TARTU ÜLIKOOL
ÕIGUSTEADUSKOND
Karistusõiguse osakond

Kristjan Pahk

KRIMINAALMENETLUSE DIGITALISEERIMINE KOHTUEELSES MENETLUSES

Magistritöö

Juhendaja:
Ph D Andreas Kangur

Tartu
2019

SISUKORD

SISSEJUHATUS

Infotehnoloogiliste vahendite kasutamine on muutunud tänases maailmas igapäevaseks ning inimesed ei kujuta enam tegelikkuses ette enda elu ilma nendeta. Innovatiivne lähenemine on muutnud nii mitmedki protsessid meie elus oluliselt lihtsamaks ning produktiivsemaks. Käib pidev võidujooks era- ja avaliku sektori vahel, kes tegelikkuses loovad teineteist toetavaid kaasaegseid lahendusi. Väga tugevalt on põimunud sektoritevaheline koostöö, kus näiteks erafirmad aitavad riigi vajadusest lähtuvalt luua uuri tarkvaraarendusi ning samas vähendavad innovatiivsed avalikud teenused eraettevõtluse bürokraatiakoormust riigi ees.

Väikese riigina on Eesti pikka aega otsinud valdkonda, milles näidata ennast eesrindlikuna ning seeläbi omada ka suuremat sõnaõigust rahvusvahelisel areenil. Viimase paarikümne aasta jooksul on selle nimel tehtud suuri jõupingutusi ja jõutud ka kaugele. Ei saa otseselt väita, justkui oleks Eesti IT-eduloo võtmeks riigi või rahvastiku väiksus. Pigem on kõige aluseks olnud julgus teisiti mõelda. Irooniliselt võib ju väita, et Eesti kui e-riigi areng on saanud võimalikuks tänu riikliku iseseisvuse heitlikule ajaloole, sest pärast taasiseseisvumist on tulnud riigi uuesti ülesehitamiseks vastu võtta mitmeid julgeid otsuseid. Üheks võimaluseks on olnud minna sama rada teistega, kuid õnneks on valitud teine tee ning täna proovib Eesti teha midagi teisiti ning midagi paremini.

Selleks, et inimesed saaksid ennast siinses elukeskkonnas turvaliselt ning hästi tunda, on riigi poolt ülimalt oluline tagada muuhulgas nende turvalisus ning õigusriigile kohaste põhimõtete järgimine. Kriminaalmenetluse seisukohast on oluline kogu menetluse laitmatu toimimine selle algusest kuni lõpuni. Käesolevas töös vaadeldakse eelkõige kriminaalasjade eduka kohtuliku lahendamise eelduseks ning kriminaalmenetluse esimeseks etapiks olevat kohtueelset menetlust, kuid käsitlemist leiavad osaliselt ka teised menetluse faasid ja liigid. Kriminaalmenetluse läbiviimine selle kõikides astmetes on riigi ülesanne ning loomulikult tuleb teha seda parimal võimalikul viisil menetlusosaliste ning kriminaalasjaga puutumuses olevate isikute õigusi järgides. Eesrindliku IT-riigina saab justkui pidada Eesti kohustuseks rakendada e-riigi põhimõtteid ja kaasaegseid tehnoloogiaid ka kriminaalmenetluses.

Infotehnoloogiliste võimaluste kasutamine kriminaalmenetluses, näiteks distantsilt toimikuga tutvumine või kaitseakti elektroonne esitamine muudab kindlasti menetluses osalemise selle osapooltele mugavamaks. Mugavus ei tohiks aga olla eraldi eesmärgiks, vaid oluline on tagada

kiire, menetlusosaliste õigusi järgiv ja oma eesmärki täitev kriminaalmenetlus tervikuna. Ei saa väita, justkui tänases menetluses isikute õigusi ei järgitaks või menetlus oleks ülemäära aeglane, kuid efektiivsuse ja menetluse kiiruse osas on minna veel pikk tee. Töö autori seisukohast on lisaks liigse bürokraatia vähendamisele hetkel realiseerimata veel mitmed võimalused, mis läbi uudsete menetluslahenduste aitaksid saavutada märgatava kokkuhoiu menetlust läbiviival poolel ehk riigil ning menetlusosaliseks olevatel isikutel. Sinna hulka kuulub säästmine nii menetlusele kuluvate rahaliste-, kuid ka sinna panustavate ja seal osalevate inimeste koormatuse ning aja arvelt. Seega on võimalik saavutada tarbetu bürokraatia vähendamisega kõikide menetluspoolte jaoks vähema koormatusega objektiivsem tulem.

Käesolev magistritöö uurib digitaalsete lahenduste kasutamist kohtueelses kriminaalmenetluses. Töö koosneb kolmest peatükist, millest esimene vaatleb lähemalt infoühiskonna arenemist laiemalt ning selle puutumust õigusmaailmaga. Teises peatükis analüüsib töö autor elektroonsete võimaluste kasutamise hetkeseisu ning töö viimases osas leiab põhjalikumat käsitlemist kriminaaltoimikute ja menetluse osaks olevate menetlustoimingute digitaliseerimise võimalikkus ning sellega kaasneda võivad kitsaskohad.

Töö keskendub peaasjalikult kohtueelses menetluses läbiviidavate toimingute digitaliseerimise võimalikkusele. Töö teemat ei tohiks sassi ajada digitaalseid tõendeid puudutavaga. Viimaste hulgas tuleks silmas pidada nn virtuaalseid, tõendamisesemeks kasutatavaid objekte, mis on tajutavad ainult tehniliste vahendite abil ning neid talletatakse andmekandjatel.[1] Digitaalsed menetlustoimingud hõlmavad aga klassikalist kohtueelse menetluse tööd, mille aastaid muutumatuna püsinud metoodika juurde kaasatakse optimaalsema tulemuse saavutamiseks kaasaegse tehnika ning infosüsteemide abi.

Üheks enam kõneainet pakkunud digitaalsuse ja kriminaalmenetluse kokkupuutepunktiks saab pidada digitaalset kohtutoimikut. Tänases menetluses muutub kriminaalasja toimik küll osaliselt digitaalseks prokuratuurist kohtusse saates, kuid kohtueelses menetluses peetakse seda senini paberkandjal. Hetkel käimasolev kriminaalmenetluse revisjon küll käsitleb antud teemat, kuid konkreetsed ajalised eesmärgid on seadmata ning lükatud teadmata tulevikku. Revisjoni käigus on lähemalt analüüsinud täisdigitaliseeritud kriminaalmenetlust küll M. Hirvoja[2], kuid

[1] G. Buzarovska Lazetik, O. Koshevaliska. Digital Evidence in Criminal Procedures. - Balkan Social Science Review XII/2013, lk 65.

[2] M. Hirvoja. Kriminaalmenetluse revisjoni analüüs - üleminek täisdigitaliseeritud kriminaalmenetlusel - 31.05.2016. Arvutivõrgus: https://www.just.ee/sites/www.just.ee/files/uleminek_taisdigitaliseeritud_kriminaalmenetlusele_m_hirvoja.pdf (15.04.2019).

käsitlemist on leidnud peamiselt digitaalne toimik, saavutatava kokkuhoiu üldised printsiibid ning piirdutud on peaasjalikult kohtumenetluse faasiga. Täisdigitaalsele kriminaalasja toimikule üleminekut ei näe töörühm näiteks ette enne 2022. aastat.[3] Lähemalt on digitoimiku rakendamist kohtumenetluses tervikuna käsitlenud veel R. Karja enda 2015. aasta magistritöös[4], sellest tulenevalt keskendub käesoleva töö autor peamiselt kohtueelse menetluse digitoimikut puudutavat, mida eelnevalt käsitletud ei ole.

Digitaalse kriminaalasja toimiku pidamise kaasajastamine aitab küll oluliselt menetlusressurssi kokku hoida, kuid sellest isegi suurem menetluse optimeerimine on võimalik saavutada läbi menetluse sisu moodustavate menetlustoimingute kaasajastamise. Tegelikkuses võtavad just need menetluse algfaasis teostatavad tegevused peamise aja kohtueelse menetluse kogumahust. Lisaks omavad selle etapi käigus kogutud tõendid olulist tähtsust menetlustulemuse osas, sest nende pinnalt hakatakse hilisema kohtumenetluse käigus süüdistatava süüküsimust arutama.[5] Seega on väga oluline pöörata tähelepanu ka kohtueelses menetluses toimetavate asutuste igapäevatööle ning suunata neid võimalikule optimaalsemale tegevusele menetlustoimingute teostamisel. Siinkohal püstitab magistritöö autor hüpoteesi, et tänases kohtueelses kriminaalmenetluses ei kasutata piisavalt kaasaegseid infotehnoloogilisi võimalusi, et saavutada efektiivsem menetlus.

Magistritöö eesmärk on selgitada välja kriminaalmenetluse kohtueelses menetluses koostatava digitaalse kriminaalasja toimiku kasutusele võtmise võimalikkus ning sellega kaasnev võimalik positiivne tulem menetlusökonoomika seisukohast. Tuvastada kohtueelses menetluses digitoimiku kasutusele võtmiseks ning kriminaalmenetluses teostatavate menetlustoimingute kaasajastamiseks vajalikud muudatused kehtivas õiguses. Lisaks teha kindlaks kohtueelses menetluses tõendite kogumisele suunatud menetlus- ja uurimistoimingute digitaliseerimisega saavutatav ressursikokkuhoid. Analüüsida elektroonsete menetluslike võtete rakendamisega kaasnevaid ohte ja seda takistada võivaid tegureid.

[3] Justiitsministeerium. KrMS revisjoni VTK kooskõlastamisel laekunud arvamused ja otsused revisjoni I etapi teemaderingi osas, p 1.1. Arvutivõrgus: https://www.just.ee/sites/www.just.ee/files/ettepanekute_loetelu_ja_otsused.pdf (15.04.2019).
[4] R. Karja. Digitaalne toimik kriminaalmenetluses. Magistritöö. Tartu, 2015. Arvutivõrgus: http://dspace.ut.ee/bitstream/handle/10062/47395/karja_rasmus.pdf? sequence=1&isAllowed=y (15.04.2019).
[5] E. Kergandberg, M. Sillaots. Kriminaalmenetlus. Tallinn: Juura 2006, lk 258.

Uurimisprobleemi käsitlemiseks on töö autor püstitanud järgnevad uurimisküsimused:

1. Millise positiivse tulemi annab täielikult digitaalsele kriminaalasja toimikule üleminek ning millised on sellega kaasnevad ohud? – Küsimuse lahendamise käigus keskendutakse peamiselt kohtueelses menetluses toimiku koostamisele ning pidamisele. Lisaks leiavad põhjalikumalt käsitlemist digitaalset toimikut varitseda võivad ohud ning nende minimaliseerimise võimalused.
2. Milliseid kohtueelse kriminaalmenetluse menetlustoiminguid oleks optimaalsema menetluse tagamiseks võimalik teostada digitaalselt? – Küsimuse lahendamise käigus vaadeldakse lähemalt kohtueelses menetluses teostatavaid menetlustoiminguid, nende sisu ning eesmärgist tulenevat võimalust teostada neid digitaalsete vahendite abil.
3. Millise positiivse tulemi annab kohtueelse menetluse raames menetlustoimingute teostamine digitaalsete vahendite abil ning millised on kaasnevad ohud? – Küsimuse lahendamise käigus vaadeldakse lähemalt kaasaegsete vahendite abil menetlustoimingute teostamise mõju menetlusosalistele. Käsitlemist leiab võimalik kokkupuude isikute põhiõigustega ning lisaks analüüsitakse menetluslike õiguste tagamist takistada võivaid tegureid.
4. Millised on vajalikud muudatused digitaalsete menetlusvõtete kasutuselevõtuks tulevikus? - Küsimuse lahendamise käigus tuuakse välja olulisemad ettepanekud vajalike seadusmuudatuste osas ning juhitakse tähelepanu digitaalsete vahendite kasutamisega kaasneva võivatele kitsaskohtadele. Samas ei keskendu töö otseselt regulatsiooni muutusi puudutavale, vaid ikkagi digitaalsete võtete kasutamisele menetlusmetoodikas.

Loomulikult ei tohiks asuda pealiskaudselt kõikide seniste juurdunud protsesside lammutamisele, vaid eelnevalt tuleb võimalik saavutatav kasu kõrvutada ohtude ja riskidega. Digitaliseerimisega saavutatav edu kohtueelses menetluses ei tohiks omada vastupidist efekti hilisemas kohtumenetluses.[6]

[6] M. Kurm. Kriminaalmenetluse revisjoni analüüs - Tõendite kogumisel dubleerimise vältimine kohtu- ja kohtueelses menetluses - 31.05.2016, lk 2. Arvutivõrgus: https://www.just.ee/sites/www.just.ee/files/toendamine_m._kurm.pdf (15.04.2019).

Magistritöö mahupiirangu tõttu on käsitletud eelkõige kohtueelse menetluse faasi ning kahtlustatavat puudutavat, kuid mõttekäikude paremaks mõistmiseks on kohati käsitletud ka vahetut perioodi pärast kohtueelset menetlust ning antud menetlusfaasis süüdistatava staatuse omandanud isikut puudutavat.

Antud töös kasutatakse kombineeritult kvalitatiivset ja analüütilis-empiirilist uurimismeetodit. Uurimisküsimustele otsitakse vastuseid analüüsides kättesaadavaid materjale koos töö autori poolt läbi viidud vestluste tulemustega. Vesteldud on peamiselt kohtueelset menetlust läbi viivate ametnikega ning lisaks teiste praktikute seisukohtadele tugineb töös käsitletu ka autori enda praktilisel kogemusel.

Kaasaegsete menetlusvõtete kasutamine kriminaalmenetluses on puutumuses peamiselt kahe valdkonnaga. Ühelt poolt õigusega, mis sätestab tingimused ja korra vastavate toimingute kasutamise ja viiside üle. Teiselt poolt puudutab teema aga infotehnoloogia valdkonda, mis seab piirid eelkõige tehniliste vahendite kasutamisele ning loob veelgi suurema väljakutse infosüsteemidele. Nende keskseks teguriks saab aga pidada menetluses osalevat isikut, kes kujuneb justkui indikaatoriks, mis näitab kokkupuutepunkti tulemuslikkust.

Käesolevas töös on rõhk eelkõige õigusvaldkonda puudutaval, kuid samas proovib töö autor enda pädevuse piirides pakkuda välja ka tehnoloogilisi lahendusi kasutajamooduli piires, mis aitab paremini mõista konkreetsete toimingute elektroonseks muutmisega taotletavat tulemit.

Töö teema valik on suuresti ajendatud autori ning teiste praktikute kogemusest, mis on viidanud otsesele vajadusele ümber vaadata tänaste menetlustoimingute teostamise viisi ja elektroonsete vahendite kasutamise nendes käigus. Mahuka töö tulemusel on loodud näiteks E-toimikuga liidestuv ning väga mitmekesiste võimalustega Politsei menetluse infosüsteem, kuid praktikute sõnul ei täida see oma eesmärki ning soovitud kokkuhoidu menetlusressursilt ei ole saavutatud. Samal ajal on kasvanud nii menetlejate kui ka menetlusosaliste infotehnoloogiline teadlikus ning võimekus, mis igati toetavad kaasaegsetele meetoditele üleminekut.

Allikamaterjalidena on töö koostamisel kasutatud nii eesti- kui võõrkeelset kirjandust, eelnevalt kehtinud ning täna kehtivaid õigusakte, kohtupraktikat ning hulgaliselt infomaterjale. Suures osas sisaldab töö erinevate kohtueelset menetlust läbiviivate praktikute seisukohti ning töö autori enda praktilisest kogemusest tulenevat teavet. Teema uudsuse tõttu ei ole menetlustoimingute ja sinna hulka kuuluvate uurimistoimingute digitaliseerimise valdkonda varasemalt suurel määral käsitletud.

Teema vajalikkus on tõstatatud ka kriminaalmenetluse revisjoni käigus, kuid autorile teadaolevalt ei ole käesolevas töös käsitletud teemadega revisjoni käigus süvitsi mindud. Samas näeb autor menetluse kaasajastamise arenguga edasi minemiseks hädavajalikuna käsitleda menetluse algfaasis teostatavaid toiminguid ka iseseisvalt. Toimingute kaasajastamise käsitlus tugineb antud töös peamiselt toimingute metoodikal ning nende eesmärgist tuletatud analüüsil. Rahvusvahelist praktikat ja suundumust vaadeldes piirdub töö Euroopa riikide praktikaga. Etteruttavalt võib öelda, et ka välisriikide kohtueelse menetluse digitaalsusega ei ole enamasti veel algust tehtud ning seetõttu on ka sealne teemakäsitlus minimaalne.

Märksõnad: kriminaalmenetlus, eeluurimine, digitaliseerimine, menetlustoimingud.

1. INFOÜHISKOND

1.1. Tänapäeva infoühiskond

Infoühiskond on informatsiooni tähtsustav ja seda kõigis eluvaldkondades maksimaalselt kasutav (hankiv, tootev, talletav, levitav) ühiskond.[7] *Doctor iuris* Mario Rosentau leiab, et „küsides infoühiskonna järele, peame vaatama, kuivõrd informatsiooni- ja kommunikatsioonitehnoloogia on muutnud normide ja väärtuste alussüsteemi võrreldes seniste ühiskondadega. Ehk kui infoühiskond on uus loomus, peab selles võrreldes senise normide ja väärtuste alussüsteemiga olema tekkinud midagi põhjalikult uut: kas uued normid ja väärtused või koguni ühiskonna käsitamise uus paradigma.“[8] Selle mõiste ja ühiskonnaolemuse justkui enesestmõistetavust saab tõepoolest täna pidada juba paradigmaks, millega kohanemiseks on kujunenud uued normid ja võib öelda isegi ootused millegi seni veel reaalselt hoomamatu suhtes.

Ükski eelnev inimkooslus ei ole ennast väidetavalt nimetanud infoühiskonnaks. Eneken Tikki sõnul ei ole kunagi varem informatsioon ja sellele juurdepääsu võimaldamine olnud ühtaegu rahvusvahelise ja riigisisese poliitika prioriteet ning ükski ühiskond pole tuhandete aastate jooksul eriti juurelnud selle üle, millises ulatuses tuleks indiviidile tagada õigus informatsioonilisele enesemääratlemisele, mil viisil võiks kodumasin rikkuda inimeste privaatsust või millise osa sisemajanduse kogutoodangust moodustab avaliku teabe koguväärtus.[9]

Mõiste infoühiskond on kõigile justkui tuttav, kuid seda formuleerima asudes ei pruugi see enam aga niivõrd lihtne tunduda. Proovides seda terminit tõlgendada, võib esmalt jõuda millegi juurde, mis seostub informatsiooniga. Informatsioonina tuleks siinkohal käsitleda teatavat infot või teadmisi, mis omakorda levivad ühiskonnas. Seeläbi jõuamegi antud mõiste tuumale lähemalt ning seostub see juba informatsiooni vahetuse ja levikuga inimkonna ehk ühiskonna liikmete vahel. Paratamatus on see, et väga suures osas peegeldab inimestele selle mõiste kasutamine ka erinevaid tehnoloogilisi lahendusi. Seda ei saa pidada valeks, sest eelpool

[7] Raamatukogusõnastik. Eesti Rahvusraamatukogu. Arvutivõrgus: https://termin.nlib.ee/view/4830 (31.03.2019).
[8] M. Rosentau. E-tempora, e-mores. - Juridica II/2015, lk 138.
[9] E. Tikk. Informatsioon ja õigus. - Õiguskeel IV/2007, lk 2.

mainitud informatsiooni levitamist lihtsustavadki just eelkõige tehnilised vahendid. Abiks on nii arvutid, arvutivõrgud, kui ka televisioon ning raadio. Siinkohal tuleks jõuda järeldusele, et infoühiskond justkui peegeldab meie tänast võimet planeedil Maa vahetada inimeste vahel teadmisi, uudiseid jms silmapilkselt. Sellist võimalust ei peeta kaugeltki enam utoopiliseks, vaid sellest on kujunenud sõltuvus, ehk elanikkond ei suudaks enam ilma selleta toimida ning kuna suurem osa olmetingimustest tuginevad just infoühiskonna lakkamatul toimimisel, siis selle äkiline lõppemine tooks kaasa endaga küllaltki fataalsed tagajärjed.

Infotehnoloogiliste vahendite kasutamise näol ei ole enam tegemist pelgalt võimalusega, vaid väga suurel määral ka sundliku seisuga. Tihtipeale ei olegi inimestel enam valikuid, kas nad soovivad infotehnoloogilisi vahendeid kasutada või mitte. Tänasel päeval teadvustab pea iga maailmakodanik asjaolu, et me elame infoühiskonnas. Informatsioon ümbritseb meid kõikjal ning elu ilma selleta ei suudeta enam ette kujutada. Infoühiskonda tervikuna iseloomustab väga suur arvutite ning nendega seonduvate võrkude arvukus ja mitmekesisus. Meie igapäevaelu sõltub üha enam elektroonikast ning infotehnoloogilistest vahenditest. Inimesed on sellest tuleneva mugavusega igati harjunud ning tegelikkuses juba väga olulises sõltuvuses. Saadaval olevad lahendusi on lugematul arvul ning esindatud on pea iga eluvaldkond alates reoveemajandusest lõpetades kohtumenetlusega. Kindlasti ei tohiks infoühiskonna mõiste all käsitleda ainult tehnoloogilisi lahendusi, vaid teisalt on tegemist keerulise ühiskonnakorraldusliku nähtusega, mille abil ühiskond omandab, jagab ning ka vahetab informatsiooni väga erineval kujul.

Ettevõtetel lubab IKT kasutuselevõtt optimeerida nii tänaseid äriprotsesse kui ka luua sootuks uusi ja innovaatilisi tooteid ja teenuseid. Üksikisikule annab IKT juurdepääsu lõpututele infovaradele, näiteks maailma kultuuripärandile ja õppematerjalidele, mis avardavad märkimisväärselt võimalusi enda arendamiseks ja oma heaolu suurendamiseks. Avalike teenuste korraldamine ja osutamine IKT lahendustega võimaldab suunata maksumaksja raha valitsusasutuste haldustegevustelt sisuliste ülesannete lahendamisele, luues ühtlasi eeldused suhtlemise lihtsustamiseks kodanikele ja ettevõtetele.[10] Kogu infoühiskonna areng tähendabki enamat kui vaid uute tehnoloogiliste võimaluste kasutuselevõttu. Järjest rohkem räägitakse nimelt IKT nutikast kasutuselevõtust[11], mis viitab, et eesmärk ei ole lihtsalt teenuse või suhtluse

[10] Majandus- ja Kommunikatsiooniministeerium. Eesti infoühiskonna arengukava 2020, lk 4. Arvutivõrgus: https://www.mkm.ee/sites/default/files/elfinder/article_files/eesti_infouhiskonna_arengukava.pdf (15.04.2019).
[11] K. Põder (toim.). Infoühiskond, Tallinn: Statistikaamet 2010. Arvutivõrgus: https://www.stat.ee/publication-download-pdf?publication_id=21188 (15.04.2019).

elektrooniliseks muutmine, vaid see peab kaasa tooma teenuse üldise kvaliteedi tõusu või muul moel hinnatava kasu.[12]

Infotehnoloogia (edaspidi IT) ei ole eesmärk omaette, vaid vahend, mis aitab tõsta eri eluvaldkondade toimimise taset. Sestap peab IT olema läbiv teema kõigi valdkondade poliitikadokumentides.[13] Euroopa Liit on valitsussektori digitaalse arengu kiirendamiseks koostanud tegevuskava aastateks 2016-2020. Antud kava juhindub visioonist, et 2020. aastaks peaksid ELi haldusasutused ja avalikud institutsioonid olema avatud, tõhusad ja kaasavad ning pakkuma piirideta, personaalseid, kasutajasõbralikke, digitaalseid avaliku sektori teenuseid kõigile kodanikele ja ettevõtjatele.[14] Peaasjalikult keskendub kõnealune strateegia küll liikmesriikide turutingimuste parandamisele ning seeläbi majandustegevuse soodustamisele, kuid muuhulgas on eesmärkidena püstitatud ka Euroopa e-õiguskeskkonna portaali loomine ning avaliku sektori digiteenuste kasutusele võtmine tervikuna. Vastav raamdokument on kindlasti üheks oluliselt liidusiseseks suunanäitajaks, mis kinnitab veelgi, et infoühiskonna arengujärku kuhu me jõudnud oleme saab pidada alles alguseks..

Eesti on olnud samuti tubliks e-valitsemise idee levitajaks ning saavutatut on toodud eeskujuks mitmetes riikides, kes Eesti kogemuselt õppides on asunud iseseisvate e-riikide ehitamisele. 2017. aastal Tallinnas toimunud Euroopa Liidu liikmesriikide ja Vabakaubanduspiirkonna riikide (Liechtenstein, Norra, Island ja Šveits) digivaldkonna ministrite kohtumisel allkirjastati Tallinna deklaratsioon[15], mis annab veelgi täpsemad juhised, milliste e-lahenduste ja e-teenuste poole riigid liikuma peaksid. Näiteks jõuti deklaratsioonis ühisele arusaamale, et kõik riigid peavad oma kodanikele ja ettevõtetele looma võimalused tarbida riigiteenuseid digitaalsel teel ja seda kodust lahkumata.

[12] J. Matt, H. Hinsberg, A. Laido. Tulevikuraport: Kuidas infoühiskonna muutused ja mõju enda kasuks tööle panna?, lk 3. Arvutivõrgus: https://heakodanik.ee/wp-content/uploads/2013/09/Infoyhiskonna_raport_0.pdf (15.04.2019).
[13] K. Põder (toim.). Infoühiskond, lk 16.
[14] Euroopa Komisjon. Valitsussektori digitaalse arengu kiirendamine ELis – tegevuskava aastateks 2016–2020, kokkuvõte.
[15] Tallinn Declaration on eGovernment at the ministerial meeting during Estonian Presidency of the Council of the EU – 06.10.2017. Arvutivõrgus: https://www.mkm.ee/sites/default/files/tallinn_egov_declaration_with_signatures.pdf (15.04.2019).

Samuti on plaanis võtta ID-kaardid kasutusele üle Euroopa, et oleks võimalik digiallkirju anda rahvusvaheliselt. Võrreldes 2009. aastal Malmös allkirjastatud e-valitsemise deklaratsiooniga on maailm vahepeal oluliselt muutunud. Inimeste julgeoleku küsimused ei puuduta enam ammu ainult füüsilist turvalisust, vaid küberturvalisus on muutunud vähemalt sama tähtsaks. Tallinna deklaratsiooniga lepiti ka ühiselt kokku, et riigi e-teenuste arendamisel peavad turvalisuse ja privaatsuse põhimõtted vastama kõrgeimatele nõuetele.[16]

1.2. Infoühiskond Eestis

Eesti üheks esimeseks riiklikuks infopoliitikat kujundavaks alusdokumendiks saab pidada 1998. aastal Riigikogu poolt heaks kiidetud arengudokumenti „Eesti infopoliitika põhialused".[17] Dokument sätestab põhimõtted, millest riik peaks infoühiskonna arengut puudutavate poliitiliste otsuste tegemisel lähtuma. Muuhulgas seati eesmärgiks riigi infopoliitika abil majanduse konkurentsivõime tõstmine, eesti keele ja kultuuri säilitamine ning arendamine, demokraatia edendamine ning riigikaitse tõhustamine. Dokumendis käsitletud infoühiskonna arendamise põhimõtteid saab pidada päevakohaseks ka täna.[18]

2004. aastal kiitis valitsus heaks dokumendi „Infopoliitika põhialused aastateks 2004–2006"[19], mis on esimese infopoliitika põhialuseid puudutava dokumendi edasiarendus. Kõnealuse dokumendi puhul on oluline rõhutada ka asjaolu, et see koostati vahetult enne Eesti liitumist Euroopa Liiduga (edaspidi EL), seega kajastusid EL-i infopoliitilised suundumused ja strateegiad (eEurope, eEurope+) ka meie riigisiseses dokumendis. Kui Eesti esimesed kaks infopoliitika dokumenti keskendusid eelkõige infrastruktuuri loomisele ning e-teenuste arendamisele ja kasutuselevõtule, siis 2006. aastal valitsuses heaks kiidetud „Eesti infoühiskonna arengukava 2013"[20]

[16] Majandus- ja Kommunikatsiooniministeerium. Euroopa digiministrid allkirjastasid Tallinna e-valitsemise deklaratsiooni, pressiteade – 06.10.2017.
[17] Eesti infopoliitika põhialuste heakskiitmine. RKo 13.05.1998 - RT I 1998, 47, 700.
[18] K. Põder (toim.). Infoühiskond, lk 15.
[19] Majandus- ja Kommunikatsiooniministeerium. Infopoliitika põhialused aastateks 2004-2006. Arvutivõrgus: https://www.mkm.ee/sites/default/files/infopoliitika_pohialused_2004-2006.pdf (15.04.2019).
[20] Majandus- ja Kommunikatsiooniministeerium. Eesti infoühiskonna arengukava 2013. Arvutivõrgus: https://www.mkm.ee/sites/default/files/eesti_infouhiskonna_arengukava_2006.pdf (15.04.2019).

on sootuks laiema haardega, käsitledes info- ja kommunikatsioonitehnoloogiat (edaspidi IKT) eelkõige kui töövahendit selleks, et muuta ühiskonna ja majanduselu tõhusamaks ning konkurentsivõimelisemaks. Strateegia seadis keskmesse inimese ja tema elukvaliteedi ning nägi ette tegevused kolmes valdkonnas: sotsiaalses, majanduslikus ja institutsionaalses.[21]

2012. aasta sügisest kuni 2013. aasta kevadeni kogunesid Majandus- ja Kommunikatsiooniministeeriumi ning Riigikantselei eestvedamisel eksperdid era-, vaba- ja avalikust sektorist, et koos seada Eesti IKT poliitika tulevikusihte ning valis kirjutada „Eesti infoühiskonna arengukava 2020". Arengukava kohaselt on Eesti e-valitsuse areng, eriti avaliku sektori e-teenuste väljatöötamine ning nende kasutuselevõtt kodanike ja ettevõtjate poolt olnud märkimisväärne edulugu. Eesti on maailmas ainulaadne elektroonse ID kasutuse, sealhulgas e-hääletuse praktika ja populaarsuse poolest. Tänu elektroonsele autentimisele ja digitaalsele allkirjastamisele on asjaajamine võimalik muuta peaaegu paberivabaks, tehes sellega paljud igapäevased toimingud paindlikumaks ja kiiremaks. Eestis on võimalik ettevõte luua kodust lahkumata või teha seda suisa mõnest välisriigist ning vähem kui 20 minutiga. Ettevõtete majandusaasta aruandeid esitatakse täna pea 100% elektroonselt. Nii kodanikud kui ka ettevõtjad on mõistnud, et avalike e-teenuste kasutamine võimaldab neil säästa nii raha kui aega ning seega on nad avalike teenustega rahul. Enda rahulolu e-teenustega väljendas 2014. aastal 71% Eesti kodanikest ning 2015. aastal 69,6% ettevõtjatest.[22]

Info- ja kommunikatsioonitehnoloogia mõju riikide majanduse konkurentsivõimele ja ühiskondlikule heaolule ning riigivalitsemisele on raske üle hinnata. Uuringufirma McKinsey poolt läbi viidud analüüsi andmetel annab ainuüksi internet 21% sisemajanduse koguprodukti kasvust, kusjuures 75% interneti mõjust tuleneb selle kasutamisest traditsioonilistes majandusharudes.[23] Arengufondi analüüsi[24] kohaselt võib IKT-sektori tekitatav majanduskasv Eestis käesoleva kümnendi jooksul olla hinnanguliselt vahemikus 0,9–1,3%.[25] Seega on igati tervitatav, et riik on panustamas vastavasse valdkonda ning kindlasti on tegemist ka ühe võimalusega pidurdada küllaltki suurt noorte väljarännet riigist.

[21] K. Põder (toim.). Infoühiskond, lk 15.
[22] Vabariigi Valitsus. Eesti infoühiskonna arengukava 2020 (uuendatud 2018). Arvutivõrgus: https://www.mkm.ee/sites/default/files/eesti_infouhiskonna_arengukava_2020_ja_kuberturvalisuse_strateegia_2019-2022.pdf (15.04.2019).
[23] Majandus- ja Kommunikatsiooniministeerium. Eesti infoühiskonna arengukava 2020, lk 5. Arvutivõrgus: https://www.mkm.ee/sites/default/files/elfinder/article_files/eesti_infouhiskonna_arengukava.pdf (15.04.2019).
[24] Eesti Arengufond. Nutikas spetsialiseerumine - kitsaskohtade ja uute võimaluste analüüs. Arvutivõrgus: http://www.arengufond.ee/wp-content/uploads/2013/06/AF_kitsaskohad_final2.pdf (15.04.2019).
[25] Eesti infoühiskonna arengukava 2020, lk 4.

Nagu eelpool mainitud, siis infoühiskonna toimimiseks ei piisa ainuüksi tehnoloogiliste vahendite olemasolust, vaid isegi olulisemale kohale tuleb paigutada neid seadmeid ühendavad võrgustikud. Üheks tuntumaks võrguks on vaieldamatult Internet. Internet teeb võimalikuks erinevate seadmete ühendamise ning seeläbi nendevahelise infovahetuse tekkimise.
Eesti on 2018. aasta seisuga Euroopa Komisjoni poolt hinnatava DESI indeksi (digitaalmajanduse ja -ühiskonna indeks) kohaselt 28 liikmesriigi seas 9. kohal. Aruande põhjal on Eesti olnud aastaid internetipõhiste avalike teenuste osutamisel esirinnas ning tegemist on valdkonnaga, kus riigi tulemused on kõige paremad. Eesti tegi 2018. aasta jooksul edusamme, kuid langes koha võrra. E-valitsuse kasutajate osakaal (96 %) on Euroopa suurim (ELi keskmisest ligi kaks korda kõrgem) ning eeltäidetud vormide kasutamise, e-teenuste lõpuleviimise ja ettevõtjatele suunatud digiteenuste vallas on Eesti esimese viie riigi hulgas. Võrreldes avalike e-teenuste kohaga tabelis, võib pidada küllaltki madala üldkoha tulemuseks Eesti vähest digitehnoloogia integreerimise võimekust. Peamise põhjusena tuuakse välja küll spetsialiseerunud tööjõu vähesus, kuid ka puuduv strateegia majanduse digitaliseerimiseks.[26]

Maailmapanga andmetel kasutas 2017. aasta seisuga Eestis internetti ligi 88% elanikkonnast, ehk ligi 1,2 miljonit inimest. Sellega asetus Eesti maailma riikide hulgas 21. kohale.[27] Selline küllaltki suur interneti kasutajaskond toob omakorda kaasa nende samade elanike üha kasvavad ootused erinevate teenuste kättesaadavuse osas e-maailma vahendusel. Kindlasti ei saa seda pidada riigile aga koormavaks, sest kasu saab olla vastastikune. Teisisõnu elanikele avalike teenuste kättesaadavaks tegemine e-teenuste kaudu pakub rohkem mugavust just kodanikele ning riigile loob see võimaluse eelkõige rohkem panustada süsteemide optimeerimisse. Optimeerimine annab kindlasti võimaluse vähendada koormust riigi rahakotile, mis tuleneb omakorda inimressursi mõistlikumast kasutusest. Samuti vähenevad kulutused sidele (nt. postiteenus), paberile ning ka kõikidele kaudsetele kuludele, mis kaasnevad inimressursi kasutusega (riigihoonete haldus jms).

[26] Euroopa Komisjon. Digital Economy and Society Index 2018 – Eesti. Arvutivõrgus: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=52352 (15.04.2019).
[27] The World Bank. Individuals using the Internet 2017. Arvutivõrgus: https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=EE&view=chart (15.04.2019).

Eesti on Euroopas ning ka laiemalt tuntust kogunud e-riigi omajana. Tundub, et oleme leidnud riigina enese niši, mida ühelt poolt tugevasti arendada ja teiselt poolt ka välisriikidele turundada. Kindlasti on selle arengus suureks abiks olnud meie rahvaarvu ning ka territooriumi väiksus, täna millele on jõudnud enamike elanikeni nii internetiühendus kui ka teadmine erinevate teenuste kasutusvõimalustest.

Senise riikliku IKT-poliitika suurim tugevus on olnud riigi infosüsteemi süstemaatiline väljaarendamine, sealhulgas selle turvalisena rajamine. Eestis on rakendatud selleks Eesti infopoliitika aluspõhimõtteid, kuhu hulka kuuluvad hajus teenusepõhine arhitektuur, andmete ja andmevahetuse asjakohane turvalisus, veebipõhisus, orienteeritus e-teenustele ning tugevate autentimisvahendite kasutamine. Riigi infosüsteemi baasinfrastruktuur ehk teenustetaristu (X-tee, avaliku võtme infrastruktuur ja eID, dokumendivahetuskeskus, teabevärav eesti.ee) on läbi aastate toetanud avalike teenuste arendamist kiirelt ja paindlikult valmivate IKT-lahendustega. Hajusalt ja samas üldiselt koostoime võimelisena üles ehitatud riigi infosüsteem on loonud Eestile head eeldused tulla toime ning potentsiaalselt lõigata kasu trendist, kus üha enam seadmeid ja masinaid on ühendatud arvutivõrku.[28]

Kui ühelt poolt elanikkond Eestis küll vananeb, siis hoolimata sellest on üllatavalt kiirelt võetud omaks mitmete e-teenuste kasutamine. 2019. aastal avalikustati uuring, milles vaadeldi riiklike e-teenuste (X-tee) kasutajate vanuselist jaotumist Eesti koguelanikkonnast aastatel 2003-2015. Uuringu tulemusel nähtub selgelt, et kogu uuringualuse perioodi vältel on e-teenuste kasutajate hulk järjepidevalt tõusnud. Kuni 50-aastaste hulgas on see tõus olnud küll kiirem, kuid ka 80-aastaste hulgas on see olnud järjepidev.[29] Kindlasti on selline elanikkonna kohanemine pakutavate teenustega igati tervitatav. Tõenäoliselt ei osanud täna juba 80-eluaastates olevad inimesed Nõukogude Liidu lagunemisele järgnenud perioodil isegi ette kujutada, millised digitaalsed võimalused neid tulevikus ootavad. E-teenuste kasutegur on eelkõige vastastikune ning kokku ei hoia see ainult riigi tehtavaid kulutusi ning inimressurssi, vaid otseselt mõjutab see ka teenuse tarbijaid, kelle kodus arvuti taga tehtavad toimingud hoiavad ideaalis kokku ka nende aega ja raha. 2016. aastal auditeeris Riigikontroll avalike e-teenuste kasutatavust ning hindas riigihangete registri, avaliku e-toimiku, riikliku statistika tegemiseks vajalike andmete esitamise infosüsteemi ja ruumilise planeeringu menetluste infosüsteemi puhul seda, kas riigi avalikud e-teenused on kvaliteetsed ja loovad lisandväärtust, ehk aja ja raha kokkuhoidu teenust

[28] Eesti infoühiskonna arengukava 2020, lk 7.
[29] M. Solvak jt. E-governance diffusion: Population level e-service adoption rates and usage patterns - Telematics and Informatics 36/2019, lk 39-54.

pakkuvatele asutustele ning teenuste kasutajatele. Riigikontroll jõudis hinnangule, et riigi pakutavate e-teenuste kasutatavus ja kvaliteet on ebaühtlane ning mitmed e-teenused ei ole ühtlaselt lihtsad, kasutajasõbralikud ega lisandväärtust pakkuvad. Teisalt me liigume üha rohkem olukorra poole, kus pakutavad e-teenused kujunevad monopoolseteks ning alternatiivseid võimalusi paralleelselt enam ei säilitata. [30] Selline olukord võib tekitada suure probleemi, kus riiklikult nõutavaid teenuseid ei suudeta nende keerukuse tõttu kodanike poolt enam kasutada.

Täna on küll juba välja mõeldud lahendused, kus mainitud näite puhul abistavad näiteks klienditeenindajad taotlust esitada soovijaid sellega, et assisteerivad neid taotlusvormide täitmisel. Ühelt poolt võib küll öelda, et sellise käitumise puhul ei ole ju tegemist enam e-teenusega, vaid klienditeenindaja vahendusel ikkagi taotluse esitamisega. Teisalt aga saab pidada sellist käitumismalli tulevikku suunatuks, sest vastava assisteerimise ja juhendamise tulemusel jääb ikkagi lootus, et tulevikus ehk oskvavad abivajajad vajalikke teenuseid ise kasutada. Õhku jääb aga ikkagi rippuma küsimus, kas sellisel puhul on jäetud kliendile võimalus valida elektroonse või sellele eelnenud pabertaotluste esitamise võimaluse vahel.
Jättes siinkohal kõrvale sotsiaalteenuste valdkonna, tuleb lisaks meeles pidada, et Eestis eksisteerivad veel mitmed e-teenused, mille tarbijaks ei ole enam mitte tavainimene, vaid just eelkõige riigiasutused ning nendega seonduvad organisatsioonid ise. Hea näitena selliste teenuste osas võib õigusvaldkonnas välja tuua riigi õigusabi infosüsteemi RIS, millega töötavad advokaadid, prokurörid, kohtutöötajad ning ka kohtueelsed menetlusasutused. Samas ei ole võrreldes erasektoriga ametnikel enam valikuvõimalust, vaid neil tuleb lähtuda ametkondlikest kokkulepetest ning sisemisest töökorraldusest. Ka selliseid teenuseid saab kohati nimetada obligatoorseks.

Eesti kui e-riigi edu on viinud meil olukorrani, kus enam ei kujutata ette elu ilma digitaalsete lahendusteta. Hoolimata sellest, et mitmed e-lahendused ei ole veel täie valmiduse juures, siis ollakse varmad neid kiirustades kasutusele võtma ning samaaegselt vanu tegevusvariante kõrvaldama ja unustama. Kui tegutseda ainult rutates, siis võib selline tegevus viia meid aga hoopis e-katastroofini, mida tuleks loomulikult igal võimalikul juhul vältida.

[30] Riigikontroll. Avalike e-teenuste kasutatavuse aruanne riigikogule 2016. Arvutivõrgus: https://www.riigikontroll.ee/DesktopModules/DigiDetail/FileDownloader.aspx?AuditId=2411&FileId=13797 (15.04.2019).

1.3. Infoühiskonna ja õiguse puutumus

Eelpool kirjeldatust võib järeldada, et Eesti edulugu seoses innovatiivsete e-teenuste kasutusele võtuga on olnud silmapaistev. Samas on kohati kiputud kiirustama ning väline tunnustusvajadus ja majanduslik edu on jätnud varju mitmedki rakenduslikud vajadused, milleta e-riigi sisuline väärtus ei saa olla täiuslik. Ühe sellise vajadusena võib välja tuua kooskõla õigusruumiga, mille puudumisel muutub keeruliseks teenuse rakendamine või võivad ohtu sattuda suisa inimeste põhiõigused. Õigusriigile kohaselt ei saa lasta Eestis aga sellisel olukorral tekkida ning vajalik on juba teenuste planeerimis- ja ettevalmistusfaasis pöörata juriidilistele aspektidele olulist tähelepanu. Paloma Krõõt Tupay ja Monika Mikiver leiavad enda artiklis „E-riik ja põhiõigused“, et „Eesti kui eduka ja avatud e-riigi maine ülesehitamise üheks oluliseks määrajaks on osutunud ka seadusandja kui innovatsioonisõbra kaasamine. Õigusnormide kindlaks eesmärgiks on läbi aastate kujunenud Eesti infoühiskonna uute digilahenduste ja e-leidlikkuse toetamine.“[31]

Infoühiskond oma olemuselt ei ole midagi eraldiseisvat ühiskonnast selle klassikalises mõttes. Pigem on tegemist ühe ühiskonna alaliigiga, mis peegeldab endas õiguslikus võtmes juriidilist kaalu omavate toimingute teostamist elektrooniliste vahendite abil või vahendusel.

Haldusmenetluse seaduse (edaspidi HMS) § 5 lg 6 kohaselt on haldusmenetluses elektrooniline asjaajamine võrdsustatud kirjaliku asjaajamisega, võttes arvesse elektroonilisest asjaajamisest tulenevaid erisusi.[32] Vastava normiga on seadusandja selgelt andnud mõista, et elektroonilise ja kirjaliku asjaajamise ainsaks sisuliseks erinevuseks on ainult toimingu teostamise meetod. Sisuliselt omavad need aga täpselt samasugust kaalu. Selline säte on aga üldregulatiivne ning selle abil ei saa kõrvaldada teisi valdkonnas tekkida võivaid õiguslünki. Kuigi kõik lüngad, mis tekivad e-teenuste ja seni kehtiva õiguste kokkupuutepunktist (nt vastutus riiklike e-teenuste toimimise osas), ei pruugigi hetkel veel olla ületatavad, siis tuleb vähemalt selle suunas liikuda.

Siseriikliku õiguse ja infoühiskonna arenguga kaasnevate muutustega puutub avaliku õiguse valdkonnas kokku tõenäoliselt kõige rohkem e-teenuste puhul. Näiteks on Riigikontroll enda aruandes jaganud avalikud e-teenused kahte suurde rühma. Esimesse kuuluvad avalike teenustena soodustavate haldusaktide andmiseks (nt toetuse määramine), õiguste kasutamiseks

[31] P.K. Tupay, M. Mikiver. E-riik ja põhiõigused. - Juridica III/2015, lk 175.
[32] Haldusmenetluse seadus - RT I, 13.03.2019, 55.

(nt valimistel hääletamine) ja kohustuste täitmiseks (nt maksude deklareerimine) kasutatavad teenused. Teise rühma liigitas Riigikontroll avalike teenuste pakkumiseks nende laiemas tähenduses kasutatavaid teenused (nt jäätmekäitluse, vee- ja energiavarustuse, ühistranspordi või arstiabi tagamist).[33]

Tehnoloogiliste võimaluste hüppeline areng on esitanud esmalt väljakutse kehtiva õiguse järgijatele ning seejärel seadusandjale endale, kelle puhul on märgata suutmatust tehnoloogia arenguga kaasas käia. Näiteks haldusmenetluse seaduse puhul on mindud lihtsamat teed ning samastatud on asjaajamise liigid ja vahel piisav kõigest puutumuses olevasse seadusesse asjakohase normi uute teenuste kasutamise võimaldamiseks. Samas ei saa seadusandluse muutmisel lähtuda ainult üksikjuhtumitest, vaid muudatused peavad sobituma ka riigi ning rahvusvahelise õiguse tervikpilti.

Raske on leida tänases siseriiklikus õiguses kehtivat õigusakti, mille keskmes oleks avalike teenuste elektoonilise kättesaadavusetagamise reguleerimine.. 14.04.2004 on küll vastu võetud infoühiskonna teenuse seadus, kuid oma olemuselt see riiklike e-teenuste toimimist ei reguleeri. Infoühiskonna teenuse seadus on oma olemuselt vertikaalne ning mõeldud reguleerimaks piiratud teenuste ringi (infoühiskonna teenuseid).[34]

Üheks riiklike e-teenuste puhul oluliseks punktiks on veel turvalisuse tagamine. Näiteks on kehtestatud Euroopa Parlamendi ja nõukogu 23. juuni 2014. a määruse (EL) nr 910/2014, millega määratakse kindlaks elektrooniliste isikutuvastamise vahendite usaldusväärsuse tagamiseks ette nähtud meetodid, koostöö liikmesriikidega ning osaliselt ka vastutus. Selliste tingimuste määratlemine on oluline, et liikmesriigid mõistaksid ühtselt elektroonilise identifitseerimise standardeid ning selle tulemusel tekiks valdkondlik vastastikune usaldus.

[33] Riigikontroll. Avalike teenuste kvaliteet infoühiskonnas 2010. Arvutivõrgus: https://www.riigikontroll.ee/DesktopModules/DigiDetail/FileDownloader.aspx?AuditId=2162&FileId=11158 (15.04.2019).

[34] Elektroonilise side seaduse ja infoühiskonna teenuse seaduse muutmise seaduse seletuskiri 137. Arvutivõrgus: https://www.osale.ee/konsultatsioonid/files/consult/137_SELETUSKIRI_13_01.rtf (15.04.2019).

Usalduse loomine internetikeskkonnas on majandusliku ja sotsiaalse arengu alus. Usalduse puudumise tõttu, mida eelkõige põhjustab arvatav õiguskindluse puudumine, on tarbijad, ettevõtjad ja ametiasutused elektrooniliste tehingute tegemise ja uute teenuste kasutuselevõtu suhtes ebalevad.[35] Siseriiklike usaldusteenuste korralduse määrab Eestis e-identimise ja e-tehingute usaldusteenuste seadus.[36]

Paraku jõuame taas tõdemuseni, et riiklike e-teenuste ühtne regulatsioon puudub, kuid on võimalik, et see oleks ka liigselt üldregulatiivse iseloomuga. Praeguse praktikaga on seadusandja mitmed kasutatavad e-teenused loonud ning nendega seonduva reguleerinud Vabariigi Valituse või ministrite määrustega ning selle tulemusel sisse viinud vajalikud muudatused puutumuses olevates õigusaktides. Näiteks E-toimiku kasutusele võtmine eelduseks lisati esmalt e-toimikut käsitlevad normid asjakohastesse seadustesse ning seejärel kehtestati kriminaalmenetluse seadustiku[37] (edaspidi KrMS) § 210 lõike 3, väärteomenetluse seadustiku[38] (edaspidi VTMS) § 811 lõike 3 ja tsiviilkohtumenetluse seadustiku[39] (edaspidi TsMS) § 601 lõike 3 alusel E-toimiku süsteemi asutamine ja e-toimiku süsteemi pidamise põhimäärus (edaspidi E-Toimiku põhimäärus).[40] E-toimik sisaldab endas mitmeid iseseisvaid, kuid e-toimikuga liidestatud mooduleid, mille puhul tuleb vajalikud normid leida e-toimiku põhimääruse, kohtute dokumentide esitamise korra, kriminaalmenetluse seaduse, maa-, haldus- ja ringkonnakohtu kantselei kodukorra, tsiviilkohtumenetluse, väärteomenetluse ja teiste puutumuses olevate õigusaktide koostoimes. On arusaamatu, miks ei ole näiteks koondatud kõik E-toimikut puudutavad normid kokku E-toimiku põhimäärusesse. Teise variandina oleks ülereguleerimise vältimiseks võimalik jätta mainitud õigusaktides üldse käsitlemata konkreetselt süsteem E-toimik, vaid piirduda sõnastusega, mis võimaldavad asjakohaste infosüsteemide kasutamise. Selline normatiivne killustatus võib tekitada küllaltki keerulise olukorra, kui õiguse poole pöörduja jääb hätta kohase normi leidmisega.

[35] Euroopa Parlamendi ja Nõukogu 23.07.2014 määrus nr 910, e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul - ELT L257/73.
[36] E-identimise ja e-tehingute usaldusteenuste seadus - RT I, 12.12.2018, 30.
[37] Kriminaalmenetluse seadustik - RT I, 13.03.2019, 77.
[38] Väärteomenetluse seadustik - RT I, 13.03.2019, 200.
[39] Tsiviilkohtumenetluse seadustik - RT I, 19.03.2019, 22.
[40] E-toimiku süsteemi asutamine ja e-toimiku süsteemi pidamise põhimäärus. VVm 03.07.2008 nr 111 - RT I, 09.03.2018, 5.

2. DIGITAALSUS KRIMINAALMENETLUSES

2.1. Kriminaalmenetluse digitaalsuse hetkeseis

Vabariigi Valitsuse tegevusprogramm 2015-2019 aastaks, mis koostati toonase võimuliidu kavatsuste fikseerimiseks, nägi punktis 11.16 ette õigusrikkumiste menetlemise (sh kriminaalmenetluse) paindlikumaks ja lihtsamaks muutmise, tagades menetluse inimest vähimal koormaval viisil ning arvestades rikkumiste raskusastet ja tagajärgi. Selle eesmärgi saavutamiseks nähti ette kriminaalmenetluse seadustiku uuendamine ning politsei ja prokuratuuri töökorralduse tõhustamise, et tagada kiirem kriminaalmenetlus. Vastava eesmärgi täitmiseks nägi võimuliit efektiivse kriminaalmenetlusregistri loomise ja menetluse digitaliseerimise vajadust.[41] Seda otsust saab pidada üheks oluliseks lähtepunktiks pikale kriminaalmenetluse revisjoni ning digitaliseerimise teele. Vastav tegevusprogramm kinnitati alles 2015. aastal ning selleks hetkeks oli tehtud juba küllalti suur samm kriminaalmenetluse digitaliseerimiseks. Näiteks oli juba pikka aega kasutusel e-toimiku süsteem ning hulgaliselt menetluse tagamiseks vajalikke andmebaase. Kui selle ajani nähti digitaalsete võimaluste kasutamist kohtueelses menetluses pigem võimalusena, siis Vabariigi Valitsuse kavatsus justkui muutis üha suurema elektroonsete võimaluste kasutamise hoopis kohustuseks.

Õigusriigile kohaselt peab kohtumenetlus olema muuhulgas piisavalt kiire, tõhus ning menetlusosalisi võimalikult vähe koormav. Kriminaalmenetlusse digitaalsete võimaluste kaasamine on kindlasti üheks võimalikuks abivahendiks kirjeldatud omaduste tagamiseks, kuid sealjuures unustamata alternatiivsete võimaluste säilitamist. Kriminaalmenetlus puudutab Eestis kokku 9 menetlejate sihtrühma (Kohus, Prokuratuur, Politsei ja Piirivalveamet, Maksu- ja Tolliamet, Konkurentsiamet, Keskkonnainspektsioon, Sõjaväepolitsei, Kaitsepolitseiamet, Vanglad), kus kokku igapäevaselt töötab vahetult kriminaalmenetlusega ca 2 000 töötajat. Lisanduvad kuni 300 kaitsjat/advokaati, kelle igapäevatöö on samuti kriminaalmenetlus.[42]

[41] Vabariigi Valitsus. Tegevusprogramm 2015-2019, p 11.16. Arvutivõrgus: https://valitsus.ee/sites/default/files/contenteditors/arengukavad/valitsuse_tegevusprogramm_2015-2019_2.xlsx (15.04.2019).

[42] M. Hirvoja. Kriminaalmenetluse revisjoni analüüs - üleminek täisdigitaliseeritud kriminaalmenetlusel - 31.05.2016, lk 7. Arvutivõrgus: https://www.just.ee/sites/www.just.ee/files/uleminek_taisdigitaliseeritud_kriminaalmenetlusele_m_hirvoja.pdf (15.04.2019).

Kokku seega professionaalidest tegeleb Eestis igapäevatöö raames kriminaalmenetlusega ca 2300 inimest.[43] Sellise märkimisväärse huvigrupi puhul muutub digitaalsete võimaluste abil menetluse tõhustamise tulem mitmekordseks. Seega on hoomamatu võimalik ajaline ning halduskoormuslik kokkuhoid, mida muudatustega saavutada võib. Kui aga kaasaegsed lahendused pigem hakkavad menetlust takistama, siis mastaabiefekt muutub vastupidiseks. Eeldusel, et kaasaegsed süsteemid ja digitoimik võimaldavad hoida kriminaalmenetlusega puutumuses olevatel inimestel kokku ainuüksi ühe tunni tööaega päevas, siis Eesti 2018. aasta keskmise töötasu[44] juures tähendaks see juba ainuüksi inimressursilt kokkuhoidu ligi 4,4 miljoni eurot aastas.[45]

2.2. Kriminaalmenetluses kasutusel olevad infosüsteemid

Kesksеks andmekoguks süütegusid menetlevate asutuste vahelise menetlusinfo hoidmiseks ja edastamiseks on tänase seisuga interaktiivne teenus nimega E-toimik. Justiitsministeerium kirjeldas 2009. aastal E-toimikut kui radikaalselt uuenduslikku andmekogu, kuna see põhineb valdkondliku tööloogika teenindamise eesmärgil – toetatakse tervet (kriminaal)menetlusprotsessi läbi mitme eraldiseisva asutuse ja andmekogu.[46] E-toimik on veebipõhine infosüsteem, mille kaudu on võimalik tsiviil-, kriminaal-, väärteo- ja haldusmenetluses osaleda elektrooniliselt. E-toimiku kaudu on võimalik esitada menetlejale dokumente ning jälgida menetluse käiku.[47]

[43] M. Hirvoja. Kriminaalmenetluse revisjoni analüüs - üleminek täisdigitaliseeritud kriminaalmenetlusel - 31.05.2016, lk 7..
[44] Statistikaamet. Keskmine Eesti brutotunnipalk 2018.a. Arvutivõrgus: https://www.stat.ee/stat-keskmine-brutotunnipalk.
[45] Arvutuskäik: 21,17 (keskmine tööpäevade arv kuus) X 12 (kuud) X 7,56 (keskmine brutopalk) X 2300 (kriminaalmenetlusega tegelevad isikud).
[46] Justiitsministeerium. Ülevaade E-Toimiku projektist ja esmakordse rakendamisega kaasnevatest muudatustest töökorralduses – 29.06.2009. Arvutivõrgus: https://www.riha.ee/api/v1/systems/e-toimik/files/da5a8578-f169-db42-fd89-a685b9b6e621 (15.04.2019).
[47] V. Kõve, jt. Tsiviilkohtumenetluse seadustiku, kommenteeritud väljaanne, Juura 2017, § 311^1 komm. 3.1.1.

Kriminaalmenetluse seadustiku § 210 lg 1 sätestab E-toimiku menetlemise infosüsteemi eesmärgid, milleks on:

1) tagada ülevaade uurimisasutuste, prokuratuuri ja kohtute menetluses olevatest kriminaalasjadest, samuti alustamata jäetud kriminaalasjadest;
2) kajastada andmeid kriminaalmenetluse käigus tehtud toimingute kohta;
3) võimaldada menetleja töö korraldamist;
4) tagada kriminaalpoliitiliste otsustuste tegemiseks vajaliku kuritegevuse statistika kogumine;
5) võimaldada andmete ja dokumentide elektroonilist edastamist.

E-toimikusse kantakse KrMS § 210 lg 2 alusel:
1) andmed menetluses olevate, alustamata jäetud ja lõpetatud kriminaalasjade kohta;
2) andmed kriminaalmenetluse käigus tehtud toimingute kohta;
3) digitaalsed dokumendid käesolevas seadustikus sätestatud juhtudel;
4) andmed menetleja, menetlusosalise, süüdimõistetu, eksperdi, asjatundja ja tunnistaja kohta;
5) kohtulahend.

Kriminaalmenetluses ühendab E-Toimik erinevad menetlevad osapooled ja organisatsioonid (politsei, prokuratuur, kohus) ühtsesse inforuumi tagades kehtiva informatsiooni pideva kättesaadavuse kõikidele menetlejatele. E-Toimiku süsteem laiemas tähenduses koosneb n.ö tsentraalsest andmebaasist, E-Toimikust, mis sisaldab toimiku informatsiooni ning põhisüsteemidest, mis toimiku informatsiooni manipuleerivad – kasutavad ja muudavad. Igas põhisüsteemis on kirjeldatud ligipääsuõigused vastava ametkonna töötajatele E-Toimiku tsentraalsetele teenustele. Põhisüsteemides hoitakse eraldiseisvalt informatsiooni, mis ei ole vajalik teistele menetlusosalistele (näiteks informatsioon kohtuniku või prokuröri menetlusgrupi kohta, informatsioon asjade jagamisaluste ja spetsialiseerumiste kohta, informatsioon täiendavate ressursiotsuste kohta ja nende tegemise äriloogika jms).[48]

E-toimiku süsteemi Kriminaalmenetluses kasutatavate liideste hulka kuuluvad:

1) Karistusregistri kasutajaliides (KARR) – andmed isikute eelnevate süütegude kohta;

[48] Justiitsministeerium. Ülevaade E-Toimiku projektist ja esmakordse rakendamisega kaasnevatest muudatustest töökorralduses – 29.06.2009. Arvutivõrgus: https://www.riha.ee/api/v1/systems/e-toimik/files/da5a8578-f169-db42-fd89-a685b9b6e621 (15.04.2019).

2) Avalik e-toimiku liides (AET) – mõeldud kodanikule eelkõige lihtsamaks menetluses osalemiseks, võimaldab mh seaduses ja käesolevas määruses sätestatud juhtudel ja mahus isikule juurdepääs e-toimiku süsteemile ning selles sisalduvatele andmetele tema kohta, võimaldada isikul esitada süütegusid menetlevatele asutustele elektrooniliselt taotlusi ja dokumente;[49]
3) Kriminaalmenetluse liides (PRIS) – eesmärk on võimaldada prokuratuuril ja uurimisasutustel kriminaalmenetluse andmete edastamist ja tarbimist e-toimiku süsteemis.[50] [51]

E-toimiku süsteemiga on lisaks tema enda liidestele ühendatud ka teised asjasse puutuvad ning iseseisvad infosüsteemid. Kriminaalmenetlusega puutumuses olevad ning e-toimikuga liidestuvad andmebaasid:

1) Kohtute infosüsteem (KIS) – registri eesmärk on koondada kohtuasjad ühtsesse andmekogusse, töödelda menetlustoimingute andmeid, võimaldada elektroonilisi menetlusdokumente, võimaldada kohtuasja andmete automatiseeritud kasutamist menetlusdokumentide ja statistiliste aruannete koostamisel, tagada pidev ülevaade kohtumenetluse käigust, võimaldada kohtute töökoormuse jaotamist, lahendite ja kohtumenetluse statistiliste ülevaadete tegemist, võimaldada kohtulahendite sisulist analüüsimist ja süstematiseerimist erinevate otsinute abil, võimaldada elektrooniliste menetlusdokumentide esitamist ja säilitamist, teha kohtulahendid arvutivõrgus avalikkusele kättesaadavaks;
2) Politsei infosüsteem (POLIS) – infosüsteemi eesmärgiks on töödelda korrakaitse ja süüteomenetlusega seotud andmeid, et tagada avalik kord ja siseturvalisus;[52]
3) Riigi õigusabi infosüsteem (RIS) – infosüsteemi eesmärgiks on riigi õigusabi tellimuste elektrooniline haldamine, advokatuuri liikmete andmete elektroonilise kättesaadavuse võimaldamine, riigi õigusabi teenuse kiirema kättesaadavuse tagamine, statistiliste ülevaadete saamine riigi õigusabi teenuse osutamisest.[53] [54]

[49] E-toimiku põhimäärus - RT I, 09.03.2018, 5.
[50] Riigi Infosüsteemi Haldussüsteemi kataloog. E-toimiku süsteemi kriminaalmenetluse liides PRIS. Arvutivõrgus: https://www.riha.ee/Infos%C3%BCsteemid/Vaata/70000310-pris (15.04.2019).
[51] E-toimiku põhimäärus - RT I, 09.03.2018, 5.
[52] Politsei andmekogu põhimäärus. SiMm 22.12.2009 nr 92 - RT I, 12.03.2019, 39.
[53] Riigi Infosüsteemi Haldussüsteemi kataloog. E-toimikuga liidestunud süsteemide loogiline arhitektuur – 01.11.2017. Arvutivõrgus: https://www.riha.ee/api/v1/systems/e-toimik/files/a2c800e1-f14a-3cd3-3d09-1fb3c02fa303 (15.04.2019).
[54] E-toimiku põhimäärus - RT I, 09.03.2018, 5.

Lisaks Justiitsministeeriumile on ka Siseministeerium, endine Politseiamet ning tänane Politsei- ja Piirivalveamet (PPA) teinud väga suuri jõupingutusi, et liikuda kaasas infotehnoloogiliste võimaluste arenguga, et seeläbi muuta kõikide kohtueelse menetlusega puutumuses olevate osapoolte menetluses osalemine veelgi tõhusamaks ja mugavamaks. Kui E-toimiku süsteem toimib peaasjalikult ametkondliku (politsei-prokuratuur-kohus) infovahetuse tagamiseks menetluse raames, siis nähti E-toimiku loomisega paralleelselt vajadust ka ametisisese süsteemi järele.

05.06.2008 võeti kasutusele tänaseks suurimaks Politsei- ja Piirivalveameti infosüsteemiks kasvanud POLIS ning E-toimikuga liidestuv uus versioon, mis on juba 1995. aastal kasutusele võetud süsteemi edasiarendus. Infosüsteemi eesmärk on politseiliste ülesannetega seotud toimingute ja menetlustega seotud andmete kogumine ühtsesse andmekogusse politseiliste ülesannete efektiivseks ja kiireks täitmiseks ning tõhusa järelevalve teostamiseks.[55]

POLIS näol ei ole tegemist pelgalt ainult kriminaalmenetluse läbiviimiseks kasutatava süsteemiga, vaid mh sisaldab see ka näiteks riigikassa teenuseliidese ja hoiatusmenetluse alamsüsteeme. Siiski on tegemist ühe väga olulise tööriistaga kohtueelse menetluse läbiviijate igapäevatöös. POLIS puhul on tegemist infosüsteemiga, mille allharusid nimetatakse andmestikeks. POLIS andmestike hulka kuuluvad ühiste infoobjektide andmestik, süüteomenetluse andmestik, haldustegevuse andmestik, ennetava tegevuse andmestik, reageeriva tegevuse andmestik, arestimajade tegevuse andmestik, otsimise andmestik ja jälitusmenetluse andmestik.[56]

Kriminaalmenetlusega Politsei- ja Piirivalveametis kohtueelse menetluse raames tegelevad uurijad kasutavad enda igapäevatöös süütegude andmestiku, mis on tuntud ka kui Menetluse infosüsteem (MIS). Kõnealusesse andmebaasi kantakse vahetult pea kõik menetluse käigus tekkivad digitaalsed failid (nt ülekuulamiste ja vaatluste protokollid). Samas on kasutusel olev süsteem praktikute seisukohast küllaltki kapriisne ning jääb tihti hätta suuremate andmemahtudega. Liikudes aga üha rohkem täisdigitaalse kriminaalmenetluse suunas, ei ole vastuvõetav, et peamiseks menetlust aeglustavateks ja takistavateks elementideks kujunevad just tehnilise võimekuse puudujäägid. Lisaks on loodud mitmeid ametisiseseis infosüsteeme, mis on kasutusel eelkõige tulenevalt mõne kindla tööliini eripärast, kuid kohtueelses menetluses

[55] Riigi Infosüsteemi Haldussüsteem. Infosüsteem POLIS. Arvutivõrgus: https://vana.riha.ee/riha/main/inf/infosusteem_polis (15.04.2019).
[56] Politsei andmekogu põhimäärus. SiMm 22.12.2009 nr 92 - RT I, 12.03.2019, 39.

niivõrd laialdast kokkupuudet ei oma. Näiteks on veel PPA poolt läbiviidavas kohtueelses menetluses kasutusel jälitustegevuse infosüsteem JÄTIS ja jälitusinfo süsteem KAIRI. Süsteemi JÄTIS kasutavad peamiselt PPA prefektuuride kriminaalbürood või keskalluvusega struktuuriüksused, siis KAIRI on pea iga politseiniku igapäevane tööriist.

2.3. Hübriidtoimik

Riigikohtu asjaajamiskord defineerib hübriidtoimikut kui omavahel sisuliselt seotud dokumentide kogumit, mille andmed asuvad erinevatel andmekandjatel.[57]

Justiitsministeeriumi kriminaaltoimiku nõudeid käsitlev määrus näeb ainsa võimaliku toimiku pidamise vormina kriminaalmenetluses paberkandjal toimikut.[58] Kriminaalasja toimikut peetakse täna paberkandjal köidetuna, samas hiljem moodustatavat kohtutoimikut on kehtiva korra kohaselt võimalik pidada kas täielikult või osaliselt digitaalsena. Kriminaalmenetluses täna *de facto* digiformaadis peetav osaline toimik ei oma õiguslikku tähendust ning kujutab endast sisuliselt paralleelselt peetavat osaliselt dubleerivat digitaalset abitoimikut. Tänaseks on tekkinud paberkandjal toimiku ja digitaalse toimikupidamise hübriidsüsteem, mis on menetlusressurssi rohkem koormav kui oleks kas üksnes paber või üksnes digimenetlus.[59]

2015. aastal soovis prokuratuur juurutada veel kahe toimiku põhimõtet ning üleminekust ainult digitoimikule ei olnud juttugi. Toonase nägemuse järgi sooviti tagada parem ning kiirem tõendite leitavus. Pabertoimikusse sooviti koondada kõik kohtuistungil vajaminevad materjalid, mis tõendasid süüteo toimepanemist ning digitaalses toimikus sooviti hoiustada teisi uurimise käigus kogutud materjale, mis olid küll menetlust assisteerivad, kuid mitte otseselt süütegu tõendavad.

Kohtud on sammhaaval alustanud paberivabale toimikule üleminekut ning digitaalsele toimikule on antud ka õiguslik tähendus. 2015. aasta lõpus valmis ning 2018. aastal võeti pärast testperioodi kasutusele digitaalse kohtutoimiku infosüsteem, mis võimaldab menetlusosalistel

[57] Riigikohus. Riigikohtu asjaajamiskord – 17.12.2012, lk 3. Arvutivõrgus: https://www.riigikohus.ee/sites/default/files/elfinder/dokumendid/asjaajamiskord_kinnitatud.pdf (15.04.2019).
[58] Nõuded kriminaaltoimikule ja kaitseakti näidisvormi kehtestamine. JMm 16.07.2008 nr 39 - RT I, 26.01.2016, 8.
[59] Hirvoja, lk 2.

ja kohtul tutvuda ning töötada elektroonilise kohtutoimikuga. Projektiga seotud arengueesmärgiks on kaotada hiljemalt 2019. aasta lõpuks tsiviil- ja halduskohtumenetluses õiguslikku tähendust omav pabertoimik täielikult ning võimaldada kohtunikul, kohtuametnikul ja menetlusosalisel töötada digitaalse kohtutoimikuga.[60] Paraku ei ole hoolimata regulatsiooni võimalikkusest vastava süsteemi kasutusele võtmisega jõutud veel kriminaalkohtumenetlusteni ning seda ei ole eraldi välja toodud ka Justiitsministeeriumi arengukavas aastateks 2019-2022. Samas juba täna viiakse hulgaliselt toiminguid ka kriminaalkohtumenetluses läbi elektroonselt ning kriminaalasjas on lubatud pidada KrMS § 160^1 lg 4 kohaselt kohtutoimikut täielikult või osaliselt digitaalsena.

Kriminaalmenetluse revisjoni ühe ettepanekuna on laekunud, et kriminaaltoimiku pidamine toimub tulevikus digitaalselt ja loobutakse paralleelselt paberil toimiku pidamisest. Ette nähakse, et toimikut hakkab tulevikus endiselt pidama menetleja ning paberil algdokumendid lisatakse digitoimikusse ja säilitatakse samuti menetleja juures. Ettepaneku kohaselt toimub üleminek digitoimikule järk-järguliselt eraldi rakendusaktiga, mitte varem kui 2022. aastal.[61] Niivõrd pikk üleminekuperiood annab küll võimaluse teha seda sujuvalt ning erinevate väiksemate testperioodide tulemusel valutumalt, kui kas õigustatud on sellel perioodil topelttoimiku pidamise jätkamine. Kohtueelses menetluses on tekkinud olukord, kus hoolimata pabertoimiku pidamise nõudest on menetlejatel kohustus kanda mõningad uurimistoimingute protokollid paralleelselt ka politsei menetluse infosüsteemi MIS ning teised kohtueelset menetlust läbiviivad asutused E-toimiku kriminaalmoodulisse PRIS. Sellise nõude eesmärk on suurema kättesaadavuse tagamine protokollidele ametisiseselt, prokuratuuri ja eeluurimisasutuse paralleelse töö võimaldamine ning ka statistika kujundamine läbi süütegude klassifikaatorite. Raske on mõista, miks ei ole ka kohtueelsele kriminaalmenetlusele loodud sarnaselt kohtutoimikule alternatiivset võimalust, ehk toimiku pidamist kas täielikult või osaliselt digitaalsena.

[60] Justiitsministeerium. Justiitsministeeriumi valitsemisala arengukava aastateks 2019 – 2022, lk 29. Arvutivõrgus: https://www.just.ee/sites/www.just.ee/files/justiitsministeeriumi_arengukava_2019-2022.pdf (15.04.2019).
[61] Justiitsministeerium. KrMS revisjoni VTK kooskõlastamisel laekunud arvamused ja otsused revisjoni I etapi teemaderingi osas, p 1.1.

Politsei menetluse infosüsteem on oma olemuselt loodud sellisena, et uurijal on võimalik vajalike lahtrite täitmise järel genereerida automaatne toimingu protokoll. Teise ning ka praktikas rohkem levinud võimalusena on võimalik koostada protokoll arvuti tekstitöötlusprogrammis ning seejärel see üles laadida infosüsteemi. Tulemuseks on aga see, et uurija peab ikkagi koostatud protokolli lisaks ka välja printima ning tegeliku tõendusväärtuse omandamiseks lisama pabertoimikusse, mis lõppjärgus liigub uurimisasutusest prokuratuuri.

Kriminaalmenetluse seadustiku § 224 lg 1 kohaselt esitab aga prokuratuur kaitsjale kriminaaltoimiku koopia elektroonilisel andmekandjal või kaitsja kirjaliku põhistatud taotluse alusel paberil. Samuti sätestab KrMS § 226 lg 3, et süüdistusakt edastatakse kohtule prokuratuuri poolt samuti elektroonselt. KrMS § 160^1 sätestab, et kui kohtutoimikut peetakse digitaalselt, siis tuleb kriminaaltoimiku paberdokumendid skaneerida ning seejärel lisada e-toimikus asjakohase menetluse juurde. Ei ole arusaadav, millest tuleneb menetlusetappides toimiku pidamise viisi erinevus ja vajadus selle järele. Seega on mõistlik liikuda täisdigitaalse toimiku kasutusele võtmise poole kogu kriminaalmenetluse raames.

2.4. Menetlustoimingud kriminaalmenetluses

Kriminaalmenetluses rakendatava digitaliseerimisega seonduva paremaks mõistmiseks tuleks esmalt avada menetlustoimingute mõistet laiemalt. Õigusteadlased leiavad üldiselt, et kriminaalmenetlust saab pidada üheks inimtegevuse valdkonnaks. Psühholoogide poolt on omaks võetud arvamus, et igasugune inimtegevus koosneb omavahel seostuvatest toimingutest. Seega võib väita, et kriminaalmenetluse kui käitumise sisuks on erinevad menetlustoimingud.[62]

Raivo Öpik on jaganud menetlustoiminguid lähtuvalt oma eesmärgist kaheks:

- korraldava ja tagava iseloomuga toimingud;
- tõendusteabe kogumisele suunatud toimingud (uurimistoiming, ekspertiis, revisjon/audit, esemeliste objektide väljanõudmine või esitamine, jälitustoimingud).[63]

[62] R. Öpik. Kriminalistiline taktika ja tehnoloogia I. Tallinn: Sisekaitseakadeemia 2008, lk 5.
[63] R. Öpik, lk 6.

Prokuratuuri seletav sõnastik defineerib menetlustoiminguid kui süüteomenetluse tagamiseks teostatavaid toiminguid ehk kõiki menetleja toiminguid kriminaalmenetluses. Iga uurimistoiming on menetlustoiming, kuid mõni menetlustoiming ei ole uurimistoiming. Menetlustoiminguks, mis ei ole uurimistoiming, on näiteks kahtlustatava vahi alla võtmine. Selle tulemusena ei saada tõendeid, mis aitaksid kahtlustatava süüd tõendada, vaid selle eesmärgiks on üksnes tagada, et kahtlustatav ei põgene õigusemõistmise eest.[64] Kohtueelses menetluses on juba liigutud digitaalsete menetlustoimingute kasutusele võtmise poole, kuid seni ei ole see puudutanud uurimistoiminguid. Sellest tulenevalt analüüsitakse käesolevas töös eelkõige menetlustoimingute hulka kuuluvaid uurimistoiminguid, mille keskseks eesmärgiks on kohtueelses menetluses koguda tõendeid, et kinnitada või lükata ümber kahtlustatava süü olemasolu.

Kohtueelse menetleja jaoks on kuritegu peaaegu koguaeg ning kohtu jaoks alati minevikusündmuseks, seega ei ole võimalik neile seda presenteerida vahetult. Kuriteosündmuse ettekujutamise võimalikustamiseks tuleb luua sündmust kajastavate tõendite abil selle retrospektiivne mudel. Vastav mudel peab andma ettekujutuse sündmuse asjaoludest ja selles osalenud isikutest tõendite vahendusel. Toimunud kuriteosündmusest mudeli loomine saab olla võimalik seetõttu, et kuriteo toimepanemise mehhanismil on omadus oma olemust peegeldada ja peegelduda. See tähendab seda, et iga kuriteo toimepanemine jätab ümbritsevasse keskkonda ja inimeste teadvusesse jälgi. Seaduses ettenähtud korras kogutud kuriteo mehhanismi jäljed on tõendite allikaks, aga nendes sisalduv informatsioon on kriminaalasjas tõenditeks.[65]

Kriminaalmenetluse seadustiku § 63 lg 1 kohaselt saab tõendiks olla kahtlustatava, süüdistatava, kannatanu, tunnistaja või asjatundja ütlus, ekspertiisiakt ning ekspertiisiakti andmisel antud eksperdi ütlus, asitõend, uurimistoimingu, kohtuistungi ja jälitustoimingu protokoll või videosalvestis. Lisaks saab tõendiks olla muu dokument, foto, film või muu teabetalletus. Seega üheks peamiseks tõendite kogumise viisiks on uurimistoimingute teostamine, mida toetavad muuhulgas assisteerivad menetlustoimingud näiteks ekspertiiside ja jälitustoimingute näol.

[64] Prokuratuur. Seletav sõnastik. Arvutivõrgus: https://www.prokuratuur.ee/et/pressile/seletav-sonastik (15.04.2019).
[65] R. Öpik, lk 5.

KrMS sätestab järgnevad uurimistoimingute liigid:

- ülekuulamine (tunnistaja, kahtlustatava, kannatanu, asjatundja);
- vastastamine;
- ütluste seostamine olustikuga;
- äratundmiseks esitamine;
- vaatlus (sündmuskoht, laip, dokument, muu objekt, asitõend, läbivaatuse korral isik või posti- ja telegraafisaadetis);
- läbiotsimine;
- uurimiseksperiment.[66]

2.5. Digitaalselt teostatavad menetlustoimingud

Justiitsministeerium on võtnud küll suuna täisdigitaalsele kriminaalmenetlusele, mille hulka kuulub loomulikult ka kohtueelne menetlus, kuid läbitav tee soovitud edu saavutamiseks on veel küllaltki pikk. Eelnevalt on käesolevas töös välja toodud menetlustoimingute jaotumine, mille kohaselt tõendusteabe kogumisele suunatud toiminguteks peetakse uurimistoiminguid, ekspertiise, revisjon/audit, esemeliste objektide väljanõudmine või esitamine, jälitustoiminguid. Vaadeldes kõnealuseid toiminguid, saab järeldada, et areng on olnud küllaltki ebavõrdne. Nimelt on jõutud ekspertiiside ning jälitustegevusega kaasnevate toimingute teostamisel tehniliste abivahendite kasutusele võtmiseni, paraku aga ei ole seda tehtud uurimistoimingutega, mis moodustavad valdava osa klassikalisest kriminaalmenetlusest.

Ekspertiis saab täieliku tõendiväärtust omada kolme peamise elemendi olemasolul. Esiteks on vajalik menetleja lähteülesanne ekspertiisiks, ehk teisisõnu ekspertiisimääruse koostamine. Määrusega kirjeldab uurimisasutuse menetleja, mis on ekspertiisi määramise põhjuseks, milliseid eriteadmisi on vajalik rakendada ning millised on eksperdile esitatavad küsimused. Teiseks oluliseks elemendiks on ekspertiisi sisuline läbiviimine ning selle tulemusel vastuste leidmine lähteküsimustele. Ekspertiisi võtab kolmanda elemendina kokku ekspertiisiakt, mis kirjeldab läbi viidud uuringute ja nende tulemuste sisu, mis peab olema kõigile osapooltele kergesti jälgitav ja mõistetav. Peaasjalikult viib Eestis läbi kriminaalasjade ekspertiise justiitsministeeriumi hallatav Eesti Kohtuekspertiisi Instituut (edaspidi EKEI). Jõutud on praktikas selleni, et uurimisasutuse töötajad ei pea enam ekspertiisimäärusi pärast nende

[66] Kriminaalmenetluse seadustik - RT I, 13.03.2019, 7.

koostamist arvutis välja printima ning seejärel ametkondliku kulleri või postiasutuse vahendusel koos uuritava objektiga ekspertiisiasutusse toimetama. Määruste digitaalseks koostamiseks ning edastamiseks on loodud vastav võimekus nii politsei infosüsteemil MIS kui ka E-toimiku kriminaalmenetluse moodulil PRIS. Sama teed liigub tagasi ka uurimistulemuste saavutamisel EKEI poolt koostatav ekspertiisiakt ning seega puudub peale ekspertiisi objekti transportimise vajadus dokumente asutuste vahel liigutada. Kui objektideks on elektroonsel teel edastatavad materjalid, siis ka neid ei ole vaja enam füüsilisele andmekandjale kopeerida, et seejärel ekspertiisi saata, vaid ka nende edastamine on võimalik läbi loodud e-teenuste. Tulnevalt vestlustest erinevate uurimisasutuste menetlejatega on nad tekkinud võimalusega väga rahul ning suhteliselt kiirelt uue süsteemi omaks võtnud. Küllaltki väikese muudatusega on saavutatud oluline kokkuhoid menetlejate ajas ning uurimisasutuse vahendites. Paraku aga leidub endiselt ka neid menetlejaid ning EKEI töötajaid, kes harjumusest ja mugavusest ei kasuta loodud e-võimalust ning edastavad dokumente endiselt paberkandjal. Loodetavasti ka nemad kohanevad peagi uue süsteemiga ning võtavad selle omaks.

Teatud kuriteokoosseisude puhul tuleb kriminaalmenetluses mängu jälitustoimingute teostamine. KrMS § 126^1 lg 1 kirjeldab, et jälitustoimingute kui isikuandmete töötlemine seaduses sätestatud ülesande täitmist, mille eesmärgiks on andmete töötlemise fakti varjamine andmesubjekti eest. Vastav legaaldefinitsioon on küllaltki üldsõnaline ning jälitustoimingute sisu otseselt ei ava. Teisisõnu peetakse jälitustoimingu all silmas tõendite kogumisele suunatud uurimistegevust, mille käigus kogutakse teavet kuriteo ettevalmistamise kohta eesmärgiga kuritegu avastada või tõkestada. Lisaks võib jälitustoiminguid teostada tagaotsitavaks kuulutamise määruse täitmiseks, teatud juhtudel konfiskeerimismenetluse huvides teabe kogumiseks ja vajadusel kriminaalmenetluses teabe kogumiseks kuriteo kohta. Jälitustoiminguid eristab peamiselt teistest menetlustoimingutest nende küllaltki suur riive isikute eraelu puutumatusele. Jälitustegevusega hangitava informatsiooni maht on tavapäraselt väga suur ning PPA poolt on loodud selleks asjakohased infosüsteemid JÄTIS ja KAIRI, kuhu kogutud info ning koostatud kokkuvõtted talletada. Kuna jälitustoiminguks annab loa sõltuvalt toimingu liigist kas prokurör või eeluurimiskohtunik, siis on igati vajalik, et lubade väljastamiseks, kontrolliks ja pikendamiseks oleksid ka nemad võimelised kõnealuste infobaasidega töötama. Jälitustegevust läbi viivate ametnikega vesteldes selgus, et täna esineb aga probleem just eelkõige eeluurimiskohtunikega, kellele esitatakse tutvumiseks jälitustoimik paberkandjal hoolimata asjaolust, et toimiku sisu oleks kättesaadav ka JÄTIS ja KAIRI vahedusel. Selline hübriidse jälitustoimingu pidamine on väga koormav jälitusametnikule ning teisest küljest ei ole saavutatud puutumuses olevate andmebaaside loomisega taotletud ressursi

kokkuhoidu. Võttes arvesse asjaolu, et jälitustoimikus sisalduv informatsioon on oma olemuselt oluliselt tundlikum võrreldes klassikalise kriminaaltoimiku sisuga ning tihti võib sisaldada ka riigisaladust, siis nii ohutuse kui nõuete täitmise tagamise seisukohast oleks täisdigitaalse jälitustoimiku pidamine igati mõistlikum ning väheneks võimalikud toimiku kuritahtliku muutmise või kõrvalistesse kätesse sattumise tõenäosus. Samas ei tohi liigselt lootma jääda, et üha kasvava küberkuritegevuse käigus jäävad toimumata kriminaalmenetluse vastu suunatud rünnakukatsed.

Uurimis- või muu menetlustoimingu või selle tervikliku osa võib KrMS § 150 lg 1 kohaselt filmida või heli- või videosalvestada. Video- või helisalvestise esitamisel teeb uurija märkmeid uurimistoimingu protokolli koostamiseks. Seetõttu on salvestus ühtaegu uurimistoimingu protokolli täielikkuse tagamise vahend.[67] Video- ja helisalvestise kasutamine on küll tugevalt seotud digimaailmaga, kuid seda ei tohiks ennatlikult pidada kriminaalmenetluse digitaliseerimise elemendina.Kui jõuda tulevikus selleni, et video- või helisalvestus asendaks täielikult täna koostatavat menetlustoimingu protokolli, siis võiks sellele digitaalse menetlustoimingu tiitli omandada. Kas selline teguviis oleks aga ka mõistlik ning realistlik, analüüsib töö autor järgnevates peatükkides.

E-toimiku kriminaalmenetluse liideses PRIS on värskelt loodud võimalus laadida lisaks toimingu protokollile üles ka videosalvestis näiteks kahtlustatavana kinnipidamise, sündmuskoha vaatluse, isiku läbivaatuse, vastastamise, äratundmiseks esitamise ja läbiotsimise protokollide juurde. Kuid nagu eelnevalt mainitud, siis võib salvestiste kasutamine menetluses lihtsustada küll protokollimise tööd või hilisemat protokolli sisu õigsuse kontrolli, siis tänane õigus ei anna videole iseseisvat tõendiväärtust, ilma selle juurde kuuluva vaatlusprotokollita.

Uurimistoimingute hulgast ei saagi tegelikult täna tuua välja ühtegi konkreetset toimingut, mida kohtueelses menetluses praktikas igapäevaselt digitaalselt teostataks. Kõige lähemal sellele ollakse vast hetkel ülekuulamistega, kus tegemist ei ole pelgalt menetluse optimeerimisele suunatud tegevusega, vaid tihtipeale sundseisuga. Näiteks kasutatakse ülekuulamistel vajadusel kaugtõlgi abi. Sisuliselt tähendab see seda, et menetleja koos ütluste andjaga asub ühes asukohas ning üle videosilla ollakse üheduses tõlgiga, kes näiteks asub teises Eesti otsas. Kui aga on vaja üle kuulata menetleja asukohast kaugel asuv tunnistaja või kannatanu, kelle füüsiline kohale kutsumine ei ole vajalik ega otstarbekas, siis praktikas ei ole levinud olukord,

[67] H. Lindmäe. Menetlustaktika I. Tartu: Juura 1995, lk 19.

kus uurijad teeksid seda telesilla vahendusel. Pigem kasutatakse sellistes olukordades teiste prefektuuride uurijate abi, kes lähtuvalt kriminaalasja menetleja suunistest ja küsimustest viivad ise ülekuulamise teises piirkonnas läbi.

Käesolevas peatükis käsitlemata jäänud menetlustoimingute puhul ei ole paraku elektroonsete võtete kasutamine kohtueelses menetluses levinud. Võib esineda üksikuid menetleja initsiatiivil põhinevaid näiteid, kuid töö autorile ei ole need teada. Samas on kohtueelse menetlusega igapäevaselt kokkupuutuvate isikute soov nii mitmeidki toiminguid just tänu infotehnoloogiliste vahendite kasutamisele lihtsustada, et seeläbi saavutada kokkuhoid menetlusressursside ja menetlusosaliste koormamise osas.

2.6. Euroopa riikide menetluse digitaalsus

Oleme küll nüüd jõudnud ajastusse, kus avalike e-teenuste vahendusel kohtupidamine ja menetlus muutub järjest tavapärasemaks, siis kümmekond aastat tagasi valitses selles osas aga Euroopas veel suur ebakindlus. Kodanikud on võtnud järjest üle infoühiskonna põhimõtteid, kuid sama kergelt ei ole see käinud avalikus sektoris. Näiteks Lawyer Partners a.s. v. Slovakia kaasuses vaieldi alles selle üle, kas kohus peab võtma vastu digitaalselt esitatud avaldusi ning nende pinnalt alustama menetlusega. Tegemist oli küll tsiviilõigusliku kaasusega, kuid seisnes selles, et hageja soovis esitada hagiavalduse DVD plaatide vahendusel. Paraku kohus, konsulteerides sealse justiitsministeeriumiga leidis, et neil puudub tehniline võimekus ja ka kohustus sellisel viisil esitatud dokumentide töötlemiseks. Esitatud andmekandjad olid valitud tulenevalt dokumentide tohutust mahust, mis oleks nende välja printimisel ulatunud ligi 43 miljoni leheküljeni. Hoolimata sellest jäeti siseriiklike kohtute poolt hagiavaldused registreerimata ja menetlusse võtmata. Sellise käitumisega ei saanud aga nõustuda Euroopa Inimõiguste kohus, kes enda 06.11.2009 otsusega luges põhjendamatuks säärase käitumise ning juhtis kohtute tähelepanu, et avaldus ei tohi jääda menetlusse võtmata seetõttu, et see on esitatud elektroonselt.[68]

Kui infoühiskonna võidujooks leiab aset pea kõikides Euroopa riikides, siis elektrooniliste võimaluste olemasoluga kriminaalmenetluses niivõrd roosiline ei ole. On igati loogiline, et peamiselt käib õigusvaldkonna ITK areng käsikäes riigi üldise tasemega. Ei ole võimalik

[68] EIKo 16.06.2009, 54252/07 jt, Lawyer Partners a.s. v. Slovakia.

eeldada täisdigitaalse kohtumenetluse kasutamist, kui interneti või arvutite kasutamine ei ole siseriiklikult niivõrd levinud. Jättes kõrvale muu osa maailmast, käib Euroopa Liidu liikmesriikides järkjärguline vilgas töö, et arendada siseriiklike infotehnoloogilisi süsteeme. Arengutasemed on riigiti küll erinevad, kuid ühtlast liidrit on raske leida. Käesoleva töö keskmeks on küll digitaliseerimine kohtueelses menetluses, kuid see käib käsikäes kohtumenetluse üldiste IT arengutega. Euroopa Nõukogu kohtute efektiivsust hindav komisjon CEPEJ on enda 2018. aasta raportis väitnud, et elektroonilise toimiku võimaluse on kasutusele võtnud pea kõik liikmesriigid peale Küprose. Raport tõstab esile oma potentsiaali poolest Eesti justiitssüsteemi infosüsteemi E-toimik ning Norra süsteemi Lovisa. E-toimikut peetakse esimeseks süsteemiks Euroopas, mis on oma kasutuselevõtuga andnud ka reaalse tulemuse senise kohtumenetluse optimeerimiseks. Norra süsteemi Lovisa puhul tuuakse välja kogutud statistilise baasi tulemusel saavutatud töökoormuse parem jaotus kohtutes, mille tulemusel on kokku hoitud nii rahalist kui inimressurssi. [69] Raportis käsitletakse küll riikide kohtusüsteeme tervikuna, kuid eraldi ei ole analüüsitud kriminaalmenetlust. Hoolimata sellest võib eeldada, et enim arenenud riigid jõuavad ka esimeste seas digitaalse kriminaalmenetluseni.

Euroopa Liit on samuti proovinud panustada soosivalt liikmesriikide elektroonilise menetluse arendamisse. Euroopa Liidu Nõukogu e-õiguskeskkonna strateegia aastateks 2019-2023 sätestab, et Euroopa e-õiguskeskkonna eesmärk on parandada õiguskaitse kättesaadavust üle kogu Euroopa ning selle raames arendatakse info- ja kommunikatsioonitehnoloogiaid, mida saaks kasutada juurdepääsuks õigusteabele ja õigussüsteemidele. Digitaalselt läbiviidavatest menetlustest ja elektroonilisest suhtlusest kohtumenetluse osaliste vahel on saanud oluline komponent liikmesriikide kohtute töös.[70] Kaugema eesmärgina nähakse loomulikult vastava strateegiaga ette ühise süsteemi kasutuselevõttu, mis lihtsustaks riikidevahelist infovahetust ja koostööd justiitsküsimustes. Samas on strateegias jäetud küllaltki lahtised käed liikmesriikidele ning sätestatud on ainult üldised arengueesmärgid.

Kui mitmed riigi Euroopas on liikunud digitaalse kriminaalmenetluse poole ning võtnud kasutusele ka osaliselt digitaalsed kohtutoimikud, siis täisdigitaalsele kriminaalmenetlusele ei ole seni teadaolevalt üksi Euroopa Nõukogu liikmesriik ega ilmselt ka muu riik üle läinud.[71]

[69] Council of Europe. European judicial systems - Efficiency and quality of justice, lk 216. Arvutivõrgus: https://rm.coe.int/rapport-avec-couv-18-09-2018-en/16808def9c (15.04.2019.
[70] Euroopa Nõukogu. Euroopa e-õiguskeskkonna strateegia (2019–2023) - C96/04.
[71] M. Hirvoja. Kriminaalmenetluse revisjoni analüüs - üleminek täisdigitaliseeritud kriminaalmenetlusel - 31.05.2016, lk 23.

2.7. Kriminaalmenetluse digitaliseerimise õiguslik regulatsioon

Vältida tuleks kindlasti olukorda, kus mõningad menetlustoimingud on juba digitaliseeritud või loodud on suisa mõni andmebaas, millele ei ole aga kehtiv õigus järele jõudnud ning kehtestatud ei ole seda kasutata võimaldav regulatsioon. Näitena selle kohta, kuidas vahepealsel ajal tehnilised lahendused ja praktilised vajadused liikusid seadusandjast kiiremini, saab tuua 2007. aastal õiguskantsleri menetluses olnud piirivalve infosüsteemi juhtumi. Piirivalve infosüsteemi koguti alates 2003. aastast teavet järgmistest andmekogudest: sissesõidukeeldude riiklik register, ärandatud sõidukite andmebaas, infosüsteem POLIS ning Kodakondsus- ja Migratsiooniameti (KMA) väljaantavate isikut tõendavate dokumentide andmekogu.[72] Juurdepääsusildade loomine oli toimunud siseministri ja politseipeadirektori käskkirjade ning KMA ja Piirivalveameti vahel allkirjastatud isikuandmete üleandmise akti alusel. Õiguskantsler rõhutas, et põhiseaduse § 3 lõike 1 esimesest lausest tuleneva halduse seaduslikkuse põhimõtte järgi ei saa sellist andmekogude seadusega vastuolus olevat andmete edastamise õigust luua andmekogu põhimääruse, siseministri käskkirja ega isikuandmete üleandmise aktiga.[73]

Riigikontroll on enda 2016. aasta avalike e-teenuste auditis välja toonud ühe probleemina, et mitmete e-teenuste puhul järgitakse endiselt paberitel põhinevat asjaajamise loogikat ning seeläbi ei ole saavutatud tegelikku eesmärki. Paberprotsessi ülekandumine elektroonilisse on tingitud MKMi hinnangul sellest, et riigiasutused ja KOVid on valdavalt seisukohal, et teenuseid tuleb pakkuda, lähtudes rangelt õigusaktides kehtestatust ja õigusaktide muutmist ei algatata ka siis, kui selleks ilmneb vajadus. Näiteks viis MKM 2013. aastal Riigi Teataja andmete põhjal läbi analüüsi ja koostas selle kohta memo, millest selgus, et 71 seaduses oli nimetatud 172 dokumenti, mida võis üle anda või saata üksnes paberil ning nende elektrooniliselt esitamine ei olnud võimalik.[74]

[72] Õiguskantsler. Õiguskantsleri 2007. aasta tegevuse ülevaade, lk 207. Arvutivõrgus: https://www.oiguskantsler.ee/sites/default/files/6iguskantsleri_2007._aasta_tegevuse_ylevaade.pdf (15.04.2019).
[73] P.K. Tupay, M. Mikiver. E-riik ja põhiõigused. - Juridica III/2015, lk 165.
[74] Riigikontroll. Avalike e-teenuste kasutatavuse aruanne riigikogule 2016, lk 18. Arvutivõrgus: https://www.riigikontroll.ee/DesktopModules/DigiDetail/FileDownloader.aspx?AuditId=2411&FileId=13797 (15.04.2019).

Tulles kriminaalmenetluse kohtueelse menetluse juurde, saab vähemalt kinnitada, et digitaliseerimisele suunatud toimingute ja kehtiva õiguse vahel otsest konflikti ei eksisteeri. Seda aga mitte põhjusel, et seadusandlus oleks niivõrd kaasaegne, vaid pigem pelgavad menetlejad tänapäevaseid meetodeid kasutada ning seda ei võimalda ka olemasolevad tehnilised vahendid.

Tehnika arenguga kaasas käimiseks pööratakse üha rohkem tähelepanu digitaalsete tõendite kasutamisele kriminaalmenetluses. Digitaalsete tõenditena mõistetakse füüsilisel kujul mittetajutavaid tõendamisesemeid, mis on taasesitatavad ainult nende digitaalsel kujul. Teisisõnu on tegemist näiteks andmetega, millele pääseb ligi läbi seadme või serveri, kuhu need on eelnevalt talletatud. Euroopa Komisjon on vastava teemaga tugevalt tegelenud ning tegeleb aktiivselt seda eesmärki toetava seadusandluse loomisega. Elektrooniliste tõendite kõrval Euroopa Liidu õiguses jäänud määratlemata kord või vähemalt suund füüsiliste tõendite hankimisel digitaalsete vahendite kasutamise osas. Põhjuseks võib eelduslikult pidada asjaolu, et digitaalsete tõendite kogumine erinevalt elektroonsele kujule viidavatest tõenditest eeldab tihtipeale rahvusvahelist koostööd ning seeläbi on vajalik ka ühtsete aluste kehtestamine. Sarnaselt ei saa EL aga määratleda siseriiklikus õiguses rakendatavaid menetlusmeetodeid ja viise, vaid saaks ainuüksi suunata riike järgima isikute menetlusõiguseid. Liidusiseselt on oluline, et tagatud on õiglase kohtupidamise põhimõte ning tõendite kogumise viisi laiemalt ei määratleta.

Menetlusseadustik (KrMS) näeb ette mitmeid elektroonsel viisil teostatavaid menetlustoiminguid. Paraku on kehtiv regulatsioon digitaalsete vahendite vahendusel või abil tõendite kogumiseks suunatud hetkel olukordadele, kui muul viisil ei ole võimalik saavutatud eesmärki täita. Näiteks on ette nähtud kaugülekuulamise (KrMS § 69 lg 1) või vastastamise läbiviimine alles siis, kui tavapärase ülekuulamise läbiviimine on näiteks raskendatud või ülemääraseid kulutusi põhjustav. Tänaste arenenud tehniliste võimaluste juures tuleks aga pigem suunata menetlejaid sarnaseid meetodeid igapäevaselt kasutama ning mitte püsima vanades harjumustes ja mugavustsoonis.

3. KOHTUEELSE MENETLUSE DIGITALISEERIMINE

3.1. Digitaalne kohtueelne menetlus

Kriminaalmenetluse seadustiku ja teiste seaduste muutmise seaduse eelnõu seletuskirja kohaselt on mh kriminaalmenetluse revisjoni eesmärkideks:

1) võimaldada üleminek täisdigitaalsele kriminaalmenetlusele, milleks muudetakse seaduse sõnastus tehnoloogianeutraalseks ning loobutakse mõistetest, mis viitavad paberdokumentide vormistamisele. Samuti nähakse ette üldreegel, et teabevahetus kriminaalmenetluse raames toimub eelkõige digitaalses vormis;
2) kõrvaldada seaduse nõuded, mis kohustavad menetlejaid sama tõendi kogumisel ja vormistamisel tegema dubleerivaid tegevusi. Selleks lihtsustatakse erinevate menetlustoimingute protokollimise nõudeid ning soodustatakse heli- ja videosalvestiste tegemist, samuti võimaldatakse isikutel anda kriminaalmenetluses ütlusi menetleja juurde kohale tulemata.[75]

Kohtueelse menetluse digitaliseerimisega ei tohiks aga liigselt hoogu sattuda ning tagada tuleks selle täielik toimekindlus. Menetluslike, sageli formaalsete puudujääkide tuvastamisest on saanud eeluurimisasutuste vastaspoole rutiinne kaitsetaktika. Tõe kriteeriumi hägustumine avab kaitsele uued taktikalised võimalused, kus vaidlustatakse mingid kuriteosse puutuvad pisidetailid, veendakse kohut nende olulisuses ja aetakse menetlus sisuliselt ummikusse sellega, et nõutakse kuriteo mõne detaili üksikasjalikku taasesitamist ja faktilist tõendamist.[76] Selle tulemusel võib tekkida olukord, kus ainuüksi menetlusökonoomika seisukohast rakendatud digitaalne menetlustoiming võib muutuda kasutuks, sest selle teostamise viis ei vasta näiteks praktikas levinud metoodikale ning ei ole seega kohtumenetluses enam kontrollitav. Hilisemas võistlevas menetluses peab olema võimalik veenduda, et kogutud tõendid on valiidsed ning kogutud kehtivaid õigusnorme jälgides. Lisaks peab olema tagatud kõikide menetluses osalevate poolte võrdsus elektroonsete vahendite vahendusel menetlusest osa võtta ning ükski pool ei tohi jääda selles osas nõrgemasse seisu.

[75] Kriminaalmenetluse seadustiku ja teiste seaduste muutmise seaduse eelnõu seletuskiri – 04.05.2018, lk 1.
[76] J. Saar. Eesti kriminaalmenetluse juhtum. - Juridica V/2018, lk 299-306.

3.2. Digitaliseerimise vajalikkus ja eesmärk

Kriminaalmenetluse digitaliseerimise peamiseks eesmärgid saab jagada üldistades kaheks. Üheks eesmärgiks on kindlasti läbi elektroonsete lahenduste saavutada kokkuhoid inimeste aja ja koormatuse arvelt ning vähendada otseseid rahalisi kulusid pabertoimikutelening toimingutele ja näiteks ka kütusele, mis nende transportimiseks või teostamiseks kulub. Teiseks ning tegelikult veelgi olulisemaks eesmärgiks tuleb aga pidada menetluse optimeerimist, läbi mille saavutatakse kiirem, läbipaistvam ja eesmärki paremini silmas pidav kohtueelne ning ka hilisem kohtumenetlus. Inimeste koormatuse ning rahaliste kulutuste kokkuhoid ei vaja vast laiemalt selgitamist. Optimeerimise all peab aga autor silmas olukorda, kus väiksema vaevaga saavutatakse esmalt kiirem ning kindlasti ka menetluse eesmärke paremini järgiv ning objektiivne tulemus. Teisisõnu kannatanut, tunnistajaid ning ka uurimisasutuse töötajaid ja kaasatud eksperte koormatakse vähem ning kuni vastupidise kohtuotsuseni oleks tagatud kahtlusaluseid ja hilisemaid süüdistatavaid puudutav süütuse presumptsioon.

Ajaline võit tuleks saavutada eelkõige kahe elemendi koosmõjus. Esmalt tuleb kaotada dubleerivad toimingud ning seejärel peab e-lahenduste kasutamine jõudma selle suurepärase võimaluse juurde, kus loetud sekunditega saab laadida kogutud uurimismaterjalid selleks kohandatud andmebaasi, mille vahendusel saavad enda rolli menetluses kujundada juba teised asjasse puutuvad isikud. See tähendab, et sündmuskohal talletatud digitaalne teave on süsteemist kättesaadav kõigile, kel juurdepääsuks vajadus ja selle alusel saab teha näiteks kohtuarst, ekspertiisi, prokurör valmistada ette järgmisi toiminguid ja eeluurimiskohtunik vajadusel kasutada andmeid jälitustegevuse, läbiotsimise või vahistamise loa väljastamiseks. Sisuliselt on tegemist ühendatud anumate süsteemiga, kus andmed liiguvad vabalt ja kõigile on tagatud võimalus teha oma tööd kiirelt ja kvaliteetselt.[77] Hea näitena võib näiteks tuua kokkuleppemenetluse kiirmenetluse vormis, mille ajaline kestvus peab mahtuma 48 tunni sisse. Praktikale tuginedes saab väita, et umbes poole või kohati isegi suurema osa menetluse ajast võtab endale bürokraatia, mille käigus on menetlejal vaja koguda kokku erinevad kahtlustatavat puudutavad andmed, need nõuetele vastavalt vormistada ning seejärel pabertoimikusse köita. Samuti peab ajaraami sisse mahtuma ka toimiku prokuratuuri toimetamine, misjärel alles saab prokurör asuda kokkuleppe sõlmimise juurde. Kusjuures kogutavad andmed hangitakse klassikaliste tüüppäringutega erinevate andmebaaside vahendusel. Näiteks kriminaalses joobes

[77] Peaprokuröri kõne Prokuröride XX üldkogul – 06.04.2018. Arvutivõrgus: https://www.prokuratuur.ee/sites/www.prokuratuur.ee/files/elfinder/Peaprokur%C3%B6ri%20k%C3%B5ne.pdf (15.04.2019).

tabatud autojuhi puhul kuulub toimikusse kogutava materjali hulka mh andmed isiku juhtimisõiguse, sõiduki kuuluvuse ning ka isiku eelnevate karistuste kohta. Kõik need andmed oleks aga vastava süsteemi olemasolul võimalik automaatselt pärida ja samaaegselt liita digitoimiku juurde kõigest paari hiireklikiga. Lisaks uurimisasutuse ja prokuratuuri aja kokku hoidmisele annab süsteemide automatiseerimine paremad võimalused ka kahtlustatavale ja kaitsjatele. Vastava õiguse omandamise järel on täisdigitaalse kriminaaltoimiku puhul ka kaitsjal võimalik näiteks toimikuga tutvuda ja menetluses taotlusi esitada läbi E-toimiku süsteemi.

Kriminaalmenetluse üheks osapooleks menetlusosaliste hulgas võib sõltuvalt menetlusliigist olla kannatanu, kelle liigset koormamist uurimisasutuse poolt tuleks ehk isegi rohkem vältida, kui seda kahtlustatavate puhul. Justiitsministeeriumi poolt määratletud kriminaalpoliitika põhialused aastani 2030 on seadnud eesmärgiks lisaks süüteomenetluse tõhusaks (sh digitaalseks) muutmisele ka menetluse muutmine personaalseks ja ohvrisõbralikuks, asjatut bürokraatiat vältivaks, seades võimalikult paljude juhtumite puhul eesmärgiks õigusrikkumisele eelnenud olukorra taastamise (taastav õigus, sh lepitamine).[78] Seega ei saa pidada kohtueelses menetluses digitaalsete võtete kasutamist ainuüksi kahtlustatavat ja menetlejat toetavaks, vaid keskmesse tuleks seada just eelkõige see, kes tõenäoliselt on menetlusosaliseks sattunud kõige väiksema teopanusega ning juhuse tahtel. Sama põhimõtet tuleb rakendada ka tunnistajate puhul, kes tihtipeale on sattunud menetlusosalise staatusesse ise selleks midagi tegemata ning oleks ebaõige nende aega ja emotsionaalset tasakaalu asjata kulutada.

Eelpool on mainitud ühe digitaliseerimise eesmärgina ka menetluse läbipaistvuse paremat tagamist. Loomulikult ei saa väita, justkui tänane kriminaalmenetlus ei toimuks läbipaistvalt ning selle parandamiseks oleks vaja just menetlus digitaliseerida. Pigem tuleb selle all silmas pidada menetlusosaliste paremaid võimalusi veenduda õiglase menetluse toimimises ning osalt ka menetluskäigu jälgimiseks. Ei ole harvad kahtlustatavate süüdistused uurimisasutuse töötajate suunas, kes väidetavalt on toimikus asuvaid dokumente muutnud või fabritseerinud ning vahel ka süüstava eesmärgi saavutamiseks kaotanud. Kui pabertoimiku kasutamise puhul on see teoreetiliselt küll võimalik, siis digitoimikus ilma jälgi jätmata selline teguviis pea võimatu. Elektroonilistes andmebaasides logitakse absoluutselt kõik muudatused toimikus ning isegi selle vaatamised. Kui pärast kohtueelse menetluse lõppenuks lugemist prokuratuuri poolt

[78] Justiitsministeerium. Kriminaalpoliitika põhialused aastani 2030. Arvutivõrgus: https://www.just.ee/sites/www.just.ee/files/kriminaalpoliitika_pohialused_2030.pdf (15.04.2019).

muuta näiteks süüdistatavale nähtavaks osaliselt menetleja logiandmed, siis muutub toimiku koostamine tagantjärgi jälgitavaks ning hoiab kindlasti ära ka suurel hulgal väärarusaame. Sellise võimaluse tekkimisel tuleb aga eelnevalt põhjalikult analüüsida, et vastavate logiandmete põhjal ei oleks tulevikus võimalik teha kaitsjatel ja ka kahtlusalustel/süüdistatavatel järeldusi uurimisasutuse menetlustaktika suhtes. Samas peab olema kaitsjal ja kahtlustataval/süüdistataval võimalik enda õiguste kaitsmiseks jälgida paremini menetluse käiku.

Jättes hetkel kõrvale tohutu tehnilise taristu ja andmemahuvõimekuse vajaduse, võime eeldada, et ühel hetkel oleme olukorras, kus digitaalsed võimalused mitte ainult ei paku lihtsamaid töömeetodeid, vaid toetavad ka õiglase menetluse läbiviimist. Prokuratuuri Infosüsteem on jõudnud enda arendustega sinnamaale, et näiteks kahtlustatavana kinnipidamise protokolli või läbiotsimisprotokolli ning ka mitmete teiste uurimistoimingute juurde on võimalik lisada ka videosalvestusi. Nagu ikka, on ka sellisel võimalusel nii positiivseid kui negatiivseid külgi. Positiivsena võib välja tuua süsteemi laetud video abil täiendava tõendamisvõimaluse loomise, kui video abil on võimalik edasi anda midagi, mis ei ole läbi teksti ja fotode tajutav. Teisalt aga toob see ilmselt kaasa suurema kaitsjate poolse vigade otsimise maania, kus hakatakse võrdlema video ja protokolli lahknevusi. Sellist käitumist tuleks aga pidada võistlevas menetluses täieõiguslikult osalemiseks. Osalt on ilmselt vastava video üleslaadimise võimaluse taga ka tahe pakkuda lihtsamaid tõendamisvõimalusi, kuid eelduslikult ei hakka vähemalt esialgu video asendama selle vaatlusprotokolli täies ulatuses ning hetkel on tegemist pigem rohkem võimaluse kui eesmärgiga.

Siinkohal on veel käsitlemata kohtueelse menetluse digitaliseerimisega kaasnev preventiivne võimekus. Kriminaalmenetluse andmete sisestamisega elektroonilistesse andmebaasidesse ei tehta kogutud andmetega muud, kui muudetakse need sisuliselt masinloetavaks. Teisisõnu koguneb hulk andmeid, mida on võimalik klassifikaatorite abil eraldada ja pidada nende üle jooksvat arvestust. Kui andmebaas hakkab tulevikus sisaldama infot kõikide kriminaalmenetluste kohta, siis on võimalik vastava võimekuse olemasolul sealt mängleva kerglusega leida näiteks informatsioon selle kohta, millises Tallinna piirkonnas on toime pandud kõige rohkem vargusi, või millisel kellaajal armastavad liikluses seigelda roolijoodikud. Juba täna kasutab politsei tänu enda statistilistele andmebaasidele antud võimalusi, kuid praegusesse informatsiooni tuleb suhtuda teatava reservatsiooniga.

Kogutud andmete kvaliteet sõltub hetkel oluliselt menetleja suvast kanda relevantne informatsioon paralleelselt pabertoimikule ka infosüsteemi, kuna pabertoimik omab täna ikka veel primaarset tähendust. Kui jõuda aga täisdigitaalse kriminaalmenetluseni, siis kogutava statistika abil on võimalik tulevikus kujundada politseilist ennetustegevust ning ka riikliku kriminaalpoliitikat.

3.3. Digitaliseerimist vajavad uurimistoimingud

3.3.1. Uurimistoimingud

Eelpool käsitletu põhjal tuleb menetlustoimingute all mõista esmalt tõendusteabe kogumisele suunatud toiminguid ning seejärel korraldava ja tagava iseloomuga toiminguid. Uurimistoiminguid eristab teistest tõendite kogumisele suunatud menetlustoimingutest pealiselt kaks olulist tunnust:

1) Muude menetlustoiminguteta tõendite kogumine on tavapäraselt korraldava iseloomuga ning esitatakse menetlusotsuste kaudu. Sellisteks otsusteks võivad olla näiteks nõudekirja esitamine, ekspertiisimäärus vms. Selleks, et teostada klassikalist uurimistoimingut, ei ole korraldavat menetlusotsust uurija poolt vaja koostada. Erandina võib välja tuua ainult läbiotsimise toimetamise, sest selle teostamiseks on vajalik eelnev luba prokuratuurilt või kohtult.

2) Uurimistoimingu läbiviimisel teostatakse uurimisasutuse menetleja poolt tõendite kogumist vahetult. Muude menetlustoimingute puhul sisuliselt uurija delegeerib enda koostatud menetlusotsusega selle ülesande teistele, nt ekspertiisimäärusega eksperdile või nõudekirjaga kolmandale isikule. Ekspertiisiga saadavat kriminaalasja tõendit ei saa pidada uurimistoiminguks, kuna see pärineb kaksikallikast (ülesande andnud menetleja ja tulemuse saavutanud ekspert). Sellest tulenevalt saab uurija tegevust tõendamiseseme kohta asjaolude vahetul kogumisel nimetada uurimistoiminguks.[79]

Uurimistoimingute näol on tegemist ühe peamise viisiga, kuidas kohtueelse menetluse käigus tõendite kogumist teostatakse. Seega on igati loogiline, et kui suurima osa kohtueelse menetluse käigust moodustab just uurimistoimingute teostamine, siis just sinna tuleb suunata ka menetluse

[79] R. Öpik, lk 6.

optimeerimist taotlev digitaliseerimise raskuspunkt. Samuti saab töös eelnevalt käsitletu põhjal väita, et muude menetlustoimingute puhul (nt jälitustoimingud, ekspertiis) on areng olnud eesmärgipärane ning jättes uurimistoimingud kõrvale, teostatakse need enamjaolt juba elektrooniliselt. Menetluse suurimat mahtu nõudvate uurimistoimingutega kahjuks aga lood nii head ei ole. Peamiseks aeglase arengu põhjuseks võibki ehk pidada uurimistoimingute suuremat hulka võrreldes teiste menetlustoimingutega, mis tähendab ka suuremat puutumuses olevat isikute hulka ning mahukamat vajadust infotehnoloogilistele lahenduste arendamisse. Järgnevalt lahkab töö autor põhjalikumalt erinevate KrMS sätestatud uurimistoimingute olemust, nende digitaalsuse hetkeseisust ning vaatleb ambitsioone, kuhu postitiivsete ja negatiivsete külgede analüüsimisel menetluspraktika jõudma peaks.

3.3.2. Ülekuulamine

Ühe digitaliseeritava menetlustoiminguna on olnud arutlusel tunnistaja ja kannatanu ülekuulamine. Visionärid näevad, et menetlusosalistel ei ole tulevikus enam tarvilik teatud juhtudel politseisse füüsiliselt ise kohale tulla ning nende ütlused oleks võimalik menetlejale edastada elektroonselt digiallkirjastatuna.[80]

Ülekuulamine on uurimistoiming, mille eesmärk on saada kriminaalmenetluse seadustiku sätteid ning menetlustaktika nõudeid ja soovitusi järgides tunnistajalt, kannatanud või kahtlustatavalt tõendamiseseme asjaolude kohta ütlusi tema vabas jutustuses või vastustes uurija küsimustele.[81] Ühtlasi saab pidada ülekuulamiste teostamist pea kõikide lõpule viidud kohtueelsete kriminaalmenetluste lahutamatuks osaks. Oluline on ülekuulamise käigus saavutada tõeste ja tõendamisesemena kasutatavate ütluste saamine, ülekuulatavaid võimalikult vähe koormaval viisil. Kuna ülekuulamisi saab pidada ka üheks kõige sagedasemaks uurimistoiminguks, siis tuleks selle võimalikku digitaliseerimist analüüsida põhjalikumalt.

Prokuratuur leiab, et oluline on kannatanu säästmine menetluse vältel. Mitmeid kuritegusid saaks tõendada tänases IT ühiskonnas tehniliste abivahendite toel, nagu näiteks on politsei rinnakaamerate abil ning nende tõendite paberkujul dubleerimine ei ole mõistlik. Samuti

[80] Kriminaalmenetluse seadustiku ja teiste seaduste muutmise seaduse eelnõu seletuskiri seisuga 04.05.2018. Arvutivõrgus: https://www.advokatuur.ee/uploads/files/SK%20 KrMS%20revisjon.pdf (15.04.2019).
[81] H. Lindmäe. Menetlustaktika I. Tartu: Juura 1995, lk 21.

tahame vältida korduvaid ülekuulamisi, mis võivad haavatavaid ohvreid liigselt traumeerida.[82] Siinkohal on rinnakaamerate video abil tõendamise näite all silmas peetud eelkõige tõendite dubleerimist ütlustega. Selline lahendus on kindlasti mõistlik ning tegelikult saab seda juba praegu rakendada, sest video näol tõendi olemasolu on piisav ning menetlusökonoomika põhimõttest tulenevalt ei tohiks seda niigi dubleerima hakata.

Kriminaalmenetluse seadustiku § 6 tulenev legaliteedipõhimõte kohustab pädevaid ametivõime alustama kuriteo tunnuste sedastamisel kriminaalmenetlust sõltumata mis tahes isiku või riigiasutuse arvamusest. Eeltoodust järeldub ühtlasi, et uurimisasutusel ja prokuratuuril puudub kuriteole viitava teabe saamisel pädevus hinnata kriminaalmenetluse alustamise otstarbekust üksikjuhtumil. Sellise lähenemisega saavutatakse kõigi asjassepuutuvate isikute võrdne ja õiglane kohtlemine. Üksnes olukorras, kus pädevatele ametiasutustele laekunud teabe põhjal ilmnevad vahetult kriminaalmenetlust välistavad asjaolud KrMS § 199 tähenduses, on uurimisasutus ja prokuratuur õigustatud jätma kriminaalmenetluse alustamata.[83]

Prokuratuur juhtis juba 2015. aastal uurimisasutuste tähelepanu asjaolule, et digitaalselt esitatud süüteoavaldused on piisavad, et neid käsitleda esmase menetlustoiminguna. Kui menetleja leiab, et süüteoavalduses välja toodud informatsioon on ammendav või vähemalt piisav kriminaalmenetluse algatamiseks, siis tuleb seda ka teha ilma, et vajalik oleks eelnevalt kannatanu üle kuulata. Kui menetleja leiab, et vajalik on kannatanult lisainformatsiooni hankimine, siis peaks ta esmalt kaaluma, milline meetod on selleks parim. Kui avaldaja on juba korra valinud süüteost teatamise vormiks digitaalse võimaluse, siis tuleks eeldada, et tegemist on eelistatud asjaajamisvormiga kogu menetluse ulatuses. Hetkel politsei kodulehel kasutuses oleva süüteost teatamise vormi[84] lõpus on avaldajalt küsitud, kas ta on nõus kokkuleppemenetlusega, kas ta on nõus menetlusega seotud dokumentide edastamisega tema e-posti aadressile ning kas ta soovib teavet E-Toimiku kaudu. Sellised kontrollküsimused on menetlustoimingute digitaliseerimise perspektiivist küll olulised, kuid praktikas jäetakse need täna tahaplaanile. M. Hirvoja on leidnud, et edasises menetluses digitaalse tabevahetuse kaudu

[82] Prokuratuur. Riigi peaprokuröri ülevaade Riigikogu Põhiseaduskomisjonile seadusega Prokuratuurile pandud ülesannete täitmise kohta 2016. aastal, lk 4. Arvutivõrgus: http://www.prokuratuur.ee/sites/www.prokuratuur.ee/files/elfinder/article_files/peaprokurori_ulevaade_15.06_ps_komisjonile_2016_kohta.docx (15.04.2019).
[83] RKKK 14.04.2010, 3-1-1-19-10, p 8.2.
[84] Politsei- ja Piirivalveamet. Politseile avalduse esitamise digitaalne vorm. Arvutivõrgus: https://www2.politsei.ee/et/teenused/politseile-avalduse-esitamine.dot (15.04.2019).

osalemiseks tuleks küsida menetlusosalistelt eelnevalt nõusolek.[85] Töö autor on seisukohal, et kui kodanik on pöördunud politsei poole digitaalse kanali kaudu, siis tuleks eeldada tema valmisolekut ka elektroonseks sidepidamiseks ning eraldi nõusoleku küsimine ei ole vajalik. Pigem tuleks edasise menetluse käigus keskenduda menetlusosalise õiguste tagamisele ning sellest tulenevalt valida edasine teabevahetuse viis.
Jõudes täisdigitaalse kannatanu ülekuulamiseni, peaks aga menetlejale jääma hoolimata näiteks elektrooniliselt esitatud kuriteoteatest kaalutlusõigus isiku füüsiliseks kohale kutsumiseks kui tekib näiteks kahtlusi kahtlustatava tehnilises pädevuses või esinevad probleemid näiteks eneseväljendusega. Rõhutada tuleb aga veel, et tegemist peab olema menetleja kaalutlusest, mitte harjumusest või mugavusest tuleneva otsusega.

Olukorras, kus isik on langenud süüteo ohvriks, oleks elektroonne ülekuulamine kindlasti eelistatuim. Ühelt poolt on see kindlasti kannatanuid vähem koormav ning minimaliseerib tema võimalikke korduvaid läbielamisi. Teisalt tõotab selline menetluspraktika, kus ütlusi antakse e-kirja või kuriteoteate teel, muuta ülekuulamised sisuliselt kaootiliseks, sest ütlusi andev isik ei saa juhinduda menetleja vahetutest küsimustest ega oska enese ütlusi eriteadmiste puudumisel paremini sõnastada. Samuti võivad ütlustes seeläbi pealiskaudseks või suisa välja jääda olulised teemakäsitlused, mis viivad aga selleni, et soovitud kokkuhoid kannatanu või tunnistaja koormamise osas muutub hoopis vastupidiseks. Kui ütlused ei ole üheselt mõistetavad ja tekitavad küsimusi, siis ei jää menetlejal ikkagi muud üle, kui ta uurimisasutusse välja kutsuda. Selline olukord tekitab aga situatsiooni, kus näiteks kannatanu peab korduvalt sama sündmust oma mõtetes läbi elama ning see osutub kindlasti vaimselt koormavamaks.

Olukorras, kus tunnistaja vahetu ülekuulamine on raskendatud või võib põhjustada liigseid kulutusi võib KrMS § 69 lg 1 kohaselt menetlejale korraldada tunnistaja kaugülekuulamise. Samuti on võimalik seda teha, kui see on vajalik tunnistaja või kannatanu kaitset silmas pidades. Laiendada tuleks aga kaugülekuulamise piiritlust. Kehtiv regulatsioon nimetab kaugülekuulatavate isikutena vaid tunnistajaid. Kuivõrd muude ülekuulamiste puhul lähtutakse tunnistajate ülekuulamise kohta käivatest sätetest, järeldub sellest ka kaugülekuulamise lubatavus nt kannatanu ülekuulamisel.

[85] M. Hirvoja. Kriminaalmenetluse revisjoni analüüs - üleminek täisdigitaliseeritud kriminaalmenetlusel - 31.05.2016, lk 5.

Asendades sõna „tunnistaja“ sõnaga „isik“, avardatakse kaugülekuulamise rakendusala sõnaselgelt kõikidele neile, keda on vaja üle kuulata. See ei tähenda loomulikult kaugülekuulamise kohustuslikuks muutmist, vaid lihtsalt seda, et ülekuulamise vormi valib menetleja vastavalt menetlustaktikalistele vajadustele.[86]

Kaugülekuulamise säte määratleb ära kolm konkreetset olukorda, millal on võimalik seda meetodit kasutada. Vastavat võimalust saab KrMS § 69 lg 1 kohaselt kasutada ammendavalt ainult juhul, kui tunnistaja vahetu ülekuulamine on raskendatud, põhjustab ülemääraseid kulutusi või see on vajalik tunnistaja või kannatanu kaitset silmas pidades. Kahjuks ei võimalda sätte sõnastus laiendada antud meetodit hetkel menetlustoimingute digitaliseerimise kontseptsioonist tulenevalt. Kaugülekuulamise kasutamine võiks tulevikus tuleneda eelkõige menetleja kaalutletud otsusest. Vastavat võimalust tuleks kasutada ühel poolt vaadeldes ressursikokkuhoidu ning ütlusi andva isiku võimalikult vähest koormamist. Teisena tuleks jõuda menetlustaktika valikust tulenevale seisukohale, kas distantsilt isiku ülekuulamine võib seada ütluste andmise adekvaatsuse ja õigsuse ohtu või mitte. Vastava otsuse adekvaatsus võimaldaks tulevikus üle kuulata lisaks tunnistajale ja kannatanule, miks mitte lihtsamates asjades ka kahtlustatavaid. Kuid viimaste puhul peab tegemist olema loomulikult väga põhjalikult analüüsitud otsusega.

Kui menetleja peaks kohtueelses menetluses kokku põrkama olukorraga, kus on tekkinud tugev kahtlus kaugülekuulamisel saadud ütluste õigsuses, siis talle jääb alati õigus korraldada kordusülekuulamine ning seda juba menetleja tööruumides. Menetluse omaette eesmärgiks ei saa olla ajaline ning rahaline kokkuhoid või ülekuulatava mugavus, vaid keskne eesmärk on ikkagi tagada õiglane ning objektiivsele tulemusele jõudev menetlus.

Üheks digitaalse kannatanu ülekuulamise või elektrooniliselt esitatud avalduse pinnalt menetluse alustamise ning hilisema eeluurimise ohukohaks on isikute valideerimine. Ainsaks tõsiseltvõetavaks lahenduseks saab pidada riiklikult tunnustatud autentimisteenused nagu digiallkiri ID-kaardiga ja Mobiil ID. Antud meetodite kasutamine peaks esmalt minimaliseerima ohu, kus süüteoteate või ütluste andmisel käitutakse pahatahtlikult. Teiseks annab isiku identifitseerimine parema võimaluse talle tutvustatud õiguste ja kohustuste ning tema poolt antud ütluste kinnitamiseks. Liialt ei tohiks karta seda, et inimesed hakkavad massiliselt kuritarvitama võimalikke loodavaid võimalusi ning kasutavad seda näiteks

[86] Kriminaalmenetluse seadustiku ja teiste seaduste muutmise seaduse eelnõu seletuskiri – 04.05.2018, lk 9.

valeavalduste või tunnistajad valeütluste esitamiseks. Selline teguviis oleks uurimisasutusele väga koormav ning seaks süsteemi tegeliku otstarbekuse kahtluse alla. Õnneks on seadusandja näinud ette vastava olukorra vältimiseks ka sanktsiooni ning karistusseadustiku (edaspidi KarS) § 320 lg 1 kohaselt karistatakse kannatanu või tunnistaja poolt kriminaal- või väärteomenetluses või tsiviilkohtu- või halduskohtumenetluses teadvalt vale ütluse andmise eest või menetlusosalise poolt vande all teadvalt vale seletuse või vande all teadvalt vale vara nimekirja või sissetulekute või kulude arvestuse andmise eest rahalise karistuse või kuni kolmeaastase vangistusega.[87]

Lisaks on võimalikuks ohukohuks kaugülekuulamise puhul ka ütluste mõjutamine nö kaarditaguse isiku poolt. Selliste olukordade mõju vähendamiseks objektiivsetele menetlustulemustele saab vähendada. Selleks tuleb selgelt ülekuulamise käigus isikule tema õigusi tutvustades rõhutada, et kui keegi toimingu käigus või sellele eelnevalt on leidnud aset isiku mõjutamine ütluste muutmiseks, siis tuleb esimesel võimalusel sellest teavitada menetlejat. Kordusülekuulamine saab aset leida järgnevalt juba uurimisasutuse ruumides. Liialt ei tohiks sellist ohtu aga karta, sest mõjutamine võib samuti leida aset enne uurija tööruumides ülekuulamist ning kui ülekuulatav sellest teada ei anna, siis ei erine see mõjust kaugülekuulamisele.

Käesoleva töö autor näeb visioonina, et tulevikus võiks toimuda kõik menetleja kaalutlusel läbi viidavad kaugülekuulamised läbi e-toimiku keskkonna. Eeldusena peaks kõigil uurimistoimingus elektroonselt osalevatel isikutel olemas olema toimiv ID-kaart koos pääsukoodidega, töötav internetiühendusega arvuti, millel olemas mh veebikaamera ja mikrofon. Tänapäeva sülearvutitel on need enamjaolt juba vaikimisi olemas ning seega ei tohiks pidada vastava tehnika olemasolu vähetõenäoliseks. Toimingus osalemiseks tuleks riigil luua ühelt poolt vajaliku funktsionaalsusega menetlejapoolne keskkond, kuhu on võimalik sisestada kõik ülekuulamist ettevalmistavad andmed alates kriminaalasja numbrist, lõpetades ülekuulatava isikuandmetega ning samas keskkonnas peaks olema võimalik paralleelselt näha ja kuulda videosilla vahendusel ülekuulatavat ning trükkida protokolliks antud ütlusi. Ütlusi andval isikul on aga vajalik omaltpoolt logida ID-kaardi abil avalikku E-toimikusse. ID-kaardiga sisse logimine loob lisaks tema tuvastamisele eelduse, et isik on võimeline sama kaardi vahendusel andma ka hilisema protsessi käigus digiallkirja. Seejärel on võimalik liikuda uurimistoimingu lehele, kus ülekuulatav saab luua menetlejaga vajaliku videoühenduse.

[87] Karistusseadustik - RT I, 13.03.2019, 77.

Järgnev protsess toimub kõik menetleja juhtimisel, mille tulemusel kannab ta vastavatesse lahtritesse ütlusi andva isiku andmed, tutvustab talle õigusi ning palub need fikseerida ütlusi andva isiku digiallkirjaga samas keskkonnas. Edasi järgneb juba klassikaline ütluste andmise ja uurija poolt nende protokollimise faas, mille lõppemise järel tutvustab menetleja vastaspoolele protokolli ja palub selle kohta esitada märkused. Ülekuulamise protokolli kinnitavad lõpus kõik toimingus osalenud isikud. Vastav süsteem tagaks kiire ja mugava ütluste andmise võimaluse distantsilt ning digiallkirja kasutamine võimaldab asendada tavapärase käekirjalise allkirja andmist. Samuti peaks olema võimalik sama süsteemi vahendusel sarnaselt videokonverentsile liita menetlustoimingusse tõlk, kaitsjaid või teisi asjakohaseid osapooli. Tulevikus võib kaaluda ka kaugülekuulamise automaatse salvestamise rakendamist, kuid kirjeldatud süsteemi toimekindluse tagamise puhul ei saa seda pidada vajalikuks. Samuti eeldab salvestiste talletamine oluliselt suuremat tehnilist võimekust ja andmemahtusid, mis võrdluses välja pakutud süsteemi rakendamisega osutuksid tõenäoliselt kulukamaks.

Lugeja võib väita, et ka täna arvutis trükitavat ülekuulamise protokolli on samuti võimalik digiallkirjastada ning vajalik ei ole selleks eraldi funktsionaalsusega keskkonna loomine. M. Hirvoja on enda KrMS revisjoni analüüsis mh välja toonud ühe probleemina keerukuse dokumendi osade (nt õiguste tutvustamine) eraldi digiallkirjastamiseks. Hirvoja pakub välja alternatiivsed lahendused, milleks on kogu protokolli allkirjastamine ühe allkirjaga, võtta allkiri eraldi dokumendile või üleüldse loobuda selliste protokollide puhul digiallkirjastamisest ning liikuda taas paberdokumendile.[88] Töö autor ei saa selliste lahendustega kindlasti nõustuda, sest eraldi dokumendile allkirja võtmine tekitab kokkuhoiu asemel hoopis täiendada kohustuse ning teised kaks pakutud varianti ei täida allkirja võtmise eemärki üldse. Käesoleva töö autori poolt välja pakutud eraldi funktsionaalsusega süsteem aga lahendaks tekkiva kitsaskoha ning allkirjastada oleks sellega võimalik ka eraldi protokolli osasid.

Täiendava, kuid vähem analüüsi vajavaks võimalikuks digitaliseerimise elemendiks ülekuulamise juures on muuta elektroonseks ülekuulamise protokolli koostamine. Täna trükitakse uurimistoimingu protokoll valmis arvuti tekstitöötlusprogrammis ning seejärel prinditakse see välja ning allkirjastatakse toimingus osalenud isiku poolt käsitsi. Kui liikuda tulevikus täisdigitaalsele toimikule, oleks vajalik ka vastava toimingu muutmine paberivabaks. Jättes hetkeks kõrvale distantsilt ülekuulamised, vaatleme siinkohal uurimisasutuses menetleja ja ülekuulatava vahetul kokkupuutel toimuvat ülekuulamist. Hetkel prinditakse protokoll välja

[88] M. Hirvoja. Kriminaalmenetluse revisjoni analüüs - üleminek täisdigitaliseeritud kriminaalmenetlusel - 31.05.2016, lk 40.

ainult selle allkirjastamiseks ning pabertoimikusse lisamiseks. Seega, oleks siinkohal vajalik luua toimiv infosüsteem, kuhu kanda sisse kogu toimingu andmed selle algusest kuni lõpuni. Samuti peaks olema võimalik läbi mugava digiallkirjastamise ülekuulatava poolt kinnitada talle õiguste ja kohustuste tutvustamist ning lõppfaasis ütluste õigsust. Hetkel politseis kasutusel olev menetluse infosüsteemis on sarnane funktsionaalsus loodud, kuid seda ilma digiallkirjastamise võimaluseta. Peamiseks probleemiks, miks vastavat võimalust tänases süsteemis aga ei kasutata, on selle toimekindluse puudumine. Samuti ei ole võimalik sealses süsteemis kasutada videosilla võimalust. Ka tulevikus võimalikul loodaval e-teenusel tuleks pöörata suurt tähelepanu selle süsteemiarhitektuurile, sest ei ole mõeldav, et pika ülekuulamise lõpus protokollitud ütlused näiteks võrguteenuse kadumise tõttu ei talletu ning kogu protsessi tuleks kordama hakata. Täiendava võimalusena võiks tulevikus jõuda ka automatiseeritud süsteemini, mis suudab suusõnaliselt antud ütlused transkribeerida arvutis tekstiks. Sarnaseid süsteeme on levinumates keeltes arendatud, kuid eesti keele puhul ollakse sellega alles algjärgus. Vastava süsteemi kasutusele võtmise puhul peaks ka tulevikus säilima võimalus menetlejal koostöös ülekuulatavaga kõrvaldada protokollist asjasse mittepuutuvad osad, mille esinemine ütluste vaba jutustuse puhul on väga tõenäoline.

Urmas Krüger on enda kriminaalmenetluse õppematerjalis leidnud, et „kriminaalmenetluse ajalise ökonoomsuse seisukohast tuleks viia sisse vastav KrMS muudatus, mis võimaldaks ütlusi saada ainuüksi salvestatavate ülekuulamiste teel.“[89] Täielikult video- või helisalvestatud ülekuulamistele üleminekut ei saa käesoleva töö autori seisukohast pidada hetkel mõistlikuks. Peamiseks põhjuseks on antud salvestiste puhul hilisemas võistlevas menetluses problemaatiline viitamine või relevantse osa leidmine. Kui ka digitaalsete ütluste protokollide puhul on mahukast tekstist võimalik leida soovitud osasid küllaltki kiirelt ning samuti neid tulevikus leidmiseks märgistada, siis video- ja helifailide puhul see niivõrd lihtne ei ole. Teise võimaliku probleemina saab välja tuua ütlusi andva isiku kõne selguse ja intonatsiooni. Kui näiteks ülekuulamisel osalevale menetlejale on ütlused üheselt mõistetavad, siis hiljem salvestist kuulates ei pruugi prokurör või kohtunik halva kõnekvaliteedi tõttu seda enam üheselt mõista. Ülekuulamise protokolli puhul võiks leida teatava sarnasuse vaatlusprotokolliga. Menetleja ütluste sõnastamisel ja kirjutamisel justkui vaatleb ütluste andja jutustust ning selle tulemusel koostab protokolli. Ülekuulatava kinnitus protokolli õigusele annab justkui nõusoleku, et trükitud laused vastavad sellele, mida väljendada sooviti. Kui isiku kõne aga ei ole salvestisel selge, siis võib tekkida olukordi, kus erinevad inimesed kuulevad erinevaid asju.

[89] U. Krüger. Ülekuulamine kohtueelses menetluses, Õiguslikud aspektid. Tallinn: Sisekaitseakadeemia 2008, lk 84.

Seega satub kahtluse alla tõendamiseseme väärtus ning ütlusi ei saa tõlgendada üheselt. Ülekuulamiste heli- ja videosalvestamist saab pidada küll menetlust abistavaks, kuid seda iseseisvat tõendiväärtust omamata. Pigem tuleks seda käsitleda kui protokolli lisa.

3.3.3. Vastastamine

Vastastamine on uurimistoiming, mille eesmärgiks on lisaks uute ütluste saamisele selgitada kahe eelnevalt ülekuulatu isiku ütlustes esinenud vastuolude põhjused ning võimalusel need kõrvaldada.[90] Isikuid võib KrMS § 77 lg 1 kohaselt vastastada, kui on ilmnenud vastuolud eelnevates ütlustes ning neid ei ole võimalik teisel viisil kõrvaldada. Vastastamine on küll kohtueelse menetluse praktikas vähekasutatav toiming, kuid hoolimata sellest tuleks kaaluda ka selle uurimistoimingu rakendamise võimalikkust kaasaegsete kommunikatsioonide vahendusel.

KrMS § 77 lg 6 näeb menetleja võimalusena tehnilise lahenduse abil korraldada vastastamisest osavõtu, mis vastab samas seaduses sätestatud kaugülekuulamise nõuetele. Siinkohal on seadusandja loonud vastastamise puhul analoogia kaugülekuulamisega, mis võib aga vastastamise tegelikku eesmärki ja toimingus kasutatavaid menetlustaktikaid kasutades olla ennatlik. Vastastamise näol on tegemist menetlustoiminguga, mille taktikaline rõhk on läbi tõeseid ütlusi andnud poole mõjutada valeütlusi andnud isikut tõtt rääkima. Selleks on väga oluline isikute vahetu osalemine uurimistoimingul. Ühe osapoole osalemisel vastastamisel tehnilise lahenduse abil, võib eeldada, et isik tunneb ennast distantsil viibides oluliselt kindlamalt ning toimingu teostamine vastastatavate viibimiseta samas ruumis ei oma tulemust. Kuna toimingu keskmes peaks olema valeütlusi andnud isiku kallutamine oma ütluste muutmisele, siis oleks võimalik distantsilt kaasata ainult tõeseid ütlusi andnud osapool. Selline poolte valimine saaks tuleneda ainult menetleja subjektiivsest poolte valimisest ning õiglase menetluse printsiipi jälgides ei ole aktsepteeritav. Kõne alla võiks tulla meetme kasutamine ainult vajadusel isikut kaitsta vastaspoole eest. Sellisel juhul tuleks aga taaskord kaaluda, kas vastastamine on üldse sobiv meede ning distantsil viibiv isik ei ole hirmutatav näiteks ainuüksi vastaspoole mõjuvõimust.

[90] H. Lindmäe. Menetlustaktika I. Tartu: Juura 1995, lk 63.

Tulenevalt kirjeldatud asjaoludest ning argumentidest ei saa pidada tehniliste vahendite vahendusel vastastamist mõistlikuks. Ainsa digitaalse elemendina toimingus oleks vastastamise video- või helisalvestamine ning protokolli koostamine selleks loodud elektroonilises keskkonnas sarnaselt ülekuulamise juures käsitletule.

3.3.4. Ütluste seostamine olustikuga

Ütluste seostamisel olustikuga laseb uurija selgitada ja täpsustada eelnevalt ülekuulamisel osalenud kahtlustataval, tunnistajal või kannatanul kuriteosündmust puudutavaid asjaolusid teo toimepanemise kohas, sealjuures seostada ülekuulamise käigus antud ütlused sündmuskoha olustikuga. Ütlustest lähtudes uuritakse kohapealset olustikku, kogumaks tõendamiseks vajalikke vaatlusandmeid, avastamaks ja talletamaks kuriteojälgi ja võtmaks ära kriminaalasjas asitõendina kasutada võivaid esemeid.[91] Antud toiming leiab reeglina aset väljaspool uurimisasutuse ruume ning on suunatud ütluste andmisele toime pandud kuriteo keskkonnas. Ütluste seostamist olustikuga eristab ülekuulamisest peamiselt ainult selle toimumise asukoht. Seega digitaalsete võtete rakendamisel tuleks tegutseda analoogiliselt ülekuulamise alapeatükis käsitletuga. Küll aga on olulisem pöörata tähelepanu protsessi videosalvestamisele, mis võimaldab vahetumalt hinnata kuriteosündmusega seotud isiku ütluseid seonduvalt kohapealse olustikuga. Tõenäoliselt on väga raske ainult kirjalikult fikseerida kogu toimingu käiku selliselt, et välja oleks toodud piisava põhjalikkusega kogu toimingu käik ning selle tulemusel ilmnenud olulised detailid. Kui eelnevalt töö autor leidis, et audio- ja videosalvestistesse tuleks suhtuda reservatsiooniga ning pigem on tegemist abistatava meetmega, siis ütluste seostamisel olustikuga tuleks läheneda sellele teisest küljest. Väga oluline on tajuda võimalikult vahetult toimingu subjekti käitumist, selgitusi, ütlusi ning osundamisi, viitamisi, et eesmärgipäraselt tekitada seos isiku ning toimunud kuriteosündmuse vahel. Kuna kohapealse olustiku ning toimingus osaleva subjekti suhestumist on raske edasi anda lühikeste ja konkreetsete kirjalike protokolli osadega, siis tuleks eelistada toimingu videosalvestamist. Salvestisele tõendiväärtuse omistamiseks ning parema jälgitavuse tagamiseks tuleks menetlejal koostada siusliselt videosalvestise vaatlusprotokoll, milles osundatakse menetluse seisukohast olulistele nüanssidele. Protokolli koostamine peaks toimuma mitte sündmuskohal, vaid hiljem menetleja töökohas ning seda loodava e-toimiku liidese kaudu sarnaselt eelnevalt käsitletud

[91] H. Lindmäe. Menetlustaktika I. Tartu: Juura 1995, lk 69.

uurimistoimingutele. Protokolli lahutamatuks osaks peaks aga olema relevantsetele osadele asjakohaste videolõikude lisamine või vähemalt nende kestvuse märgistamine originaalvideos (digitaalsed markerid, hüperlingid). Tänases ütluste olustikuga seostamise puhul pannakse suurt rõhku fotografeerimisele, kuid ilma sellele eelneva helista ei oma see tegelikult tugevat tõendiväärtust. Näiteks sündmuskohale tee juhatamise puhul palutakse tihtipeale selgesti eristuvatel teekonnapunktidel osundada kahtlustataval sündmuskoha poole ning sellest teeb menetleja lihtsalt foto. Hilisemalt võib kahtlustatav aga seada osundamise eesmärgi kahtluse alla või sootuks viidata uurijate käsule osutatud suunas näidata. Kestva videosalvestise puhul on selgesti jälgitav nii hetkele eelnev kui ka järgnev ning hilisemad vastuargumendid ei ole kaalukad.

M. Hirvoja leiab enda KrMS revisjoni analüüsis sarnaselt töö autorile, et kogu audiovisuaalne materjal tuleb lisada ja salvestada digitoimikusse, millega on võimalik sealt koos koostatud toiminguprotokolliga koheselt tutvuda.[92]

Kirjeldatu rakendamiseks on vajalik luua politsei menetluse infosüsteemi või otse e-toimikuga liidestuv protokollimise e-teenus, mille juurde on lihtsasti võimalik lisada ja seostada videojäädvustusi ning vajadusel ka teisi andmetalletusi. Sisuliselt võikski tegemist olla juba nö digitoimiku teenusega. See ühtlustaks ning seeläbi ka lihtsustaks menetlejate meetodeid ja viise, mida rakendatakse toimingute protokollimisel, mille lahutamatuks osaks on ka heli- või videosalvestis.

3.3.5. Äratundmiseks esitamine

Äratundmiseks esitamise näol on tegemist uurimistoiminguga, mille käigus eelnevalt ütlusi andnud kahtlustatav, kannatanu või tunnistaja võrdleb mälu järgi talle esitatud objekti tunnuseid tema poolt eelnevalt kuriteosündmusega seoses tajutud objektiga ning selle tulemusel jõuab järeldusele objekti samasuses, sarnasuses või erinevuses.[93] Toimingu läbiviimine eeldab eelnevate ütluste andmist isiku poolt ning seda sama sündmuse kohta. Antud ütlused peavad võimalikult detailselt kirjeldama ka äratundmiseks esitatavat objekti, et seda hiljem võrrelda objekti endaga. Oluline on ütlustega tuvastada nii sündmuse objektiivsed kui ka subjektiivsed

[92] M. Hirvoja. Kriminaalmenetluse revisjoni analüüs - üleminek täisdigitaliseeritud kriminaalmenetlusel - 31.05.2016, lk 4.
[93] H. Lindmäe. Menetlustaktika I. Tartu: Juura 1995, lk 88.

tingimused.[94] Äratundmiseks esitatakse kõige tihedamini erinevaid isikuid, kuid sama toimingut saab rakendada ka teiste objektide puhul, nagu näiteks laiba, paikkonna, hoone, foto- või videosalvestise ning mistahes muu tajutava objekti puhul. Teoreetiliselt on võimalik äratundmiseks esitada pea kõik objektid ka digitaalselt. Ainsaks eelduseks on nende tajutavuse ülekandumine ka läbi elektroonse talletus- ning esitlusviisi. Tulles tagasi praktikas kõige levinuma olukorra juurde, kus isikule esitatakse äratundmiseks kolme sarnase isiku fotod, kellest üks on kuriteosündmusega seotud isik. Ei ole mingisugust vahet, kas äratundja vaatab fotosid paberil või arvutiekraanilt. Olgugi, et tajumine peaks toimuma äratundmist soodustavates tingimustes, siis oluline on jälgida ka toimingu optimaalsust sellega saavutatava tõendiväärtuse suhtes. Otstarbekas ei ole iga äratundmise puhul otsida füüsilisi isikuid, keda kõrvutada äratuntava isikuga uurimisasutuse ruumides. Samuti ei ole tihti mõistlik laipade tuvastamisel viia lähedasi surnukuuri, vaid sama eesmärgi saab saavutada foto esitamisega. Kuna vastava menetlustoimingu puhul on vajalik esitada ka objektiga mistahes sarnased võrdlusobjektid, siis on seda tihtipeale lihtsam teha taasesitamist võimaldavas vormis talletatud uurimisasutuse nn reservi abil. Siit edasi liikudes oleks tulevikus menetlejatel väga hea leida võrdlusobjekte selleks spetsiaalselt loodud baasist. Veel enam, kui see baas suudaks ise tunnuste analüüsimise põhjal pakkuda toimingus kasutatavaid võrdlusobjekte. Enne mainitud baasi loomist ning sinna piisava võrdlusmaterjali kogunemist, tuleks aga esmalt pöörata tähelepanu interaktiivsete võimaluste vahendusel äratundmiseks esitamise rakendamisele. Loodav süsteem peab võimaldama uurimisasutuse töötajal ette valmistada äratundmiseks esitatavad objektid ning need eelnevalt süsteemi üles laadida, seejärel peab olema võimalik jälgida ja pidevalt juhendada menetlustoimingus osalevat isikut (heli- ja videoühendus). Toimingu läbiviimise käigus peab menetleja lähtudes kehtivast menetlusseadustikust paluma kirjeldada ära tuntud objekti tunnuseid ning selle seost käsitletava kuriteosündmusega. Kogu toimingu käik tuleb protokollida ning seejärel poolte poolt digiallkirjastada.

Sarnaselt kaugülekuulamise temaatika juures käsitletule, tuleks enne toimingu juurde asumist esmalt menetlejal kaaluda toiminguga kaasneda võivaid võimalikke riske. Kuna äratundmiseks esitamine on oma olemuselt suunatud toimingus osaleva isiku subjektiivsele tajule, siis võib objektiivsele tulemusele jõudmise ära rikkuda isikuga koos arvuti taga viibivad kõrvalised isikud. Kui isikule on esitatud näiteks avaliku e-toimiku kaudu isikute fotod ning neid vaatab ning oma arvamuse avaldab väljaspool uurimisasutust temaga koos viibiv kõrvaline osapool. Sellise olukorra tulemusel võib saada isiku otsustus mõjutatud ning ei pruugi olla enam

[94] *Ibid*, lk 90.

adekvaatne. Niivõrd piiripealsete olukordade esinemist tuleks pigem pidada harvadeks ning toimingu digitaliseerimine annaks kokkuvõttes olulise mastaabisäästu. Paralleelselt tuleb aga jätta võimalus ning seda ka menetlustoimingus osalejale rõhutada, et olukorras, kus teda mõjutati videosilla kaardi tagant enda ütlusi muutma, siis tuleb sellest esimesel võimalusel teavitada menetlejat ning kordutoiming peaks aset leidma juba uurimisasutuse ruumides. Võimalusel tuleks kaaluda vastava äratundmiseks esitamise võimekuse loomist e-toimiku süsteemi.

3.3.6. Vaatlus

Vaatluse eesmärgi sätestab KrMS § 83 lg 1, mille kohaselt kogutakse antud toimingu käigus kriminaalasja lahendamiseks vajalikke andmeid, avastatakse kuriteojälgi või võetakse ära asitõendina kasutada võivaid objekte. KrMS § 83 lg 2 kohaselt võivad vaatlusalusteks objektideks olla sündmuskoht, laip, dokument või muu objekt ja asitõend ning läbivaatuse toimetamise korral isik ning posti- või telegraafisaadetis. Vaatlusel on praktikas kaks peamist ülesannet, millest esimese on muuta objekti vaatlusega tekkinud tõendi jõudmine kriminaalasja juurde vaadeldavaks. Teine oluline ülesanne on tõenduseseme asjaolude fikseerimine, millega tagatakse tõendi säilimine pika perioodi vältel ka pärast kuriteosündmuse toimumist.[95]

Vaatluse, kui ühe uurimistoimingu digitaliseerimise juures on võimalik suurim ressursikokkuhoid saavutada selle protokollimise arvelt. Vaatluse protokollimist tuleks ka tulevikus pidada selle lahutamatuks osaks. Peamine erinevus tänase protokollimise juures peaks tulevikus seisnema selle elektroonsuses ning seeläbi paremas protokolli moodustamises. Vaatluse sisu võib näha justkui tandemit, kus esmalt esitatakse vaadeldav objekt ning sellele järgneb kirjeldav osa, mis pöörab tähelepanu tõendamise seisukohast olulistele detailidele. Kuna vaatlusalused objektid võivad teineteisest oma olemuselt tugevalt erineda, siis peaks loodav süsteem olema küllaltki paindlik erinevate vaadeldavate osade liitmises protokolliga. Sinna peab olema võimalik lisada dokumente, fotosid, videosalvestisi jms. Tänases praktikas lisataksegi vaatlusprotokollile eranditult fotosid. Loomulikult võib protokolli lisade hulka arvata ka muul kujul objekte, kuid levinud on olukord, kus isegi dokumente või videosalvestisi vaadeldakse läbi nende fotografeerimise või ekraanikuvade.

[95] 13. E. Kergandberg, P. Pikamäe. Kriminaalmenetluse seadustiku kommenteeritud väljaanne, Juura 2012, §83 kom 2.2 ja 2.6.

Seega võiks tänaseid vaatluseid nimetada elektroonsuse mõistes hübriidseteks, kus kasutatakse digitaalsuse võimalusi objektide jäädvustamiseks ning klassikalist protokolli, kus kirjeldatakse nähtut ning seejärel prinditakse see välja.

KrMS § 149 lg 3 kohaselt tuleb menetlustoimingu protokollis või selle lisas kasutatav digifoto fail säilitada ka e-toimiku süsteemis. Paraku seda nõuet praktikas ei järgita ning foto säilitamisel on lähtutud uurija subjektiivsest arvamusest. Seni on digifoto kõigest välja prinditud ning lisatud pabertoimikusse. Hea juhul on uurija lisanud fotofaili ka protokolli lisaks olevale andmekandjale, kuid selline tegevusviis on vähetõenäoline.

On palju spekuleeritud küsimuse üle, miks on vaja näiteks turvasalvestise videos nähtav kirjutada lahti paberil. Käesoleva töö autor leiab, et vähemalt esialgu on väga keeruline muuta näiteks poevargust kajastav videofail nn täisdigitaalseks tõendiks, kaotades selle kõrvalt videovaatluse protokoll. Kui tõendi eesmärgiks on tõestada süüteo toimepanemise fakti, siis see peab olema kõigile menetlusosalistele ning menetlejatele ka selgesti jälgitav. Kui vaatlusprotokolli koostamisega antakse selge viide ja kirjeldus nii toime pandud teole, isikule, ajale ning kohale, siis paljas videopilt ei pruugi seda iseseisvalt teha. Samuti puuduvad uurimisasutuse töötajatel täna nii tehnilised vahendid kui ka oskused, et videopilti ajakohasemaks lõigata ning seal näiteks arusaadavalt tähistada teo toime pannud isik. Ei ole ju mõeldav, et hilisemal kohtuistungil vaadeldakse videosalvestist, kus ainuüksi prokuröri suusõnaliste kirjelduste pinnalt selekteeritakse välja kahtlusalune ning seda suurema rahvahulga sees. Seega on veidikene rutakalt liigutud kriminaalmenetluses vaatluste asendamisega videote vastu. Täna küll rakendatakse seda peamiselt ainult kokkuleppemenetluste puhul ning üldmenetlusse minnes nõuab lähtuvalt kokkuleppest menetlejatega prokuratuur ikkagi täieliku vaatluse teostamist. Loomulikult ei ole mõistlik multifilmile sarnaselt kopeerida lugematuid video ekraanitõmmiseid vaatlusprotokolli, kuid protokoll peaks piisavalt lühidalt, aga samas konkreetselt edasi andma kirjelduse, kellele ja mis ajahetkel tuleks videot vaadates tähelepanu pöörata. Küll muudaks selle lihtsamaks kaasaegne elektrooniline vaatlusprotokolli koostamise süsteem, kus on paralleelselt võimalik lisada asjakohaseid fotosid ning neile kõrvutada nähtava kirjeldused. Veelgi parem oleks, kui süsteem võimaldaks menetleja poolt välja toodud kirjeldused siduda näiteks protokolli lisaks olevas originaalvideos konkreetsete ajahetkedega. See tõstaks ühelt poolt vaatluse tõendiväärtust ning teisest küljest muudaks asjakohaste tõendite leidmise lihtsaks ja kontrollitavaks. Samuti võimaldaks selline süsteem tõendina hinnata eraldi nii vaatlusprotokolli kui vaadeldavat objekti.

Kui ilmneb mingi vastuolu protokollis ja sellele lisatud salvestises kajastatu vahel, siis lähtudes KrMS § 63 lg 1 sätestatust on hilisemas kohtumenetluses kohus õigustatud käsitama iseseisvate tõenditena nii protokolli kui sellele lisatud salvestist ja hindama neid kahte enda siseveendumusest lähtuvalt.[96]

3.3.7. Uurimiseksperiment ja läbiotsimine

Tõendamisel tähtsaks asjaoluks kujuneda võiva, toimingu esinemise või tajumise võimalikkuse välja selgitamiseks on menetlejal võimalik läbi viia uurimiseksperiment. Antud toiming peab toimuma kuriteosündmusele võimalikult sarnastes tingimustes.[97] Sisuliselt on tegemist katsete läbiviimisega, mille käigus proovitakse jäljendada võimalikult täpselt kuriteosündmuse toimumise ajal ja kohas eksisteerinud olustikku. Seda tehakse eesmärgiga tuvastada toimingu või sündmuse võimalikkus või mingi objekti tajumise võimalikkus.[98] Mingi kindla hüpoteesi tuvastamiseks läbi viidav eksperiment tuleb KrMS § 94 lg 1 kohaselt fikseerida uurimiseksperimendi protokollis, kuhu märgitakse kogu hüpotees, katse toimumise olustiku ja protsessi kirjeldus ning katse tulemused.

Läbiotsimise eesmärgiks on KrMS § 91 lg 1 alusel kriminaalasja lahendamiseks leida vajalik dokument, asi või isik või kriminaalmenetluses arestitav vara või laip. Lisaks on selle eesmärgiks tabada võimalusel tagaotsitav. Läbiotsimise saab läbi viia hoones, ruumis, sõidukis või piirdega alal. Sarnaselt uurimiseksperimendile on oluline läbiotsimise puhul fikseerida uurimistoimingu eesmärk, olustiku ja protsessi kirjeldus ning tulemus. Seega on mõlema menetlustoimingu puhul mõistlik algusest lõpuni kogu protsess jäädvustada ning sellele tuginedes hiljem protokollida. Siinkohal võib paralleeli tuua ütluste seostamisega olustikuga ning osaliselt videovaatlusega, kus töö autor soovitab samuti videojäädvustada kogu protsess (videovaatluse puhul olemasolev salvestis), mille tulemusel oleks võimalik loodetavasti loodavas interaktiivses keskkonnas seostada menetleja kommentaarid koheselt salvestisega. Salvestis muutub protokolli lisaks ning protokoll annab uurimiseksperimendile eraldi kirjeldava tõendiväärtuse.

[96] RKKK 07.05.2009, 3-1-1-21-09, p 9.1.
[97] H. Lindmäe. Menetlustaktika I. Tartu: Juura 1995, lk 142.
[98] E. Kergandberg, P. Pikamäe. Kriminaalmenetluse seadustiku kommenteeritud väljaanne, Juura 2012, § 93 p 1.

3.4. Digitaalne kriminaaltoimik

Kohati on mõistetamatu, miks justiitsministeerium ning suurim kriminaalmenetluse kohtueelset menetlust läbiviiv organisatsioon Politsei- ja Piirivalveameti näol ei ole suutnud jõuda tegeliku menetluse optimeerimiseni läbi pabertoimiku täieliku kaotamise. Üheks põhjuseks on kindlasti vastuolu kehtiva õigusega, mis aga ei ole kindlasti ületamatu ning eeldab kõigest mõningate rakendusaktide muutmist.. Nagu eelpool juba mainitud, siis kriminaalmenetluse seadustiku § 160^1 lg 4 on vastava võimaluse juba loonud. Hetkel sätestab konkreetselt kriminaaltoimiku vormi kohtueelses menetluses ainuüksi Justiitsministri määrus, mille kohaldamine elektroonse menetluse tarvis ei ole kindlasti keeruline. Pigem saab uuele süsteemile ülemineku peamiseks teguriks pidada inimest, eelkõige neid, kes igapäevaselt peavad hakkama digitoimikuid koostama ning nendesse kogutud tõendeid lisama.

Täisdigitaalsele kriminaaltoimikule üleminek toob endaga kaasa pigem positiivse tulemi, mis aitab saavutada menetluse optimeerimise läbi selle tõhususe kasvu ning vähendades seniseid kulutusi ajale ning rahale. Üheks suureks plussiks saab pidada elektroonse toimiku kasutusele võtmisel uurimisasutuse, prokuratuuri ja kohtu samaaegse töö võimaldamist. Eriti oluline on menetlusprotsesside puhul, mis on piiritletud lühikese ajaraamiga. Näiteks annab selline võimalus märgatava edu olukorras, kus prokurör soovib esitada kohtule isiku vahistamistaotluse ning ta peab seda tegema 48 tunni jooksul alates isiku kahtlustatavana kinnipidamisest. Kui menetleja jõuab jooksvalt vastavasse menetlussüsteemi kas üles laadida või ideaalis samas keskkonnas koostada uue menetlustoimingu protokolli, siis saab prokurör seda kasutades juba vahistamistaotlust ette valmistama hakata. Samuti annaks loodav süsteem eelise näiteks kiireloomuliste läbiotsimiste puhul, kui prokuröril ning eeluurimiskohtunikul on lihtsam kujundada läbiotsimismääruse väljastamiseks oma seisukoht. Seisukoha kujundamiseks annab aga aluse kogutud informatsioon või tõendid, mille edastamine elektroonse süsteemi vahendamisel oleks kindlasti mobiilsem. Jättes kõrvale aga kiireloomulised toimingud kriminaalmenetluses, siis oluline kasutegur ilmneb ka tavalises tempos kulgevate kriminaalasjade puhul. KrMS § 213 lg 1 kohaselt on prokuratuuri ülesandeks juhtida kohtueelset menetlust, samaaegselt tagades selle seaduslikkuse ja tulemuslikkuse. Selleks, et uurija tehtud tööd paremini hinnata ning kohtueelset menetlust ka reaalselt juhtida, on vajalik pidevalt kriminaalasja käiguga kursis olla.

Kuna ühes kriminaalasjas on ka üks pabertoimik, siis tekitab tihtipeale selle liigutamine menetlusasutuste vahel tööseisakuid. Kui toimik on prokuratuuris, et prokurör saaks planeerida edasist menetluskäiku, siis häiritud või suisa takistatud on uurija paralleelne töö sama kriminaalasjaga ning kui toimik on uurija käes, siis ei ole jälle prokuröril ilmselgelt võimalik sellega tutvuda.

Lisaks uurimisasutuse, prokuratuuri ja kohtu aja kokkuhoiule on võimalik saavutada märkimisväärne võit ka kaitsjal ning seeläbi süüdistataval/kahtlustataval. KrMS § 34^1 lg 1 kohaselt on kahtlustataval õigus taotleda juurdepääsu tõenditele, mis on olulised tema vastu esitatud kahtlustuse sisu täpsustamiseks, kui see on vajalik õiglase menetluse ja kaitse ettevalmistamise tagamiseks. Kogutud tõenditele tuleb juurdepääs tagada hiljemalt pärast seda, kui kohtueelne menetlus on prokuratuuri poolt lõpuleviiduks tunnistanud ja kriminaaltoimik on kahtlustatavale ja tema kaitsjale esitanud tutvumiseks KrMS § 224 järgi. Lisaks on sama paragrahvi lõike 2 kohaselt kahtlustataval õigus taotleda juurdepääsu tõenditele, mis on olulised vahistamistaotluse põhjendatuse arutamiseks ning kinnipidamise ja vahistamise vaidlustamiseks kohtus. KrMS § 35 lg 2 kohaselt on süüdistataval kaitsja vahendusel õigus tutvuda kriminaaltoimikuga ja võtta osa kohtulikust arutamisest. Kõikide eelpool kirjeldatud õiguste tagamiseks on võimalik prokuratuuri vastava otsuse tulemusel täisdigitaalses toimikus anda näiteks läbi E-toimiku kaitsjale ligipääs relevantsetele dokumentidele või toimikule tervikuna.

Vastav eelis tõstatub kindlasti ka kiirmenetluse puhul, kus kaitsjal on pärast kahtlustatava ülekuulamist kuni kohtuistungi alguseni õigus tutvuda kõigi kriminaalasja materjalidega. Taotluste ja kaebuste esitamine ja lahendamine toimub prokuratuuris KrMS § §256^2 lg 6 alusel kuni kohtule kiirmenetluse taotluse esitamiseni, mis peab toimuma 48 tunni jooksul alates isiku kahtlustatavana ülekuulamisest või isiku kahtlustatavana kinnipidamisest. Niivõrd lühikese aja jooksul on kaitsjale iga tund oluline. Reeglina saavad kaitsjad tulenevalt kaitsealuse soovist või riigi õigusabi taotlusest tulenevalt endale kriminaalmenetluse osalise rolli ootamatult. Seega on eesmärgipärase kaitse saavutamiseks vajalik ajaline faktor ülimalt tähtis ning läbi e-toimiku materjalidega tutvumise võimaldamine oleks seda igati toetav. Samuti peaks olema kaitsjal võimalus tulenevalt kehtivast õigusest tulevikus ka läbi avaliku e-toimiku esitada soovi korral taotlusi ja kaebusi kriminaalasjas. E-teenuse kasutamine mitte ainult ei lihtsustaks ilma füüsilise kohaloluta materjalidega tutvuda ja kaitset ette valmistada, vaid ka konkretiseeriks menetluslike võimaluste järjekorda.

Kuna kaitsja poolt taotluste ja kaebuste edastamine on võimalik kuni prokuratuuri poolt kiirmenetluse taotluse esitamiseni kohtule, siis vastava toimingu teostamisel peaks süsteem sellest automaatselt ka kaitsjat teavitama ning süsteemis fikseeritud taotluste esitamise ajahetk ei ole vaieldav.

Seega oleks mõistlik kohtueelses menetluses sarnaselt kohtumenetlusega kasutusele võtta täisdigitaalne kriminaalasja toimik. Ühelt poolt vähendab see tänast menetlejate topelttööd, pakub paremad võimalused samaaegseks tööks prokuratuurile ja uurimisasutusele ning lõppfaasis muudab paremini kättesaadav toimik tõhusamaks kaitsja töö kahtlustatava huvide esindamisel.

3.5. Menetluse digitaliseerimisega kaasnevad riskid

3.5.1. Kasutajate toimetulek süsteemi käsitlemisel

Eesti e-teenuste edulugu jälgides ei tohiks kõrvale jätta ka kogu digiriigi varjupooli. Järgnevalt tulevad vaatluse alla käesoleva töö autori seisukohast peamised riskid, mis võivad jääda vajaliku tähelepanuta liigselt kiire digitaliseerimismaaniaga kohtueelse menetluse raames.

Üheks täiendavaks ohuks ja kitsaskohaks on juba praeguseks kujunenud menetlusosaliste oskamatus tulla toime kriminaalmenetluses kasutusel olevate ning tulevikus arendatavate süsteemidega. Loodud tehnilistest võimalustest on kasu ainuüksi siis, kui selle kasutajatel on olemas vajalik oskus ja motivatsioon süsteemi kasutamiseks. Ehk teisisõnu jääb väga suur hulk menetlejaid ning teiselt poolt menetlusosalisi hätta infosüsteemide kasutamisega. See muudab vajalike teenuste kasutamise nende jaoks ebameeldivaks ning tekib veelgi tugevam barjäär. Kui menetlejapoolseid puudujääke saab parandada täiendavate koolituste ning panustamisega süsteemide kasutajamugavusse, siis menetlusosaliste puhul on isikute ring aga oluliselt suurem. Mõistlik oleks ka kaasata tänaseid praktikuid uute süsteemide arendamisse, mis aitaks saavutada kasutajasõbralikumad süsteemid ning sujuvama ülemineku nendele. Kuna infotehnoloogid ja programmeerijad ei oma otsest kokkupuudet kriminaalmenetlusega, siis on hädavajalik vähemalt neile lähteülesande koostamise faasis kaasata sellesse praktikuid.

Näiteks kriminaalmenetluse revisjoni poolt välja pakutud 2022. aastaks täisdigitaalsele toimikule üleminekuni[99] on piisavalt aega, et lähtuvalt praktilisest kogemusest õppida vigadest ning vältida hilisemaid komplikatsioone süsteemide kasutuselevõtul.

Inimeste IT-tehnilised oskused ei tohiks kindlasti tekitada olukorda, kus menetlusosaliste õigused saavad seeläbi kannatada. Samas on töö autor seisukohal, et kohtueelse menetluse etapis on menetlusosaliste võimalused uurimistoiminguid mõjutada niigi minimaalsed ning menetluse võistlevus tuleb mängu alles pärast hetke kui prokuratuur loeb kohtueelse menetluse lõppenuks. Kindlasti vajab analüüsimist menetlusosalistele digitaalse menetluse tulemusel tekkida võivad takistused kohtueelse menetluse järgses etapis, kui kaitsjal on võimalik juba toimikuga tutvuda ning selle alusel koostada kaitseakt. Töö mahu piiratuse tõttu ei kuulu aga antud küsimus lähemalt analüüsimisele. Seega võib kokkuvõtlikult väita, et kohtueelses menetluses tuleb hoida uurimisasutuse töötajate tehnilist pädevust, et nad oleksid võimelised digitaalseid menetlustoiminuid ellu viima ning menetlusosaliste roll on pigem minimaalne.

Kaitsjad on omalt poolt tõstatanud probleemi, milles leiavad, et digitaalsele toimikule täielikult üle minnes ei pruugi olla vajalikud dokumendid enam niivõrd lihtsasti leitavad. Sellist väidet saab pidada aga pigem meelevaldseks, sest vastava kohandatud süsteemi loomisel muutub kindlasti kriminaaltoimikus orienteerumine pigem lihtsamaks ning seda tänu elektroonsele sisukorrale, hüperlinkidele ning digitaalsele otsinguvõimalusele. Loodavas süsteemis oleks mõistlik tekitada tehniline võimalus ka oluliste kohtade märgistamiseks, et need näiteks kohtuistungil või prokuratuuris kokkuleppe sõlmimisel kiiremini üles leida. Seega tulevikus soovitud dokumentide leidmine sõltub pigem loodava digitoimiku süsteemi moodulitest ja kasutajavõimalustest, mitte ei ole ammendatud ainuüksi oma elektroonsuse tõttu.

3.5.2. Süsteemide toimekindlus

Käesoleva töö kirjutamise käigus on selgunud ilmselged puudujäägid tarkvaralistes süsteemides ning tehnilises taristus. Ei ole võimalik liikuda täisdigitaalse kriminaalmenetluse suunas ilma, et tagataks uurimisasutuste kasutuses olevate infosüsteemide ja tehniliste vahendite laitmatu töötamine. Kuna elektroonsete toimingute talletamine saab toimuda eelkõige tehnika vahendusel ning digitaalsena, siis tuleb tagada kasutajasõbralike ja töökindlate

[99] Justiitsministeerium. KrMS revisjoni VTK kooskõlastamisel laekunud arvamused ja otsused revisjoni I etapi teemaderingi osas, p 1.1.

infosüsteemide toimimine. Süsteem saab olla kasutajasõbralik ja töökindel ainult juhul, kui ka nende lõpptarbija tuleb vastava koolituse läbimisel ja kerge vilumuse omandamisel toime selle kasutamisega. Vestluses PPA uurijatega ilmnes, et politsei menetlejate igapäevane digitaalne tööriist andmebaasi MIS näol on ülimalt hea näide süsteemist, mille puhul ei ole võimalik mitmeid loodud võimekusi kasutada. Samas on tegemist süsteemiga, mille vahendusel peaks toimuma peamine töö kriminaaltoimikuga, kus ideaalis on mh ette nähtud ka võimalus koostada lahtreid täites näiteks uurimistoimingute protokolle. Praktikas aga ei ole teada, et keegi menetlejatest seda ka reaalselt kasutaks, sest keegi ei soovi tehtud töö luhtumise riski võtta. MISi üheks suurimaks ohuks ongi just see, kui uurija täidab näiteks kahtlustatava ülekuulamise blanketil kõik vajalikud lahtrid ning jõuab paaritunnise ülekuulamise lõpuks toimingu protokolli salvestamiseni, kuid koostatud protokoll ei salvestugi tehnilise vea tõttu. Seega ei jääkski uurijal tagantjärgi muud üle, kui kogu toiming uuesti korrata. Selline käitumine aga ei oleks enam pelgalt menetlejat, vaid ka ütluste andjat ning näiteks ka kaitsjat koormav ja kogu kordusprotsess tekitaks juba ka otsese lisakulu riigile näiteks kaitsja tasu või uurija töötundide arvelt.

Infosüsteemide toimekindluse tagamiseks ei ole vajalik ainult süsteemi enda lakkamatu töö, vaid vajalik on ka tehniliste seadmete, võrguühenduse ning teenusepakkuja laitmatu toimimine. IT süsteemide ja sidevõrkude pidev arendamine viib meid edasi ühtlasi toimekindlamate sideteenusteni, kuid selle arengust oodatakse rohkem, kui see hetkel pakkuda suudab. Praktiliste näidate pinnalt on kerkinud esile probleem, et riiklikud sidesüsteemid on liigselt tsentraliseeritud.[100] Ei saa pidada normaalselt korduvalt ning reaalselt aset leidnud vahejuhtumeid, kus näiteks mõne eraettevõtte rikete näol on ajutiselt olnud halvatud näiteks kogu riigi sisejulgeoleku sideühendused. Sellist nõrkust saab ja tulebki pidada reaalseks siseriiklikuks julgeolekuohuks, mille vähendamiseks tuleb järjepidevalt tööd teha. Võib spekuleerida, et kohtueelses kriminaalmenetluses ei ole niivõrd määrav e-teenuste lühiajaliste katkestuste mõju, kuid selline spekulatsioon muudaks meid veelgi lühinägelikumaks. Tulles tagasi ajakriitiliste toimingute juurde, võib tuua jällegi näite vahistamisprotsessist. Olukorras näiteks, kus uurimisasutus on kinni pidanud ohtliku kurjategija, kelle puhul esineb kõrge tõenäosus, et isik paneb vabadusse pääsedes toime uue teo. Kokku on uurimisasutusel, prokuratuuril ja kohtul taaskord aega 48 tundi, et otsustada isiku vahistamine. Selle protsessi teises pooles aga lakkavad infosüsteemid töötamast ning prokurör ei jõua vajalikus mahus ette

[100] Siseministeeriumi pressiteade „Kriisikomisjon keskendus valitsusasutuste valmisolekule elutähtsa teenuse katkemisel“ – 15.06.2017. Arvutivõrgus: https://www.siseministeerium.ee/et/uudised/kriisikomisjon-keskendus-valitsusasutuste-valmisolekule-elutahtsa-teenuse-katkemisel (15.04.2019).

valmistada vahistamistaotlust ning kättesaadavad ei ole ka isiku vahistamist ajendavat eelnevat infot tema karistatuse kohta. Süüteo toime pannud isik tuleb seejärel tema õiguste tagamiseks vabastada ning kas uue teo toimepanemisel peaksime siis süüdistama infosüsteemi? Kirjeldatud näidete muutumist reaalseteks juhtumiteks saame ära hoida sellele eelnevalt mõeldes ning süsteemide toimekindlust järjepidevalt parandades. Kui kriminaalmenetlus jõuab täielikult digitaalse toimiku kasutamiseni, siis säilitada tuleks alternatiivsed võimalused ning ka menetlejate oskused neid teostada.

3.5.3. Digitaalsete menetlustoimingute sisu kaitse

Menetlustoimingute digitaalseks muutmine esitab kindlasti kriminaalmenetlust läbiviivatele ametnikele täiendava väljakutse menetluse sisu kaitsmise osas. Menetlustaktika ning uurimise edukas tagamine eeldab tihtipeale toimiku materjalidele piiratud ligipääsu ainult selleks vajadust omavatele isikutele. Seega ei tohiks ka uurimistoimingu materjalidega kokku puutuda isikud, kes ei ole ise selles osalenud. Sellest tulenevalt on seadusandja näinud ette ka konkreetsed piirangud kohtueelses menetluses uurimistoimingute protokollide koopiate ning tutvumise võimaluste osas. Kokkuvõtvalt võib väita, et need on menetlusosalistele küllalt piiratud ning mõeldud tagamaks eelkõige nende tõele vastavust. Näiteks ei ole võimalik saada kahtlustataval enda ülekuulamise ütluste osa kohta või äratundmiseks esitamise puhul esitatud objektide kohta koopiat. Kui aga rakendada tulevikus käesolevas töös käsitletud uurimistoiminguid digitaalsena, siis võib seniste põhimõtete tagamine probleemiks kujuneda. Näiteks on äratundmiseks esitamise juures oluline tagada võimalik maksimaalne kaitse eelkõige võrdlusobjektidena esitatud materjali osas. Tänapäeva infotehnoloogiliste võimaluste juures on küllaltki lihtne salvestada arvuti ekraanipilt või suisa jäädvustada kogu interaktiine tegevus arvutis koos heliga. Menetluse huvides ei ole kindlasti see, kui äratundmiseks esitamise käigus presenteeritud juhuslikud võrdlusobjektid jäädvustatakse toimingus osaleja poolt. Sellega kaasneks oht nende levimisele, mis ei ole kindlasti menetluses aktsepteeritav. Samuti ei ole menetluse seisukohast kuidagi kasulik, kui kahtlustatav või tunnistaja saab enda antud ütlused ekraanipildi abil salvestada ning nende abil edasist menetlust või kaitsetaktikat enne kohtueelse menetluse lõppu mõjutama hakata. Teisest küljest ei saa väita, et selline võimalus oleks omane ainuüksi digitaalsetele toimingutele. Kui menetleja viib läbi täna näiteks ülekuulamise uurimisasutuses, siis praktikas esineb samuti väga suur võimalus, et isikud saavad soovi korral salvestada näiteks antud ütlused nende taskus oleva diktofoni või mobiiltelefoniga.

Selliste olukordade vältimiseks digitaalsete toimingute puhul tuleb peamiselt pidada taaskord menetleja kaalutletud otsust, mis peaks enne toimingute teostamist elektrooniliselt, analüüsima ka siinkohal välja toodud ohukohti. Teiseks tuleb suurt tähelepanu pöörata süsteemide tehnilisele ettevalmistusele, et minimaliseerida menetluste torpedeerimist. Kolmandaks võimaluseks saab pidada ka toimingute läbiviimist käsitleva regulatsiooni muutmist selliselt, et tekkinud võimaluste pahatahtlik kasutamine oleks rangemalt karistatav, mille kasutamise juurde ei tohiks aga liialt rutata.

Kaugmeetodil tulevikus teostatavate uurimistoimingute puhul on hilisemaks tõendiväärtuse ning ümberlükatavuse kaitsmiseks võimalik kasutada kogu toimingu videosalvestamist. Kui toimingud viiakse läbi elektroonilisel teel ning näiteks kasutades e-toimiku keskkonda, siis salvestis peaks jäädvustama poolte heli ning ekraanipildid koos veebikaamerate piltidega. Salvestise saab elektroonilisse toimikusse lisada kui toiminguprotokolli lisa ning selle järelevaadatavus oleks võimalik kõigil, kes antud ajahetkel kriminaalasja toimikule juurdepääsu omavad. Loomulikult eeldaks salvestiste arhiveerimine olulist andmemahu võimekust, kuid selle teostatavus peaks jääma pigem infotehnoloogide pärusmaaks.

3.5.4. Menetluse turvalisus

Lisaks menetlusosalistest tulenevatele ohtudele tuleb tagada ka tehnilise poole turvalisus. Süsteemis ei tohi esineda pidevaid tõrkeid ja mis veelgi olulisem – tagatud peab olema andmete kindel varundamine. Tuues võrdluseks pabertoimikust näiteks uurimistoimingu protokolli kadumist, ei saa samuti kõne alla tulla sarnase dokumendi kadumine infosüsteemist.
E-toimiku süsteemi asutamine ja e-toimiku süsteemi pidamise põhimäärususe § 21 lg 1 sätestab E-toimiku kaitse, mille kohaselt kaitstakse andmete käideldavust, tagades andmete kättesaadavus.[101] E-toimikule on määratud kolmeastmelise etalonturbe süsteemi (ISKE) turvaklass K2T2S3, mis tähendab, et lubatud summaarne seisak nädalas on umbes 2 tundi (K2), info allikas, selle muutmise ja hävitamise fakt peavad olema tuvastatavad, vajalik on info õigsuse, täielikkuse ja ajakohasuse perioodiline kontroll ning baas sisaldab ülisalajast infot, mille kasutamine on lubatud ainult teatud kindlatele kasutajatele, juurdepääs teabele on lubatav juurdepääsu taotleva isiku õigustatud huvi korral.[102]

[101] E-toimiku põhimäärus - RT I, 09.03.2018, 5.
[102] Infosüsteemide turvameetmete süsteem. VVm 20.12.2007 nr 252 - RT I 2007, 71, 440.

Täiendavalt tuleks mõelda täisdigitaalsele kriminaalmenetlusele jõudes ka olukordadele, kui näites siseriiklikust kriisist lähtuvalt ei ole võimalik või on hoopis äärmiselt koormav elektroonsete võimaluste kasutamine menetluses. Meenutada võib kasvõi pronksiöö sündmusi Eestis, kui menetlusmahu kasvamise järel toimetasid lõppfaasis politseinikud, prokuratuur ja kohus kinnipidamisasutuse ruumides ning tegelesid kiirendatud meetoditel menetluste läbiviimisega. Kui aga kõik isikute karistatust või menetlusi puudutavad andmed ja materjalid koondada arvutivõrku või digitaalsetele andmekandjatele, siis kas sarnastes olukordades õigussüsteemi tagamine on enam võimalik? Kui kriisi olemus seisneb näiteks siseriiklike asutuste omavahelise võrguühenduse lakkamises, siis kuidas jõuavad menetluseks vajalikud andmed menetlejani? Näitek on probleemkohaks digitaalse karistusregister, mille puhul paberkandjal arhiiviandmeid enam ei säilitata. Korduvust eeldavate süütegude puhul ei ole sellisel juhul ju võimalik enam ei menetlejal, ega prokuratuuril määrata asjakohast kvalifikatsiooni. Selliseid olukordi aitaks vältida mõningate nn „offline“ töökohtade loomine piirkonda, mis vähemalt suudaks tagada esmase teadmisvajaduse menetluse läbiviimiseks. Mainitud töökohtade all peab silmas töö autor teatava sagedusega ning piiratud mahuressurssi vajavate andmete varundamisega füüsiliselt eri piirkonna keskustes asuvatesse masinatesse. Mis aga peamine, menetlejad ja ka ajaga kohanev õigus ei tohiks unustada vajadusest sõltuvat pabermenetlust, mida äärmuslikes olukordades kasutada.

3.6. Puutumuses olevad põhiõigused

Põhiõiguste kaitse Euroopas on üks tõhusaimaid maailmas, kuid samal ajal ka üks keerulisemaid. Samas geograafilises ruumis eksisteerib kolm normatiivset korda. Need on põhiseadusega loodud rahvuslik, Euroopa Nõukogu liikmete loodud rahvusvaheline ja Euroopa Liidu õiguskord. Nende süsteemide olulisemad põhiõiguste allikad on Eestis põhiseadus, Euroopa inimõiguste ja põhivabaduste kaitse konventsioon koos selle protokollidega ning Euroopa Liidu põhiõiguste harta. Kõik need kolm akti on ühtlasi ka kriminaalmenetlusega seotud põhiõiguste olulisemad allikad.[103]

[103] U.Lõhmus. Põhiõigused kriminaalmenetluses. Tallinn: Juura 2014, lk 19, 21.

Eestis praegu toimivat kriminaalmenetlust võib määratleda kui hübriidset ehk segasüsteemi, kus kohtueelsel uurimisel kehtib inkvisitsiooniline mudel ja kohtumenetluse etapis hakkab kehtima võistleva menetluse reeglistik.[104] Inkvisitsiooniline eeluurimine tekitab olukorra, kus menetlusosaliste võimalused teostatavaid toiminguid mõjutada või vastuargumente esitada on minimaalsed. Seega on ülimalt oluline, et seadusandja on juba eelnevalt seadnud küllaltki kitsa ja konkreetse mänguruumi, kus menetlejal orienteeruda on võimalik. Kuna kohtueelses menetluses on piiratud kaitsja võimalused enda esindatava kaitsmiseks, siis tuleb hoolikalt jälgida, et täisdigitaalsele kriminaaltoimikule üleminek või mõne menetlustoimingu elektroonseks muutmine ei tekitaks võimaliku riivet menetlusosaliste põhiõigustele.

Kui kriminaalmenetlusel tervikuna on kokkupuude väga mitmete eelpool kirjeldatud allikatest tulenevate põhiõigustega, siis järgnevalt kuuluvad vaatluse alla ainult antud õigused, millele avaldatav mõju võib tuleneda digitaalsete vahendite aktiivsema kasutuselevõtuga kohtueelses kriminaalmenetluses.

Õiglase kohtumenetluse mõiste ei ole selge ja üheselt mõistetav. See pole üksik õigus, vaid üldmõiste, mis sisaldab menetluse eri aspekte, põhimõtteid ja õigusi, mille kataloog on avatud. Õiglus on muutuv standard ja menetluses võib see sõltuda nii menetluse tehnilistest küsimustest kui ka üldisematest asjaoludest. Inimõiguste kohus räägib ka õiglase kohtumenetluse laiemast kontseptsioonist, mis hõlmab selliseid põhimõtteid nagu poolte võrdsus ja õigus võistlevale menetlusele.[105] Nagu eelpool mainitud, siis kohtueelne uurimine rakendab inkvisitsioonilist mudelit ning seega on piiratud ka menetlusosaliste võimalused menetlust mõjutada. Näiteks ei ole võimalik tagada kohtueelses menetluses võistlevuse põhimõtet, kuivõrd see saab alguse alles kohtueelse menetluse lõppemise järel. Hoolimata vähestest võimalustest, tuleb ka digitaalse kohtueelse menetluse puhul jälgida seda, et kõikidel menetlusosalistel, aga eelkõige kahtlustataval oleks võimalik osaleda menetluses samaväärselt menetleva poolega.

Inimõiguste ja põhivabaduste kaitse konventsioon (EIÕK) artikkel 6 sisaldab terve kompleksi eri õigusi ja põhimõtteid, millest osa saab kasutada üksikõigustena, osa aga kombineeritult teiste õiguste või põhimõtetega. Õigus olla informeeritud süüdistusest tekib kohtueelse uurimise käigus, nagu ka õigus vaikida.[106]

[104] J. Saar. Eesti kriminaalmenetluse juhtum. - Juridica V/2018, lk 299-306.
[105] U.Lõhmus. Põhiõigused kriminaalmenetluses. Tallinn: Juura 2014, lk 194.
[106] *Ibid*, lk 50

Näiteks tulevikus digitaalsena teostatavate uurimistoimingute puhul tuleb samuti tagada kahtlustatava õigus toimingu protokolliga tutvuda ning teha soovi korral märkusi selle kohta. Kuna tihtipeale toimub menetlustoimingu protokolli tutvustamine koheselt pärast toimingu lõppu, siis jääb tehnilise võimekuse loomine eelkõige menetleja kanda. Ei ole mõistlik eeldada, et kahtlustatav hakkaks näiteks koostatud protokolli läbi lugema enda arvutist läbi avaliku E-toimiku. Üldiselt võiks eeldada, et uurimistoimingute digitaalsus ei tohiks seada ohtu puutumuses olevate isikute põhiõigusi.

Sarnaselt tuleks läheneda ka elektroonse kriminaaltoimiku puhul. KrMS kirjeldatud aluse tekkimisel tuleb tagada kahtlustatavale läbi kaitsja toimikuga tutvumise võimalus ning seda peab võimaldama ka loodav digitoimiku süsteem. Selle kasutamine peab olema subjektile lihtne ning teostatav ilma eriteadmisi ning tehnilisi vahendeid omamata. Seega peab jääma ka hetkel KrMS § 224 lg 1 sisalduv võimalus, et kriminaaltoimikuga on võimalik põhistatud taotluse alusel tutvuda ka paberkandjal. Ei ole muidugi mõeldav, et näiteks tehnilise võimaluse puudumisel hakkaks riik tagama kaitsjatele sülearvuteid ja võrguühendust. Küll on prokuratuuril võimalus näiteks luua vajaduse tekkimisel avalikud töökohad, mille vahendusel on võimalik kaitsjal toimikut enda kaitsealusele tutvustada. Siin tuleks aga kaaluda, kas rahaliselt oleks odavam soovi korral toimikuid paljundada või luua ühiskasutatavad töökohad prokuratuuri kantseleide juurde.

M. Hirvoja leiab enda analüüsis, et tulevikus oleks mõistlik rakendada kahtlustatava või süüdistatava suhtes tegutsemiskohustusena kohaldatud tõkend, mille tulemusel muutuks neile kohustuslikuks kontrollida elektroonilise sidevahendi vahendusel edastatud teateid.[107] Eeluurimise raames ei ole kahtlustataval kohustuslik kaasata protsessi kaitsjat ning seega langeks kogu koormus ainult kahtlustatavale endale. Sellist nõuet ei saa töö autor pidada kuidagi põhjendatuks ning pigem tuleks lähtuda kas kahtlustatava enda valikust sidepidamise viisi osas või kehtestada regulatsioon vastavalt, mis võimaldaks kasutada kahtlustatava enda poolt eelnevalt kasutatud viisi obligatoorsena.

[107] M. Hirvoja. Kriminaalmenetluse revisjoni analüüs - üleminek täisdigitaliseeritud kriminaalmenetlusel - 31.05.2016, lk 5.

Inimõiguste ja põhivabaduste kaitse konventsiooni (edaspidi EIÕK) artikkel 6 sätestab muuhulgas süüdistatava õiguse menetluse toimumisele mõistliku aja jooksul.[108] Menetluse mõistliku kestuse üle otsustamisel arvestatakse menetluse pikkuse sisse ka eeluurimise aeg.[109] Piisavalt kiire menetluse toimumine digitaalse menetluse kasutamisel võib olla takistatud ainuüksi eelnevas peatükis kirjeldatud tehniliste oskuste ja võimekuse puudumisel. Samas tõi töö autor välja võimalikud alternatiivsed lahendused erandlikeks olukordadeks, et kirjeldatud probleem ei ole mõistlike vahenditega ületamatu. Pigem tuleks eeldada, et elektroonsed võimalused pigem kiirendavad menetluse kulgemist tervikuna ning seeläbi loovad ka suurema eelduse mõistliku menetlusaja põhimõtte järgimiseks. Analoogiliselt menetluse mõistliku aja põhimõttega, aitab kaasaegsete võimaluste kasutuselevõtmine tagada paremini ka kaitse ettevalmistamiseks piisava aja saamise õigust.

Üheks EIÕK artikkel 6 lõikes 3 sätestatud õiguseks on süüdistatava õigus kaitsele ning selle all tuleks silmas pidada ka kaitsja juurdepääsu kriminaaltoimiku materjalidele. Kehtiva kriminaalmenetluse seadustiku[110] kohaselt tagatakse kaitsjale ligipääs kriminaaltoimiku materjalidele alles pärast kohtueelse menetluse lõppu. Hoolimata kaitsja piiratud võimalustest eeluurimise käigus kriminaalasja toimikuga tutvuda, esinevad mõningad erandid, kus kaitseõiguse tagamiseks on see ilmtingimata vajalik. Inimõiguste kohus on kaitsja toimiku materjalidele juurdepääsu küsimust käsitlenud EIÕK artikli 5 lõike 4 alusel esitatud kaebuse kohta tehtus otsustes. See EIÕK säte annab sarnaselt KrMS § 34^1 lg 2 vahistatule õiguse taotleda kohtumenetlust enda kinnipidamise seaduslikkuse kontrollimiseks. Kohtu suurkoda on Mooren v. Germany asjas tehtud otsuses võrrelnud vastava õiguse tagamist poolte võrdsuse põhimõttega.[111] Konventsiooni artikli 5 lõikes 4 nimetatud menetlus peab olema võistlev ja kindlustama prokuröri ja vahistatu võrdsuse. Poolte võrdsus pole aga tagatud, kui kaitsjal puudub juurdepääs neile toimiku dokumentidele, mis on olulise tähtsusega vahistamise vaidlustamiseks.[112] Sellest tulenevalt on oluline tagada kaitsja ligipääs vajalikele materjalidele juba vahistamistaotluse arutamise etapis, et oleks võimalik efektiivse kaitse tulemusel esitava vajadusel süüdistatava poolseid vastuargumente. Sellise kohtueelse menetluse toiminguga nagu vahistamine, piiratakse oluliselt isiku vabadust ning seetõttu on oluline pöörata suuremat tähelepanu isiku põhiõiguste tagamisele. Digitaalse kohtutoimiku roll saab selles olla tagav, ehk prokuröril on paari hiireklikiga võimalik selekteerida tutvumiseks vajalikud dokumendid

[108] Inimõiguste ja põhivabaduste kaitse konventsioon – RT II 2000, 11, 57.
[109] U.Lõhmus. Põhiõigused kriminaalmenetluses. Tallinn: Juura 2014, lk 51.
[110] Kriminaalmenetluse seadustik - RT I, 13.03.2019, 7.
[111] U.Lõhmus. Põhiõigused kriminaalmenetluses. Tallinn: Juura 2014, lk 194.
[112] EIKo 09.07.2009, 11364/03, Mooren. vs. Germany, p 124.

e-toimiku süsteemis ning seejärel muutuvad need kaitsjale nähtavaks. Jääb ära igasugune dokumentide selekteerimine pabertoimikus, köidete lahtiharutamine ning füüsiline poolte kohaletulek. Samuti võiks tulevikus tekkida andmebaasi prokuröri abistav eelloend näiteks kaitsjale ligipääsetavad dokumendid vahistamistaotluse arutamiseks. Sinna hulka saaksid juba automaatselt kuuluda kahtlustatava ülekuulamise protokoll, kinnipidamise protokoll, vahistamistaotlus ning teised asjasse puutuvad tuleks valida prokuröril lihtsalt käsitsi.

3.7. Vajalikud muudatused kehtivas regulatsioonis

Justiitsministeeriumis 02. aprillil 2015 aset leidnud kriminaalmenetluse seadustiku muutmisvajaduse arutelul toodi välja selge põhimõte, et digitaliseerimisega ei tohiks unustada kaasnevaid vajalikke seadusemuudatusi ning tulemus ei tohi olla see, et paneme sisuliselt paberi arvutisse. Digitaliseerimine peaks andma ka ressursiefekti.[113]

KrMS § 160^1 lg 4 näeb võimalusena ette kohtutoimiku pidamise kriminaalmenetluses kas osaliselt või täielikult digitaalsena. Vastav regulatsioon ei käsitle aga kriminaaltoimiku pidamise vormi kohtueelses menetluses, vaid selle pidamise nõuded tulenevad justiitsministri määrusest. Määrus „Nõuded kriminaaltoimikule ja kaitseakti näidisvormi kehtestamine“ näeb oma sisult ette ainuüksi paberkandjal toimiku pidamise kohtueelses menetluses.[114] Seega oleks vajalik vastava tehnilise võimekuse saavutamisel muuta ka kehtivat määrust, mis võimaldaks tulevikus rakendada alternatiivselt ka digitaalset kriminaaltoimikut. Et mitte olla lühinägelik, ei tohiks näha ette ainult ühte, ehk digitaalse toimiku pidamise viisi. Peab säilima erandolukordadeks ka alternatiivsete võimaluste kasutamine. Määruse sõnastus võiks olla sarnane KrMS § 160^1 lg 4, mis säilitab mõlemas vormis toimiku pidamise variandi. Näiteks on selline võimalus veel ette nähtud Vabariigi Valitsuse määrusega „Jälitustoimiku pidamise ja säilitamise kord“, mille § 2 lg 1 võimaldab ka jälitustoimikut pidada nii paberkandjal kui digitaalsena.[115]

[113] Justiitsministeerium. KrMS muutmisvajaduse arutelu: kokkuvõte -02.04.2015. Arvutivõrgus: https://www.just.ee/sites/www.just.ee/files/krms_muutmisvajaduse_arutelu_-_kokkuvote_uldine_02_04_2015.pdf (15.04.2019).
[114] Nõuded kriminaaltoimikule ja kaitseakti näidisvormi kehtestamine. JMm 16.07.2008 nr 39 – RT I, 26.01.2016, 8.
[115] Jälitustoimiku pidamise ja säilitamise kord. VVm 03.01.2013 nr 3 - RT I, 08.01.2013, 9.

Tulles menetlustoiminguid puudutavate muudatusvajaduste juurde, tuleks esmalt liigitada tõendid nendes sisalduva sisu, mitte kogumise või presenteerimise meetodist sõltuvalt. Vastasel korral tekiks juba ka liigne segadus digitõendi ja tõendi digitaalse vormi vahel. Kohtueelses menetluses tuleb selgelt aru saada, et digitaliseerimise tulemusel me ei kogu mitte digitaalseid tõendeid vaid tõendeid digitaalselt.[116]

Enim uurimistoimingute hulgast käsitlemist leidnud ülekuulamise regulatsioonis oleks autori pakutud metoodika rakendamiseks vajalik teha mitmeid muudatusi. Eelneva analüüsi põhjal on vajalik parandada kaugülekuulamist reguleeriva KrMS § 69 sõnastust selliselt, et oleks selgelt arusaavad normi kohandamise võimalikkus lisaks kohtumenetlusele ka kohtueelses menetluses. Hetkel kirjeldab kõnealune säte ainult tunnistaja ülekuulamist, kuid võimalus tuleks laiendada ka teistele kriminaalmenetlusi ütlusi andvatele osapooltele. Sinna hulka kuuluvad lisaks tunnistajale ka kannatanu, kahtlustatav ja vajadusel ka ekspert. Digitaalsete menetlusvõtete laiendamiseks oleks vajalik ka ära kaotada ammendav loetelu olukordadest, millal on võimalik kaugülekuulamist rakendada. Hetkel saab seda KrMS § 69 lg 1 alusel kohaldada ainult juhul, kui tunnistaja vahetu ülekuulamine on raskendatud, põhjustab ülemääraseid kulutusi või see on vajalik tunnistaja või kannatanu kaitsmist silmas pidades. Kuna kaugülekuulamist saab täna pidada pigem erandiks kui tavaks, siis hetkel on võimalik küll menetlejal toiming võimalik läbi viia menetluse optimeerimise eesmärgil ning tõlgendades seda kui ülemääraste kulude põhjustamisena. Võttes aluseks soovitava menetluse digitaalse tendentsi, siis oleks mõistlik asendada hetkel kehtiv loetelu menetleja kaalutletud otsustusõigusega antud toimingut rakendada.

Vastastamise puhul tuleks kaotada KrMS § 77 lg 6 ette nähtud tehnilise lahenduse kasutamise võimalus, kuna tulenevalt käesolevas töös esitatud analüüsist ei saa pidada sellise meetodi kasutamise uurimistoimingu eesmärgi saavutamist toetavaks.

Nõustudes autori poolt pakutud võimalustega erinevate uurimistoimingute teostamise metoodika osas, tuleks tulevikus digitaalsena kasutatavate toimingute osas kirjeldada toimingu teostamise järjekord ning sisulised nõuded. Lähtuda tuleks toimingu eesmärgist ning tänase protokolli lahutamatutest osadest, mille kaotamist autor ei toeta, vaid pigem peaks muutuma nende taasesitamise viis.

[116] J. Tehver. Kriminaalmenetluse revisjoni analüüs – digitaalsete tõendite kasutamise võimaldamine - 01.05.2016. Arvutivõrgus: https://www.just.ee/sites/www.just.ee/files/ digitaalsed_toendid_j._tehver.pdf (15.04.2019).

Sarnaselt M. Hirvoja seisukohale peab autor vajalikuks regulatsiooni kehtestamist, mis võimaldaks erandolukordades jätta kõrvale digitaalsete vahendite abil teostatavad toimingud ning pakub võimaluse kriminaalmenetluse läbiviimiseks ka täielikult paberkandjal.[117] Vajalik on ette näha ka menetluse ühetaolisust tagav ühtne lähtumine olukorras, kui kättesaadavad ei ole näiteks enam elektrooniline karistusregister või korduvate süütegude puhul eelnevate tegude toimikud.

[117] M. Hirvoja. Kriminaalmenetluse revisjoni analüüs - üleminek täisdigitaliseeritud kriminaalmenetlusel - 31.05.2016, lk 4.

KOKKUVÕTE

Käesoleva magistritöö keskmes oli kohtueelses kriminaalmenetluses digitaalsete menetlusvõtete kasutamine. Analüüsi eesmärk oli jõuda järeldusele, milliseid seniseid mittedigitaalseid toiminguid oleks võimalik ja samas ka mõistlik tulevikus teostada elektroonselt ning millised muudatused on vajalik nende rakendamiseks sisse viia. Süvitsi vaadeldi kriminaalmenetluses digitoimiku kasutusele võtmise ning erinevate menetlustoimingute digitaliseerimise hetkeseisu ja võimalikku laiendamist tulevikus. Kohtueelses menetluses läbiviidavate uurimistoimingute ning digitoimiku kasutusele võtmise temaatika juures leidis põhjalikumat käsitlemist ka võimalikud ohukohad ning puutumus isikute põhiõigustega.

Selleks, et jõuda tulevikku vaatava teemakäsitluse juurde, oli esmalt vaja kaardistada täna kasutusel olevad infosüsteemid ning vaadelda, milline on olukord digitaalsete võtete kasutamisega kriminaalmenetluses laiemalt. Töö tulemusel saab väita, et Eesti on proovinud e-riigi põhimõtteid kanda üle ka protsessiõiguse rakendamisse, kuid kohtueelne menetlus on jäänud mingil põhjusel vaeslapse rolli. Peamiseks põhjuseks saab tõenäoliselt pidada kohtueelse menetluse mahukust ning seda läbiviivate asutuste ja isikute paljusust. Ühelt poolt on problemaatiline vanade harjumuste järgimine ning teisest küljest puudub menetlejatel tehniline võimakus ning seadusandlusest tulenev julgustus uudseid võtteid kasutada.

Kui riik on peamiseks menetluse digitaliseerimise eesmärgiks näinud ressursikokkuhoidu avalikus sektoris, siis töö autor leiab, et see võimaldaks saavutada kokkuhoiu ning õiglasema positsiooni menetluses ka menetlusosalistel.

Kohtueelse menetluse digitaliseerimise uurimisel jagas töö autor uuendatavad meetodid laialt kaheks. Ühes pooles leidis analüüsimist digitaalse kriminaaltoimiku rakendamine ning teises pooles käsitleti kriminaalmenetluses teostatavaid menetlustoimingud.

Kohtumenetluses on juba täna peamiselt kasutusel digitoimik, kuid vastava kuju saab see alles prokuratuuris pabertoimiku sisse skaneerimise tulemusel. Kohtueelses menetluses rakendatakse sisuliselt hübriidset süsteemi, kus osaliselt koostatakse menetlustoimingud arvutis ja laetakse ka menetluse infosüsteemi, kuid seejärel prinditakse ikkagi välja ning lisatakse pabertoimikusse. Samas ei saa pidada sellist praktikat jätkusuutlikuks ning infosüsteemi

dokumentide laadimine ei anna soovitud tulemust. Seega tuleks astuda tugevaid samme, et võimalikult kiiresti minna üle täisdigitaalsele kriminaaltoimikule alates kohtueelsest menetlusest kuni kohtumenetluseni välja. Täna on määratletud, et vastavat digitoimikut ei rakendata enne 2022. aastat, kuid vähemalt on võetud see plaani ning loodetavasti kiirendab protsessi ka käimasolev kriminaalmenetluse revisjon.

Kui digitoimiku kasutamise osas on riik suuna võtnud ning loodab järgmises kümnendis üle minna täielikule digitaalsele kriminaaltoimikule, siis menetlustoimingute osas veel selget visiooni ei omata. Menetlustoimingute osas on küll osaliselt võetud kasutusele ka elektroonsed võimalused, kuid kahjuks on pea täielikult kõrvale jäetud uurimistoimingud. Uurimistoimingud moodustavad klassikalise (jälitustoiminguid mittesisaldavast) kriminaalmenetluse mahust valda osa, seega ei saa neid pidada kuidagi vähemolulisteks.

Töö käigus jõudis autor seisukohale, et peamiselt saaks uurimistoiminguid digitaliseerida läbi nende protokollimise ning sellega kaasnevate toimingute. Elektroonilise protokollimise võimaluse võiks toimingu eripärasid arvesse võttes kohaldada kõikide uurimistoimingute puhul. Ülekuulamiste ja äratundmiseks esitamiste puhul leidis autor, et neid on uurija kaalutlusest tulenevalt võimalik teostada ka teatud juhtudel täielikult digitaalsena. Vastastamise puhul ei saa aga tulenevalt toimingu iseloomust pidada selle distantsilt teostamist eesmärki taotlevaks, kuigi seda toetab tänane regulatsioon. Ütluste seostamisel olustikuga, läbiotsimise, uurimiseksperimendi ja vaatluse puhul võib töös käsitletu põhjal pidada tulevikus mõistlikuks videojäädvustamise ja digitaalse protokollimise hübriidsüsteemi.

Käsitletud uurimistoimingute digitaalseks muutmine aitab paremini tagada menetlusosaliste õigusi menetluses. Seda nii rohkemate võimaluste näol selle võistlevuses osalemiseks, kui ka hilisema tõendiväärtuse kontrollimise võimaldamise teel. Lisaks vähendab see piisava toimekindluse saavutamisel uurimistoimingutes osalevate isikute koormatust ning pakub vajadusel neile täiendavat kaitset. Tervikuna muutub menetlus kiiremaks, vähemat ressurssi nõudvaks ning paremini kontrollitavaks.

Täna on juba kasutusel elektroonilisel teel ekspertiisimääruste ning aktide koostamine ja digitaalselt toimub ka enamus jälitustegevusega kaasnev. Uurijate sõnul on selline areng vähendanud nende töömahtu ning parandanud nõutavate toimingute teostamise efektiivsust.

Samas ei suuda tänaseks ikkagi kõik kohtud veel jälitustegevuse lubade andmisel ja pikendamisel kasutada saadaolevaid infosüsteeme ning tegevus toimub endiselt pabertoimiku alusel. Sarnaste lünkade ületamisega tuleks tegeleda ning seejärel saab alles väita, et näiteks jälitustegevuse elektroonne süsteem on soovitud optimeerimise taganud.

Peamise kitsaskohana, mis on kindlasti ka üheks menetluse digitaliseerimise takistavaks teguriks, on kasutusel olevad infosüsteemid. Tänastes süsteemides puudub suures ulatuses näiteks autori poolt välja pakutud funktsionaalsus, et kasutusele võtta uudsel teel teostatavad toimingud. Eeskujulikuks süsteemiks võib pidada e-toimikut, mis oma olemuselt kattub autori nägemusega. Samas on vaja teostada hulgaliselt arendusi just eelkõige menetlevate asutuste süsteemides. Mitmed uurimisasutused on hakanud näiteks kasutama e-toimiku kriminaalmenetluse liidest PRIS, kuhu pideva arenduse käigus lisatakse ka tulevikku vaatavaid võimekusi (viimati nt videosalvestiste lisamise näol). Samas suurimaks kohtueelse menetluse läbiviijaks olev Politsei- ja Piirivalveamet kasutab menetluse infosüsteemi MIS, mis on praktikas paraku pigem menetlust ruineeriv, kui toetav. Seega peab menetluse kaasajastamine käima käsikäes õigusteadlaste ning infotehnoloogide töö ja arendustegevusega.

Kehtiva õiguse ja vajalikke muudatusi käsitledes jõudis autor järeldusele, et menetlusseadustik (KrMS) näeb küll ette mitmeid digitaalseid meetodeid kasutavaid alternatiivvõimalusi, kuid nende sisuline eesmärk ei tulene otseselt menetluse efektiivsuse ja optimeerimise tagamisest. Digitaalse kohtutoimiku pidamise võimalikkus on sisse viidud, kuid tänane regulatsioon ei võimalda sama kohtueelse menetluse toimikuga. Otseselt ei sätesta ka uurimistoimingu protokolli vorminõudeid, kuid selguse huvides oleks mõistlik see võimaliku alternatiivina ette näha. Suurt tähelepanu tuleks teiste käsitletud toimingute kõrval pöörata autori poolt välja pakutud muudatusvajadustele kaugülekuulamiste teostamise soodustamiseks.

Käesoleva töö autor püstitas hüpoteesi, et tänases kohtueelses kriminaalmenetluses ei kasutata piisavalt kaasaegseid infotehnoloogilisi võimalusi, et saavutada efektiivsem menetlus. Antud hüpotees leidis töö tulemuse kinnitamist ning saab järeldada, et oluliselt efektiivsem kohtueelne menetlus on võimalik saabutada täisdigitaalsele kriminaaltoimikule ülemineku ning töös käsitletud uurimistoimingute kaasasjastamisega. Rakendamata on väga suur potentsiaal, et saavutada digitaliseerimise tulemusel efektiivsem menetlus kõigile osapooltele.

Digitalizing criminal proceedings in pre-trial procedure.

Abstract

In today's society, the vast majority of the population probably cannot imagine a life without technical means. The use of various technical means and the services they offer has become commonplace. The use of innovative tools has not become widespread due to its novelty and the curiosity of people alone, it has also made many processes in our lives much easier and more productive in their final phase.

In Europe, Estonia is widely known as an e-country. To achieve this, the small country has made great efforts, and despite its small size, it has found a niche to pioneer. Several Estonian private companies in the IT sector are prominent internationally, and the country is also known as the developer of the concept of e-government. Estonia has invested substantially into modernising public services. Thanks to this, the top three spots in the rankings of European public IT services have been earned a number of times. The desire of a small country to try to do something differently and better has borne fruit.

In addition to the rapid development in the technical sector, Estonia has been able to build a functioning and ambitious country during the relatively short period after the restoration of its independence. In order for people to be able to feel safe and good in their living environment, it is of utmost importance for the state to ensure their security and sense of justice, among other things. One of the inseparable parts of Estonia's rule of law is the functioning of an impeccable judicial system. First and foremost, this thesis addresses the pre-trial procedure, which is a prerequisite for a successful settlement of criminal cases, but other phases and types of proceedings are also touched upon. Conducting criminal procedures is the responsibility of the state in all stages of the proceedings and naturally, this must be done in the best possible manner, observing the rights of the parties to the proceedings as well as the persons involved in the criminal procedure.

Befittingly to an innovative state, criminal procedure also falls within the scope of the public services, which are offered on a “compulsory” basis, but are increasingly being provided by involving electronic solutions. While the use of information technology solutions in criminal procedures may provide considerably more convenient opportunities for the parties to the proceedings, better opportunities to participate in the proceedings and thus protect their rights may be considered even more important. On the other hand, the conducting party (i.e. the state)

is able to achieve significant savings through these innovative procedural solutions. This includes savings on the resources of the organisations involved in the proceedings, as well as on the burden on the staff involved in the proceedings. It is, therefore, possible to achieve a profitable result for all parties to the proceedings and to reduce unnecessary bureaucracy. Thousands of people are exposed to pre-trial criminal procedures on a daily basis, and any change in the procedures and methods used in the proceedings can be considered as having a very significant impact.

This Master's thesis examines the use of digital solutions in the pre-trial criminal procedure. More specifically, it focuses on the pre-trial procedure stage and the procedures and investigative activities to be carried out at this stage. The choice of the topic of the thesis is largely driven by the experience of the author and other practitioners, which has pointed to a direct need to review the way in which current proceedings are conducted and the use of electronic means used in these procedures. Although various e-services have been created to simplify the work of the investigative bodies, these services do not fulfil their purpose in practice in full, and the desired savings on procedural resources have not been achieved.

The use of modern procedural techniques in criminal procedures is mainly related to two areas. On the one hand, the law which sets out the conditions and procedures for the use and methods of the corresponding acts. On the other hand, the subject concerns information technology, which limits the use of technical tools in particular, and creates an even greater challenge for information systems. In this work, the emphasis is primarily on the first, i.e. the legal field, and the author of the thesis has also proposed technological solutions within the scope of the user module. This helps to better understand the results sought by turning to electronic solutions for specific operations.

It can be argued that the current situation with the use of modern solutions in the Estonian legal system is quite good. For example, civil and administrative courts are about to switch to fully digital records, and almost all activities are already electronic. Modern technical equipment is also used in the day-to-day work of the authorities conducting criminal procedures. Despite this, there are bottlenecks and even more opportunities for further development.

The digital criminal case file, which has been the focal point of digitalism and criminal procedures, is partly addressed in the thesis. In the current procedure, the criminal case file becomes partially digital when sent to the court by the prosecutor's office, but it is still kept on

paper in the pre-trial procedure. In the pre-trial procedure, a hybrid system is implemented in practice, in which the procedural acts are partly compiled on a computer and also uploaded to an information system of procedures, but then still printed out and added to paper records. However, such a practice cannot be considered sustainable and uploading the documents into an information system does not produce the desired result. Strong steps should therefore be taken to move to a full digital criminal file as soon as possible, from pre-trial procedures to judicial procedures. While the ongoing criminal procedure review deals with this subject, specific time targets have not been set and they have been pushed to the unknown future.

In addition to the digital criminal case file, the modernisation of pre-trial procedures is also addressed as the second research problem. Criminal procedures are divided into various procedural acts, some of which are of an organisational and ensuring nature and others are actions for the taking of evidence. Expert assessments, investigative activities, as well as surveillance activities are targeted to the taking of evidence, for example. Currently, examination ruling and acts are already compiled electronically, and most surveillance activities are conducted digitally as well. Such a development has certainly significantly reduced the workload of investigators and surveillance officers, and improved the efficiency of the required operations. At the same time, however, not all courts are able to use the available information systems for granting and extending surveillance permissions, and activities are still based on files in paper. Overcoming similar gaps should be addressed, after which it can be said that an electronic surveillance system has ensured the desired optimisation.

It can be argued that in pre-trial criminal procedures, the vast majority of the investigator's work is investigative activities. At the same time it seems that these have been discarded from modernising the procedure and their potential is unused. The author believes that the investigative activities could be digitized mainly through their reporting and the accompanying activities. The possibility of electronic reporting could be applied to all investigations, taking into account the specificities of the activity. In the case of interrogations and presentation for identification, the author found that according to the investigator's discretion, in some cases, these activities can be performed digitally in full. However, in the case of confrontation, due to the nature of the act, carrying it out remotely cannot be considered purposeful, although this is supported by the current regulation. In terms of linking testimonies with the context, searches, investigative experiments, and inspections, a hybrid system for video capture and digital recording may be considered reasonable in the future.

The digitalisation of the investigative activities addressed will help to ensure that the rights of the parties to the proceedings are safeguarded. This is done by allowing direct participation in the proceedings as well as subsequent verification of the evidence value. In addition, it reduces the burden on individuals involved in investigative activities and provides them with additional protection, if necessary. As a whole, the procedures become faster, less resource-intensive and more controllable.

The main bottlenecks, which are certainly one of the obstacles to the digitalisation of the procedure, are the information systems in use and in need of development. For example, the current systems largely lack the functionality suggested by the author to introduce novel activities. The e-File, which by its nature overlaps with the author's vision, can be considered a promising system. At the same time, it is necessary to carry out numerous developments, especially in the systems of the processing institutions. For example, several investigative bodies have begun to use the e-File criminal procedure interface PRIS, which will have forward-looking capabilities incorporated into it with continuous development. At the same time, the Police and Border Guard Board, the conductor of the most pre-trial procedures, uses a separate information system for procedures, which, unfortunately, ruins the proceedings rather than supporting them. Thus, the modernisation of the procedure must go hand in hand with the work and development by information technology experts.

In the thesis, consideration was also given to the fundamental rights of individuals in digitalisation. The pre-trial investigation is inquisitive, and adversary will become evident only at the judicial procedures stage. Thus, it is of utmost importance that the legislator has already created a fairly narrow and specific playing field where the body conducting proceedings can be orientated. This minimises the risk of violating a person's fundamental rights and their transfer to the judicial procedures. Digital procedural acts must be treated similarly. With these it must be ensured that the savings in pre-trial procedures would not become fatal in the judicial procedures. In the circumstances arising from the digitalisation of fundamental rights and the proceedings, emphasis must be placed on ensuring equality between the parties to the proceedings. As the state is always the stronger party in the procedure, it has better opportunities for technical infrastructure and training of employees as well. It must be guaranteed that the use of criminal justice e-services is feasible and possible for the parties to the proceedings.
Although the author offers a number of modern solutions contributing to increasingly efficient criminal procedures in this thesis, it must not be forgotten for a moment that awareness and mitigation of potential threats must be preserved. Once again, it is a task for information

technology experts rather than for lawyers, but one cannot do anything without the other. While errors in databases and e-services in the pre-trial procedure are currently commonplace, it will be increasingly less permissible in the future. The 24 hour operation of the services must be ensured and any disruptions may only be short-lived and easily overcome. Time-critical works and operations must not be disturbed by technical issues. In order to ensure the operational reliability of information systems, not only does the system itself need to work continuously, but it also requires the proper functioning of the technical equipment, the network connection and the service provider. It is also necessary to ensure the functioning of criminal procedures in a situation where it is not possible to use electronic means in the proceedings or it would be extremely burdensome, for example due to a national crisis. However, law enforcers cannot wash their hands clean of responsibility. The role of the body conducting the proceedings is very important in considering whether to take any procedural action in criminal matters. The dangers outlined in this thesis should also be taken into account when making decisions. All procedures must be in accordance with the investigative practice applied by the investigator and must not infringe the taking of evidence for the purpose of the proceedings.

When addressing current law and the necessary changes, the author came to the conclusion that the Code of Criminal Procedure provides for several alternative ways of using digital methods, but their substantive purpose is not directly related to ensuring the efficiency and optimisation of the procedure. The possibility of keeping digital judiciary records has been introduced, but current regulation does not allow the same for pre-trial procedure records. While the format requirements for the protocol of the investigative activity are not explicitly provided for, for the sake of clarity, it would be reasonable to foresee it as a possible alternative. In addition to other procedures addressed, great attention should be paid to the need for simplifying remote interrogation, which was put forward by the author.

Interrogation can now be carried out via means of communication as well, but only in very specific cases. The law also allows witnesses to be interrogated remotely. It is certainly necessary to introduce a more flexible regulation, and remote interrogation must be made an everyday practice, rather than an exception.

It was hypothesised that modern pre-trial criminal procedures do not use enough modern information technology to achieve a more efficient procedure. This hypothesis was confirmed in the thesis and it can be concluded that the advancement of the pre-trial procedure must be actively pursued. There is a huge potential unapplied to achieve a more efficient procedure for

all parties as a result of digitisation. Rather, it can be argued that there is a need to change existing practices and that the alignment of the rules will be simple, not overwhelming. In addition, the digital criminal procedure poses a major challenge for technical developers. It would be sensible to involve more practitioners in the IT development process at an early stage to achieve a better result for the end user.

Both Estonian and foreign language literature, former and current legislation, case law and numerous information materials have been used as sources in the preparation of the thesis. The thesis also includes information from the practical experience of the author. Due to the novelty of the topic, the area of digitisation of procedural acts and investigative activities included therein has not been dealt with to a large extent in the past. While the necessity for the topic has also been raised in the course of the criminal procedure review, to the knowledge of the author, the topics discussed in this thesis have not been thoroughly dealt with during the review. In this thesis, the approach to modernising the procedures is mainly based on the methodology of the proceedings and an analysis of their purpose. Looking at international practice and trends, the thesis is limited to the countries of the Continental European judicial area.

LÜHENDID

EIK – Euroopa Inimõiguste Kohus

EIKo - Euroopa Inimõiguste Kohtu otsus

EIÕK - Inimõiguste ja põhivabaduste kaitse konventsioon

ELT – Euroopa Liidu Teataja

MKM – Majandus- ja Kommunikatsiooniministeerium

HMS - Haldusmenetluse seadus

JM - Justiitsminister

KrMS - Kriminaalmenetluse seadustik

RKKK – Riigikohtu kriminaalkolleegium

RKo - Riigikogu otsus

RT – Riigi Teataja

SiM - Siseminister

TsMS - Tsiviilkohtumenetluse seadustik

Vl - välisleping

VTMS - Väärteomenetluse seadustik

VVm - Vabariigi Valitsuse määrus

KASUTATUD MATERJALID

Kasutatud kirjandus

1. Council of Europe. European judicial systems - Efficiency and quality of justice. Arvutivõrgus: https://rm.coe.int/rapport-avec-couv-18-09-2018-en/16808def9c (15.04.2019).
2. E. Kergandberg, M. Sillaots. Kriminaalmenetlus. Tallinn: Juura 2006.
3. E. Kergandberg, P. Pikamäe. Kriminaalmenetluse seadustik. Kommenteeritud väljaanne. Tallinn: Juura 2012.
4. E. Tikk. Informatsioon ja õigus. - Õiguskeel IV/2007.
5. Eesti Arengufond. Nutikas spetsialiseerumine - kitsaskohtade ja uute võimaluste analüüs. Arvutivõrgus: http://www.arengufond.ee/wp-content/uploads/2013/06/AF_kitsaskohad_final2.pdf (15.04.2019).
6. Eesti infopoliitika põhialused aastateks 2004-2006. Arvutivõrgus: https://www.mkm.ee/sites/default/files/infopoliitika_pohialused_2004-2006.pdf (15.04.2019).
7. Eesti infoühiskonna arengukava 2013. Arvutivõrgus: https://www.mkm.ee/sites/default/files/eesti_infouhiskonna_arengukava_2006.pdf (15.04.2019).
8. Eesti infoühiskonna arengukava 2020 (uuendatud 2018). Arvutivõrgus: https://www.mkm.ee/sites/default/files/eesti_infouhiskonna_arengukava_2020_ja_kuberturvalisuse_strateegia_2019-2022.pdf (15.04.2019).
9. Eesti infoühiskonna arengukava 2020. Arvutivõrgus: https://www.mkm.ee/sites/default/files/elfinder/article_files/eesti_infouhiskonna_arengukava.pdf (15.04.2019).
10. Elektroonilise side seaduse ja infoühiskonna teenuse seaduse muutmise seaduse seletuskiri 137. Arvutivõrgus: https://www.osale.ee/konsultatsioonid/files/consult/137_SELETUSKIRI_13_01.rtf (15.04.2019).
11. G. Buzarovska Lazetik, O. Koshevaliska. Digital Evidence in Criminal Procedures. - Balkan Social Science Review XII/2013.
12. H. Lindmäe. Menetlustaktika I. Tartu: Juura 1995.
13. H. Lindmäe. Menetlustaktika II. Tartu: Juura 1997.
14. J. Matt, H. Hinsberg, A. Laido. Tulevikuraport: Kuidas infoühiskonna muutused ja mõju enda kasuks tööle panna? Arvutivõrgus: https://heakodanik.ee/wp-content/uploads/2013/09/Infoyhiskonna_raport_0.pdf (15.04.2019).

15. J. Saar. Eesti kriminaalmenetluse juhtum. - Juridica V/2018.
16. J. Tehver. Kriminaalmenetluse revisjoni analüüs – digitaalsete tõendite kasutamise võimaldamine - 01.05.2016. Arvutivõrgus: https://www.just.ee/sites/www.just.ee/files/digitaalsed_toendid_j._tehver.pdf (15.04.2019).
17. Justiitsministeeriumi kriminaalpoliitika põhialused aastani 2030. Arvutivõrgus: https://www.just.ee/sites/www.just.ee/files/kriminaalpoliitika_pohialused_2030.pdf (15.04.2019).
18. Justiitsministeeriumi valitsemisala arengukava aastateks 2019 – 2022. Arvutivõrgus: https://www.just.ee/sites/www.just.ee/files/justiitsministeeriumi_arengukava_2019-2022.pdf (15.04.2019).
19. Justiitsministeeriumi ülevaade E-Toimiku projektist ja esmakordse rakendamisega kaasnevatest muudatustest töökorralduses – 29.06.2009. Arvutivõrgus: https://www.riha.ee/api/v1/systems/e-toimik/files/da5a8578-f169-db42-fd89-a685b9b6e621 (15.04.2019).
20. K. Põder (toim.). Infoühiskond, Tallinn: Statistikaamet 2010. Arvutivõrgus: https://www.stat.ee/publication-download-pdf?publication_id=21188 (15.04.2019).
21. Kriminaalmenetluse seadustiku ja teiste seaduste muutmise seaduse eelnõu seletuskiri seisuga 04.05.2018. Arvutivõrgus: https://www.advokatuur.ee/uploads/files/SK%20KrMS%20revisjon.pdf (15.04.2019).
22. M. Hirvoja. Kriminaalmenetluse revisjoni analüüs - üleminek täisdigitaliseeritud kriminaalmenetlusel - 31.05.2016. Arvutivõrgus: https://www.just.ee/sites/www.just.ee/files/uleminek_taisdigitaliseeritud_kriminaalmenetlusele_m_hirvoja.pdf (15.04.2019).
23. M. Kurm. Kriminaalmenetluse revisjoni analüüs - Tõendite kogumisel dubleerimise vältimine kohtu- ja kohtueelses menetluses - 31.05.2016. Arvutivõrgus: https://www.just.ee/sites/www.just.ee/files/toendamine_m._kurm.pdf (15.04.2019).
24. M. Rosentau. E-tempora, e-mores. - Juridica II/2015.
25. M. Solvak jt. E-governance diffusion: Population level e-service adoption rates and usage patterns - Telematics and Informatics 36/2019.
26. P.K. Tupay, M. Mikiver. E-riik ja põhiõigused. - Juridica III/2015.
27. R. Karja. Digitaalne toimik kriminaalmenetluses. Magistritöö. Tartu, 2015. Arvutivõrgus: http://dspace.ut.ee/bitstream/handle/10062/47395/karja_rasmus.pdf?sequence=1&isAllowed=y (15.04.2019).
28. R. Öpik. Kriminalistiline taktika ja tehnoloogia I. Tallinn: Sisekaitseakadeemia 2008.

29. Riigi peaprokuröri ülevaade Riigikogu Põhiseaduskomisjonile seadusega Prokuratuurile pandud ülesannete täitmise kohta 2016. aastal. Arvutivõrgus: http://www.prokuratuur.ee/sites/www.prokuratuur.ee/files/elfinder/article_files/peaprokurori_ulevaade_15.06_ps_komisjonile_2016_kohta.docx (15.04.2019).
30. Riigikohtu asjaajamiskord 17.12.2012 seisuga. Arvutivõrgus: https://www.riigikohus.ee/sites/default/files/elfinder/dokumendid/asjaajamiskord_kinnitatud.pdf (15.04.2019).
31. Riigikontrolli aruanne avalike teenuste kvaliteedi kohta infoühiskonnas 2010. Arvutivõrgus: https://www.riigikontroll.ee/DesktopModules/DigiDetail/FileDownloader.aspx?AuditId=2162&FileId=11158 (15.04.2019).
32. Riigikontrolli avalike e-teenuste kasutatavuse aruanne riigikogule 2016. Arvutivõrgus: https://www.riigikontroll.ee/DesktopModules/DigiDetail/FileDownloader.aspx?AuditId=2411&FileId=13797 (15.04.2019).
33. U. Krüger. Kriminaalmenetlus: Tõendamine kohtueelses menetluses. Üldkäsitlus 1. osa. Tallinn: Sisekaitseakadeemia 2005.
34. U. Krüger. Ülekuulamine kohtueelses menetluses, Õiguslikud aspektid. Tallinn: Sisekaitseakadeemia 2008.
35. U.Lõhmus. Põhiõigused kriminaalmenetluses. Tallinn: Juura 2014.
36. V. Kõve, jt. Tsiviilkohtumenetluse seadustik. Kommenteeritud väljaanne II. Tallinn: Juura 2017.
37. Vabariigi Valitsuse tegevusprogramm 2015-2019. Arvutivõrgus: https://valitsus.ee/sites/default/files/contenteditors/arengukavad/valitsuse_tegevusprogramm_2015-2019_2.xlsx (15.04.2019).
38. Õiguskantsleri 2007. aasta tegevuse ülevaade. Arvutivõrgus: https://www.oiguskantsler.ee/sites/default/files/6iguskantsleri_2007._aasta_tegevuse_ylevaade.pdf (15.04.2019).

Kasutatud normatiivaktid

39. Eesti infopoliitika põhialuste heakskiitmine. RKo 13.05.1998 - RT I 1998, 47, 700.
40. E-identimise ja e-tehingute usaldusteenuste seadus - RT I, 12.12.2018, 30.
41. E-toimiku põhimäärus - RT I, 09.03.2018, 5.
42. E-toimiku süsteemi asutamine ja e-toimiku süsteemi pidamise põhimäärus. VVm 03.07.2008 nr 111 - RT I, 09.03.2018, 5.

43. Euroopa Parlamendi ja Nõukogu 23.07.2014 määrus nr 910, e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul - ELT L257/73.
44. Haldusmenetluse seadus - RT I, 13.03.2019, 55.
45. Infosüsteemide turvameetmete süsteem. VVm 20.12.2007 nr 252 - RT I 2007, 71, 440.
46. Inimõiguste ja põhivabaduste kaitse konventsioon – RT II 2000, 11, 57.
47. Jälitustoimiku pidamise ja säilitamise kord. VVm 03.01.2013 nr 3 - RT I, 08.01.2013, 9.
48. Karistusseadustik - RT I, 13.03.2019, 77.
49. Kriminaalmenetluse seadustik - RT I, 13.03.2019, 77.
50. Nõuded kriminaaltoimikule ja kaitseakti näidisvormi kehtestamine. JMm 16.07.2008 nr 39 - RT I, 26.01.2016, 8.
51. Politsei andmekogu põhimäärus. SiMm 22.12.2009 nr 92 - RT I, 12.03.2019, 39.
52. Tsiviilkohtumenetluse seadustik - RT I, 19.03.2019, 22.
53. Väärteomenetluse seadustik - RT I, 13.03.2019, 200.

Kasutatud kohtupraktika

54. EIKo 09.07.2009, 11364/03, Mooren. vs. Germany.
55. EIKo 16.06.2009, 54252/07 jt, Lawyer Partners A.S. vs. Slovakia.
56. RKKK 07.05.2009, 3-1-1-21-09.
57. RKKK 14.04.2010, 3-1-1-19-10.

Muud allikad

58. Eesti Rahvusraamatukogu Raamatukogusõnastik. Arvutivõrgus: https://termin.nlib.ee/view/4830 (31.03.2019).
59. Euroopa Komisjon. Digital Economy and Society Index 2018 – Eesti. Arvutivõrgus: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=52352 (15.04.2019).
60. Justiitsministeerium. KrMS revisjoni VTK kooskõlastamisel laekunud arvamused ja otsused revisjoni I etapi teemaderingi osas, p 1.1. Arvutivõrgus: https://www.just.ee/sites/www.just.ee/files/ettepanekute_loetelu_ja_otsused.pdf (15.04.2019).

61. Justiitsministeeriumi KrMS muutmisvajaduse arutelu kokkuvõte -02.04.2015. Arvutivõrgus: https://www.just.ee/sites/www.just.ee/files/krms_muutmisvajaduse_arutelu_-_kokkuvote_uldine_02_04_2015.pdf (15.04.2019).
62. Majandus- ja Kommunikatsiooniministeeriumi pressiteade „Euroopa digiministrid allkirjastasid Tallinna e-valitsemise deklaratsiooni“ – 06.10.2017. Arvutivõrgus: https://www.mkm.ee/et/uudised/euroopa-digiministrid-allkirjastasid-tallinna-e-valitsemise-deklaratsiooni (15.04.2019).
63. Peaprokuröri kõne prokuröride XX üldkogul – 06.04.2018. Arvutivõrgus: https://www.prokuratuur.ee/sites/www.prokuratuur.ee/files/elfinder/Peaprokur%C3%B6ri%20k%C3%B5ne.pdf (15.04.2019).
64. Politsei- ja Piirivalveameti kodulehe avalduse esitamise digitaalne vorm. Arvutivõrgus: https://www2.politsei.ee/et/teenused/politseile-avalduse-esitamine.dot (15.04.2019).
65. Prokuratuuri seletav sõnastik. Arvutivõrgus: https://www.prokuratuur.ee/et/pressile/seletav-sõnastik (15.04.2019).
66. Riigi Infosüsteemi Haldussüsteemi koduleht. E-toimiku süsteemi kriminaalmenetluse liides PRIS. Arvutivõrgus: https://www.riha.ee/Infos%C3%BCsteemid/Vaata/70000310-pris (15.04.2019).
67. Riigi Infosüsteemi Haldussüsteemi koduleht. E-toimikuga liidestunud süsteemide loogiline arhitektuur – 01.11.2017. Arvutivõrgus: https://www.riha.ee/api/v1/systems/e-toimik/files/a2c800e1-f14a-3cd3-3d09-1fb3c02fa303 (15.04.2019).
68. Riigi Infosüsteemi Haldussüsteemi koduleht. Infosüsteem POLIS. Arvutivõrgus: https://vana.riha.ee/riha/main/inf/infosusteem_polis (15.04.2019).
69. Siseministeeriumi pressiteade „Kriisikomisjon keskendus valitsusasutuste valmisolekule elutähtsa teenuse katkemisel“ – 15.06.2017. Arvutivõrgus: https://www.siseministeerium.ee/et/uudised/kriisikomisjon-keskendus-valitsusasutuste-valmisolekule-elutahtsa-teenuse-katkemisel (15.04.2019).
70. Statistikaamet. Keskmine Eesti brutotunnipalk 2018.a. Arvutivõrgus: https://www.stat.ee/stat-keskmine-brutotunnipalk (15.04.2019).
71. Tallinn Declaration on eGovernment at the ministerial meeting during Estonian Presidency of the Council of the EU – 06.10.2017. Arvutivõrgus: https://www.mkm.ee/sites/default/files/tallinn_egov_declaration_with_signatures.pdf (15.04.2019).
72. The World Bank. Individuals using the Internet 2017. Arvutivõrgus: https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=EE&view=chart (15.04.2019).

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, KRISTJAN PAHK,
(autori nimi)

annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose

KRIMINAALMENETLUSE DIGITALISEERIMINE KOHTUEELSES MENETLUSES,
(lõputöö pealkiri)

mille juhendaja on Ph D Andreas Kangur,
(juhendaja nimi)

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

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

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

Tartus, 30.04.1019.