile. Üksnes asjaolu, et potentsiaalsed tehnoloogilised võimalused töötaja jälgimiseks on suurenenud, ei tähenda seda, et nende kasutamine on lubatud. IKT vahendite kaudu kogutud isikuandmete töötlemist ei ole autori hinnangul vajalik reguleerida seaduse tasandil. Sisustades tööandja õigustatud huvi IKT vahendite jälgimiseks erinevate näidete kaudu, on autor seisukohal, et õigusliku aluse leidmine on keeruline, mistõttu on risk töötaja isikuandmete kaitse riiveks väike.

Kõikide väljatoodud IKT vahendite kasutamise kaudu kogutud isikuandmete töötlemine peab olema kooskõlas andmekaitse üldpõhimõtetega. Autori hinnangul võib töötaja isikuandmete kaitset riivata eelkõige läbipaistvuse põhimõtte mittejärgimine ehk ebapiisav teavitamine. Kõige mõistlikuma lahendusena näeb autor tööandjale kuuluvate IKT vahendite kasutamise ja nende kaudu kogutud isikuandmete töötlemise reeglistiku koostamist. Eeskiri peaks olema piisavalt detailne ja sisaldama teavet selle kohta, kas tööandjale kuuluvaid IKT vahendeid on lubatud kasutada isiklikul eesmärgil; milliste IKT vahendite kaudu kogutud andmeid tööandja töötleb; millised on konkreetsed jälgimisviisid; kuidas on tagatud kogutud andmete turvalisus; kellel on volitatud juurdepääs kogutud andmetele; millised on andmesubjekti õigused jms. Kuna suur osa vaidlustest on seotud töötajate ebapiisava teavitamisega, siis lisaks tule- ja tööohutuse ning töötervishoiunõuete tutvustamise nõudele võiks tööandja jaoks kohustulikuks muuta ka tööandjale kuuluvate IKT vahendite kasutamise eeskirja kehtestamise. Siseriikliku õigusega on võimalik töötaja IKT vahendite kasutamise eeskirja nõue mõistlikult ja efektiivselt reguleerida. See muudaks ühelt poolt tööandjate tegevuse palju läbipaistvamaks ning töötajate isikuandmete kaitse oleks paremini tagatud. Vastav regulatsioon võiks sisalduda autori hinnangul töölepinguseaduses tööandja kohustuste all.

Lisaks IKT vahendite jälgimisele võib isikuandmete töötlemine seisneda töötaja sotsiaalmeedia jälgimises. Tööandjal peab olema töötaja sotsiaalmeedia kaudu isikuandmete kogumiseks õigustatud huvi ning ainuüksi asjaolu, et töötaja sotsiaalmeedia profiil on avalik, ei anna tööandjale õigust sealseid andmeid enda huvides töödelda. Lisaks tööandja õigustatud huvile peab andmetöötlusel olema selge eesmärk. Jälgimine on õigus- ja eesmärgipärane näiteks olukorras, kus tööandja tähelepanu juhitakse asjaolule, et tema töötaja avaldab sotsiaalmeedias ärisaladusega seotud postitusi. Kindlasti ei ole tööandjal õigustatud huvi töötaja sotsiaalmeedia jälgimiseks, eesmärgiga leida ebasobivat sisu või kommentaare. Samuti ei saa tööandjal olla õigustatud huvile vastavat õiguslikku alust nõuda, et töötaja lisaks tööandja oma isiklikult sotsiaalmeedia kontolt sõbraks. Isikuandmete kaitse üldmääruse valguses on töötaja sotsiaalmeedia kaudu kogutud isikuandmete töötlemise aluseks oleva õigustatud huvi tõendamine vähetõenäoline. Kuna tööandjal ei ole reeglina lubatud töötaja sotsiaalmeedia kasutust jälgida, on töötaja isikuandmete kaitse piisavalt tagatud. Autori hinnangul on tegemist praktilise probleemiga, sest vaatamata andmekaitse üldmääruse seatud piirangutele, ilmneb mitmesugustest uuringutest ja meediaväljaannetest, et tööandjad jälgivad oma töötajate sotsiaalmeedia kasutust.

Summary

As most of the working-age society spends a major part of their life at work, working plays a significant role in people's lives. Because of that, privacy cannot be solely attributed to the worker's home environment. As a matter of fact, every employee has an expectation that their workplace privacy will not be interfered with either. Privacy in the workplace is mainly related to right to informational self-determination, meaning that the employee has the power to decide how much information related to them is collected, stored or published. Processing personal data by using various technological resources or ICT tools which are available to the employee, may infringe their privacy. Due to privacy not being an absolute fundamental right, in case of a lawful basis the limitation of privacy in employment relationship is allowed.

The aim of the master's thesis is to find out whether the general data protection law guarantees the protection of employee's personal data in the context of rapid technological development or there is a need to introduce a new labor law legislation. The author points out that the purpose of data processing rules is not narrowly related to personal data, but rather to ensure the protection of the fundamental rights and to prevent possible violation.

To achieve the aim, author of this master thesis analyzes different data processing methods, such as using the surveillance cameras at work environment; tracking the location by using the Global Positioning Systems (GPS); using Radio Frequency Identification (RFID) attendance systems that enables to track employees; using biometric identification systems; implanting microchips to employees. As well, author illustrates the data processing which is expressed through monitoring the use of the ICT tools, such as phone and computer (including internet and email monitoring) and through monitoring the employee's social media accounts.

To process data of an employee lawfully at least one General Data Protection Regulation (GDPR) lawful basis of Article 6 has to be covered. The lawful basis for processing personal data by means of monitoring equipment or using ICT tools cannot be the consent of an employee. Typically, in the context of employment relationship, the employee may not voluntarily refuse or withdraw consent. The most common lawful basis for processing personal data is associated with a legitimate interest of the employer. Since this is a very broad principle, it has to be variously interpreted depending on the case. When the employer relies on the legitimate interest as the legal basis, the

use of the monitoring equipment must be justified and the chosen method or a specific technology has to be in compliance with necessity.

In addition to lawful basis, the processing of personal data of employees must comply with the principles of data processing referred to in Article 5 of the GDPR. The personal data processing of an employee must be proportional to the business needs of an employer and employee's fundamental rights. Furthermore, the processing of personal data has to be lawful, fair, transparent and accurate. Also, such principles relating to processing of personal data as purpose limitation, data minimation, storage limitation, integrity and confidentiality must be followed. According to the principles of data protection by design and by default, it is important to take into account and prevent the potential risks of the protection of personal data rather than waiting for them to take place.

The author of the master thesis hereby points out the most important deductions when the data processing by means of using image, sound or signal transmitting devices or monitoring ICT tools is lawful and points out legal and practical problems that may affect the employee's right to data protection. According to the GDPR a legitimate interest for using cameras must be clear and unambiguous, but in reality employers often justify the use of surveillance cameras with a general reference to reduce security risks. If the employer justifies the legitimate interest by aim to reduce security risks, each specific risk must be individually and accurately stated – inexplicable fear alone does not fulfill the legal basis. In general employer does not have legitimate interest for using hidden surveillance cameras and certainly it is not allowed to install surveillance systems into area where employees have absolute expectation of privacy, such as restrooms, praying rooms etc. In addition, it is not lawful to use the data, gathered by surveillance camera, to check the productivity of the employees. In general employer does not have legitimate interest to monitor their employees during entire workday. The use and installation of surveillance cameras must be in compliance with the data protection principles stated in the GDPR. In everyday working life, employee's right to data protection might be affected by the fact, that employers often do not even consider to implement more proportionate and less intensive means, to achieve the aim. Furthermore, employers often do not follow the transparency principle, which may also affect the scope of data protection of employees. Based on the fact that employers use surveillance systems without hesitation and do not inform employees properly (to fulfill the transparency principle), the author of this thesis is sure, that problems related to the unlawful use of cameras can be solved reasonably by updating the guidelines of Estonian Data Protection Inspectorate and by informing and training

employers. Despite the fact that employers do not consider less intensive means, the author finds it difficult to ensure by law or collective agreements the sample list of situations where the use of surveillance cameras is lawful. In reality, the legitimate interest of an employer is always up to discretion.

Data processing may also take place by using the Global Positioning Systems (GPS). In general, it is confirmed that employer has a legitimate interest for using GPS devices when the sphere of company is related with vehicles carrying people or goods. Although it is important to take into account the context on specific case – even if the main sphere of the company is the transportation, a legitimate interest for data processing by use of GPS device may be questionable. For example in case, when the employees are authorized to organize their journeys independently. Mostly employers do not have legitimate interest to monitor the vehicle in real-lime, unless it is necessary to detect possible theft. As well, it is not lawful to use GPS devices in aim to check productivity of employees. According to the opinion of the author of this thesis, there is no specific need to draw up detailed regulation for using the GPS devices. Most important principle to follow is that GPS devices are only intended to monitor the vehicle and it is not allowed to use them in aim to monitor employees and their behavior.

RFID based technology is used in a variety of smart card readers. In a workplace environment the technology is mostly used in the attendance systems. Usually, there is no justifiable reason for an employer to monitor the movements of the employees. There are exceptions such as when the RFID attendance system is used for time clocking or in a facility that uses the technology for security reasons, like factories, prison etc. If the employer has a rightful reason for processing the collected data, then the general principles of data protection also must be fulfilled.

In addition to RFID technology, the biometric identification systems are becoming widly in use. The rights for processing biometric personal data of an employee are very restricted. Essentially, in the context of employment relationship there is no justified interest for the employer to process personal biometric data. Member states are allowed to further regulate the processing of delicate personal data. The author is on the opinion that the control over processing of delicate personal data is relatively general, especially in terms of employee monitoring and control. Since employers are progressively implementing biometric identification devices, there might be at one point a need for regulation that would regulate the processing of delicate personal data. But currently, as

Estonian employers rarely use biometric identification systems, the protection of delicate personal data is guaranteed by the strict general regulation of personal data protection.

The author has also analyzed a less significant and relatively novel employee monitoring option, which consists of injecting microchip implants into employees. Unlike other data processing options, injecting microchip implants can only be done on an employee who has given voluntary, specific, informed, unambiguous and explicit consent. The employer cannot rely on a legitimate interest for implementing microchips to it's employees. Further processing of the data collected from the microchip, such as information recording can only be done if the employer has legitimate interest in doing so. The author states, that currently, it is rather difficult for the employer to have a legitimate interest in data collection using microchip, since there are several alternatives for reaching the same goal.

To process data that is collected through monitoring the use of ICT tools, employers must prove their legitimate interest. It is rather difficult to justify the need to record telephone calls or analyze the distinction between them, however, even if the if the employer succeeds to justify the legitimate interest, there are generally other comparable solutions for achieving the objective that was initially set for the data processing. There are many different types of personal data, which can be gathered from monitoring computer activity, such as: employee use of computer, tracking of browser history, tracking email accounts that are on the employer's domain. The employer must have a legitimate interest for implementing all of the methods above. As a rule, the employer has no justifiable interest in using screen-monitoring devices, key loggers or spyware. The monitoring can be justified if it is done for ensuring information security, however the potential security risks should be clearly stated. In practice, the disputes over personal data gathering have been mainly related to teleworking. Regardless of the limited control over the teleworker, it is generally not allowed to install a monitoring software or cloud services on the device of the employee. The lawful basis for monitoring the use of the internet is usually related to protecting the network. Processing personal data by monitoring the use of the internet is linked to protecting the network and the data related to the clients, business secrets and intellectual property. Generally, it is not reasonable to monitor the activity of the entire internet and if the abuse of the internet can be detected by other means, such as firewalls or content filters, then the monitoring of the internet is not lawful. The author finds, that it is possible to achieve an aim that was initially set for website use monitoring without processing personal data of the employees by introducing technological tools such as web filters, firewalls, antivirus softwares etc.

An employer may have a legitimate interest to process personal data collected by monitoring and reading e-mails, if it is related to the failure of the computer systems, ensuring data protection or a need to review important messages during the absence of the employee. Reading work emails is legitimate and does not violate the privacy of an employee. However, an employer does not have a justifiable interest to process or read personal letters of an employee. On rare occasions, it can be justifiable if it is related to the breach of confidentiality, violation of the coercive ban or industrial espionage.

The processing of personal data collected through the use of ICT tools must comply with the general principles of the data protection. According to the author, the protection of the personal data of the employee can be violated, in particular, by failing to follow the principle of transparency. The author believes that the most rational solution would be to regulate the use of ICT tools provided by the employer and the ways they are processed. The regulation should be sufficiently detailed and include information about the use of employer's ICT tools for personal purposes; which data gathered by the ICT tools are processed by the employer; what are the specific monitoring methods; how is the security of the collected data ensured; who has the authorized access to the collected data; which rights does the data subject have etc. Due to the fact, that a large number of disputes are related to providing insufficient information to the employees, it should be obligatory for the employer to introduce the rules on the use of ICT tools belonging to the employer, in addition to the requirements of fire, safety and occupational health. The activities of the employers are not always transparent, since they are not obliged to impose rules for processing personal data collected through ICT tools. Under member state law it is possible to regulate in a reasonable and effective way that employer has to draw up and disclose guidelines for use of ICT tools at work. This would increase the transparency of the employers and also guarantee the protection of personal data of employees. Author believes that corresponding regulation should be included in the Employment Contracts Act under the employer's obligations chapter.

In addition to monitoring ICT tools, the processing of personal data may involve monitoring the employee's social media. The employer must have a clear legitimate interest in collecting personal data of an employee through the social media and the mere fact that the employee's social media profile is public does not give the employer the right to process the data there for their own benefit. In addition to the interest of the employer, the purpose of the data processing must be clear as well.

Monitoring employee's social media can be lawful and justifiable in such situations where the attention of the employer is drawn to the fact that the employee publishes business secrets in the social media. There is no legitimate interest of an employer to monitor employee's social media with a purpose to find inappropriate content or comments. Additionally, the employer does not have a rightful interest in claiming that the employee should be their friend on his / her private social media account.

By analyzing different ways of data processing, the author of the Master's thesis concludes that in case where the processing personal data through methods that are outlined above has clear legitimate interest and the principles of the GDPS art.5 are clearly followed, the protection of the employee's personal data is secured. Despite the fact, that GDPR provisions are quite general and abstract, it is rather difficult to justify the use monitoring systems at work environment. The fact that the lawful base for processing data through technological monitoring systems is fairly narrow and limited, ensures that data protection and right to privacy at work are secured.

Kasutatud lühendid

AKI – Andmekaitse Inspektsioon

AKI juhis - Andmekaitse Inspektsiooni abistav juhendmaterjal „Isikuandmete töötlemine töösuhetes”

Andmekaitseinspektor – Euroopa andmekaitseinspektor

EIK – Euroopa Inimõiguste kohus

GPS seade – asukoha määramise (inglise keeles *Global positioning system)* seade

IKS – isikuandmete kaitse seadus

MTA – Maksu- ja tolliamet

NFC – kontaktivaba lähivälja identifitseerimise tehnoloogia (inglise keeles *Near Field Communication*)

RFID - raadiosagedustuvastusel põhinev identifitseerimistehnoloogia (inglise keeles *Radio-frequency identification)*

TLS – töölepingu seadus

Üldmäärus - Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679, 27. Aprill 2016, Füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). – (ELT L 119, 04.05.2016).

Kasutatud kirjandus

1. Advokaadibüroo Legal ICT Amsterdam. Fact sheet privacy and monitoring at work under the GDPR. Arvutivõrgus: https://legalict.com/content/uploads/sites/2/2017/07/Fact-sheet-Privacy-and-monitoring-at-work-under-the-GDPR-Legal-ICT.pdf. (22.02.2019).
2. Advokaadibüroo Taylor & Wessing. Employee monitoring update. 03.2017. - Global data hub. Arvutivõrgus: https://globaldatahub.taylorwessing.com/article/employee-monitoring-update (11.02.2019).
3. AMA/ePolicy Institute research. Electronic monitoring and surveillance survey. 2007. Arvutivõrgus: http://www.plattgroupllc.com/jun08/2007ElectronicMonitoringSurveillanceSurvey.pdf (16.03.2019).
4. Andmekaitseinspetsiooni abistav juhendmaterjal. Isikuandmete töötlemine töösuhtes. Tallinn. 24.01.2011. Arvutivõrgus: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikuandmed%20t%C3%B6%C3%B6suhetes%20juhendmaterjal26%2005%202014_0.pdf. (10.01.2019).
5. Andmekaitse inspektsioon. Töötajate arvutikasutuse privaatsus. Arvutivõrgus: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/T%C3%B6%C3%B6tajate%20arvutikasutuse%20privaatsus_.pdf (10.01.2019).
6. Andmekaitse inspektsioon. Telefonikõnede salvestamise lubatavuse juhend 25.09.2012. Arvutivõrgus: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Telefonik%C3%B5nede%20salvestamise%20lubatavuse%20juhend.pdf. (22.03.2019).
7. Andmekaitse inspektsioon. Spioon töötaja arvutis. 13.02.2013. Arvutivõrgus: https://www.aki.ee/et/uudised/meediakajastus/spioon-tootaja-arvutis. (15.03.2019).
8. Andmekaitse inspektsioon. Kas tööandjal on õigus lugeda minu e-kirju? 31.05.2013. Arvutivõrgus: https://www.aki.ee/et/kas-tooandjal-oigus-lugeda-minu-e-kirju (22.02.2019).
9. Andmekaitse inspektsioon. Juhis personalitöötajale: Isikuandmed töösuhtes. 06.06.2011. Arvutivõrgus:

https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikuandmed%20t%C3%B6%C3%B6suhetes%20juhis%20personalit%C3%B6%C3%B6tajale.pdf. (22.02.2019).

10. Andmekaitse inspektsioon. Tööandja ei tohi töötajaid varjatult kaamerate abil ja telefonikõnede salvestamisega jälgida. 09.02.2015. Arvutivõrgus: https://www.aki.ee/et/tooandja-ei-tohi-tootajaid-varjatult-kaamerate-abil-ja-telefonikonede-salvestamisega-jalgida (26.02.2019).
11. Article 29 Data Protection Working Party. Working document on the surveillance of electronic communications in the workplace, 29.05.2002. Arvutivõrgus: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdf (14.02.2019).
12. Article 29 Data protection Working Party. Opinion 2/2017 on data processing at work. Arvutivõrgus: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169. (20.01.2019).
13. Article 29 Data Protection Working Party. Opinion 8/2001 on the processing of personal data in the employment context. Arvutivõrgus. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf (20.02.2019).
14. Article 29 Data protection Working Party. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7(f) of Directive 95/46/EC. 14.11.2014. Arvutivõrgus: https://ec.europa.eu/justice/article-29/press-material/public-consultation/notion-legitimate-interests/files/20141126_overview_relating_to_consultation_on_opinion_legitimate_interest_.pdf (14.03.2019).
15. Article 29 Data protection working party. Opinion 13/2011 on Geolocation services on smart mobile devices. 16.05.2011. Arvutivõrgus: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf (15.03.2019).
16. Bevitt, A. Employee „consent“ under the GDPR. – Thomson & Reuters. 16.08.2017. Arvutivõrgus: http://in-houseblog.practicallaw.com/employee-consent-under-the-gdpr/ (20.02.2019).
17. Birnstill, P. jt. Privacy-preserving surveillance: an interdisciplinary approach. – International Data Privacy Law. Oxford academic. 04/2015. Arvutivõrgus: https://www.researchgate.net/publication/282349311_Privacy-preserving_surveillance_an_interdisciplinary_approach (17.03.2019).

18. Chinese workers hold managers hostage after toilet break changes. – The Guardian. 22.01.2013. Arvutivõrgus: https://www.theguardian.com/world/2013/jan/22/chinese-managers-hostage-toilet-breaks (14.03.2019).
19. Ciccoletti, C. A. The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring. - American Business Law journal. Vol 48. Issue 2. 2011
20. Dietrich, G. Social media polocy: When are Your owm opinions not okay? 24.09.2013. Arvutivõrgus: https://spinsucks.com/social-media/social-media-policy-when-are-your-own-opinions-not-okay/ (29.03.2019).
21. EDRi – Protecting digital freedom. Deutsche Telecom under investigation for spying its employees - 14.06.2008.Arvutivõrgus: https://edri.org/edrigramnumber6-11deutsche-telekom-spying-employees/ (15.03.2019).
22. Euroopa komisjon. Kas mu tööandja saab mind sundida nõustuma minu isikuandmete kasutamisega? 2018. Arvutivõrgus: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/can-my-employer-require-me-give-my-consent-use-my-personal-data_et. (15.02.2019).
23. Euroopa parlament. Tööhõive ja sotsiaalvaldkonna komisjon. The Use of Chip Implants for workers. Lk. 20. Arvutivõrgus: http://www.europarl.europa.eu/RegData/etudes/STUD/2018/614209/IPOL_STU(2018)614209_EN.pdf. (17.03.2019)
24. European data protection supervisor. The EDPS video-surveillance guidelines. 17.03.2010. Arvutivõrgus: https://edps.europa.eu/sites/edp/files/publication/10-03-17_video-surveillance_guidelines_en.pdf (27.02.2019).
25. Euroopa andmekaitse inspektor. Access to e-communications data when an employee is absent. 2017. Arvutivõrgus: https://edps.europa.eu/data-protection/data-protection/reference-library/access-ecommunications-data-when-employee-absent_en (07.03.2019).
26. Employee monitoring technologies: gone too far? – GDPR informer. 12/2018. Arvutivõrgus: https://gdprinformer.com/gdpr-articles/employee-monitoring-gone-far (16.03.2019).
27. Firfiray, S Microchip implants are threating worker's rights. 26.11.2018. Arvutivõrgus: https://phys.org/news/2018-11-microchip-implants-threatening-workers-rights.html, (17.03.2019).

28. Hartshorn, A. Transparency and consent. Why data protection legislation is getting stricter? – Real business. 04/2017 Arvutivõrgus: https://realbusiness.co.uk/data-protection-legislation-getting-stricter/. (19.02.2019).
29. Heywood, D. Lawful processing og HR data under the GDPR. – Global data hub. 03.2017. Arvutivõrgus: https://globaldatahub.taylorwessing.com/article/lawful-processing-of-hr-data-under-the-gdpr (20.02.2019).
30. Ilus, T. Andmesubjekti osaluse põhimõte Euroopa Nõukogu konventsioonide ning Euroopa Inimõiguste kohtu lahendite valguses. Juridica VIII/2005
31. Iro, M. Isikuandmed töösuhtes. Mida peab teadma uuest isikuanmdete kaitse üldmäärusest? – Personaliuudised. 18.05.2018. Arvutivõrgus: https://www.personaliuudised.ee/uudised/2018/04/18/isikuandmed-toosuhetes-mida-peab-teadma-uuest-isikuandmete-kaitse-uldmaarusest. (27.04.2019).
32. Irwin, L. EU regulators to curb employers searching social media. – IT governance European blog. 14.08.2017. Arvutivõrgus: https://www.itgovernance.eu/blog/en/eu-regulators-to-curb-employers-searching-social-media (25.03.2019).
33. Jalakas, M Andmekaitse uue määruse valguses. – IT ja andmekaitse – Mart Jalakas. Arvutivõrgus: https://mtjholding.ee/andmekaitse-uue-maaruse-valguses/ (20.03.2019).
34. Joncour, L. Ten things to know about labour and employment law in France. – Advokaadibüroo Norton Rose Fulbrright. 03.2017. Arvutivõrgus: https://www.nortonrosefulbright.com/en/knowledge/publications/f1d8c939/ten-things-to-know-about-labour-and-employment-law-in-france (11.02.1019).
35. Johnson, M. Employee Use of IT. – Rocket lawyer. Arvutivõrgus: https://www.rocketlawyer.co.uk/article/employee-use-of-it.rl (11.02.2019).
36. Jõks, A. Eraelu kaitse töösuhtes – väljakutsed tööandjale. 27.01.2010. Arvutivõrgus: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Allar%20J%C3%B5ks%202010.pdf (07.03.2019).
37. Kanarbik, L. Võtmed naha alla ehk miks Ülemiste linnaku töötajad end kiibistada lasevad. – Eesti Päevaleht. 11.10.2018. Arvutivõrgus. https://epl.delfi.ee/eesti/votmed-naha-all-ehk-miks-ulemiste-linnaku-tootajad-end-kiibistada-lasevad?id=83959080, (17.03.2019).
38. Kim, S. Company Limits Worker Bathroom Use to 6 Minutes a day, Union claims. – ABC News. 16.07.2014. Arvutivõrgus: https://abcnews.go.com/Business/regulate-bathroom-work/story?id=24581940 (14.03.2019).

39. Kirst, O. Sõnumisaladuse kaitse tööandja sidevahendi kasutamisel. – Juridica IV/2012.
40. Kook, K. Tallinna ettevõte kiibistab töötajaid. – Digigeenius. 18.04.2017. Arvutivõrgus: https://digi.geenius.ee/rubriik/uudis/tallinna-ettevote-kiibistab-enda-tootajaid/ (17.03.2019)
41. Kookmaa, T. Kaks soovitust andmekaitse trahvide vältimiseks. – Äripäev.19.02.2019. Arvutivõrgus: https://www.aripaev.ee/uudised/2019/02/19/kaks-soovitust-andmekaitse-trahvi-valtimiseks (20.02.2019).
42. Käärats, E. jt. Töölepingu seadus. Selgitused töölepingu seaduse juurde. – Juura 2013.
43. Lane, M. Monitoring employee emails in the UK, France, Singapore and Germany. CMS Law now. 24.02.2016. Arvutivõrgus: http://www.cms-lawnow.com/ealerts/2016/02/monitoring-employee-emails-in-the-uk-france-singapore-and-germany?cc_lang=en (20.03.2019).
44. Lampe, C. Social media and the workplace. – Pew Reseach Center, Internet & Technology. 22.06.2017. Arvutivõrgus: https://www.pewinternet.org/2016/06/22/social-media-and-the-workplace/ (14.03.2019).
45. Lasprogata, G. jt. Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada. – Stanford Technology Law Review. 2004/04
46. Larson, S. Beyond passwords. Cpompanies use fingerprints and digital behaviour to ID employees. – CNN Business. 18.02.2018. Arvutivõrgus: https://money.cnn.com/2018/03/18/technology/biometrics-workplace/index.html (14.03.2019).
47. Liiv, M. Miidla-Vanatalu. M. Kaugtöö ja paindliku töösuhte probleemid. – Personaliuudised. 16.05.2017. Arvutivõrgus: https://www.personaliuudised.ee/uudised/2017/05/16/kaugtoo-ja-paindliku-toosuhte-probleemid (28.03.2019).
48. Lohr, S. Unblinking Eyes Track Employees. – New York Times. 21.06.2014. Arvutivõrgus: https://www.nytimes.com/2014/06/22/technology/workplace-surveillance-sees-good-and-bad.html?action=click&module=RelatedCoverage&pgtype=Article&region=Footer (14.03.2019).

49. Lugaresi, N. Electronic Privacy at the workplace: Transparency and Responsibility. – International review of Law, Computers & Technology 24/2010.
50. Lyon, D. Surveillance Studies. An overview. Oxford. Polity Press. 2007
51. Madise, Ü. jt. Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. 4. täiend. Vlj. Tallinn: Juura, 2017
52. Maruste, R. Konstitutsionalism ning põhiõiguste ja vabaduste kaitse. Tallinn: Juura 2004
53. Männiko, M. Õigus privaatsusele ja andmekaitse. Tallinn. Juura 2011
54. Mantouvalou, V. I Lost mt Job Over a Facebook Post: Was that Fair? – UK Labour Law. 21.06.2018. Arvutivõrgus: https://uklabourlawblog.com/2018/06/22/i-lost-my-job-over-a-facebook-post-was-that-fair/ (26.03.2019).
55. Nõmper, A. Michelson, K. Kas tööandja saab sidevahendite kasutamist kontrollida? 23.03.2010. Arvutivõrgus: https://majandus24.postimees.ee/240487/kas-tooandja-saab-sidevahendite-kasutamist-kontrollida (11.02.2019).
56. Ojaver, A. Valvekaamerate kasutamine töökohtadel ja kaubanduspindadel – kontrollide sõnaline kokkuvõte. 24.10.2010. Arvutivõrgus: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Valvekaamerate%20seire.pdf (14.03.2019).
57. Palm, E. Privacy Expectations at Work – What is Reasonable and Why? - The Royal Institute of Technology Stockholm. Arvutivõrgus: https://ecpr.eu/Filestore/PaperProposal/f0449221-bc1a-46d7-98c0-fbff05c57826.pdf (27.02.2019).
58. Pau, A Tele2 paneb töötajatele naha alla riskantse kiibi. – Postimees. 11.10.2018. Arvutivõrgus: https://tehnika.postimees.ee/6426622/video-tele2-paneb-tootajatele-naha-alla-riskantse-kiibi, (17.03.2019).
59. Pilving, I. Õigus isikuandmete kaitsele. – Juridica VIII/2005
60. Randveer, K. Isikuandmete kaitse töötaja värbamisprotsessis – väljakutse tööandjale. Magistritöö. Tallinn 2011. Arvutivõrgus: https://www.toooigusabi.ee/failid/Upload/tooted_failid/MAG_TOO_Isikuandmete_kaitse_tootaja_varbamisprotsessis_Kadri_Randveer.pdf (15.02.2019).
61. Russell, C. The use of RFID in the workplace sparks privacy concerns. Blogi Olender Feldman – Attorneys at law. Arvutivõrgus: https://www.olenderfeldman.com/rfid-and-workplace-privacy/ (11.03.2019).

62. Saarep, K. Kaameraid kasutatakse töökohal tihti valedel eesmärkidel. 17.05.2018. Arvutivõrgus: http://www.tooelu.ee/et/uudised&nID=1963 (15.02.2019)
63. Sajari, P. Nokia jatkoi työntekijöidensä viestiliikenteen urkintaa. 09.06.2008 – Helsingin Sanomat.
64. Sander, A. Töötaja kontrollimine ja isikuandmete kaitse. Kas ja kuidas võib tööandja töötajat kontrollida? 30.11.2016. – Advokaadibüroo TGS Baltic. Arvutivõrgus: http://www.tarkgruntesutkiene.lv/uudised/kasulik/toeoetaja-kontrollimine-ja-isikuandmete-kaitse-kas-ja-kuidas-voib-toeoeandja-toeoetajat-kontrollida (20.03.2019).
65. Sarap, K. Kuusik, S. Kolm põhjust, miks me vajame nii karme andmekaitse reegleid. - Njord advokaadibüroo. 09.02.2018. Arvutivõrgus: https://www.njordlaw.com/et/kolm-pohjust-miks-vajame-nii-karme-andmekaitse-reegleid/ (22.02.2019).
66. Seletuskiri isikuandmete kaitse seaduse juurde. 16.04.2018. Arvutivõrgus: https://www.koda.ee/sites/default/files/content-type/content/2018-05/Seletuskiri%20%282%29.pdf. (25.02.2019).
67. Sibold, G. Tööandja võib lugeda ka su isiklikke e-kirju, aga väga hea põhjusega. – Digigeenius. 10.01.2018. Arvutivõrgus: https://digi.geenius.ee/rubriik/uudis/tooandja-voib-lugeda-ka-su-isiklikke-e-kirju-aga-vaid-vaga-hea-pohjusega/ (16.03.2019).
68. Sibold, G. Millistel juhtudel võib tööandja uurida, mida sa sotsiaalmeedias teed? – Digigeenius. 19.10.2017. Arvutivõrgus: https://digi.geenius.ee/rubriik/uudis/millistel-juhtudel-voib-tooandja-uurida-mida-sa-sotsiaalmeedias-teed (16.03.2019).
69. Suder, S. Tööandja, ära konda Facebookis! – Personaliuudised. 22.08.2017. https://www.personaliuudised.ee/uudised/2017/08/22/tooandja-ara-konda-facebookis (29.03.2019).
70. Süld, R. Biomeetrilise isikutuvastuse levik muudab kogu ühiskonda. 03.06.2016. - Postimees. Arvutivõrgus: https://arvamus.postimees.ee/3719871/rein-suld-biomeetrilise-isikutuvastuse-levik-muudab-kogu-uhiskonda (15.03.2019).
71. The office of the future: microchipped employees. – Business World blogi. 26.09.2018. Arvutivõrgus. https://businessworld-usa.com/office-future-microchipped-employees/ (17.03.2019).
72. Thompson, S. Can employers legally monitor employees' e-mails at work? - GDPR report. 11/2017. Arvutivõrgus: https://gdpr.report/news/2017/11/17/5383/ (19.03.2019).

73. Tsai, P. Data snapshot: Biometrics in the workplace commonplace, but are they secure? – Spiceworks. 12.03.2018 Arvutivõrgus: https://community.spiceworks.com/security/articles/2952-data-snapshot-biometrics-in-the-workplace-commonplace-but-are-they-secure (15.03.2019).
74. Wacks, R. Privacy. A Very Short Introduction. Oxford University Press, 2010
75. Weihermann, R. Social media in the employment context and the nw EU General Data Protection regulation (GDPR). – Employment Germany blog. 27.06.2016. Arvutivõrgus: https://blogs.dlapiper.com/employmentgermany/2016/06/27/social-media-in-the-employment-context-and-the-new-eu-general-data-protection-regulation-gdpr/ (24.03.2019).
76. Wildhaber, L. Diggelmann, O. Euroopa inimõiguste konventsioon ja eraelu kaitse. Uuemad arengusuunad. – Juridica I/2007.

Kasutatud õigusaktid

77. Eesti Vabariigi põhiseadus. - RT I, 15.05.2015, 2
78. *Euroopa Parlamendi ja Nõukogu direktiiv 95/46/EÜ, 24. oktoober 1995, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. (ELT L 281, 23.11.1995)*
79. *Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679, 27. aprill 2016, Füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). – (ELT L 119, 04.05.2016).*
80. Isikuandmete kaitse seadus. - RT I, 04.01.2019, 11
81. Turvaseadus. - RT I, 03.03.2017, 27
82. Töölepingu seadus. - RT I, 26.06.2018, 15

Kasutatud kohtulahendid

83. EIK 61496/08, *Barbulescu v Romania*
84. EIK 62617/00, *Copland v The United Kingdom*
85. EIK 20605/92, *Halford v. The United Kingdom*
86. EIK 70838/13, *Antonovic and others v Montenegro*
87. EIK 1874/13, 8567/13, *Lopez Ribalda and others v Spain*
88. EIK 5493/72 *Handyside v The United Kingdom*
89. Inglismaa kõrgema kohtu lahend 2015 EWHC 376, *Williams v Leeds*
90. Saksamaa föderaalse töökohtu lahend 07.07.2017, a AZR 681/16
91. Riigikohtu tsiviilkolleegiumi 31. märts 2008 a. Otsus 3-2-1-13-08

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, Katrin Kullamäe,

1. Annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose „Töötaja isikuandmete kaitse tehnoloogilise arengu kontekstis“, mille juhendaja on professor Merle Erikson,

1.1. reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace-is lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
1.2. üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace´i kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.
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.

Tartus, 30.04.2019