TARTU ÜLIKOOL
SOTSIAALTEADUSTE VALDKOND
ÕIGUSTEADUSKOND
Karistusõiguse osakond

Marta Mägi

ÄRISALADUSE KAITSE KARISTUSÕIGUSLIKU REGULATSIOONI EFEKTIIVSUS KEHTIVAS ÕIGUSES

Magistritöö

Juhendaja:
MA Mare Tannberg
Kaasjuhendaja:
Prof. Jaan Sootak

Tartu 2017

Sisukord

Sissejuhatus

Ärisaladus on raskesti defineeritav õigusmõiste, mille sisustamisel lähtutakse mitmetest kriteeriumitest. Peamised kriteeriumid, millest ärisaladuse sisustamisel lähtuda, on paika pandud intellektuaalomandi õiguse kaubandusaspektide lepinguga (TRIPS-leping). Eesti kohtud on õiguse mõistmisel samuti sageli kasutanud just TRIPS-lepingu artiklis 39 lõikes 2 sätestatud ärisaladuse nõudeid. Üldjoontes võib öelda, et ärisaladus on seesugune teave, mis oma salajasuse tõttu loob ettevõtjale eelise turul tegutsemiseks, ja see teave ei ole üldsusele lihtsasti ligipääsetav.

Kuuludes Euroopa Liitu, peab Eesti järgima ka sealt tulenevaid suuniseid ning 08. juunil 2016 võttis Euroopa Liit vastu direktiivi 2016/943, milles käsitletakse avalikustamata oskusteabe ja äriteabe (ärisaladuste) ebaseadusliku omandamise, kasutamise ja avalikustamise vastast kaitset[1]. Liikmesriigid peavad oma seadusandluse direktiivis sätestatuga kooskõlla viima 9. juuniks 2018. Euroopa Komisjon tegi ettepaneku avalikustamata oskusteabe ja äriteabe regulatsiooni ühtlustamiseks liikmesriikides seetõttu, et praegusel juhul on regulatsioon liikmesriigiti niivõrd erinev, et selline killustatus takistab efektiivset ärisaladuse kaitset, mis omakorda mõjutab majanduslikku arengut ja ühisturu toimimist.

Euroopa Liidu 2013. aastal läbiviidud uuringuga leiti, et olenemata TRIPS-lepingu olemasolust ning kõikide liikmesriikide võimalusest seda ärisaladuse sisustamisel järgida, on liikmesriigid siiski oma regulatsioonides kasutanud küllaltki erinevaid lähenemisviise ning ärisaladuse kaitse on reguleeritud niivõrd erinevalt, et tegelikkuses ei ole praeguste sätetega efektiivne ärisaladuse kaitse sugugi tagatud[2]. Ka Eesti ei ole otseselt seadustesse kirjutanud TRIPS-lepingus sätestatud ärisaladuse sisustamise kriteeriumeid, kuid kohtud on kaasuste lahendamisel siiski neid sageli järginud. Eesti seadusandluses on ärisaladus reguleeritud peamiselt konkurentsiseaduses, äriseadustikus ning ka karistusseadustikus, kuid need regulatsioonid on küllaltki piiratud ega taga ärisaladuse piisavalt tõhusat kaitset.

[1] Euroopa Parlamendi ja Nõukogu direktiiv 2016/943, milles käsitletakse avalikustamata oskusteabe ja äriteabe (ärisaladuste) ebaseadusliku omandamise, kasutamise ja avalikustamise vastast kaitset. Brüssel, 08.06.2016

[2] Baker & McKenzie. Study on Trade Secrets and Confidential Business Information in the Internal Market, Final Study Prepared for the European Comission, Aprill 2013, lk 3-4. Arvutivõrgus kättesaadav: http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/130711_final-study_en.pdf (06.11.2016).

Ärisaladuse rikkumise vastaste kaitsenormide loomine muutus olulisemaks 19. sajandi keskpaigas tööstusrevolutsiooni tekkega, kui ettevõtted kasvasid ning hoogustus ettevõtetevaheline suhtlus.[3] Enamikes Euroopa riikides oli tööstusrevolutsiooni tekke ajaks juba mingisugune ettevõtete kaitse olemas. Tööstusrevolutsiooni käigus tõsteti enamik nendest varasematest seadustest, mis olid loodud ettevõtete kaitsmiseks, ümber seadustesse, mis olid otseselt suunatud tööstussaladuse kaitsmisele.[4] Ärisaladuse efektiivne regulatsioon oli eelkõige oluline Ameerika Ühendriikide suurettevõtjatele, kuna neil oli, mida kaitsta ning USA kiire tehnoloogiline areng muutis Ameerika Ühendriikide tööstused teistest riikidest pärit spioonide ja teabehankijate sihtmärgiks.Välismaalaste poolt ärisaladuse vargusega tekitatud kahju oli väga ulatuslik ning kahjueelse olukorra taastamine ega kahju hüvitamine polnud enamikel juhtudel võimalik, kuna kahju tekitaja oli põgenenud välismaale. Sellest tulenevalt võeti USA-s vastu Majandusspionaaži akt (*Economic Espionage Act*), mis sätestas majandusliku spionaaži eest kriminaalkaristused rikkujatele.[5] Ärisaladuse väga tugev kaitse oli suurettevõtete lobitöö tulemus.[6] Arvestades ärisaladuse tugeva kaitse tekkimise ajalugu ning seda, et Ameerika suurettevõtted omasid selle loomisel väga suurt mõjujõudu, tuleb tänapäeval, kui suuremat tähelepanu on hakatud pöörama ka töötajate vabale liikumisele ja võimalikult väheste põhiõiguste piiramisele, suhtuda ärisaladuse tugevasse kaitsesse ka teatava kriitilisusega.

Ärisaladuse rikkumise vastase kaitse vajalikkust on sageli põhjendatud majandusliku arengu ja innovatiivsuse suurendamise eesmärgiga. Nimelt on ärisaladuse rikkumise vastase kaitse olemasolu korral võimalik ettevõtjatel vabamalt läbirääkimisi pidada, kartmata kahju tekkimist läbi ärisaladuse rikkumise. Näiteks J. Pooley on oma artiklis öelnud, et ärisaladuse rikkumise vastase kaitse puudumisel pidurduks majanduslik areng, kuna ettevõtted palkaksid tööle vähem inimesi, sest iga inimene ettevõttes suurendab ärisaladuse avalikustumise riski, samuti suureneksid ettevõtte kulutused ärisaladuse kaitsmise meetmete rakendamiseks. Pooley toob välja, et kõige enam pidurduks majanduslik areng seetõttu, et mitmed ettevõtete vahelised läbirääkimised võivad üldse ära jääda, kuna ettevõtetel puudub vajalik kindlustunne selle

[3] Sandeen, S. K. – P. K. Yu (toim). Intellectual Property and Information Wealth: Issues and Practices in the Digital Age, vol 2: Patents and Trade Secrets. Praeger Publishers, USA 2007, lk 400. Veebis kättesaadav: http://books.google.ee

[4] Merges, Robert P., Menell, Peter S., Lemley, Mark A. Intellectual property in the new technological age. New York : Aspen Publishers ; Austin [etc.] : Wolters Kluwer Law & Business, 2007, lk 34.

[5] Caenegem, William van, „Trade Secrets and Intellectual Property. Breach of Confidence, Misappropriation and Unfair Competition. The Netherlands. Kluwer Law International BV, 2014; lk 119

[6] Adede, Adronico O., Bellmann C., Dutfield G., Melendez-Ortiz, R. (toim) Trading in Knowledge: Development Perspectives on TRIPS, Trade and Sustainability. UK: London Earthscan Publications Ltd, 2003, lk 24

suhtes, et uus äripartner saadud salajase informatsiooniga kohe minema ei jookse ja seda oma äris rakendama ei hakka.[7]

2012. aastal alustati Eestis intellektuaalomandi õiguse kodifitseerimisega[8], millega hõlmati ka ärisaladuse regulatsioon. Ühtlasi leidis intellektuaalomandi kodifitseerimiseks loodud töögrupp, et ärisaladuse regulatsioon peaks asuma tööstusomandi seaduses[9]. Sageli aga ei peeta ärisaladust omandisarnaseks õiguseks. Seda peamiselt seetõttu, et ärisaladusel puudub omadus välistada teiste isikute õiguseid nii, nagu see on omane näiteks patendile. Olenevalt sellest, kas ärisaladuse rikkumise vastane kaitse on reguleeritud omandisarnase õiguse kaitsena või mitte, sõltub ka ärisaladuse kaitsmiseks kasutatava regulatsiooni ulatus tsiviilõiguses. Samuti toob ärisaladuse omandisarnase õigusena käsitlemine kaasa muudatused ärisaladuse kaitse karistusõiguslikus regulatsioonis. Praegu on ärisaladuse kaitse reguleeritud majandusalaste süütegude peatükis ning karistusõigusliku vastutuse subjektide ring on väga kitsas, kuid juhul, kui ärisaladust lugeda omandisarnaseks õiguseks, tuleks ka karistusõiguslik regulatsioon ilmselt tõsta pigem intellektuaalse omandi vastaste süütegude peatükki ning seesuguse muudatuse läbi peaks ilmselt suurenema ka subjektide ring, kellele see regulatsioon kohalduks.

Käesoleval ajal on tulenevalt Euroopa Liidu suunistest ja intellektuaalomandi õiguse kodifitseerimisest ärisaladuse kehtiv tsiviilõiguslik regulatsioon veel muutumises. Juhul, kui reguleerida ärisaladusega seonduvad rikkumised tööstusomandi seaduses tööstusomandi alaliigina, siis võrreldes praeguse kaitseulatusega muutub ärisaladuse kaitse laiemaks. Olukorras, kus ärisaladus ei kuuluks omandisarnaste õiguste alla, ei laieneks talle need õiguskaitsevahendid, mis on suunatud omandiõiguse kaitsele, näiteks alusetu rikastumise sätted VÕS § 1037, § 1039 ja kahju tekitava õigusvastase tegevuse keelamise säte VÕS § 1055 lg 3, samuti ka TsMS § 280 tulenev teabe andmise kohustuse säte intellektuaalset omandit puudutava hagi korral. Nagu juba eelnevalt öeldud, on ärisaladuse tsiviilõiguslikku regulatsiooni põhjalikult käsitletud intellektuaalomandi õiguse kodifitseerimise raames, kuid Eesti seadusandluses on lisaks tsiviilõigusele ärisaladuse rikkumine karistatav ka kriminaalvastutuse korras. Ärisaladuse rikkumise vastutuse osas puuduvad selged suunised selle kohta, millal tuleks pöörduda tsiviilõiguses sätestatud õiguskaitsevahendite poole ning millal oleks vajalik isiku vastutusele võtmine kriminaalkorras. Vabale turumajandusele on omane riigi võimalikult vähene sekkumine majandustegevusse, mistõttu võiks ka ärisaladuse rikkumise eest

[7] Pooley, J. Trade Secrets: The Other IP Right – WIPO Magazine 2013/03, lk 3. Veebis kättesaadav: http://www.wipo.int/wipo_magazine/en/2013/03/article_0001.html

[8] Intellektuaalne omand. Intellektuaalomandiõiguse kodifitseerimisest. Ajaveeb. Veebis kättesaadav: https://ajaveeb.just.ee/intellektuaalneomand/

[9] Tööstusomandi seadustiku eelnõu seletuskiri. Veebis kättesaadav: http://www.just.ee/sites/www.just.ee/files/toostusomandioiguse_seletuskiri_22-7-2014.pdf

kriminaalvastutus lähtuda just sellest põhimõttest. Sellisel juhul tuleks alati eelistada pöördumist tsiviilõiguses sätestatud õiguskaitsevahendite poole, kuid olukorras, kus ettevõtjatel puuduvad piisavad vahendid ja võimalused oma õiguste tagamiseks, võib sageli olla lihtsam pöörduda uurimisasutuse poole kriminaalmenetluse alustamiseks. Samas, kui arvestada, et ärisaladuse efektiivne kaitse võib aidata olulisel määral kaasa riigi majanduse arengule, siis tuleks silmas pidada ka seda, et kõige suuremat preventiivset mõju ärisaladuse rikkumiste vähendamisel omab kindlasti tõhus karistusõiguslik regulatsioon.

Eelnevast tulenevalt on käesoleva töö eesmärgiks uurida ärisaladuse regulatsiooni tsiviil- ja kriminaalõiguses ning selgitada välja, kas praeguses sõnastuses kehtiv ärisaladuse kaitse karistusõiguslik regulatsioon tagab ärisaladuse efektiivse kaitse. Analüüsi tulemusena selgub, kas ärisaladuse praegu kehtiv karistusseadustiku regulatsioon vajaks muutmist või täpsemate kriteeriumite paika seadmist, et tagada tasakaal nii ettevõtjate kui ettevõtte töötajate õiguste vahel. Samuti selgub töös see, kuidas mõjutab või peaks mõjutama ärisaladuse kriminaal-vastutuse ulatust ärisaladuse omandisarnase õigusena käsitlemine.

Käesoleva töö hüpotees on püstitatud järgnevalt: Eestis kehtiv karistusõiguslik ärisaladuse kaitse regulatsioon ei täida ärisaladuse kaitse eesmärki parimal võimalikul viisil.

Selleks, et püstitatud hüpoteesi kontrollida, tuleb eelkõige leida vastused järgnevatele küsimustele:

1) Mis on ärisaladus?
2) Miks on vaja reguleerida ärisaladuse kaitset?
3) Kuidas peaks ärisaladuse kaitse olema reguleeritud?
4) Millised on tsiviilõiguskaitse vahendid ärisaladuse rikkumise korral ning millisel juhul kaasneb kriminaalvastutus?
5) Millised on erinevad võimalused ärisaladuse karistusõiguslikul reguleerimisel?

Lähtudes püstitatud hüpoteesist ning vastust vajavatest uurimisküsimustest, tuleb eeskätt selgeks teha, mis üldse on ärisaladus ning millistele kriteeriumitele peab teave vastama, selleks, et see oleks ärisaladusena kaitstav. Samuti on oluline selgitada, miks ärisaladus üldse kaitset vajab ning kuidas mõjutavad erinevad ärisaladuse olemust puudutavad seisukohad ärisaladuse kaitseulatust Eesti õiguskorras. Seega keskendub töö esimene osa just ärisaladuse sisustamisele ning ärisaladuse kaitsmise vajalikkusele, võrreldes seejuures erinevaid ärisaladuse rikkumise vastaseid õiguskaitsevahendeid, samuti võrreldakse töös ärisaladuse kaitseulatust lähtuvalt sellest, kas ärisaladust käsitletakse omandisarnase õigusena või mitte. Töö teine osa keskendub põhiliselt ärisaladuse rikkumise karistusõigusliku regulatsiooni analüüsimisele olukorras, kus

ärisaladus on isikule teatavaks saanud tööülesannete käigus või kus ärisaladus on isikule usaldatud. Ülevaate andmiseks ja puuduste väljaselgitamiseks võrreldakse Eestis kehtivat karistusõiguslikku regulatsiooni Saksamaal kehtiva sarnase sättega ning tuuakse näiteid ka Ameerika Ühendriikide regulatsioonist.

Töö kolmandas osas keskendutakse ärisaladuse karistusõiguslikule regulatsioonile olukorras, kus ärisaladusele saadakse juurdepääs ebaseaduslikke meetmeid kasutades. Tegemist on seesuguse ärisaladuse rikkumisega, milles juba ärisaladuse teada saamise või omandamise viis on ühiskondlikult mitteaktsepteeritav. Ülevaate andmiseks ja puuduste väljaselgitamiseks on jällegi asjakohane võrrelda Eesti õigust kehtiva Saksa õigusega. Samuti on selle teema juures oluline vaadelda ka Rootsis kehtivat ärisaladuse kaitse regulatsiooni, kuna Rootsi õiguse lähtepunkt on täielikult vastupidine Eestis kehtivale ärisaladuse karistusõiguslikule regulatsioonile. Samuti võrreldakse ärisaladuse karistusõiguslikku regulatsiooni Ameerika Ühendriikides kehtiva regulatsiooniga, millele tuleks tähelepanu pöörata eelkõige seetõttu, et sealne ärisaladuse karistusõiguslik kaitse on toiminud juba küllaltki pikka aega ning sealsed tähelepanekud reguleerimise osas võivad olla olulised ka Eesti karistusõiguslikku kaitset luues või muutes. Lisaks on töös ärisaladuse karistusõiguslikku regulatsiooni analüüsides toodud näiteid ka teistest Euroopa Liidu liikmesriikidest.

Käesoleva töö näol on tegemist mitteempiirilise ehk teoreetilise uurimusega. Töös on lühidalt selgitatud, millest ja millises riigis on ärisaladuse kaitse alguse saanud, samuti on võrreldud ärisaladuse kaitstust Ameerika Ühendriikides ning Euroopa Liidu liikmesriikides. Töö koostamiseks kasutati mitmete tuntud õigusteoreetikute kirjutatud artikleid, uurides erinevaid seisukohti. Seega on uurimistöös kasutatud ajaloolist, võrdlevat, analüütilist ning sünteetilist käsitlust.

Töö kirjutamisel on suureks abiks olnud Euroopa Komisjoni poolt tehtud uuringud ning William van Caenegemi 2014. aastal avaldatud teos *„Trade Secrets and Intellectual Property: Breach of Confidence, Misappropriation and Unfair Competition“*. Varasemalt on Eestis ärisaladuse regulatsiooni käsitlenud ka M. Maarand oma 2014. aastal avaldatud magistritöös, kuid M. Maarand ei käsitle oma töös kriminaalvastutuse küsimust, vaid keskendub ärisaladuse kaitsele lepinguvälistes võlasuhetes.

1. Ärisaladuse olemus

1.1. Ärisaladuse mõiste

Ärisaladust on keeruline täpselt defineerida, kuna tegemist on väga laia tähendusega õigusmõistega ning ärisaladus on oma sisult lihtsalt mingit laadi informatsioon, mis on seda kasutavale ettevõtjale majanduslikult tulutoov ning võib ettevõtjale tagada turul tegutsedes konkurentsieelise võrreldes teiste ettevõtjatega. Seepärast võibki öelda, et ärisaladuse kindlat definitsiooni ei ole paika pandud, kuid enamasti lähtutakse kindlatest kriteeriumitest, millele informatsioon peaks vastama selleks, et tegemist oleks ärisaladusega ning et see informatsioon oleks ka õiguslikult kaitstav. Ärisaladuseks ei saa pidada igasugust ettevõttes kasutatavat teavet, vaid teave, mida ettevõtja peab oma ettevõtluse seisukohalt oluliseks ehk ärisaladuseks, peab ettevõttesiseselt olema konkreetselt määratletud. Sama on leidnud ka Riigikohus oma lahendis 3-2-1-103-08[10], kus on öeldud, et ärisaladuse hoidmise kohustus ei või kaasa tuua olukorda, kus isik ei saa pärast töölepingu lõppemist samas tegevusvaldkonnas üldse töötada ning seetõttu peaks ärisaladus igas ettevõttes olema võimalikult täpselt piiritletud.

Üldiselt peetakse ärisaladuseks igasugust teavet (kaasaarvatud nt valemid, struktuurid, andmete kogumid, seadmed, programmid, meetodid, tehnikad ja protsessid), mis omab kas üksikosadena või kogumis iseseisvat tegelikku või potentsiaalset majanduslikku väärtust ning see informatsioon ei ole avalikkusele lihtsalt kättesaadav ning teabevaldaja on teabe salajas hoidmiseks teinud mõistlikke pingutusi.[11] Ameerika Ühendriikide kohus on ühes oma 2006. aasta otsuses[12] öelnud, et ärisaladus on oma olemuselt lihtsalt mingi informatsioon, mida selle valdaja püüab hoida salajas seeläbi, et sõlmib konfidentsiaalsuslepinguid ning varjab informatsiooni kõrvaliste isikute eest, rakendades selleks vajalikke meetmeid (näiteks dokumentide seifis hoidmine, krüpteerimine), nii et ärisaladuse tahtevastane avaldamine oleks võimalik üksnes rikkumise läbi.

Nagu juba eelpool mainitud, peab ärisaladus olema seesugune teave, mis omab kas tegelikku või potentsiaalselt majanduslikku väärtust ettevõtja jaoks. Seega ei ole oluline, et ärisaladuse majanduslik väärtus oleks kindlalt juba välja kujunenud ning reaalsete tulemustega tõendatav,

[10] RKTKo 3-2-1-103-08 p 20

[11] Bouchoux, Deborah E. 2006. Protecting Your Company's Intellectual Property: A Practical Guide to Trademarks, Copyrights, Patents & Trade Secrets. New York : AMACOM, 2006, lk 193. Veebis kättesaadav: http://site.ebrary.com.ezproxy.utlib.ut.ee/lib/tartu/reader.action?ppg=3&docID=10005784&tm=1480262074385

[12] Ameerika Ühendriikide Apellatsioonikohus – Confold Pacific, Inc., Plaintiff-Appellant, v. Polaries Industries, Inc., Defendant-Appellee. No. 05-1285. Decided: January 10, 2006

vaid kaitstav on ka seesugune teave, mis üksnes potentsiaalselt võib omada väärtust. See tähendab, et tegelikkuses on ärisaladus kaitstav ka täiesti algusest peale, juba kujunemise protsessis ning kaitstav on ka poolik versioon ärisaladusest (näiteks mõne retsepti või toote väljatöötamine). Lisaks on oluline arvestada ka seda, et ärisaladuse kaitse tekkimiseks ei ole tähtis, mil viisil ettevõtja, kes ärisaladust valdab, selleni jõudis. Oluline on üksnes see, et teabel oleks majanduslik väärtus ning selle teabe kasutamine annab või võiks anda konkurentsieelise selle valdajale.

Nagu aimata võib, on ärisaladuse üks olulisemaid komponente salajasus. See tähendab, et selleks, et ettevõttel üldse oleks olemas ärisaladus, on väga oluline ka kasuliku äriteabe salajas hoidmine. Vastasel juhul oleks see hõlpsasti ligipääsetav ka teistele turul konkureerivatele ettevõtetele ning selline teave ei saaks ettevõtjale pakkuda konkurentsieelist, mistõttu ei ole sellise teabe kaitsmine vajalik. Nagu eelpool nimetatud, tuleb ettevõtjal endal teha pingutusi selleks, et kasulikku teavet salajas hoida ning selle üldsusele teatavaks saamist võimalikult raskendada.

Tuntuim näide, mida ärisaladuse kirjeldamiseks kõikjal tuuakse, on Coca-Cola retsept. Coca-Cola retsepti kohta räägitakse, et see on täielikult teada vaid mõnele üksikule töötajale ning seda retsepti hoitakse kindlalt panga hoiulaekas. Seega võib ärisaladuseks olla teave, milleni jõudmiseks tehti rohkelt tööd ja katseid ning kulus mitmeid aastaid, kuid samas võib ärisaladusena olla käsitletav ka informatsioon, mis avastati läbi juhuslikkuse, kuid mis osutus ettevõttele väga väärtuslikuks. Näiteks on ühtmoodi kaitstav nii see töötlusprotsess, mida kasutati toote tootmisel, kuid ei saavutatud soovitud tulemust, kui ka protsess, millega jõuti parima võimaliku lahenduseni.[13]

Nii ärisaladuse EL direktiivi 2016/943 artikli 2 punktis 1 kui ka Eestis toimuva intellektuaalomandi kodifitseerimise protsessi käigus loodud tööstusomandi seadustiku eelnõus[14] § 228 on toodud ära kriteeriumid, millele ärisaladus peaks vastama selleks, et ta oleks kaitstav. Tööstusomandi seadustiku § 288 sätestab järgmised nõuded ärisaladusele: 1) see on salajane selles tähenduses, et teave ole kogumis või üksikosade täpses paigutuses ja kokkupanus üldteada või kergesti kättesaadav nende ringkondade isikutele, kes tavaliselt kõnesolevat laadi teabega tegelevad ja 2) sellel on kaubanduslik väärtus selle salajasuse tõttu ja 3) ärisaladuse omaja on asjaoludest lähtuvalt võtnud vajalikke meetmeid, et hoida teavet salajas.

[13] Sandeen, S. K., (3), lk 399

[14] Tööstusomandi seadustik. 22.07.2014. Veebis kättesaadav: https://ajaveeb.just.ee/intellektuaalneomand/wp-content/uploads/2014/08/ToS-EN-22-7-2014.pdf

1.1.1. Ärisaladuse salajasus

Nii nagu juba eelpool öeldud, ei ole mitte igasugune ettevõtluses kasutatav informatsioon kaitstav õiguskaitsevahendite abil. Selleks, et teave oleks kaitstav, peab ta esiteks olema saladus, ehk piirangud on seatud sellele, kui laialt mingi teave isikutele teada on. See, et ärisaladus peab olema saladus, on täiesti ilmne tulenevalt selle teabe nimetusest.

Selleks, et informatsioon oleks ärisaladus, peab tal olema ka majanduslik tähendus, see teave peab olema kuidagi struktureeritud ning koosnema faktidest[15]. Teave, mis kvalifitseerub ärisaladuseks, ei pea olema saladus kõikide komponentide osas eraldivõetuna, vaid saladus võib olla ka näiteks nende komponentide omavaheline suhestumine. Samuti tehakse vahet ka absoluutse ja relatiivse salajasuse vahel. Absoluutne salajasus tähendab, et seda teavet ei ole mitte kellelgi teisel, kuid relatiivne salajasus võib tähendada ka mõne konkurendi teadmatust ärisaladusest. Üldiselt on ärisaladuse saladuses hoidmise kriteeriumiks siiski relatiivne saladuses olemine, mis tähendab, et ettevõtjad võivad oma saladust ka teistele ettevõtjatele litsentsi alusel müüa. Samas on aga võimalik, et selline ärisaladuse litsentsi alusel kasutada andmine võib omada mingit piiri, millest alates võiks öelda, et ärisaladus on teada juba piisavalt suurele ringile ettevõtjatele, et pidada seda üldiselt selles ringkonnas teadaolevaks teabeks ning välistada sellise teabe kaitse.[16] Sellisel juhul on ilmselt võimalik siiski lepingutega reguleerida konfidentsiaalsuskohustus ja selle rikkumise korral ette näha leppetrahvi isegi juhul, kui tegemist ei ole enam ärisaladusega. Näiteks Inglismaal on kohtunikud ärisaladusena enamasti välistanud teabe, mis on väga tavapärane, ebamoraalne, ebamäärane või avalikus kasutuses[17]. Ilmselt ei kvalifitseeritaks ka Eesti kohtutes seesugust teavet ärisaladusena.

Nagu eelnevalt juba öeldud, on ärisaladuse salajasus suhteline ning saladus võib teada olla mitmetele töötajatele, kuid sellegi poolest olla kaitstav. Seega ei ole selge, kust jookseb piir saladuses olemise ja avalikus kasutuses oleva teabe vahel. Õiguskirjanduses on leitud, et see piir, millal saladus muutub avalikuks on küllaltki suhteline ja sõltub mitmetest erinevatest asjaoludest. Eelkõige on oluline lähtuda konkreetse teabe iseloomust ja sellest, kui suurel määral on see teave avalik kasutatavas ringkonnas. Teiseks tuleks arvestada, kui oluliselt võiks sellise teabe laiem avalikustamine konkreetsele ettevõtjale kahju tekitada.[18] Mõningatel juhtudel võib teave olla küll salajas hoitud, kuid see ei tee seda teavet siiski koheselt

[15] Nuno, Sousa, S. What exactly is a trade secret under the proposed directive? – Journal of Intellectual Property Law and Practice 2014/9 No 11, lk 10. Veebis kättesaadav: https://doi.org/10.1093/jiplp/jpu179
[16] *Ibid,* lk 14
[17] Shakya, S. Trade Secrets & Its Protection as Intellectual Property: Revisiting proprietary concerns in Trade Secrets, lk 7. Veebis kättesaadav: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2399311
[18] *Ibid,* lk 7

ärisaladuseks. Näiteks olukorras, kus teabe avalikuks saamine ehk saladuse kadumine ei tekita kahju ettevõtjale, vaid on lihtsalt ebameeldiv või tekitab kahju mõnele töötajale, võib tegemist olla lihtsalt konfidentsiaalse teabega, mis ei ole ärisaladus ega ärilisel eesmärgil kasutatav teave. Seega võiks kahju tekkimise võimalikkus ja selle ulatus olla üheks indikaatoriks ärisaladuseks oleva teabe ja konfidentsiaalse teabe eristamisel. Lisaks tuleks ilmselt eristada ka mainekahju tekkimist ning seesuguse teabe avalikuks tulek, mis tõepoolest kahjustab ettevõtjat, kuid pigem ettevõtja mainet, ei tohiks olla käsitletav ärisaladuse kahjustumisena.

Saksa õiguses on ärisaladuse ja lihtsalt konfidentsiaalse teabe piiritlemisel lähtutud seotusest ettevõtjaga. Saksa konkurentsiseaduse kommentaarides on öeldud, et saladus peab olema seotud ettevõtlusega. See tähendab sisuliselt seda, et saladus peab olema omistatav justnimelt sellele konkreetsele ettevõtjale ning seeläbi peab olema välistatud olukord, kus seesama teave on omistatav ka teistele sarnases valdkonnas tegutsevatele ettevõtjatele[19]. Samuti tähendab ettevõtlusega seotud teave seda, et tegemist ei ole muu isiklikku laadi teabega, mille avaldamine on piiratud muude seadustega[20]. Teabe salajasuse nõue peaks üldiselt ka vältima ärisaladuse kaitseala kattumist registreeritud intellektuaalomandi õigustega, nagu näiteks patendi kaitsega[21]. Teadaolevalt on patendi kaitseks oluline just teabe avalikustamine ja seeläbi ühiskonna arengusse panustamine, kuid ärisaladuse puhul on kaitse olemasoluks vajalik teabe salajasus.

Euroopa Liidu ärisaladuse kaitse direktiivi 2016/943 artikkel 3 lõike 1 punkti b kohaselt peab ärisaladuse omandamist seaduslikuna käsitlema juhul, kui see on omandatud mõne turule toodud toote või eseme uurimise või analüüsimise tulemusena. See tähendab seda, et pöördprojekteerimine peab olema lubatud ja isik, kes on sel viisil teada saanud mõne ettevõtja ärisaladuse, on siiski käitunud õiguspäraselt. Saksa õiguses oli enne EL-i ärisaladuse direktiivi 2016/943 aga pöördprojekteerimine karistatav olukorras, kus mingi toote või seadme analüüsimiseks tuli panustada aega ja teadmiseid määral, mis ei ole tavapärane lihtne analüüsimine, kuid seoses EL-i juhistega tuli see säte ümber hinnata[22]. See tähendab seda, et teave, milleni isik on võimeline ise jõudma või mis on talle mingi analüüsi tulemusena kättesaadav, ei saa olla käsitletav salajase teabena.

Eelneva põhjal võib seega öelda, et ärisaladus on mingisugune teave, mis ei ole avalik ehk see ei ole mingis valdkonnas tegutsevate ettevõtjate ringile teada ega lihtsalt kättesaadav ning selle

[19] Henning Harte-Bavendamm & Frauke Henning-Bodewig, Gesetz gegen den unlauteren Wettbewerb (UWG), Kommentar, 3 Auflage (2013), Beck, München. Veebis kättesaadav beck-online.beck.de
[20] Ohly, A., & Sosinitza, O., Gesetz gegen den unlauteren Wettbewerb (UWG), Kommentar, 7 Auflage (2016), Beck, München. Veebis kättesaadav beck-online.beck.de
[21] Nuno, Sousa e Silva, (15), lk 15
[22] Henning Harte-Bavendamm *et al* (19)

avalikuks saamine tekitab ettevõtjale kahju, mis tähendab, et ärisaladus on ettevõtjale väärtuslik just tänu sellele, et seda on hoitud saladuses. Lisaks peab see teave olema piisaval määral seotud ettevõtlusega, et välistada igasuguse konfidentsiaalse informatsiooni kaitsmine ärisaladusena ning see teave peab olema kasutatav ettevõtluses.

1.1.2. Kaubanduslik väärtus

Teine ärisaladuse kaitse tagamise kriteerium on see, et kaitstaval teabel peab olema mingisugune äriline väärtus ettevõtja jaoks. Üldiselt leitakse, et teabe väärtus peab tulenema just sellest, et see teave ei ole teistele konkurentidele üldteada ja tagab seetõttu mingisuguse konkurentsieelise turul tegutsemisel. Seda sama on öelnud ka USA kohtunik J. Ruvolo otsuses, kus ta leidis, et klientide nimekiri on ettevõtja ärisaladuseks üksnes juhul, kui see teave oma salajasuse tõttu annab ettevõtjale arvestatava eelise[23]. Sarnasele järeldusele on jõudnud ka Eesti Riigikohus on oma lahendis 3-1-1-46-09, kus punktides 10.3 ja 10.4 leitakse, et andmebaasides sisalduv teave hankijate kohta on ärisaladusena käsitletav näiteks juhul, kui see teave on kuidagi töödeldud või süstematiseeritud, nii et need erineksid avalikult kättesaadavatest andmetest. Süstematiseerimine või töötlemine ilmselt kannaks samuti töö lihtsustamise ja ettevõtjale eelise andmise eesmärki. Ärisaladuse väärtus ja salajasuses olek on omavahel tihedalt seotud ka seetõttu, et juhul, kui ärisaladus muutub avalikuks ning konkureerivad ettevõtjad saavad teavet kasutama hakata, siis ettevõtja kaotab oma majandusliku eelise ning see saladus on väärtusetu[24]. Samas, ettevõtja ei kaota oma ärisaladuse väärtust üksnes toote turule laskmisega või kättesaadavaks tegemisega, kuid juhul, kui ärisaladus on pöördprojekteerimise teel avastatav, siis võib ärisaladus siiski oma väärtuse kaotada.[25] Ilmselt on seesugused tooted, mis on küll turul vabalt kättesaadavad, kuid mille ärisaladus ei ole seetõttu avalikustunud näiteks mingid kreemid, mille koostist ei ole nii lihtne kindlaks teha, või ka näiteks Coca-Cola või Snickersi šokolaadi koostisosade täpne kogus ja tootesse lisamise järjekord.

Eelnevalt on töös viidatud sellele, et ärisaladusena on kaitstav ka potentsiaalselt väärtuslik teave, nii on leidnud nii Bouchoux kui ka Carvalho[26], kuid Nuno Sousa leiab, et potentsiaalselt

---

[23] Ameerika Ühendriikide Apellatsioonikohus – Morlife, Inc. v. Perry, 56 Cal.App.4th 1514, 1522, 66 Cal.Rptr.2d 731 (1997)

[24] Moohr, Geraldine S. The Problematic Role of Criminal Law in Regulating Use of Information: The Case of The Economic Espionage Act. United States of America: North Carolina Law Review Association. North Carolina Law Review. Vol 80, No. 3, 2002, lk 874 Veebis kättesaadav: http://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=3981&context=nclr

[25] Bone, Robert, G. A New Look at Trade Secret Law: Doctrine in Search of Justification. United States of America, California: California Law Review, Inc. Vol. 86, No. 1998, lk 249. Veebis kättesaadav: http://www.jstor.org/stable/3481134

[26] vt alajaotis 1.2, Bouchoux, Deborah E. 2006. Protecting Your Company's Intellectual Property, lk 193 ja Carvalho, Nuno P., The TRIPS Regime of Antitrust and Undisclosed Information, lk 235

väärtuslik ärisaladus on samane väärtusetu ärisaladusega ning sellisel juhul puudub ärisaladuse kaitse tagamiseks nõue, et ärisaladusena kaitstav teave peab omama majanduslikku väärtust.[27] Võimalik, et potentsiaalse väärtuse hindamisel tuleks lähtuda konkreetsest teabest igal üksikul juhul eraldi ning siiski anda hinnang teabe võimalikule väärtusele, kuna juhul, kui ärisaladus on alles nö arendamisjärgus ning hakkab tulevikus ettevõtjale ärilist eelist tagama, siis ei oleks selle väärtus veel kaitstav. Selline olukord aga looks suurema ebakindluse, mistõttu võiksid ettevõtjate investeeringud uute toodete või protsesside arendamisse väheneda. Samas ei tohiks potentsiaalselt väärtusliku teabe kategooriasse olla võimalik paigutada igasugu kaheldava väärtusega informatsiooni.

1.1.3. Vajalikud meetmed

Inglismaa kohus on ühes ärisaladuse lahendis leidnud, et ettevõtja peab olema võimeline absoluutselt selgelt kirjeldama, millist teavet ta oma ärisaladuseks peab ja mida ta on soovinud kaitsta.[28] Lisaks peab ettevõtja olema oma ärisaladuse kaitseks kasutusele võtnud vajalikke meetmeid. Dreyfus on öelnud, et ettevõtja kaitseb oma ärisaladuseks peetavat teavet üksnes juhul, kui see on temale väärtuslik ning juhul, kui teabel puudub tähtsus ettevõtja jaoks, siis ei vaevu ta seda teavet ka kaitsma[29]. See tähendab, et see nõue, et ettevõtja peab mingid meetmed ärisaladuse kaitsmiseks kasutusele võtma, peaks seega kindlustama ka selle, et ärisaladusena kaitstakse üksnes seesugune teave, mis omab majanduslikku väärtust. Lemley aga ütleb, et vajalike meetmete kasutusele võtmine ei taga mitte kuidagi seda, et teabel ka majanduslik väärtus oleks ja et ärisaladuseks ei peetaks igasugu ettevõttesisest teavet. Lemley leiab, et seesugune nõue ärisaladuse kaitseks tuleneb deliktiõigusest, kus rikkuja vastutust ei pruugi järgneda, kui isik, kelle vastu rikkumine toime pandi ise sellele rikkumisele kaasa aitas või selle rikkumise põhjustas.[30] See tähendab ärisaladuse kaitse puhul seda, et kui ettevõtja ise ei püüa oma ärisaladust salajas hoida ning seetõttu ei rakenda piisavat hoolt teabe saladuses hoidmiseks, siis ei ole esiteks võimalik kindlalt öelda, et see üldse oli ärisaladus, kuna ettevõtja ei väärtustanud seda ning teiseks toimus rikkumine ettevõtja enda hooletuse tulemusena.

Euroopa Liidu ärisaladuse kaitse direktiivi 2016/943 artikkel 2 punkt 1 alapunkt c küll sätestab, et ettevõtja peab ärisaladuse kaitseks võtma kasutusele vajalikud meetmed, kuid ei ütle selgelt,

[27] Nuno, Sousa e Silva, (15) lk 17
[28] Ühendkuningriikide Ülemkohus – Thomas v Mould, [1968] QB, 913
[29] Dreyfus, R. C., Trade Secrets: How Well Should We Be Allowed To Hide Them? The Economic Espionage Act of 1996. Ameerika Ühendriigid: Fordham Intellectual Property Media and Entertainment Law Journal. Vol 9 No 1, 1999, lk 11
[30] Lemley, M. A. The Surprising Virtues of Treating Trade Secrets as IP Rights – Stanford Law Review, vol. 61, no. 2, 2008, lk 348, Arvutivõrgus kättesaadav: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1155167

millised need vajalikud meetmed on. Dreyfus ütleb, et vajalike meetmete kasutusele võtmise kriteeriumit võib vaadelda kui nõuet ettevõtjale andmaks märku, et tal on oluline teave, mida ta soovib salajas hoida. Samuti peaks ettevõtja sõlmima lepinguid isikutega, kes tema ärisaladusega kokku puutuvad ning seeläbi tagama oma ärisaladuse kaitse läbi konfidentsiaalsuskohustuse seadmise ja ärisaladuse hoidmise kohustuse sätestamise. Vajalike meetmete kasutusele võtmine ei pea tähendama mingisuguse kuluka ja keeruka meetme rakendamist oma ärisaladuse kaitseks, vaid see tähendab seda, et ettevõtja peab tagama, et tema ärisaladus ei oleks tavapärastes ärilistes suhetes kõikidele lihtsalt kättesaadav. Vajalike meetmete määratlus peaks sõltuma ka sellest, kui väärtuslik on ettevõtja teave, mida ta peab oma ärisaladuseks. Olukorras, kus teave on küllaltki lihtne ning mitte väga suure majandusliku väärtusega, võib kaitsemeetmena piisata ka üksnes sellest, et ärisaladus avaldatakse vaid nendele isikutele, kellel on seda ettevõtte tegevuses vajalik teada ning samuti ärisaladuse rikkumise vastaste lepingute sõlmimisest.[31]

Eelnevast nähtuvalt võib öelda, et ärisaladuse kaitsmiseks vajalike meetmete kasutusele võtmise all ei pruugita silmas pidada midagi muud, kui seda, et ettevõtja ise oma ärisaladust vabalt kõigile ei jaga ning takistab töötajatele ärisaladusele ligipääsemist lähtuvalt sellest, kas neil on ärisaladusena kvalifitseeritavat teavet oma töös vaja või mitte. Seega ei ole see nõue ärisaladuse kaitse tagamiseks sugugi midagi ületamatut, vaid pigem mõistlik nõue, mis peaks muutma ärisaladuse rikkumise keerukamaks ning seeläbi ka vähendama kohtuvaidluste ja riikliku sekkumise määra.

1.1.4. Ärisaladuse liigid

Karistusseadustiku kommenteeritud väljaandes on märgitud, et ärisaladused võib jaotada kolme gruppi. Esimesse gruppi kuuluvad ärisaladused, mis on seotud *know-how*'ga, näiteks igasugu tehnilist laadi ärisaladused nagu välja töötatud valemid või mõni tootmisprotsess. Teise gruppi kuuluvad ärisaladused, mis on seotud ettevõtja turundustegevusega, nagu näiteks kliendinimekirjad ja allahindlusprotsendid. Kolmandasse gruppi kuuluvad muud ettevõtjasisest teavet puudutavad ärisaladused nagu näiteks veel avalikustamata majandusaastaaruanne ja rahalised kohustused.[32] Iseenesest ei ole praegu Eestis kehtiva ärisaladuse kaitse regulatsiooni puhul ärisaladuste liikide vahel erinevuse määratlemine kuigivõrd oluline, kuna seaduse regulatsioon hõlmab lihtsalt ärisaladust või konfidentsiaalset informatsiooni, mistõttu toob erinevatesse liikidesse kuuluva ärisaladuse rikkumine kaasa sama tagajärje. Samas võib

[31] Dreyfus, R. C., (29), lk 12-13
[32] Vutt, A., KarS kommenteeritud väljaanne. IV trükk 2015, § 377 p 2.3,

ärisaladuse rikkumisega ettevõttele kahju tekitamise ulatus sõltuda ka sellest, mis liiki ärisaladusega tegemist on. Näiteks tehnilist laadi ärisaladuse rikkumise puhul võib ärisaladuse tekke taga olla suur töö ja ettevõttepoolne investeering, mis võib ettevõtjale rikkumise korral minna oluliselt kallimaks maksma, kui näiteks ettevõtte kliendinimekirjade salajasuse rikkumine ehk turundustegevusega seonduvate ärisaladuste rikkumine võib kaasa tuua väiksema kahju. Kahju tekkimise võimaluse ja suuruse ulatust võiks olla võimalik silmas pidada näiteks karistusõigusliku regulatsiooni loomisel, kus mitte iga rikkumine ei tooks kaasa karistusõiguslikku vastutust, vaid vastutus kaasneks suurema kahju tekitamisel.

Eestis on *know-how'*na käsitletavat ärisaladust puudutatud Riigikohtu otsuses 3-2-1-115-05, kus ettevõtja pidas oma ärisaladuseks tervisekapsleid puudutavat teavet. Samas ei ole ükski kohtuaste seejuures analüüsinud, kas see teave vastab mingitele ärisaladuse kriteeriumitele, vaid tuginetakse pigem sellele, et ei ole tõendatud hageja ärisaladuse kasutamine ning lisaks puudub igasugune kokkulepe ärisaladuse hoidmise ja konkurentsikeelu kohta ettevõtja ja ettevõtja juhatuse liikme vahel. Enamasti on *know-how'*d sisaldav ärisaladus eristatud teistest ärisaladuse liikidest selle poolest, et *know-how* ärisaladusel on mingisugune praktiline väärtus ja see on kasutatav praktilises äritegevuses[33]. Enamasti on Eesti kohtutes ärisaladuse kuritarvitamisega seonduvad kohtulahendid käsitlenud pigem teist ärisaladuse liiki, milleks on turundustegevusega seonduvad ärisaladused.

Üks põhilisemaid kohtulahendeid, millele on sageli ärisaladust puudutavate vaidluste lahendamisel viidatud on Riigikohtu 29.12.2008 otsus 3-2-1-103-08, milles kohus leidis, et ärisaladuse sisustamisel tuleb lähtuda TRIPS-lepingus sätestatud ärisaladuse kriteeriumitest ning vajaduse korral võib võrrelda Eesti õiguskorda meile lähedaste õiguskordadega, saamaks suuniseid sarnaste õigusnormide rakendamiseks. Samuti ütles Riigikohus samas lahendis, et klientide andmed võivad olla mõningatel juhtumitel ärisaladuseks, kui need ei ole oma kogumis üldteada ja vastavatele ringkondadele lihtsasti kättesaadavad.

Sarnaselt on ärisaladust sisustatud Kriminaalkolleegiumi lahendis 3-1-1-46-09, kus kohus on leidnud samuti, et ärisaladus tuleb sisustada TRIPS-lepingu kriteeriumite kohaselt, kuid rõhutab, et ei ole mitte mingisugust alust käsitleda teavet hankijate ja nende tarnitavate toodete kohta automaatselt ärisaladusena. Kohus ütleb, et ärisaladus tuleb sisustada lähtuvalt konkreetsest turust ja ärisituatsioonist ning olukorras, kus ei ole võimaik tõendada, et teavet hankijate kohta on mingil viisil süstematiseeritud või töödeldud selliselt, et see teave annaks mingisuguse eelise võrreldes avalike andmetega, ei ole võimalik öelda, et tegemist on ettevõtja

[33] Nuno, Sousa e Silva. (15), lk 8

ärisaladusega. Lisaks eelnevale juhib kohus tähelepanu ka sellele, et ärisaladuse hoidmise kohustus ei tohi kaasa tuua olukorda, kus isik ei saa enam samal tegevusalal töötada ning kui töötaja puutus hankijate andmetega töö käigus kokku, siis on need andmed talle lähtuvalt tavapärasest töökogemusest nagunii teada ning ei ole võimalik keelata töötajal oma teadmiste kasutamist. Riigikohus viitab selles lahendis asjaolule, et isiku süüdimõistmiseks ei piisa üksnes ärisaladuseks olevate andmete avaldamise faktist, vaid lisaks tuleb ära näidata ka nende avaldamise eesmärk, näiteks äriline eesmärk võib olla andmete avaldamise korral juhul, kui neid andmeid edaspidi äritegevuses ka kasutati. Konkreetses kaasuses avaldas isik küll teabe hankijate kohta, kuid seda teavet ei oldud kasutatud, mistõttu leidis kohus, et avaldamisel puudus äriline või kahju tekitamise eesmärk.

Muud ettevõtjasisest teavet puudutav ärisaladus on käsitlemist leidnud 12.06.2008 tehtud Harju Maakohtu otsuses 2-07-25724, kus kohus leidis, et ettevõtja ärisaladusena on käsitletavad ettevõtte investeeringud, nende tootlikkus ja investeerimise motiivid. Samuti leidis kohus, et informatsiooni ärisaladuse kohta võivad sisaldada ka ettevõtte tegevuskava ja plaanid tulevikuks. Kohus lähtus ärisaladuseks kvalifitseeritava teabe analüüsimisel pigem sellest, millise teabe avaldamine võiks ettevõtjale turul konkureerides kahju tekitada ja seega ka sellest, milline informatsioon tagab ettevõttele konkurentsieelise. Seega pidas maakohus teabe hindamisel eelkõige silmas ärisaladuse olulisust ja väärtust ettevõtja jaoks.

Nagu ka eelnevalt öeldud sai, ei pruugi ärisaladuse liigitamine mängida praegu kehtiva regulatsiooni puhul olulist rolli, kuid seesugune liigendamine võib aidata ärisaladuse rikkumise korral kahju ulatuse hindamisele kaasa ning võiks olla otstarbekas ka näiteks karistusõigusliku vastutuse ulatuse määramisel. Samas tuleb kindlasti arvestada ka sellega, et ärisaladuse erinevate liikide vahetegu võib olla küllaltki aeganõudev, keeruline ning mõnel juhul ilmselt ka võimatu ülesanne, mistõttu reguleerimine erinevate ärisaladuse liikide raames ei pruugiks tagada efektiivsemat ärisaladuse kaitset. Ärisaladuse kaitse efektiivsuse tõstmise puhul on oluline eelkõige teha selgeks, millisel tasemel Eestis hetkel ärisaladuse kaitse on.

1.2. Ärisaladuse kehtiv regulatsioon Eestis

Eestis on ärisaladuse regulatsioon laiali erinevates seadustes ning ärisaladuse regulatsiooni võib leida nii konkurentsiseadusest, töölepingu seadusest, võlaõigusseadusest, äriseadustikust kui ka karistusseadustikust. Samas, mitte üheski neist ei ole ärisaladuse täpset definitsiooni. Ärisaladuse sisu kirjeldusest võib aimu saada konkurentsiseaduses sätestatud regulatsiooni põhjal.

Konkurentsiseaduse § 63 lõige 1 sätestab: „Ärisaladuseks loetakse niisugune teave ettevõtja äritegevuse kohta, mille avaldamine teistele isikutele võib selle ettevõtja huve kahjustada, eelkõige oskusteavet puudutav tehniline ja finantsteave ning teave kulude hindamise metoodika, tootmissaladuste ja -protsesside, tarneallikate, ostu-müügi mahtude, turuosade, klientide ja edasimüüjate, turundusplaanide, kulu- ja hinnastruktuuride ning müügistrateegia kohta. Ärisaladus ei ole avalikustamisele kuuluv või avalikustatud teave...“ Sellest sättest on tuletatav ärisaladuse sisu, kuid kuna säte ise asub konkurentsiseaduse peatükis 8, mis reguleerib riiklikku järelevalvet ning enamik konkurentsiseaduses ärisaladust puudutavad sätted reguleerivad järelevalvet, siis ilmselt on selle normi adressaadiks järelevalvet teostav organ, ehk praegusel juhul Konkurentsiamet. Sama on oma lahendis öelnud ka Riigikohus[34]. Ehkki see norm on suunatud ametnikele, ei tähenda see siiski seda, et seda ei võiks kasutada ärisaladuse sisustamisel ning mitmetel juhtudel on kohtud ka sellest sättest lähtunud.

Töölepingu seaduse § 22 lõige 1 sätestab, et tööandja võib määrata, millise teabe kohta kehtib töötajal tootmis- või ärisaladuse hoidmise kohustus ning lõike 2 kohaselt on ärisaladuse rikkumise kaitseks võimalik kokku leppida leppetrahvi kohaldamises ning lõige 3 lisab veel, et juhul, kui leppetrahv ei kata kogu tekitatud kahju, on võimalik ka see kahju sisse nõuda. Selle sätte kohaselt on tööandjal endal õigus määratleda, mida ta oma tootmis- või ärisaladuseks peab ning mingisugust järelevalvet selle üle ei teostata. Samas on kohus oma 02.07.2010 tehtud otsuses nr 2-05-19678 öelnud, et ärisaladus peab olema täpselt piiritletud, kuna ärisaladuse hoidmise kohustus ei tohi töötajat ülemääraselt piirata edaspidistes töö- või ametikoha otsuste osas valikute tegemisel, näiteks ei tohi olla takistatud täielikult mingis tegevusvaldkonnas edaspidine töötamine. See tähendab seda, et tööandjal on küll vaba voli määratleda, mis on tema tootmis- või ärisaladus, kuid igasuguse ettevõtjasisese informatsiooni lugemine ärisaladuseks ei ole mõttekas ega ka lubatav, ning vaidluse korral peab ettevõtja olema võimeline põhjendama miks ja kuidas see teave tema ärisaladuseks kvalifitseerub, kuna üldjuhul, kui ettevõtja ei suuda põhjendada, miks mingi teave on tema ärisaladus, siis ei ole see teave ka kaitstav. Samuti tuleb silmas pidada ka TLS § 6 lõikest 3 tulenevat informeerimiskohustust, ehk ei ole võimalik olukord, kus tööandja sätestab ärisaladuse ja lepib töötajaga kokku selle hoidmise kohustuse, kuid töötaja ei teagi täpselt, mida tööandja ärisaladuseks peab. Lisaks on sättes viide TLS §-le 5, mis tähendab seega seda, et ärisaladuse sisu, juhul kui töötaja peab seda hoidma, peab olema talle kirjalikult teatavaks tehtud.

Töölepingu seaduse § 15 lõikest 1 tuleneb töötaja lojaalsuskohustus tööandja suhtes. See tähendab, et töötaja peab tööandja suhtes käituma heas usus, ega tohi teadlikult kahju tekitada

[34] RKKKo 08.06.2009, 3-1-1-46-09 p 10.2

või tööandja mainet õõnestada. See säte võiks teatud olukordades funktsioneerida ka ärisaladuse kaitseks juhul, kui tööandja ja töötaja ei ole ärisaladuse sisus ja selle hoidmise kohustuses kokku leppinud, kuid ettevõtja ärisaladuse olemasolu ja selle kaitsetahe on töötajale eksimatult mõistetavad olnud.

Võlaõigusseaduse § 625 lõige 1 sätestab käsundisaaja tootmis- ja ärisaladuse hoidmise kohustuse juhul, kui käsundiandjal on selleks õigustatud huvi ning lõike 2 kohaselt on käsundisaaja kohustatud saadud saladust ka pärast käsundisuhte lõppu edasi hoidma, et kaitsta käsundiandja huve. Samas võimaldab sama paragrahvi lõike 2 teine lause ärisaladuse avaldada juhul, kui selleks on seadusest tulenev kohustus või käsundiandja luba. Ilmselt on seadusest tulenev kohustus ärisaladuse avalikustamiseks näiteks mingite lepingute või arvete esitamine maksuhaldurile maksumenetluse läbiviimiseks.

Äriseadustikus on ärisaladuse hoidmise kohustus osaühingu juhatuse liikmele sätestatud § 186 lõikes 1 ning samasugune kohustus on sätestatud aktsiaseltsi juhatuse ja nõukogu liikmele vastavalt § 313 lg 1 ja § 325 lg 1, kuid ka need sätted ei selgita, mida tuleks ärisaladuseks pidada. Samuti ei ole äriseadustikus ühtki sätet, mis kuidagi piiraksid ärisaladuse hoidmise kohustuse kestust või muudaksid hoidmise kohustuse sõltuvaks ärisaladuse sisu tutvustamisest, nii nagu see on töösuhete puhul. Ka Riigikohus on oma otsuse 3-2-1-103-08 punktis 20 öelnud, et juhatuse liikme ärisaladuse hoidmise kohustus eksisteerib nii juhul, kui tema juhatuse liikme lepingus on ärisaladuse sisu määratlus üldine, kui ka juhul, kui seesugune leping üldse puudub. Riigikohus on samas lahendis öelnud, et ärisaladuse hoidmise kohustuse kestuse määramisel tuleks lähtuda VÕS § 625 lõikest 2, mis ütleb, et ärisaladust tuleb pärast käsundisuhte lõppu edasi hoida määral, milles käsundiandja õigustatud huvi seda nõuab.

Karistusseadustiku § 377 kohaselt karistatakse isikut töö- või ametiülesannete käigus teatavaks saanud ärisaladuse kasutamise või avaldamise eest, kui seda on tehtud ärilisel või kahju tekitamise eesmärgil. See tähendab, et objektiivse koosseisu elementideks on asjaolu, et ärisaladus saadi teada töö- või ametiülesannete käigus, isik on ärisaladuse avaldanud või ärisaladust kasutanud ning sellel on äriline eesmärk, nagu näiteks endale tulu tekitamine, või ettevõtjale kahju tekitamise eesmärk. Norm ei piira kuidagi saladuse hoidmise kohustuse kestust, mis tähendab, et ettevõtja ärisaladusi tuleb saladuses hoida piiramatult ning ka pärast töösuhte lõppu[35]. Sisuliselt ei piira saladuse hoidmise kestust ka eelpool toodud sätted, kuna VÕS § 625 lg 2 kohustab ärisaladust ka pärast käsundisuhte lõppu edasi hoidma, kui selleks on õigustatud huvi ning TLS § 22 lg 1 viitab selles osas võlaõigusseaduse sättele.

[35] A. Vutt (koost), KarS kommenteeritud väljaanne. IV trükk 2015, § 377/4.4

See näitab, et eelkõige on Eesti õiguses siiski reguleeritud ärisaladuse hoidmise kohustus tööja ametialastes suhetes ning suhetes, mis nendega sarnanevad. See on ka mõistetav, sest kõige enam võivadki tööandja ärisaladuse säilimist ohustada just ettevõtjaga tööalases suhtes olevad isikud, kes näiteks töö- või ametikohti vahetades võivad endise töötaja ärisaladust soovida ka järgmises ettevõttes rakendada, mis aga kahjustaks endise tööandja konkurentsieelist. Sama kehtib ka juhatuse liikmete suhtes.

Kuna ärisaladus on väga tihedalt seotud konfidentsiaalse teabe mõistega, tuleks tähelepanu pöörata ka konfidentsiaalse teabe regulatsioonile. Konkurentsiseaduse § 52 lõike 1 kohaselt on konfidentsiaalse teabe kuritarvitamine konkurendilt ebaseaduslikul viisil saadud teabe kuritarvitamine. On selge, et iga konfidentsiaalne info ei ole veel ärisaladus, kuid ärisaladuse avaldamisele või kasutamisele võiks mõningatel juhtudel selle sätte regulatsioon kohalduda. Tööstusomandi seaduse koondkaardistamisel on välja toodud, et selle sätte puhul on probleemiks see, et seda sätet saab kohaldada üksnes olukorras, kus teave on seadusevastaselt saadud just konkurendilt ning olukorras, kus isik kasutab võõrast ärisaladust mingis muus valdkonnas, mis ei konkureeri selle ettevõtja kaubaturuga, kellelt ärisaladus saadi, siis ei ole see norm kohaldatav.

Ärisaladuse peamiseks kaitsmise eesmärgiks Euroopa Liidu direktiivi 2016/943 kohaselt on ettevõtjate konkurentsieeliste ja innovaatilisuse tagamine ning ärisaladuse kaitsemeetmeid ühtlustatakse selleks, et ei oleks võimalik varguse ja muude ebaausate meetodite kaudu saada kellegi teise loome- ja teadustegevuse pealt ebaausat konkurentsieelist. Lisaks on ärisaladuse parema kaitse vajalikkust põhjendatud argumentidega, et ärisaladuse puudulik kaitse ei lase innovaatilistel ettevõtetel oma töö tulemustest esimesena kasu saada ning see piirab ettevõtjate arenemist üle piiri ning ei võimalda ära kasutada ärisaladuse võimalusi investeeringuteks ja majanduskasvuks.[36] Kui nüüd arvestada viidatud ärisaladuse parema kaitse tagamise eesmärki ning seda, et kui mittekonkurent ebaausal teel omandab kellegi ärisaladuse ning kasutab seda mittekonkureerivas valdkonnas, siis majanduslikust perspektiivist lähtudes on turul olukord paranenud, sest keegi kahju ei kannatanud ning ühe ettevõtja majanduslik efektiivsus ilmselt kasvas. Samas on ilmne, et seesugust ebaseaduslikku teise ettevõtja ärisaladuse omandamist ei tohiks tolereerida ning lisaks peaks olema mingil viisil ka kindlustatud, et see ettevõtja, kes ärisaladuse ebaausalt omandas, kuid ise ei konkureeri, seda edasi ei jagaks ettevõtjatele, kes esialgse ärisaladuse loojaga konkureerivad.

[36] EL direktiiv 2016/943, 08.06.2016, preambula p 3, 4

Samas näiteks karistusseadustiku § 377 lg 1 ei sätesta mingisugust piirangut sellele, kas ärisaladuse rikkumine toimub konkureeriva ettevõtja poolt või mitte. Karistusseadustiku kohaselt on ärisaladuse avaldamine ja kasutamine karistatav, kui see on toime pandud ärilisel või kahju tekitamise eesmärgil. See tähendab seda, et ärisaladuse kaitse karistusõiguslik ulatus on justkui laiem kui konfidentsiaalse teabe kaitseulatus konkurentsiseaduse alusel. Seega ilmselt olukorras, kus rikutud on ettevõtja konfidentsiaalset teavet, mis on ühtlasi ettevõtja ärisaladus, kuid rikkujaks on keegi, kes ei kasuta seda teavet konkureerival kaubaturul, siis ei ole konkurentsiseaduse sätete kohaldamine võimalik, kuid võimalik on pöörduda karistusõiguse sätete poole, juhul, kui ülejäänud koosseisuelemendid on täidetud.

Konfidentsiaalse teabe regulatsioon, mis puudutab ka ärisaladust on veel näiteks tsiviilkohtumenetluse seadustikus § 741, mis sätestab vahekohtuniku saladuse hoidmise kohustuse, kui selleks on pooltel õigustatud huvi ning konfidentsiaalset infot reguleerib veel ka riigihangete seaduse § 43 lg 4, mis kohaldub näiteks esitatud pakkumustele. On ilmne, et ärisaladuse ja konfidentsiaalse teabe regulatsioon esineb mitmetes seadustes, kuid mitte üheski ei ole seesugust regulatsiooni, mis tagaks ärisaladusele piisava kaitse, lisaks raskendab ärisaladuse kaitsenormide rakendamist ja nende mõistmist asjaolu, et need normid on kõik eriseadustes laiali ning ühtne norm puudub.

Üldjuhul on praeguse regulatsiooni korral kõige parem ärisaladuse kaitseks sõlmida vastavasisulised lepingud, kus on reguleeritud ka kahju hüvitamine ärisaladuse rikkumise korral. Võimalik on rikkumise puhuks kokku leppida ka leppetrahvis, kuna sel juhul ei ole vaja hakata tõendama tekitatud kahju ulatust. Juhul, kui lepingus puudub kokkulepe leppetrahvi kohta ärisaladuse rikkumise korral, tuleb ettevõtjal ära tõendada tekkinud kahju suurus ning ka VÕS § 127 lg 4 tuleneva põhjusliku seose olemasolu kahju ulatuse ning ärisaladuse rikkumise vahel. Riigikohus on korduvalt rõhutanud, et põhjusliku seose tuvastamiseks tuleb kasutada *conditio sine qua non* põhimõtet, mille kohaselt kahju tekkimine on kahju tekkimise aluseks oleva teoga põhjuslikus seoses juhul, kui ilma selle teota ei oleks kahju tekkinud. Vastasel juhul tuleb põhjusliku seose olemasolu eitada.[37] See tähendab, et juhul, kui ärisaladust on rikutud peab ettevõtja suutma ära näidata oma kahju ulatuse, mis võib näiteks nähtuda vähenenud käibest või väiksemast tulust, kuid ühtlasi peab suutma ka tõendada, et kehvem käive ja väiksem tulu on tingitud justnimelt ärisaladuse rikkumisest ning mitte üldisest majandusliku olukorra langusest või mõne teise konkurendi turule tulekust.

[37] Vt RKTKo 3-2-1-173-12 p 18, RKTKo nr 3-2-1-42-16, p 19, RKTKo nr 3-2-1-101-16, p 18

Euroopa Liidu ärisaladuse kaitse direktiivist 2016/943 artiklist 14 punktidest 1 ja 2 tuleneb, et liikmesriigid peavad tagama ettevõtjale, kelle ärisaladust rikkumise tõttu kahjustati, õiglase kahjuhüvitise ning hüvitise määramisel peab arvestama kõikide negatiivsete majanduslike mõjutustega nagu näiteks saamata jäänud tulu ja rikkuja saadud ebaõiglast tulu ning asjakohasel juhul tuleb hüvitada ka tekitatud moraalne kahju.

Intellektuaalomandi kodifitseerimise töögrupi loodud tööstusomandi seadustiku eelnõust[38] nähtub, et ärisaladust soovitakse reguleerida tööstusomandi valdkonna alla kuuluva õigusena. Nimelt sätestab tööstusomandi seadustiku eelnõu § 2 lõige 1 seda, et tööstusomand on isiku täielik õiguslik võim tööstusomandi eseme üle ning sama paragrahvi lõige 2 punkt 6 ütleb, et tööstusomand hõlmab õigusi seoses ärisaladusega. Lisaks loetakse § 4 punkti 1 kohaselt tööstusomandi omanikuks ka isikut, kellele kuulub tööstusomandi ese. See tähendab, et selle regulatsiooni kohaselt käsitletakse ärisaladust kui omandisarnast õigust, mis toob kaasa ärisaladuse senises regulatsioonis mõningaid muudatusi.

Ärisaladus omandisarnase õigusena toob põhilise muutusena kaasa selle, et ärisaladusele hakkavad kehtima need sätted, mis praegu kehtivad omandile, kuid ei kehti teabele. Näiteks, kui lugeda ärisaladus omandisarnaseks õiguseks, siis võlaõigusseaduse kohaselt kohalduks ka ärisaladuse kaitsele alusetu rikastumise sätetest tulenev väärtuse hüvitamise nõue õiguse rikkumise korral (VÕS § 1037). Praegusel juhul see säte ei rakendu, kuna ärisaladus kui teave ei kvalifitseeru isiku omandiks, muuks õiguseks ega valduseks. Muu õigusena peetakse selle sätte kohaselt silmas absoluutset õigust[39], kuid ärisaladusel pole omadust välistada teiste isikute õigusi, mistõttu ta absoluutse õiguse alla ei kuulu. Samuti ei ole võimalik ärisaladuse rikkumise osaks saanud isikul VÕS § 1055 lõikest 3 tuleneva nõude kasutamine, millega oleks võimalik nõuda kahju tekitava tegevuse lõpetamist, kuna see säte kehtib üksnes autoriõiguse, autoriõigusega kaasneva õiguse või tööstusomandiõiguse rikkumises. See tähendab, et senikaua, kui ärisaladus ei ole Eesti õiguskorras reguleeritud tööstusomandi alaliigina või ei ole muul viisil tagatud ärisaladuse omaniku õiguste kaitse, siis ei ole tsiviilõiguslikud õiguskaitsevahendid piisavalt efektiivsed rikkumiseelse olukorra taastamiseks. Arvestades, et kriminaalmenetluses ärisaladuse kaitsmisel toimub kahju hüvitamine samuti läbi eraõiguslike hagide, siis omavad eraõiguslikud kahjuhüvitamise võimalused suurt tähtsust ka karistusõiguse aspektist, ehkki karistusõiguses sätestatud ärisaladuse kaitse regulatsioon omab preventiivset tähendust ka pelgalt läbi karistuste kehtestamise.

[38] Tööstusomandi seadustiku eelnõu (14)
[39] Varul, P. *et.al*. (koost.) Võlaõigusseadus III osa. Kommenteeritud väljaanne. 2010, § 1037 3.1.1. a

Ilmselt olukorras, kus ärisaladus oleks käsitletav omandisarnase õigusena, oleksid ettevõtjatel paremad tsiviilõiguslikud õiguskaitsevahendid ning sel juhul võiksid ka need sätted omada piisavat preventiivset mõju ärisaladuse rikkumise vähendamisel ning ärisaladuse karistusõiguslik regulatsioon võiks jääda pigem raskemate juhtumite tarbeks. Samas, kui ärisaladus reguleerida omandisarnase õigusena, tuleks ärisaladuse karistusõiguslik regulatsioon nagunii üle vaadata.

1.3. Ärisaladus omandisarnase õigusena

Ärisaladuse õigusliku kaitse loomisel jagunevad vaated ärisaladuse olemusest põhiliselt kaheks peamiseks. Ühe õigusliku suuna esindajad käsitlevad ärisaladust kui ühte omandiõiguse osa ning liigitavad ärisaladuseks oleva teabe intellektuaalomandi valdkonda kuuluvaks. Teise suuna esindajad aga näevad ärisaladuse rikkumises mitte niivõrd omandiõiguse rikkumist kui ebasündsat ja ebaausat käitumist, mistõttu on ärisaladuse rikkumine vaadeldav pigem õigusvastase kahju tekitamisena ning ärisaladuse kaitse-eesmärgiks on majanduslikult õige ja aktsepteeritava käitumise tagamine[40]. Sellest, kas ärisaladust käsitleda omandisarnase õigusena või mitte, sõltub ka tema kaitseulatus. Juhul, kui ärisaladust reguleerida omandisarnase õigusena, siis rakenduksid ärisaladuse kaitsele kõik sätted, mis reguleerivad omandi kaitset.

Sageli ei peeta ärisaladust omandiõiguseks seetõttu, et ärisaladusel puuduvad mõned olulised omadused, mis üldiselt omandiõiguse puhul olemas on. Omandiõigus jaotub positiivseks omandiõiguseks ja negatiivseks omandiõiguseks. Positiivse omandiõiguse korral on isikul, kellele mingi asja omand kuulub, võimalus oma asjaga käituda nii nagu ta ise soovib, ehk isikul on eriline õigus seda asja vallata, kasutada ja käsutada vastavalt omale äranägemisele. Omandiõiguse negatiivne sisu hõlmab aga endas omaniku õigust teistelt isikutelt nõuda temale kuuluva omandi rikkumise vältimist ja rikkumise korral ka nende tagajärgede kõrvaldamist. Omand tähendab üldjuhul ainult omanikule kuuluvat õigust oma asjaga käituda nii, nagu ta ise soovib ning seda õigust võivad piirata vaid teiste isikute õigused või seadusest tulenevad piirangud.[41] Püüdes neid kriteeriumeid rakendada ärisaladusele, siis näib, et omandiõiguse positiivsed küljed on ärisaladusel olemas. See tähendab, et iga ettevõtja, kellel on mingi ärisaladus, võib sellega käituda just nii nagu ta ise soovib. Igal omanikul on võimalik oma ärisaladust edasi salajas hoida ja seda kasutada või litsentseerida mõnele teisele ettevõtjale või hoopis avalikustada ning seeläbi ärisaladusest loobuda.

[40] Merges, Robert P., Menell, Peter S., Lemley, Mark A. (4) lk 37-38
[41] Varul, P. *et al.* Asjaõigusseadus I. Kommenteeritud väljaanne, lk 277. Kirjastus Juura, Tallinn 2014.

Peamine probleem ärisaladuse omandisarnase õigusena käsitlemisel tuleb enamasti just sellest, et ärisaladuse omanikul ei ole õigust keelata teistel ettevõtjatel samasuguse ärisaladuse kasutamist või avaldamist juhul, kui sellele teisele ettevõtjale on see ärisaladus teatavaks saanud seaduslikul viisil. See tähendab seda, et ärisaladust omaval ettevõtjal puudub õigus välistada teiste isikute õigust samale ärisaladusele. Samas on ettevõtjal, kellele ärisaladus kuulub, õigus keelata teistel isikutel ebaseaduslikult ja ebaausate meetmete läbi tema ärisaladusele ligi pääseda ning samuti on ettevõtjal absoluutne õigus keelata teistel isikutel tema ärisaladuse rikkumine, kui seda on tehtud ilma õigusliku aluseta.

Omandisarnaseks õiguseks on ärisaladust sageli peetud Ameerika Ühendriikides. Näiteks kohtulahendis *Van Products Company v. General Welding and Fabricating Company*[42] loeti ärisaladus just omandisarnaseks suhteks, mitte konfidentsiaalsussuhteks, kuna leiti, et alguspunkt ärisaladuse rikkumise tuvastamisel ei ole mitte konfidentsiaalse suhte olemasolu, vaid see, kas üldse eksisteeris ärisaladus, mida oli võimalik väärkasutada[43]. Konfidentsiaalse teabena käsitletakse ärisaladust puudutavat informatsiooni enamasti aga Inglismaal. Kohtuasja *Coco v A N Clark (Engineers) Ltd* kohaselt peab teave õiguskaitsevahendite kasutamiseks olema konfidentsiaalse iseloomuga ning jõudnud isikuni sellisel viisil, et isikul on võimalik eeldada, konfidentsiaalsuskohustuse tekkimist ning seejärel on isik kasutanud saadud teavet lubamatul viisil. Konfidentsiaalsuskohustus tekib, kui mõistlik isik saaks aru, et teave, mis talle usaldati on konfidentsiaalne[44]. Eesti õiguses ei ole siiani käsitletud ärisaladust kui omandisarnast õigust, pigem on kohtud ärisaladust sisustades lähtunud konkurentsiseaduse mõttest ning samuti kohaldanud konfidentsiaalse teabe kaitseks mõeldud kriteeriumeid. Konkurentsiseadusest lähtudes käsitletakse ärisaladuse rikkumist pigem kõlvatu konkurentsi meetmena, mis näitab, et Eesti õiguskorras on pigem hukka mõistetud mingisugune käitumisviis, mis ei vasta üldiselt aktsepteeritud käitumisstandarditele.

Eestis on küll seni käsitletud ärisaladust kui konfidentsiaalset informatsiooni ning ärisaladuse rikkumise korral on pöördutud kõlbmatu konkurentsi sätete poole, kuid autoriõiguse kodifitseerimise raames ja tööstusomandi seadustiku eelnõus on asutud seisukohale, et ärisaladus peaks siiski kuuluma omandisarnaste õiguste hulka. Eesti Vabariigi põhiseaduse kommenteeritud väljaande § 32 punktis 4.7 on öeldud, et omandi puutumatus hõlmab ka intellektuaalomandi liike, milleks on autoriõigus, autoriõigusega kaasnevad õigused ja

[42] Ameerika Ühendriikide Ülemkohus – Van Prods. Co. v. General Welding & Fabricating Co., 213 A.2d 769, 780 (Pa. 1965)
[43] „The starting point in every case of this sort is not whether there was a confidential relationship, but whether, in fact, there was a trade secret to be misappropriated."
[44] Ühendkuningriikide Ülemkohus. - Coco v A N Clark (Engineers) Ltd (1969) RPC 41.

tööstusomand. Karistusseadustikus on intellektuaalse omandi vastased süüteod reguleeritud 14. peatükis. KarS § 226 reguleerib tööstusomandi õiguse rikkumist ning sätestab rikkumise korral karistusena rahatrahvi, mis näitab et tegemist on väärteona käsitletava rikkumisena. Praegusel juhul, kui ärisaladus ei ole käsitletav mitte tööstusomandi alaliigina, vaid ärisaladuse rikkumine on reguleeritud majandusalaste süütegude peatükis, on ärisaladuse rikkumine karistatav rahalise karistuse või üheaastase vangistusega.

Võrreldes praegust ärisaladuse karistusõiguslikku regulatsiooni kehtiva tööstusomandi õiguse regulatsiooniga, võib öelda, et ärisaladuse rikkumine on reguleeritud märgatavalt kitsamalt ning ärisaladuse rikkumise korral on ette nähtud karmim karistus, kui tööstusomandi õiguse rikkumise korral. Samuti on selge, et intellektuaalomandi valdkonda kuuluvate õiguste rikkumise eest vastutavad kõik rikkujad võrdsel määral ning mingisuguseid kitsendusi ei ole seadusega ette nähtud, samas kui ärisaladuse rikkumise eest vastutavad praegusel juhul üksnes ettevõtja töötajad, kellele on ärisaladus teatavaks saanud läbi tööülesannete. Seega ilmselt juhul, kui ärisaladus kuuluks intellektuaalomandi valdkonda ning oleks reguleeritud karistusseadustiku 14. peatüki all, siis peaks ärisaladus kui omandisarnane õigus olema samuti kaitstud kõikide isikute rikkumiste eest, mitte üksnes töötajate rikkumise eest.

Samuti võib öelda, et ärisaladuse rikkumise eesmärk ei pruugi olla üksnes varalise kasu saamine, nagu seda sätestab KarS § 226 tööstusomandi õiguse rikkumise korral, vaid ärisaladuse rikkumise eesmärk võib tuleneda ka soovist ärisaladuse omajat kahjustada ning seega läbi ärisaladuse avalikustamise ettevõtja ärisaladus väärtusetuks muuta. Võttes arvesse ärisaladuse omadust luua ettevõtjale ärilisi eeliseid justnimelt seetõttu, et kasulik informatsioon püsib saladuses, võib kindlalt väita, et teiste tööstusomandi liikide puhul on tegemist pigem vastupidise olukorraga – ehk tööstusomandi õigused (näiteks patent või kaubamärk) omavad kaitset, kui nad on registreeritud ning seeläbi ka avalikustatud. See tähendab seda, et kui reguleerida ärisaladus lihtsalt samas karistusõiguslikus sättes nagu tööstusomandi õiguse kaitse, siis jääks ärisaladus olulisel määral kaitseta. Samuti tuleks arvesse võtta seda, et ärisaladuse avalikustamisel ei ole selle väärtus enam endisel kujul kuidagi taastatav, mistõttu oleks ilmselt ebaõige seesuguseid rikkumisi karistada üksnes väärteona. Juhul, kui ärisaladus reguleeritaks tööstusomandi alaliigina, tuleks läbi mõelda ka ärisaladuse kaitse vajalik ulatus ning lähtuvalt ärisaladuse erisustest võrreldes teiste tööstusomandi alaliikidega teha vastavad muudatused ka karistusõiguslikus regulatsioonis. Samas, kui asuda seisukohale, et ärisaladus on intellektuaalse omandi alaliik ning peaks olema sellena ka kaitstav, siis tuleks tähelepanu pöörata ka sellele, et intellektuaalomandi õigused on eraõigused[45] ning seega tuleks neid ka kaitsta eraõiguslike

[45] Põhiseadus. Kommenteeritud väljaanne § 32 p 4.7.

õiguskaitsevahenditega. Karistusõiguse revisjoni käsitlevas karistusseadustiku muutmise seaduse seletuskirjas on peamiseks ja läbivaks põhimõtteks *ultima ratio* põhimõte, mille kohaselt tuleb karistusõiguse poole pöörduda üksnes juhul, kui teiste õigusharudega tagatavatest õiguskaitsevahenditest ei piisa[46]. Seega juhul, kui reguleerida ärisaladus tööstusomandi alaliigina, võiks olla mõeldav see, et ärisaladus ei peakski ehk olema karistusõiguslikult tugevamalt kaitstav kui muu tööstusomand, kui eraõiguslikud õiguskaitsevahendid on tagatud. Sellisel juhul oleks siiski oluline kaitsta ärisaladust ka kahju tekitava eesmärgiga käitumise vastu, mis tuleks sel juhul praegu kehtivasse KarS § 226 juurde lisada. Arvestades aga ärisaladuse erinevusi võrreldes teiste tööstusomandi seadustega, näiteks seda, et ärisaladuse avaldamise korral ei ole kuidagi võimalik taastada endist õiguslikku olukorda, tuleks asuda seisukohale, et seesugune regulatsioon, kus ärisaladuse rikkujat karistataks üksnes väärteo korras, ei pakuks piisavalt vajalikku kaitset.

Seega, kui reguleerida ärisaladus karistusõiguslikult ja intellektuaalomandi rikkumist käsitlevas peatükis, siis tuleks ilmselt luua eraldiseisev koosseis, mis arvestaks ka ärisaladuse rikkumisega tekitatud kahju ulatust, ehk kuriteokoosseis võiks ette näha mingi tekitatud kahju piirmäära, millest alates oleks tegemist kuriteoga. Ärisaladus peaks sel juhul olema kindlasti kaitstav kõikide isikute rikkumiste vastu ning ilmselt tuleks arvestada ka sellega, et kahju võidakse tekitada lisaks ärilisele eesmärgile veel ka kahju tekitamise eesmärgil. Üldiselt tuleks karistusõiguslik kaitse tagada üksnes raskete rikkumiste puhuks ning lähtuda vastutuse ulatuse määramisel ka endise olukorra taastamise võimalikkusest, mis võib näiteks ärisaladuse kasutamise ja mitte avaldamise puhul kõne alla tulla.

Praegune ärisaladuse kaitse karistusõiguslik regulatsioon tundub olevat pigem suunatud tööandjate kaitsele olukorras, kus töötajad võivad tööandjate huve kahjustada läbi usalduse kuritarvitamise, reetmise ja konfidentsiaalsussuhte rikkumise. See näitab, et praeguse ärisaladuse käsitluse puhul on Eesti õiguses on pigem siiani lähtutud mitte omandisarnase õiguse regulatsioonist, vaid pigem on hukka mõistetud ebaaus ja majanduskeskkonnas mitteaktsepteeritav käitumine.

Autoriõiguste, sellega kaasnevate õiguste ja tööstusomandi õiguste kaitse intellektuaalomandina tuleneb ühiskonnas heaks kiidetud õiguspoliitikast, mille kohaselt on nende õiguste kaitse intellektuaalomandina vajalik selleks, et tagada majanduse areng ja innovatsioon. Sellest tulenevalt tagab riik autoriõiguste piiratud ja tähtajalise kaitse, kuna see

[46] Riigikogu XII koosseis. Karistusseadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seadus 554 SE, lk 7. Veebis kättesaadav: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/78433b29-8b2f-4281-a582-0efb9631e2ad

on ühiskonna arengu huvides vajalik.[47] Võib argumenteerida, et ilma riigipoolse autoriõiguse või tööstusomandiõiguse kaitseta puuduks autoritel huvi panustada oma loominguga ühiskonda, kuna autorid ei saaks sellisel juhul oma loodud tööst ja nähtud vaevast mingit kasu. Riigipoolse kaitsega on neil aga mõneajane eelis teiste isikute ees ning seetõttu säilib motivatsioon luua ja oma tooteid edasi arendada.

Võttes arvesse intellektuaalomandi peamist eesmärki kaitsenormide tagamiseks, milleks, nagu eelpool öeldud, on ühiskonna arengusse panustamine ja informatsiooni jagamine ühiskonnaga, et tagada majanduse innovatsioon, siis ärisaladuse puhul võib selgelt väita, et ärisaladuse kaitse eesmärgiks ei saa kindlasti olla teabe jagamine ühiskonnaga, kuna ärisaladuse kaitse kaob, kui saladus saab teatavaks. Ühiskonna arengusse panustamine võib mõningal määral olla ärisaladuse kaitse tagamise eesmärk, kuna ärisaladuse kaitse tagab ettevõtjatele kindluse, et nende ärisaladust ei ole nii vabalt võimalik õigustamatult omandada ning ettevõtjad võivad seeläbi säästa kaitsekulutustelt ja teha investeeringuid toodete ja teenuste arendamiseks. Moohri sõnul ei ole ärisaladuse puhul tagatud see nõue, mis on üldiselt ette nähtud intellektuaalomandi kaitse tagamiseks, ehk isikud saavad tähtajalise majandusliku eelise ja oma loomingu kaitse vastukaaluks sellele, et nad jagavad ühiskonnaga väärtuslikku informatsiooni. Lisaks on ärisaladusel oluline erinevus ka patendiga selles osas, et patendikaitse tagamiseks peab patendiga kaitstava toote omanik ära näitama, et tema toode on tõesti ainulaadne ning seetõttu väärib kaitset, kuid ärisaladuse puhul puudub igasugune eelneva kontrolli võimalus teabe kvaliteedi üle, kuna ärisaladusena määratletava teabe sisu üle otsustab esmajärjekorras ettevõtja ise. Moohr leiab seega, et seesugune kaitsemeetme loomine, mis on osaks saanud intellektuaalomandi õigustele, võib olla ärisaladuse puhul liigne, kuna ärisaladuse kaitsmine intellektuaalomandi õigusena looks ärisaladusele kui üpriski ebamäärasele kontseptsioonile liialt tugeva kaitse.[48] Seega, arvestades ärisaladuse omadusi, selle kaitse tekkimiseks vajalikke kriteeriumeid, erisusi teiste intellektuaalomandi valdkonda kuuluvate õigustega, kuid pöörates tähelepanu ka ärisaladuse kaitse positiivsetele aspektidele, võiks asuda seisukohale, et ärisaladuse efektiivne kaitsmine on küll ühiskonna ja majanduse arengu seisukohalt väga oluline, kuid selle kaitseulatusega ei tohiks ka liialt kaugele minna. Intellektuaalomandi kaitse võiks siiski jääda pigem selgelt piiritletavate ja enne kaitse tagamist kontrollitavate kriteeriumitega õiguste kaitsmiseks.

Ärisaladuse kaitse loomisel tuleb kindlasti arvesse võtta ka Eesti majanduse väiksuse konteksti. Võib oletada, et ärisaladuse kaitse vajalikkus võib olla tõusev trend, kui lähtuda erinevate start-

[47] Moohr, Geraldine S. (25), lk 896.
[48] *Ibid*,(25) lk 901

up ettevõtete innovaatilisusest, mistõttu võib olla vajalik kaitsta ärisaladust efektiivsemalt, kui seda on seni tehtud. Samas, kui võtta arvesse praeguseks kohtutest läbi käinud ärisaladuse kaasuseid, millest valdav enamus on turundustegevust puudutavad ärisaladused, mille rikkumine kujutab endast üldjuhul endise ettevõtja hinnapoliitika või kliendinimekirjade kaasavõtmist, siis ei näi olevat nende andmete kaitsmine intellektuaalomandina kuigi põhjendatud. Seda ka seetõttu, et ilmselt konkurentsivõimelise hinnastrateegia või toimivate kliendiandmebaaside kujundamine ei sõltuks ka sellest, kas need on ärisaladusena kaitstavad või mitte. Iga ettevõte panustaks kaitsest hoolimata ilmselt konkurentsivõimelise turundusstrateegia loomisesse. Ärisaladuse kaitse võiks intellektuaalomandi kaitsega võrreldav olla tõesti juhul, kui tegemist oleks oskusteavet, nagu näiteks tootmisprotsesse või arvutiprogramme puudutava ärisaladusega, kuna sellisel juhul võivad ettevõtjad tõepoolest panustada arendamisse rohkem, kui efektiivne kaitse on tagatud. Arvestades, et praegu ei ole Eesti kohtud lähtunud ärisaladusest kui intellektuaalomandist ning arvestades Eestis kohtutest läbi käinud ärisaladuse rikkumise kaasuseid ning ärisaladuse üldisi erinevusi võrreldes intellektuaalomandi õigustega, tuleks praegusel juhul eelistada ärisaladuse kaitse loomist muude meetmetega ning mitte lugeda ärisaladust tööstusomandi alaliigiks, ehkki ärisaladusel on ka küllaltki palju sarnasusi teiste intellektuaalomandi õigustega.

2. Ärisaladuse rikkumise kriminaliseerimine

2.1. Ärisaladuse karistusõigusliku regulatsiooni vajalikkus

Pooley ja Lemley on oma artiklis välja toonud tsiviilõigusliku ja kriminaalõigusliku regulatsiooni peamise erinevusena tõendamiskoormuse. Karistusõiguses peab süüdistaja tõendama iga süüdistuses esineva asjaolu nii, et seda saaks kindlusega külgneva tõenäosusega väita, ehk kahtluse korral tuleb asjaolusid tõlgendada süüdistatava kasuks. Tsiviilõiguses aga on tõendamiskoormus väiksem ning kohtunik hindab, kumma osapoole versioon juhtunust on paremini tõendatud. Mitmed kaitsjad ja kannatanud, kes on harjunud oma õigusi kaitsma tsiviilkohtumenetluses, ei pruugi mõista, kui suur on tegelik tõendamiskoormus karistusõiguses.[49] Eesti kriminaalmenetluses on KrMS § 7 lõikes 3 samuti sätestatud, et kõrvaldamata kahtlus tuleb tõlgendada isiku kasuks. See põhimõte kuulub Eesti seadusandluses süütuse presumptsiooni alla. See sama, *in dubio pro reo* põhimõte, on sätestatud ka Põhiseaduse § 22. Eelnev tähendab ühtlasi seda, et kriminaalmenetluses süüdimõistva otsuse tegemiseks on tõepoolest vajalik ilma kahtlusteta kõik süüdistuses esinevad asjaolud ära tõendada. Tsiviilkohtumenetluse seadustikust seesugust põhimõtet aga ei tulene, mis ei tähenda siiski seda, et tsiviilkohtus ärisaladuse kaitsmisega esitatud nõudeid tõendada ei tule. Samas on aga kriminaalmenetluses ärisaladuse rikkumise tõendamine mõnes mõttes kannatanu jaoks lihtsam. Kriminaalmenetluses on KrMS § 38 lõike 1 punkti 2 kohaselt kannatanul õigus esitada tsiviilhagi läbi uurimisasutuse või prokuratuuri ning vastavalt KrMS § 38^1 lõike 4 kohaselt on varalise nõudega tsiviilhagi esitamine kriminaalmenetluses riigilõivuvaba. Samuti on tsiviilhagi asjaolud tõendatud kriminaalmenetluses kogutud tõenditega. See aga tähendab seda, et kui prokuratuuri taotlusel on tõendite kogumiseks tehtud läbiotsimine isiku äriruumides, siis on seeläbi võimalik saada oluliselt kindlamad tõendid ärisaladuse rikkumise tõendamiseks, kui seda oleks võimalik saavutada eraõiguslikus korras. Tsiviilkohtumenetluses on olemas säte, mis käsitleb dokumentide väljanõudmist intellektuaalset omandit puudutava hagi korral (TsMS § 280), kuid seni, kuni Eesti õiguses ei käsitleta ärisaladust intellektuaalomandi valdkonda kuuluvana, ei ole võimalik neid tõendavaid dokumente ka rikkujalt välja nõuda. Praegu Eestis kehtiva regulatsiooni puhul on kriminaalmenetluses ärisaladuse rikkumisega seonduvate õiguste taastamine pigem odavam ja kindlam, kui seda on õiguste kaitsmine tsiviilkohtumenetluse korras.

[49] Pooley, James. A.H., Lemley, Mark. A., Toren, Peter, J., Understanding the Economic Espionage act of 1996. Texas intellectual property law journal 5. United States of America, Texas: The State Bar 177 1996-1997, p 206. Veebis kättesaadav: http://heinonline.org/HOL/Page?handle=hein.journals/tipj5&collection=journals&startid=&endid=250&id=197

Ärisaladuse kaitse regulatsioon on oluline majandusarengu ja ettevõtete innovaatilisuse tagamise seisukohalt. Olukorras, kus ettevõtjaid ümbritseb turvaline majanduskeskkond, on ettevõtjad võimelised rohkem investeerima toodete arengusse. See sama idee on välja toodud ka uuringus, mis näitab, et nii tänu Aasia turult pärinevatele piraatkaupadele kui ka ebaühtlasele ärisaladuse kaitsele Euroopa Liidu territooriumil on ettevõtjate motivatsioon arengusse panustamisel märgatavalt vähenenud. Madal ja nõrk ärisaladuse kaitse demotiveerib ettevõtjaid toodete arengusse panustamast.[50] Robert G. Bone on aga leidnud, et ärisaladuse kaitse regulatsiooniga kaasnev kasu ei pruugi ületada sellega kaasnevat kulu. Näiteks võib ärisaladuse kaitse ohustada patendiseaduse poolt patentidele tagatud kaitse ja uute leiutiste loomise tasakaalu, kuna ärisaladuse kaitse võimaldaks ilma avalikustamata tootele küllaltki suurt kaitseulatust.[51] Patendiseaduse § 37 lõike 1 kohaselt kestab patendikaitse kuni 20 aastat ning pärast seda patenditud toodet enam kaitsta ei saa ning ettevõtjatel on lubatud samasuguse tootega turule tulla. Autori- ja tööstusomandiõigused tagavad ettevõtjate huvi uuringute tegemise ja arendamise vastu seeläbi, et autor teenib tulu oma leiutise, teose või muu sellise pealt seetõttu, et konkurents on seadusega piiratud.[52] Samas, nagu juba öeldud, on kaitse piiratud teatud aastatega ning pärast seda kaitse kaob. Seesugune piiratud kaitse peaks võimaldama majanduse arengut vähemalt selles mõttes, et sama toodet ei peaks mitu korda algusest alates uuesti leiutama hakkama. Ilmselt peab Robert Bone ärisaladuse kaitsekuludega seoses silmas ka seda, et ärisaladusena mingit toodangut või informatsiooni kaitstes, võib kaitseulatus kesta oluliselt kauem, kui see kestab näiteks patendi puhul ning sellisel juhul ei tule turule uut informatsiooni piisavalt kiiresti, mis tähendaks seda, et majanduse kiirem areng oleks mõnevõrra pärsitud.

Ärisaladuse efektiivse kaitse positiivse küljena on sageli välja toodud ka seda, et ärisaladuse tugevam kaitse võimaldaks ettevõtjatel investeerida suurema summa toodete arendamisse, kuna hirm oma investeerimistulemustest ilma jääda on väiksem ning ettevõtjad ei pea oma ärisaladuse kaitsmiseks võtma kasutusele kulukaid ja keerukaid kaitsemeetmeid, vaid piisaks lihtsalt mõistlike kaitsemeetmete rakendamisest. Samuti suurendab ärisaladuse regulatsiooni olemasolu nii töötajate kui äripartnerite teadlikkust ärisaladuse rikkumise tagajärgedest, mis omakorda toimiks preventiivse meetmena.[53] Ilmselt omaksid mõningal määral ärisaladuse

[50] Cronin, C. et al. Trade Secrets: European Union Challenge in a Global Economy, lk 8. International Fragrance Association, 2012. Arvutivõrgus kättesaadav: http://www.ifraorg.org/view_document.aspx?docId=22900

[51] Bone, Robert G., The (Still) Shaky Foundations of Trade Secret Law. United States of America: Texas Law Review; U of Texas Law, Public Law Research Paper No. 563, June 1, 2014. p 7-8. Veebis kättesaadav: http://ssrn.com/abstract=2445024

[52] Lemley, Mark, A. (30), lk 329.

[53] Friedman et.al, "Some Economics of Trade Secret Law", Journal of Economic Perspectives, 5 (Winter), pp. 61-72 lk 67 Arvutivõrgus kättesaadav: http://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.5.1.61

rikkumise suhtes preventiivset toimet ka tsiviilõiguslikud õiguskaitsevahendid, kuid karistusõiguslikud õiguskaitsevahendid on üldiselt omanud suuremat mõju rikkumiste vähendamisele.

Robert. G. Bone aga leiab, et ärisaladuse tugevama kaitse mõju investeeringute suurenemisele ei ole kuidagi tõendatud, vaid tegelikkuses võib olla olukord hoopis vastupidine. Nimelt peavad need ettevõtjad, kes soovivad kellegi teise ärisaladust omandada, suurendama kulutusi, et sellele ärisaladusele ligipääsu saada ning arvestades ka seda, et ärisaladuse rikkumise korral on väga oluline selle võimalikult kiire avastamine, siis peavad ärisaladust omavad ettevõtjad suurendama oma kulutusi selleks, et teha võimalik ärisaladuse rikkumine ilma suurema viivituseta kindlaks. See aga võiks omakorda viia olukorrani, kus ebaseaduslikult ärisaladusele juurde pääseda sooviv ettevõtja suurendaks veelgi oma kulutusi selleks, et vähendada võimalikku ärisaladuse ebaseadusliku omandamisega seotud vahelejäämise riski. Seetõttu võivad ettevõtjad ärisaladuse parema kaitsega seoses küll säästa mõningaid kulutusi, kuid sisuliselt ei muutu majanduslikus perspektiivis midagi, kuna neid sääste ei suunata toote arendamisele, vaid parema kaitse tagamisele.[54]

Olenemata sellest, et mitmetes ärisaladuse regulatsiooni teemalistes artiklites on leitud, et ärisaladuse efektiivne kaitse soodustab ettevõtjate innovatsiooni ning tagab neile suurema hulga vabu vahendeid investeeringuteks, ei tohi siiski unustada, et ärisaladuse iseseisev avastamine või selle teadasaamine pöördprojekteerimise teel ei ole karistatav. See sama on öeldud ka Euroopa Liidu direktiivi 2016/943 artikli 3 lõikes 1, mille kohaselt ärisaladuse iseseisev avastamine või loomine ning üldsusele kättesaadavaks tehtud toote või eseme jälgimine, uurimine ja demonteerimine peavad olema ühenduse liikmete regulatsioonide kohaselt lubatavad. See tähendab seda, et täielik ärisaladuse kaitse ettevõtjatele ei ole tagatud.

James, A. Johnson on leidnud, et ärisaladuse kaitse on vähemalt sama oluline kui patendi, autoriõiguse või kaubamärgi kaitse. Patendi kaitse on oluline ja vajalik, kuid juhul kui selle alusidee tuleneb mingist kindlast programmist, meetodist või protsessist, millel on omaette majanduslik väärtus, siis on ettevõtjale oluline ka selle meetodi või protsessi kaitsmine ning seda selleks, et vältida kulukaid vaidlusi juhul, kui ettevõtja idee ära varastatakse[55]. See näitab seda, et ettevõtjale oluliseks ja kaitset vajavaks väärtuseks peetakse ka seesugust informatsiooni, mis ei pruugi olla patendina kaitstav. Samuti on Johnson toonud välja ärisaladuse kaitse vajalikkuse juhul, kui ettevõtja alles loob patenteeritavat toodet ning

[54] Bone, Robert G., (51), lk 9-10
[55] Johnson, James. A. Keeping Your Secrets Secret. New York State Bar Assoc. Journal, Vol. 87, No. 6. July/August, p 25. United States of America: New York 2015

mõningatel juhtudel võib selle loomine aega võtta aastaid ning selle perioodi jooksul puudub ettevõtte loodaval toodangul reaalne kaitse, mistõttu on seda oluline senikaua salajas hoida ning kaitsta ärisaladusena.[56] Näiteks võib seesugust ärisaladuse kaitset vajada mõni hooajalise tootmisega ese, mille eesmärgiks ongi tagada ettevõtjale konkurentsieelis turul ajutiselt, läbi selle, et konkurendid ei tea, missuguse tootega ettevõte turule tuleb. Seesugusteks toodeteks võivad olla näiteks mänguasjad, mis on mõeldud lastele jõuludeks ning mille osas on ettevõtjad uuringuid teinud, selgitamaks välja, mis parasjagu populaarne ja edukas toode võiks olla. Samasugused tooted võivad olla näiteks uued mobiiltelefonid, mille uuendused hoitakse salajas kuni toodangu väljastamiseni.

G. Moohr on öelnud, et ärisaladuse karistusõiguslik regulatsioon võib pärssida majanduse arengut, kuna töötajad, kes on seadusekuulekad, ei julge enam töökohti vahetada või ise ettevõtlusega tegelema hakata, kuna sellega kaasnevad suuremad riskid kuidagiviisi endise tööandja ärisaladust kahjustada. Samuti on oht, et juhul, kui ärisaladuse rikkumise eest karistatakse ka kolmandaid isikuid, kes teadvalt omandasid või said oma töötaja kaudu teise ettevõtja ärisaladusest teadlikuks, ei julge ettevõtjad enam konkurentide töötajaid tööle võtta, kuna täpne piir töötaja omandatud kogemuste (mida võib kasutada ka edaspidises äritegevuses) ja ettevõtja ärisaladuse vahel ei ole selgelt määratletud. Olenevalt ärisaladuse karistusõiguslikust kaitsest, võivad head töötajad tunda vähem huvi teistes ettevõtetes enesearendamise vastu ning ärisaladuse karistusõiguslik kaitse võib olla pigem suunatud ettevõtja huvide kaitsele kui töötajate vaba liikumise ja arenemise kaitsele. Lisaks on võimalik, et väga tugeva ärisaladuse kaitse korral võivad ettevõtjad kasutada väiksemal määral patenteerimist ja sellest tulenevat kaitset ning rohkemal määral ärisaladuse kaitset. Sellisel juhul aga liiguks turul jällegi vähem informatsiooni ning sellest tulenevalt oleks ilmselt ka teiste ettevõtjate ja majanduse areng märgatavalt aeglasem.[57] See tähendab eelkõige seda, et ärisaladuse karistusõigusliku regulatsiooni kehtestamisel tuleks pöörata tähelepanu mõlema osapoole, nii ettevõtjate kui ka töötajate huvidele võrdselt, et oleks tagatud tasakaal majanduses. Vastasel juhul, ehk olukorras, kus huvide tasakaal on paigast ära, ei pruugi ärisaladuse kaitse täita enam oma peamist eesmärki, milleks on majanduse areng ja innovatsiooni edendamine.

Samuti on õiguskirjanduses leitud, et enne igasugu ärisaladuse kaitse tugevat reguleerimist peab eelkõige üldse olema selge, kui palju ärisaladuse rikkumisi esineb. Vastasel juhul võib ärisaladuse kaitse minna majandusele kalliks maksma. Samas ei ole selge, kuidas oleks võimalik uurida, kui palju ärisaladuse rikkumisi esineb ning kui suure kahju nad endaga kaasa

[56] *Ibid*, (55) lk 25
[57] Moohr, Geraldine S. (24), 916

toovad, kuna näiteks juhul, kui ettevõtjate käest küsida nende ärisaladuste rikkumiste ja tekitatud kahju kohta, ei saa olla veendunud, et ettevõtjad oma ärisaladust ja selle väärtust adekvaatselt hindavad, samuti ei pruugi nad teha vahet seaduslikul ja ebaseaduslikul ärisaladuse omandamise viisil.[58] James A. Johnson on öelnud, et reaalsuses on ärisaladust omaval ettevõtjal õigus ärisaladuse kaitsemeetmeid kasutada üksnes kahte sorti isikute vastu. Esimesse gruppi kuuluvad isikud, kes on seotud konfidentsiaalsuslepingute või muude piirangutega ärisaladuse avaldamisel ning teise gruppi kuuluvad isikud, kes püüavad ettevõtja ärisaladust omandada ebaseaduslikul viisil.[59] Samamoodi on ärisaladuse rikkumisi jaotanud Chatterjee, kes on öelnud, et ärisaladuse rikkumine võib tuleneda põhiliselt kahest erinevast situatsioonist. Ühel juhul on isikule usaldatud ärisaladus selle isiku poolt, kes ärisaladust omab ning sellisel juhul ületab rikkumine mingisuguseid sätestatud piiranguid ärisaladuse kasutamisel ja hoidmisel. Teisel juhul on tegemist olukorraga, kus isik juba omandab ärisaladuse läbi kõlbmatute meetodite, näiteks varastab ärisaladuse või omandab selle läbi isiku, kelle kohta ta teab, et ärisaladus on teatavaks saanud ebaausa käitumise tulemusena.[60] Järgnevates osades on täpsemalt selgitatud neid rikkumise viise eraldi ning võimalusi ärisaladuse kaitse reguleerimiseks ka tulenevalt ärisaladuse olemusest.

2.2. Ärisaladuse liigitamise tähtsus karistusõiguslikust aspektist

Lisaks eelpool kirjeldatud ärisaladuse kaitse kaheks kategoriseerimise meetodile, kus ärisaladust võib ühest küljest kaitsta usalduse kuritarvitamise vastu ning teisest küljest ärisaladusele ebaseadusliku ligipääsu saamise vastu, tuleb karistusõigusliku regulatsiooni puhul tähelepanu pöörata ka ärisaladuse olemusele. Ärisaladuse olemusest võib sõltuda nii rikkuja teo raskusaste kui ka ettevõtja poolt kantava kahju ulatus. Saksa õiguses tehakse suuremal või vähemal määral vahet erinevatel ärisaladuse liikidel. Eristatakse ärisaladusi, mis puudutavad majandustegevust, nagu näiteks kliendinimekirjad, raamatupidamise dokumendid, allahindluse ja reklaami meetodid, hinnakirjade loomise tingimused, ning ärisaladusi, mis puudutavad *know-how'd* ehk sisuliselt praktilised teadmised, millele ei ole patenti taotletud, kuid mis on saadud läbi kogemuste ja katsetuste, nagu näiteks tootmisprotsessid, disaini ideed, järelevalve- ja

[58] Bone, Robert G., Secondary Liability for Trade Secret Misappropriation: A Comment, Santa Clara Computer and High Tech Law Journal 529, lk 531-533. Ameerika Ühendriigid: California 2006. Veebis kättesaadav: http://heinonline.org/HOL/Page?handle=hein.journals/sccj22&g_sent=1&collection=journals&id=539
[59] Johnson, James, (55), lk 25
[60] Chatterjee, N. Should Trade Secret Appropriation be Criminalized? Hastings Communication and Entertainment Law Yournal Vol. 19, No 873, p 863. United States of America: California, O'Brien Center for Scholarly Publications, 1996-1997

majandusanalüüside tulemused, arvutiprogrammid, programmikoodid.[61] Samas ei ole Saksa õiguses selline vahetegu ei määrav ega vajalik, kuna mõlema saladuse rikkumise korral rakendub sama norm ning ühesugune vastutuse ulatus[62]. Ka Eestis on karistusseadustiku kommenteeritud väljaandes jaotatud ärisaladused kolmeks liigiks: *know-how*, turundustegevuse ärisaladused ning ärisaladused muudes ettevõtjasisestes valdkondades[63], millest eelmises peatükis ka juttu oli, kuid nii nagu Saksamaal, ei tehta ka Eestis tegelikkuses erinevate ärisaladuse liikide vahel vahet ning see ei ole praktikas ka oluline, kuna iga ärisaladuse rikkumise eest on ette nähtud samasugune karistus.

Võrdluseks võiks siinkohal välja tuua ärisaladuse karistusõigusliku regulatsiooni Prantsusmaal, kus seesugune erinevate ärisaladuse liikide täpne piiritlemine mängib olulist rolli. Prantsuse õiguses on karistusõigusliku normi kaitse suunatud ainult sellisele ärisaladusele, mis on nii-öelda tehasesaladus, ehk hõlmab üksnes originaalseid tootmisprotsesse, mis loovad ettevõtjale praktilise või kaubandusliku eelise, mida kasutatakse tööstuses ja mis on hoitud saladuses. Tehasesaladuse juurde kuuluvad kõik erinevad tootmismeetodid ja materjalid, mida kasutatakse tootmisel, kuid näiteks kliendinimekirjad ja muud seesugused majanduslikku valdkonda kuuluvad ärisaladused ei ole karistusõiguslikult kaitstavad. Teiste ärisaladusele rakendatavate kaitsekriteeriumite poolest on Prantsuse õigus sarnane Eesti õiguse regulatsiooniga, see tähendab, et karistusõiguslikult saavad vastutada üksnes ettevõtja töötajad või töösuhtega sarnases suhtes olevad isikud, kellele tagati juurdepääs ärisaladusele seoses töö- või ametiülesannetega.[64] See tähendab, et Prantsusmaal on ärisaladuse karistusõiguslik regulatsioon oluliselt kitsam kui Eestis ning teiste liigituste alla kuuluva ärisaladuse rikkumise korral tuleb abi saamiseks pöörduda tsiviil- või konkurentsiõiguse normide poole.

Ameerika ühendriikides jaotuvad ärisaladused peamiselt kaheks alaliigiks, milleks on tehnilised ärisaladused ja turundustegevust puudutavad ärisaladused. Esialgu hõlmas ärisaladuse kaitse üksnes tehnilist laadi ärisaladusi[65]. Ilmselt põhjustab tehnilist laadi ärisaladuse rikkumine suuremat kahju ettevõtjale, kui turundustegevust puudutava ärisaladuse rikkumine ning lisaks, nagu juba eelpool ka välja toodud sai, siis panustavad ettevõtjad turundusstrateegiate loomisele ja efektiivse hinnataktika kehtestamisele ka juhul, kui see teave ei ole seadusega kaitstav. Ameerika Ühendriikide ärisaladuse kaitse on aga aja jooksul laienenud ka turundusteavet puudutavale informatsioonile. Kuna ärisaladust on aastate jooksul

[61] Köhler/Bornkamm, Gesetz gegen den unlauteren Wettbewerb (UWG), Kommentar, 35 Auflage (2017), Beck, München. Veebis kättesaadav beck-online.beck.de
[62] Henning Harte-Bavendamm *et al* (19)
[63] Vutt, A. KarS kommenteeritud väljaanne (32) § 377 p 2.3
[64] Caenegem, William van (5) lk 129-130
[65] *Ibid*, (5), lk 103

püütud täpsustada ja luua mingeid kriteeriumeid, siis on praegu kehtiva UTSA kohaselt ärisaladusena kaitstav informatsioon, mis hõlmab valemeid, andmebaase, programme, seadmeid, meetodeid, tehnikaid või protsesse, kuid see ei välista siiski turundusliku sisuga ärisaladuse kaitse olemasolu, kuigi on ilmne, et UTSA regulatsioon on pigem kaldu tehnilist laadi ärisaladuse kaitsmise poole ning ka enamik ärisaladuse rikkumisega seonduvaid kaasuseid Ameerika Ühendriikides on siiski seotud tehnilist laadi ärisaladuse rikkumisega.[66] Seega ka Ameerika Ühendriikides on ärisaladused oma olemuse järgi ära jaotatud, kuid otsest karistusõigusliku kaitse välistamist liigipõhiselt ei esine, nii nagu see on Prantsusmaal. Pigem on ilmselt kohtud ja ühiskond suunatud tehnilist laadi ärisaladuste tugevamale kaitsele, kuid samas on kaitse tagatud ka teise sisuga ärisaladustele, juhul, kui on täidetud ärisaladuse kaitseks nõutavad kriteeriumid, milleks on ärisaladuse väärtus, mis tagab konkurentsieelise, selle salajasus ja ettevõtja poolne pingutus ärisaladust salajas hoida.

Rootsi õiguses ärisaladuse erinevaid liike ei eristata. Rootsi ärisaladuse kaitse akti kohaselt loetakse ärisaladuseks äri- või tööstusega seonduvat informatsiooni, mida isik kasutab ärilistel või tööstuslikel eesmärkidel ja mida see isik soovib hoida saladuses ning selle informatsiooni avalikustamine kahjustaks tõenäoliselt selle isiku konkurentsivõimet[67]. Eelnevad käsitlused näitavad, et erinevaid lähtekohti ärisaladuse karistusõigusliku regulatsiooni kehtestamiseks on mitmeid ning ühe võimaliku lahendusena võib olla ärisaladuse reguleerimine lähtuvalt ärisaladuse liigist. Iga riigi seadusandluse otsustada jääb see, kui suurel määral on mingi käitumise karistusõiguslik regulatsioon vajalik ning kuivõrd ulatuslikult on riigil õigus sekkuda majandustegevusse ning kehtestada nii-öelda hoiatusnorme õiguskuuleka käitumise tagamise eesmärgil ning millises ulatuses võib samasuguse käitumise reguleerida üksnes lepingute ja tsiviilõiguse normidega.

2.3. Ärisaladuse rikkumine usaldust kuritarvitades

Karistusseadustiku kommenteeritud väljaande kohaselt tuleneb usaldusseisund isiku hoolsus- ja järelevalvekohustusest teise isiku vara suhtes.[68] Eesti õiguses tuleneb töötaja hoolsus- ja lojaalsuskohustus oma tööandja suhtes töölepinguseadusest. Samas võib seesugune hoolsuskohustus tuleneda ka tööandja ja töötaja vahel sõlmitud lepingust või ettevõtja sõlmitud lepingust koostööpartneriga. Seega võib öelda, et need teod, millega ärisaladust rikutakse ei ole

[66] *Ibid* (5), lk 111
[67] Act on the Protection of Trade Secrets. (Act 1990:409, of May 31, 1990). Article 1 Veebis kättesaadav: http://www.wipo.int/edocs/lexdocs/laws/en/se/se005en.pdf
[68] Sootak, J. KarS Kommenteeritud väljaanne. IV trükk 2015 § 217^2 p 4

iseenesest karistatavad, vaid ärisaladuse rikkumise karistatavus tuleneb mingisuguse ühiskonnas aktsepteeritava käitumismalli rikkumisest, näiteks lojaalsuskohustuse rikkumisest.

Ameerika Ühendriikide kõrgeim kohus leidis oma lahendis *Kewanee Oil Co. v. Bicron Corp,* et ärisaladuse kaitsmise üks põhimõtetest on tagada aktsepteeritav, aus ja heas usus käitumine majandustehingute tegemisel.[69] Juhul, kui pidada ärisaladuse kaitseks loodud regulatsiooni pigem ausa käitumise regulaatorina, siis põhineks ärisaladuse olemus justkui mingitele isikutevahelistele suhetele, mitte mingi asja või õiguse kaitsele.

Isikutevahelised suhted, millest rikkumised tulenevad, on sageli reguleeritud teatud lepingutega. Näiteks sõlmivad ettevõtjad koostööpartneritega erinevaid lepinguid, milles sätestatakse ka konfidentsiaalsuskohustus ning selle kohustuse rikkumisest tulenev vastutus. Samas võib konfidentsiaalsuskohustus tuleneda ka mõistliku inimese arusaamisvõimest, ehk kui isik pidi aru saama, et tegemist on ettevõtja ärisaladusega ning ettevõtja sooviks on, et see teave jääb saladuseks, siis võib konfidentsiaalsuskohustuse tuletada ka vastavast olukorrast ning lepingu sõlmimine ei pruugi olla nõutav.[70] Näiteks karistusseadustik ei sea ärisaladuse rikkumise eest sätestatud vastutust sõltuvusse konfidentsiaalsuskohustust sisaldava lepingu sõlmimisest. Samas peab karistusseadustiku regulatsiooni kohaldamiseks esinema töösuhe või töösuhtega sarnane suhe ning sageli on töösuhtes ärisaladuse hoidmise kohustus lepinguga reguleeritud. Üldiselt peab tööandja töölepingus lähtuvalt TLS § 22, § 6 lõikest 3 ja § 5 kirjalikult fikseerima tööandja kohustuse ärisaladuse hoidmiseks, kuid samas kohustab TLS § 15 lõige 1 töötajat ka käituma tööandja suhtes lojaalselt, mis tähendab seda, et reaalsuses peaks olema võimalik ärisaladuse rikkumise eest vastutusele võtta ilma kirjalikult ärisaladuse hoidmiskohustuses kokku leppimata, kui töötajale pidid tööandja huvid ilmsed olema.

Kõige tugevamad ja selgemad isikutevahelised suhted, kus võib ka üpriski sageli esineda usalduse kuritarvitamist, on töösuhted või töösuhetega sarnased suhted. On ilmne, et ärisaladusele on ettevõtte töötajatel kõige lihtsam ligipääsu saada ning seega on neil ka kõige lihtsam seda rikkuda. Ärisaladuse kaitsemeetmed, mis on suunatud töötajate poolse rikkumise ärahoidmiseks, peaksid üldiselt seeläbi aitama kaasa ka väljapoolt ettevõtet tulenevate rikkumiste vähendamisele.[71] Väljapoolt ettevõtet tulenevad ärisaladuse rikkumised võivad olla näiteks juhud, kus ettevõtja endine töötaja võtab ärisaladuse uude ettevõttesse kaasa ning uus tööandja kasutab oma tegevuses teadlikult võõrast ärisaladust, mis jõudis temani läbi töötaja.

[69] Ameerika Ühendriikide Ülemkohus. - Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470 (1974)
[70] Godfrey, Eleanore, R. Inevitable Disclosure of Trade Secrets: Employee Mobility v. Employer's Rights, lk 165, Journal of High Technology Law Volume 161, Number 3. Ameerika Ühendriigid: Boston, 2004
Martin, Derek P, An Employer's Guide to Protecting Trade Secrets from Employee Misappropriation lk 949, Brigham Young University law review 1993/949. Veebis kättesaadav: http://heinonline.org/HOL/Page?handle=hein.journals/byulr1993&g_sent=1&collection=journals&id=959

Seega, kui ettevõtja suudab ära hoida oma endise töötaja rikkumise, siis ei toimu ka rikkumist uue tööandja poolt.

Ameerika Ühendriikides on kasutusel nö vältimatu avaldamise doktriin[72], mis võimaldab tööandjal töötaja konkurendi juurde tööle minemist takistada läbi selle, et tööandja tõendab ära, et töötaja teab tema ärisaladust ning juhul, kui ta läheb konkureerivasse ettevõttesse tööle ja hakkab täitma sarnaseid tööülesandeid, siis on töötajal võimatu vältida ärisaladuse avalikustamist uuele tööandjale ning sellega kaasneb ettevõttele oluline kahju. Pärast ettevõtja pöördumist kohtu poole, hindab kohus, kui suur on võimalus, et töötaja peab ärisaladuse uuele ettevõtjale tööülesannete täitmisel avaldama ning samas peab kohus arvestama ka töötaja huve vabalt oma töökohta valida. Juhul, kui kohus leiab, et ettevõte kaotaks väga olulise ärisaladuse, siis võib kohus keelata töötajal uue tööandja juurde tööle minemise. Esialgu kasutati seda doktriini üksnes tehniliste ärisaladuste kaitseks, kuid nüüdseks on see laienenud ka igasugusele muule ärisaladusena käsitletavale teabele, nagu näiteks finantsinformatsioonile või turundusstrateegiatele. Esialgu kaldusid kohtud pigem töötajate kasuks otsuseid langetama, kuid hiljem on kohtud ka keelanud töötajatel konkurendi juurde tööle asumise.[73] Ilmselt võib seesuguse keeluga tõmmata paralleeli Eesti õiguses võimaliku konkurentsikeelu kokkuleppega.

Ärisaladuse karistusõiguslik regulatsioon karistusseadustiku §-s 377 sätestab vastutuse ärisaladuse õigustamatu avaldamise ja kasutamise eest. Selleks, et analüüsida ärisaladuse kaitse tõhusust, tuleb eelkõige süüvida karistusseadustikus sätestatud normi eeldustesse. Normi sõnastuse kohaselt on karistatav töö- või ametiülesannetega teatavaks saanud ärisaladuse avaldamine või kasutamine ilma ettevõtja loata, kui see on toime pandud ärilisel või kahju tekitamise eesmärgil. Seaduse sõnastusest on selgelt väljaloetavad piirangud nii ärisaladuse teatavaks saamise viisile kui ka ärisaladuse avaldamise ja kasutamise eesmärgile. See tähendab, et isik, kes ärisaladuse ilma ettevõtja loata avaldab või seda kasutab, peab olema ettevõtjaga töö- või ametialases seoses ning ärisaladus peab isikule teatavaks saama töö- ja ametiülesannete täitmisega, mis tähendab, et norm ei hõlma juhtumeid, kus töötaja ebaseaduslikult pääseb ligi ettevõtja ärisaladusele. Karistusseadustiku seletuskirja[74] kohaselt peetakse silmas isikuid, kes on ettevõtjaga seotud töö- või käsunduslepingu kaudu ning sellest tulenevalt on neil isikutel kohustus hoida ettevõtja ärisaladust. Sama seletuskirja kohaselt on seesuguste isikutena silmas peetud eelkõige ettevõtte juhtivtöötajaid ning järelevalve teostajaid (näiteks juhatuse liikmed,

[72] Inglise keeles *inevitable disclosure doctrine*
[73] Godfrey, Eleanore R., (68), lk 165-168. Vaata lisaks ka *A. Eastman Kodak Co. v. Power Film Products, Inc. (1919)* ja *PepsiCo, Inc. v. Redmond, 54 F.3d 1262 (7th Cir. 1995)*
[74] Riigikogu X koosseis. Karistusseadustiku ja selle muutmisega seonduvate seaduste muutmise seadus 931 SE, 07.06.2006 lk 56

nõukogu liikmed, audiitorid). Eelduslikult on just sellele isikute ringile töö- ja ametiülesannete täitmisel ligipääs ärisaladusele kõige ulatuslikum, kuid samas ei välista seadus ka muude töötajate vastutust ärisaladuse õigustamatu avaldamise ja kasutamise korral.

Karistusseadustiku kommenteeritud väljaande kohaselt tähendab ärisaladuse avaldamine selle teatavaks tegemist teistele isikutele ning kasutamise all peetakse silmas ärisaladuse kasutamist töötaja või ametniku enda poolt[75]. Samas tuleb meeles pidada ka seda, et ärisaladuse avaldamisel ja kasutamisel peab olema kas ettevõtjat kahjustav eesmärk või äriline eesmärk. See tähendab, et tegemist peab olema teadliku ja tahtliku teoga, kusjuures kasu saamise või kahju tekitamise osas peab olema kavatsetus. Normi sõnastuse kohaselt piisab süüteo toimepanemiseks ärisaladuse avaldamisest või kasutamisest, kuid nõutav ei ole ettevõtjale kahju tekkimine. Võttes arvesse varem mainitud Riigikohtu Kriminaalkolleegiumi 08.06.2009 tehtud otsust, tuleb normi sõnastuse pinnalt tehtud järeldust siiski täpsustada. Süüteo toimepanemiseks piisab küll ärisaladuse avaldamisest kahju tekitamise eesmärgil või ärilisel eesmärgil, kuid selleks tuleb kindlasti ka eesmärgi olemasolu ära näidata. Olukorras, kus töötaja on ettevõtja ärisaladust (nt klientide andmebaasi või hinnapakkumisi) avaldanud kolmandale isikule, kuid kui see kolmas isik nende andmetega midagi ette ei võta, siis on keeruline tõendada, et ärisaladuse avaldamisel üldse oli mingi eesmärk. Seesugune olukord oli viimati mainitud kohtukaasuses[76], kus süüdistus ei suutnud ära tõendada, et andmed olid avaldatud ärilisel eesmärgil, kuna kolmas isik ei kasutanud saadud hinnapakkumise andmeid.

Karistusseadustiku kommenteeritud väljaandes on tõdetud, et KarS § 377 rakendusala võib reaalsuses jääda pigem väheseks just tänu ettevõtetes sõlmitud lepingutele ja konfidentsiaalsuskohustustele, millest tuleneb ka kahju hüvitamise kohustus[77]. Samas ei ole saladuse hoidmise kohustust sätestava lepingu olemasolu kuidagi piiranguks ka karistusõigusliku vastutuse tekkimisel. See tähendab, et isegi olukorras, kus ettevõtja on sõlminud töötaja või ametnikuga konfidentsiaalsus- ja ärisaladuse hoidmise kohustusega lepingu, võib nende lepingute rikkumise korral siiski alustada ka kriminaalmenetluse. Samas peaks karistusõigusliku vastutuse teke olema pigem erandlik ning KarS § 377 olema rakendatav vaid rasketel juhtudel. Riigi sekkumine majandustegevusse peaks olema vaba turumajanduse tingimustes võimalikult vähene ning seetõttu oleks otstarbekas lähtuda mingitest kindlatest kriteeriumitest karistusõigusliku vastutuse tekkimisel. Praegusel juhul ei ole seesuguseid

[75] Vutt, A. KarS kommenteeritud väljaanne. IV trükk 2015, § 377 p 4.1
[76] Vt RKKKo 3-1-1-46-09 p 10.5, 28.06.2009
[77] Vutt, A. KarS kommenteeritud väljaanne. IV trükk 2015, § 377 p 3

kriteeriumeid olemas ning näiteks ärisaladuse avalikustamisel, mis võib ühtlasi olla ka lepingurikkumine, ei ole välistatud ka isiku karistusõiguslik vastutus.

Üheks karistusõiguse regulatsiooni piiritlemise võimaluseks võiks olla kahju suurus, see tähendab, et olukorras, kus ettevõtja on ärisaladuse rikkumise tõttu kannatanud olulist kahju, võiks olla võimalik ka rikkuja kriminaalvastutus. Ühe võimalusena võib siinkohal näha mingi kahjusumma sätestamist, kuid samas võiks arvesse võtta ka rikkuja teo iseloomu, tema kavatsetust ning teo raskusastet, samuti ka ärisaladuse olemust ja ärisaladuse väärtust ettevõtja jaoks.

Saksa õiguses on ärisaladuse kaitseks Eesti õiguses sätestatuga sarnane säte konkurentsiseaduses, kuid on siiski karistusõiguslik, ehk sätestab rikkumise korral vangistuse või rahalise karistuse. Saksa õiguses on ärisaladuse säte, mis tuleneb UWG[78] artiklist 17 suhteliselt sarnane Eestis sätestatud normiga. Saksa säte ütleb sisuliselt, et isik vastutab ärisaladuse avaldamise eest ajal, kui ta on ettevõtjaga tööalases suhtes ning avaldab ilma ettevõtja loata ärisaladuse, mis temale usaldati või millele tal oli ligipääs tööülesannete täitmise käigus ning kui ta teeb seda konkurentsi eesmärgil, isikliku kasu saamise eesmärgil, kolmandale isikule kasu toomise eesmärgil või sooviga tekitada kahju ettevõtjale[79]. Esmapilgul näivad Eesti ja Saksa õiguse sätted küllaltki ühesugused, kuid tegelikkuses esineb mõningaid olulisi erinevusi. Erinevuste täpsemaks mõistmiseks on ilmselt otstarbekas süüvida Saksa õiguse vastavatesse kommentaaridesse.

2.3.1. Ärisaladuse avaldamine ja kasutamine

Tulles tagasi Eesti sätte ja Saksa sätte võrdluse juurde, siis esimene erinevus, mis silma hakkab, on see, et Eesti karistusõiguse regulatsioon keelustab nii ärisaladuse avaldamise kui ka kasutamise, kuid Saksa normis on viide üksnes avaldamisele *(mitteilung)*. UWG § 17 kommentaarid kinnitavad, et Saksa õiguses on tõepoolest kriminaliseeritud üksnes ärisaladuse õigustamatu avaldamine ning igasugune muu tegevus, kasvõi ettevalmistav tegevus ärisaladuse kasutamiseks, millega toodaks kasu ärisaladuse rikkujale või kolmandale osapoolele, ei ole selle sättega hõlmatud. Avaldamiseks peetakse ärisaladuse teatavaks tegemist viisil, mille tagajärjeks võib olla ärisaladuse avalikuks saamine või teise isiku poolt kasutusse võtmine. Samas, piisab üksnes sellest, kui kolmas osapool on ärisaladuse teada saanud ning selle kasutuselevõtt ei oma tähtsust. Ärisaladuse avaldamine võib toimuda ka ettevõtte siseselt,

[78] Saksa keeles Gesetz gegen den unlauteren Wettbewerb, inglise keelde tõlgituna The Act Against Unfair Competition. Veebis kättesaadav: http://www.gesetze-im-internet.de/englisch_uwg/englisch_uwg.html#p0139
[79] Saksa keeles veebis kättesaadav: http://www.gesetze-im-internet.de/uwg_2004/__17.html

näiteks olukorras, kus kõrgemal positsioonil olev töötaja avaldab ärisaladuse madalamal positsioonil olevale töötajale. Juhul, kui madalamal positsioonil olev töötaja juba ärisaladust teadis ning ärisaladuse avaldaja oli kursis teise töötaja informeeritusega, siis loomulikult rikkumine puudub. Samas olukorras, kus madalama astme töötaja küll teadis ärisaladust, kuid avaldaja uskus, et ta seda ei tea, võib olla võimalik avaldaja vastutusele võtmine ärisaladuse avaldamise katse järgi[80]. Võrreldes eelpool kirjeldatud olukorda Eesti õiguse järgi, siis KarS § 377 juures küll puudub otsene märge katse karistatavuse kohta ning Saksa õiguses on otsene viide olemas UWG § 17 lg 3, kuid Eesti õiguses on katse reguleeritud üldiselt üldosa sätete all ning kuritegude puhul eriosa koosseisu juures katse karistatavusele eraldi ei viidata. Karistusseadustiku kommentaari kohaselt on süütegu lõpule viidud, kui ärisaladus on avaldatud või seda kasutatakse, samas ei ole avaldamise korral oluline, kas isik, kellele ärisaladuse teatavaks sai, seda ka mõistab või kasutab[81]. Siinkohal tuleb meenutada eelpool mainitud Riigikohtu otsust, kus seetõttu, et teadasaaja ärisaladust ei kasutanud, jäi äriline või kahju tekitamise eesmärk tõendamata ning seega puudus lõpuleviidud tegu. KarS § 26 lg 1 kohaselt võiks seesuguse ärisaladuse avaldamise katse, kus isik juba teab ärisaladust, liigitada pigem kõlbmatuks süüteokatseks[82]. Samas ei tähenda kõlbmatu süüteokatse seda, et ilmtingimata peaks selline tegu tooma kaasa ka väiksema karistuse.

Isegi juhul, kui tegu ei ole karistatav karistusseadustiku kohaselt, on töötajatel siiski töölepingust ja muudest sõlmitud lepingutest tulenev konfidentsiaalsus- ja lojaalsuskohustus. Samamoodi on olukord ka Saksa õiguses. UWG § 17 kommentaari kohaselt kaasneb vastutus igasuguse tööandja reetmise eest töötaja poolt, kui mitte karistusõiguslik, siis tsiviilõigusest tulenev. Vastutust välistavaks asjaoluks on näiteks EL direktiivi 2016/943 artiklis 5 nimetatud juhtumid[83]. Direktiivi artikli 5 kohaselt peavad liikmesriigid õiguskaitsevahendite kohaldamise taotluse jätma läbi vaatamata, kui ärisaladuse ebaseaduslik avaldamine, kasutamine või omandamine toimus a) sõna- ja teabevabaduse õiguste teostamiseks, b) ebaseadusliku tegevuse paljastamiseks, kui kostja tegutses üldsuse huvides, c) kui ärisaladuse avalikustasid töötajad oma esindajale ja see oli vajalik nende ülesannete täitmiseks või d) tunnustatud õigustatud huvi kaitsmise eesmärgil. Ehkki Eesti õiguses puudub nii otsene viide vastutust välistavatele asjaoludele kui ka seadusesätte kommentaar, mis sellele viitaks ja erandite rakendamine on jäetud puhtalt kohtu kanda, siis tegelikkuses võiks oletada, et juhul, kui on täidetud üks või mitu EL-i direktiivi 2016/943 artikkel 5 kriteeriumitest ärisaladuse avaldamisel, siis peaks ühtlasi

[80] Henning Harte-Bavendamm *et al* (19)
[81] Vutt, A. KarS kommenteeritud väljaanne. IV trükk 2015, § 377 p 5
[82] Vt ka RKKKo otsus nr 3-1-1-41-14 p 12 ja 12.2, kus ametiisik avaldas salastatud isikuandmeid, kuid kuna andmed olid varasemalt avalikustatud, ei õnnestunud ametnikul süütegu lõpule viia.
[83] Henning Harte-Bavendamm *et al* (*Unbefugte Mitteilung*), (19)

puuduma ka äriline või kahju tekitamise eesmärk ning sel juhul ei oleks KarS § 377 koosseis täidetud.

2.3.2. Ärisaladuse rikkumise aeg

Teine erinevus, mis Saksa sätte puhul silma hakkab, on see, et ärisaladuse avaldamine peab toimuma töö- või ametisuhte kestel *(während der Geltungsdauer des Dienstverhältnisses... mitteilt)*. UWG § 17 kommentaaride kohaselt tähendab see seda, et ärisaladuse õigustamatu avaldamine võib kaasa tuua kriminaalkaristuse üksnes juhul, kui seda on tehtud töösuhte kestuse ajal. See, kas isik täidab sel hetkel tööülesandeid, on kodus haiguslehel või on töölepingu ilma ette teatamata mõjuva põhjuseta üles öelnud, ei oma tähtsust. Oluline on reaalse töösuhte olemasolu. Samas, kui ettevõtja ütleb isikuga töölepingu erakorraliselt üles, kuid õiguslik alus selleks puudub, võib ta kaotada võimaluse karistusõiguslikule ärisaladuse kaitsele. Sellisel juhul jäävad ettevõtjale ärisaladuse rikkumise korral kasutada üksnes tsiviilõiguslikud õiguskaitsevahendid. Lisaks, olukorras, kus ettevõtja on töötajaga lepingu alusel kokku leppinud, et ärisaladuse avaldamise keeld kehtib ka pärast töösuhte lõppemist, ei pikenda seesugune kokkulepe aga siiski seaduse sättes mainitud „töö- või ametisuhte kestel“ perioodi. See tähendab, et seesugune lepinguline kokkulepe ei muuda karistusõigusliku sätte rakendamise perioodi pikemaks, vaid kui reaalne töösuhe on lõppenud ning endine töötaja pärast töösuhte lõppemist kas avaldab või kasutab ärisaladust õigustamatult, jäävad ettevõtjale üksnes tsiviilõiguslikud õiguskaitsevahendid.[84] Tuues siinkohal võrdluseks Eesti karistusõigusliku ärisaladuse kaitse sätte, võib selgelt öelda, et meie sättes puudub seesugune selge piir, millal on võimalik isik karistusõiguslikult vastutusele võtta. KarS § 377 kohaselt on oluline üksnes see, et isikule on ärisaladus teatavaks saanud töö-või ametiülesannete täitmisel, kuid avaldamise ja kasutamise kestust KarS § 377 kohaselt piiritletud ei ole. See tähendab aga seda, et isegi endise töötaja puhul võib tööandja igal ajal, kui talle näib, et endine töötaja kasutab või avaldab tema ärisaladuse, teha avalduse kriminaalmenetluse alustamiseks. Selline olukord võib aga saada väga piiravaks töötajale, kes soovib ametikohta vahetada, kuid sisuliselt samas valdkonnas edasi töötada. Isegi olukorras, kus töötajal puudub tahtmine ärisaladuse avaldamiseks, ei ole Eesti õiguses ka selgelt piiritletud, millised on töötaja ametiülesannete täitmisel omandatud kogemused ja oskusteave, mis kuulub sellele töötajale endale ning kuidas eristada sellest teabest ettevõtja ärisaladust. See aga tähendab, et tööandjal võib olla väga suur võim töötajat enda juures hoida ning seega takistada turul töötajate vaba liikumist.

[84] Henning Harte-Bavendamm *et al* (*Während der Dauer des Dienstverhältnisse*), (19)

Saksa õiguses on seega selgelt piiratud kriminaalvastutuse rakendamise periood, mis tähendab, et pärast töösuhte lõppemist toimepandud ärisaladuse rikkumise eest vastutab endine töötaja üksnes tsiviilõiguslikus korras, kuid seda juhul, kui töötaja ei ole töösuhte kestvuse ajal salvestanud tööandja ärisaladust kusagile mälupulgale või muudele dokumentidele, et siis pärast töösuhte lõppemist ärisaladust siiski avaldada või kasutada. Sellist käitumist reguleerib Saksa õiguses UWG 17 lg 2 p 1, mille kohaselt ei tohi ärisaladust tehniliste vahendite abil omandada ega salvestada ilma õiguseta ning punkti 2 kohaselt ei tohi sellel viisil omandatud ärisaladust ka avaldada ega kasutada. Seega võib öelda, et Saksa õiguses piiratakse kriminaalvastutuse rakendamist endistele töötajatele, kes ei ole ärisaladust tegelikkuses ebaseaduslikult omandanud ning sellise sätte sõnastusega püütakse vähendada tööandjate võimu töötajate vaba liikumise ja konkurentsi piiramisel, kuid olukorras, kus töötaja on teadlikult ja tahtlikult salvestanud omale tööandja ärisaladuse, et seda hiljem avaldada või kasutada, kriminaalvastutusele võtmise võimalus siiski säilib.

Järelikult Saksa õiguses olevad erinevused võrreldes Eesti õigusega, st asjaolu, et karistatav on üksnes töötajale teada oleva ärisaladuse avaldamine, kuid mitte kasutamine selle sätte alusel, ning teiseks asjaolu, et see avaldamine peab toimuma töösuhte kestel, piiravad karistusõigusliku vastutuse ainult nende juhtumite jaoks, kui töötaja teadlikult ja tahtlikult räägib tööandja ärisaladuse edasi või avaldab selle kuidagi muul viisil ilma, et töötaja oleks ärisaladuse saamiseks kasutanud tehnilisi vahendeid.

Iseenesest võiks karistusõigusliku regulatsiooni kehtestamise puhul võttagi lähtekohaks üksnes ärisaladuse avaldamise kriminaliseerimise ning jätta ärisaladuse kasutamine kriminaliseerimata, rakendades sellisel juhul üksnes eraõiguslikke õiguskaitsevahendeid. William Van Caenegem on leidnud, et preventiivse meetmena omab karistusõiguslik regulatsioon suurt mõju, kuid seda tuleks pigem rakendada raskemate juhtumite puhul, kus tagantjärele kompensatsioon enam võimalik ei ole. Ärisaladust on võimalik suuremas ulatuses kahjustada juhul, kui see avaldatakse ja mitte niivõrd juhul, kui ärisaladust ise kasutatakse.[85] Juhul, kui ärisaladus avaldatakse mõnele teisele ettevõtjale, kaob esialgsel ärisaladuse omanikul kontroll ärisaladuse leviku üle ning ärisaladus võib avaldamise teel muutuda väga lihtsalt väärtusetuks, kuna juhul, kui ärisaladus ei ole enam saladus, siis ei ole sellel ka väärtust ning see ei ole mõistetavalt ka enam kaitstav. Samas, kui ettevõtte endine töötaja otsustab ise oma ettevõttes endise tööandja ärisaladust kasutama hakata, siis on ärisaladusel tema väärtus siiski veel mingil määral alles ning seesugust olukorda on ka lihtsam tagasi pöörata. Näiteks on

[85] Caenegem, William van, (5), lk 235

võimalik keelustada võõra ärisaladuse kasutamine ning seeläbi praktiliselt taastada endine olukord.

2.3.3. „Ilma ettevõtja loata“ kui objektiivse koosseisu tunnus

UWG § 17 kommentaarides on selgitatud ka väljendi „ilma ettevõtja loata“ täpsemat tähendust. Ehkki väljendi tähendus on üpriski selge, on UWG kommentaarides arutletud selle üle, kas ettevõtja loa olemasolu on objektiivse koosseisu tunnus või õigusvastasust välistav asjaolu. Saksa õiguses on leitud, et ettevõtja loa puudumine on pigem sätte koosseisuline tunnus kui õigusvastasust välistav asjaolu. See tähendab seda, et kui tegemist on koosseisulise tunnusega, siis olukorras, kus isik usub, et tal on saladuse avaldamise õigus olemas (näiteks teiste ettevõtjatega lepingute sõlmimisel), kuid tegelikkuses tal seda õigust ei ole, on tegemist koosseisueksimusega[86]. Saksa õiguses on faktieksimus reguleeritud karistusseadustiku § 16 lõikes 1[87], mis vastab sisu poolest Eesti karistusseadustiku § 17 lõikele 1 ja mille kohaselt isik ei pane tegu toime tahtlikult, kui ta ei tea asjaolu, mis vastab koosseisutunnusele ning sellisel juhul võib isik vastutada ettevaatamatusest toime pandud süüteo eest. Saksa karistusseadustiku § 16 kommentaari kohaselt ei tohi seesugune koosseisueksimus tuleneda isiku enda hooletusest, vastasel juhul isiku vastutus tahtlikult toimepandud teo eest välistatud ei ole.[88] Riigikohus on oma lahendis 3-1-1-108-13[89] selgitanud, et keelueksimuse puhul on isiku vastutus välistatud ainult sel juhul, kui see eksimus oli isiku jaoks vältimatu, kuid õigusvastasuse tasandil vabaneb isik vastutusest igal juhul ning asjaolu, kas see eksimus oli tema jaoks välditav või mitte, ei oma tähtsust. See tähendab, et eelpool kirjeldatud olukorras, kus isik avaldab ärisaladuse, arvates, et tal on ettevõtja luba seda teha, tuleb vastutuse ulatuse välja selgitamiseks lähtuda sellest, kas isiku eksimus oli välditav või mitte. Olukorras, kus eksimus oli välditav, vastutab isik tahtlikult toimepandud teo eest. Ilmselt on ärisaladuse kaitse puhul põhjendatud lugeda ettevõtja loa puudumine objektiivse koosseisu tunnuseks ning pidada võimalikuks ka isiku vastutus juhul, isik pidas võimalikuks ettevõtja ärisaladuse lubamatut avaldamist ning ei võtnud selle väljaselgitamiseks midagi ette. Seesugune lähtekoht oleks ärisaladuse olulisust arvestades mõistlik ning lisaks tuleb isegi juhul, kui loa puudumine ärisaladuse avaldamiseks oli isiku jaoks välditav, ära tõendada ka asjaolu, et isik avaldas ärisaladuse ärilisel või kahju tekitamise eesmärgil. Juhul, kui ettevõtja loa olemasolu oleks aga õigusvastasust välistav asjaolu, siis isegi

[86] Ohly, Sosinitza, (*Unbefugte*), (20)
[87] Strafgesetzbuch. Veebis kättesaadav: http://www.gesetze-im-internet.de/stgb/
[88] Kudlich, Beck'scher Online Kommentar StGB, v. Heintschel-Heinegg 32 Auflage (2016), Veebis kättesaadav beck-online.beck.de
[89] RKKKo, 3-1-1-108-13 p 14, 6.12.2013

välditava eksimuse korral ei vastutaks töötaja üldse, kuna ärisaladuse kaitseks sätestatud norm ei näe ette vastutust ettevaatamatusest toimepandud süüteo eest.

2.4. Karistusõigusliku vastutuse välistamine, kui ärisaladust on rikutud läbi usalduse kuritarvitamise

Ühe võimaliku lähenemisena ärisaladuse karistusõiguslikku regulatsiooni planeerides võib tuua väljavastupidise seisukoha Saksa ja Eesti õiguses sätestatule. Võib küsida, kas oleks põhjendatud ärisaladuse karistusõigusliku regulatsiooni ulatust oluliselt vähendada või jätta täielikult ära ning reguleerida ettevõtjate ja töötajate vahelisi suhteid üksnes eraõiguslike õiguskaitsevahenditega. Seesugune lähenemine tagaks töötajate ja ühiskonna huve isikute vaba liikumise soodustamiseks.

Sellisel juhul töötajad, kellele ärisaladus usaldati või kellele anti ligipääs ärisaladusele, ei vastuta karistusõiguslikult ärisaladuse rikkumise eest. Samuti ei vastuta karistusõiguslikult ettevõtja lepingupartnerid, kellele sai ärisaladus teatavaks läbi lepinguliste suhete. Põhjendusena võib tuua asjaolu, et tegelikkuses on nii töötajate kui lepingupartnerite puhul ärisaladuse rikkumise vastase meetmena väga lihtsalt võimalik rakendada neidsamu lepinguid, mis on nagunii töötajate ja lepingupartneritega sõlmitud. Ilmselt on ettevõtjatel ka oluliselt lihtsam juhul, kui vastavad lepingud on sõlmitud, üles leida rikkuja ning oma huve eraõiguslike vahenditega kaitsta.

Võttes arvesse ärisaladuse olemuslikku sarnasust intellektuaalomandi õigusega ning arvestades, et intellektuaalomandi õigused on eraõigused, siis peaks ska ärisaladus olema eraõigus ning seetõttu peaks esmajärjekorras kasutatama eraõiguslikke õiguskaitsevahendeid, mitte koheselt pöörduma karistusõigusliku regulatsiooni ja riigi abi poole. Reaalsuses on ettevõtjal tänu sõlmitud lepingutele väga head võimalused oma rikutud ärisaladuse kaitseks rakendada sobilikke õiguskaitsevahendeid ning saavutada oluliselt paremad tulemused eraõiguslikult. Ilmselt ei ole riigi sekkumine iga ärisaladuse rikkumise korral põhjendatud, eriti juhul, kui eraõiguslikud õiguskaitsevahendid on piisavad. Eestis valitsevat hetkeolukorda arvestades aga ei pruugi eraõiguslikest õiguskaitsevahenditest piisata, kuid intellektuaalomandi õiguse kodifitseerimise korral paranevad ka eraõiguslikud õiguskaitsevahendid, ning ilmselt ei ole tulevikus enam nii tugevat karistusõiguslikku kaitset ärisaladuse rikkumise vastu läbi usalduse kuritarvitamise tarvis.

Eelkirjeldatud ärisaladuse karistusõigusliku kaitse lähenemise näitena võib tuua Rootsi õiguses kehtiva ärisaladuse kaitse. Nimelt on Rootsi ärisaladuse kaitse kehtestamisel olnud väga olulisel

kohal seisukoht, et töötajate vaba liikumine ettevõtete vahel peab pigem olema ilma piiranguteta. Sellest tulenevalt on Rootsi ärisaladuse kaitse akti artiklis 2 sätestatud, et akt reguleerib üksnes õigustamatut ärisaladuse rikkumist ning ärisaladuse rikkumiseks ei peeta ärisaladuse kasutamist või avaldamist juhul, kui ärisaladusele oli tagatud õiguslik ligipääs.[90]

Eelnev ei tähenda aga seda, et ettevõtte töötajad või lepingupartnerid, kes ärisaladust rikuvad, pääseksid täielikult igasugusest vastutusest. Rootsi ärisaladuse kaitse akti artikkel 6 kohaselt peab iga isik, kes tahtlikult või ettevaatamatusest kasutab või avaldab ettevõtja ärisaladuse, mis sai talle teatavaks läbi tehinguliste suhete, hüvitama ettevõtjale seeläbi tekitatud kahju. Artikkel 7 kohaselt peab aga iga isik, kes tahtlikult või ettevaatamatusest kasutab või avaldab oma tööandja ärisaladuse, millest ta sai teadlikuks tööülesannete käigus ja mille osas ta teadis või oleks pidanud teadma, et ta ei tohi seda avaldada, hüvitama ettevõtjale tekitatud kahju. Sama seaduse artikkel 7 sätestab veel, et juhul, kui ärisaladuse rikkumine leidis aset pärast töölepingu lõppemist, siis peab endine töötaja kahju hüvitama üksnes juhul, kui ilmnevad eriti rasked asjaolud.

Rootsi õiguses on aktsepteeritud mitmeid erinevaid ärisaladuse rikkumisega tekitatud kahju ulatuse arvutamise viise, millest enim kasutatavad on kasumi vähenemise ulatus, alusetu rikastumine ja ettevõtte väärtuse vähenemine ärisaladuse rikkumise tõttu. Kahju hüvitise määramisel võetakse arvesse ka rikutud ärisaladuse olemust[91] (nt kas on tehniline ärisaladus või nt kliendiandmebaasidega seonduv ärisaladus) või rikkuja tahtlust[92]. Arvestades Rootsi õiguses kehtiva ärisaladuse rikkumisest tuleneva kahju hüvitamise võimalustega, võib öelda, et need on ilmselt efektiivsemad kui Eesti õiguses tagatud vahendid, kuna näiteks Eesti õiguskorras saab alusetust rikastumisest tulenevat kahjuhüvitist nõuda üksnes juhul, kui on rikutud isiku omandit, valdust või muud õigust ning nende määratluste alla ärisaladus praegu kehtiva seaduse kohaselt ei kuulu. Eestis peab ärisaladuse rikkumise osaks saanud ettevõtja ära tõendama tekkinud kahju ulatuse ning ka põhjusliku seose ärisaladuse rikkumise ning kahju tekkimise vahel (VÕS § 127 lg 4). See tähendab, et Eesti õiguskorra järgi on ärisaladuse rikkumisega tekitatud kahju hüvitamist küllaltki keeruline tõendada, kuna näiteks kasumi vähenemine võib olla tingitud ka mitmetest muudest asjaoludest, nagu näiteks mõne konkurendi turule lisandumisest või majanduslangusest. Samas alusetu rikastumise sätete korral peab rikkuja hüvitama rikkumise teel saadu hariliku väärtuse (VÕS § 1037 lg 1 ja lg 3),

[90] Act on the Protection of Trade Secrets. (Act 1990:409, of May 31, 1990), (67)
[91] Tonell, M. The Protection of Trade Secrets and Know-How in Sweden. Swedish report. ADN Law Advokatfirma KB. Sweden: Stockholm, 2015, lk 11. Veebis kättesaadav: www.ligue.org/uploads/documents/.../2015rapportsuedoisB.pdf
[92] *ibid*

mis ei ole enam rikkumisega otseses põhjuslikus seoses, kuid eeldab siiski mingisuguse ärisaladuse väärtuse leidmist, mis võib olla näiteks ärisaladuse litsentseerimise hind.

Ärisaladuse töötajapoolse rikkumisega tekitatud kahju ulatuse kindlaks tegemist raskendavad ka igasugused andmekaitseseadusest tulenevad nõuded. Näiteks Soome on võtnud lähtekohaks kaitsta töötajate privaatsust eriti tugeval määral ning seetõttu ei ole tööandjatel ärisaladuse rikkumise kahtluse korral võimalik uurida töötaja tegemisi või arvutisuhtlust ning kohati ainus võimalus tõendusmaterjali kogumiseks on pöörduda politsei poole. Samas on mitmetel ettevõtjatel ärisaladuse rikkumise puhul üksnes kahtlus, kuid kui isegi esialgseid tõendeid on raske koguda, siis on raskendatud ka ärisaladuse rikkumise kohta avalduse tegemine. Rootsi ettevõtjad on paremas olukorras, kui Soome omad, kuna Rootsi ettevõtjatel on teabe lekkimise kahtluse korral võimalik korraldada ettevõttesiseseid uuringuid.[93] Eestis on Andmekaitse Inspektsiooni 2013. aastal avaldatud juhiste kohaselt samuti tööandjal keelatud töötajate veebilehitsemist või saadetud ja vastuvõetud e-kirju jälgida, kui selleks ei ole sõlmitud eelnevat kokkulepet töötajaga. Isegi põhjendatud kahtluse korral tuleb alati austada töötaja põhiseadusest tulenevaid õigusi sõnumisaladusele ning töötaja peab olema teadlik võimalusest, et ettevõtja tema e-kirju või muid dokumente rikkumise kahtluse korral kontrollib.[94] See tähendab seda, et olukorras, kus ettevõtja ei ole töötajaga sõlminud vastavasisulist lepingut, mis lubaks tööandjal monitoorida töötaja tegemisi tööarvutis, siis on ilmselt ärisaladuse rikkumise tuvastamine küllaltki raske, kui mitte võimatu. Töötaja erakirjade lugemiseks peab alati olema töötaja nõusolek, kas siis lepingust tulenev nõusolek või töötaja poolt tagantjärele antud nõusolek.

Ilmselt on ärisaladuse karistusõigusliku regulatsiooni olemasolu praegu ettevõtjatele väga sobivaks just seetõttu, et sellisel juhul korraldab prokuratuur kohtu loal vajalikud läbiotsimised ning kohtusse pöördumiseks vajalik tõendusmaterjal saab seeläbi lihtsamalt kogutud. See näitab, et ettevõtja töötajate isiklike õiguste ja privaatsuse kaitset tuleks samuti ärisaladuse regulatsiooni planeerimisel arvesse võtta, kuna isegi efektiivsetest ja headest eraõiguslikest õiguskaitsevahenditest ei piisa, kui ettevõtjal puudub õigus pääseda ligi oma töötajate kirjavahetusele. Eesti eraettevõtetes üldiselt ei keelata tööpostkasti kasutamist ka oma erakirjade saatmiseks, kuid erakirjade lugemine tööandja poolt siiski ilma nõusolekuta lubatud ei ole. Ilmselt tuleks luua ettevõtjatele võimalus põhjendatud kahtluse korral saada luba või

[93] Lilja, J., Johansson-Heigis, B. Rochier. Employee privacy and protection of trade secrets at odds in Finland, 2015. Veebis kättesaadav: http://www.lexology.com/library/detail.aspx?g=66ff497f-ee6a-4d8e-a580-b88443c8030d

[94] Andmekaitse Inspektsioon. Töötajate arvutikasutuse privaatsus. Juhendmaterjal ESS[1] , IKS[2] ja TLS[3] kokkupuutealade selgitamiseks, 2013, lk 9-10. Veebis kättesaadav: http://www.aki.ee/et/juhised

nõusolek ka töötajate kirjavahetusele ligipääsemiseks. Praegusel juhul prevalveerib ettevõtja õiguste üle töötaja põhiseadusest tulenev õigus privaatsusele, kuid ilmselt juhul, kui ärisaladus oleks Eesti õiguses tööstusomandi alaliigina reguleeritud, suureneksid ka tööandjate õigused oma ärisaladuse kui omandi kaitseks rakendatavate meetmete kasutusele võtmisel. Seega tuleb kindlasti arvestada ka andmekaitseõigusest tulenevaid aspekte ärisaladuse reguleerimisel.

3. Ärisaladuse kaitse ebaseadusliku omandamise vastu

Euroopa Liidus küll püütakse ühtlustada ärisaladuse kaitse regulatsiooni ning seetõttu püütakse ka Eestis luua efektiivset ärisaladuse õiguskaitsevahendite süsteemi, kuid karistusõigusliku ärisaladuse kaitse reguleerimiseni Euroopa Liidu õigus ei ulatu. See tähendab, et ärisaladuse regulatsioon ühtlustatakse mingil minimaalsel tasemel ning igal riigil on endal võimalus otsustada, kas karmistada ärisaladuse kaitseks kehtivat regulatsiooni või mitte. Nagu näha, on Euroopa Liidu liikmesriikidel küllaltki erinev regulatsioon. Eesti õiguses on siiani eelistatud üksnes seesuguse ärisaladuse rikkumise karistusõiguslikku reguleerimist, mis on toime pandud läbi usalduse kuritarvitamise ja reetmise, ehk ärisaladusele ligipääs on küll saadud õiguslikult, kuid seejärel on toime pandud rikkumine avaldamise või kasutamise läbi. Seejuures kaasneb kriminaalkaristus rikkumise eest üksnes töötajatele.

Saksa õiguses on kriminaliseeritud nii ärisaladuse rikkumine läbi usalduse reetmise, kui ka ärisaladusele ilma õigusliku aluseta ligipääsu saamine ning Rootsi karistusõiguslik regulatsioon on vastupidine Eesti omale. Rootsi õiguse kohaselt tuleb austada töötajate vaba liikumise võimalusi ning ärisaladuse rikkumise eest kaasneb töötajatele üksnes rikkumisega tekitatud kahju hüvitamine tsiviilõiguslikus korras. Ameerika Ühendriikides reguleeritakse ärisaladust karistusõiguslikult kõige pikemat aega ning rikkumise korral on ette nähtud väga karmid karistused, kuid samas on Ameerika Ühendriikides ka oluliselt suurema kahju ulatusega ärisaladuse rikkumised kui Eestis. Erinevaid reguleerimise võimalusi on mitmeid, kuid Eesti õiguses võiks olla otstarbekas võrrelda teiste riikide regulatsioone ning ärisaladuse parema kaitse huvides hetkel kehtiv regulatsioon üle vaadata.

3.1. Ärisaladuse kaitseregulatsiooni võrdlus Saksa õigusega

Saksa õiguse karistusõiguslik ärisaladuse kaitse regulatsioon ei piirdu üksnes eelmises peatükis kirjeldatud sättega, nii nagu see on Eesti õiguskorras, vaid Saksa õiguses on samal sättel veel teine lõige, millega sätestatakse vastutus juhul, kui tegemist ei ole ettevõtte töötajaga ega isikuga, kes on töötajale sarnases suhtes ettevõtjaga. UWG § 17 lg 2 ütleb sisuliselt, et isik, kes konkurentsi, isikliku kasu, kolmanda isiku kasu või ettevõtjale kahju tekitamise eesmärgil omandab ilma ettevõtja loata ärisaladuse a) kasutades tehnilisi vahendeid, b) luues kehalise salvestise informatsioonist, või c) eemaldades eseme, kus saladust hoitakse, vastutab ärisaladuse rikkumise eest. Samuti ütleb sama paragrahv, et see kehtib ka juhul, kui ärisaladus

on saadud isiku kaudu, kes on eelnimetatud punktide kohaselt ärisaladuse ebaseaduslikult omandanud[95]. Lisaks eelnevale on Saksa õiguses reguleeritud ka ärisaladuse kaitse rikkumise eriti rasked juhud. UWG § 17 (4) sätestab vastutuse olukorras, kus rikkuja a) tegutseb professionaalsel tasemel, b) teab ärisaladuse avaldamise hetkel, et saladust hakatakse kasutama välismaal, või c) kasutab ise ilma õiguseta omandatud ärisaladust välismaal[96]. Seesugune säte võimaldab Saksa õiguses ärisaladust kaitsta suuremas ulatuses ning rohkemate rikkumiste vastu, kui see on võimalik Eesti õiguse kohaselt.

3.1.1. Ebaseaduslik ligipääs ärisaladusele

Karistusseadustiku § 377 sõnastus viitab ärisaladusele, mis on isikule teatavaks saanud töö- või ametiülesannetega seoses, see tähendab, et isikule on tööülesannete täitmiseks usaldatud ärisaladus, mida töötaja on seetõttu kohustatud hoidma. Seadus ei ütle midagi seesuguse ärisaladuse kohta, mis on küll omandatud töösuhte kestuse perioodil, kuid ettevõtja ei ole töötajale ärisaladust usaldanud ega tööülesannete täitmiseks ka ligipääsu ärisaladusele võimaldanud, kuid töötaja on omal algatusel ärisaladuse siiski teada saanud. Seega olukorras, kus ettevõtte töötaja omal initsiatiivil saab ligipääsu ärisaladusele ning seejärel seda kasutab või selle avaldab, KarS § 377 kohalduda ei saa, kuna ärisaladus ei ole töötajale või ametnikule teatavaks saanud seoses tööülesannetega. Ei seaduse kommentaaridest ega seletuskirjast selgu, miks on seesugune vahetegu tehtud, et karistusõiguslik vastutus rakendub üksnes juhul, kui ettevõtja on ise võimaldanud töötajale ligipääsu ärisaladusele ning töötaja seejärel seda usaldust kuritarvitab, kuid mitte olukorras, kus töötaja täiesti ebaseaduslikult ärisaladusele ligipääsu saab ja seejärel seda kasutab või selle avaldab.

Ilmselt on võimalik, et kui isik omandab ärisaladuse ebaseaduslikult ja talle ei ole seda tööülesannete tõttu kättesaadavaks tehtud, siis võib ta vastutada mõne muu karistusseadustikus sätestatud koosseisu järgi. Näiteks olukorras, kus isik võtab kaasa ettevõtte dokumendid või kõvaketta, millele on talletatud ärisaladus, võib ta vastutada varguse koosseisu järgi, kuid arvestades asjaolu, et tänapäeval on enamik informatsiooni arvutites, siis selle informatsiooni hankimise korral võib töötaja tegevus vastata ka mõnele karistusseadustikus sätestatud arvutikuriteo koosseisule. Olukorras, kus isik võtab kaasa ettevõtja kõvakettale salvestatud ärisaladuse või dokumendid, vastutaks isik üksnes nende asjade varguse eest, arvestamata tegelikku sisulist väärtust, mis sõltub teabe ehk ärisaladuse väärtusest. Varguse koosseis hõlmab üksnes vallasasjade vargust ning teave kui ärisaladus ei ole vallasasi, vaid üksnes

[95] UWG § 17 (2). Veebis kättesaadav: http://www.gesetze-im-internet.de/uwg_2004/__17.html
[96] UWG § 17 (4). Veebis kättesaadav: http://www.gesetze-im-internet.de/uwg_2004/__17.html

informatsioon. Seega jääb kehtiva ärisaladuse regulatsiooni kohaselt ettevõte, kelle ärisaladus omandatakse ebaseaduslikult, oma huvide kaitsmisega kehvemasse olukorda, kuna karistusõiguslikult kaitstakse ettevõtet üksnes usaldatud ärisaladuse rikkumise vastu. Samas jääb siiski mõistetamatuks, miks on seaduses just seesugune vahetegu õiguslikult ligipääsetava ärisaladuse avaldamise ja kasutamise ning ebaseadusliku ärisaladuse avaldamise ja kasutamise vahel ning miks on Eesti õiguses otsustatud ettevõtjaid kaitsta pigem töötajate rikkumiste vastu, kuid mitte väljapoolt tulenevate rikkumiste vastu, arvestades, et ettevõtjatel on väljapoolt tulenevaid rikkumisi ja rikkujaid keerulisem tuvastada ning samuti on keerulisem koguda rikkumise kohta tõendeid, kuna puuduvad lepingud, mis seda lihtsustaksid. Reaalsuses oleks ilmselt võimalik ilma KarS § 377 sätteta ka töötajad, kellele on ärisaladusele ligipääs tööandja poolt võimaldatud, vastutusele võtta muude karistusseadustiku koosseisude alusel, näiteks mõnel juhul võib kõne alla tulla usalduse kuritarvitamise koosseis, kui rikutakse teise isiku varaliste huvide järgimise kohustust, kuid sellisel juhul tuleb lisaks ära tõendada ka suure varalise kahju tekitamine. Hetkel kehtiva karistusõigusliku ärisaladuse kaitse regulatsiooni lähtekoht jääb selgusetuks ning ei pruugi tagada piisavat preventiivset toimet ärisaladuse rikkumise vähendamisel.

Ärisaladuse rikkumise vastase kaitse regulatsioon on hetkel suunatud äriühingute majandustegevuse, majandustegevuse seaduslikkuse ja ka õiguslike ja eetiliste aluste kaitsele.[97] Juhul, kui ärisaladust aga käsitleda tööstusomandi alaliigina ehk intellektuaalomandina, oleks ärisaladuse kaitse suunatud omandile ning sellisel juhul võiks kõne alla tulla ka KarS § 199 varguse koosseisu rakendamine ärisaladust sisaldava teabekandja varguse korral. Näiteks arvutiprogrammid iseseisvalt ei ole asjad, vaid mõttetegevuse tulemusena tekkinud immateriaalne hüve, kuid juhul, kui arvutiprogrammid talletatakse mingile andmekandjale, muutuvad ka arvutiprogrammid asjadeks, hoolimata sellest, et nende sisuline väärtus sõltub andmekandjatele kantud informatsiooni väärtusest. Sama kehtib andmekandjatele salvestatud muusika, audioraamatute ja filmide kohta.[98] Seega, kui käsitleda ärisaladust intellektuaalomandi valdkonda kuuluva õigusena ning pidada kaitstavaks õigushüveks omandit, mitte äriühingute majandustegevust, siis võiks ettevõtjalt ärisaladust sisaldava kõvaketta varguse puhul tulla kõne alla ka varguse koosseis, kuna teabekandjale salvestatud informatsioon muutuks seeläbi vallasasjaks.

Praeguse regulatsiooni kohaselt ning arvestades Eesti kohtute seisukohta, milles ärisaladust ei käsitleta intellektuaalomandi alaliigina, ei ole ärisaladus ettevõtteväliste isikute ebaseadusliku

[97] Vutt, A. KarS kommenteeritud väljaanne. IV trükk 2015, § 377 p 1
[98] Varul, P. e*t.al* Tsiviilõiguse üldosa kommenteeritud väljaanne, 2010, § 49 p 3.1.3

omandamise eest karistusõiguslikult kaitstud ning eelpool sai ka selgitatud, miks ärisaladuse käsitlemine intellektuaalomandi alaliigina ja seeläbi ärisaladusele rakendatava kaitse suurendamine võib olla problemaatiline.

Võrreldes sama probleemi esinemist Saksa õiguses, kus ärisaladust samuti ei peeta intellektuaalomandi alaliigiks, vaid loetakse intellektuaalomandi õigustega sarnanevaks õiguseks, selgub, et Saksa õiguses on olukord, kus töötaja omal initsiatiivil pääseb ligi ärisaladusele ja selle avaldab või seda kasutab, reguleeritud UWG § 17 lõikes 2. Selle sätte kohaselt vastutab isik, kes ilma loata omandab või salvestab ärisaladuse, isikliku kasu, kolmandale isikule kasu toomise või ettevõtja kahjustamise eesmärgil, kui ta kasutab selleks tehnilisi vahendeid; või kui isik ilma ettevõtja loata kasutab või avaldab ärisaladuse, mis oli talle teatavaks tehtud või temale usaldatud või mille ta omandas tehnilisi meetodeid kasutades või kui isik omandas või salvestas ärisaladuse, millele ta omandas ligipääsu ilma ettevõtja loata.[99] See säte hõlmab sisuliselt nii need isikud, kes on ärisaladusele juurdepääsu omandanud ebaseaduslikult, kui ka need isikud, kes on ärisaladuse teada saanud küll seaduslikul viisil, kuid on selle salvestanud või mõnel andmekandjal omandanud ilma ettevõtja loata ning kasutavad või avaldavad ärisaladuse pärast töösuhte lõppemist.

UWG § 17 kommentaari kohaselt hõlmab viidatud säte nii endiseid töötajaid kui ka muid kolmandaid isikuid, kellel ettevõtjaga töösuhe puudub. Säte rakendub seega ka olukordades, kus ettevõtja endine töötaja on töölepingu kehtivuse ajal omandanud ärisaladuse (näiteks teinud koopiaid või väljakirjutusi dokumentidest või salvestanud ärisaladuse mõnele andmekandjale) ning pärast töösuhte lõpetamist kasutab või avaldab selle isikliku kasu saamise, kolmandale isikule kasu toomise või ettevõtja kahjustamise eesmärgil[100]. See näitab, et Saksa õiguses on regulatsioon täpsem ja reguleerib sarnaseid olukordi võrdsemalt.

3.1.2. Tööstusspionaaž

Saksa õiguses nimetatakse UWG § 17 lõike 2 punktis 1 sätestatut spionaaži sätteks, kuna see säte võimaldab kriminaalvastutust rakendada igale isikule, kes salvestavad või omandavad ärisaladuse, kasutades kindlaid tehnilisi meetodeid ning teevad seda ilma ettevõtja loata. See säte kaitsebki ärisaladust õigustamatu omandamise ja salvestamise eest läbi kindlate meetodite kasutamise.[101] Seaduses sätestatud ärisaladuse omandamise ja salvestamise keelatud meetoditeks on teabele lubamatu ligipääsu saamine tehniliste vahendite kaudu; informatsiooni

[99] Strafgesetzbuch § 17 lg 2. (87)
[100] Henning Harte-Bavendamm *et al* (*Täter*), (19)
[101] Caenegem, William van (5), lk 178

salvestamine andmekandjale, ja sellise eseme kaasavõtmine, mis sisaldab endas ärisaladust. Eelpool nimetatud meetodeid nimetatakse kommentaarides kõige tavapärasemateks ning eriti ohtlikeks majandusspionaaži meetoditeks, mis põhjendab seda, miks seaduses on nende meetodite abil ja isikliku kasu saamise, kolmandale isikule kasu toomise või ettevõtja kahjustamise eesmärgil ilma loata ärisaladuse omandamine või salvestamine kriminaliseeritud olenemata sellest, kas seda informatsiooni edaspidi kasutatakse või avaldatakse.[102] Samuti on nö spionaaži sätte erinevuseks, võrreldes esimeses lõikes sätestatud ärisaladuse avaldamise sättega see, et need nimetatud meetodid, mille abil ärisaladus kas omandatakse või salvestatakse, ei ole ausa konkurentsi meetodid, vaid tegemist on juba täiesti teadliku ja tahtliku ärisaladuse omandamise või salvestamisega. Samas on spionaaži säte mõneti kitsam, kui töötajate vastutust ärisaladuse rikkumise eest reguleeriv säte, kuna seadusandja on välja toonud just need kolm konkreetset viisi, millal ärisaladuse omandamine või salvestamine vastab spionaaži sättele ning muudel juhtudel see lõige ei rakendu.[103] Selle sätte puhul on ettevõtja töötaja vastutusele võtmise puhul peamine raskuspunkt just sellel asjaolul, et ettevõtte töötaja, kes on seaduslikult saanud ligipääsu ärisaladusele, teeb lisaks mingeid tegusid või sooritusi, et juba olemasolevat teavet paremini kinnistada ja seeläbi tegutseb teadlikult ärisaladuse rikkumise nimel.[104] Tahtluse element on peamine, millele tuleb tähelepanu pöörata kriminaalvastutuse rakendamisel. Seega ilmselt olukorras, kus ettevõtte töötaja kahjustab ettevõtja ärisaladust ilma tehnilisi meetmeid kasutamata ja ilma tahtluseta, võib töötaja vastutada tsiviilõiguse korras ning vastav rikkumisega tekitatud kahju hüvitamise ulatus võib tuleneda pigem töölepingus sätestatud kohustuste rikkumisest.

Tehniliste seadmete abil ärisaladuse omandamise või salvestamise all peetakse silmas näiteks koopiamasinaid, fotoaparaate, arvuteid ja arvutiprogramme. Oluline on see, et omandatakse teave, mida ilma tehniliste vahenditeta omandada ei saaks. Siia alla kuulub ka näiteks dokumentidelt kopeerimiskeelu eemaldamine ning programmide manipuleerimine, mis võimaldaks andmebaasides olevaid andmeid paremini analüüsida ja hinnata. Samamoodi on keelatud paroolide eemaldamine või äraarvamine selleks, et ärisaladusele ligi pääseda.[105] Seega kokkuvõtvalt kuuluvad selle punkti alla kõikvõimalikud tehnilised vahendid, nagu koopiate tegemine, pildistamine, mobiilide ühendamine arvutitega, igasugu juhtmete, mälupulkade ja

[102] Henning Harte-Bavendamm *et al* (*Normzweck* rn 18), (19)
[103] Hasselblatt, Bossel von, MAH Gewerblicher Rechtsschutz. Gesetz gegen den unlauteren Wettbewerb (UWG) (Die Tatbestände rn 15-52), Kommentar, 4 Auflage (2012), Beck, München. Veebis kättesaadav beck-online.beck.de
[104] McGuire, M.-R., Germany. Protection of Trade Secrets through IPR and Unfair Competition Law. AIPPI Research Question Q215, 2010, lk 6-7.
Veebis kättesaadav: https://www.aippi.org/download/commitees/215/GR215germany_en.pdf
[105] Hasselblatt, Bossel von (*Die Tatbestände* rn 15-52), (103)

väliste kõvaketaste kasutamine. Arvestades, et tänapäeval on ettevõtetes kõiksugu andmebaasid, klientide nimekirjad, lepingud ning muud ärisaladust sisaldavad dokumendid eelkõige digitaalsel kujul, siis on ilmne, et ärisaladuse omandamine või salvestamine käibki eelkõige läbi tehniliste abivahendite.

Teise võimalusena on karistus ette nähtud juhul, kui isik loob kehalise salvestuse ärisaladusest. UWG § 17 kommentaaride kohaselt on see punkt eelkõige ette nähtud nendeks juhtudeks, kus isik loob endale mingisuguse võimaluse *know-how*'na käsitletavat ärisaladust (nt tootmisprotsessid, programmid, mudelid) hiljem taasluua.[106] Ilmselt võiks selle punkti alla käia näiteks mingisuguse ärisaladust sisaldava masina või tootmisprotsessi osast mudeli loomine.

Mõlemad eelpool toodud käitumisviisid võivad selgelt ka koos esineda. Näiteks on võimalik olukord, kus isik loob koopia andmebaasist koos selle andmetega ning teeb ühtlasi ka nendest andmetest väljatrüki. Samuti võivad koos esineda olukorrad, kus isik on lindistanud üles oma kirjelduse tootmisprotsessist või teinud sellest video. Siis sellisel juhul, on selgelt kasutatud ka tehnilisi vahendeid, mis on nimetatud esimese punktis. Omaette tähendus on teisel alternatiivil üksnes juhul, kui ettevõtja ärisaladus on omandatud ja salvestatud ilma tehniliste vahenditeta, näiteks, kui isik on käsitsi teinud endale vastavad märkmed.[107]

Kolmanda alternatiivina on toodud käitumine, milles isik võtab kaasa eseme, millel ärisaladus on talletatud. Selle alternatiivi kõige lihtsam ja tavapärasem näide on see, kui ettevõtja ärisaladust sisaldavad konfidentsiaalsed dokumendid lihtsalt varastatakse. See alternatiiv hõlmab kõiki tegusid, mille kaudu isikul tekib võimalus avaldada või kasutada ärisaladust ilma ettevõtja loata. Samas ei pea selles alternatiivis kirjeldatud varguse objektiivne koosseis kattuma karistusseadustiku varguse sätte objektiivse koosseisuga, kuna isikul ei pea olema nende dokumentide omastamise ja valdamise tahet.[108] Nagu juba eelpool kirjeldatud, ei rakendu viidatud spionaaži säte mitte üksnes nende isikute rikkumistele, kes ei ole ettevõtjaga töösuhtes või sellele sarnases suhtes, vaid see rakendub ka töötajatele, kes omandavad või salvestavad ettevõtja ärisaladuse omaalgatuslikult, ilma, et neil oleks sellele juurdepääs varasemalt võimaldatud olnud. Seesugust regulatsiooni Eesti õiguses ei ole.

Ilmselt on vaieldav Eesti õiguses karistusliku sätte olemasolu vajalikkus spionaaži juhtumite tarbeks, kuid arvestades tegelikku Saksa õiguses rakendatava sätte sisu, siis võib öelda, et sellele sättele oleks võimalik rakendust leida ka Eesti õiguses. Selge on see, et iga tegevus ei peagi olema kriminaliseeritud ning mida vähem sekkub riik majandustegevusse, seda parem,

[106] *ibid*
[107] *ibid*
[108] *ibid*

kuid kui Eesti õiguses on juba olemas selline säte nagu KarS § 377, mis sätestab töötajate karistusõigusliku vastutuse olukorras, kus nad rikuvad ärisaladust, millele neile töö- või ametiülesannetega seoses tagati ligipääs, siis tekib tahes tahtmata küsimus, et miks ei kriminaliseerita sel juhul neid olukordi, kus töötajad lihtsalt nö varastavad ärisaladuse? Mille poolest peaks ärisaladuse ebaseaduslik omandamine töötaja poolt olema teisiti reguleeritud kui lihtsalt ärisaladuse rikkumine? Ühe võimaliku seletusena võib siinkohal näha just seda asjaolu, et kõige sagedamini esinebki ärisaladuse rikkumisi just seeläbi, et ettevõtja endised töötajad kasutavad uue ettevõtja huvides ära varem omandatud ärisaladust ning ettevõtjatele tuleb ette näha kaitse seesuguse usalduse kuritarvitamise vastu. Ärisaladusele ebaseaduslikku ligipääsu omandavate isikute vastu saab ettevõtja ennetavalt õiguskaitsevahendid kasutada juba seetõttu, et ettevõtjal on võimalik potentsiaalseid rikkujaid ärisaladusest eemal hoida. Samas on ilmselt paremaid õiguskaitsevahendeid võimalik kasutada olukorras, kus rikkunud isikutega on eelnevalt sõlmitud lepingud, kuna lepingutega on võimalik ettevõtjal end ka rikkumisega tekitatud kahju vastu paremini kaitsta ning tekitatud kahju hüvitamises ja ulatuses on võimalik eelnevalt kokku leppida. On võimalik, et seadusandja ei ole tahtlikult ja teadlikult kahte lähenemist eristada soovinud, kuid praeguses sättes on selge erinevus siiski olemas.

3.1.3. Ärisaladuse õigustamatu kasutamine

Saksa õiguses on lisaks ka veel säte, mis reguleerib ärisaladuse õigustamatut avaldamist ja kasutamist juhul, kui isik on ärisaladuse omandanud tööandja usaldust reetes, kuid töö- ja ametiülesannete käigus ning olukordi, kus isik on ärisaladuse omandanud või salvestanud eelpool kirjeldatud ebaausate meetodite abil või omandanud või salvestanud ärisaladuse muul ebaausal viisil. UWG § 17 kommentaaride kohaselt on see säte kõige vajalikum, reguleerimaks neid suhteid, kus töötajad on töölt juba lahkunud, kuid pärast töösuhte lõppemist avaldavad või kasutavad ärisaladust. Samas võib rikkujaks selle sätte tähenduses olla iga isik, mitte üksnes ettevõtja endine töötaja.[109] Esialgu näib, et UWG § 17 lg 2 punkti 2 esimese lause kohaselt järgneb karistusõiguslik vastutus ärisaladuse ilma loata avaldamise ja kasutamise eest konkurentsi, isikliku kasu saamise, kolmandale isikule kasu toomise või ettevõtjale kahju tekitamise eesmärgil, kui see ärisaladus oli isikule usaldatud tööülesannete täitmiseks või kui talle tagati juurdepääs ärisaladusele. Näib, nagu hõlmaks see säte lõpuks ikkagi kõik juhud, mis esialgu sätete ulatusest välja jäid, nagu näiteks töötajate karistusõiguslik vastutus pärast töösuhte lõppemist, kui ärisaladus on teatavaks saanud tööülesannete täitmise käigus ehk täpselt samas ulatuses nagu Eesti karistusõiguse kohaselt. Kuid UWG § 17 kommentaar ütleb, et selle

[109] *ibid*

sättega ei ole siiski tagatud ärisaladuse kõikehõlmav kaitse, kuna seda sätet rakendatakse üksnes olukordades, kus ärisaladus on saadud selgelt ebaausal ja mitteaktsepteeritaval viisil. Lisaks peab UWG § 17 lg 2 p 2 esimese lause kohaldamiseks olema täidetud UWG § 17 lg 1 nii objektiivne kui subjektiivne koosseis.[110] Seega peaks see säte rakenduma üksnes olukorras, kus ettevõtja töötaja on küll ärisaladusele juurdepääsu saanud tööülesannete täitmise käigus, kuid on ettevõtja usaldust väga ulatuslikult reetnud ning ärisaladuse avaldanud või seda kasutanud kavatsetult.

Arvestades, et Eesti karistusõigusliku regulatsiooni kohaldatavus ei sõltu üldse sellest, kas ettevõtja töötaja on teo toimepanemise hetkel ettevõtjaga töösuhetes või on ta juba endine töötaja, siis ei oleks sellisel sättel meie õiguskorras mõtet. Samas arvestades, et tulenevalt põhiseaduse §-st 29[111] on igal isikul õigus vabalt valida oma töö- ja ametikohta, mis kuulub seega isiku põhiõiguste hulka ning võttes arvesse ka seda, et Riigikohus varem välja toonud[112], et ärisaladus on põhiseaduse § 24 kohaselt samuti üks põhiseaduses loetletud väärtustest, tuleks tagada nende kahe väärtuse omavaheline tasakaal. See tähendab, et karistusseadustikus reguleeritud ärisaladuse kaitse peaks võrdselt võtma arvesse nii töötaja kui tööandja huve ning samuti peaks karistusõigusliku vastutuse kehtestamisel arvestama ka olemasolevate tsiviilõiguslike õiguskaitsevahenditega. Karistusõiguslik kaitse ei tohiks olla tugevalt ärisaladust omava ettevõtja huvide poole kaldu, vaid peaks arvestama ka asjaoluga, et töö- ja lepingulistes suhetes on ettevõtjatel võimalik rakendada paremaid õiguskaitsevahendeid, kui väljapool lepingu- ja töösuhet. Lisaks tuleb arvestada asjaolu, et ärisaladuse kaitse sai alguse just seetõttu, et ettevõtjad soovisid seada piiranguid töötajate konkureerimisele ettevõtjatega[113] ning ajalooliselt on ettevõtetel olnud läbirääkimistel tugevam positsioon, mistõttu ei pruugi kunagi kehtestatud regulatsioon tänapäevases kontekstis kõiki õigusi piisavalt arvestada. Seejuures tuleb veel täheldada ka seda, et õiguslikult tasakaalus oleva regulatsiooni kehtestamiseks tuleb selgelt eristada teavet, mis on ettevõtja ärisaladuseks ning teavet, mida isik võib pidada oma töökogemuseks ning vabalt kasutatavaks.

Saksa õiguses võib segadust tekitavaks sätteks oma ulatuse osas pidada sama sätte (UWG § 17 lg 2 p 2) kolmandat lauset, mille kohaselt võib isik karistusõiguslikult vastutada, kui ta avaldab või kasutab ärisaladust, mille ta on omandanud või salvestanud ilma loata. Seesugune säte tundub oma olemuselt ülimalt lai, hõlmates kõikvõimalikud ärisaladuse rikkumise juhud. UWG § 17 kommentaari kohaselt peaks see säte olema ette nähtud nendel juhtumitel, kui isikud on

[110] Henning Harte-Bavendamm *et al* (*Normzweck* rn 26), (19)
[111] Eesti Vabariigi Põhiseadus, RT 1992, 26, 349; RT I, 15.05.2015, 2.
[112] Vt RKTKo 3-2-1-103-08 punkt 20
[113] Moohr, Geraldine S. (24) lk 903

ärisaladusest teatavaks saanud läbi lepingute või läbirääkimiste ettevõtjaga, samuti töötajatele altkäemaksu andmise kaudu või muud taolised olukorrad.[114] Samas tundub sätte sõnastuse ja viidatud kommentaaride kohaselt, et ärisaladusest teatavaks saamine ei pea sugugi siinkohal olema mingi rikkumisega seotud, nagu ka kommentaarides toodud näitest võib järeldada, piisab üksnes lepingu kaudu ärisaladusest teatavaks saamisest ning seejärel selle avaldamisest või kasutamisest. Lisaks ei tundu olevat kuidagi piiratud need juhtumid, kus töötajad on õiguslikul alusel saanud teatavaks ärisaladusest, kuid pärast töölepingu lõppemist ärisaladuse hoidmise kohustust rikuvad. Samas oli seesugune käitumine karistatav ka varasemalt kirjeldatud normide alusel. Seega ei ole selle sätte ulatus selge.

Kohati näib Saksa õiguses sätestatud karistusõiguslikku ärisaladuse kaitsenormi analüüsides, et Saksa õigus on konkreetsem ning et Eesti õiguskorras võib olla otstarbekas Saksa regulatsioonist õppida, kuid samas on ka Saksa karistusõiguslikus normis segaseid aspekte ning eelpool kirjeldatud normidega on ärisaladuse kaitse karistusõiguslikult reguleeritud samas ulatuses nagu Eestiski ning veelgi enam[115]. Saksa õiguse kohaselt rakendub karistusõiguslik säte ka nö spionaaži ja töötajapoolse ärisaladuse ebaseadusliku omandamise osas. Vastavad sätted Eesti karistusõiguses puuduvad.

Saksa õiguses ärisaladuse kaitse positiivse küljena võib veel välja tuua asjaolu, et Saksa õiguse kohaselt on tsiviilõiguse korras võimalik nõuda kahju tekitava tegevuse lõpetamist ja sellest hoidumist nii hagi tagamise abinõuna kui püsivalt. See tähendab, et seda abinõu on võimalik rakendada nii sellel juhul, kui ärisaladust on juba rikutud kui ka juhul, kui esineb reaalne oht ärisaladuse rikkumisele. Kõige sagedamini kasutatakse lõpetamise ja hoidumise nõuet just ärisaladuse õigustamatu kasutamise ära hoidmiseks.[116] Euroopa Komisjoni poolt tellitud uuringu kohaselt ei ole ka Saksa õiguses ärisaladus käsitletav intellektuaalse omandi õigusena, kuid sellegi poolest rakenduvad ärisaladusele samasugused tsiviilõiguskaitsevahendid nagu intellektuaalsele omandile.[117] Nagu juba eelpool öeldud, siis Eesti õiguses seesugune nõue võimalik ei ole, kuna ärisaladuse puhul ei ole Eesti õiguses tegemist omandisarnase õigusega, mis võimaldaks esitada nõuet kahju tekitava tegevuse lõpetamiseks ja sellest hoidumiseks VÕS § 1055 lg 3 järgi.

---

[114] Köhler/Bornkamm, (*Tatvoraussetzungen* rn 44-47), (61)

[115] Saksa õiguses on lisaks eelpool nimetatule reguleeritud ka ärisaladuse rikkumise eriti rasked juhud, mis hõlmavad peamiselt olukordi, kus ärisaladuse rikkuja juba ärisaladuse rikkumise hetkel teab, et see avaldatakse välisriigis või hakatakse välisriigis kasutama. Vt UWG § 17 lg 4

[116] McGuire, M.-R., lk 6-7, (104)

[117] Hogan Lovells International LLP. Study on Trade Secrets and Parasitic Copying (Look-alikes) MARKT/2010/20/D. Report on Trade Secrets for the European Commission. 2012, lk 19. Veebis kättesaadav: ec.europa.eu/internal_market/.../trade-secrets/120113_study_en.pdf

Saksa õiguses on ärisaladuse rikkumisega tekitatud kahju hüvitamist võimalik nõuda ka alusetu rikastumise sätete korras[118], mis jällegi Eesti õiguses võimalik ei ole. Samuti on Saksa õiguse kohaselt tekitatud kahju tõendamiseks võimalik ärisaladuse rikkujalt välja nõuda ettevõtte raamatupidamise dokumendid, et oleks võimalik kuidagi tõendada tekitatud kahju ulatust. [119] Peab tõdema, et Eesti õiguskorras on ärisaladuse rikkumise eelse olukorra taastamiseks ja kahju suuruse leidmiseks oluliselt piiratumad õiguskaitsevahendid, kui seda on Saksa õiguses. Eeldatavasti ei kesta seesugune olukord aga enam kaua, kuna töö ärisaladuse regulatsiooni tõhustamiseks eraõiguse valdkonnas juba käib ning korrektsete eraõiguslike õiguskaitsevahendite olemasolu võimaldab paremini analüüsida ka seda, kuidas oleks ärisaladuse regulatsiooni vajalik täiustada karistusõiguslikult.

Ilmselt võib öelda, et ärisaladusel on küllaltki palju sarnasusi intellektuaalomandi õigustega, kuid ka piisavalt suured erinevused, selleks, et tagada ärisaladusele niivõrd tugev kaitse, nagu on intellektuaalomandi õigustel. Samas on ärisaladuse kaitse majandustegevuse arenguks väga oluline, mistõttu peavad olema tagatud õiguskaitsevahendid ärisaladuse rikkumise korral. Arvestades, et ärisaladus on samuti eraõigus nagu seda on intellektuaalomandi õigused, siis tuleks ka ärisaladuse kaitse regulatsiooni loomisel lähtuda eelkõige sellest põhimõttest, et karistusõiguse poole tuleks pöörduda alles siis, kui teised õiguskaitsevahendid ei ole tulemuslikud. See tähendab seda, et olukorras, kus ettevõtjatele on loodud efektiivsed ja toimivad eraõiguslikud õiguskaitsevahendid ja on tagatud kahju hüvitamise võimalused, siis peaks olema piiratud võimalus karistusõigusliku kaitse jaoks. Olukord, kus ettevõtjal on võimalik lepingutega reguleerida oma ärisaladuse kaitset, tagab isegi praeguste õigusnormidega võimaluse nõuda lepingupartnerilt või ettevõtja töötajalt tekitatud kahju hüvitamist näiteks leppetrahvi näol. Samas aga olukorras, kus lepingud või töösuhe puudub, ei ole võimalik enam nii lihtsalt kahju hüvitamist nõuda. Seega tundub praegu kehtiv karistusõiguslik regulatsioon pigem olevat vastuolus *ultima ratio* põhimõttega, kuna töötajate puhul on selgelt kõige suurem võimalus kahju hüvitamise tingimused ja leppetrahvid ärisaladuse kaitseks kokku leppida, samas aga kaitseb karistusõiguslik regulatsioon ettevõtjaid just üksnes töötajate rikkumise vastu ning teiste isikute rikkumise suhtes või ka ebaseadusliku ärisaladuse omandamise suhtes jätab ettevõtja kaitseta.

[118] *ibid*
[119] *ibid*

3.2. Ärisaladuse kaitseregulatsiooni võrdlus Rootsi õigusega

Nagu juba eelnevalt märgitud, on Rootsi ärisaladuse kaitse regulatsioon teistest Euroopa Liidu liikmesriikides kehtivast regulatsioonist erinev selle poolest, et Rootsis on ärisaladuse rikkumise vastane kaitse reguleeritud iseseisvas õigusaktis. Ehkki Rootsi ärisaladuse kaitse regulatsiooni on peetud Euroopa Liidu üheks kõige ulatuslikumaks ja üpriski efektiivseks, on ka Rootsi regulatsiooni puhul leitud mõningaid puudujääke.[120] Ärisaladuse kaitse akti artikli 1 kohaselt loetakse ärisaladuseks äri- või tööstusega seonduvat informatsiooni, mida isik kasutab ärilistel või tööstuslikel eesmärkidel ja mida see isik soovib hoida saladuses ning selle informatsiooni avalikustamine kahjustaks tõenäoliselt selle isiku konkurentsivõimet.[121] Seega vastab Rootsi ärisaladuse definitsioon sisuliselt enam-vähem TRIPS lepingus sätestatud kriteeriumitele, mille kohaselt ärisaladus on informatsioon, mis peab olema saladuses ja seeläbi omama majanduslikku väärtust ning mille kaitseks ettevõtja on kasutusele võtnud vastavad meetmed. Rootsi ärisaladuse definitsioon aga ei märgi kohustusliku nõudena kaitsemeetmete kasutuselevõttu.

Rootsi õiguses on kaitstav igasugune informatsioon, mis vastab ärisaladuse definitsioonile ning seadusest tulenevalt ei pea ettevõtja olema kasutusele võtnud mingeid konkreetseid meetmeid, et seda väärtuslikku teavet saladuses hoida. Samas M. Levin on oma artiklis öelnud, et tegelikkuses peab ettevõtja siiski ärisaladusena käsitletavat teavet ise pidama konfidentsiaalseks ja salajaseks ning ka vastavalt sellele käituma. Rootsi kohtud on selgitanud, et teavet peab ka ettevõtja ise käsitlema kui konfidentsiaalset teavet, kuid see, kuidas nad seda väljendavad, on iga ettevõtja enda otsustada.[122] See tähendab, et tegelikkuses on Rootsi ärisaladuse kaitse akti lõplik ärisaladuse definitsioon kooskõlas TRIPS-lepingus sätestatud kolme kriteeriumiga, mis peavad olema täidetud selleks, et teave oleks ärisaladus ning sellena ka kaitstav.

Sanktsioonid ärisaladuse rikkumise eest on ette nähtud artiklites 3 ja 4, mis sätestavad ärisaladuse rikkumise eest vangistuse või rahalise karistuse. Artikli 3 sõnastuse kohaselt võetakse isik, kes tahtlikult ja ilma loata omandab juurdepääsu ärisaladusele, vastutusele spionaaži eest ning teda karistatakse rahalise karistusega või vangistusega mitte üle kahe aasta, kuid juhul, kui tegemist oli raske rikkumisega siis vangistusega mitte üle kuue aasta.

[120] Schultz, M., Lippoldt, D., (2014), Approaches to Protection of Undisclosed Information (Trade Secrets): Background Paper, *OECD Trade Policy Papers*, No. 162, OECD Publishing, Paris. Veebis kättesaadav: http://dx.doi.org/10.1787/5jz9z43w0jnw-en

[121] Act on the Protection of Trade Secrets. (Act 1990:409, of May 31, 1990), (67)

[122] Levin, M., Protection of trade secrets through IPR and unfair competition law. AIPPI (International Association for the Protection of Intellectual Property) Research Question Q 215., 2010 lk 2. Veebis kättesaadav: aippi.se/files/user/aippi/Q215_SE.pd

Ärisaladuse rikkumise raskuse hindamisel võetakse arvesse seda, kas tegu oli eriliselt ohtlik, hõlmas suurt rahalist väärtust või põhjustas eriti suure kahju. Artikkel 4 kohaselt on karistatav ka see, kui ärisaladus omandatakse teadmisega, et eelnevalt on isik, kes ärisaladuse avaldab või mõni isik enne teda ärisaladuse teada saanud spionaažina kvalifitseeritava tegevuse läbi. Sellisel juhul on karistusena samuti ette nähtud rahaline karistus või kuni 2-aastane vangistus või eriti rasketel juhtudel kuni 4-aastane vangistus. Lisaks eelnevale sätestab ärisaladuse kaitse akti artikkel 5, et isikud, kes panid toime artiklis 3 või artiklis 4 sätestatud teod, ehk ärisaladuse rikkumise, peavad kompenseerima ka ärisaladuse rikkumisega tekitatud kahju.

Nagu eelnevast nähtub, on Rootsi õiguses karistatav ärisaladuse mitteõiguspärane omandamine. See tähendab, et karistusõiguslikult ei ole reguleeritud olukorda, kus ärisaladusele on ligipääs saadud õiguslikke teid pidi. Seega olukorras, kus ettevõtte töötajale on usaldatud ärisaladus või kui talle on tagatud ligipääs ärisaladusele ning töötaja seejärel seda ärisaladust kasutab või selle avaldab, ei ole karistusõiguslik vastutus kohaldatav. See tähendab, et ärisaladuse rikkumise karistusõiguslik vastutus on reguleeritud vastupidiselt Eestis kehtivale regulatsioonile. Sellist lähtekohta kinnitab ka Rootsi ärisaladuse kaitse akti artikkel 2, mille kohaselt kohaldub akt üksnes seesugustele ärisaladuse rikkumistele, mis on õigustamatud. Samuti sisustab artikkel 2 viimane lause mõnes mõttes ka õigustamatu ärisaladuse rikkumise – selle kohaselt ei loeta õigustamatuks ärisaladuse rikkumiseks olukorda, kus keegi, kes algselt omandas ärisaladuse seaduslikul teel, selle hiljem avaldab või seda kasutab.

Rootsi ärisaladuse kaitse akt seab piirangud regulatsiooni rakendamisele artiklites 1 ja 2, mis sisaldavad ärisaladuse definitsiooni ning õigustamatu ärisaladuse rikkumise sisustamise põhimõtteid. Need piirangud on ette nähtud selleks, et leida tasakaal efektiivse ärisaladuse kaitse ja töötajate vaba liikumise ja väljendusvabaduse vahel. Esialgne ärisaladuse kaitse akt ei sisaldanud artiklit 2, mistõttu leiti, et ärisaladuse kaitse regulatsioon on liialt karm ning see võib piirata töötajate ettevõtlus- ja väljendusvabadust ning samuti võib takistada töötajatel avaldamast teavet selle kohta, kui ettevõtja tegeleb millegi ebaseaduslikuga. Sellest tulenevalt sai akti lisatud artikkel 2, mis lisaks sellele, et välistab ärisaladuse õigustamatu rikkumise alt olukorra, kus ärisaladus isikule usaldati, vabastab vastutusest ka isiku, kes kaebab ettevõtja peale, kui viimane paneb toime seaduse rikkumise.[123] Ärisaladuse direktiiv 2016/943 sätestab artiklis 5, et ärisaladuse rikkumiseks ei peeta ettevõtja ebaseadusliku tegevuse avaldamist, seega on Rootsi ärisaladuse kaitse akti artikkel 2 ärisaladuse direktiivi nõudega kooskõlas. Nagu juba eelnevalt mainitud, siis Eesti seaduste sätetest sellist piirangut ei tulene, kuid eeldatavasti on võimalik see piirang tuletada mingite muude kriteeriumite järgi. Näiteks

[123] Tonell, M., lk 3,(91).

karistusseadustikus sätestatud vastutus ärisaladuse rikkumise eest kohaldub juhul, kui ärisaladuse rikkumisel oli äriline või kahju tekitamise eesmärk. Ilmselt võib öelda, et kui isikul oli ärisaladuse avaldamise eesmärgiks hoida ära või takistada ettevõtte edasist seaduserikkumist, siis kumbki eesmärkidest täidetud ei ole. Samas võiks ka Eesti seadusandluses vaidluste ja probleemide vältimiseks, olla selgelt ära märgitud, et ettevõtja seaduserikkumisest teavitamise korral ja seetõttu ärisaladuse avaldamisel, isikule vastutust ei kaasne.

M. Tonell lisab veel, et juhul, kui ettevõtte töötaja avaldab ettevõtte ärisaladuse eesmärgil takistada ettevõtja seaduse rikkumist, siis peavad ühiskondlikud huvid kaaluma üle ettevõtja ärisaladuse salajas hoidmise huvid, ehk see tähendab, et rikkumine peab olema küllaltki tõsine. Samuti ütleb Tonell, et sellisel juhul ärisaladuse avaldamine peab siiski toimuma üksnes nendele ametnikele või asutustele, kes on võimelised ettevõtja rikkumist kontrollima ning kes ettevõtja ärisaladust vajadusel ebaõige avalikustamise eest kaitsevad.[124] See tähendab siiski seda, et ettevõtte töötajad ei tohi ärisaladust ühiskonna kaitse huvides avaldada kusagil internetis või ajalehes, vaid peavad pöörduma vastavate asutuste poole. Sellisel juhul on ka oluliselt lihtsam jaatada töötaja huve takistada seaduse rikkumist ning mitte lihtsalt tekitada kahju ettevõtjale. Seega ettevõtjate huvide kaitseks peaks seesugune teatud tingimustel ärisaladust avaldada lubav säte olema ka seaduses selgelt kirjas ja piiritletud.

Rootsi ärisaladuse kaitse akti regulatsiooni ulatusest jääb väljapoole ka töötajate omandatud teave ja oskused. Selle peaks välistama ärisaladuse mõistes kasutatav väljend „äri- või tööstusega seonduv informatsioon“.[125] Samas ei ole selgelt arusaadav, kuidas see väljend iseenesest peaks välistama töötaja isiklikud teadmised ja oskused ärisaladuse määratluse ulatusest, kuna ettevõtte töötaja teadmised ja oskused võivad olla teabeks, mis on seotus äri- või tööstusega, mida soovitakse hoida salajas ja mis annavad ettevõtjale konkurentsieelise. Samas on Tonell, M. selgitanud, et Rootsi ärisaladuse kaitse akti eelnõus on selgelt öeldud, et teavet, mida iga piisava ja vastava haridustasemega isik suudab kasutada äris või tööstuses, peab käsitlema kui äri- ja tööstusega seonduvat teavet. Kuid juhul, kui see teave koosneb teadmistest ja kogemustest, mida ei ole võimalik läbi juhendamise lihtsasti edasi anda, tuleb seda teavet lugeda isiku oskusteabeks ja seega ei ole see ärisaladusena kaitstav.[126] Seega on Rootsis vähemalt seaduseelnõuga püütud teha vahet ärisaladuseks kvalifitseeruval teabel ja töötaja oskusteabel. Eesti õiguses seesugust eristatavust ei nähtu, kuid kohtud on ärisaladust

[124] Tonell, M., lk 6, (91)
[125] *ibid* , lk 5, (91)
[126] *ibid*

puudutavate kaasuste lahendamisel sageli viidanud Riigikohtu otsusele 3-2-1-103-08 (p 20), milles öeldakse, et ärisaladuse kaitsega ei ole võimalik minna nii kaugele, et isikul pole enam üldse võimalik samal tegevusalal töötada ning selleks, et eristada isiku oskusteavet ettevõtte ärisaladusest, tuleb kohtutel igal üksikjuhtumil võimalikult täpselt välja selgitada, mis on konkreetse ettevõtte ärisaladus.

Rootsi ärisaladuse kaitse akti eelnõus on lisaks töötaja oskuste ja kogemuste eristamisele ärisaladusena käsitletavast teabest veel lisaks ära toodud ka juhis olukorraks, kui nende kahe teabeliigi eristamisel raskusi tekib. Levin, M. toob välja, et eelnõus on selgelt öeldud, et olukorras, kus esineb kahtlusi, kas teave on ärisaladus või töötajale kuuluv teave, tuleb seda igal juhul tõlgendada töötaja kasuks, ehk tegemist on töötaja oskusteabega, mitte ärisaladusena kaitstava teabega.[127] See näitab, et Rootsi seadusandlus on pigem suunatud töötajate vaba liikumist soosivale regulatsioonile ning karistusõiguslikku vastutust ärisaladuse rikkumise korral, juhul, kui see eelnevalt omandati õiguslikult, ei järgne. See aga ei tähenda, et töötaja ei vastutaks üldse ärisaladuse rikkumise eest. Töötaja vastutus on sätestatud samas aktis, kuid eraõiguslikus korras.

Rootsi ärisaladuse kaitse regulatsiooni on just seetõttu väga palju ka kritiseeritud, et see ei kaitse ettevõtjaid selle vastu, kui ettevõtte töötaja, kellel on õigus teada ärisaladust, selle edasi müüb. See tähendab, et karistusõiguslik kaitse ei ulatu mitte ühelegi õiguslikult saadud ärisaladuse rikkumisele. Samas tuleb meeles pidada, et karistatav on see, kui keegi pääseb ärisaladusele ligi ilma selleks õigust omamata. Seesugune tegu loetakse Rootsi ärisaladuse kaitse akti kohaselt ärisaladuse spionaažiks artikli 2 kohaselt.

Rootsi ärisaladuse kaitse puudust kirjeldava näitena on sageli toodud nö Ericssoni juhtum. Ericssoni juhtumis oli töötajale tagatud ligipääs ärisaladusele ning see töötaja avaldas ettevõtja ärisaladuse ühele teisele isikule, kes omakorda avaldas Ericssoni ärisaladuse välismaisele ettevõtjale. Ettevõtte töötajat süüdistati rängas tööstusspionaažis osalemise eest, kuid Rootsi apellatsioonikohus mõistis töötaja õigeks, kuna Rootsi ärisaladuse kaitse akti regulatsiooni ulatusse ei kuulu juhtumid, kus isik on ettevõtja ärisaladuse saanud õiguslikul alusel. Samas, see isik, kes ettevõtja töötajalt ärisaladuse sai ning selle välismaisele ettevõtjale edastas, mõisteti kaheksaks aastaks vangi ränga spionaaži eest.[128] See näitab selgelt, et Rootsis on karistusõiguslikult keelatud võõrale ärisaladusele juurdepääsu hankimine, kuid juba teadaoleva ärisaladuse avaldamise eest vastutatakse üksnes eraõiguslikus korras.

[127] Levin, M., lk 3, (122)
[128] *Ibid*, lk 5.

See, millises ulatuses ärisaladuse rikkumine kriminaliseerida, sõltub igast õiguskorrast ning riigis valitsevast õiguspoliitikast, millest sõltub, kas võetakse töötajate vaba liikumist soosiv lähtekoht või otsustatakse ettevõtjate salajase teabe kaitse kasuks. Ilmselt oleks eelistatuim leida tasakaal töötajate ja ettevõtjate huvide vahel. Ärisaladuse kaitse kriminaliseerimine teenib Eestis hetkel nende kahe huvi võrdluses pigem ettevõtjate huve. Karistusõigusliku regulatsiooni kehtestamisel tuleb kindlasti arvesse võtta ka teistes õigusharudes kehtivaid regulatsioone, mis võivad rolli mängida ka karistusõigusliku regulatsiooni kehtestamisel, näiteks tugeva ja efektiivse eraõigusliku regulatsiooni korral ei pruugi üldse tekkida vajadust karistusõigusliku regulatsiooni järele ning karistusõiguslik regulatsioon võiks tõesti rakenduda üksnes väga rasketel juhtumitel, kus tsiviilõiguslikest õiguskaitsevahenditest ei piisa. Lisaks tuleb arvestada ka muude valdkonna seadustega, nagu näiteks andmekaitseõiguses kehtivate regulatsioonidega, mis võivad ettevõtjale oma ärisaladuse kaitsmisel väga suuri piiranguid seada ning kindlasti tuleks arvestada sellega, kas ettevõtjal üldse on võimalus ja õigus koguda tõendeid ärisaladuse rikkumise kohta või kontrollida kahtluse korral töötajate tegevust ja e-kirjavahetust, või on see liigne sekkumine töötajate privaatsusesse. Seega tuleb karistusõigusliku ärisaladuse regulatsiooni kehtestamisel arvesse võtta mitmeid aspekte. Samas tuleb karistusõiguslikku regulatsiooni kehtestades arvestada ka seda, et liialt ranged karistuses ärisaladuse õigustamatu omandamise korral võivad hakata koormama ka ettevõtjaid endid, seda näiteks juhul, kui ärisaladuse rikkumise vastutus võiks ettevõtjale kaasneda ka juhul, kui ettevõtja võtab tööle töötaja konkureerivast ettevõttest, kes toob endaga kaasa ärisaladuse.

James Pooley on öelnud, et ärisaladuse kaitse range kriminaliseerimine võib põhjustada lisakulutusi ka ettevõtjatele. Seda seetõttu, et kriminaalkaristus on ette nähtud ka nendele ettevõtetele, kes läbi uute töötajate omandavad töötaja eelmise tööandja ärisaladuse. See tähendab, et olukorras, kus ettevõtja võtab tööle uusi isikuid, peab ta olema veendunud, et nad ei too endaga kaasa teise ettevõtja ärisaladust, mille kasutamise korral uues ettevõttes võib järgneda kriminaalmenetlus ja ka karistus. Sellise olukorra välistamiseks peaksid ettevõtjad uute töötajate kollektiivi lisandumisel kasutusele võtma mingisugused meetmed vältimaks ärisaladuse õigustamatut kasutamist.[129] Ilmselt võib Eestis olla seda kriteeriumit lihtsam täita, kuna ettevõtted on piisavalt väikesed, mistõttu on ettevõtte juhtidel parem ülevaade lisandunud töötajatest, kuid suuremates ettevõtetes või ettevõtetes, kus töötajate voolavus on kõrge, võib see olla suurem probleem. Ilmselt võib ärisaladuse range kriminaliseerimine pärssida ka töötajate vaba liikumist, mitte üksnes töötajate hirmu tõttu võimaliku kriminaalkaristuse ees,

[129] Pooley, J., The Top Ten Issues According to Trade Secret Law – Temple Law Review 1997/70, lk 8. Veebis kättesaadav: http://heinonline.org/HOL/Page?handle=hein.journals/temple70&g_sent=1&collection=journals&id=1191

vaid ka ettevõtted võivad konkurentide endiste töötajate palkamisse suhtuda mõnevõrra ettevaatlikumalt.

Arvestades hetkel Eestis kehtivat regulatsiooni, siis seda hirmu ettevõtjatel olla ei saa, kuna ärisaladuse õigustamatu avaldamise ja kasutamise eest vastutavad üksnes ärisaladust omava ettevõtte praegused ja endised töötajad. See võib olla ka üheks põhjuseks, miks Eestis on viimasel ajal sagenenud uute töötajate töölevõtmisel just konkurentidelt töötajate üleostmiste hulk.[130] On ilmne, et iga töötaja soovib ennast arendada ja teenida kõrgemat palka, kuid juhul, kui ettevõtte endine töötaja võtab endaga kaasa lisaks isiklikele oskustele ka ettevõtte ärisaladuse, siis läbi karistusõigusliku regulatsiooni üksnes töötajate õiguskuuleka käitumise survestamine ilmselt ei pruugi tagada vajalikku eesmärki. Reaalsuses võivad näiteks kasu saavad ettevõtjad ka uuele töötajale endise tööandja ärisaladuse rikkumist püüda hüvitada või tagada talle hea kaitse kriminaalmenetluses, kuna ettevõtjat ennast üldiselt karistusõiguslikult vastutusele võtta ei saa, kuna ärisaladuse rikkumise eest vastutavad karistusõiguslikult üksnes ettevõtja töötajad, kellele ärisaladus usaldati või tööülesannete käigus teatavaks sai. Seega need ettevõtjad, kes võtavad tööle konkurentide töötajaid, kes toovad eelmisest ettevõttest kaasa ärisaladuse, võivad praeguse regulatsiooni kohaselt saada kasu võõra ärisaladuse näol, kuid vastutuse ulatus on üpriski vähene.

3.3. Karistusõiguslik kaitse Ameerika Ühendriikides

Nagu juba eelnevalt ka öeldud sai, on ärisaladuse kui informatsiooni tugev karistusõiguslik regulatsioon saanud ka palju negatiivset vastukaja ning seda ilmestab kõige enam Ameerika Ühendriikides ärisaladuse karistusõigusliku regulatsiooni kriitika. Ameerika Ühendriikides on ärisaladuse kaitsenormid olnud kasutusel kõige kauem ning 1996. aastal võeti vastu Majandusspionaaži akt (*Economic Espionage Act edaspidi ka EEA*), mis kriminaliseerib ärisaladuse spionaaži, mille eesmärgiks on kaitsta Ameerika Ühendriikide ettevõtja ärisaladust välisriiki väljaviimise eest ning välisriigi ettevõtjatele või valitsusele ebaausa kasu toomise eest. Enne selle sätte rakendamist peab aga selleks saama loa Rahvusliku Julgeoleku Osakonnalt. Lisaks on kriminaliseeritud ka ärisaladuse vargus või omastamine enda või kellegi teise kasu saamise eesmärgil või ettevõtjale kahju tekitamise eesmärgil, kui see ärisaladus on seotud tootega, mis on mõeldud USA turule või välismaisele turule.[131] EEA on saanud palju kriitikat

[130] Äripäev. ITs ja ehituses kahmatakse spetsialiste 6.02.2017. Veebis kättesaadav: http://www.aripaev.ee/uudised/2017/02/06/it-sektoris-kahmatakse-spetsialiste

[131] Krotoski, Mark. L, Common Issues and Challenges in Prosecuting Trade Secret and Economic Espionage Act Cases. Economic Espionage and Trade Secrets 2009 Volume 57 Number 5. Ameerika Ühendriigid: North Carolina 2009, lk 5. Veebis kättesaadav: https://www.justice.gov/sites/default/files/usao/legacy/2009/12/10/usab5705.pdfs

seetõttu, et seal sätestatud ärisaladuse regulatsioon on väga laiahaardeline, kuid samas on seda rakendatud küllaltki vähe.[132] Näiteks perioodil 1996 kuni 2009 on spionaaži artiklit, mis reguleerib ärisaladuse vargust välismaiste ettevõtete ja valitsuste poolt, kasutatud üksnes kuuel korral.[133] Samas ei saaks kuidagi väita, et regulatsiooni rakendatavuse vähesus võiks näidata selle regulatsiooni ebaotstarbekust. Ilmselt on selge, et ettevõtjaid tuleb välisriikidest lähtuva ärisaladuse varguse eest kaitsta isegi olukorras, kui neid juhtumeid on vähe. Võimatu pole ka see, et neid juhtumeid küll on, kuid nende menetlust ei toimu kas seetõttu, et neid on keerukas avastada või seetõttu, et pole piisavalt tõendeid informatsiooni kuritarvitamise kohta.

Ameerika Ühendriikides karistusõiguslikult reguleeritud ärisaladuse kaitse on oluliselt karmim kui karistusõiguslik kaitse Eestis. Krotoski on oma artiklis öelnud, et kriminaalkaristus ärisaladuse rikkumise eest peab omama preventiivset mõju ning rakendub üksnes raskete rikkumiste korral. Rasketeks rikkumisteks EEA järgi võiks pidada näiteks:

- teise riigi poolt rahastatud ja toetatud ärisaladuse ja tehnoloogia ebaseaduslikku omastamist;
- rikkumist, kus ettevõtja usaldusväärne töötaja, kellel on ligipääs olulisele ärisaladusele, edastab selle ärisaladuse kellelegi, kes müüb selle ärisaladuse edasi kõrgeima pakkumise tegijale;
- rikkumist, kus ettevõtja töötaja, kes on selgeks saanud mingi prototüübi loomise protsessi, otsustab ise seda ärisaladust oma ettevõtte loomiseks ja konkureeriva toodangu tegemiseks ära kasutada;
- rikkumist, kus konkureeriv ettevõtja loob võimaluse või skeemi, et pääseda ligi teise ettevõtja olulisele informatsioonile ja ärisaladusele ning seeläbi täidab oma rahvusvahelisest lepingust tuleneva kohustuse;
- rikkumine, kus ettevõtja töötaja varastab ärisaladuse ning soovib seda viia välismaale ning ta peetakse kinni lennujaamas;
- rikkumist, kus ettevõtja töötajale tehakse ettepanek asuda tööle otsese konkurendi juhtival kohal ja enne lahkumisavalduse esitamist kasutab ära oma positsiooni, et saada ligipääs ärisaladusele, millele tal tavaolukorras ligipääsu ei oleks olnud ning seejärel annab sisse lahkumisavalduse ja võtab kaasa kogu ärisaladuse kohta saadud informatsiooni konkureerivasse ettevõttesse.[134]

Sätte täpne sõnastus on EEA § 1832 – Theft of trade secret. Veebis kättesaadav: https://www.law.cornell.edu/uscode/text/18/1832

[132] Caenegem, William van (5), lk 120

[133] Krotoski, Mark. L (131), lk 7

[134] Krotoski, Mark. L, lk 3 (131)

See kirjeldatud loetelu näitab seda, et EEA sätete rakendamiseks peab pigem olema tegemist tõsiste rikkumiste ja täiesti tahtliku ärisaladuse vargusega ning enamikel juhtudel peetakse rasketeks juhtudeks eelkõige neid olukordi, kus ärisaladust püütakse viia välismaale või müüa maha nendele, kes tegelevad ilmselt nö ärisaladuste oksjoniga.

Ameerika Ühendriikide ärisaladuse karistusõiguslik regulatsioon sätestab ärisaladuse spionaaži eest ka väga rasked karistused. Näiteks ärisaladuse rikkumise eest, mille eesmärgiks oli ärisaladus välismaale viia või mille vargus oli toetatud välismaise valitsuse poolt, on ette nähtud karistusena kuni 15-aastane vangistus või kuni 5 miljoni dollari suurune trahv, või mõlemad[135]. Ärisaladuse varguse eest, mille eesmärgiks on kasu toomine kellelegi teisele peale ärisaladuse omava ettevõtja ja teades, et seeläbi tekib kahju ärisaladust omavale ettevõtjale, on ettenähtud karistusena kuni 10-aastane vangistus või kui rikkujaks oli mõni juriidiline isik, siis kuni 5 miljoni dollari suurune rahaline karistus või rahaline karistus, mis vastab kolmekordsele ärisaladuse väärtusele.[136] On selge, et Ameerika Ühendriikide ärisaladuste väärtust on küllaltki raske kuidagi kõrvutada Eesti ärisaladustega, kuna nii tegutsevate ettevõtete suurus kui kaubaturu ulatus on niivõrd erinevad, kuid ilmselt on siiski mõistlik pöörata tähelepanu EEA kriitikale.

EEA regulatsiooni on küllaltki palju kritiseeritud, kuna selle sõnastus ei ole selge ja täpne ning sellega sätestatakse väga karmid kriminaalkaristused ärisaladuse rikkumise eest. G. Moohr on oma artiklis öelnud, et enne ärisaladuse karistusõiguslikku regulatsiooni oleks tulnud luua efektiivsed tsiviilõiguslikud normid ärisaladuse kaitseks ning alles pärast nende normide rakendamist ja efektiivsuse analüüsi võiks mõelda karistusõiguslike normide loomise vajalikkusele. Samuti ütleb G. Moohr, et EEA on ehe näide sellest, et tark oleks hoiduda informatsioonil või teadmistel põhineva toote karistusõiguslikust kaitsmisest.[137] Meenutades siinkohal Eesti kohtutes arutatud ärisaladuse kaasuseid, millest enamik on töötajate poolt kliendinimekirjade või koostööpartnerite kaasavõtmine uude ettevõttesse ning võttes arvesse, et eraõiguslikud ärisaladuse kaitsenormid on seadustesse paigutatud väga killustatult ning efektiivne ärisaladuse kaitse sisuliselt puudub, siis tegelikkuses ei pruugi Eestis pärast efektiivsete eraõiguslike ärisaladuse kaitsenormide kehtestamist üldse ärisaladuse karistusõiguslik kaitse vajalik olla ning juhul, kui see on preventiivse toime saavutamiseks oluline, siis tuleks ehk pärast eraõiguslike normide loomist üle vaadata ka karistusõiguses

[135] EEA U.S Code § 1831 – Economic espionage. Veebis kättesaadav: https://www.law.cornell.edu/uscode/text/18/1831
[136] EEA U.S Code § 1832 – Theft of trade secrets. Veebis kättesaadav: https://www.law.cornell.edu/uscode/text/18/1832
[137] Moohr, Geraldine S., lk 919. (24)

sisalduva normi sõnastus ja selle eesmärk ning parema regulatsiooni loomiseks võtta arvesse ka teiste riikide kogemusi.

Kokkuvõte

Töö peamiseks eesmärgiks oli selgitada välja, kas hetkel kehtiv ärisaladuse karistusõiguslik regulatsioon tagab efektiivse ärisaladuse kaitse ning pakkuda välja võimalikud lähenemisviisid ärisaladuse karistusõigusliku regulatsiooni muutmiseks. Samuti oli töö eesmärgiks analüüsida ärisaladuse karistusõiguslikku regulatsiooni, lähtudes käimasolevast tööstusomandi kodifitseerimise protsessist ning analüüsida ärisaladuse regulatsiooni muutumist seoses ärisaladuse käsitlemisega tööstusomandi alaliigina. Sellest tulenevalt oli töö hüpoteesiks väide, et Eestis kehtiv karistusõiguslik ärisaladuse kaitse regulatsioon ei täida ärisaladuse kaitse eesmärki parimal võimalikul viisil.

Ärisaladus on oma olemuselt teave, mis on seda kasutavale ettevõtjale majanduslikult tulus ning tagab turul konkurentsieelise. Ärisaladuse kaitse tekkeks on vajalik, et see teave oleks saladus, ehk ei ole samas valdkonnas tegutsevatele ettevõtjatele teada ning ettevõtja peab ise pidama seda teavet piisavalt väärtuslikuks, et selle kaitseks mingeid meetmeid kasutusele võtta. Ärisaladuse kaitsmise peamine eesmärk on tagada majanduse areng läbi selle, et võimaldatakse ettevõtjatel keskenduda teenuste ja toodete arendamisele ning panustama mõnevõrra vähem igasugu kaitsemeetmetele, mis takistaksid konkurentidel ettevõtte kasulikku teavet omandamast. Ärisaladuse efektiivne kaitse võimaldab ettevõtjatel investeerida suurema summa ettevõtluse arendamisse ning pidada tehingupartneritega läbirääkimisi, kartmata ärisaladuse vargust. Samuti võimaldab ärisaladuse kaitse ettevõtjatel valida tööle paremate oskuste ja teadmistega töötajad, mitte keskenduma pigem töötajate lojaalsuse väljaselgitamisele, kartuses, et töötaja võib ettevõtja ärisaladust teades luua konkureeriva ettevõtte või minna teise ettevõttesse tööle. Samas ei tohi ärisaladuse kaitse reguleerimisel ära unustada ka töötajate põhiseadusest tulenevaid õiguseid, milleks on näiteks õigus vabalt valida oma töö- ja ametikohta (PS § 29). See tähendab, et ettevõtjate soodustamise eesmärgil loodud ärisaladuse kaitsega ei tohi hakata liialt piirama töötajate õiguseid, vaid tuleb leida sobiv tasakaal.

Eestis on ärisaladuse regulatsioon nii konkurentsiseaduses, töölepingu seaduses, võlaõigusseaduses, äriseadustikus kui ka karistusseadustikus. See tähendab, et Eestis kehtiv ärisaladuse regulatsioon on jagatud erinevate seadusesätete vahel ning tegelikkuses puudub terviklik ülevaade ärisaladuse olemusest ja ärisaladuse kaitsmise võimaluste leidmine on raskendatud. Sellest ning Euroopa Liidu ärisaladuse kaitse regulatsiooni ühtlustamisest tulenevalt loodi Eestis intellektuaalomandi kodifitseerimise töögrupp. Töögrupp on praeguseks loonud tööstusomandi seadustiku eelnõu, mille kohaselt soovitakse ärisaladust reguleerida

tööstusomandi valdkonda kuuluva õigusena. See tähendab, et ärisaladuse reguleerimiseks on valitud lähtekoht, milles ärisaladust käsitletakse omandisarnase õigusena. See tooks praegu kehtivas ärisaladuse regulatsioonis kaasa mitmeid muudatusi.

Põhiline muudatus ärisaladuse omandisarnase õigusena käsitlemisel oleks see, et ärisaladuse kaitseks oleksid rakendatavad need sätted, mis kaitsevad omandit. Selline lähenemine looks ettevõtjatele paremad eraõiguslikud õiguskaitsevahendid, mis võimaldaksid ärisaladuse rikkumise korral esitada nõudeid ka alusetu rikastumise sätete alusel (VÕS § 1037 ja § 1039) ning esitada ka VÕS § 1055 lõikest 3 tuleneva kahju tekitava tegevuse lõpetamise nõude. Ilmselt omaks preventiivset mõju ärisaladuse rikkumise vähendamisele ka efektiivsete tsiviilõiguslike kaitsemeetmete olemasolu ning ärisaladuse karistusõiguslik kaitse võiks jääda ärisaladuse raskete rikkumiste puhuks, kus ettevõtja on kannatanud suurt kahju või on ettevõtja rikkumiseelse olukorra taastamine vähe tõenäoline või võimatu.

Juhul, kui ärisaladust käsitleda tööstusomandi alaliigina ning võtta arvesse seda, et põhiseaduse § 32 kohaselt hõlmab omandi puutumatus ka intellektuaalomandi liike, siis ilmselt peaks ärisaladus kui omandisarnane õigus samuti olema kaitstud kõikide isikute rikkumiste eest, mitte üksnes töötajate rikkumiste eest, nagu ta seda hetkel kehtiva KarS § 377 järgi on. Samuti tuleks üle vaadata ka ärisaladuse kaitsenormide asukoht karistusseadustikus. Hetkel asub KarS § 377, mis kaitseb ettevõtjaid ärisaladuse õigustamatu avaldamise ja kasutamise vastu, majandusalaste süütegude peatükis, kuid ärisaladuse tööstusomandi alaliigina peaks ta olema reguleeritud karistusseadustiku 14. peatükis ehk intellektuaalse omandi vastaste süütegude peatükis. Praegu reguleeritakse tööstusomandi õiguse rikkumist KarS § 226 ning rikkumise korral on karistusena ette nähtud rahatrahv, mis näitab et tegemist on väärteona käsitletava rikkumisena. Arvestades ärisaladuse omadusi ning sisulist erinevust teistest tööstusomandi õigustest, võib kindlalt väita, et kui reguleerida ärisaladus lihtsalt koos teiste tööstusomandi õigustega KarS § 226, siis jääks ärisaladus olulisel määral kaitseta. Samas, kui võtta arvesse, et intellektuaalomandi õigused on oma olemuselt siiski eraõigused ning nende reguleerimisel tuleks lähtuda *ultima ratio* põhimõttest, mille kohaselt tuleks eraõiguslikke õiguseid kaitsta ka eelkõige eraõigusest tulenevate õiguskaitsevahenditega ning karistusõigus peaks rakenduma üksnes juhul, kui eraõiguslikest õiguskaitsevahenditest ei piisa, siis võib argumenteerida, et võib-olla piisakski sellisel juhul üksnes ärisaladuse rikkumise korral väärteokaristatavusest. Samas aga tundub selline seisukoht olevat tasakaalust väljas, kui võtta arvesse üldiselt ärisaladuse omadusi ning ärisaladuse olulisust majandustegevuses, samuti seda, et mitmetel juhtudel ei ole võimalik ärisaladuse rikkumise korral taastada ka ettevõtja rikkumiseelset õiguspositsiooni, mistõttu võiks mõningatel juhtudel, näiteks, kui ärisaladuse väärtus on jäädavalt kadunud, kaaluda siiski

ka karistusõiguslikku vastutust. Lisaks aga tuleks arvestada ka asjaoluga, et kui ärisaladus oleks omandisarnane õigus ning ärisaladuse kaitse oleks suunatud omandi kaitsele, siis juhul, kui ärisaladus oleks salvestatud näiteks kõvakettale ning see kõvaketas ettevõttest varastataks, siis võiks kõne alla tulla ka karistusseadustikus sätestatud varguse koosseis ning sellisel juhul tuleks asja ehk kõvaketta väärtust arvestada ka lähtuvalt sellel olevast teabest. See tähendab, et kui käsitleda ärisaladust tööstusomandi alaliigina, tuleb kindlasti üle vaadata ka ärisaladuse karistusõiguslik regulatsioon.

Arvestades aga ärisaladuse erinevuseid teistest intellektuaalomandi liikidest ja ka Eesti kohtute senist seisukohta, mille kohaselt ei ole ärisaladuse puhul tegemist õigusega, mis peaks olema kaitstav võrdselt intellektuaalomandiga, võib eelnev ärisaladuse käsitlus olla meie õiguskultuuris mitte aktsepteeritav. Ärisaladuse puhul on üheks peamiseks erinevuseks asjaolu, et ta ei välista täielikult teiste isikute õiguseid, ehk tegemist ei ole absoluutse õigusega. Samuti peab ärisaladus kaitse saamiseks olema salajas, kuid teiste intellektuaalomandi õiguste puhul kehtib pigem vastupidine nõue, ehk näiteks patent peab olema registreeritud ja avalik, et see oleks kaitstud. Samuti peab näiteks patendikaitse tagamiseks olema tõendatud, et tegemist on erilise ja uudse lahendusega, mis toob riigi majandusele ja ühiskonnale tulu läbi selle, et seda on võimalik kasutada ja samasuguse toote leiutamisesse ei tule enam investeerida ning vastutasuks selle eest tagatakse loojale mingi perioodi vältel täielik kaitse ja konkurentsieelis. Ärisaladuse puhul aga hoitakse teavet salajas, mistõttu ei saa ühiskond seda kasutada ning mingisugune tehniline informatsioon võib ühiskonna eest salajaseks jääda väga pika aja jooksul. Lisaks sellele ei ole võimalik kuidagi enne ärisaladusele kaitse tagamist veenduda, et tegemist on tõepoolest väärtusliku ja kasuliku teabega, kuna ärisaladust sisustavad ettevõtjad siiski eelkõige ise. See tähendab, et ärisaladuse puhul tagatakse kaitse suhteliselt ebaselgele väärtusele. Ärisaladuse väärtus selgub alles järelkontrolli käigus, kui ärisaladust on rikutud ja ettevõtja pöördub rikkumisega kohtute poole. Lisaks tuleks ärisaladuse kaitse sätestamisel arvestada ka praegu Eesti kohtutest läbi käinud ärisaladuse rikkumise kaasuseid, mille kohaselt nähtub, et tegelikult on enamjaolt tegemist siiski turundustegevuse valdkonda kuuluva informatsiooniga nagu näiteks kliendiandmebaasid või hinnakujundusmeetodid, mida ettevõte tegelikkuses arendaks ka juhul, kui puuduks tugev ärisaladuse kaitse. Seega võttes arvesse neid asjaolusid, tundub, et ärisaladusele intellektuaalomandiga võrdse kaitse tagamine võib olla ülemäärane reguleerimine ning ärisaladuse efektiivse kaitse tagamiseks võiks ärisaladust lugeda pigem teiste intellektuaalomandiga sarnanevaks, kuid luua ärisaladuse kaitseks efektiivsed normid eraldi tööstusomandi alaliikide normidest.

Ärisaladust on võimalik kaitsta kahte sorti rikkumiste vastu. Ühel juhul on rikkujateks need isikud, keda ettevõtja on usaldanud, kes on ettevõtjaga kas töösuhtes või lepingulises suhtes ning kes on õiguslikul viisil saanud teada ettevõtja ärisaladuse ning seejärel rikuvad seda, kuritarvitades seeläbi ettevõtja usaldust. Teisel juhul rikuvad ettevõtja ärisaladust kolmandad isikud, kes jäävad ettevõttest väljapoole ning kes juba ärisaladusele ligipääsu saades on rikkunud ühiskondlikult aktsepteeritavaid käitumisnorme, ehk sisuliselt on tegemist ärisaladuse nö varastamisega, kuid mitte KarS § 199 sisalduva varguse koosseisu mõttes.

Eestis on karistusõiguslikult otsustatud reguleerida üksnes esimesena välja toodud rikkumise võimalust ning seda üksnes töötajate suhtes, mitte lepingupartnerite suhtes (KarS § 377). Seega tagab ärisaladuse karistusõiguslik regulatsioon ärisaladuse kaitse üksnes töötajate rikkumise korral ning üksnes juhul, kui töötajad on ärisaladusele ligipääsu saanud seaduslikult. See tähendab, et olukorras, kui mõni ettevõtteväline isik või töötaja saavad ärisaladusele ligipääsu omavoliliselt ning seejärel seda rikuvad, siis jääb ettevõtjal üle kohaldada üksnes tsiviilõiguslikke kaitsevahendeid. Eesti karistusõigusliku ärisaladuse kaitse regulatsiooni puhul puudub põhjendus selle kohta, miks toob kriminaalkaristuse kaasa üksnes töötajate poolne rikkumine ja üksnes juhul, kui ettevõtja neile ärisaladuse usaldas. Ilmselt võib tegemist olla mingil määral suurema usalduse kuritarvitamisega, kui tavapärane vargus seda on, kuid arvestades, et tekkiva kahju ulatus peaks mõlemal juhul olema üsna samasugune, siis ei ole selge, miks on Eesti õiguses valitud just seesugune lähenemine. Lisaks, kui võtta arvesse, et ettevõtjal on väljapoolt tulenevaid rikkumisi oluliselt keerulisem avastada ja tõendada ning seega pole ka selge, kelle vastu tsiviilõiguslik nõue esitada, siis võiks hoopis väljapoolt tuleneva rikkumise korral ettevõtjale tagada kriminaalmenetluse ja uurimisel seega riigi abi võimaluse.

On ilmne, et olukorras, kus ettevõtte töötajaid või lepingupartnereid seovad ettevõttega konkreetsed lepingud, siis on ettevõtjal ka oluliselt lihtsam end ärisaladuse kuritarvitamise vastu kaitsta, kuna ettevõtjal on selleks puhuks võimalik lepingus kokku leppida kahju hüvitamise kord või leppetrahvid. See tähendab aga seda, et karistusõigusliku kaitse loomisega üksnes juhuks, kui ettevõtte töötaja rikub ärisaladust, ei ole tegelikkuses lähtutud *ultima ratio* põhimõttest, mille kohaselt tuleks karistusõiguslike normide poole pöörduda üksnes juhul, kui eraõiguslikud ja muu õigusvaldkonna normid ei taga isiku õiguste kaitset vajalikul määral. Võiks lausa öelda, et olukorras, kus isikul on ettevõtjaga kehtiv tööleping, on hetkel kehtivate normide kohaselt kõige rohkem tsiviilõiguskaitsevahendeid võimalik kasutada, mistõttu peaks sellisele rikkumisele kohaldama eelkõige eraõiguslikke vahendeid ning mitte pöörduma karistusõiguse poole.

Saksa õiguses on olemas sarnane norm Eesti õiguses kehtiva normiga. Saksa õiguse kohaselt on karistatav see, kui töötaja avaldab õigusliku aluseta töösuhte kestel ärisaladuse, mis on talle teatavaks saanud tööülesannete käigus. Eesti regulatsiooni kohaselt on karistatav nii avaldamine kui kasutamine ning karistatavus ei sõltu avaldamise või kasutamise ajast. Saksa konkurentsiseaduse kommentaar ütleb, et selline regulatsioon on ette nähtud selleks, et ei piirataks töötaja vaba liikumist pärast töösuhte lõppu. Saksa õiguses on siiski pärast töösuhte lõppu karistatav ka seesugune ärisaladuse rikkumine, mis on toime pandud kasutades tehnilisi abivahendeid – seega peab nähtuma töötajal selge kavatsetus ärisaladuse rikkumisele. Samuti on Saksa õiguses karistatav ka väljapoolt ettevõtet tulenev ärisaladuse rikkumine, mis on toime pandud konkurentsi, isikliku kasu, kolmanda isiku kasu või ettevõtjale kahju tekitamise eesmärgil ning karistatav on nii ärisaladuse avaldamine kui ka kasutamine. See tähendab, et Saksa õiguses reguleeritakse ärisaladuse rikkumist ulatuslikumalt ja täpsemalt, reguleerides erinevaid rikkumise võimalusi erinevate normi lõigete kujul. Samuti on ette nähtud karmimad karistused eriti raskete juhtumite puhul ning need juhtumid hõlmavad üldiselt ärisaladuse rikkumisi, kus rikkuja teadlikult ja tahtlikult avaldab ettevõtja ärisaladuse välismaisele ettevõtjale või rikub ärisaladust eesmärgiga seda välismaal kasutada.

Rootsi õiguses on otsustatud võtta vastupidine lähenemine sellele, millest lähtutakse Eesti õiguses. See tähendab seda, et Rootsi õiguses on peetud ettevõtjate huvide kaitsmisest olulisemaks töötajate vaba liikumise võimaluse kaitsmist ning seetõttu puudub karistusõiguslik ärisaladuse kaitse regulatsioon töötajate suhtes. See tähendab, et Rootsi õiguse kohaselt vastutavad ettevõtja töötajad ärisaladuse rikkumise eest üksnes eraõiguslikus korras ning on kohustatud hüvitama ettevõtjale tekitatud kahju. Nimelt on Rootsi ärisaladuse kaitse akti artiklis 2 sätestatud, et akt kohaldub üksnes õigustamatutele ärisaladuse rikkumistele ning õigustamatuks ärisaladuse rikkumiseks ei loeta olukorda, kus keegi, kes algselt omandas ärisaladuse seaduslikul teel, selle hiljem avaldab või seda kasutab. See tähendab seda, et ka ettevõtte lepingupartnerid, kes läbirääkimiste käigus said teada ettevõtja ärisaladuse, ei vastuta karistusõiguslikult ärisaladuse rikkumise eest.

Rootsi ärisaladuse karistusõiguslik regulatsioon kohaldub seega üksnes nendele juhtudele, kus isikud on ärisaladusele ligipääsu saanud tahtlikult ja ilma loata ning karistusõiguslik vastutus järgneb ka juhul, kui isik sai ärisaladuse teada läbi kellegi teise, kelle kohta ta teadis või oleks pidanud teadma, et see isik sai ärisaladuse teada ilma ettevõtja loata ehk õigustamatult. Karistuse määramisel võetakse arvesse ka rikkumise raskust, mis sõltub teo ohtlikkusest ning tekitatud kahju ulatusest. Seetõttu, et Rootsi ärisaladuse kaitse akt kohaldub üksnes õigustamatutele ärisaladuse rikkumistele ning ärisaladuse kahjustamise korral, kui see

esialgselt saadi õiguspäraselt, karistusõiguslikku vastutust ei järgne, on Rootsi ärisaladuse kaitse akt saanud ka palju kriitikat. Näiteks juhul, kus ettevõtte töötaja avaldab ärisaladuse teisele isikule, kes selle omakorda edasi avaldab, pääseb esimene isik ehk ettevõtte töötaja karistusõiguslikust vastutusest, kuid teine isik, kellel esialgu ärisaladusele ligipääs puudus, kuid kes selle omal initsiatiivil hankis, vastutab karistusõiguslikult spionaaži eest. Sellest hoolimata on Rootsi ärisaladuse kaitse reguleerimisel jäänud siiani töötajate vaba liikumist pooldavaks ning taganud ettevõtjatele ka efektiivsed eraõiguslikud õiguskaitsevahendid, mis lihtsustavad kahju ulatuse kindlaks tegemist.

Kolmanda võrdlusriigina võib välja tuua Ameerika Ühendriikide ärisaladuse kaitse regulatsiooni. Ameerika ühendriikides on ärisaladuse karistusõiguslik kaitse kehtinud alates 1996. aastast, mis tähendab, et regulatsiooni on rakendatud pikalt ning seetõttu võib olla otstarbekas Eesti karistusõigusliku ärisaladuse kaitsenormi muutmisel arvesse võtta ka USA regulatsioonile osaks saanud kriitikat. Ameerika Ühendriikides on ärisaladuse karistusõiguslik kaitse oluliselt karmim, kuid seda rakendatakse ka üksnes raskete rikkumiste korral. Rasketeks rikkumisteks peetakse üldjuhul juhtumeid, kus ärisaladus püütakse viia välismaale, või kus ärisaladust püütakse müüa kõrgeima pakkumise teinud konkurendile, või kus ettevõtja juhtivtöötaja keskendub enne konkurendi juures tööle asumist võimalikult suures ulatuses ärisaladuse teadasaamisele, või kus ärisaladuse rikkujat rahastatakse välismaise valitsuse rahadega. See näitab, et arvestades Eestis siiani kohtutes menetletud ärisaladuse rikkumistega, kus peamiselt on ettevõtjalt kaasa võetud hinnapakkumised või kliendinimekirjad, siis on ilmne, et Ameerika Ühendriikide ärisaladuse rikkumiste juhtumitega ei ole neid võimalik võrrelda. Ka karistusena on Ameerika ühendriikides ette nähtud kuni 5 miljoni dollari suurune rahaline karistus ja/või vangistus kuni 10 aastat. Kuid, nagu juba öeldud, tasuks arvesse võtta regulatsioonile osaks saanud kriitikat.

Majandusspionaaži akt on saanud väga suurt kriitikat just seetõttu, et selle sõnastus ei ole piisavalt läbi mõeldud ning võib olla konarlik või laiahaardeline. Samuti on öeldud, et niivõrd karmid karistused pigem pärsivad majanduse arengut, kuna takistavad töötajate liikumist, sätestades karmid karistused nii töötajatele kui ka neid palkavatele ettevõtetele ning samuti on ühe argumendina välja toodud seda, et tegelikkuses kulutavad ettevõtjad oma raha siiski ärisaladuse kaitsemehhanismide väljatöötamisele, kuna ka ärisaladust ebaseaduslikult omandada soovivad ettevõtted panustavad rohkem, et tugevalt kaitstud ärisaladust kätte saada ning seetõttu võib niivõrd tugev regulatsioon tegelikkuses osutuda majanduslikult pigem kulukaks. Sellest tulenevalt on sageli asutud seisukohale, et enne karistusõiguslikku ärisaladuse rikkumise reguleerimist oleks pidanud eelkõige panustama tsiviilõiguslikule regulatsioonile

ning selle puudujääke täiendama karistusõigusliku regulatsiooniga. Seega võiks ka Eestis enne karistusõigusliku sätte korrigeerimist korda seada eraõiguslikud ärisaladuse kaitsevahendid. Samuti peaks karistusõiguslik regulatsioon olema ette nähtud üksnes raskete ärisaladuse rikkumise juhtudel.

Erinevate riikide võrdlusest selgub, et võimalusi ärisaladuse kaitse karistusõiguslikuks regulatsiooniks on väga mitmeid, kuid oluline on leida tasakaal ettevõtjate huvide ja töötajate huvide vahel. Praegu Eestis kehtiv ärisaladuse kaitse karistusõiguslik regulatsioon pigem ületähtsustab ettevõtjate huve võrreldes töötajate huvidega ning tegelikkuses ei taga ka efektiivset ärisaladuse kaitset. Arvestades, et karistusõiguslik vastutus ärisaladuse rikkumise korral järgneb üksnes töötajale ning ärisaladust kasutama hakkav uus ettevõte ei vastuta kuidagi ärisaladuse rikkumise eest, siis ei ole kindlasti tegemist hea preventiivse meetodiga. Lisaks tuleb arvestada ka sellega, et hetkel puuduvad Eestis ka head eraõiguslikud õiguskaitsevahendid, millega ettevõtjatelt saadud kasu välja nõuda või mille alusel nõuda rikkumise lõpetamist, siis kindlasti üksnes töötajate karistusõigusliku vastutuse sätestamine ei taga head ärisaladuse kaitset. Ärisaladuse karistusõigusliku kaitse reguleerimisel tuleb lisaks olemasolevatele eraõiguslikele õiguskaitsevahenditele arvestada ka teiste valdkondade õigusnormidega. Näiteks tuleb arvesse võtta andmekaitse ja ettevõtte töötaja privaatsuse kaitseks loodud norme ning uurida, kas ettevõtjal üldse on piisavalt võimalusi rikkumise korral tõendeid koguda või jääb isegi eraõiguslike normide olemasolu korral parimaks tõendite kogumise meetodiks kriminaalmenetlus. Eesti ettevõtetes on töötajatel üldiselt lubatud tööandja meilikonto kasutamine ka erakirjade saatmiseks, samas on tööandjal väga piiratud võimalused kontrollimaks töötajate kirjade sisu ning isegi rikkumise kahtluse korral ei pruugi ettevõtjal olla piisavalt vahendeid rikkumise kontrollimiseks või tõendite kogumiseks, kui tegemist on töötaja erakirjadega. Seega tuleb ärisaladuse kaitse reguleerimisel arvestada väga mitmete aspektidega.

Karistusõiguslikult võiks reguleerida siiski vaid raskemaid ärisaladuse rikkumisi. Üheks võimaluseks oleks karistusõiguslik vastutus sätestada üksnes tehnilist laadi ärisaladuste rikkumiste puhuks, mis eeldatavasti toovad ettevõtjale kaasa ka raskemad tagajärjed, kuid sel juhul tuleb otsustada, kui keeruline on erinevaid ärisaladuse liike teineteisest eristada ning otsustada, kas selline lähenemine tasuks end ära. Võimalik, et erinevate liikide eristamine võib olla liialt keerukas, et tagada efektiivset kaitset. Teise võimalusena võiks ärisaladuse rikkumisega tekitatud kahju ulatusest lähtuda ning sätestada karistusõigusliku vastutuse üksnes mingist kahju piirist alates. Kolmanda võimalusena võiks arvesse võtta tekitatud kahju või kahju tekkimise võimalust lähtuvalt teo raskusastmest, näiteks ärisaladuse avaldamine võib ettevõtjale tuua kaasa suurema kahju, kui selle kasutamine, kuna avaldamise korral muutub

ärisaladus väärtusetuks ning rikkumise eelset olukorda ei ole enam võimalik taastada, kuid näiteks ärisaladuse kasutamise korral võiks hüvitamise meetmena tulla kõne alla saadud tulu väljanõudmine ning kahju tekitava tegevuse lõpetamine. Samuti võiks ärisaladuse rikkumise karistusõigusliku vastutuse sätestamisel pigem lähtuda teo ja tagajärje raskusest, kui subjektiivsest rikkujast endast ning karistusõigusliku vastutuse sätestamisel peaks võrdselt arvestama nii töötajate kui ettevõtjate huvidega.

Effectiveness of the criminal trade secret protection in Estonia

Summary

The object of this research work is trade secrets and the main purpose of the work is to compare civil and criminal regulation of trade secrets to find out if currently effective trade secret regulation is effective to protect companies' rights and if it takes into account the rights of workers to move freely. The further perspective of the research is to map the existing problems of trade secret regulation and to propose possible solutions for more effective criminal regulation. To analyze trade secrets criminal regulation it is also important to decide whether to treat trade secrets as part of intellectual rights or not.

The hypothesis of this research: Current criminal regulation of trace secrets does not protect trade secrets in the most effective way.

The research work is divided into three main parts. First chapter gives an overview of what really are trade secrets and what are the criteria to qualify some information as trade secrets. First chapter also explains why it is important to protect trade secrets and how should their protection and regulation change if to consider trade secrets as part of intellectual property rights. Second part of the research analyzes trade secrets criminal regulation, which applies to cases where person has legally acquired companies' trade secrets but then uses or discloses it without the consent. To get the better overview of the possible regulation methods it is important to compare Estonia's criminal trade secrets regulation to German's and United States' regulation. Third chapter analyzes trade secrets criminal regulation, which applies to cases of unauthorized acquirement of trade secrets. Shortly, in those cases already the way of acquiring a trade secret is in itself a misappropriation since the way of action is generally unacceptable. To give better overview of possible solutions it is important to compare Estonia's legislation to Germany's, Sweden's and United States' regulation of trade secrets. To conclude the research work author used historical, comparative, analytical and synthetic approach.

Trade secret is information which has economic value for the company and which gives the company commercial advantage in the market. For trade secret protection trade secret as information must be secret and unknown for the parties usually conducting business in the similar market. The company must value its trade secret enough to try to keep it secret and to take special measures to protect it from others. Generally, it is argued that effective trade secret protection helps to decrease unfair competition in economy, being therefore important to both, businesses and public. Stronger regulation in trade secrets law gives better mechanisms for companies to protect their rights and to claim compensation for damage. Better means for

indemnity prevent misuse of trade secrets overall. Effective trade secret protection allows companies to invest in products and research instead of creating strong trade secrets protection themselves. Regulating trade secrets is important not to over regulate. It is essential to create balance between the rights of employers and employees. Employees' free movement between different jobs must be granted but too harsh criminal protection of trade secrets may restrain employees from changing their jobs.

Current regulation of trade secrets is located in many different codes, which means there is no clear understanding or overview of the protective measures that apply for trade secrets. There is an ongoing codification process to codify Estonian's intellectual property rights and the workgroup has proposed to regulate trade secrets as part of intellectual property rights. If to consider that trade secrets are intellectual property rights then it changes the whole perspective of the current understanding of trade secrets and the regulation.

Treating trade secrets as intellectual property rights would mean that all regulating norms that protect property would also apply to trade secrets. This concept would give better civil measures for compensation for damage since it would become possible to claim for unjust enrichment or to request the violator to refrain from further violation. In current regulation those claims do not apply to trade secret misappropriation. Considering trade secrets as part of intellectual property rights is somewhat troublesome. Trade secrets differ from other intellectual property rights since trade secrets cannot absolutely exclude others from using same trade secrets in cases where the other company has obtained the trade secret by all legal means. It means that trade secret rights are not absolute. Other major difference is that intellectual property rights, in order to get the relevant protection must be public, whereas trade secret must be private, in fact, trade secret must be secret to get the protection of law. In this case, trade secret gives less value to community and to economic progress than other intellectual property rights and it is not possible to estimate trade secrets value prior giving it the protection. To consider all the aforementioned and Estonian justice system's view of trade secret infringement as unacceptable act in competition, it is clear that trade secrets are too vague to be protected as intellectual property rights. Intellectual property rights should protect intellectual work, which is controllable and estimated before the protection. Property view in trade secret cases would protect trade secrets excessively strongly and there are ways as effective to protect trade secrets.

Estonia's legislative system protects trade secret with both civil and criminal measures. As already said, trade secrets regulation is not yet systemized and the work to create effective system is on progress. Penal code protects trade secrets from employees' infringements only.

Criminal conduct is disclosing or using trade secrets without authorization if the person became aware of the secret in connection of his or her professional duties. The main principle to regulate some conduct criminally is *ultima ratio* principle, which means that civil rights ought to protect by civil measures and criminal measures should only apply if civil measures alone are not sufficient. As said, trade secret protection currently is not well established and needs many changes in order to ensure effective measures for entrepreneurs but in case of employees who have not terminated their employment contract, there are many possible ways to claim for damages using civil measures. Employers are able to enter into a contractual agreement with the employee to compensate any unlawfully caused damages or to pay contractual penalty in case of unauthorized disclosure or use of trade secret. This means that Estonia's legislative system does not entirely follow the aforementioned *ultima ratio* principle.

There are several different ways to protect trade secrets criminally and ensure stronger preventive measures against trade secrets misappropriation. In Germany trade secrets are also criminally protected. German law protects trade secrets against violations of employees and against violations of out comers. It means that trade secret protection seems more homogeneous and does not create a difference between employees' infringement and other person's infringements. This also grants better protection for trade secrets since trade secrets are protected against the acts when trade secrets are acquired or secured without authority.

Swedish approach for trade secrets regulation is entirely different. Sweden values clearly employees' rights of free movement than employers' rights for their trade secrets. In Sweden, the Act on the Protection of Trade Secrets provides criminal sanctions only for violators who are not employees. Employees are obligated to compensate for damages by civil measures. The act states that it applies only to unwarranted infringements of trade secrets and therefore employees to whom trade secrets are entrusted are not criminally liable. This type of regulation has been an object of criticism since employees who give out trade secrets entrusted to them are not criminally liable but person, who is not an employee but willingly receives the secret and sells it abroad can be sentenced for trade espionage. Despite the critics, Sweden has not yet changed the law and still valuates strongly employees' right of free movement and does not see the need to establish stronger preventive measures.

United States of America has had criminal penalty for trade secrets misappropriation since 1996. For Estonia, it might be useful to look at the critics, which Economic Espionage Act as the penal code of trade secrets in United States has received in order to prevent making the same mistakes. Criminal penalties for trade secret misappropriation in the United States are

severe but they only apply to serious infringements. Cases that are considered to be severe usually contain foreign element. For example it is serious case if theft of a trade secret is meant to benefit a foreign company or foreign country; serious infringement is also when violator tries to sell trade secret for a highest bidder, or if a companies' senior manager plans to leave company but tries to gather as much secret information as possible before termination of the employment contract. It is evident that these cases are not relevant for comparison to the cases in Estonia where most violations are associated to commercial secrets (e.g. customer lists) nevertheless it is important to account for critics.

Economic Espionage Act has received lots of criticism because it regulates trade secrets very widely and strongly, but is rarely enforced. It is said that such harsh criminal penalties restrain economic development as strong criminal regulation restrains employees form free movement. Strong criminal penalties in United States apply also to companies knowingly receiving the trade secret and therefore severe sanctions may force companies to carefully examine the risks of misappropriation while employing a new person and therefore it might be necessary to apply preventive measures in order not to receive competitors' trade secrets with new employees. Overall, it said that before creating strong criminal regulation to protect trade secrets it would have been useful to create civil measures beforehand and leave criminal measures to fill the gaps.

Estonia should consider all possible methods to effectively regulate trade secrets infringements. Before creating effective and acceptable criminal penalties for protection of trade secret it is essential to create effective civil regulation beforehand. For criminal regulation *ultima ratio* principle should be followed. After creating sufficient civil measures for damage compensation trade secret protection should be reevaluated for filling the gaps with criminal regulation.

As said, current criminal trade secret regulation is not effective and does not follow *ultima ratio* principle. Criminal penalties for trade secret protection should apply only in severe cases. One option is to criminalize only technical secrets and leave commercial secrets for civil regulation. Technical secrets usually are of more value and losing those secrets may result in greater damages for companies, therefore it might be useful to protect this kind of secrets criminally. Second option for criminalization is to consider the damages caused by the infringement and apply criminal sanction only if damages exceed some pre-fixed sum. Third option to criminalize trade secrets misappropriation is to consider damages in accordance to the conduct. For example, damages might be greater if the violator discloses trade secret, as there might be no possibility to restore companies' rights since trade secret is permanently lost. Restoration of

companies' rights might be possible when the violator uses the trade secret himself and the value of the secret is not entirely lost. There are several methods to protect trade secrets criminally, however it is essential to take into account other possible measures (civil regulation), consequences and damages caused and subjective elements of the offence. Overall, employees rights and employers rights should be in balance when creating criminal regulation for trade secret protection.

Kasutatud lühendid

KarS – Karistusseadustik

KrMS – Kriminaalmenetluse seadustik

TLS – Töölepingu seadus

TsMS – Tsiviilkohtumenetluse seadustik

TsÜS – Tsiviilseadustiku üldosa seadus

VÕS – Võlaõigusseadus

EEA – Economic Espionage Act

TRIPS-leping – Intellektuaalomandi õiguste kaubandusaspektide leping

UTSA – Uniform Trade Secrets Act

EL – Euroopa Liit

WIPO – Maailma Intellektuaalse Omandi Organisatsioon

Riigikohtu lühendid

RKKK – Riigikohtu kriminaalkolleegium

RKTK – Riigikohtu tsiviilkolleegium

Esimese ja teise astme kohtute lühendid

HMK – Harju Maakohus

Kasutatud materjalide loetelu

Kasutatud kirjandus

1. Adede, Adronico O., Bellmann C., Dutfield G., Melendez-Ortiz, R. (toim) Trading in Knowledge: Development Perspectives on TRIPS, Trade and Sustainability. UK: London Earthscan Publications Ltd, 2003;
2. Andmekaitse Inspektsioon. Töötajate arvutikasutuse privaatsus. Juhendmaterjal ESS1, IKS2 ja TLS3 kokkupuutealade selgitamiseks, 2013. Veebis kättesaadav: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/T%C3%B6%C3%B6tajate%20arvutikasutuse%20privaatsus_.pdf;
3. Baker & McKenzie. Study on Trade Secrets and Confidential Business Information in the Internal Market, Final Study Prepared for the European Comission, Aprill 2013. Arvutivõrgus kättesaadav: http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/130711_final-study_en.pdf (11.04.2017).
4. Bone, Robert G., Secondary Liability for Trade Secret Misappropriation: A Comment – Santa Clara Computer and High Tech Law Journal 2006/529 No 22. Veebis kättesaadav: http://heinonline.org/HOL/Page?handle=hein.journals/sccj22&g_sent=1&collection=journals&id=539
5. Bone, Robert G., The (Still) Shaky Foundations of Trade Secret Law – University of Texas Law Review, Public Law Research Paper 2014, No 563. Veebis kättesaadav: http://ssrn.com/abstract=2445024
6. Bone, Robert, G. A New Look at Trade Secret Law: Doctrine in Search of Justification – California Law Review, Inc. 1998/86, No 2. Veebis kättesaadav: http://www.jstor.org/stable/3481134
7. Bouchoux, Deborah E., Protecting Your Company's Intellectual Property: A Practical Guide to Trademarks, Copyrights, Patents & Trade Secrets. New York: AMACOM 2006. Veebis kättesaadav: http://site.ebrary.com.ezproxy.utlib.ut.ee/lib/tartu/detail.action?docID=10005784
8. Caenegem, William van, „Trade Secrets and Intellectual Property. Breach of Confidence, Misappropriation and Unfair Competition. The Netherlands. Kluwer Law International BV, 2014;

9. Chatterjee, N., Should Trade Secret Appropriation be Criminalized? – Hastings Communication and Entertainment Law Journal. 1996/19, No 873., p 863. Veebis kättesaadav: http://heinonline.org/HOL/Page?handle=hein.journals/hascom19&id=&page=&collection=journals&id=877
10. Cronin, C. et al. Trade Secrets: European Union Challenge in a Global Economy. International Fragrance Association 2012. Arvutivõrgus kättesaadav: http://www.ifraorg.org/view_document.aspx?docId=22900
11. Dreyfus, R. C., Trade Secrets: How Well Should We Be Allowed To Hide Them? The Economic Espionage Act of 1996. – Fordham Intellectual Property Media and Entertainment Law Journal. 1999/9, No 1;
12. Friedman, David, D., et.al, Some Economics of Trade Secret Law – Journal of Economic Perspectives. 1991/5, No 1. Veebis kättesaadav: http://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.5.1.61
13. Gabral, K., ITs ja ehituses kahmatakse spetsialiste – Äripäev 6.02.2017. Veebis kättesaadav: http://www.aripaev.ee/uudised/2017/02/06/it-sektoris-kahmatakse-spetsialiste;
14. Godfrey, Eleanore, R. Inevitable Disclosure of Trade Secrets: Employee Mobility v. Employer's Rights – Journal of High Technology Law Volume 2004/161, No 3. Veebis kättesaadav: http://heinonline.org/HOL/Page?handle=hein.journals/jhtl3&g_sent=1&collection=journals&id=152
15. Harte-Bavendamm, Henning; Henning-Bodewig, Frauke, Gesetz gegen den unlauteren Wettbewerb (UWG), Kommentar, 3 Auflage (2013), Beck, München. Veebis kättesaadav: beck-online.beck.de
16. Hasselblatt, Bossel von, MAH Gewerblicher Rechtsschutz. Gesetz gegen den unlauteren Wettbewerb (UWG) (Die Tatbestände rn 15-52), Kommentar, 4 Auflage (2012), Beck, München. Veebis kättesaadav beck-online.beck.de
17. Hogan Lovells International LLP. Study on Trade Secrets and Parasitic Copying (Look-alikes) MARKT/2010/20/D. Report on Trade Secrets for the European Commission. 2012. Veebis kättesaadav: ec.europa.eu/internal_market/.../trade-secrets/120113_study_en.pdf
18. Johnson, James, A., Keeping Your Secrets Secret – New York State Bar Association Journal, 2015/87, No. 6. Veebis kättesaadav: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2650449

19. Karistusseadustiku kommenteeritud väljaanne. Koost. Sootak, J., Pikamäe, P. jt. Tallinn: Juura 2015;
20. Kelli, A., Sehver, A., Härmand, K., et al. Seletuskiri tööstusomandi seadustiku ning autoriõiguse ja autoriõigusega kaasnevate õiguste seaduse rakendamise seaduse eelnõu juurde. 22.07.2014 Veebis kättesaadav: http://www.just.ee/sites/www.just.ee/files/rakendusseaduse_seletuskiri_22-7-2014.pdf
21. Köhler/Bornkamm, Gesetz gegen den unlauteren Wettbewerb (UWG) (Tatvoraussetzungen rn 44-47), Kommentar, 35 Auflage (2017), Beck, München. Veebis kättesaadav beck-online.beck.de
22. Krotoski, Mark. L, Common Issues and Challenges in Prosecuting Trade Secret and Economic Espionage Act Cases – Economic Espionage and Trade Secrets, 2009/57 No 5. Veebis kättesaadav: http://www.justice.gov/usao/eousa/foia_reading_room/usab5705.pdf
23. Kudlich, Beck'scher Online Kommentar StGB, v. Heintschel-Heinegg 32 Auflage (2016), Veebis kättesaadav beck-online.beck.de
24. Lemley, M. A., The Surprising Virtues of Treating Trade Secrets as IP Rights – Stanford Law Review, 2008/61, No. 2. Arvutivõrgus kättesaadav: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1155167
25. Levin, M., Protection of trade secrets through IPR and unfair competition law. – AIPPI (International Association for the Protection of Intellectual Property) Research Question Q 215., 2010. Veebis kättesaadav: aippi.se/files/user/aippi/Q215_SE.pd
26. Lilja, J., Johansson-Heigis, B., Employee privacy and protection of trade secrets at odds in Finland, 2015. Veebis kättesaadav: http://www.lexology.com/library/detail.aspx?g=66ff497f-ee6a-4d8e-a580-b88443c8030d
27. Martin, Derek P., An Employer's Guide to Protecting Trade Secrets from Employee Misappropriation – Brigham Young University law review 1993. Veebis kättesaadav: http://heinonline.org/HOL/Page?handle=hein.journals/byulr1993&g_sent=1&collection=journals&id=959
28. McGuire, M.-R., Germany. Protection of Trade Secrets through IPR and Unfair Competition Law – AIPPI Research Question Q215, 2010. Veebis kättesaadav: https://www.aippi.org/download/commitees/215/GR215germany_en.pdf
29. Merges, Robert P., Menell, Peter S., Lemley, Mark A. Intellectual property in the new technological age. New York : Aspen Publishers ; Austin [etc.] : Wolters Kluwer Law & Business, 2007.

30. Moohr, Geraldine S. The Problematic Role of Criminal Law in Regulating Use of Information: The Case of The Economic Espionage Act – North Carolina Law Review. 2002/80, No 3. Veebis kättesaadav: http://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=3981&context=nclr
31. Nuno, Sousa, S. What exactly is a trade secret under the proposed directive? – Journal of Intellectual Property Law and Practice 2014/9 No 11. Veebis kättesaadav: https://doi.org/10.1093/jiplp/jpu179
32. Ohly, A., Sosinitza, O., Gesetz gegen den unlauteren Wettbewerb (UWG), Kommentar, 7 Auflage (2016), Beck, München. Veebis kättesaadav: beck-online.beck.de
33. Pooley, J. Trade Secrets: The Other IP Right – WIPO Magazine 2013/03. Veebis kättesaadav: http://www.wipo.int/wipo_magazine/en/2013/03/article_0001.html
34. Pooley, J., The Top Ten Issues According to Trade Secret Law – Temple Law Review 1997/70. Veebis kättesaadav: http://heinonline.org/HOL/Page?handle=hein.journals/temple70&g_sent=1&collection=journals&id=1191
35. Pooley, James A.H., Lemley, Mark A., Toren, Peter J., Understanding the Economic Espionage act of 1996. – Texas intellectual property law journal, 1997/5. Veebis kättesaadav: http://heinonline.org/HOL/Page?handle=hein.journals/tipj5&collection=journals&startid=&endid=250&id=197
36. Riigikogu X koosseis. Karistusseadustiku ja selle muutmisega seonduvate seaduste muutmise seadus 931 SE, 07.06.2006
37. Riigikogu X koosseis. Karistusseadustiku ja selle muutmisega seonduvate seaduste muutmise seadus 931 SE, 07.06.2006 lk 56
38. Riigikogu XII koosseis. Karistusseadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seadus 554 SE, 18.06.2014
39. Sandeen, S. K. – P. K. Yu (toim). Intellectual Property and Information Wealth: Issues and Practices in the Digital Age, Vol 2: Patents and Trade Secrets. Texas: Praeger Publishers 2007. Veebis kättesaadav: http://books.google.ee
40. Schultz, M., Lippoldt, D., Approaches to Protection of Undisclosed Information (Trade Secrets): Background Paper, OECD Trade Policy Papers, 2014, No. 162. Veebis kättesaadav: http://dx.doi.org/10.1787/5jz9z43w0jnw-en
41. Shakya, S., Trade Secrets & Its Protection as Intellectual Property: Revisiting IPR Regime, 2014. Veebis kättesaadav: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2399311

42. Tonell, M., The Protection of Trade Secrets and Know-How in Sweden. Swedish report. ADN Law Advokatfirma KB. Stockholm, 2015. Veebis kättesaadav: www.ligue.org/uploads/documents/.../2015rapportsuedoisB.pdf
43. Tööstusomandi seadustik. 22.07.2014. Veebis kättesaadav: https://ajaveeb.just.ee/intellektuaalneomand/wp-content/uploads/2014/08/ToS-EN-22-7-2014.pdf
44. Varul, P., jt. (koostajad). Asjaõigusseadus I. Kommenteeritud väljaanne, Tallinn: Juura, 2014;
45. Varul, P., jt (koostajad). Tsiviilseadustiku üldosa seadus. Kommenteeritud väljaanne, Tallinn: Juura, 2010;
46. Varul, P. jt. (koostajad). Võlaõigusseadus III osa. Kommenteeritud väljaanne. Tallinn: Juura, 2009.

Kasutatud õigusaktid

1. Eesti Vabariigi Põhiseadus, RT I, 15.05.2015, 2. Võlaõigusseadus RT I, 31.12.2016, 7
2. Karistusseadustik, RT I, 31.12.2016, 14
3. Konkurentsiseadus RT I, 30.12.2014, 15
4. Kriminaalmenetluse seadustik, RT I, 31.12.2016, 46
5. Tsiviilkohtumenetluse seadustik, RT I, 28.12.2016, 22
6. Äriseadustik, RT I, 22.06.2016, 32
7. Euroopa Parlamendi ja Nõukogu direktiiv 2016/943, milles käsitletakse avalikustamata oskusteabe ja äriteabe (ärisaladuste) ebaseadusliku omandamise, kasutamise ja avalikustamise vastast kaitset. Brüssel, 08.06.2016

Teiste riikide kasutatud õigusaktid

1. Act on the Protection of Trade Secrets. (Act 1990:409, of May 31, 1990). Veebis kättesaadav: http://www.wipo.int/edocs/lexdocs/laws/en/se/se005en.pdf
2. EEA U.S Code – Economic espionage. Veebis kättesaadav: https://www.law.cornell.edu/uscode/text/18/1831
3. Gesetz gegen den unlauteren Wettbewerb, Veebis kättesaadav: http://www.gesetze-im-internet.de/englisch_uwg/englisch_uwg.html#p0139

4. Strafgesetzbuch Veebis kättesaadav: http://www.gesetze-im-internet.de/uwg_2004/__17.html. Inglise keeles: http://www.gesetze-im-internet.de/englisch_uwg/englisch_uwg.html#p0139
5. Uniform Trade Secrets Act With 1985 Amendments. Veebis kättesaadav: http://www.uniformlaws.org/

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina _____Marta Mägi_____
(*autori nimi*)

(sünnikuupäev: 02.01.1989)

annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose
Ärisaladuse kaitse karistusõigusliku regulatsiooni efektiivsus kehtivas õiguses,
(*lõputöö pealkiri*)

mille juhendaja on _____Mare Tannberg ja kaasjuhendaja on Jaan Sootak_____,
(*juhendaja ja kaasjuhendaja nimi*)

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

olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.

kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tartus, 02.05.2017