TARTU ÜLIKOOL
SOTSIAALTEADUSTE VALDKOND
ÕIGUSTEADUSKOND
Karistusõiguse osakond

Helen Vahkal

INFOTEHNOLOOGIA JA DIGIVORMI KASUTAMISE PERSPEKTIIVID TÕENDAMISEL KRIMINAALMENETLUSES

Magistritöö

Juhendaja: *dr. iur.* Mario Rosentau

Tartu
2022

SISUKORD

SISSEJUHATUS

Viimastel aastakümnetel on tehnoloogia areng mõjutanud inimeste ja riikide andmevahetust ning -töötlust. Esimese mikroprotsessori valmimisest 1970. aastatel on *Moore*'i seaduspärasuse järgi mikrokiibil olevate transistorite arv iga kahe aasta tagant kahekordistunud, mis on toonud endaga kaasa elektrooniliste seadmete odavnemise ja kättesaadavamaks muutmise lõpp-tarbijate jaoks. Seega täitub tehnoloogia arengu tõttu meid ümbritsev keskkond seadmetega, mis toodavad üha enam digitaalseid andmeid. 2013. aastal loodi 500 miljardit Microsoft Office'i dokumenti[1], 2017. aastal tehti kaamerate ja nutitelefonidega 1,2 triljonit pilti[2], 2020. aastal saadeti ja saadi kätte umbes 306 miljardit e-kirja päevas[3], kusjuures need arvud suurenevad igal aastal.

Samal ajal väheneb analoogkujul toodetavate dokumentide hulk. Seda eriti e-riigis Eestis, kus veel hiljuti oli vaid kaks toimingut, mida ei saanud teha digitaalselt: kinnisvara osta ning abielluda või lahutada. 1. veebruaril 2020. a jõustusid tõestamisseaduse muudatused[4], mis andsid võimaluse notaritel teha kaugtõestamise teel mõningaid lihtsamaid toiminguid, sealhulgas osa võõrandamise tehinguid, volikirjade tõestamisi ja pärandvara inventuuri nõudeid[5]. Kuna Vabariigi Valitsus kuulutas 12.03.2020. a välja eriolukorra seoses COVID-19 haigust põhjustava koroonaviiruse pandeemilise levikuga maailmas, muutis Justiitsministeerium tsiviilkäibe edendamiseks notariaadimäärustikku[6], kus tõestamisseaduse § 13 lõikes 8 sisalduva volitusnormiga on kehtestatud kaugtõestamise teel tehtavate

[1] Guess How Many Microsoft Office Documents Were Made Last Year. Business Insider, 2014. Arvutivõrgus kättesaadav https://www.businessinsider.com/how-many-microsoft-office-documents-were-made-last-year-2014-2 (06.04.2022).

[2] Keypoint Intelligence, Our Best Photos Deserve to Be Printed. 2018. Arvutivõrgus kättesaadav https://www.keypointintelligence.com/news/editors-desk/2018/september/our-best-photos-deserve-to-be-printed/ (06.04.2022).

[3] Number of sent and received e-mails per day worldwide from 2017 to 2025. Statista, 2021. Arvutivõrgus kättesaadav https://www.statista.com/statistics/456500/daily-number-of-e-mails-worldwide/ (06.04.2022).

[4] Tõestamisseaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seadus 719 SE eelnõu ja seletuskiri on leitavad Riigikogu veebilehel https://www.riigikogu.ee/tegevus/eelnoud/eelnou/1ef1f0ea-7e3a-410c-b597-878a97191140 (06.04.2022).

[5] Kaugtõestamise korra ning kaugtõestamise teel tehtavate ametitoimingute ja tehingute nimekirja kehtestab tõestamisseaduse § 13 lg 8 alusel justiitsminister määrusega. 1. veebruaril 2020 jõustunud justiitsministri 19. juuni 2009. a määruse nr 23 „Notariaadimäärustik" § 12[1] lg 6 lubas kaugtõestamise teel teha järgmisi ametitoiminguid: osa võõrandamise ning pantimise kohustus- ja käsutustehingud; volikirjade tõestamine ja kehtetuks tunnistamine; abiellumis- ja lahutamisavalduse esitamine; lapsendamiseks antava nõusoleku esitamine juhul, kui lapsendajaks on teise bioloogilise vanema abikaasa või registreeritud elukaaslane; pärimismenetluse algatamise, pärandi vastuvõtmise ja pärandist loobumise avalduse tõestamine; pärandvara inventuuri nõude esitamine; asjaõiguste ja kommertspandi kustutamine ja loovutamine, kui sellisele toimingule on ette nähtud notariaalse kinnitamise vorm, muu hulgas kokkulepe kinnistu vabastamiseks ühishüpoteegi alt ja järjekoha muutmiseks ning asjaõiguste pidaja tahteavaldus koormatud varaga tehingu tegemiseks.

[6] Justiitsministri 19. juuni 2009. a määruse nr 23 „Notariaadimäärustik" muutmise eelnõu ja seletuskiri on leitavad Justiitsministeeriumi avalikust dokumendiregistrist https://adr.rik.ee/jm/dokument/7375024 (06.04.2022).

ametitoimingute ning tehingute loetelu. Alates 6. aprillist 2020. a on notaritel võimalik kaugtõestamise teel teha kõiki tõestamistoiminguid, sealhulgas tõestada kinnisvara võõrandamise lepinguid. Ainukeseks erandiks on keeld kinnitada kaugtõestamise teel abielu sõlmimist ja lahutamist ja teha abielu- ja abielulahutuse kannet perekonnaseaduse ja perekonnaseisutoimingute seaduse alusel. Seega soosib Eesti õigusmaastik digitaalsete dokumentide koostamist. Sealhulgas on Justiitsministeerium võtnud ette nii tsiviil-, haldus- kui kriminaalasjades digitaalsetele kohtutoimikutele ülemineku. Samuti näeb Vabariigi Valitsuse tegevusprogrammi[7] punkt 8.34. ette justiitsvaldkonna digitaliseerimise, sealhulgas süüteomenetluse maksimaalselt digitaalseks viimise.

Kohtuasja toimikut peetakse praegu paberkandjal köidetuna. Justiitsminister on oma määrusega[8] nimetanud tsiviil- ja haldusasjade liigid, kus pabertoimikuid ei moodustata. Kõigis teistes kohtuasjades peetakse aga paralleelselt kahte toimikut, millest õiguslik tähendus on paberkandjal oleval toimikul. Dokumentide vorm on praktikas muutunud ja nii ei ole mõistlik, et pabertoimiku jaoks prinditakse välja nii kohtu enda poolt loodud kui kohtule saadetud elektroonilisi dokumente ning infosüsteemis juba talletatud andmeid.[9] Digitaalset kohtumenetlust on kohtutes osaliselt rakendatud alates 13. märtsist 2017. a., kuid vaid umbes 30% kõikidest kohtuasjadest on kohtutes ilma pabertoimikuta.[10] Seetõttu on Justiitsministeerium koostanud menetlusseaduste muutmise eelnõude väljatöötamiskavatsuse, mille üheks eesmärgiks on anda kõikides tsiviil- ja haldusasjades digitaalsele kohtutoimikule õiguslik jõud ja jätta paberkandjal toimikule vaid informatiivne tähendus.

Samal ajal on ka kriminaalmenetluses käimas üleminek täisdigitaalsele kohtumenetlusele. 5. aprillil 2021 algatas Riigikogu *kriminaalmenetluse seadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse (kriminaalmenetluse seadustiku revisjon) 367 SE* menetluse[11], millega muuhulgas võimaldatakse üleminek täisdigitaalsele kriminaalmenetlusele ning väärteomenetlusele. Ennekõike tähendab see digitaalse kohtutoimiku kasutuselevõttu,

[7] Vabariigi Valitsuse tegevusprogramm 2021-2023. Arvutivõrgus kättesaadav https://valitsus.ee/valitsuse-eesmargid-ja-tegevused/valitsemise-alused/tegevusprogramm (10.04.2022).
[8] Justiitsministri 25.01.2020 määrus nr 7 „Maa-, haldus- ja ringkonnakohtu kantselei kodukord“, RT I, 08.12.2020, 16.
[9] Tsiviilkohtumenetluse seadustiku muutmise seaduse eelnõu väljatöötamise kavatsus. Arvutivõrgus kättesaadav https://adr.rik.ee/jm/dokument/7420901 (06.04.2022).
[10] Samas, lk 6.
[11] Kriminaalmenetluse seadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seadus (kriminaalmenetluse seadustiku revisjon) 367 SE. Arvutivõrgus kättesaadav https://www.riigikogu.ee/tegevus/eelnoud/eelnou/d10291ef-980a-4b1d-8852-bab30d7e25f3/Kriminaalmenetluse%20seadustiku%20muutmise%20ja%20sellega%20seonduvalt%20teiste%20seaduste%20muutmise%20seadus%20(kriminaalmenetluse%20seadustiku%20revisjon) (10.04.2022).

kuid kriminaalmenetluse seadustikku luuakse ka dokumentaalse tõendi mõiste. Eraldi digitaalse tõendi mõiste eriregulatsiooni seadustikku ei planeerita. Oluline on siinkohal ära märkida ka Euroopa Liidu määrus eIDAS[12], millega on keelatud elektroonilist dokumenti lugeda kohtumenetlustes tõenduskõlbmatuks ainuüksi seetõttu, et see on elektroonilisel kujul. Eesti siseriiklikkus õiguses ei ole seda keeldu sätestatud, kuna eIDAS on otsekohalduv.

Kuna infotehnoloogia muutub kiiremini kui head õigusloome tava järgides seadusi muuta jõutakse, tekib õiguslik ja argumenteeritud lahendust vajav probleem: kas digitaalsete andmete kasutamine kohtumenetluses vahetute tõenditena, st ilma kohtuekspertiisita, on üldse võimalik?

Digitaalsete tõendite ja üleüldse digitaalse kohtumenetluse küsimused on väga ajakohased, kuna digitaalses vormis andmete ja seega sündmuste digitaalsete „jälgede“ maht üha kasvab. Infotehnoloogia arengusuundade tõttu on ka Justiitsministeerium prioriseerinud digitaalse kohtumenetluse loomist. Eesti riik püüdleb mitte ainult digitaalsemaks, vaid nutikamaks ja tehnoloogianeutraalseks saamise suunas. Digitaalsetest tõenditest on kirjutanud 2017. aastal Mari Luuk magistritöös „Digitaalsete tõendite kasutamise erisused“. M. Luugi magistritöö on kirjutatud ennekõike prokuratuuri vaatenurgast ning peatub pikemalt pilveandmetöötluse ja rahvusvahelise koostöö küsimustel. M. Luuk jõudis järeldusele, et digitaalsed tõendid ja nende erinevus klassikalistest tõenditest vajab eriregulatsiooni, et tagada ühtne praktika digitaalsete tõendite kasutamisel. Digitaalsetest tõenditest on kirjutanud ka 2018. aastal Gerd Raudsepp magistritöös „Digitaalsete tõendite kogumise ja kasutamise perspektiivikus kriminaalmenetluses“. G. Raudsepa magistritöö keskendub rohkem digitaalkriminalistika küsimustele. G. Raudsepp jõudis oma töös järeldusele, et olemasolev regulatsioon on piisav digitõendite kogumiseks ning kasutamiseks kriminaalmenetluses, kuid toonitas vajadust sätestada kriminaalmenetluse seadustikus eriregulatsioon asitõenditest digitaalse koopia loomiseks, säilitamiseks ning kasutamiseks kohtumenetluses. Võrreldes mainitud töödega on käesolev magistritöö uudne, sest paneb põhirõhu tõendite kasutamisele kohtumenetluse etapis. Samuti on käesolevas magistritöös pööratud tähelepanu süvavõltsingu tehnikatele, mis kujutavad tõsist ohtu digitaalsete tõendite usaldusväärsusele.

Käesoleva magistritöö eesmärk on analüütilist meetodit kasutades hinnata, kas kehtiv regulatsioon võimaldab kasutada digitaalsel kujul andmeid tõenditena kriminaalmenetluses.

[12] EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ. Arvutivõrgus kättesaadav https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32014R0910&from=ET (10.04.2022).

Sealhulgas ei peeta magistritöös digitaalseteks tõenditeks mitte ainult digitaalsel kujul esitatud tõendeid, vaid ka telesilla vahendusel antud ütlusi. Samuti heidab magistritöö pilgu Riigikogu menetluses olevale kriminaalmenetluse seadustiku revisjoni eelnõule ja sellega kaasnevatele muudatusele: kas need mõjutavad digitaalsete tõendite kasutamise võimalusi? Magistritöö hüpoteesiks on et digitaalses vormis andmeid saab kasutada Eesti kriminaalmenetluse seadustiku kohaselt digitaalsete tõenditena ning eriregulatsiooni sätestada ei ole vaja.

Käesoleva magistritöö kirjutamiseks on töö autor töötanud läbi suure hulga rahvusvahelisi ingliskeelseid teadusartikleid, mis on avaldatud usaldusväärsetes andmebaasides. Ingliskeelsed allikaid on kasutatud ennekõike seetõttu, et eestikeelsete teaduslike artiklite hulk digitaalsete tõendite valdkonnas on olematu. Samuti uuris töö autor käesoleva magistritöö koostamiseks sadu Eesti kohtute otsuseid, sh nii esimese kui teise astme kohtuotsuseid, aga ka Riigikohtu lahendeid.

Käesolev magistritöö koosneb kolmest peatükist. Esimene peatükk jaguneb kolmeks alapeatükiks, millest esimene tutvustab infoühiskonna mõju kohtumenetlusele. Teine alapeatükk defineerib digitaalse tõendi mõiste ja selgitab, et digitaalset tõendit kasutakse sünonüümina elektroonilisele tõendile. Kolmas alapeatükk pakub välja digitaalsete tõendite liigitamise võimalusi.

Teine peatükk puudutab digitaalsete tõendite kontrollimist ja jaguneb neljaks alapeatükiks. Esimene alapeatükk räägib tõendite usaldusväärsusest ja sellest, kuidas ajalooliselt on kohtud suhtunud uutel tehnoloogiatel põhinevatesse tõenditesse umbusklikult. Teine alapeatükk puudutab digitaalsete tõendite tervikluse küsimust, st seda, kuidas veenduda, et digitaalses vormis andmeid pole lubamatult muudetud, need on õiged, täielikud, ajakohased ja autentsed. Kolmandas alapeatükis peatub autor digitaalsete tõendite päritolu tuvastamisel ning neljandas digitaalsete tõendite ehtsusel. Kuna digitaalseid tõendeid on lihtsam muuta kui teatud füüsilisi tõendeid (nt paberdokumente), on nende kasutamisel suuremad riskid. Seetõttu on neljandas alapeatükis selgitatud ka süvavõltsingute ohtu digitaalsetele tõenditele.

Kolmas peatükk arutleb digitaalsetest tõenditest Eesti kriminaalmenetluses. See peatükk jaguneb sarnaselt teisele peatükile neljaks alapeatükiks. Esimene alapeatükk uurib, kuidas digitaalses vormis andmeid on võimalik esitada kriminaalmenetluses tõendina. Selleks tuleb hinnata, millise tõendiliigina on võimalik käsitleda digitaalseid dokumente ja millisena metaandmeid ehk andmeid andmete kohta. Teine alapeatükk selgitab, kuidas erineb digitaalsete

tõendite hindamine klassikalise tõendi hindamisest. Kolmandas alapeatükis on töö autor peatunud audiovisuaalses vormis ütluste andmisele. Viimases, neljandas alapeatükis hindab töö autor kriminaalmenetluse seadustiku revisjoni kavandatud mõjusid digitaalses vormis andmete kriminaalmenetluses tõendina kasutamisele. Selleks on neljandas alapeatükis toodud välja käesoleva magistritöö teema jaoks olulisemad kriminaalmenetluse seadustiku revisjoni muudatused ja nende eeldatav mõju. Ennekõike tuleb uurimise alla dokumentaalse tõendi mõiste kavandatud määratlemine kriminaalmenetluse seadustikku.

Magistritööd enim iseloomustavad märksõnad: digitaalsed tõendid, kriminaalmenetlus, tõendid.

1. DIGITAALSETE TÕENDITE OLEMUS

1.1.INFOÜHISKONNA MÕJU KOHTUMENETLUSELE

Kogu maailmas on toimumas digitaalsete muutuste ja ühiskonna digitaliseerimise areng. Inimkond on jõudnud infoühiskonda, kus isikud, organisatsioonid, targad seadmed, teadmised, infosüsteemid ning andmed on ühendatud koosvõimeliseks võrgustikuks, mis suudab piisavalt kiiresti edastada ja töödelda kõiki inimtegevuseks vajaminevaid infokogumeid. Enamikku ühiskonnas talletatud teavet hoitakse, teisendatakse ja edastatakse universaalsel digitaalsel kujul. Üldist andmeedastusvõrku kasutades on juurdepääs teabele kõigil ühiskonnaliikmetel.[13] Interneti üha laiem kasutamine on toonud kaasa ka digitaalsete andmete laialdasema leviku ning analoogkujul dokumentide või muude teabesalvestuste liikumine jääb üha enam minevikku.

Digitaalse revolutsiooni alguses oli juurdepääs internetile avatud üksnes neile, kes töötasid või omasid arvutit. Pärast seda toimus selline tehnoloogiaareng, mille tulemusena said juurdepääsu internetile ka teised seadmed, mis tähendas, et arvuti[14] kasutamine ei olnud enam hädavajalik interneti kasutamiseks.[15] Nüüd on võimalik internetti kasutada igalt seadmelt: alustades tahvelarvutitest ning lõpetades nutikate külmkappideni, mis oskavad poenimekirju koostada ja edastada. Tänaseks mõjutab info- ja kommunikatsioonitehnoloogia (edaspidi *IKT*) inimeste elu ja tegevust paljudel nii kodus kui ka tööl – näiteks suheldes, uudistega tutvudes, meelt lahutades, riigiasutustega suheldes, tasudes arveid või osteldes veebis. Juurdepääsu IKT-le peetakse töö efektiivsuse ja piirkondade konkurentsivõime tõstmise aluseks. IKT võimaldab suuremat paindlikkust töökeskkondadele (nt võimaldades inimestel töötada kodus või teistes kohtades väljaspool kontorit), pakkudes samas laia võimaluste valikut olla kolleegide, pere ja sõpradega ühenduses.[16] Samuti on IKT e-riigi üks olulisi alustalasid, mis võimaldab nii erinevatel riigiasutustel omavahel kui ka kodanike ja ettevõtetega suhelda ning andmeid vahetada.

[13] Praust, V. Infoühiskond ja selle teetähised. Infotehnoloogia haldusjuhtimises. Aastaraamat 1998.
[14] Silmas on peetud vaid lauaarvuteid, hilisemalt ka süle- ja tahvelarvuteid.
[15] Information society. Eurostat regional yearbook 2014. Arvutivõrgus kättesaadav https://ec.europa.eu/eurostat/documents/3217494/5786345/KS-HA-14-001-08-EN.PDF/d713d26a-2272-4500-aa67-cced7e73f2ff (10.04.2022).
[16] Information society. Eurostat regional yearbook 2020, lk 132 Arvutivõrgus kättesaadav: https://ec.europa.eu/eurostat/documents/3217494/11348978/KS-HA-20-001-EN-N.pdf/f1ac43ea-cb38-3ffb-ce1f-f0255876b670?t=1601901088000 (10.04.2022).

Eestis on kasutusel andmete ühekordse küsimise ehk *once only* põhimõte. Eelmainitud põhimõte tähendab, et kui riigil on isiku kohta andmed ühes infosüsteemis olemas, siis ei küsita isikult enam teises infosüsteemis neid samu andmeid. Näiteks kui rahvastikuregistris on olemas andmed alaealise lapse olemasolu, nime ja isikukoodi kohta, ei pea isik enam esitama oma lapse andmeid lapsetoetuse taotlemiseks. Andmed liiguvad siis rahvastikuregistrist otse Sotsiaalkindlustusameti infosüsteemi.

Ühekordse küsimise põhimõtet üritab Eesti ka Euroopa Liidus propageerida, et oleks võimalik andmete liikumine ka liikmesriikide vahel. Piiriülese andmevahetuse värskeima näitena saab tuua Euroopa Komisjoni ettepaneku Euroopa Parlamendi ja Nõukogu direktiivile *mehhanismide kohta, mille liikmesriigid peaksid kehtestama, et hoida ära finantssüsteemi kasutamist rahapesu või terrorismi rahastamise jaoks, ning millega tunnistatakse kehtetuks direktiiv (EL) 2015/849*[17] ehk nn VI rahapesu direktiiv. Direktiiviga soovitakse võimaldada piiriülest andmevahetust rahapesu tõkestamiseks, sidestades omavahel liikmesriikide automatiseeritud keskmehhanismid, mille kaudu saaksid liikmesriikide rahapesu andmebürood piiriülest teavet teises liikmesriigis asuvate panga- ja maksekontode ning hoiulaegaste omanike kohta.[18] Eestis hakkab liikmesriigi keskmehhanismi rolli täitma elektrooniline arestimissüsteem, mille vahendusel liiguvad juba praegu rahapesu andmebüroo päringud krediidiasutustele ning vastused päringutele[19].

Infotehnoloogia areng on jõudnud ka kohtumenetluseni. IKT võimaldab kohtumenetlust muuta efektiivsemaks, tagab menetlusosalistele parema juurdepääsu kohtule ja lihtsustab asjaajamist. Kohtusüsteemide haldamise eest vastutavad isikud pöörduvad üha enam digiteerimise ja tehnoloogiliste lahenduste poole, eesmärgiga parandada õigusemõistmise tõhusust ja kättesaadavust.[20] Näiteks Euroopa Liidus on selleks loodud piiriülene süsteem *e-Justice*

[17] Ettepanek: EUROOPA PARLAMENDI JA NÕUKOGU DIREKTIIV mehhanismide kohta, mille liikmesriigid peaksid kehtestama, et hoida ära finantssüsteemi kasutamist rahapesu või terrorismi rahastamise jaoks, ning millega tunnistatakse kehtetuks direktiiv (EL) 2015/849 ehk nn VI rahapesu direktiiv. COM/2021/423. Arvutivõrgus kättesaadav https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=celex%3A52021PC0423 (10.04.2022).

[18] VI rahapesu direktiivi ettepaneku selgituspunkt 41.

[19] Täitemenetluse seadustiku § 63[1] lg 1 kohaselt on elektrooniline arestimissüsteem infokanal täitemenetlusregistri, maksukohustuslaste registri ja krediidiasutuse infosüsteemi vahel, mille eesmärk on lisaks võlgniku konto arestimisele ja arestide haldamisega seotud toimingute kohta elektrooniliselt taotluse edastamisele krediidiasutusele võimaldada ka päringute tegemist krediidiasutuse valduses olevate andmete kohta ning tagada osapoolte tahteavalduste viivitamatu ja turvaline edastamine. Sama paragrahvi lõikega 2 on lubatud liituda süsteemiga ka valitsusasutustel ja selle valitsemisalasse kuuluvatel asutustel, kes vajavad elektroonilise arestimissüsteemi kasutamist seadusest tuleneva ülesande täitmiseks. Rahapesu andmebürool on seadusest tulenev ülesanne sätestatud rahapesu ja terrorismi rahastamise tõkestamise seaduse § 58 lõikes 1.

[20] Lupo, G., Bailey J. Designing and Implementing e-Justice Systems: Some Lessons Learned from EU and Canadian Examples, Laws 2014, 3. 2014, lk 354. Arvutivõrgus kättesaadav

Communication via Online Data Exchange ehk e-CODEX[21], mille eesmärgiks on pakkuda Üle-Euroopalist juurdepääsu piiriülesele õigusemõistmisele ja kiirendada kohtumenetluste digiteerimist. 2020. aasta detsembris võttis Euroopa Komisjon vastu Euroopa Parlamendi ettepaneku võtta vastu määrus, milles käsitletakse arvutipõhist süsteemi piiriüleste tsiviil- ja kriminaalmenetluste andmete vahetamiseks ehk nn e-CODEXi määruse. Õigusakti ettepaneku eesmärk on arendada e-CODEXit senisest edasi, et tagada selle pikaajaline jätkusuutlikkus, laialdasem kasutamine ja operatiivjuhtimine.[22]

Piiriülese digitaalse infovahetuse jaoks on oluline aga ennekõike see, et ka siseriiklik kohtusüsteem seda võimaldaks. Eesti kohtusüsteem on Euroopa justiitssüsteemide võrdlustabeli *Justice Scoreboard* kohaselt Euroopa Liidu tõhusamate seas eelkõige just kohtuga elektroonilise suhtlemise poolest – see hõlmab nii kohtuasja esitamist kohtule kui ka selle hilisemat käekäiku.[23] Samuti on Eesti kolmandal kohal kohtumenetluse kiiruse[24] poolest, st kui kiiresti kohus ühte kohtuasja lahendab.[25] Lisaks on Eesti esikohal elektroonilise juurdepääsu poolest avalikustatud kohtuotsustele[26] ning kolmandal kohal kohtuotsuste masinloetavaks kättesaadavaks tegemise poolest[27].

Nii efektiivsuse, kiiruse kui ka elektroonilise suhtluse taga on mitmed Eestis nii kohtute kui menetlusosaliste poolt laialdaselt kasutusele võetud arenenud infosüsteemid. 2006. aastal võeti kasutusele „kohtute infosüsteem“ (edaspidi *KIS*), mille eesmärkideks on selle põhimääruse § 2 kohaselt koondada kohtuasjad ühtsesse andmekogusse; töödelda menetlustoimingute andmeid; töödelda elektroonilisi menetlusdokumente; võimaldada kohtuasja andmete automatiseeritud kasutamist menetlusdokumentide ja statistiliste aruannete koostamisel; tagada pidev ülevaade kohtumenetluste käigust; võimaldada kohtute töökoormuse, lahendite analüüsi ja

https://www.researchgate.net/publication/272661563_Designing_and_Implementing_e-Justice_Systems_Some_Lessons_Learned_from_EU_and_Canadian_Examples (10.04.2022).

[21] E-CODEXi veebileht on arvutivõrgus kättesaadav https://www.e-codex.eu/ (10.04.2022).

[22] Ettepanek: EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS, milles käsitletakse arvutipõhist süsteemi piiriüleste tsiviil- ja kriminaalmenetluste andmete vahetamiseks (e-CODEXi süsteem) ning millega muudetakse määrust (EL) 2018/1726. Arvutivõrgus kättesaadav https://eur-lex.europa.eu/legal-content/EN-ET/ALL/?uri=CELEX:52020PC0712 (10.04.2022).

[23] The 2020 EU Justice Scoreboard, European Commission, Luxembourg: Publications Office of the European Union, 2020. Arvutivõrgus kättesaadav https://ec.europa.eu/info/sites/info/files/justice_scoreboard_2020_en.pdf (10.04.2022).

[24] EU Justice Scoreboard'i metoodika on hõlmanud hinnanud siinkohal vaid kõigi mitte-kriminaalasjade menetlemise kiirust. Kriminaalasjade menetlemise kiirust ei ole kokku hinnatud, kuid eraldi on välja toodud rahapesu asjade lahendamise kiirus, milles Eesti on samuti Euroopa Liidus teisel kohal (vt The 2020 EU Justice Scoreboard lk 18).

[25] The 2020 EU Justice Scoreboard, lk 8.

[26] The 2020 EU Justice Scoreboard, lk 26.

[27] The 2020 EU Justice Scoreboard, lk 27.

kohtumenetluste statistiliste ülevaadete tegemist; võimaldada kohtulahendite sisulist analüüsimist ja süstematiseerimist; võimaldada elektrooniliste menetlusdokumentide esitamist ja säilitamist ning teha kohtulahendid arvutivõrgus avalikkusele kättesaadavaks.[28] KIS on seega õigusemõistmise ja kohtute haldamise töövahendiks. KIS vähendab kohtute töökoormust, menetlustoimingute läbiviimiseks ajakulu ja seeläbi otseselt ka menetlustähtaegu.

Menetlusosaliste jaoks on oluline ja kasulik veebipõhine infosüsteem nimetusega „e-toimiku süsteem"[29], mis võimaldab menetlusosalistel ja nende esindajatel esitada kohtule elektrooniliselt menetlusdokumente ja jälgida nendega seonduvat kohtumenetluse käiku.[30] E-toimiku eesmärk on:

1) TsMS § 60[1] lg 1 kohaselt tsiviilkohtumenetluses tagada ülevaade kohtute menetluses olevatest tsiviilasjadest; kajastada andmeid tsiviilkohtumenetluse käigus tehtud toimingute kohta; võimaldada kohtute töö korraldamist; tagada õiguspoliitiliste otsustuste tegemiseks vajaliku kohtustatistika kogumine; võimaldada andmete ja dokumentide elektroonilist edastamist;[31]
2) KrMS § 210 lg 1 kohaselt kriminaalmenetluses tagada ülevaade uurimisasutuste, prokuratuuri ja kohtute menetluses olevatest kriminaalasjadest, samuti alustamata jäetud kriminaalasjadest; kajastada andmeid kriminaalmenetluse käigus tehtud toimingute kohta; võimaldada menetleja töö korraldamist; tagada kriminaalpoliitiliste otsustuste tegemiseks vajaliku kuritegevuse statistika kogumine; võimaldada andmete ja dokumentide elektroonilist edastamist.[32]

Lisaks KIS-ile ja e-toimikule oli Justiitsministeeriumi valitsemisalas aastatel 2018-2021 õigusemõistmise ja õiguskaitse valdkonnas peamiseks planeeritud tegevuseks paberivabale menetlusele ülemineminek (sh kohtuistungite protokollide asendamine helisalvestistega).[33] Ka Justiitsministeeriumi programmis aastateks 2022-2025 on prioriseeritud õigusemõistmist toetavate digilahenduste arendamine[34] ja õigusemõistmise läbipaistvuse tagamine läbi parema

[28] Kohtute infosüsteemi põhimäärus, RT I, 09.10.2020, 6
[29] E-toimiku keskkond on juurdepääsetav arvutivõrgus https://etoimik.rik.ee/index.html (10.04.2022).
[30] E-toimik. Registrite ja Infosüsteemide Keskuse veebileht. Kättesaadav arvutivõrgus: http://www.rik.ee/et/e-toimik (10.04.2022);
[31]Tsiviilkohtumenetluse seadustik, RT I, 22.03.2021, 5.
[32] Kriminaalmenetluse seadustik, RT I, 29.12.2020, 10
[33] Justiitsministeeriumi valitsemisala arengukava aastateks 2018 – 2021, Justiitsministeerium, lk 26. Arvutivõrgus kättesaadav https://www.just.ee/et/ministeerium-kontaktid/arengukavad-ja-tooplaanid (10.04.2022).
[34] Justiitsministeeriumi programmi kohaselt on selleks ette nähtud tegevusteks KIS-i uuenduskuur, kohtuistungi helisalvestuste tekstiks muutmise kõnetuvastustööriista juurutamine ning digitaalsetele kohtutoimikutele üleminek.

digiligipääsu kohtuteabele.[35] Sealhulgas on oluline märkida, et digitaalsele menetlusele üleminek on vajalik kogu süüteomenetluse ahelas. See hõlmab endas muu hulgas mahukate toimingute kiiret läbiviimist läbi innovaatilise tarkvara arendamise ja digitõendite eelistamise, elektroonilisele kriminaaltoimikule üleminekut kui ka kõrgetasemelise ekspertiisi-tehnoloogia kasutamist.[36]

Seega võib öelda, et tehnoloogia areng ja maailma digitaliseerumine on jõudnud ka kohtumenetluse korraldamisse. Lisaks kohtumenetluse digitaliseerimisele on oluline ka see, kuidas menetlusosalistel on võimalik kohtuga suhelda. Kriminaalmenetluse üheks tähtsaimaks alustalaks on kvaliteetsed tõendid, kuna ilma nendeta ei ole võimalik õiglane otsus. Lisaks nn traditsioonilistele tõenditele on digitaalsed tõendid üha suurem osa kohtumenetluses esitatud tõenditest.

[35] Justiitsministeeriumi programm aastateks 2022-2025, lk 18. Arvutivõrgus kättesaadav https://www.just.ee/ministeerium-uudised-ja-kontakt/ministeeriumist-ja-minister/strateegilised-alusdokumendid (23.04.2022).

[36] Justiitsministeeriumi programm aastateks 2020-2023 „Usaldusväärne ja tulemuslik õigusruum“, lk 16-17. Arvutivõrgus kättesaadav https://www.just.ee/et/ministeerium-kontaktid/arengukavad-ja-tooplaanid (10.04.2022).

1.2.DIGITAALSE TÕENDI MÕISTE

Selleks, et digitaalseid tõendeid oleks võimalik kasutada, on mitmed eksperdid üritanud defineerida digitaalse tõendi mõistet. Nagu igal uuel terminil, on ka digitaalse tõendi mõistel mitmeid erinevaid määratlusi. Sisuliselt on digitaalsed tõendid informatsioon, mis on talletatud digitaalsel kujul ja mida on võimalik õiguslikult vastuvõetaval viisil taasesitada. Termineid „elektrooniline tõend" ja „digitaalne tõend" kasutatakse tihti sünonüümidena. Selguse huvides kasutatakse käesolevas magistritöös terminit „digitaalne tõend", mis tähendab igasugust digitaalsel ehk elektroonilisel kujul olevat tõendit, mida talletatakse digitaalsetes seadmetes. Selleks, et digitaalse tõendi tähendusest ja olemusest paremini aru saada, tuleb pöörduda digitaalsete tõendite rahvusvaheliste asjatundjate poole, kes on üritanud seda mõistet defineerida.

1998. aastal defineeris digitaalsete tõendite teaduslik töörühm SWDGE ehk *the Scientific Working Group on Digital Evidence* digitaalse tõendina igasuguse informatsiooni, millel on mistahes tõenduslik väärtus ja mis on salvestatud või edastatud binaarsel kujul.[37] Hiljem muudeti termin „binaarne" „digitaalseks".[38] Digitaalseid tõendeid on Eoghan Casey defineerinud kui „igasugused andmed, mida säilitatakse või edastatakse arvuti abil, mis toetab või lükkab ümber teooria selle kohta, kuidas õigusrikkumine aset leidis või mis käsitleb kuriteo olulisi asjaolusid nagu näiteks tahtlus või alibi."[39] Andmed eelnimetatud definitsioonis on põhimõtteliselt kombinatsioon numbritest [binaarkood tegelikult pole vaid numbrikombinatsioon, vaid teabe kahendarvu-süsteemis kodeerimise vahend – autori täpsustus], mis esindab [millesse on kodeeritud – autori täpsustus] väga erinevat teavet, sealhulgas teksti, pilte, heli ja videot.[40] Seega on nii SWDGE kui Casey digitaalset tõendit defineerinud läbi selle, millisel kujul tõend eksisteerib. Olgu selleks „binaarne" või „numbrite kombinatsioon", silmas on peetud selliseid tõendeid, mis eksisteerivad digitaalsel kujul ja mille tajumiseks peab inimene kasutama mõnda seadet.

---

[37] Whitcomb, C.M.. An Historical Perspective of Digital Evidence: A Forensic Scientist's View. International Journal of Digital Evidence, Spring 2002 Volume 1, Issue 1, 2002. Arvutivõrgus kättesaadav https://www.researchgate.net/publication/2573124_An_Historical_Perspective_of_Digital_Evidence_A_Forensic_Scientist's_View (10.04.2022) .

[38] Scientific Working Group on Digital Evidence (SWGDE). International Organization on Digital Evidence (IOCE). 2002. Arvutivõrgus kättesaadav https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm (10.04.2022)

[39] Casey, E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd Edition. 2011, lk 7.

[40] Casey, E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd Edition. 2011, lk 7.

Stephen Mason ja Daniel Sen on kirjutanud, et „elektroonilise“ tõendi defineerimine ei ole lihtne töö ja nendib, et neid tõendeid on kirjeldatud ka kui „digitaalsed tõendid“ või „arvutitõendid“. Kõik kolm terminit väljendavad mõningaid aspekte sellest, et seda tüüpi tõenditel on mõned eripärad, mis eristavad neid teistest tõendamismeetmetest, kusjuures ka nende eripärade kirjeldamine ei ole lihtne. Infotehnoloogia valdkonna kiire tehnoloogiline areng tähendab, et igasugune kitsalt määratletud definitsioon võib kiirelt vananeda. Seevastu definitsioonid, mis vastupidi on tulevikukindlad, kipuvad olema liiga abstraktsed ning jälgivad traditsioonilise tõendi regulatsiooni kategooriaid.

Seetõttu on Mason ja Seng võtnud lähenemisviisiks juristi vajaduse muuta teatud esemeid – digitaalsed objektid – tõenditeks, mida saab kasutada kohtumenetluses tõendamiseks. Kuigi selline õiguskeskne definitsioon ei pruugi sobituda arvutiteaduste terminoloogiasse, on võimalik luua toimiv definitsioon, mis sobib enamikeks olukordadeks ja eesmärkideks.[41] Seetõttu pakuvad Mason ja Seng välja järgmise digitaalse (ehk elektroonilise) tõendi definitsiooni: „andmed (koosnedes analoogseadmete väljundist või andmetest digitaalsel kujul), mida on muudetud, säilitatud või kommunikeeritud mistahes toodetud seadme, arvuti või arvutisüsteemi poolt või edastatud üle sidesüsteemi, mis võib muuta kummagi poole faktilise olukorra rohkem või vähem tõenäolisemaks kui see oleks ilma tõendita“.[42] Seega lähtuvad Mason ja Seng sellest, et digitaalseks tõendiks saab nimetada kõiki neid andmeid, mis on ühel hetkel olnud digitaalsel kujul – need on kas loodud, muudetud või edastatud mõnes elektroonilises seadmes – ning neid saab ka kasutada tõendamisel. Mason’i ja Seng’i pakutud definitsioon on kergesti mõistetav ja loogiliselt jälgitav, mistõttu on see ka käesoleva töö autori hinnangul kõige selgem digitaalse (elektroonilise) tõendi definitsioon.

Seega on Mason’i ja Seng’i järgi oluline just elektroonilise seadme olemasolu, kus digitaalne tõend on loodud, kus seda on muudetud või mille abil seda on edastatud. Oluline on märkida seda, et elektrooniliste seadmete all peetakse silmas rohkemat kui ainult klassikalised arvutid. Mason ja Seng on selgitanud, et ajalooliselt on terminit „arvuti“ tihti kasutatud kirjeldamaks igat sorti töötlevat seadet.[43] Nüüd on digitaalsed arvutus- ja salvestusruumid iseloomulikud paljudele seadmetele, mis on kaugel traditsioonilistest arvutitest. Sellisteks seadmete hulka

[41] Mason, S., Seng, D. Electronic evidence. Fourth Edition. 2017, lk 18-19. Arvutivõrgus kättesaadav https://humanities-digital-library.org/index.php/hdl/catalog/view/electronicevidence/16/93-1 (10.04.2022).
[42] Mason, S., Seng, D. Electronic evidence. Fourth Edition, lk 19.
[43] Mario Rosentau on kirjutanud, et arvutiks minimaalses tähenduses on mäluga varustatud protsessor, laiemas tähenduses mistahes terviklik riistvara, mille tööd arvutiprogramm protsessori kaudu juhib. M. Rosentau - Intellektuaalse omandi õigused infotehnoloogia valdkonnas. Juridica III/2008, lk 171.

kuuluvad mh mängukonsoolid, igasugune „kantav tehnoloogia“ (nt aktiivsusmonitorid ja spordikellad), targad koduseadmed (nt nutikad energiamõõturid, automatiseeritud keskküttesüsteemid).[44] Lisaks võimaldavad digitaalseid tõendeid salvestada arvuti kõvakettad, välised kõvakettad, USB pulgad, mälukaardid, CD-d, DVD-d, mobiilid, PDA-d (*personal digital assistent* ehk pihuarvutid), flopikettad, traadita võrgu pääsupunktid jpm.[45]

Ka üha populaarsemad nuti- ja spordikellad ning muud treeningut jälgivad trenniseadmed talletavad ja edastavad nii palju andmeid, et ühe sellise seadme kogutud ja pilve esitatud andmete pinnalt on võimalik teha järeldusi seda kandva isiku tegutsemisest. Kuna nutiseade on pikki perioode isiku küljes, suudab see tema kohta koguda väga palju andmeid. Näiteks avaldas treeningute jälgimise rakendus *Strava* kogemata salajaste Ameerika Ühendriikide armee baasid. Nimelt avaldas *Strava* 2017. aasta novembris kaardi kolme miljardi GPS andmepunktiga, mis moodustus kasutajaandmetest. Kuna kaardile oli kantud kõikide kasutajate andmed, sisaldas see ka tundlikku infot sõjaväelaste kohta, kes olid kasutanud *Strava*t oma jooksutreeningute jälgimiseks. Seega olid kaardile kantud ka sõjaväelaste jooksuringid muuhulgas Afganistanis, Djiboutis, Iraanis ja Süürias, kus ainukesteks rakendust kasutavateks inimesteks olid sõjaväelased ja seetõttu jäid detailsed sõjaväebaasid kaardile ka väga detailselt.[46]

Kokkuvõtteks: digitaalseks tõendiks võib pidada andmeid, mille tajumiseks inimese poolt tuleb neid vaadelda mõne elektroonilise seadme kaudu (digitaalses vormis) või on need andmed digitaalsel kujul mingil hetkel olnud – sisuliselt on neid kas loodud, muudetud või edastatud elektroonilise seadme kaudu. Lisaks on andmete tõendiks lugemise puhul oluline just tõendamise faktor: andmetega peab saama tõendada faktilisi asjaolusid.

[44] Mason, S., Seng, D. Electronic evidence. Fourth Edition, lk 1.
[45] Craiger, P. Training and Education in Digital Evidence, Handbook of Digital and Multimedia Forensic Evidence. 2008, lk 14.
[46] Fitness tracking app Strava gives away location of secret US army bases. The Guardian, 2018. Arvutivõrgus kättesaadav https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases (10.04.2022).

1.3.DIGITAALSETE TÕENDITE LIIGID

Kuna digitaalsete tõendite mõiste definitsioone on mitmeid, on neid võimalik ka kategoriseerida erinevaid meetodeid kasutades. Näiteks on Mason ja Seng jaotanud digitaalsed tõendid selle järgi, kust neid on võimalik koguda.

Esiteks on võimalik neid koguda elektroonilistest seadmetest. See, et digitaalseid tõendeid on võimalik koguda elektroonilistest seadmetest, ühtib ka eelmises alapeatükis kirjeldatud Mason'i ja Seng'i digitaalse tõendi definitsiooniga. Mason ja Seng on toonud loetelu erinevatest tõenditüüpidest, mida saab koguda digitaalsetest seadmetest.

1. Failid – arvutites, sülearvutites, tahvelarvutites ja mobiiltelefonides kasutatakse erinevat tarkvara, sealhulgas programme, mis võimaldavad kasutajal saata sõnumeid, koostada tabeleid, andmebaase ja tekstidokumente, teha digitaalseid fotosid ning luua multimeediat ja esitlusi. Need failid, mis sisaldavad eelnimetatud andmeid, võivad olla elektroonilised tõendid.[47]
2. Koopiad – igasugune kohtuekspertiis algab selle seadme „kopeerimisega", millel võivad asuda digitaalsed tõendid. Kopeerimise protseduur on mittedestruktiivne protsess, mis loob kõigist seadmes asuvatest andmetest täpse digitaalse koopia. Seejärel uuritakse koopiat, mitte originaalseadmes olevaid andmeid.[48]
3. Süsteemi ja programmi logid - enamikus kaasaegsetes operatsioonisüsteemides nagu *Windows* ja *Linux* salvestatakse logidena praktiliselt kõik, mis süsteemis ja süsteemiga toimub. See hõlmab teavet süsteemi sündmuste kohta, sealhulgas rakenduste käivitamise ja erinevate veateadete klasside kohta.[49]
4. Ajutised failid ja vahemälufailid - kui arvuti ühendub internetiga, luuakse ja salvestatakse lokaalselt mitmesugust informatsiooni selle tegevuste, sh külastatud veebisaitide ja vaadatud sisu kohta. Selleks, et brauser saaks kasutajakogemust paremaks muuta ja sirvimist kiirendada, salvestatakse külastatud veebisaitide ajutised koopiad vahemälukaustadesse. Need kaustad sisaldavad fragmente veebilehest, sealhulgas pilte ja teksti.[50]

[47] Mason, S., Seng, D. Electronic evidence. Fourth Edition, lk 7.
[48] Mason, S., Seng, D. Electronic evidence. Fourth Edition, lk 7-8.
[49] Mason, S., Seng, D. Electronic evidence. Fourth Edition, lk 8.
[50] Mason, S., Seng, D. Electronic evidence. Fourth Edition, lk 8-9.

5. Kustutatud failid – faili kustutamise korral arvutist kustutatakse viide faili asukohale, kuid mitte fail ise. Sel põhjusel on enamikel juhtudel võimalik taastada kustutatud andmeid.[51]
6. Mobiilseadmete failid – tahvelarvutid ja nutitelefonid ühendavad endas personaalarvuti funktsionaalsuse telefoni ja kaameraga. Sellised seadmed on arvutid, kuna neil on protsessor, mälu, klahvistik või mikrofon (sisend) ning ekraan või kõlar (väljund). Sarnaselt arvutitele on ka mobiilseadmetel ROM [*read-only memory* ehk püsimälu – autor] ja RAM [*random-access memory* ehk muutmälu – autor].[52]

Kuna elektroonilised seadmed on omavahel ühendatud teiste seadmetega või võrguga, toodab ka võrguühendus elektroonilisi tõendeid. Nendeks on arvutite ja serverite logid, veebilehtede vaatamise ja failide edastamise ajalugu. Võib ette tulla olukordi, kus kätte on saadavad vaid võrgus paiknevad tõendid, sest kuriteo toimepanija ise hävitas või edukalt veenis ohvrit tõendeid hävitama kõvaketta ja muu riistvara hävitamisega.[53] Sellisteks võrguühendusteks võivad Mason'i ja Seng'i kohaselt olla internet, intranetid, juhtmevabad võrgud (WiFi) ning mobiilsidevõrgud.

Lisaks võrkudele on võimalik tõendeid koguda ka võrgurakendustest. Näiteks e-kirjad on väga oluline tõendite allikas, kuigi tuleb meeles pidada, et e-kirja saatja saab väga lihtsasti varjata oma isikut. Lisaks saavad digitaalse tõendi allikaks olla kiirsõnumid, võrdõigusvõrgud (P2P-võrgud ehk *peer-to-peer* võrgud) ja ka sotsiaalvõrgustikud (üles laetud videod, pildid, blogid ja interaktiivsed suhtlused liikmete vahel).[54]

Seega eristavad Mason ja Seng digitaalsete tõendite kategooriaid sõltuvalt sellest, kust on neid võimalik koguda: elektroonilisest seadmest, võrgust ja võrgurakendusest kogutavad tõendid. Mason ja Seng ei seo seega digitaalseid tõendeid nende loojaga, vaid pigem nende asukohaga.

Digitaalseid tõendeid on võimalik kategoriseerida ka tõendi looja järgi. ÜRO uimastite ja kuritegevuse büroo on läbi „haridus õiguse eest" ehk E4J initsiatiivi[55] loonud moodulid

[51] Mason, S., Seng, D. Electronic evidence. Fourth Edition, lk 9.
[52] Mason, S., Seng, D. Electronic evidence. Fourth Edition, lk 10.
[53] Mason, S., Seng, D. Electronic evidence. Fourth Edition, lk 11.
[54] Mason, S., Seng, D. Electronic evidence. Fourth Edition, lk 11-17.
[55] E4J initsiatiivi kohta on võimalik lähemalt lugeda ÜRO uimastite ja kuritegevuse büroo veebilehelt https://www.unodc.org/e4j/en/tertiary/index.html (28.02.2021).

ülikoolis õpetamiseks. Küberkuritegevuse eriala digitaalse kohtuekspertiisi moodulis[56] on kolm digitaalse tõendi kategooriat:

1. Sisu, mille on loonud üks või mitu inimest. Kasutaja loodud sisu on lubatud tõend, kui see on usaldusväärne ja kindel, st seda on võimalik seostada konkreetse isikuga. Nendeks on kõik sellised digitaalsed andmed, mille inimene on loonud teadlikult mõne seadme abil. Siia alla kuuluvad nii kasutaja loodud failid, näiteks fotod või e-kirjad, kui ka sellised failid, mille süsteem on loonud selle tagajärjena, et inimene on kunagi seadistanud seadme midagi tegema. Selliseks näiteks on turvakaamerad, autode pardakaamerad ja muud salvestusseadmed.
2. Sisu, mille on loonud arvuti või elektrooniline seade ilma kasutaja sisendita – nt andmelogid. Seadme loodud sisu saab lubada tõendina, kui on võimalik näidata, et seade toimis andmete loomise ajal korralikult, ja kui on võimalik näidata, et andmete loomise ajal olid andmete muutmise vältimiseks olemas andmeturbe mehhanismid.
3. Sisu, mis on loodud mõlema – arvuti ja inimese – kombinatsioonis – nt Microsoft Exceli tabelid, mis sisaldavad kasutaja sisestatud andmeid ja tarkvara poolt tehtud arvutusi. Kui sisu on loodud inimese ja seadme poolt, tuleb kindlaks teha mõlema usaldusväärsus.[57]

Eelnevast liigitusest tulenevalt on oluline täiendavalt rääkida sisust, mille on loonud arvuti või digitaalne seade ilma kasutaja sisendita. Selle all on silmas peetud eelkõige metaandmeid ehk andmeid andmete kohta. Selleks, et selgitada, mis on metaandmed, on kõige lihtsam selgitada seda, tuues paralleeli paberdokumendiga. Paberdokumendi puhul oleksid otsesteks metaandmeteks dokumendi pealkiri, kuupäev, selle kirjutanud ja vastu võtnud isikute nimed ning dokumendi asukoht. Kaudseteks metaandmeteks oleksid teksti fondi tüüp (rasvane, alakriipsutatud või kursiivis), samuti dokumendi asukoha markeering ja dokumendi sildid, mis viitavad sellele, kuidas seda dokumenti on võimalik kasutada, näiteks kas see on konfidentsiaalne dokument.[58]

Kõik elektroonilisel kujul olevad failid sisaldavad endas ka metaandmeid ühel või teisel viisil, sh e-kirjad, arvutustabelid, veebisaidid ja tekstitöötlusdokumendid. Mason'i ja Seng'i sõnul peabki elektrooniline dokument omama ka metaandmeid, et oleks võimalik tõlgendada

[56] Oluline on siinkohal märkida, et samasugust digitaalsete tõendite liigitust õpetatakse ka Tartu Ülikooli infotehnoloogiaõiguse eriala aines „Digitaalsed tõendid, küberkriminalistika ja küberkuritegevus" (OIAO.01.047).
[57] E4J University Module Series: Cybercrime. Module 4: Introduction to Digital Forensics. Digital evidence.
[58] Mason, S., Seng, D. Electronic evidence. Fourth Edition, lk 27.

dokumendi eesmärki.[59] Metaandmed on seega teave, mis tekib siis, kui kasutatakse erinevaid infotehnilisi lahendusi ja süsteeme ning mis annab teada, kes, mida, kus, millal ja kuidas tegi.[60]

Metaandmed ütlevad digitaalse dokumendi kohta järgmist: millal ja kuidas dokument loodi (väidetav aeg ja kuupäev); failitüüp; väidetava autori nime (ehkki see ei pruugi olla usaldusväärne); asukoht, kust fail avati või kuhu see salvestati, kui fail viimati avati (väidetav kellaaeg ja kuupäev); millal seda viimati muudeti; millal fail viimati salvestati; millal seda viimati välja prinditi; dokumendi väidetavad eelmised autorid; faili asukoht igal salvestamise korral; üksikasjad selle kohta, kes veel võivad sellele juurde pääseda ja e-posti korral pimekoopia (ingl. k *BCC*) aadressid.[61]

Kokkuvõtteks: digitaalseid tõendeid on võimalik liigitada mitmel moel. Näiteks selle järgi, kust neid on võimalik koguda: olgu selleks siis elektroonilised seadmed, võrgud või võrgurakendused. Samas on digitaalseid tõendeid võimalik liigitada ka selle järgi, kes selle tõendi on loonud: on selleks inimene või arvuti. Lisaks on eraldi kategoorias metaandmed, mis on sisuliselt andmed andmete kohta ja annavad võimalikku lisateavet mõne digitaalse dokumendi kohta.

[59] Mason, S., Seng, D. Electronic evidence. Fourth Edition, lk 27.
[60] Andmekaitse Inspektsioon, Metaandmed ja privaatsus Juhis organisatsioonidele1 ja kodukasutajale seaduse rakendamisel. 2015, lk 4. Arvutivõrgus kättesaadav https://www.aki.ee/et/node/1661 (10.04.2022).
[61] Mason, S., Seng, D. Electronic evidence. Fourth Edition, lk 27.

2. DIGITAALSETE TÕENDITE KONTROLLIMISE ERISUSED

2.1.DIGITAALSETE TÕENDITE USALDUSVÄÄRSUS

Kuigi suulist ja hiljem ka kirjalikku tõendusmaterjali on kohtumenetlustes kasutatud juba sajandeid, on kohtud pidanud hakkama harjuma ka sellise tõendusmaterjaliga, mida näiteks 50 aastat tagasi oli keeruline ette kujutada. Dokumendid pole enam vaid arvutites, nende abil või nende poolt automaatselt genereeritud, vaid suur hulk elektroonilisi andmeid on jõudnud ka kohtutesse.[62] Ameerika Ühendriikides, mis oli 20. sajandi üks kiireima arenguga riike, koostati föderaalsed tõendite kasutamise reeglid enne arvutite, e-kirjade, interneti ja digitaalsete kaamerate jõudmist tavaliste ameeriklaste ellu –1960ndatel aastatel.[63] Huvitaval kombel on aga need reeglid (kuigi üldised) üsna hea raamistik ka digitaalsete tõendite kasutamisel.[64] See annab märku, et ka 60 aastat tagasi olid digitaalsed tõendid juba kohtutesse jõudnud või jõudmas, mistõttu nende kasutamise reguleerimine oli juba tollal päevakorral.

Ajalugu on täis näiteid sellest, kuidas kohtud reageerivad selliste tõendite vastuvõtmisele, mis tuginevad uutel tehnoloogiatel.[65] Näiteks 1899. aasta kohtuotsuses asjas *Cunningham v. Fair Haven & Westville R. Co* kirjeldab kohus, kuidas hageja üritas kohtuasjas tõendina esitada fotot. Nimelt oli Westville'i raudtee-ettevõte hooletusest lubanud raudteerööbastel mitu tolli sõidutee pinnast välja ulatuda ja seetõttu juhtus selles kohas ka õnnetus. Hageja esitas kohtule tõendina umbes kuu enne õnnetuse toimumist tehtud foto tänavast, kuhu oli peale jäänud ka õnnetuspaik. Foto esitamise eesmärk oli näidata tee väga halba seisukorda. Kohus leidis, et kunstniku oskuste puudumise, puudulike instrumentide või materjalide, või tahtliku ja oskusliku manipuleerimise tõttu võib foto olla mitte ainult ebatäpne, vaid ka ohtlikult eksitav.[66]

Hiljem on kohtud kahtlevalt suhtunud ka näiteks helisalvestistesse[67]. Iga sellise uue tehnoloogia saabumisega on esialgne vastuseis ja järeleandmatus asendunud lõpuks vastumeelse

[62] Goode, S. The Admissibility of Electronic Evidence. Review of Litigation, Vol. 29, Issue 1. 2009, lk 2.
[63] Goode, S. The Admissibility of Electronic Evidence, lk 2.
[64] Goode, S. The Admissibility of Electronic Evidence, lk 3.
[65] Goode, S. The Admissibility of Electronic Evidence, lk 4.
[66] *Cunningham v. Fair Haven & Westville R. Co*, Supreme Court of Connecticut Third Judicial District, New Haven, June Term, Aug 1, 1899. Arvutivõrgus kättesaadav https://casetext.com/case/cunningham-admx-v-fair-haven-westville-r-co (27.04.2022).
[67] Näiteks 1934. aastal arvas kohus *State v. Simon*, 174 A. 867, 872 (N.J. Sup. Ct. 1934) – arvutivõrgus https://casetext.com/case/state-v-simon-72, asjas helisalvestise kohta, et pole teada ühegi sellist juhtumit, kus väidetava vestluse fonograafi salvestis oleks tunnistatud kohtus tõendiks.

heakskiiduga. Nõuded selliste tõendite vastuvõtmisele olid aga kõrged Seejärel, kui kohtud harjusid uute tehnoloogiatega ära, lõdvendati ka uut tüüpi tõendite aktsepteerimise nõudeid.[68]

1999. aasta kohtuasjas *St. Clair v. Johnny's Oyster & Shrimp, Inc*.[69] oli hagejaks meremees, kes sai kehavigastusi kostjale kuuluva laeva peal töötades. Kostja vaidles vastu, et temale see laev ei kuulu. Vastuseks üritas hageja tõendina esitada internetist (Ameerika Ühendriikide Rannavalve laevade andmebaasist) saadud andmeid, mis tõendaks, et laev kuulub siiski kostjale. Kohus leidis, et hageja elektroonilised tõendid on täiesti ebapiisavad, et kostja väiteid ümber lükata. Kohus ütles oma kohtuotsuses, et suhtub internetti kui ühte suurde kuulujuttude, vihjete ja valeinformatsiooni katalüsaatorisse. Kohus leidis, et see nn „võrk" ei paku ühtegi moodust, kuidas kontrollida seal paikneva teabe tõepärasust ja seetõttu jääb püsima eeldus, et internetist avastatud teave on oma olemuselt ebausaldusväärne. Igaüks võib midagi internetti panna, sest ühegi veebilehe sisu ei kontrollita. Lisaks saavad häkkerid võltsida iga veebisaidi sisu igas kohas ja igal ajal. Nendel põhjustel pole internetist hangitud tõendid peaaegu mitte millegi jaoks piisavad ja seda isegi tõendite vastuvõtmise reeglite kõige liberaalsema tõlgenduse korral. Kohus lõpetas oma mõttekäiku tõdemusega, et internetist saadud nn „*voodoo* informatsioonile" ei tasu tugineda.

Vaatamata eelkirjeldatud mõtteavaldustele on kohtud liikunud edasi selles suunas, et digitaalsed tõendid võivad teatud juhtudel siiski olla usaldusväärsed. Terminit „usaldusväärsus" kasutatakse sageli selleks, et kirjeldada, kas miski väärib olla usaldatud. Usaldusväärsuse põhimõttel on kaks kvalitatiivset mõõdet: usaldatavus (ingl. k *reliability*) ja ehtsus (ingl. k *authenticity*). Usaldatavus tähendab, et kirje suudab seista faktiliste asjaolude eest, mida see tõendab. Autentsus tähendab, et kirje on see, mida ta väidab olevat.[70] Füüsilise dokumendi ehtsust saab tõendada selliste omadustega nagu originaalsus, rikkumata olek ja kontrollitud päritolu. Kuigi digitaalne tõend on väga erinev paberist, on tõendite usaldusväärsuse hindamiseks välja kujunenud reeglid ka elektroonilistele tõenditele väga asjakohased.[71]

Digitaalseid tõendeid on võimalik lihtsasti muuta, kahjustada ja hävitada, mis on ka nende eripära võrreldes nn tavaliste tõenditega. Lisaks saavad digitaalsed tõendid paikneda rohkem

[68] Goode, S. The Admissibility of Electronic Evidence, lk 4.
[69] St. Clair v. Johnny's Oyster & Shrimp, Inc., US District Court for the Southern District of Texas - 76 F. Supp. 2d 773 (S.D. Tex. 1999). Arvutivõrgus kättesaadav https://law.justia.com/cases/federal/district-courts/FSupp2/76/773/2370358/ (27.04.2022).
[70] Mason, S., Seng, D. Electronic evidence. Fourth Edition, lk 193
[71] Mason, S., Seng, D. Electronic evidence. Fourth Edition lk 193.

kui ühes kohas korraga: näiteks võib e-kiri olla samaaegselt nii saatja kui saaja arvutis kui ka internetiteenuse pakkuja valduses. Isegi kui digitaalsete tõendite usaldusvääruses on põhjendatud kahtlus, ei muuda see tõendeid tingimata lubamatuks, vaid vähendab kohtu poolt antud kaalu.[72] Täiendavalt tõusetuvad digitaalse tõendi puhul lisaks tõendi usaldusväärsuse hindamise argumentidele ka andmete tervikluse, ehtsuse ja usutavuse küsimused.

2.2.DIGITAALSETE TÕENDITE TERVIKLUS

Digitaalsete tõendite kasutamisel kohtumenetluses on oluline tuvastada ka, kuidas tõendiga on ümber käidud. Kui eksisteerib võimalus, et digitaalseid tõendeid oleks keegi saanud vääralt käsitleda või kui need oleks võinud sattuda volitamata inimese kätte, tuleb kahelda tõendite tervikluses.[73] Andmete, sh digitaalsete tõendite terviklus tähendab seda, et neid andmeid ei ole muudetud, need on õiged, täielikud ja autentsed.

Digitaalse tõendi terviklust saab hinnata mitmel moel. Esiteks andmete terviklus, mis tähendab, et andmeid ei ole muudetud kas tahtlikult või kogemata ilma nõusolekuta. Andmete terviklus tugineb bititerviklusel, st mitte ainult bittide, vaid ka nende järjestuse õigsusel. Analoogkeskkonnas võib dokument kuluda loetamatuks, kuigi see säilitab sisu ja andmed samas järjekorras, kui need esimest korda andmekandjale nn kinnitati [nt trükiti – autor]. Seevastu digitaalmaailmas, kui algsed bitid on järjestatud näiteks 101, on edastatav väärtus 5, kuid järjestuse muutmisel 110-ks, on väärtus 5 ning 011-ks on väärtus 3. Samadel bittidel on seega erinev väärtus, kui nende järjestus muutub. Seega tähendab tervikluse kaotus erinevat [uut] sisu.[74]

Teiseks digitaalse tõendi tervikluse hindamise viisiks on dubleerimise terviklus, mis tähendab, et andmetest duplikaadi tegemine ei muuda andmeid ning duplikaat on identne bitikoopia esialgsetest andmetest. [75]

Kolmandaks oluliseks digitaalse tõendi tervikluse tüübiks on arvuti terviklus (ka süsteemi terviklus), mis tähendab, et arvuti (või süsteem) toodab õigeid tulemusi, kui seda kasutatakse

[72]Casey, E. Digital evidence and computer crime, lk 69.
[73] Shah, M. S. M. B; Saleem, S. ja Zulqarnain, R. Protecting Digital Evidence Integrity and Preserving Chain of Custody, Journal of Digital Forensics, Security and Law: Vol. 12 , Article 12. 2017, lk 121
[74] Duranti, L., Rogers, C. Trust in digital records: An increasingly cloudy legal area. Computer Law & Security Review, Volume 28, Issue 5, 2012, lk 525-526.
[75] Duranti, L., Rogers, C. Trust in digital records: An increasingly cloudy legal area, lk 526.

õigesti, ja tegu seda ja tõendi loomisel. Arvuti ja süsteemi tervikluse kindlakstegemiseks tuleb veenduda, et 1) arvutitele, võrkudele, seadmetele või salvestusruumidele loata või tuvastamata juurdepääsu vältimiseks on rakendatud piisavad turvameetmed ja 2) stabiilsed füüsilised seadmed säilitavad andmete väärtuse, kuni nad on volitatud andmeid muutma: seda saab tagada kasutajate ja nende õiguste haldusega, paroolide, tulemüüride ja süsteemilogide säilitamisega.[76]

Neljandaks ja viimaseks digitaalse tõendi tervikluse tüübiks on protsessi terviklus, mis tähendab tõendite kogumise, taastamise, tõlgendamise ja esitlemise õiguslike nõuete järgimist. Protsessi tervikluse hindamine põhineb kahel põhiprintsiibil: mittesekkumise põhimõte ja sekkumise tuvastatavuse põhimõte. Esimene tähendab, et digitaalsete andmete kogumiseks ja analüüsimiseks kasutatud meetod ei muuda digitaalseid üksusi; teine tähendab, et kui andmete kogumine ja analüüsimine muudab üksusi, on muudatused tuvastatavad.[77]

Kui tutvuda eelmistes lõikudes loetletud tervikluse tüüpidega, võime tuua paralleele Eestis kasutusel oleva infosüsteemide kolmeastmelise etalonturbe süsteemiga ISKE[78], mis kasutab turvamudelit, mis toetub kolme osaeesmärgi (käideldavuse, tervikluse ja konfidentsiaalsuse) tagamisele.[79] Neist kolmest osaeesmärgist on käesoleva alapeatüki kontekstis olulised kaks: terviklus ja konfidentsiaalsus. ISKE järgi on andmete terviklus andmete õigsuse, täielikkuse ja ajakohasuse tagatus ning päritolu autentsus ning volitamatute muutuste puudumine. Andmete konfidentsiaalsus on aga andmete kättesaadavus ainult selleks volitatud kasutajatele (isikutele või tehnilistele süsteemidele) ning kättesaamatus kõigile ülejäänutele.[80]

Tõendi tervikluse hindamisel on kõige mõistlikum keskenduda digitaalsele tõendile endale, et leida muutmise ja muude kahjustuste tagajärgi[81], ja mitte tõendi dubleerimisele või tõendi loonud arvutile (või süsteemile). Seda põhjusel, et arvuteid (süsteeme) on erinevaid, nende keerukus ja pidev areng muudab esimese hindamisviisi väga vaevarikkaks. Selleks, et kõiki arvuteid (süsteeme) ning nende normaalset toimimist hinnata, on vaja ebamõistlikult suurt

[76] Duranti, L., Rogers, C. Trust in digital records: An increasingly cloudy legal area, lk 526.
[77] Duranti, L., Rogers, C. Trust in digital records: An increasingly cloudy legal area. Computer Law & Security Review, Volume 28, Issue 5, 2012, lk 525-526.
[78] ISKE on mõeldud andmekogude pidamisel kasutatavate infosüsteemide ja nendega seotud infovarade turvalisuse saavutamiseks ja säilitamiseks. ISKE kasutamine ja kohaldamine on reguleeritud Vabariigi Valitsuse 20.12.2007 määrusega nr 252 „Infosüsteemide turvameetmete süsteem".
[79] Infosüsteemide kolmeastmelise etalonturbe süsteemi ISKE rakendusjuhend, lk 8.
[80] Infosüsteemide kolmeastmelise etalonturbe süsteemi ISKE rakendusjuhend, lk 9.
[81] Casey, E. Digital evidence and computer crime, lk 61.

hulka spetsialiseerunud tööjõudu. Täiendav keerukus arvuti hindamisel on see, et isegi arvuti (või süsteem), mis on muidu usaldusväärne, võib teatud olukordades vigaselt talitleda.[82]

Protsessi tervikluse tõendamisel on ääretult oluline, et info, mis on tõendist kogutud, on õige ja täpne esitus andmetest, mis esialgu tõendites sisaldus.[83] Selleks peab digitaalse tõendi kogumisel, käsitlemisel ja analüüsimisel käituma selliselt, et see ei põhjusta kahtlusi tõendi tõepärasuses. Oluline on digitaalsete tõendite käitlusahel (ingl. k *chain of custody*)[84]: korrektne käitlusahel näitab, et digitaalne tõend on omandatud konkreetsest süsteemist või asukohast ning et seda on pidevalt pärast selle kogumist kontrollitud. Seega võimaldab korrektne käitlusahela dokumenteerimine siduda kohtul digitaalsed tõendid kuriteoga. Puudulik dokumentatsioon võib põhjustada segadust digitaalsete tõendite hankimise kohas ja tekitada kahtlusi digitaalsete tõendite usaldusväärsuses. Tervikluse dokumenteerimine võimaldab demonstreerida, et digitaalset tõendit pole selle kogumisel ja uurimisel muudetud.[85]

2.3.DIGITAALSETE TÕENDITE PÄRITOLU

Tavalise dokumendi päritolu on võimalik tuvastada selle koostaja käekirja ja muude tõendite kaudu. Digitaalne tõend toob kaasa aga selle riski, et digitaalse faili võib luua võltsidentiteediga, mida on tõenäoliselt võimatu tuvastada või leida tõelist autorit. Näiteks võib e-kirja saata kolmandale isikule kellegi teise isiku nime või konto alt, mille tulemuseks on esialgse saatja tuvastamine keerulisem. Digitaalsed tõendid pole nagu sõrmejäljed või DNA, mida saab kasutada isiku tuvastamiseks. Pärast uurimist saab küll digitaalsest tõendist teada, millist arvutit kuriteo toimepanemiseks kasutati, kuid ei selgu toimepanija isik.[86] Näiteks on võimalik tuvastada arvuti, milles paikneb digitaalne tõend, kuid on keeruline selgitada välja, kas digitaalne tõend on siiski selle arvuti kasutaja poolt loodud või on see sinna paigutatud teiste sama arvuti kasutajate poolt või sootuks edastatud teisest arvutist.[87]

[82] Casey, E. Digital evidence and computer crime, lk 62.
[83] Nilsson, J.D, Digital Evidence in the Courtroom. Nova Science Publishers. 2010, lk 21.
[84] Terminit „käitlusahel“ kui ingliskeelse termini „*chain of custody*“ tõlget kasutatakse eesti kirjanduses harva, kuid seda on mainitud kriminaalmenetluse seadustiku ja teiste seaduste muutmise seaduse eelnõu seletuskirjas.
[85] Casey, E. Digital evidence and computer crime, lk 60.
[86] Chih-ping, C. Knowledge Production from Social Networks Sites. Using Social Media Evidence in the Criminal Procedure, lk 57.
[87] Chih-ping, C. Knowledge Production from Social Networks Sites. Using Social Media Evidence in the Criminal Procedure, lk 57

Ühendkuningriikide kohus arutas kohtuasja *Regina v Weiner*[88], mis sai alguse anonüümsest telefonikõnest politseile, milles teatati, et ühe kooli majapidaja oli seotud lapspornograafia levitamisega. Paar kuud hiljem sai politsei ka CD-ketta, mille analüüsimisel selgus, et see sisaldab tõesti pilte lastest. Seejärel teatas helistaja, et CD kettal asuvad pildid on alla laetud kooli majapidaja arvutist. Samal kuul arreteeris politsei kooli majapidaja ja konfiskeeris tema arvuti. Kooli majapidaja eitas kõiki süüdistusi ja väitis, et helistaja on esitanud valesüüdistuse ja ise lisanud need pildid arvutisse: nimelt on helistajal juurepääs tema arvutile. Lisaks polnud kooli majapidajal erilisi arvutioskusi, mistõttu oli võimalik lihtsasti näha tema arvutiparooli, kui ta seda sisestas.

Läbivaatuse tulemusena leiti arvutist 177 pilti lastest, kusjuures paljud pildid olid peidetud failidena. Lisaks olid pildid süsteemi loodud pooleteise minuti jooksul, mis andis märku sellest, et need failid olid arvutisse toodud teisest meediaallikast. Samuti paistsid need olevat eraldatud tavapärasest arvuti kasutamisest ning ei olnud ühtegi tõendit, mis vihjaks sellele, et tavaline arvuti kasutaja oleks pääsenud nendele failidele juurde. Politsei jõudis järeldusele, et failid lapspornograafiaga olid lisatud kooli majapidaja arvutisse kolmanda isiku (helistaja) poolt ilma kooli majapidaja teadmiseta. Ka kohus leidis, et failid asusid arvutis selliselt, et kooli majapidaja ei saanud neid ise leida ega kogemata kustutada. Kohus lisas ka, et kuigi politsei suutis seekord tuvastada failide arvutisse lisaja, oleks saanud kooli majapidaja ka ekslikult süüdi mõista.

Loomulikult on ka traditsioonilisi tõendeid võimalik paigutada süütu inimese teadmiseta tema elu-või asukohta ja seejärel esitada kuriteoteade. Samuti on võimalik esitada valeütlusi, näiteks vägistamise või kehalise väärkohtlemise kohta,[89] Kohtumenetluse käigus on süüdistataval võimalik esitada kaitseteese: nt et isik viibis süüteo toimepanemise ajal mujal, ta oli süüteo toimepanekuks sunnitud, ta viibis hädakaitseseisundis, kuriteo on sooritanud hoopis kolmas, senises menetluses tuvastamata isik, tema suhtes on esitatud fabritseeritud valetõendeid jne. Kõik need argumendid on suunatud nn põhjendatud kahtluse tekitamisele, mis peaks juhul, kui

[88] *Regina v Weiner* [2011] EWCA Crim 1249, [2012]. England and Wales Court of Appeal (Criminal Division), Apr 7, 2011. Arvutivõrgus kättesaadav https://www.casemine.com/judgement/uk/5a8ff70360d03e7f57ea5a58 (27.04.2022)

[89] Näiteks pöördus 2019. aastal 27-aastane naine Tartu ülikooli erakorralise meditsiini osakonda väitega, et sai tänaval peksa. Naise silm oli tõepoolest sinine ning lisaks tuvastati tema kehalt veel mõned väiksemad vigastused. Politsei alustas võimalike kurjategijate tabamiseks kriminaalmenetlust ja uurija kuulas kannatanu üle. Politsei jätkas tõendite kogumist ja tõendeid analüüsides jõuti järeldusele, et sellist kuriteosündmust ei toimunud. Kuna naine väitis, et teda ründasid kaks tundmatut meest, kuid seda tegelikult ei juhtunud, esitas prokuratuur kaebajale süüdistuse hoopis valeütluste andmises. Kohus mõistis naise valeütluste andmises ka süüdi. https://tartu.postimees.ee/6981555/kohus-moistis-vaidetava-runnaku-ohvri-valeutluste-andmises-suudi (04.04.2021).

konkreetne argument (või argumentide kogum) on tõsiseltvõetav ning seda ei suudeta tõenduslikult kummutada, viima edasiselt *in dubio pro reo* põhimõtte (KrMS § 7 lg 3) rakendamiseni ning potentsiaalselt ka õigeksmõistva otsuse tegemiseni või kriminaalmenetluse lõpetamiseni.[90]

Seega võib tekkida ka digitaalsete tõendite esitamisel kohtul või riiklikul süüdistajal vajadus kulutada aega või ressurssi, et kõrvaldada esitatud tõendite päritolu kohta esitatud kahtlusi. Digitaalsete tõendite puhul võib vaja minna ekspertide abi, sest kohtunikud ja süüdistajad ei pruugi omada piisavaid tehnilisi teadmisi digitaalse tõendi hindamiseks. Traditsiooniliste tõendite korral on kohtul võimalik lähtuda oma siseveendumusest ja tööpraktikast ning seeläbi hinnata, kas mõni väide või järeldus on eluliselt usutav või mitte.

2.4. DIGITAALSETE TÕENDITE EHTSUS

Digitaalsete tõendite ehtsus tähendab seda, et tõend kujutab endast tõesti seda, mida ta kujutama peaks ja tõendab õigesti seda, mida ta konkreetses kohtuasjas peab tõendama. See tähendab, et digitaalset tõendit pole muudetud, rikutud või võltsitud.

Tõendite rikkumisega kaasnevad ohud ei eksisteeri vaid digitaalsete tõendite puhul, kuid üldiselt usutakse, et digitaalseid tõendeid on lihtsam muuta ja rikkuda kui füüsilisi tõendeid. Näiteks on erialakirjanduses öeldud, et digitaalne tõend on vähem käegakatsutav (ingl. k *tangible*), väga muutlik ja lihtsamini rikutav kui füüsiline tõend. Samuti on öeldud, et digitaalseid andmeid saab soovi korral muuta ja sõltuvalt muutja oskustest võib muudatus jääda märkamatuks, hoolimata digitaalse kohtuekspertiisi ekspertide pädevusest ja varustusest.[91] Näiteks on tükk maad keerulisem hävitada või moonutada verist nuga, kui manipuleerida mõne olulise faili metaandmeid.[92]

Nagu iga tõendiga, võib ka digitaalsete tõendite muutmine viia valede järeldusteni. Näiteks leiab uurija kahtlustatava arvutist konkreetse kirje veebibrauseri ajaloost, millest võib järeldada, et mõni selle arvuti kasutaja on külastanud seda veebisaiti. Vahel võib see aga tähendada, et

[90] RKKKo 3-1-1-77-15, p 17.
[91] Schneider, J., Wolf, J., Freiling, F. Tampering with Digital Evidence is Hard: The Case of Main Memory Images. Forensic Science International: Digital Investigation, Volume 32. 2020, lk 51. Arvutivõrgus kättesaadav https://www.sciencedirect.com/science/article/pii/S2666281720300196 (21.03.2021).
[92] Lin. X. Introductory Computer Forensics. A Hands-on Practical Approach, Wilfrid Laurier University Waterloo, ON, Canada. 2018, lk 18.

seda veebisaiti ei ole sellest arvutist kunagi kasutatud, vaid selle asemel on brauseri ajalugu muudetud ja lisatud teadlikult selle veebisaidi külastamisest märk eesmärgiga viia uurija valele järeldusele.[93]

Digitaalseid tõendeid saab muuta mitmesuguse tarkvara abil, mis on lihtsasti internetis leitav. Tõendi võltsimist või muutmist on keeruline tuvastada. See tähendab, et digitaalseid tõendeid ei ole mitte ainult lihtne muuta, vaid ka muudetud tõendi muutmise fakti ennast on keeruline avastada.[94] Mida algelisemat meetodit digitaalse tõendi muutmiseks kasutatakse, seda lihtsam on seda muutmist ka avastada. Näiteks on väga lihtne muuta kelleltki saabunud e-kirja sisu kontoritarkvaras, et seda muudetud kujul edasi saata. Sellist võltsimist on ka väga lihtne tuvastada. Samuti on pilditöötlusprogrammiga töödeldud fotode tuvastamiseks võimalik kasutada mitmeid erinevaid internetis leiduvaid fotoanalüüsi programme, mille algoritmid tuvastavad uuritaval fotol kõik muudetud alad.

Üheks kõige ohtlikumaks ja suurima mõjuga digitaalsete tõendite tervikluse ohuks on aga üha arenev süvavõltsingu (ingl. k *deep fake*[95]) tehnoloogia, mis paneb kohtuid ja ka kohtueelseid menetlejaid tõsiste probleemide ette. Digitaalse tehnoloogia areng muudab ehtsa ja võltsi (audio- ja/või visuaal-) meedia eristamise üha keerulisemaks. Kõigile tuttav *Adobe Photoshop* proramm, millega on võimalik manipuleerida fotosid selliselt, et need ei sarnane ligilähedaseltki originaalile, on sundinud meid kahtlema piltide tõepärasuses juba aastakümneid.[96] Filmitööstus kasutab järjest võimsamat tehnoloogiat, et tuua ekraanile fantaasiamaailmu. Seda väga kulukat tehnoloogiat nimetatakse CGI-ks (ingl. k *computer generater imagery* ehk arvutiga genereeritud kujutis). Üks värskemaid tehnoloogiaid, mis süvendab, mis aitab kaasa ehtsa ja võltsi eristamise probleemi, on süvavõltsing. See tehnoloogia kasutab tehisintellekti (AI-d, ingl. k *artificial intelligence*), et kujutada kedagi pildil või video ütlemas ja tegemas midagi, mis pole kunagi juhtunud. Tihti, kuid mitte alati, on süvavõltsingus võltsitud nii isiku näoilmeid kui ka häält. [97]

---

[93] Schneider, J., Wolf, J., Freiling, F. Tampering with Digital Evidence is Hard, lk 51.

[94] Chih-ping, C. Knowledge Production from Social Networks Sites. Using Social Media Evidence in the Criminal Procedure. Studiorum Università di Bologna. Dottorato di ricerca in Law, science and technology, 29 Ciclo. 2018, lk 55. Arvutivõrgus kättesaadav http://amsdottorato.unibo.it/8304/

[95] *Deepfake* on kohversõna, mis on saanud nime sõnapaarist „*deep learning*" ehk sügavõppest (masinõppe meetod) ja „*fake*" ehk võlts, võltsing. „EKI ühendsõnastik 2020" annab sõnale *deepfake* eestikeelse vastena „sõvavõltsing", defineerides selle kui „tehisintellekti vahenditega tehtud võltsing, nt foto- või videomanipulatsioon". Vt lähemalt https://sonaveeb.ee/search/unif/dlall/dsall/s%C3%BCvav%C3%B5ltsing/1 (14.03.2021).

[96] Adobe Photoshop loodi 1998. aastal ja sai kiiret pilditöötluse standardiks.

[97] Westerlund, M. The Emergence of Deepfake Technology: A Review. Technology Innovation Management Review. November 2019 (Volume 9, Issue 11), lk 39. Arvutivõrgus kättesaadav https://www.researchgate.net/publication/337644519_The_Emergence_of_Deepfake_Technology_A_Review (14.03.2021)

Häält on võimalik võltsida mitmel moel. Esimene neist on kirjutatud teksti hääleks muutmine. Selleks kas asendatakse olemasolev heli uuega või luuakse sootuks uus heli, trükkides teksti, mille tehisintellekt ette loeb. Viimase puhul on tegemist kõnesüntesaatoriga[98]. Kõnesüntesaatorist võimsam tööriist on hääle võltsimine, millega muudetakse kellegi häält või asendatakse ühe inimese hääl teise omaga. Selleks esitatakse salvestised inimese häälest algoritmile, mis lõikab need ääretult väikesteks katkenditeks ning tõstab need vastavalt soovitule ümber. Tulemuseks on heli, kus kõlab, nagu inimene ütleks lauseid, mida ta tegelikult öelnud ei ole.[99] Süvavõltsingu heli on võimalik kasutada kas eraldiseisvana või koos videoga.

Süvavõltsingu video on tehisintellekt või masinõpperakendus, mis ühendab, kombineerib, asendab ja lisab pilte ja videoklippe üheks videos, luues seeläbi võltsi video, mis näib ehtne.[100] Olemasolevad süvavõltsingu tehnoloogiad on pidevalt täienemas ning suurim osa praegustest visuaalse domeeni süvavõltsingutest on sellised, mille käigus inimese nägu on asendatud kellegi teise näoga.[101]

Esimene süvavõltsingu video ilmus internetti üsna hiljuti, alles 2017. aasta detsembris, kui anonüümne *Reddit'i*[102] kasutaja nimega Deepfake hakkas postitama võltse, kuid realistlikuna näivaid pornograafilise sisuga videoid kuulsustest. 2018. aasta jaanuaris oli süvavõltsingu tehnoloogia kättesaadav juba kõigile, kui tasuta allalaetavaks muutusid mitmed rakendused.[103] Sellest hetkest alates on süvavõltsingu tehnoloogia muutnud videote usaldusväärsuse suure kahtluse alla. Tehnoloogia, mis loob neid videoid, on disainitud pidevalt oma jõudlust parandama. Algoritm, mis loob võltse videoid, õpib ja täiustab videoid, jätkates pidevalt isiku

[98] Eestikeelne kõnesünteesikeskkond on olemas näiteks Eesti Keele Instituudi veebilehel https://www.eki.ee/heli/ (14.03.2021). Ingliskeelse näitega on Ameerika Ühendriikide ettevõtte Descript loonud lahenduse nimega Overdub mis võimaldab kasutada realistlikku ingliskeelset häält oma kirjutatud teksti ettelugemiseks. Overdubi on võimalik testida Descrpiti veebilehel https://www.descript.com/overdub (14.03.2021).

[99] Nüüdseks juba kolm aastat vana õpetlik video on leitav YouTube'i platvormilt: https://www.youtube.com/watch?v=cQ54GDm1eL0. Selles videos jäetakse esialgu mulje, et endine Ameerika Ühendriikide president Barack Obama ütleb lauseid, mida ta tegelikult kunagi ei ütleks. Video lõpus avalikustatakse, et algoritm kasutab Barack Obama häält ja nägu, kuid näoilmete ja jutu sisendiks on video näitleja Jordan Peel'ist.

[100] Maras, M-H., Alexandrou, A. Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos. The International Journal of Evidence & Proof. 2019, Vol. 23(3), lk 255. Arvutivõrgus kättesaadav https://journals.sagepub.com/doi/10.1177/1365712718807226 (12.03.2021).

[101] Kietzmann, J., Lee, L.W., McCarthy, I.P., Kietzmann, T.C. Deepfakes: Trick or treat? Business Horizons. 2020, 63, lk 137. Arvutivõrgus kättesaadav https://www.sciencedirect.com/science/article/abs/pii/S0007681319301600 (12.03.2021).

[102] *Reddit* ehk www.reddit.com on veebileht ja sotsiaalne võrgustik, kuhu igaüks võib postitada ning teised kasutajad saavad postitusi kommenteerida ja hinnata.

[103] Tänaseks on tasuta rakendusi niivõrd palju, et avaldatud on suisa parimaid tasuta süvavõltsingu rakendusi soovitavaid artikleid.

näoilmete, žestide, hääle ja eripärade matkimist. See muudab videoid üha rohkem realistlikumaks. Ühel hetkel ei ole neid videoid enam palja silmaga võimalik ehtsatest videotest eristada.[104]

Süvavõltsingu näitlikustamiseks lõi käesoleva töö autor eksperimendi korras ise, kasutades Internetis vabalt kasutatavat ja allalaadimist mittevajavat tarkvara https://deepfakesweb.com/ (edaspidi *Deepfakesweb*).[105] Näide illustreerib, kuidas harilik arvutikasutaja saab ilma eriteadmisteta ise süvavõltsingu videot luua. Ka käesoleva töö autor ei ole varasemalt süvavõltsingu videot loonud. Töö autor valis süvavõltsingu objektideks Tanel Kiige ja Kaja Kallase. Sellise näite valis töö autor neljal põhjusel. Esiteks on tegemist kuulsate Eesti inimestega, keda kõik käesoleva töö lugejad teavad. Teiseks, vaatamata sellele, et mõlemad on poliitikud, on nad hetkel võimul oleva valitsuse liikmed ja nende poliitilised seisukohad ei ole vastandlikud[106]. Kolmandaks on nad erinevast soost, mis teeb süvavõltsingu huvitavamaks. Neljandaks on originaalvideod mõlemast YouTube'i platvormil vabalt kättesaadavad[107], et lugejal oleks võimalik kõrvutada süvavõltsingut originaaliga. Valminud süvavõltsing on leitav YouTube'i platvormilt aadressil https://www.youtube.com/watch?v=JK0y7Ncl4Ss.[108]

Tavapärane video süvavõltsimise protsess näeb välja selline, et algoritmile esitatakse salvestisi kahe inimese kohta, algoritm õpib ja vahetab inimeste näod. Teiste sõnadega, süvavõltsingud kasutavad näo kaardistamise tehnoloogiat ja tehisintellekti, et vahetada ära inimeste näod.[109] Töö autori kasutatud Kaja Kallase ja Tanel Kiige näite puhul läbiti süvavõltsingu saamiseks kolm sammu:

1. Kaja Kallase nägu kujutav osa eraldati esialgsest videoklipist;

[104] Maras, M-H., Alexandrou, A. Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos, lk 256.
[105] Süvavõltsingu loomiseks sisestas töö autor otsingumootorisse www.google.com otsingusõna „*deepfake generator*" ja avas otsingutulemuste esimese vaste, milleks oli https://deepfakesweb.com/. *Deepfakesweb* lehel tuleb esmalt kasutajaks registreerida ja seejärel saab üles laadida kaks videot: üks video inimesest A ja üks video inimesest B. Lisaks on võimalik kummastki inimesest laadida üles kuni 1500 pilti. Seejuures on oluline märkida, et kui inimesest A tuleb kindlasti üles laadida video, siis inimesest B võib üles laadida kas video või vähemalt 100 pilti.
[106] Käesoleva magistritöö eesmärk ei ole poliitiliste seisukohtade kujundamine. Süvavõltsingu loomisega ei ole töö autor väljendanud oma poliitilist arvamust.
[107] Tark majandus - Kaja Kallas | Riigikogu valimised 2019. Arvutivõrgus kättesaadav https://www.youtube.com/watch?v=Ua-GKFmxS7Q ning Sotsiaalminister Tanel Kiik. Arvutivõrgus kättesaadav https://www.youtube.com/watch?v=zRdjWvN_Hoc (10.04.2022).
[108] Video ei ole avalik, vaid selle vaatamiseks peab teadma täpselt aadressi (ingl. keeles *unlisted*).
[109] Westerlund, M. The Emergence of Deepfake Technology: A Review, lk 40.

2. seda pilti kasutati sisendina sügavas närvivõrgus (DNN, ingl. k *deep neural network* on masinõppe ja tehisintellekti valdkonna tehnika), genereeriti samasugune pilt, millel kuvati hoopis Tanel Kiike;
3. genereeritud nägu sisestati seejärel originaalpildile, et luua süvavõltsinguga video.[110]

Käesoleva töö autori loodud süvavõltsingu video puhul on näha, et originaalvideos on inimese nägu selgelt nähtav – video kvaliteet on piisavalt hea, et näha on kõiki näo detaile. Näha on sellele inimesele eripäraseid jooni. Süvavõltsingu videos on aga võltsitud näo kvaliteet kehvem, see on udusem ning detaile on vähem. Silmades ei ole võimalik eristada pupilli ja vikerkesta. Kogu ülejäänud kaadri kvaliteet on aga endisel tasemel.

Kokkuvõtvalt on süvavõltsingu loomise näite pinnalt võimalik järeldada, et süvavõltsingu video tegemise võimalus on kättesaadav ja tehtud lihtsaks ka eriteadmisteta inimestele. Vaja on vaid kahte hea kvaliteediga videot, kus mõlemad inimesed on suurema osa ajast näoga otse kaamera poole. Näitena kasutas töö autor kahte väga erineva näoga inimest, et kontrast kahe näo vahel ning võltsing oleks võimalikult lihtsasti tuvastatav. Oht tulemuse kuritarvitamisele tekib siis, kui asendatakse kahe võrdlemisi sarnase isiku näod, kuna sellisel juhul on võltsing usutavam. Kuna loodud süvavõltsingu video kvaliteet on võrdlemisi hea, võib seda, et tegemist on võltsinguga, märgata vaid tähelepanelik vaataja.

Süvavõltsingutel on kohtumenetlusele nii otsene kui kaudne mõju. Otsese mõjuna põhjustavad süvavõltsingud kohtutele täiendavat töökoormust. Sellisteks on kohtuasjad, mis käivad süvavõltsingute endi kohta, näiteks sellised, kus süvavõltsingu video on kahju hüvitamise nõude aluseks. Üheks selliseks tuntumaks näiteks on 2019. aasta kaasus, kus kurjategijad kasutasid süvavõltsingu tehnoloogiat ettevõtte tegevdirektori hääle võltsimiseks. Ühendkuningriigis asuva energiaettevõtte tegevjuht arvas, et ta rääkis telefoni teel oma ülemusega (Saksamaal asuva emaettevõtte juhiga), kes palus tal kanda 220 000 eurot Ungari tarnijale. Ülekanne tehtigi. Helistaja rõhus, et tegemist on kiireloomulise asjaga, nõudes ülekande tegemist juba tunni jooksul. Huvitav oli asjaolu, et Ühendkuningriigis asuva ettevõtte tegevjuht tundis võltsitud hääles ära oma ülemuse saksa aktsendi ja tema hääle eripärad. Seega oli tegemist küllaltki hea võltsinguga. Tegevjuht hakkas kahtlustama, et midagi on valesti, alles seetõttu, et kurjategijad muutusid ahneks ja soovisid täiendava rahasumma ülekandmist.[111]

[110] Kietzmann, J., Lee, L.W., McCarthy, I.P., Kietzmann, T.C. Deepfakes: Trick or treat?, lk 138.
[111] Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case. The Wall Street Journal, 2019. Arvutivõrgus kättesaadav https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402 (10.04.2022),

Kaudselt mõjutavad süvavõltsingud kohtuid aga seeläbi, et mängivad toetavat rolli vaidlustes, mida süvavõltsingud ise ei põhjustanud. Nendel juhtudel ei ole väidetav süvavõltsing see, mis põhjustas kohtuasja, vaid süvavõltsing on vaid üks tõend kohtumenetluses, kus on juba esitatud videotõendeid.[112] Kuna kriminaalasjades esitatakse tõenditena üha enam videosalvestisi, on süvavõltsingute oht üha reaalsem.[113]

Kohtumenetluses esitatud tõendeid saab süvavõltsingutega manipuleerida selleks, et mõjutada kohut otsustama ühes või teises suunas. Süvavõltsingud võivad tõendamise kontekstis esineda mitmel viisil. Keegi võib (teadlikult) võltsida video spetsiaalselt kohtumenetluseks, et seda kohtus esitada tõe pähe. Näiteks esitas 2020. aastal Ühendkuningriigis (küll tsiviilkohtumenetluse käigus) hooldusõiguse vaidluse käigus laste ema kohtule tõendina süvavõltsingu helifaili. Võltsitud heli jättis mulje, et laste isa oli teda telefoni teel ähvardanud. Olukord lahenes, kuna laste isa esindajal õnnestus kätte saada fail ja tutvuda selle metaandmetega, mistõttu oli võimalik tuvastada, et faili oli manipuleeritud. Ühendkuningriigis oli tegemist esimese teadaoleva süvavõltsingu esitamisega kohtule.[114]

Samuti võib esitada kohtus tõendina kellegi teise koostatud süvavõltsingu, teadmata, et see on tegelikult võltsing.[115] Samuti võivad süvavõltsingud levida juba enne menetlust pahatahtlikult või kogemata näiteks sotsiaalmeedia vahendusel ja sellega jätta mulje, et tegemist on tõega, mistõttu ei pruugita kohtumenetluses piisavalt kahelda nende tõepärasuses. Näiteks võib süüdistatava kaitsja väita mõne (tegelikult tõese) tõendina esitatud video puhul on tegemist süvavõltsinguga. Sellisel juhul võib tekkida olukord, kus süüdistaja peab hakkama kasutama keerukat tehnoloogiat, et tõendada, miks tema esitatud video on siiski usaldusväärne ja tõene. See võib endaga kaasa tuua asjatu ressursikulu: nii tööjõu- kui ka otseselt rahalise kulu, mis kaasneb vajamineva tehnoloogia soetamisega – eriti kuna süvavõltsingu tehnoloogia areneb pidevalt.

---

[112] Pfefferkorn, R. "Deepfakes" in the Courtroom, 2021, Boston University Public Interest Law Journal . Summer2020, Vol. 29 Issue 2, lk 253-254. Arvutivõrgus kättesaadav https://siliconflatirons.org/publications/deepfakes-in-the-courtroom/ (10.04.2022).

[113] Riigi Teataja kohtulahendite otsingu kohaselt kasvas maakohtute tehtud jõustunud kohtulahendites videosalvestiste kui tõendite mainimine 4 protsendilt 2010. aastal (8041 jõustunud lahendis mainiti videosalvestisi 346 korral) 15 protsendile 2020. aastal (4373 jõustunud lahendis mainiti videosalvestisi 641 korral).

[114] Doctored audio evidence used to damn father in custody battle. The Telegraph, 2020. Arvutivõrgus kättesaadav https://www.telegraph.co.uk/news/2020/01/31/deepfake-audio-used-custody-battle-lawyer-reveals-doctored-evidence/ (10.04.2022).

[115] Pfefferkorn, R. "Deepfakes" in the Courtroom, lk 255.

Kokkuvõtvalt tuleb esiteks digitaalse tõendi usaldusväärsuse kontrolliks läbida kolmeastmeline kontroll. Teiseks tuleb veenduda digitaalse tõendi tervikluses. See sisaldab nii andmete, koopiate, arvuti (süsteemi) kui ka protsessi terviklust. Kolmandaks tuleb teha kindlaks digitaalse tõendi päritolu ja kummutada kõik selle kohta esitatud kahtlused. Neljandaks peab veenduma digitaalse tõendi ehtsuses. Suurt ohtu tõendite ehtsusele kujutavad süvavõltsingud, mille kiire levik ja areng sunnivad kahtlema ka tegelikult ehtsates digitaalsetes tõendites.

3. DIGITAALSED TÕENDID EESTI KRIMINAALMENETLUSES

3.1.DIGITAALSETE TÕENDITE ESITAMINE KRIMINAALMENETLUSES

Kehtiv kriminaalmenetluse seadustiku (edaspidi *KrMS*) § 63 lg 1 defineerib tõendit väga üldiselt ja selle kohaselt on tõendiks kahtlustatava, süüdistatava, kannatanu, tunnistaja või asjatundja ütlus, ekspertiisiakt, eksperdi antud ütlus ekspertiisiakti selgitamisel, asitõend, uurimistoimingu, kohtuistungi ja jälitustoimingu protokoll või videosalvestis, samuti muu dokument ning foto või film või muu teabetalletus[116]. KrMS § 63 lg 2 lubab kriminaalmenetluse asjaolude tõendamiseks kasutada ka loetlemata tõendeid, välja arvatud juhul, kui on tegemist kuriteo või põhiõiguse rikkumise teel saadud tõendiga[117]. KrMS § 63 lg 2 ei tähenda, et oleks kohtu otsustada, mida ta lisaks seaduses sätestatud tõendite loetelule loeb veel tõenditeks, kuidas ta neid tõendeid hindab ja mida ta konkreetse tõendiga tunnistab tõendatuks. KrMS § 63 lg-s 2 sätestatu kohaselt on vaid lubatud sama paragrahvi esimeses lõikes loetlemata tõendiliike kasutada väga kitsalt vaid menetluse enese kulgu puudutavate asjaolude tuvastamiseks. Menetluse kulgu puudutavateks asjaoludeks on näiteks menetlustähtaegade järgimist, menetlejate pädevust, mingi menetlustoimingu lubatavust jne puudutavad asjaolud.[118]

KrMSis ei sisaldu tõendite absoluutselt kinnist loetelu, sest kriminaalmenetluslike asjaolude tuvastamiseks võib tõendina kasutada ka sellist teabekandjat, mida § 63 lg 1 loetelus ei sisaldu või mis ei vasta päriselt § 63 lg-s 1 loetletud tõendivormi suhtes kehtivatele nõuetele.[119] Ilmselt on seadusandja lugenud enesestmõistetavaks, et antud kriminaalasja raames on tegelikult tõendiga tegemist vaid siis, kui mingis lubatavas tõendivormis esinev teave käib kõnealuse kuriteo kohta. [120]

Digitaalsete tõendite kasutamisel on oluliseks ka otsekohalduv Euroopa Parlamendi ja Nõukogu Määrus (EL) nr 910/2014 *e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ*[121] ehk eIDAS.

[116] Kriminaalmenetluse seadustik § 63 lg 1
[117] Kriminaalmenetluse seadustik § 63 lg 2
[118] RKKKO 3-1-1-105-06, p 11
[119] Kergandberg, E., Pikamäe, P. Kriminaalmenetluse seadustik. Komm vlj. Tallinn: Kirjastus Juura, 2012, lk 218.
[120] Kergandberg, E., Sillaots, M. Kriminaalmenetlus, lk 168. 2
[121] Euroopa Parlamendi ja Nõukogu Määrus (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ, mis võeti vastu 23.07.2014. Arvutivõrgus kättesaadav https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32014R0910&from=ET

Eelmainitud määrusega on keelatud lugeda kohtumenetluses tõenduskõlbmatuks muuhulgas nii e-allkirja[122], e-ajatemplit kui ka e-dokumenti vaid seetõttu, et need on elektroonilisel kujul. Eeltoodu tähendab, et Euroopa Liidu õigusega on selgelt keelatud tõendina välistada elektroonilisel kujul dokumendid. Täiendavalt on oluline märkida, et e-allkirja ei tohi tõenduskõlbmatuks lugeda aktsepteerida ka siis, kui see ei vasta kvalifitseeritud e-allkirjadele esitatavatele nõuetele. Seetõttu võib asuda seisukohale, et kohtumenetluses tuleb tõendina arvestada ka dokumente, mis on allkirjastatud ka sellise elektroonilise allkirjaga, mis ei vasta eIDAS artikli 3 punktis 12[123] sätestatud kvalifitseeritud e-allkirja nõuetele ning kui seadusest ei tulene tehingule vorminõuet.

Selleks, et teha kindlaks, kas digitaalseid andmeid või dokumente on võimalik esitada digitaalsete tõenditena kohtumenetluses, tuleb kõigepealt hinnata, kas digitaalsed dokumendid saavad üldse vastata KrMSis sätestatud tõendi mõistele. Eraldi vajavad käsitlemist metaandmed: kas ka need on KrMSi mõttes tõendid.

3.1.1. Digitaalsete tõendite kategoriseerimine tõenditena

KrMSis ei ole erisätteid digitaalsete tõendite kohta, vaid tõendi mõiste kehtivas seaduses on küllaltki üldsõnaline, jättes ruumi kaaluda, kas see hõlmab ka digitaalseid tõendeid. Jaanus Tehver on 2016. aastal nentinud, et erisätete puudumine KrMSis iseenesest ei välista digitaalsete tõendite kasutamist tõendamiseseme asjaolude tuvastamisel, kuivõrd KrMS § 63 lg 1 loetletud tõendite liigid on piisavalt üldised hõlmamaks ka vähemalt valdavat enamikku digitaalseid tõendid.[124] Tehver on toonud välja, et temale teadaolevalt ei ole praktikas seni tekkinud olukorda, kus mõni digitaalne tõend oleks osutunud kriminaalmenetluses lubamatuks sel põhjusel, et see ei vasta KrMS § 63 lg 1 sätestatud tõendi tunnustele.[125]

Digitaalsed tõendid on teoreetiliselt võimalik kategoriseerida nn rangeks tõendiks ehk KrMS § 63 lõikes 1 loetletud tõendiliigiks, mitte nn vabatõendiks ehk KrMS §63 lõikes 2 nimetatud teabeliigiks.[126] Riigikohus on sedastanud, et salvestised ei pea olema igal juhul olema

[122] eIDAS artikkel 25
[123] eIDAS artikli 3 punkti 12 kohaselt on kvalifitseeritud allkiri täiustatud e-allkiri, mis antakse kvalifitseeritud e-allkirja andmise vahendi abil ja mis põhineb e-allkirja kvalifitseeritud sertifikaadil.
[124] Tehver, J. Digitaalsete tõendite kasutamise võimaldamine, mai 2016, lk 1. Arvutivõrgus kättesaadav http://www.just.ee/sites/www.just.ee/files/digitaalsed_toendid_j._tehver.pdf (04.03.2021).
[125] Tehver, J. Digitaalsete tõendite kasutamise võimaldamine, lk 2.
[126] Eristuse rangete ja vabatõendite vahel on teinud Eesti õiguses Riigikohus kohtuasjas nr 3-1-1-142-05 (p 10), aga neid termineid kasutatakse ka saksakeelses kohtumenetlusalases kirjanduses, kus on toodud terminid „range

salvestatud menetleja poolt, vaid selleks võivad olla ka varasemad, menetlejale üle antud või menetleja poolt muul viisil saadud salvestised. Nimelt on Riigikohtu kriminaalkolleegium 29.10.2015 otsuses kohtuasjas nr 3-1-1-83-15 p 9 öelnud, et KrMS § 63 lg-s 1 kohaselt on seadusandja salvestiste kui iseseisva tõendiliigi all pidanud eeskätt silmas uurimistoimingute käigus tehtud ning nende toimingute käiku ja tulemusi kajastavaid salvestusi, mis kokkuvõttes vormistatakse vastava uurimistoimingu protokolli lisana ja mille seos kriminaalasjaga nähtub selle protokolli tekstist. Samas ei ole välistatud aga seegi, et tõendite kogumisel võtavad menetlejad isikutelt ära mitmesuguseid varem saadud salvestisi või siis annavad erinevad isikud selliseid salvestisi menetlejaile üle omal initsiatiivil. Sellised salvestised saavad sõltuvalt nende sisust olla käsitatavad kas asitõenditena või dokumentidena ja nende vormistamisel tuleb järgida KrMS III peatüki 9. jaos sätestatut.[127]

Kohus on näiteks lugenud asitõenditeks haiglas tehtud fotod kannatanu kehavigastustest CD-plaadil ja turvakaamera salvestised DVD-plaatidel[128]; poe turvakaamera videosalvestised CD-plaatidel ja DVD-plaatidel[129]; selvepesula valvekaamera salvestiste koopiad DVD plaadil[130]. Kohus on lugenud asitõenditeks ka muid faile, nt mobiiltelefonist leitud failid koos andmetega CD-plaadil[131]: tekstifaile, milles sisalduvad omakorda pildid, ja pahavarale viitavaid faile, mis on salvestatud kõvakettale[132]; ja ka näiteks arvuti kõvakettast tehtud koopia ning sellest vaatluse käigus leitud arve blanketi faili[133].

Lisaks on kohtud lugenud tõenditeks ka e-kirjavahetust[134]. E-kirjade puhul on oluline märkida, et kui pildi- ja videofailide puhul eristatakse menetleja tehtud jäädvustusi kellegi teise tehtud jäädvustustest, siis e-kirjad on ainult menetlusosaliste endi loodud. Küsimus on tõstatatud vaid selle kohta, kas e-kirju, mis on kättesaadavad veebikeskkonnas (nt Google mail) või arvutis käivitatud programmi kaudu, võib võtta ära vaid menetleja või võib seda teha ka näiteks kannatanu.

tõend“ ehk *Strengbewess* ja „vabatõend“ ehk *Freibewess*. Viimane on toodud välja Eerik Kergandbergi ja Meris Sillaotsa kriminaalmenetluse õpikus, lk 170.

[127] RKKKo 3-1-1-83-15, p 9.

[128] Pärnu Maakohtu otsus kriminaalasjas nr 1-19-4150 (23.04.2020).

[129] Harju Maakohtu otsus kriminaalasjas nr 1-19-883 (25.11.2019).

[130] Tartu Ringkonnakohtu otsus kriminaalasjas nr 1-17-6611 (31.01.2019).

[131] Harju Maakohtu otsus kriminaalasjas nr 1-19-883.

[132] Tallinna Ringkonnakohtu otsus kriminaalasjas nr 1-14-1938 (15.07.2014).

[133] Pärnu Maakohtu otsus kriminaalasjas nr 1-10-90 (28.08.2013).

[134] Nt Viru Maakohtu kohtuotsus kriminaalasjas nr 1-19-4802 (21.08.2020), Harju Maakohtu kohtuotsus kriminaalasjas nr 1-18-1038 (19.05.2020), Tartu Ringkonnakohtu kohtuotsus nr 1-18-10464 (30.04.2020) ja paljud teised.

Kohtuasjas nr 1-17-2359 vaidles süüdistatava kaitsja kassatsioonkaebuses, et süüdistatava e-posti kontolt kannatanu poolt süüdistatava nõusolekuta ära võetud e-kirjade väljatrükid[135] on KrMS § 63 lg-s 2 sätestatud tõend.[136] Riigikohus kassaatori väitega ei nõustunud ja selgitas, et kriminaalmenetluse asjaoludeks KrMS § 63 lg 2 mõttes on nt menetlustähtaegade järgimine, menetleja pädevus, menetlustoimingu lubatavus vmt asjaolud. Riigikohus lisas, et praeguses asjas on e-kirjade puhul tegemist tõenditega KrMS § 63 lg 1 mõttes, kuivõrd nendele toetudes tuvastati KarS §-s 217^2 sätestatud kuriteokoosseisule vastavad tõendamiseseme asjaolud. Kohtupraktikas on KrMS § 63 lg-s 1 nimetatud lubatava tõendina aktsepteeritud kannatanu tehtud ja menetlejale üle antud eraelulise vestluse salvestust[137]. Niisiis pole KrMS § 63 lg-te 1 ja 2 eristamisel oluline see, missugune isik vaidlusaluse tõendi kogub, vaid määrav on, missuguste asjaolude tuvastamiseks seda kasutada soovitakse.[138]

Riigikohus on kohtuotsuses kriminaalasjas nr 3-1-1-104-05[139] lahendanud küsimust, kas e-kirjad, mille liikumist (sh arvutite IP-aadresse, elektronkirjade päiseid jms) ei ole kontrollitud tehniliste vahendite abil, on üldse tõendid KrMS § 63 lg 1 mõttes. Kui need seda ei ole, võivad need olla tõendina kõlbmatud. Tegemaks kindlaks, kas mingi elektronkiri on saadetud konkreetse isiku arvutist, saab tõesti pöörduda tehniliste lahenduste poole. IP-aadressi abil on võimalik identifitseerida arvutit, kust lähtuvalt on konkreetne e-kiri teele saadetud ja on ka jälgitav selle kirja kulgemine. Iga arvuti on temale omaste elektrooniliste tunnuste alusel individuaalne ja seetõttu ka tuvastatav. Kui kriminaalasjas on küsimuseks kirja võimalik päritolu, on vältimatu ka pöördumine selliseid andmeid kajastavate andmekandjate poole. Riigikohus selgitas, et küsimuse all olevas kriminaalasjas puudus vajadus sellise tõendamiskäigu järele. Nimelt ei ole süüdistatav kriminaalasja menetluse jooksul kordagi väitnud, et tema ei ole kannatanule e-kirju saatnud. Kogu senise kriminaalmenetluse jooksul on süüdistatav pidevat e-kirjade vahendusel kontakti otsimist kannatanuga jaatanud, muuhulgas on ta andnud tõenditena vaadeldud kirjade sisuga kattuvaid ütlusi. Kohus leidis, et sellisel juhul ei tõusetu ka küsimust selle kohta, kas tegemist on kohtukõlbmatute tõenditega.

[135] Kannatanu tegi süüdistatava e-posti kontol olnud kirjadest väljatrükke ja edastas need kuriteokaebusele lisatuna koos süüdistatava kasutuses olnud sülearvutiga menetlejale. Ka menetleja vaatles e-posti kontolt pärinevaid kirju, tegi neist väljatrükke ja fikseeris saadud tõendusteabe asitõendi vaatluse protokollis, järgides seejuures menetlusõigust.
[136] RKÜKo 1-17-2359, 03.03.2021, p 27.
[137] Sama seisukohta on Riigikohus väljendanud ka kriminaalkolleegiumi otsuses asjas nr 3-1-1-5-09 (26.03.2009), p 9 ning otsuses asjas nr 3-1-1-33-11 (4.05.2011), p 9.
[138] RKÜKo 1-17-2359, p 55.
[139] RKo 3-1-1-104-06, p 6.2

Kuna digitaalsed tõendid saab kategoriseerida kui asitõendid, tuleb neid vahetult uurida, st võimaldada tuleb asitõendi või selle foto vahetut vaatlemist. Kuna asitõendid on nn tummad tunnistajad, tuleb asitõendi või selle vaatlemise järgselt avaldada ka asitõendi vaatlusprotokoll või muu uurimistoimingu protokoll, milles on kajastatud antud kriminaalasja kontekstis olulised asitõendi tunnused.[140] Vaatlusprotokoll toob endaga kaasa suure töökoormuse ja nõuab väga detailset kirjeldust. Tõendite vormistamise nõuded on viinud praktikani, kus algselt digitaalset tõendit ega selle autentset koopiat ei lisata sageli üldse kriminaaltoimikusse ega esitata ka tõendina kohtule ning selle asemel kasutatakse tõendina vaid kohtueelse menetluse käigus paberkandjal koostatud vaatlusprotokolle.[141]

Kokkuvõttena saab öelda, et digitaalseid tõendeid, mis on faili kujul, näiteks fotod, videod ja e-kirjad, on võimalik lugeda tõenditeks KrMS § 63 lõike 1 mõttes ning kohtupraktikale tuginedes võib digitaalseid tõendeid kategoriseerida Eesti õigusruumis asitõenditeks. Digitaalseteks tõenditeks võivad olla aga ka metaandmed, mida peab käsitlema eraldi.

3.1.2. Metaandmed digitaalsete tõenditena

Metaandmed ehk andmed andmete kohta ei ole tõendid omaette. Metaandmed sisaldavad endas teavet mõne kohtule esitatud tõendi kohta. See tähendab, et metaandmed ei oma eraldi tõendamisväärtust, vaid nad aitavad mõne tõendi seostada teo toimepanemisega. Näiteks näitavad videofaili metaandmed, millal video on loodud.

Maakohus on öelnud, et failide metaandmeid (nt failide loomise ja muutmise aega) on failide looja ja andmekandja kasutaja poolt võimalik muuta ning nende andmetega manipuleerida. Seetõttu ei tugine kohus ühegi asjaolu tuvastamisel ainuüksi faili metaandmetele. Kohtu hinnangul on vastavaid andmeid võimalik tõendusteabena kasutada vaid kogumis teiste tõenditega.[142]

Maakohus on aktsepteerinud asitõenditena näiteks kiirsuhtlusprogrammi Skype vestlused koos metaandmetega[143], mobiiltelefonilt leituid pildifailid ja videofailid, mis salvestati koos

[140] Kergandberg, E., Sillaots, M. Kriminaalmenetlus, lk 97.
[141] Tehver, J. Digitaalsete tõendite kasutamise võimaldamine, lk 2
[142] Viru Maakohtu kohtuotsus kriminaalasjas nr 1-12-12478 (28.10.2015)
[143] Harju Maakohtu kohtuotsus kriminaalasjas nr 1-15-5739 (29.09.2015).

metaandmetega[144]; sideettevõtjalt saadud andmed metaandmetena[145]; keelatud failid (lapsporno) koos metaandmetega[146] ja helifailid koos metaandmetega[147]. Metaandmeid puudutati eraldi vaid ühes kohtuasjas[148], kus küsimuse all olevate telesaadete failide metaandmetest selgus, kelle kaameraga olid need saated filmitud. Kohus tugines lõpuks otsuse tegemisel siiski vaid tunnistajate ütlustele. Seega võib maakohtu praktikaga tutvumisel öelda, et metaandmeid aktsepteerib kohus tõenditena vaid selleks, et kinnitada mõne teise asitõendi loomise aega.

Maakohus on asunud ühel juhul ka seisukohale, et kohtule esitatud tõendid oleksid pidanud esitatud koos metaandmetega. Viru Maakohus on kohtuotsuses kriminaalasjas nr 1-16-5757 heitnud ette, et tõendina esitatud e-kirjavahetusele ei ole lisatud ka e-kirjavahetuse metaandmete väljatrükki, millest nähtuks kirjavahetuses osalejate e-posti aadressid, kirjade algupärane sisu, kasutatud seadmed jm oluline informatsioon, mis võimaldaks kontrollida kirjavahetuse autentsust. Seda põhjusel, et kohtule esitatud mitmeid e-kirju vaadates oli ilmne, et algset sõnumit on vähemalt osaliselt mingil hetkel töödeldud. Ei ole võimalik, et kiri saadeti ilma adressaadi eposti aadressi märkimata. Teksti korrigeerimine võib olla aset leidnud nii mõne järgneva kirja saatmisel (nt on osa algset sõnumist andmeid eemaldatud) kui ka väljatrüki tegemise eelselt.[149] Ka oli kohtul alust kahelda talle esitatud kirjavahetuse väljatrükkide autentsuses, kuivõrd esitatud ei ole mingeid andmeid (nt andmekandjad, kus kirjavahetus on salvestatud või kirjavahetuse metaandmete väljatrükki), mis võimaldaks seda kontrollida. Sel põhjusel ei saa kohus neid arvestada usaldusväärse tõendina, millele saaks järelduste tegemisel tugineda.[150] Samuti polnud kohtule uurimisasutus esitanud raamatupidamisprogrammist tehtud väljatrüki edastanud e-kirja metaandmetest. Kohus leidis, et seetõttu puudub kohtul igasugune võimalus kontrollida dokumendi päritolu. Selle liikumist algallikast uurimisasutuseni ei ole mingilgi arvestataval viisil dokumenteeritud. Kohus saab küll võrrelda dokumendis kajastuvaid andmeid muude tõenditega, kuid iseseisva tõendiallikana ei ole see kasutatav.[151]

[144] Viru Maakohtu kohtuotsus kriminaalasjas nr 1-19-4135 (09.01.2020).
[145] Harju Maakohtu kohtuotsus kriminaalasjas nr 1-19-5800 (27.08.2019).
[146] Harju Maakohtu kohtuotsus kriminaalasjas 1-16-2605 (06.04.2016).
[147] Viru Maakohtu kohtuotsus kriminaalasjas nr 1-19-7953 (16.09.2020).
[148] Harju Maakohtu kohtuotsus kriminaalasjas nr 1-18-5011 (06.02.20120).
[149] Viru Maakohtu kohtuotsus kriminaalasjas nr 1-16-5757 (19.06.2017), p 2.23.
[150] Viru Maakohtu kohtuotsus kriminaalasjas nr 1-16-5757, p 2.25.
[151] Viru Maakohtu kohtuotsus kriminaalasjas nr 1-16-5757, p 3.7.

Seega võib asuda seisukohale, et metaandmed on Eesti õiguses võimalik lugeda digitaalseteks tõenditeks ning neil on oluline väärtus tõendamisel. Siiski ei ole seni neid üksikult tõendamiseks piisavaks loetud, vaid ainult kogumis teiste tõenditega.

3.2.DIGITAALSETE TÕENDITE HINDAMINE

KrMS § 61 lg 1 kohaselt ei ole ühelgi tõendil ette kindlaksmääratud jõudu. See tähendab, et kõik KrMS § 63 lõikes 1 nimetatud lubatavad tõendiliigid ja ka kõik erinevad konkreetsed tõendid sama tõendiliigi piires on põhimõtteliselt võrdse väärtusega.[152] Tõendite hindamisel on võimalik eristada selle järgmisi etappe: asjakohasuse hindamine, lubatavuse hindamine, usaldusväärsuse hindamine ja nende lõppväärtus.[153] Nii nagu traditsiooniline tõendki, tuleb ka digitaalseid tõendeid ühekaupa hinnata. Kuna selles osas ei ole KrMSis erireegleid, tuleb vaadata digitaalsete tõendite hindamisel kriminaalmenetluse üldisi põhimõtteid.

3.2.1. Digitaalsete tõendite asjakohasuse hindamine

Tõendi asjakohaseks (kuuluvaks) hindamine tähendab veendumust, et see tõend kajastab (peegeldab) kriminaalmenetluse esemeks oleva kuriteo sellist olulist aspekti, mis võimaldab seda kasutada tõendamisesemesse kuuluva asjaolu tuvastamisel.[154] KrMS § 286[1] lõike 1 kohaselt võtab kohus vastu ainult sellise tõendi ja korraldab selliste tõendite kogumise, millel on kriminaalasjas tähtsust. Seega peab kohus hindama tõendi vastuvõtmisel ja selle kogumise otsustamisel hindama kõne all oleva tõendi asjakohasust. Juhul, kui tõend ei ole asjakohane, võib kohus keelduda selle vastuvõtmisest või kogumise korraldamisest, sest sellel tõendil ei ole kohtuasjas tähtsust. Tõendi tähtsus on oluline aspekt, mida on vaja arvestada tõendi vastuvõtmise või tõendi kogumise taotluse lahendamisel. Seega on ühtlasi oluline otsustada, millisel juhul ei ole tõendil kriminaalasja lahendamisel tähtsust.[155]

Tõendil ei ole kriminaalasja lahendamisel tähtsust, kui selle tõendi abil tõendataval asjaolul ei ole kriminaalasja lahendamisel tähtsust. Asjaolu on tähtsusetu, kui see asjaolu ei ole seoses menetlusesemega või kui asjaolu, vaatamata sellisele seosele isegi selle tõendatuse puhul ei saa

[152] Kergandberg, E., Sillaots, M. Kriminaalmenetlus, lk 205.
[153] Kergandberg, E., Sillaots, M. Kriminaalmenetlus, lk 205.
[154] Kergandberg, E., Sillaots, M. Kriminaalmenetlus, lk 205.
[155] Kergandberg, E., Pikamäe, P. Kriminaalmenetluse seadustik, lk 649.

kohtuotsust mingil moel mõjutada.[156] Samuti ei ole tõendil kriminaalasja lahendamisel tähtsust, kui vastav tõendamisvahend on täiesti ebasobiv. Tõendamisvahend on täiesti ebasobiv, kui selle abil ei ole väidetav asjaolu tõendatav.[157]

Ka digitaalse tõendi puhul tuleb hinnata, kas konkreetne tõend omab kriminaalasjas tähtsust. Siinkohal tuleb märkida, et asjakohasuse hindamisel ei hinnata seda, kas tõend on millegi tõendamiseks piisav. Näiteks on kohus leidnud, et kriminaalasjas, kus küsimuse all oli KarS § 300 lg 1 ehk riigihanke menetluse nõuete rikkumise eest menetluses osalejale eelise andmise süüdistus, ei puudutanud kohtule esitatud e-kirjavahetus seoses sooviga osta Saksamaalt veoauto koos pealisehitusega süüdistuses kirjeldatud faktilisi asjaolusid. Seega leidis kohus, et tõend ei ole asjakohane ja jättis tõendi kõrvale.[158]

Samuti on kohus arvanud tõendikogumist välja näiteks süüdistatava terviseseisundit puudutavad dokumendid, kuna kaitsja ei toonud välja, missugust tõendamiseseme asjaolu ta nende tõenditega tõendada soovis, samuti ei tulnud see välja tõendi olemusest. Seetõttu leidis kohus, et terviseseisundit puudutavad dokumendid ei ole asjakohased.[159]

Kriminaalasjas seoses sõidukijuhi poolt liiklusnõuete ja sõiduki käitusnõuete rikkumisega ettevaatamatusest on näiteks kohus jätnud võtmata materjalide juurde bülletääni „Torm ja tugev tuul“ (mi s räägib külgtuule ohtlikkusest); väljatrüki Riigi Ilmateenistuse vaatlusandmetest 21.02.2012.a kell 10.00; väljatrüki Riigi Ilmateenistuse vaatlusandmetest 15.12.2012.a kell 12.00; väljatrüki Riigi Ilmateenistuse vaatlusandmetest 11.01.2015.a kell 15.00; ning väljatrüki Riigi Ilmateenistuse vaatlusandmetest 11.01.2015.a kell 17.00 – sest need ei seondu kriminaalasja tõendamisasjaoludega. Lisaks märkis kohus, et bülletäänis sisalduv teave on käsitatav üldteada infona ja ilmateenistuse vaatlusandmed tuuleolude kohta 11. jaanuaril 2015 kell 15 ja kell 17 ei ole asjakohased, sest kaitsja on juba esitanud ning maakohus on uurinud väljatrükki orienteeruva kuriteosündmuse toimumisaja, s.o kella 16 kohta. Samas asjas leidis aga kohus, et hõõglambiekspertiisi akt ei olnud asjakohatu tõend vaatamata prokuratuuri seisukohast, sest asjas eeluurimise faasis tõe väljaselgitamise huvidest lähtuvalt oli siiski põhjendatud saada selgust selles, kas kokkupõrke toimumise hetkel suunatuli põles või mitte.[160]

[156] Kergandberg, E., Pikamäe, P. Kriminaalmenetluse seadustik, lk 649.
[157] Kergandberg, E., Pikamäe, P. Kriminaalmenetluse seadustik, lk 649.
[158] Pärnu Maakohtu kohtuotsus kriminaalasjas 1-19-2108 (27.09.2019).
[159] Harju Maakohtu kohtuotsus kriminaalasjas nr 1-17-2018 (03.07.2018).
[160] Tallinna Ringkonnakohtu kohtuotsus kriminaalasjas nr 1-15-10975 (08.09.2016).

Kohtute põhjendustega tutvudes võib jõuda järeldusele, et tõendi asjakohasuse hindamisel tuleb vastata ühele küsimusele: „Kas see konkreetne tõend on kriminaalasja lahendamisel oluline?“. Ei piisa sellest, et tõend oleks vaid seotud kriminaalasjaga. Eeltoodud kohtuasjades olid esitatud ja kohtu poolt tagasi lükatud tõendid küll seotud süüteo toimepanija või toimepanemise ajaga, kuid ei aidanud kohtul otsuse tegemisel ühele või teisele poole kalduda. Selle asemel olid need pigem vaid informatiivse tähendusega, mistõttu kohus neid oma otsustes asjakohasteks ka ei pidanud. Digitaalsete tõendite hindamisel ei tule hinnata nende asjakohasust kuidagi teisiti ega esitada ühtegi täiendavat küsimust.

3.2.2. Digitaalsete tõendite lubatavuse hindamine

Mingi kuriteo kohta käiva teabe kasutamine tõendina sõltub lisaks vormile ka sellest, kas ja kuivõrd on selle teabe saamisel (tõendite kogumisel) järgitud põhiõiguste tagamisele suunatud kriminaalmenetluse sätteid.[161] Siinkohal tuleb lähtuda tuleb kohtumenetluses üldiselt omaksvõetud arusaamast, mille kohaselt tõendi lubatavust eeldatakse. Vastavasisulise kahtluse tekkimise korral peab kohus tõendi saamise seaduslikkust kontrollima.[162]

Tõendid peavad olema kogutud KrMS §-s 64 sätestatud nõudeid järgides. See tähendab, et ennekõike tuleb tõendeid koguda viisil, mis ei riiva kogumises osaleja au ja väärikust, ei ohusta tema elu või tervist ega tekita põhjendamatult varalist kahju. Keelatud on tõendeid koguda isikut piinates või tema kallal muul viisil vägivalda kasutades või isiku mäluvõimet mõjutavaid vahendeid ja inimväärikust alandavaid viise kasutades. Digitaalsete tõendite lubatavusele kriminaalmenetluse seadustik ei sätesta, mistõttu on digitaalsed tõendid lubatud juhul, kui nende kogumine ei riku KrMS §-s 64 sätestatud nõudeid.

Eelnimetatud põhimõtet on kinnitanud ka Riigikohus kohtuotsuses kohtuasjas nr 1-17-2359, nentides, et kriminaalmenetluses loetakse tõend üldjuhul lubamatuks alles siis, kui tõendi kogumise korda on oluliselt rikutud (vt ka KrMS § 64 lg 1). Ainukese erandina on seadusandja sätestanud tõendi kasutamise absoluutse keelu olukordadeks, kus jälitustoimingu loa taotlemisel ja andmisel ning jälitustoimingu tegemisel pole järgitud seaduse nõudeid (KrMS § 126^1 lg 4). Kohtupraktika kohaselt tuleb tõendi lubatavuse üle otsustamiseks hinnata rikutud normi eesmärki ja seda, kas selliseid tõendeid poleks saadud, kui normi ei oleks rikutud. Tõend tuleb tõendikogumist kõrvaldada näiteks juhul, kui rikutud on kriminaalmenetluse

[161] Kergandberg, E., Sillaots, M. Kriminaalmenetlus, lk 197.
[162] Riigikohtu kriminaalkolleegiumi kohtuotsus asjas nr 1-17-5210 (28.11.2019), p 25.

aluspõhimõtteid (nt saadakse ütlused ähvarduste tõttu), menetlustoimingust puudutatud isiku põhiõiguste rikkumisega (nt kuulatakse alaealine kahtlustatav üle kaitsja juuresolekuta või jäetakse ülekuulatavale isikule õigused ning kohustused tutvustamata) või kui toimingu eesmärk oli algusest peale puudutatud isiku õigustest mööda minna ning rikkuda ausa kohtupidamise põhimõtet. Tõendit võib käsitada lubamatuna ka siis, kui selle saamisel on aset leidnud mitmed eraldivõetult ebaolulised menetlusõiguse rikkumised, kuid menetleja on tõendi saamisel menetlusõigust rikkunud korduvalt ja tahtlikult. Tõendi lubatavuse üle otsustamisel peab igal üksikjuhul mh kaaluma, kas tõendi kogumisel on tuvastatavad menetlusõiguslikud eksimused, missugune on nende eksimuste mõju menetlustoimingule allutatud isiku jaoks ning kuidas mõjutab konkreetne tõendusteave kriminaalasja lahendit.[163]

Eelmises lõigus nimetatud kohtuasjas oli küsimuse all, kas süüdistatava ametialaselt e-posti kontolt saadud ning menetlejale edasi antud e-kirjad on kriminaalmenetluses lubatavad tõendid. Kannatanu tegi süüdistatava e-posti kontol olnud kirjadest väljatrükke ja edastas need kuriteokaebusele lisatuna koos süüdistatava kasutuses olnud sülearvutiga menetlejale. Ka menetleja vaatles e-posti kontolt pärinevaid kirju, tegi neist väljatrükke ja fikseeris saadud tõendusteabe asitõendi vaatluse protokollis, järgides seejuures menetlusõigust. Süüdistatava kaitsja vaidles, et e-kirjade väljatrükid tehti süüdistatava e-posti kontolt tema nõusolekuta, mistõttu on need tõendina lubamatud. Riigikohus selgitas, et isegi kui leiaks tõendamist menetlusõiguse rikkumine kõnealuste tõendite kogumisel, ei tooks see vältimatuna kaasa nende lubamatust isiku süüküsimuse lahendamisel.

Samuti toonitas Riigikohus, et süüdistatava e-kirju ei kogutud tema isiklikult füüsiliselt andmekandjalt, vaid talle ametialaseks kasutamiseks antud e-posti kontolt. Töötaja või käsundisaaja arvestama, et mõnel juhul võib tema töö- või käsundiandja uurida tööülesannete täitmisega seotud e-kirju ka tema nõusolekuta, nt kuriteo või tõsiste ametialaste rikkumiste õigustatud kahtluse korral. Siinkohal tuleb töö- või käsundiandjal austada isiku eraelu puutumatust ja võtma uurimise ajal kasutusele vastavaid meetmeid[164]. Seega jõudis Riigikohus

[163] RKÜKo 1-17-2359, p 48-49.

[164] Oluline on siinkohal toonitada, et töötaja isikuandmeid sisalduvaid e-posti kontol olevaid kirju võib töödelda (sh nendega tutvuda) ainult seadusliku aluse olemasolu korral nii isikuandmete kaitse üldmääruse (Euroopa Parlamendi ja nõukogu 27. aprilli 2016. a määrus (EL) nr 2016/679) artikli 6 lg 1 kui isikuandmete kaitse seaduse § 14 p 1 kohaselt. Seega tuleb töö- või käsundiandjal veenduda, et e-kirjade tutvumisel on olemas seaduslik alus, nt lepingust tulenevate ametikohustuste (käsundi) täitmises veendumine juhul, kui on olemas õigustatud kahtlus. Isikuandmete töötlemisel ilma andmesubjekti nõusolekuta tuleb hinnata ka seda, kas huvi kaalub üles andmesubjekti põhiõigused ja -vabadused või mitte.

järelduseni, et e-kirja kui tõendi saab lugeda lubamatuks, kui selle kogumisel on rikutud rängalt menetlusõiguse põhialuseid või kui rikkumisi on toime pandud korduvalt ja süstemaatiliselt.

Kohtuasjas 3-1-1-82-16[165] loeti mõrvas süüdistatava isiku süü tõendatuks tunnistajate ütluste, turvakaamera salvestiste ja kahe ekspertiisiaktiga, mille kohaselt leiti süüdistatava jope taskust äravõetud noalt verd. Lisaks tugines maakohus süüküsimuse lahendamisel kujutiseekspertiisi aktile. Kujutiseekspertiisi käigus töödeldi turvakaamerate salvestisi nende kvaliteedi parandamiseks ning mõned failid ühendati. Süüdistatava kaitsja sõnul selline videofailide kvaliteedi parandamine ja failide ühendamine kahandab nende failide tõendusväärtust. Kuna polnud tuvastatud, millises mahus videofaile muudeti, ei saa ekspertiisiakti lubatava tõendina käsitada.[166]

Riigikohus selgitas, et kujutiseekspertiisi esimene lähteülesanne oli suurendada ja parandada erinevate videofailide kvaliteeti, samuti ühendada või sünkroniseerida need failid ühele ekraanile. Kujutiseekspert töötles videofaile ekspertiisiülesande järgi. Riigikohus leidis, et kujutiseekspertiisi käiku, sh videofailide töötlemist, on ekspertiisiaktis arusaadavalt ja piisava üksikasjalikkusega kirjeldatud. Videofailide töötlemine on ekspertiisiakti põhjal jälgitav ja kujutiseekspertiisi käik kontrollitav.[167]

Riigikohus sedastas eelpoolmainitud kohtuotsuses, et videofaili kvaliteedi parandamine ja mitme faili ühendamine üheks failiks ei ole uue tõendi loomine. Olemasolevate tõendite edasiseks uurimiseks tuleb parandada videofailide kvaliteeti, et tagada failides kujutatud isikute tuvastamine. Videofailide kvaliteedi parandamise käigus ei muudetud ega kadunud failides sisalduv info ning videol kujutatud isikud ei muutunud. See tähendab, et videofailid näitavad endiselt sündmusi, mis tegelikult aset leidsid. Ka mitme video ühendamine ühe faili loomiseks ei muutnud tegelikult aset leidnud sündmusi. Kuigi sündmuste järjekorda oli teoreetiliselt võimalik videofailides muuta, kasutati sündmuste tegeliku järjekorra tuvastamiseks ka tunnistajate ütlusi. Seetõttu ei kao videofailide usaldusväärsus kvaliteedi tõstmisel või mitme faili ühendamisel. Eeltoodule tuginedes ei leidnud Riigikohus, et vaidluse all olev kujutusekspertiisi käigus loodud videofail ja selle uurimisel loodud kujutisekspertiisi akt oleks lubamatu tõend.

[165] RKKKo 3-1-1-82-16
[166] RKKKo 3-1-1-82-16, p 4.1.
[167] RKKKo 3-1-1-82-16, p 9.

Kohtuasjas 3-1-1-82-16 on menetleja pidanud vajalikuks videokaamera salvestisele ekspertiisi tegemist ning põhjendanud otsust ennekõike vajadusega videofaili kvaliteeti suurendada ja parandada. Käesoleva magistritöö autori hinnangul võinuks jätta ekspertiisi ka tegemata ning videofailid ühendamata, kuna videofaililt süüdistatava tuvastamine oli võimalik ka ilma ekspertiisita. Sellisel juhul oleks saanud tõendina kasutada vaid videofaile ning diskussioon kujutisekspertiisi akti lubatavuse üle oleks jäänud pidamata.

Riigikohus on kohtuotsuses 1-16-6179/111 otsustanud selle üle, kas elektroonilise side seaduse (edaspidi *ESS*) § 111^1 lg 2^{168} alusel mh süüteomenetluse eesmärkidel säilitatud ja KrMS § 90^1 lg 2^{169} alusel prokuratuuri loal sideettevõtjalt saadud liiklus- ja asukohaandmed on tõendina lubatavad. Tegemist on markantse kohtuotsusega digitaalsete tõendite valdkonnas, kuna Riigikohus peatas asja menetluse ja esitas Euroopa Kohtule eelotsusetaotluse[170]. Eelotsusetaotlusega küsis Riigikohus, kas Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiivi 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris, artikli 15 lõiget 1 tuleb koostoimes Euroopa Liidu põhiõiguste harta artiklitega 7, 8 ja 11 ning artikli 52 lõikega 1 tõlgendada selliselt, et lubatavateks tõenditeks saab pidada protokolle, mille uurimisasutus on koostanud prokuratuuri loa alusel sideettevõtjalt nõutud andmete kohta.

Euroopa Kohus tegi otsuse asjas nr C-746/18[171] 2. märtsil 2021. a ja leidis, et üldise kuritegude ennetamise, uurimise, avastamise ning kohtus menetlemise eesmärgiga saab õigustada ainult neid põhiõiguste riiveid, mis ei ole rasked, kuid kui riivatakse era- ja perekonnaelu puutumatust ning õigust isikuandmete kaitsele ning riive kaasneb ametiasutuse juurdepääsuga liiklus- või asukohaandmete kogumile, on ta igal juhul raske.[172] Euroopa kohus toonitas, et juurdepääs selliste liiklus- või asukohaandmete kogumile, mida elektroonilise side seaduse § 111^1 alusel

[168] ESS § 111^1 lg 2 kohaselt on telefoni- ja mobiiltelefoniteenuse ning telefonivõrgu ja mobiiltelefonivõrgu teenuse osutaja on kohustatud säilitama nii helistaja, vastuvõtja kui ka kõne kohta mitmeid erinevaid andmeid.
[169] KrMS § 90^1 lg 2 kohaselt võis kuni 01.01.2022 kehtinud redaktsioonis uurimisasutus prokuratuuri loal kohtueelses menetluses või kohtu loal kohtumenetluses teha päringu elektroonilise side ettevõtjale ESS § 111^1 lg-tes 2 ja 3 loetletud andmete kohta, v.a. sama paragrahvi 1. lõikes nimetatud sõnumi edastamise faktiga mitteseotud andmed.
[170] RKKKm 1-16-6179/85
[171] Euroopa Kohtu otsus (suurkoda) 2. märtsil 2021 kohtuasjas C-746/18, mille ese on ELTL artikli 267 alusel Riigikohtu (Eesti) 12. novembri 2018. aasta määrusega esitatud eelotsusetaotlus. Arvutivõrgus kättesaadav https://curia.europa.eu/juris/document/document.jsf;jsessionid=4B6923E0FAC256FA06BF2302EE4D0A77?text=&docid=238381&pageIndex=0&doclang=ET&mode=lst&dir=&occ=first&part=1&cid=3528248 (03.04.2022).
[172] EK otsus kohtuasjas C-746/18, p 33 ja 39. Arvutivõrgus kättesaadav https://eur-lex.europa.eu/legal-content/et/TXT/?uri=CELEX:62018CJ0746 (27.04.2022).

säilitatakse, võimaldab tõesti teha täpseid või isegi väga täpseid järeldusi nende isikute eraelu kohta, kelle andmeid säilitatakse.[173]

Tõendi lubatavuse üle diskuteerides toonitas Riigikohus, et tõendi lubatavust hindav kohus peab veenduma, et tõendi kogumisel järgiti kehtivat õigust.[174] Tõendi lubatavuse üle otsustamiseks tuleb hinnata rikutud normi eesmärki ja seda, kas selliseid tõendeid poleks saadud, kui normi ei oleks rikutud.[175]

Arutelu all olevas kriminaalasjas tehti ESS § 111^1 lg 2 kohaselt säilitatud sideandmeid puudutavad päringud KrMS § 90^1 lg-s 2 ette nähtud loa alusel, millega rikuti era- ja perekonnaelu puutumatust, õigust isikuandmete kaitsele ning sõna- ja teabevabadust. Põhiseaduse §-ga 26 kaitstava eraelu puutumatuse riiveks, mis kaasnes sideandmete säilitamisega ja loa andmisega nende andmete kasutamiseks, ei olnud seega õiguslikku alust. Riigikohtu arvates ei põhjendanud prokuratuur ühegi KrMS § 90^1 lg-s 2 ette nähtud loa puhul sideandmete küsimise vältimatut vajalikkust viisipärasel ning jättis kriminaalmenetluse esemeks olevate tegude faktiliste asjaolude ja tõenditega seostamata ning põhjendamata, miks on teabe kogumine muude menetlustoimingutega välistatud või oluliselt raskendatud. Sellega sekkuti süüdistatava eraellu ning jäeti sekkumise vältimatu vajalikkus nõutaval moel põhjendamata.[176]

Mõnel juhul võib tõendi saamisel aset leidnud menetlusõiguse rikkumise raskust vähendada asjaolu, et tõendi oleks võinud saada ka siis, kui rikkumist poleks toimunud, kuid toimiku materjalist ei selgu kas ning missuguses mahus on sideettevõtjal ärilistel põhjustel (nt kliendile arve esitamiseks ja sidumistasude määramiseks) ESS § 111^1 lg-s 2 loetletud andmeid vaja. Seetõttu ei saa tõsikindlalt järeldada, et süüdistatava kohta sideettevõtjalt kogutud ja kriminaalasjas kasutatud andmeid oleks asjasse puutuvas osas säilitatud ilma riigi pandud kohustuseta.

Kuna tõendite kogumisel rikuti KrMS § 901 lg 3 nõudeid, on tegemist olulise rikkumisega, mis toob kaasa kogutud tõendite lubamatuse. Riigikohus jõudis põhjaliku analüüsi tulemusena seisukohale, et ükski prokuratuuri lubade alusel koostatud sideettevõtjalt saadud andmete protokoll ei ole tõendina lubatav.

[173] EK otsus kohtuasjas C-746/18, p 36.
[174] RKKKo 1-16-6179, p 54.
[175] RKKKo 1-16-6179, p 58.
[176] RKKKo 1-16-6179, p 74.

Euroopa Liidu 02.03.2021 otsusest nr C-746/18 tulenevalt muudeti KrMS-i ning asendati prokuratuuri loa nõue prokuratuuri taotluse ja kohtu loa nõudega.[177] KrMS § 90^1 uus sõnastus jõustus 01.01.2022 ning sellega sätestati, et prokuratuuri taotlusel ja kohtu loal võib päringu elektroonilise side ettevõtjale teha ESS § 111^1 lõigetes 2 ja 3 loetletud andmete kohta üldjuhul vaid siis, kui tegemist on KrMS § 126^2 lõikes 2 nimetatud kuriteoga ning kui see on vältimatult vajalik kriminaalmenetluse eesmärgi saavutamiseks.[178] Samuti tuleb kohtule loa andmise määruse tegemiseks esitada andmete kogumise põhjendus ning sideandmete loas märgitakse konkreetne ajavahemik, mille kohta andmeid soovitakse. [179]

Kokkuvõtvalt on oluline digitaalsete tõendite kogumisel jälgida, et kogudes ei oleks rikutud süüdistatava põhiõigusi. Kuigi Eesti kohtupraktikas ei ole läbi käinud tõendite lubatavuse küsimust olukorras, kus digitaalsete tõendite kogumisel oleks teadlikult rikutud süüdistatava isikuandmed, võib vaidluse korral jõuda kõrgeim kohus järeldusele, et selliselt kogutud digitaalsed tõendi ei ole lubatavad.

3.2.3. Digitaalsete tõendite usaldusväärsuse hindamine

Tõendi usaldusväärsus on küsimus sellest, millise kaalu omistab talle tõendi hindaja, kõrvutades ja analüüsides teda koostoimes teiste asjas kogutud tõenditega. Tõendi usaldusväärsusest tuleb selgelt eristada küsimust tõendi lubatavusest.[180] Lisaks ei saa tõendi usaldusväärsuse hindamisel iseenesest kriteeriumiks olla see, kuivõrd napp või mahukas on tõend - sõltumata viimatinimetatud asjaoludest on kohus tõendite hindamisel vaba, hinnates tõendeid nende kogumis ja oma siseveendumuse kohaselt.[181]

Tõendi usaldusväärsuse küsimus tõusetub kohtus üldjuhul alles pärast seda, kui kohus on tõendi vastu võtnud ja selle avaldanud ning see tõend on edukalt läbinud asjakohasuse ning lubatavuse testi. Sellises olukorras tähendab tõendi tunnistamine usaldusväärseks eeskätt kohtu

[177] Kriminaalmenetluse seadustiku muutmise seadus 392 SE.
[178] Muudatusettepanekute loetelu kriminaalmenetluse seadustiku muutmise seaduse 392 SE teise lugemise juures, lk 2. Arvutivõrgus kättesaadav Riigikogu veebilehel https://www.riigikogu.ee/tegevus/eelnoud/eelnou/69f4f636-076c-487f-93c2-3827044cfb50/Kriminaalmenetluse%20seadustiku%20muutmise%20seadus (06.04.2022).
[179] 5. aprillil 2022 tegi Euroopa kohtu suurkoda otsuse kohtasjas nr C-140/20, milles leidis, et Euroopa Liidu õigusega on vastuolus seadusandlikud meetmed, mis näevad raske kuritegevuse vastu võitlemiseks ja avalikku julgeolekut ähvardava suure ohu ärahoidmiseks ennetavalt ette liiklus- ja asukohaandmete üldise ja vahet tegemata säilitamise. See otsus toob kindlasti kaasa täiendava regulatsiooni muudatuse ka Eesti õiguses.
[180] RKo 3-1-1-19-05, p 7.3. ja 7.4.
[181] RKKKo 3-1-1-45-07, p 10.

veendumust, et see tõend kajastab uuritava kuriteo tunnust ja et seda kajastust on võimalik kriminaalmenetluses ka taasesitada. Kohtupraktikas on mingi tõendi usaldusväärsust põhjendatud ka selle kaudu, kuidas see tõend n-ö riimub teiste tõenditega. Riimuvate tõendite kogum suurendab kindlasti selle kogumiga kajastatava asjaolu tõenäosust, kuid riimumine ise ei ole siiski ühtegi tõendit iseloomustav tunnus, mis tõstaks selle usaldusväärsust. [182]

Seadusandja ei ole sätestanud tõendi usaldusväärsuse kontrollimiseks mingeid erilisi universaalseid reegleid.[183] Seetõttu ei ole kriminaalmenetluse seadustikus ka erisätteid digitaalsete tõendite usaldusväärsuse hindamiseks. Eeltoodu pinnalt on seega küsitav, kuidas kohtunik, kes ei ole mitteõiguslike eriteadmistega isik, peaks jõudma digitaalsete tõendite hindamisel veendumuseni.

Digitaalsete tõendite puhul võib pinnapealse hindamise korral jõuda kiirelt (valele) järeldusele, et hindamise all olev digitaalne tõend on usaldusväärne. Digitaalse tõendi usaldusväärsuse hindamine nõuab häid teadmisi seda tüüpi tõendite sisust ja eripärast võrreldes tavalise tõendiga. Lisaks peab hindaja mõistma, kuidas on võimalik digitaalset tõendit märkamatult muuta selliselt, et see jätab usaldusväärse mulje, kuigi see tegelikult ei ole. Tõendi usaldusväärseks tunnistamine tähendab kohtuniku veendumust, et see tõend on esiteks adekvaatselt kajastanud mingi uuritava kuriteo tunnust ja teiseks, et seda kajastust on võimalik adekvaatselt kriminaalmenetluses ka reprodutseerida.[184] Seega peab kohtunik olema digitaalseid tõendeid hinnates olema piisavate teadmistega ja pädev, et jõuda argumenteeritud veendumuseni.

Riigikohtu kriminaalkolleegium on oma otsuses nr 3-1-1-55-14 öelnud, et ekspertiis on nõutav olukorras, kui tõendamiseseme asjaolu tuvastamiseks on vaja vastata küsimusele, mille lahendamine on usaldusväärselt võimalik üksnes mitteõiguslike eriteadmiste alusel. Niisiis tuleb ekspertiis teha juhul, kui teatud liiki mitteõiguslike eriteadmiste rakendamine võib anda tõendusteavet, mille tajumine või tähenduse mõistmine jääb väljapoole menetleja üldteadmiste piire.[185]

Eelöeldu tähendab esiteks seda, et ei ole välistatud, et menetleja jõuab tema üldteadmiste piire ületavate järeldusteni ilma ekspertiisi tegemata. See on nii olukorras, kus menetleja jaoks uue

[182] RKKKo 3-1-1-89-12, p 14-15.
[183] Kergandberg, E., Pikamäe, P. Kriminaalmenetluse seadustik, lk 210
[184] E Kergandberg, E., Pikamäe, P. Kriminaalmenetluse seadustik, lk 209.
[185] RKKKo 3-1-1-55-14, p 172.

teadmise saamiseks eriteadmisi rakendada vaja ei ole. Teiseks tähendab eelmises lõigus märgitu, et ekspertiisi ei ole vaja teha juhul, kui tõendusteabe saamiseks ei ole vaja ületada menetleja üldteadmiste piire. Kas tõenduslikult olulise järelduse tegemine ületab menetleja üldteadmiste piire või mitte, sõltub konkreetse kriminaalasja asjaoludest. [186]

Seega tähendab eeltoodu, et ilmgtingimata ei ole alati digitaalse tõendi ekspertiisi vaja, kuid see sõltub iga konkreetse kriminaalasja asjaoludest, selle kriminaalasja menetlejast ja tema hinnangust oma üldteadmistele. Õiguslik regulatsioon ei anna menetlejale juhiseid, millisel juhul tuleks ekspertiis teha ja millal mitte.

Riigikohus on sedastanud, et kui süüdistatav ei ole selgitanud, kus ja millises osas on tema saadetud e-kirju moonutanud või esitanud ise kohtule kirjade originaale, ei pea tõendeid kahtluse alla üldse seadma. Seda eriti sellisel juhul, kui kohtualune ise ei ole eitanud kirjade (praegusel juhul ähvardavat) sisu eitanud. Võttes süüdistuse sellises osas omaks, ei piisa e-kirjade kui tõendite kahtluse alla seadmiseks abstraktsetest väidetest.[187]

Kohtupraktikas on mingi tõendi usaldusväärsust põhjendatud ka selle kaudu, kuidas see tõend n-ö riimub teiste tõenditega. Riimuvate tõendite kogum suurendab kindlasti selle kogumiga kajastatava asjaolu tõenäosust, kuid riimumine ise ei ole siiski ühtegi tõendit iseloomustav tunnus, mis tõstaks selle usaldusväärsust. Ka ei pruugi n-ö riimumata tõend olla ebausaldusväärne.[188]

Enamasti on kohtud kasutanud digitaalsete tõendite riimumise argumenti tunnistaja või kannatanu ütluste usaldusväärsuse hindamisel. Nii on näiteks kohus leidnud, et kannatanu ütlused riimuvad asitõendi vaatlusprotokollis vaadeldud helisalvestise sisuga. Kõnesalvestisest nähtub, et süüdistatav ärritub, kasutab kannatanu suunal ebatsensuurseid väljendeid ja solvab teda. Protokollist nähtuv kinnitab ka kannatanu ütluseid selle kohta, millest konflikt alguse sai.[189] Samuti on maakohus tuginenud ka kriminaalmenetluse käigus kogutud fotodele, kust nähtub kannatanu jalale tekitatud hematoom. Selline tõend riimub tunnistajate ütlustega kannatanu suhtes toimepandud vägivalla osas ning nimetatud tõendid kogumis andsid maakohtule piisava aluse lugeda tahtliku vägivalla toimepanemine tõendatuks.[190]

[186] RKKKo 3-1-1-55-14, p 173.
[187] RKO 3-1-1-104-05, p 6.3.
[188] RKKKO 3-1-1-89-12, p 14.
[189] Harju maakohtu kohtuotsus kriminaalasjas 1-20-98 (18.03.2020).
[190] Tallinna Ringkonnakohtu kohtuotsus kriminaalasjas nr 1-19-5662 (26.02.2020).

3.2.4. Digitaalsete tõendite lõppväärtus

Mingi tõendi lõppväärtus on hinnang selle kohta, kuivõrd olulisel kohal on see tõend kohtu jaoks, lugemaks mingit tõendamiseseme asjaolu tuvastatuks (või kummutatuks).[191] Tõendite hindamise üks põhiparadokse kipubki olema selles, et eeskätt just kaalukate tõendite puhul võivad tekkida vaidlused seoses nende lubatavuse ja usaldusväärsusega.[192] Ka digitaalsete tõendite puhul peab kohus andma lõplikku hinnangu tõendi kohta pärast seda, kui ta on hinnanud ära selle tõendi asjakohasuse, lubatavuse ja usaldusväärsuse.

Kokkuvõttena tuleb digitaalsete tõendamise hindamisel läbida kõik hindamise etapid, mida kohus peab läbima traditsioonilise tõendi hindamisel. Digitaalse tõendi asjakohasuse hindamisel tuleb hinnata, kas konkreetne digitaalne tõend omab kriminaalasjas tähtsust. Digitaalse tõendi lubatavuse hindamisel tuleb kohtul veenduda, kas see on kogutud KrMS §-s 64 sätestatud nõudeid järgides. Viimasena tuleb usaldusväärsuse hindamisel kohtul väljendada oma veendumust, et digitaalne tõend kajastab uuritava kuriteo tunnust ja et seda kajastust on võimalik kriminaalmenetluses ka taasesitada. Kohtupraktika näitab, et kohus ei ole takerdunud digitaalse tõendite hindamisel olemasoleva regulatsiooni taha, seega võib asuda seisukohale, et olemasolev KrMSi regulatsioon võimaldab kohtul viia läbi ka digitaalsete tõendite hindamine.

Kohtupraktika pinnalt võib väita, et menetlejad soovivad ekspertiisi ka siis, kui tegelikult võiks ka infotehnoloogiliste eriteadmisteta isik digitaalse tõendi pinnalt järeldusi teha. Kuna menetlejate üld- ja infotehnoloogilised teadmised on erinevad ning KrMS jätab ekspertiisi tegemise puhtalt menetleja otsustuspädevusse, on tegemist vaid käesoleva töö autori subjektiivse hinnangu ja seisukohaga. KrMSi täiendamine seni praktikas toimiva lahenduse muutmiseks ei ole vajalik.

3.3. DISTANTSILT KOHTUS OSALEMINE

Kehtiv KrMS ei sunni menetlusosalisi igal juhul viibima füüsiliselt istungisaalis. Selle asemel on võimalik kahel moel kohtus osaleda. Esimeseks selliseks lahenduseks on kaugülekuulamine, mis võimaldab ütlusi anda kas audiovisuaalsel teel või telefoni kaudu. Teiseks on võimalik

[191] E Kergandberg, E., Pikamäe, P. Kriminaalmenetluse seadustik, lk 211.
[192] E Kergandberg, E., Pikamäe, P. Kriminaalmenetluse seadustik, lk 211.

osaleda audiovisuaalses vormis osaleda kohtuistungil. Mõlema regulatsiooni laiendati suuresti 2020. aasta märtsis alanud COVID-19 haigust põhjustava koroonaviiruse levikuga seotud kriisi ja sellest tuleneva eriolukorra mõju leevendamiseks. Samas olid mõlemad lahendused olemas Eesti õiguskorras juba enne eriolukorra algust.

3.3.1. Audiovisuaalses vormis istungil osalemine

Põhiseaduse § 24 lõikes 2 on sätestatud põhiõigus olla oma kohtuasja arutamise juures. Riigikohus on täiendavalt selgitanud, et sellest lähtuvalt tuleneb ka õigus olla kohtus ära kuulatud. Kaudselt on see õigus järeldatav ka kohtusse pöördumise õigust sätestavast PS § 15 lg-st 1, mis on ausa kohtumenetluse õiguse üldnorm. Analoogsed õigused tulenevad Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 6 lg-test 1 ja 3.[193] Eeltoodud õiguste tagamiseks on KrMS § 35 lõikes 2 sätestatud, et süüdistataval on õigus võtta osa kohtulikust arutamisest, s.t viibida oma asja arutamise juures. Ka kannatanul on KrMS § 38 lg 1 p 8 alusel õigus kohtulikust arutamisest osa võtta. Selline õigus on ka tsiviilkostjal kohtuliku uurimise lõpetamiseni maakohtus (KrMS § 40 lg 1 p 6) ja kolmandal isikul[194] (KrMS § 40^2 lg 1 p 5).

Vaatamata õigusele viibida oma kohtuasja arutamise juures lubab KrMS eeluurimiskohtunikul, kohtunikul või täitmiskohtunikul korraldada istung tõkendi või muu menetlusliku sunnimeetme aruteluks või kohtulahendi täitmisel tekkinud küsimuse läbivaatamiseks või eelistung viisil, et kohtusse kutsutud isikud saavad menetlusest osa võtta tehnilise lahenduse abil, mis vastab KrMS paragrahvi 69 lõike 2 punktis 1 nimetatud nõuetele. Sellisel viisil on võimalik korraldada ka kohtulikku arutamist lihtmenetlustes (lühi- ja kokkuleppemenetluses) ning osavõttu ringkonnakohtu istungitest. Kusjuures ringkonnakohtu istungitest osavõtt võimaldati alles 2020. aasta maikuust, mil jõustus 170 SE. Seni nähtus KrMS § 334 lõikest 3, et ringkonnakohtu istungil võis tehnilise lahenduse abil üksnes prokurör. Arvestades asjaolu, et ringkonnakohtu istungil reeglina tõendeid vahetult ei uurita, polnud selline piirang põhjendatud.

Kohtu õigus korraldada kohtumenetluse poolte osalemine tehnilise lahenduse abil ei ole siiski mõeldud üldreegliks. Sel viisil istungit korraldades peab kohus veenduma, et tagatud oleks süüdistatava kaitseõigus (sh võimalus konfidentsiaalselt kaitsjaga nõu pidada) ning et istungil tehnilise lahenduse abil osalemisega ei kahjustataks õigusemõistmise huve ega kohtumenetluse

[193] RKKKm 3-1-1-24-16, p 6.
[194] KrMS § 40^1 lg 1 kohaselt on kolmas isik füüsiline või juriidiline isik, kes ei ole kuriteos kahtlustatav, süüdistatav, kannatanu ega tsiviilkostja, kuid kelle õiguste või kohustuste üle võidakse kriminaalasja lahendamisel või erimenetluses otsustada.

vahetuse ja avalikkuse põhimõtet.[195] Selleks, et isiku asja arutamise juures viibimise piirang oleks proportsionaalne, peab kohus veenduma, et isiku kaitseõigus on tagatud, mis eeldab väga hea kvaliteediga audiovisuaalsete tehniliste lahenduste kasutamist ning süüdistatavale kaitsjaga suhtlemise võimaluse tagamist. Riigikohus on otsuses nr 3-1-1-18-08, p 14.1, selgitanud, et õigus viibida oma kohtuasja arutamise juures hõlmab ka süüdistatava õigust olla kohtu poolt ära kuulatud ning seda, et kohus peab tema seisukohta kohtuotsust koostades arvestama ja sellega mittenõustumist põhjendama. Seega õigus olla oma kriminaalasja arutamise juures tähendab ka süüdistatava õigust vaielda vastu kõigile nendele süüdistuse väidetele, millest sõltub tema teole antav materiaalõiguslik hinnang.[196]

Audiovisuaalses vormis võib kohtuistungil osaleda ka tõlk – seda lubab KrMS § 161 lg 1. Seejuures on ääretult oluline, et kasutatav tehniline vahend võimaldaks tagada kvaliteetse tõlke. Tõlke kvaliteet on oluline, et tagada menetlusosalisele kohtuistungil toimuvast arusaamine. Vastasel juhul võib kehva ühenduse tõttu tõlge olla katkendlik või halvasti mõistetav. Tõlgi juuresolek on vajalik, et menetluse keelt mittevaldaval isikul oleks võimalik toimingus osaleda võrväärselt keelt valdava isikuga.[197]

Praktikas hakati nn videokonverentsi meetodit kasutama edukalt juba alates 2005. aasta veebruarist ennetähtaegsete vangistusest vabastamise taotluste menetlemisel: kinnipeetavaid ei toimetatud enam alati mitte kohtumajja, vaid nad võtsid vabastamistaotluse arutelust osa videoekraani abil.[198] Selleks loodi tehnilised 2009. aastaks vajalikud tehnilised lahendused vanglatesse, kohtumajadesse, Eesti Kohtuekspertiisi Instituuti ja Viru Ringkonnaprokuratuuri. Tänaseks on kvaliteetsed videokonverentsi seadmed olemas kõigis Justiitsministeeriumi haldusala hoonetes.

Videokonverentsi vahendusel on hakatud pidama nii terveid kohtuistungeid ning seal on ka hakanud osalema menetlusosalised just 2020. aasta märtsikuust alates, mil tekkis ootamatu vajadus lähikontaktide vältimiseks. Kõige enam osalesid kohtuistungil videokonverentsi teel prokurörid, aga ka süüdimõistetud ja nende kaitsjad.

---

[195] 170 SE seletuskiri, lk 57.
[196] 170 SE seletuskiri, lk 56.
[197] RKKKo 3-1-1-157-05, p 10.
[198] Kriminaalmenetluse seadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seadus 599 SE seletuskiri, lk 20. Arvutivõrgus kättesaadav https://www.riigikogu.ee/tegevus/eelnoud/eelnou/ab9521d9-5558-45b8-c93a-b5122208c53b/ (12.04.2021).

Süüdistatava kaitsja on kriminaalasjas nr 1-20-3240[199] esitanud apellatsiooni kokkuleppemenetluses tehtud maakohtu otsuse peale, paludes see tühistada süüdistatava süüditunnistamise kohta. Nimelt alustati ja peeti läbirääkimisi virtuaalselt, süüdistatav viibis üksinda arestimajas ning prokuröri ja kaitsjat nägi ta vaid n-ö „teleka" vahendusel. KrMS ei näe ette võimalust kokkuleppe sõlmimiseks virtuaallahendust kasutades, süüdistatav peaks saama võimaluse prokuröriga vahetult läbi rääkida ja kaitsjaga samuti vahetult nõu pidada. See on vajalik selleks, et süüdistatav saaks väljendada oma vaba tahet kokkuleppe tingimuste osas ja et talle oleks kahtlusteta selge, millele ta alla kirjutab. Kohtukolleegium leidis oma otsuses, et süüdistatava kaitseõigust nii kokkuleppe sõlmimisel kui ka kohtus selle kinnitamisel ei ole rikutud. Kuigi kokkuleppe sõlmimise seisuga KrMS virtuaallaheduse teel kokkuleppemenetluse läbirääkimiste pidamise võimalust ette ei näinud, ei saa antud juhul rääkida süüdistatava kaitseõiguse rikkumisest. Süüdistatavale oli tagatud kaitsja abi, kokkuleppe sõlmiti kaitsja juuresolekul ning virtuaallahenduse kasutamisele menetluspooled vastuväiteid ei esitanud.

Kriminaalasjas nr 1-21-3744[200] esitas süüdistatav kokkuleppemenetluses tehtud maakohtu otsuse peale apellatsiooni, taotledes kohtuotsuse tühistamist ja õigeksmõistva otsuse tegemist. Süüdistatava sõnul sai ta kohtuistungi ajal vähesest aru, sest see toimus videokonverentsina ajal, mil viibis politseis. Kunagi varem pole ta videokonverentsi vahendusel suhelnud, kus kohtunik ja tõlk peaaegu üheaegselt rääkisid. Kõik toimus kiiresti. Ringkonnakohus sedastas oma otsuses, et KrMS § 246 lg 2 kohaselt võib kohus kokkuleppemenetluses korraldada kohtumenetluse poolte osavõtu kohtulikust arutamisest tehnilise lahenduse abil, mille tulemusena menetlusosalised vahetult näevad ka kuulevad kohtus toimuvat ja saavad küsimusi esitada. Selles osas ei ole maakohus menetlusnorme rikkunud. Maakohtus toimunud kohtuistungil ei olnud süüdistataval ühtegi märkust selle kohta, et tema osalemine istungil oleks olnud tehnilise lahenduse tõttu kuidagi takistatud või raskendatud. Vastupidi, ta kinnitas, et on sõlmitud kokkuleppest aru saanud ning nõustus kõikide kokkuleppes kajastatud õiguslike järelmitega. Ühelegi muule konkreetsele kokkuleppemenetluse reegli rikkumisele ei ole süüdistatav oma apellatsioonis viidanud, mistõttu ei olnud süüdistataval õigust maakohtu otsust apellatsioonis märgitud küsimustes vaidlustada.

Eelnevad näited ilmestavad, kuidas süüdistatavad on üritanud tehnilise lahenduse abil kohtuistungil osalemist tuua ettekäändena, et vaidlustada kokkuleppemenetluses tehtud otsust,

[199] Tartu Ringkonnakohtu kohtumäärus kohtuasjas 1-20-3240 (08.06.2020).
[200] Tartu Ringkonnakohtu kriminaalkolleegiumi kohtuotsus kriminaalasjas 1-21-3744 (30.06.2021).

mis neile polnud sobilik. KrMS § 318 lg 3 p 4 ja lg 4 lubab esitada apellatsiooni kokkuleppemenetluses tehtud otsuse peale vaid juhul, kui tegemist on kriminaalmenetluse seadustiku 9. peatüki 2. jao sätete või KrMS § 339 lg 1 rikkumisega. Süüdistatav ja kaitsja võivad esitada apellatsiooni ka juhul, kui kokkuleppes kirjeldatud tegu ei ole kuritegu, see on karistusseadustiku järgi ebaõigesti kvalifitseeritud või kui süüdistatavale on kuriteo eest mõistetud karistus, mida seadus selle eest ette ei näe.

Mõlema näite puhul ei ole kohus aga lugenud kohtuistungil tehnilise vahendi abil osalemist põhjuseks, et süüdistataval oleks KrMS § 318 lg 3 p 4 ja lg 4 järgi õigust maakohtu otsust vaidlustada. Kuna kumbki süüdistatav (ega kaitsja) ei esitanud märkusi ega vastuväiteid istungi ajal, ei saa olla usutavad süüdistatavate argumendid selle kohta, et nad ei saanud tehnilise vahendi kasutamise tõttu istungil toimuvast arutelust aru. Seega on reaalne, et ka videokonverentsina toimuvatel istungitel on süüdistataval võimalik osaleda täiemahuliselt, võtta osa aruteludest, vaielda vastu ja esitada küsimusi. Arvestades vähest kohtuvaidluste arvu, kus süüdistatav oleks ette heitnud asjaolu, et ta ei saanud videokonverentsina toimunud istungil toimuvast aru, võib asuda seisukohale, et kehtiv KrMSi säte on piisav ja sobiv.

3.3.2. Kaugülekuulamine

KrMS § 63 lõikes 1 sisalduv tõendi mõiste hõlmab ka kahtlustatava, süüdistatava, kannatanu, tunnistaja või asjatundja ütlusi[201]. Lisaks traditsioonilisele füüsilisele kohtumisele lubab KrMS korraldada ka kaugülekuulamist. KrMS §-s 69 sätestatud kaugülekuulamise võimalus on nüüdisaegsete tehnoloogiliste võimaluste juures järjest kasutatavam alternatiiv traditsioonilisele näost näkku ülekuulamisele. Olukorras, kus audiovisuaalset ülekannet võimaldavad seadmed on laialt kättesaadavad üle kogu maailma, annab isiku ülekuulamine, ilma et menetleja peaks füüsiliselt isiku juurde minema või isik menetleja juurde tulema, võimaluse märkimisväärselt kokku hoida nii reisimisele kuluvat aega kui ka selleks kulutatavat raha.[202]

Juba 2003. aastal vastu võetud KrMSis oli ette nähtud võimalus korraldada tunnistaja kaugeülekuulamine. Riigikogule esitatud esialgses eelnõu versioonis oli § 64 lõikes 4 tunnistaja

[201] Kriminaalmenetluse seadustik RT I, 29.12.2020, 10.
[202] Kriminaalmenetluse seadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse (kriminaalmenetluse seadustiku revisjon) eelnõu kolmandale kooskõlastusringile esitatud seletuskiri. Arvutivõrgus kättesaadav eelnõude infosüsteemis https://eelnoud.valitsus.ee/main/mount/docList/aca7e3cf-d349-4a40-a700-bbdb2b5a115c?activity=1#9eHB2tIo (28.02.2021).

turvalisuse tagamise meetmena märgitud järgmist: „Kohtumenetluses kuulatakse leppenimega tunnistaja üle telefonitsi või muude tehnikavahendite abil, kasutades vajaduse korral häälemuutmisseadmeid.“.[203] Eelnõu arutelude käigus asendati § 64 lõikes 4 sõnad „telefonitsi või muude tehnikavahendite abil” „telefonitsi käesoleva seadustiku § 69 lõike 2 punktis 2 sätestatud korras”. Samuti täiendati seadust eraldiseisva kaugülekuulamise paragrahviga, milles sisaldus detailsemalt kirjeldatud kaugülekuulamise kord.[204]

Kaugülekuulamine KrMS § 69 kohaselt tähendab ülekuulamist kas tehnilise lahenduse abil, mille tulemusena on ütluste andjat näha ja kuulda vahetult ja talle on võimalik esitada küsimusi, või telefonitsi, mille tulemusena on ütluste andjat vahetult kuulda ja talle on võimalik esitada küsimusi.[205] Lühidalt tähendab see seda, et ütluste andjat on võimalik üle kuulata selliselt, et ta ei pea samal ajal füüsiliselt kohtusaalis viibima.

Praktikas toimub kaugülekuulamine nii, et menetlusosaline viibib kohtulikul arutamisel ülekuulamise ajal väljaspool istungisaali ja tema ülekuulamine kantakse samaaegselt pildis ja helis üle istungisaalis. Ülekuulatav võib audiovisuaalse kaugülekuulamise ajal viibida ka mõnes kohtu ruumis, kuid mitte istungisaalis. Ta võib viibida ka mõnes teises hoones või oma eluruumis.[206] Oluline on see, et kaamera on seatud üles selliselt, et võetakse üles ja kantakse üle lisaks näole ka kehahoiak ja žestid.[207]

KrMSi kuni 7. maini 2020 kehtinud regulatsioon nägi ette vaid tunnistajate või kannatanute (ja mitte teiste menetlusosaliste) kaugülekuulamise kolmel juhul: kui vahetu ülekuulamine on raskendatud, põhjustab ülemääraseid kulutusi (on koormav) või kui see on vajalik tunnistaja või kannatanu kaitseks.[208] Kõige olulisem kaugülekuulamise eesmärk oli seega tunnistaja või kannatanud kaitsmine. Kaugülekuulamine võimaldab tunnistajat kohtusaalis säästa otsesest kontaktist süüdistatavaga ning ühtlasi aitab tagada tema kaitset avalikkuse, süüdistatava lähikondlase ja meediaesindajate eest. [209] Lisaks on kaugülekuulamine hea lahendus alaealise

[203] Kriminaalmenetluse seadustik 594 SE. Eelnõu algtekst. Arvutivõrgus kättesaadav Riigikogu veebilehel https://www.riigikogu.ee/tegevus/eelnoud/eelnou/3cbbe022-95f6-32ec-be3c-9c4aa0001f34/Kriminaalmenetluse%20seadustik (28.02.2021).
[204] Muudatusettepanekud kriminaalmenetluse seadustik 594 SE juurde. Muudatusettepanekud on kättesaadavad Riigikogu veebilehel kriminaalmenetluse seadustik 594 SE menetluse juures failides pealkirjaga „ME loetelu 2“ (ettepanekud nr 36 ja 37) ja „ME loetelu 2“ (muudatusettepanek nr 6).
[205] Kuni 7. maini 2020 kehtinud redaktsioon RT I, 20.12.2019, 8 ja käesoleva magistritöö koostamise ajal kehiv redaktsioon RT I, 29.12.2020, 10.
[206] Kergandberg, E., Sillaots, M. Kriminaalmenetlus, lk 355.
[207] Kergandberg, E., Sillaots, M. Kriminaalmenetlus, lk 356.
[208] Kriminaalmenetluse seadustik, RT I, 20.12.2019, 8.
[209] Kergandberg, E., Sillaots, M. Kriminaalmenetlus, lk 357.

tõendiallika ülekuulamiseks, kuna võimaldab säästa alaealist ülekuulatavat ristküsitlusega kaasnevate negatiivsete tagajärgede eest.[210]

7. mail 2020. aastal jõustusid *abipolitseiniku seaduse ja teiste seaduste muutmise seaduse (COVID-19 haigust põhjustava viiruse SARS-Cov-2 levikuga seotud meetmed) eelnõu 170 SE* (edaspidi *170 SE*)[211] muudatused. COVID-19 haigust põhjustava koroonaviiruse pandeemilise levikuga seotud mõjude ja tagajärgede leevendamiseks väljatöötatud meetmete elluviimiseks esitas Vabariigi Valitsus Riigikogule eelnõu, kuhu oli koondatud ministeeriumide ettevalmistatud seadusemuudatused. Muuhulgas laiendati eelnõuga KrMSis kaugülekuulamise regulatsiooni, et oleks võimalik vähendada isikute vahelist füüsilist kontakti.

Esiteks lubati muudatusega muus menetlusseisundis kui tunnistajana kriminaalmenetluses osalevate isikute kaugülekuulamine. Asendades sõna „tunnistaja“ sõnaga „isik“, avardati kaugülekuulamise rakendusala sõnaselgelt kõikidele neile, keda on vaja üle kuulata. Lisaks sätestati KrMS § 75 lõikes 4 võimalus ka kahtlustatava kaugülekuulamiseks – järgida tuleb vastavaid kahtlustatava ülekuulamise kohta käivaid erisätteid. Süüdistatava kaugülekuulamise näeb teatud tingimustel ette KrMS § 269 lg 2 p 4.[212]

Teiseks lubati muudatusega kaugülekuulamine ülekuulatava mugavuse eesmärgil. Muudatus andis menetlejale võimaluse kaaluda kaugülekuulamise võimalust ka ülekuulatava seisukohast ning kaugülekuulamist rakendada juhtudel, kus vahetust ülekuulamisest saadav lisaväärtus (võimalus vahetult ülekuulatavaga samas ruumis viibides jälgida tema käitumist ning veenduda, et keegi ülekuulatavat ülekuulamise ajal ei mõjuta) ei kaaluks üles ülekuulatavale tekitatavat ebamugavust, mida talle menetluskuludena ei hüvitata.[213]

Kolmandaks võimaldati muudatusega korraldada kaugülekuulamine isiku huvide kaitset silmas pidades. See mis annab menetlejale võimaluse võtta arvesse isiku huvisid laiemalt, mitte ainult tunnistaja või kanatanu kaitset. Seadusemuudatus võimaldab kriminaalmenetluses otstarbekamalt kasutada olemasolevaid tehnoloogilisi võimalusi ning seeläbi hoida kokku menetlusressurssi ja väärtustada menetluses osalevate isikute aega.[214]

---

[210] RKKKo 3-1-1-104-16, 21.12.2016, p 11
[211] Abipolitseiniku seaduse ja teiste seaduste muutmise seadus (COVID-19 haigust põhjustava viiruse SARS-Cov-2 levikuga seotud meetmed) 170 SE. Seletuskiri arvutivõrgus kättesaadav https://www.riigikogu.ee/tegevus/eelnoud/eelnou/000826a5-0c93-407c-9fab-f173221748b4/ (28.02.2021).
[212] 170 SE seletuskiri.
[213] 170 SE seletuskiri.
[214] 170 SE seletuskiri.

Varasemalt on Margus Kurm, kriminaalmenetluse revisjoni töörühma liige, oma 2016. aasta analüüsis „Tõendite kogumisel dubleerimise vältimine kohtu- ja kohtueelses menetluses“ toonud välja, et kaugülekuulamise võimaluste laiendamist tuleb kaaluda. Kurm pakkus välja kaks põhimõttelist valikut: 1) loobuda kõigist hetkel kehtivatest eeldustest, jättes ülekuulamise vormi menetleja vabaks otsustuseks. Sisuliselt muudaks see kaugülekuulamise seaduse silmis samaväärseks vahetu ülekuulamisega; 2) täiendada kaugülekuulamise eelduste loetelu, nt sellega, et kaugülekuulamine on lubatud, kui puudub alus kahelda tunnistaja usaldusväärsuses. Sellisel juhul jääks kaugülekuulamine siiski erandiks, kuid selle kasutamise võimalused oleks laiemad.[215]

Võib asuda järeldusele, et kriminaalmenetluse seadustikku täiendati liberaalsemalt kui varasemalt eksperdid ettepanekuid tegid. Kaugülekuulamist on võimalik korralda mitte ainult tunnistajaga, vaid ka teiste menetlusosalistega. Samuti on kaugülekuulamine võimalik näiteks olukorras, kus tunnistaja töögraafik ei võimalda teise linna ülekuulamisele tulla ning töölt eemale jäämisega seotud kulusid talle ei hüvitata. Seega on kaugülekuulamine võimaldanud paindlikumalt korraldada ütluste andmine.

Kohtuasjas 1-18-4600[216] apelleeris süüdistatava kaitsja, et süüdistatava endine abikaasa kui kannatanu kuulati põhjendamatult üle videokonverentsi teel, kuigi kõik teised kannatanud kuulati üle kohtusaalis. Videokonverentsi tehniline lahendus pidevalt hakkis ja seetõttu ei olnud kaitsjal ja ka temal endal võimalik teda korralikult küsitleda. Ringkonnakohtu arvates ei rikkunud maakohus kriminaalmenetlusõiguse norme sellega, et kuulas kannatanu üle KrMS § 69 lg 1 sätestatud kaugülekuulamise teel. 9. detsembril 2019 toimunud kohtuistungi protokollist nähtuvalt on kannatanu avaldanud kohtule, et ei saa kohtuistungil füüsiliselt viibida, kuna tal on kodus 3-aastane laps. Ka põhjendas kannatanu taotlust kaugülekuulamiseks transpordiühenduse puudulikkusega Jõhvi (kohtumaja asukoht) ja Pärnu (kannatanu elukoht) vahel.

Maakohus luges kannatanu poolt esitatud põhjendusi kaugülekuulamise läbiviimiseks aktsepteeritavateks ning teostas kannatanu ülekuulamise kaugülekuulamise teel. Ringkonnakohus nõustus maakohtu taolise otsustusega ning leidis, et maakohus ei rikkunud taoliselt tegutsedes KrMS § 69 lg 1 ega § 287 lg 5 sätteid. Lisaks ei nõustunud ringkonnakohus

[215] Kurm, M. Tõendite kogumisel dubleerimise vältimine kohtu- ja kohtueelses menetluses. Analüüs. 2016. lk 4. Arvutivõrgus kättesaadav https://www.just.ee/sites/www.just.ee/files/toendamine_m._kurm.pdf (21.03.2021).
[216] Tartu Ringkonnakohtu kriminaalkolleegiumi kohtuotsus kriminaalasjas 1-18-4600 (03.12.2020).

ka apellantide etteheitega, nagu takistanuks kaugülekuulamiseks kasutatud tehniline taristu neil korralikult kannatanut küsitleda. Kohtuistungi protokollist nähtuvalt on kaitsja küsitlenud kannatanut 30 minuti ja süüdistatav 7 minuti vältel, kusjuures ei kaitsja ega süüdistatav pole esitanud ühtegi märkust ülekuulamise läbiviimisel esinevate tehniliste probleemide kohta. Eeltoodut arvestades leidis ringkonnakohus, et apellantide sellekohased väited on otsitud ning kohus tagas apellantidele korrektse võimaluse kannatanu küsitlemiseks, mida apellandid ka aktiivselt kasutasid.

Kriminaalasjas nr 1-20-1578[217] anti kannatanu kohtu alla süüdistatuna KarS § 318 lg 1 järgi selles, et ta keeldus kriminaalmenetluses kannatanuna ütlusi andmast, ehkki tal polnud selliseks keeldumiseks seaduslikku alust. Viru Maakohus arutas tema süüdistust avalikel kohtuistungitel 20. ja 21. mail 2020. Süüdistatav võttis nendest kohtuistungitest osa audiovisuaalse tehnilise vahendi abil. Süüdistatav soovis viibida vahetult kohtusaalis, kuid seda taotlust kohus ei rahuldanud. Maakohus märkis, et kuigi eriolukord seoses COVID-19 haiguse levikuga on lõppenud, kehtivad valitsuse kehtestatud piirangud endiselt ja istungil osalemine video teel on eelkõige süüdistatava enda huvides. Tagatud on ka süüdistatava kaitseõigus, sest kohus teeb vaheaja, kui süüdistatav või kaitsja soovivad nõu pidada.

Ringkonnakohus leidis apellatsiooni arutades, et KrMS § 269 lg 2 p 4 järgi on süüdistatava osavõtt kohtuistungist tehnilise lahenduse abil erand, mille põhjendatust peab kohus alati hoolikalt kaaluma kaitseõiguse tagamise aspektist. Lisaks peab olema täidetud tingimus, et süüdistatava kohtuistungile toimetamine on mingil põhjusel raskendatud. Süüdistatav viibis vanglas, mistõttu tema kohtusse toimetamine ei olnud takistatud. Seega rikkus maakohus süüdistatava tehnilise lahenduse abil istungile kaasates kriminaalmenetlusõigust.

Riigikohus leidis oma otsuses[218], et tagades süüdistatava osavõtu kohtulikust arutamisest KrMS § 269 lg 2 p 4 alusel audiovisuaalse tehnilise lahenduse abil, toimis esimese astme kohus seaduslikult ning et ringkonnakohtu seisukoht on ekslik. Kohus sedastas, et tehniline lahendus, mille vahendusel süüdistatav kohtulikust arutamisest osa võttis, vastas KrMS § 69 lg 2 p 1 tingimustele. Samuti oli süüdistataval tõhus võimalus suhelda konfidentsiaalselt oma kaitsjaga. Kolleegium ei nõustunud aga ringkonnakohtuga selles, et oli täitmata KrMS § 269 lg 2 p-s 4 märgitud eeldus, mille kohaselt peab süüdistatava kohtusse toimetamine olema raskendatud.

[217] RKKKO 1-20-1578
[218] RKKKO 1-20-1578, p 16-22

Kolleegium nõustus oma otsuses ringkonnakohtu seiskohaga, et osavõtt kohtuistungist tehnilise lahenduse abil on erand ja selle võimaluse kasutamist peab kohus iga kord hoolikalt kaaluma. Samas ei pruugi kohtusse ilmumise raskendatus KrMS § 269 lg 2 p 4 mõttes seisneda alati vaid selles, et süüdistatava kohtusse tulek või toimetamine on füüsiliselt takistatud. KrMS § 269 lg 2 p 4 praeguse redaktsiooni kehtestanud seaduse eelnõu seletuskirjast selgub, et selle sätte põhieesmärk oli leevendada COVID-19 haigust põhjustava koroonaviiruse pandeemilise leviku mõju ja tagajärgi. KrMS § 269 lg 2 p 4 muutusega sooviti tagada eelkõige pandeemia ajal kõigi tavapäraste menetluste kulg ja see, et kohtupidamine ei peatuks teadmata ajaks. Seega laiendas seadusandja süüdistatava kaugosavõtu võimalust just koroonaviiruse pandeemilise leviku tõttu.

Seetõttu jõudis kolleegium seisukohale, et COVID-19 haigust põhjustava koroonaviiruse leviku oht võib teatud tingimustel olla käsitatav KrMS § 269 lg 2 p-s 4 nimetatud asjaoluna, mis raskendab süüdistatava kohtusse toimetamist. Käsilolevas asjas tuli süüdistatava kohtusse toimetamise raskendatust jaatada. Istungiprotokollist nähtub, et maakohus tegi otsustuse süüdistatava kohtuistungile toimetamata jätmise kohta kaalutletult. Sellel, et eriolukord Eestis lõppes 18. mail 2020, määravat tähendust ei ole. Eriolukord asendus tervishoiualase hädaolukorraga, koroonaviiruse levik jätkus. Arvestada tuleb kohtuistungi ajalist konteksti. Ehkki nakatumisnäitaja oli 2020. a mai teises pooles palju väiksem kui näiteks 2020. a lõpus või 2021. a esimeses pooles, oli tegemist võrdlemisi uue ja harjumatu nähtusega ning selle suhtes valitses palju teadmatust. Ühiskonnas oli tavapärane rakendada viiruse leviku vältimiseks rangeid ettevaatusabinõusid. Seda silmas pidades oli esimese astme kohus õigustatud arutama kriminaalasja nii, et süüdistatav osales kohtuistungil video teel. Seejuures väärib esiletoomist, et kohus tagas süüdistatavale võimaluse suhelda oma kaitsjaga privaatselt. Riigikohus märkis oma otsuses ka, et pandeemia mõju vähenemisel väheneb ka õigustus KrMS § 269 lg 2 p 4 erandi kasutamiseks.

Kaugülekuulamise korraldamisel tuleb silmas pidada ohtusid, mida kujutavad endast süvavõltsingud. Nimelt võib ülekuulatav lisaks mõnele kohturuumile (mis ei ole istungisaal) või vangla pakutavale videokonverentsi võimalusele ruumile ka oma eluruumis. Ülekuulatava isiku isikusamasuse tuvastamisel ning ka hiljem kogu ülekuulamise vältel peab menetleja olema pidevalt veendunud, et tehnilise vahendi kaudu on ütlusi andmas õige inimene ning tegemist ei ole võltsinguga.

Süvavõltsingu tuvastamise ja riskide maandamise näitena võib tuua ühe hiljutise Eesti eduloo – kaugtõestamise teel notariaalsete toimingute tegemine. Kaugtõestamise abil on võimalik teha

notariaaltoiminguid videosilla vahendusel, st klient ei pea enam notaribüroosse tehingu tegemiseks ilmtingimata minema.[219] Kaugtõestamiseks on kaks võimalust: tehingus osaleja viibib kas Eesti välisesinduses[220], kus on vajalik videosilla loomise ühendus olemas, või väljaspool välisesindust, nt kodus.

Kaugtõestamise oluliseks etapiks on isikusamasuse tuvastamine. Selleks kasutavad notarid kahte võimalust. Kui klient soovib kaugtõestamist välisesinduses, tuvastab tema isikusamasuse välisesinduse töötaja, kes võimaldab seejärel kliendil välisesinduses eraldatud ruumis oleva arvuti kaudu kaugtõestuses osaleda. See protsess on turvaline ja kontrollitav – välisesinduse töötaja veendub, et tegemist on õige isikuga, ning ruumis asuv arvuti vastab turvanõuetele. Kui klient soovib aga kaugtõestust selliselt, et ta osaleb väljaspool välisesindust ehk mõnes teises temale sobivas ruumis, näiteks kodus, tuvastatakse tema isikusamasus Veriffi näotuvastusteenuse abil. Reaalset kohtumist ühegi isikuga kaugtõestust soovival isikul seega pole. Juhul, kui Veriff tuvastab süvavõltsingu või muu petturluse, ei lasta isikut tehingu sooritamisele ligi. Samas on aga kaugtõestamisel kasutusel nn topeltkontroll: pärast seda, kui Veriff on näotuvastuse sooritanud, kontrollib isikusamasust veebikaamera kaudu veel ka notar. Juhul, kui notar ükskõik millisel hetkel peaks kahtlema, et isik pole tegelikult see, kes peaks tehingus osalema, on notaril õigus tehingu tõestamine katkestada. Seega võib öelda, et Notarite Koda on korraldanud efektiivse lahenduse, kuidas tagada võltsingute välistamine notariaalsete toimingute tegemisel.[221] Sellise teenuse kasutamise vajadust võiks hinnata ka Eesti kohtusüsteem.

Kokkuvõttes võimaldab KrMS, eriti pärast 2020. aasta mais jõustunud muudatusi osaleda nii kohtuistungil kui ka anda ütlusi videosilla vahendusel. Seda võimalust oodati kaua ning eriolukorra tõttu kiirelt vastu võetud seaduse muudatused on seda ka võimaldanud, tagades seeläbi paindlikuma kohtupidamise nii menetlejatele kui menetlusosalistele. Kaugülekuulamise teel antud ütlusi on võimalik kasutada tõenditena, kuid menetleja peab tähelepanelikult

[219] Magistritöö kirjutamise ajal on võimalik vaid sajaprotsendiline kaugtõestamine, st kõik tehinguosalised peavad olema virtuaalruumis. Nn hübriidtõestus, kus osad tehingupooled on notaribüroos kohapeal ja teised osalevad videosilla vahendusel, hetkel veel võimalik ei ole. Selle võimaldamiseks on arutelud veel Notarite Koja ja Justiitsministeeriumi vahel käimas.

[220] Välisesindustes saab kaugtõestamise teel teha vaid notariaadimäärustiku § 12^1 lõikes 6 nimetatud ametitoiminguid, milleks on nt tehinguid osaühingu osadega, volikirjade tõestamine, abiellumis- ja lahutamisavalduse ning pärimisavalduse esitamine. Kaugtõestamise teel on toiminguid võimalik hetkel teha viies Eesti välisesinduses - Helsingis, Stockholmis, Brüsselis, Riias ja Londonis.

[221] Süvavõltsingu tehnoloogia arenemisel võib aga Notarite Koja poolt usaldatav eraettevõte ebaõnnestuda süvavõltsingu tuvastamisel. Sellisel juhul jääb vastutus notari õlule. Notaritel on praktikas kasutusel mitmeid meetodeid, kuidas veenduda, et teisel pool ekraani on üldse reaalne inimene, mitte näiteks süvavõltsinguga videosalvestis, kuid tehnoloogia arenemisel võivad need meetodid jääda liiga arhailisteks.

veenduma, et ülekuulamise ajal on teisel pool ekraani siiski päris inimene, mitte sünteesitud võltsing.

3.4. KRMSI REVISJONIST TULENEVATE MUUDATUSTE MÕJU DIGITAALSETE TÕENDITE KASUTAMISELE

Vabariigi Valitsus esitas Riigikogule 01.04.2021 *kriminaalmenetluse seadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse (kriminaalmenetluse seadustiku revisjon) 367 SE* (edaspidi *KrMSi revisjon*). Riigikogu algatas eelnõu 05.04.2021[222]. 12.04.2021 toimunud õiguskomisjoni istungil tegi komisjon ettepaneku võtta eelnõu täiskogu päevakorda 05.05.2021 ning määras muudatusettepanekute tähtajaks 19.05.2021. Esimest lugemist Riigikogu täiskogus ei toimunud[223], küll aga esitati eelnõule mitmeid muudatusettepanekuid.

KrMSi revisjoni eelnõuga tehakse KrMSis ja teistes seadustes mitmeid muudatusi, millest osad puudutavad ka tõendeid. Paljude teiste muudatuste seas on eelnõuga võetud eesmärgiks täiustada tõendite süstemaatikat: korrastatakse tõendite liigitust ja luuakse dokumentaalse tõendi mõiste.[224] Eelnõuga asendatakse senine dokumendikeskne keelekasutus, mis lähtub traditsioonilisest menetluse paberil vormistamisest, neutraalsema keelekasutusega, mille puhul ei ole oluline, kas teave on talletatud elektroonselt, paberil või muul viisil (nt analoogtehnoloogial põhinev helisalvestis).[225]

Senine tõendite põhiliigitus on fikseeritud KrMS § 63 lõikes 1, loetledes üpris detailselt tõendina kasutatavad asitõendid, dokumendid, teabetalletused jms. See sõnastus jääb KrMSi revisjoniga minevikku ning muudetakse ja sõnastatakse järgmiselt: "Tõend kriminaalasjas on ütlus, asitõend või dokumentaalne tõend.". Muudatus on tingitud üldise mõisteaparaadi muutmisest (eelkõige dokumentaalse tõendi mõiste kriminaalmenetlusse toomisest).[226]

[222]Kriminaalmenetluse seadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seadus (kriminaalmenetluse seadustiku revisjon) 367 SE menetluskäik Riigikogu veebilehel. Arvutivõrgus kättesaadav https://www.riigikogu.ee/tegevus/eelnoud/eelnou/d10291ef-980a-4b1d-8852-bab30d7e25f3/Kriminaalmenetluse%20seadustiku%20muutmise%20ja%20sellega%20seonduvalt%20teiste%20seaduste%20muutmise%20seadus%20(kriminaalmenetluse%20seadustiku%20revisjon) (12.04.2021).

[223] Eelnõu esimest lugemist pole käesoleva magistritöö esitamise ajaks (juba ligi aasta) endiselt Riigikogu täiskogus toimunud. Magistritöö autor usub, et eksisteerib tõenäosus, et poliitilise toetuse puudumise ja eelnõule tervikuna tugevalt kritiseerivate arvamust tõttu langeb eelnõu Riigikogu kodu- ja töökorra seaduse § 96 alusel menetlusest välja seoses Riigikogu volituste lõppemisega 2023. aasta kevadel.

[224] KrMS revisjoni seletuskiri, lk 3

[225] KrMS revisjoni seletuskiri, lk 6.

[226] KrMS revisjoni seletuskiri, lk 11.

Dokumentaalse tõendi mõiste alla mahuvad kõik seni kehtinud § 63 lõikes 1 eraldi loetletud dokumendid – menetlustoimingute protokollid ja erinevad salvestised (nt videosalvestis ja helisalvestis). Dokumentaalne tõend on igasugune teabetalletus, mis sisaldab andmeid kriminaalasja lahendamiseks tähtsust omavate asjaolude kohta. Ei ole tähtis, kas andmekogum on inimese poolt vahetult tajutav või taasesitatav mingi tehnilise lahenduse abil. Selliselt on dokumentaalse tõendi mõistesse haaratud ka digitaalsel kujul esinevad andmehulgad – iseenesest ei ole vajalik, et dokumentaalsel tõendil oleks füüsiline keha. Veelgi enam, oluline on eristada andmekandjat ja dokumentaalset tõendit: mälupulk, millel ehk tuhandeid faile, on andmekandja ning võib olla asitõend, dokumentaalseks tõendiks on aga need failid, mis on mälupulgale salvestatud ja millel on kriminaalasjas tähtsust. Füüsilist keha omava dokumentaalse tõendi eristamisel asitõendist on oluline eelkõige see, milles seisneb objekti tõendiväärtus. Asitõendiks saab olla vaid kehaline ese. Kui eseme tõendiväärtus seisneb selle individuaaltunnustes, st tema väliskujus, füüsikalistes või keemilistes omadustes, toimimisviisis, asukohas või olemasolus, on tegu asitõendiga. Kui aga eseme tõendiväärtus seisneb sellel talletatud teabes (olgu selleks siis mingi tekst või pilt), on tegu dokumentaalse tõendiga. Sealjuures ei ole välistatud, et sama ese on korraga nii dokumentaalne kui ka asitõend.[227]

Digitaalsete tõendite vaatenurgast on see muudatus äärmiselt oluline, kuna muudatuse tulemusena tuleb digitaalse tõendi puhul eristada edaspidi digitaalseid andmeid sellest elektroonilisest seadmest, millele see talletatud on. See tähendab, et kohus ei pea enam iga digitaalse tõendi juures märkima, millisel teabeallikal see paikneb, vaid saab seda teha siis, kui selleks ilmneb vajadus. Samuti on muudatus tehnoloogianeutraalne, võimaldades kasutada kõikvõimalikul kujul (mitte ainult digitaalseid, vaid ka mõne tulevikutehnoloogiaga loodud) olevaid tõendeid, millel pole füüsilist keha.

Dokumentaalseks tõendiks on ka video- ja helisalvestised, mis tähendab, et tõendamisel nendes sisalduva teabe kasutamiseks ei ole vaja korraldada vaatlust kui eraldi menetlustoimingut ja seda protokollida. Liigitades elektroonilised teabetalletused (eriti erinevad salvestised) dokumentaalsete tõendite alla, ei kehti nende kohta enam ka asitõendite regulatsioon, mida praktikas on sageli tõlgendatud selliselt, et salvestiste kohta tuleb kohustuslikult alati vaatlusprotokoll koostada. Lisaks süstemaatilisele selgusele annab dokumentaalse tõendi

[227] KrMS revisjoni seletuskiri, lk 20.

mõiste sätestamine seega ka mõõdetava kokkuhoiu erinevate menetlusdokumentide vormistamisele kuluvas ajas.[228]

Digitaalsete video- ja helisalvestiste liigitamine ümber asitõendist dokumentaalseks tõendiks on põhimõtteline muudatus. Ennekõike tähendab see seda, et nende vahetut vaatlemist ei tule korraldada. Samuti ei tule koostada ka vaatlusprotokolli, mida seni on praktikas ka koostatud. Lisaks on võimalik edaspidi digitaalseid tõendeid lisada otse kriminaaltoimikusse. See viimane haakub KrMSi suure muudatusega, millega plaanitakse näha ette üldreegel, et toimikut peetakse digitaalselt ning et ka teabevahetus kriminaalmenetluse raames toimub eelkõige digitaalses vormis.

KrMSi seletuskirjas ei ole selgelt välja toodud, kuhu võiks kategoriseerida kõik ülejäänud digitaalsed tõendid, mis ei ole dokumendid või salvestised nagu näiteks e-kirjad ja metaandmed. Siiski on seletuskirjas toonitatud, et dokumentaalne tõend on igasugune teabetalletus, mis sisaldab andmeid kriminaalasja lahendamiseks tähtsust omavate asjaolude kohta. Kuna kõik digitaalsed tõendid on oma olemuselt teabetalletused, on nad võimalik kategoriseerida muudatuse jõustumisel dokumentaalsete tõenditena.

Lisaks täiendatakse KrMSi revisjoni eelnõuga KrMSi paragrahviga 124^1, mille lõige 1 täpsustab, et iga dokumentaalse tõendi või asitõendi puhul peab menetleja hindama selle tõendi asjakohastust. Seni § 286^1 lõikes 1 sisaldunud asjakohasuse nõue, et kohus võtab vastu ainult sellise tõendi ja korraldab selliste tõendite kogumise, millel on kriminaalasjas tähtsust, tuuakse KrMSi ka menetleja tasemele. Menetleja peab iga dokumentaalse tõendi või asitõendi puhul hindama, kas see tõend muudab mingi kriminaalasjas tähtsa asjaolu rohkem või vähem tõenäoliseks.[229] Seletuskirjas pole täpsustatud, miks selline muudatus vajalik on, kuid siin võib seadusandjal olla õigusselguse loomise eesmärk.

Viimase olulise muudatusena käesoleva magistritöö kontekstis on KrMS täiendamine ka teise §-s 124^1 asuva lõikega järgmises sõnastuses: „Kui dokumentaalne tõend või asitõend antakse menetlejale üle, võtab menetleja meetmeid, et tõend oleks hiljem selgesti identifitseeritav ning et kriminaaltoimikust nähtuks, kellelt ja millal dokumentaalne tõend või asitõend on vastu võetud.“. Seletuskirjas on täpsustatud, et kui asitõend või dokumentaalne tõend antakse üle sellise menetlustoimingu käigus, mille kohta menetleja koostab protokolli, on käitlusahelat

[228] KrMS revisjoni seletuskiri, lk 21.
[229] KrMS revisjoni seletuskiri, lk 21.

puudutavad andmed tavaliselt fikseeritud protokollis. Kui aga protokolli ei koostata, on vaja tõendi võtmine kriminaaltoimikusse dokumenteerida muul viisil, nt menetleja koostatavas õiendis. Dokumenteerimisnõue on täidetud ka siis, kui vajalikud andmed nähtuvad muust kriminaaltoimiku dokumendist – nt toimikus leiduvas kannatanu e-kirjas menetlejale viidatakse ka digifotodele, mille kannatanu menetlejale saatis.[230] See muudatus on seotud tõendi päritolu, tervikluse ja ehtsuse kontrolliga. Menetleja jaoks on muudetud lihtsamaks käitlusahela dokumenteerimine, kuid seda, ka see muudatus omab ka reaalset kasu, näitab vaid praktika.

KrMSi revisjoniga ei ole loodud eraldi digitaalse tõendi eriregulatsiooni, kuid selle asemel on seadusandja väljendanud oma selget tahet paigutada digitaalsed tõendid dokumentaalsete tõendite kategooriasse. Seletuskirjas on avaldatud lootust, et digitaalsete tõendite kasutamine muutub selgemaks ja lihtsamaks tänu dokumentaalse tõendi mõiste juurutamisega. Käesoleva töö autori hinnangul on selline tõendite liigituse korrastamine uuenduslik ja võib potentsiaalselt lihtsustada digitaalsete tõendite kasutamist kriminaalmenetluses. Oluline on menetlejate asjakohased koolitused eelnõu jõustumisel, et muudatusi ei asutaks vääralt tõlgendama.

[230]KrMS revisjoni seletuskiri, lk 21.

KOKKUVÕTE

Käesoleva magistritöö eesmärk oli uurida, kas digitaalsel kujul andmete kasutamine kohtumenetluses tõenditena on võimalik ning kas KrMSi regulatsioon võimaldab kohtul viia läbi ka digitaalsete tõendite hindamise. Infoühiskond on sundinud viima kohtumenetlust paberil toimikute ja tõendite juurest digitaalsete lahenduste suunas Digitaalseid dokumente kasutatakse kriminaalmenetluses tõenditena üha enam. Paberkujul tõendite kasutamise vähenemine soodustab ka täisdigitaalsele kohtumenetlusele üle minemist. Eesti kohtumenetlus on üks efektiivsemaid Euroopas ennekõike oma edukalt toimivate infosüsteemide tõttu. Justiitsministeerium on võtnud suunaks viia digitaalseks nii tsiviil-, haldus- kui kriminaalmenetluse toimikud, võimendades seeläbi ka digitaalsel kujul andmete edastamist.

Digitaalseks tõendiks võib lugeda digitaalsel kujul olevaid andmeid, millel on kohtumenetluses tõenduslik väärtus. Digitaalsel kujul on andmed siis, kui nende vaatlemiseks tuleb kasutada mõne elektroonilise seadme abi või kui need on loodud, neid on muudetud või neid hoitakse elektroonilises seadmes. Digitaalseid tõendeid on võimalik kategoriseerida selle järgi, kust neid on võimalik koguda: olgu see siis elektroonilisest seadmest, võrgust või võrgurakendusest (ehk digitaalse tõendi asukoha järgi). Samuti on digitaalseid tõendeid võimalik kategoriseerida sisu looja järgi: eristada võib inimese loodud, elektroonilise seadme loodud ning mõlema kombinatsioonis loodud digitaalseid tõendeid. Oluline on eraldi markeerida, et kõik digitaalsed dokumendid sisaldavad endas ka metaandmeid, mida tuleb tõenditena käsitleda nende eripära tõttu ka eraldiseisvana. Metaandmed on andmed andmete kohta ja sisaldavad endas väga palju lisainfot digitaalse dokumendi kohta.

Uutel tehnoloogiatel tuginevatesse tõenditesse on kohtud alati esialgu pelglikult ja suisa põlglikult suhtutud. Suurima hirmu on põhjustanud nende tõendite usaldusväärsuses kahtlemine. Tänapäeval on selline hirm tegelikult isegi täiesti õigustatud, kuna digitaalsed tõendid on füüsilistest tõenditest lihtsamini muudetavad, kahjustatavad ja hävitatavad. Digitaalse tõendi usaldusväärsuses tuleb seega selle tõendina kasutamisel eriti veendunud olla. Samuti tuleb kohtul veenduda digitaalse tõendi tervikluses, ehtsuses ja usutavuses. Digitaalse tõendi terviklus puudutab seda, kuidas tõendiga ümber on käidud ning ega andmeid ei ole ilma vastava autoriseerimiseta muudetud, need on õiged, täielikud, ajakohased ja autentsed. Andmete terviklus on oluline põhimõte ka infoturbes, mistõttu on loogiline, et seda tuleb rakendada ka digitaalsete tõendite kasutamisel. Digitaalse tõendi päritolu tuleb tuvastada sarnaselt füüsilisele tõendile, lihtsalt teistsuguseid meetodeid kasutades. Kui füüsilise tõendi

autoris saab veenduda näiteks käekirja, allkirja või mõne muu tõendi abil, mis näitab tõendi loojat, siis digitaalse tõendi päritolu võib küll saada teada seadme täpsusega, kuid selle välja selgitamine, kes reaalselt selle loonud on, võib osutuda keeruliseks.

Digitaalseid tõendeid on lihtsam muuta ja rikkuda kui füüsilisi tõendeid. Samal ajal võib olla keeruline tuvastada, et tõendit on muudetud. Kehtib reegel, et mida lihtsam oli tõendit muuta, seda lihtsam on seda muutmist tuvastada. Mida keerulisem oli digitaalse tõendi muutmise tehnoloogia, seda keerulisem on ka muutmise tuvastamine. Kõige keerulisemaks tõendite muutmise tehnoloogiaks võib pidada pidevalt arenevat süvavõltsingute tehnoloogiat, millega on võimalik võltsida nii heli kui videot, luues seeläbi audivisuaalseid võltsinguid. Süvavõltsingu loomine on väga lihtne ning jõukohane igale arvutikasutajale. Süvavõltsingute mõju digitaalse meediumi usaldusväärsusele on võimas, kuid see omab ka kitsamalt mõju kohtumenetlusele. Esiteks võivad süvavõltsingud tuua kaasa kohtutele töökoormust seeläbi, et kohtutesse hakkavad jõudma kahju hüvitamise nõuded, mille aluseks on süvavõltsingu videoga tekitatud kahju. Teiseks on neil kohtumenetluses võltsitud tõendite roll. Kohtumenetluses tõese tõendi pähe teadlikult või ka ekslikult esitatud süvavõltsing võib põhjustada vääradel alustel tehtud otsuse. Samuti võib see tuua kaasa vastaspoolele tõendamiskoormuse, et veenduda ise ja veenda ka kohut tõendi võltsingus. Lisaks omab süvavõltsingu tehnoloogia olemasolu laiemat mõju üldisele tõendite usaldusvääruses kahtlemisele: näiteks võib vastaspool või kohus arvata, et tegemist on võltsitud tõendiga, kuigi tegelikult see nii pole. Süvavõltsinguid on võimalik kasutada ka videokonverentsi vahendusel istungist osavõtmisel, mistõttu kujutavad need ohtu ka sellisele ülekuulamise lahendusele. Süvavõltsingute tuvastamiseks on olemas tehnoloogiad, mis arenevad koos süvavõltsingu arenguga, kuid võivad siiski süvavõltsingu tehnoloogia arengust maha jääda.

KrMSis erisätteid digitaalsete tõendite kohta ei ole. Kehtivas KrMSis on tõendi mõiste küllaltki üldsõnaline, jättes ruumi seda ka digitaalsetele tõenditele kohaldada. Kohtupraktika toetab digitaalsete tõendite kasutamist tõendina kriminaalmenetluses. Kohtud on lugenud digitaalsel kujul salvestisi ja e-kirju asitõenditeks, mis tähendab, et need vajavad ka vaatlusprotokolli. Ka metaandmeid on kohus asitõendina kasutatavad kui digitaalsed tõendid.

Digitaalseid tõendeid tuleb sarnaselt traditsioonilistele tõenditele hinnata, läbides kõiki olulisi hindamise etappe: asjakohasuse, lubatavuse, usaldusväärsuse ja tõendi lõppväärtuse hindamise etapid. Digitaalne tõend peab omama kriminaalasjas tähtust ja olema kogutud selliselt, et seda kogudes ei ole riivatud kellegi õigusi või põhjustatud kahju. Digitaalse tõendi usaldusväärsuse

kontrollimises kriminaalmenetluses tuleb olla hoolas, et digitaalset tõendit ei oleks märkamatult muudetud, jättes usaldusväärse mulje. Digitaalsete tõendite lõppväärtus kujuneb tõendite hindamise lõppetapis. Kohtupraktikat analüüsides oli võimalik asuda seisukohale, et kohus ei ole takerdunud digitaalse tõendite hindamisel olemasoleva regulatsiooni taha, mistõttu võib pidada olemasolevat KrMSi regulatsiooni piisavaks ka digitaalsete tõendite hindamisel.

Kuna tõendiks on KrMSi järgi ka ütlused, peatus käesolev magistritöö ka kaugülekuulamisel ja seeläbi ütluste saamisel. KrMS on juba 2003. aastast võimaldanud korraldada tunnistaja ja kannatanu kaugeülekuulamist eelkõige nende turvalisuse kaalutlustel, kui vahetu ülekuulamine on raskendatud või kui see on ülemäära koormav. 2020. aasta maikuust sisaldub KrMSis ka võimalus kuulata üle lisaks tunnistajale ja kannatanule kõigi teiste isikute ülekuulamine. Lisaks leevendati kaugeülekuulamise korraldamise tingimusi ja lubati seda teha ka mugavuse eesmärgil. Vaatamata sellele, et kaugülekuulamine on lähikontaktide vähendamise eesmärgil, aga ka mugavuse ja ütluste andja turvalisuse kaalutlustel kasulik lahendus, tuleb menetlejal veenduda, et teisel pool ekraani on siiski õige inimene. Selleks tuleb tuvastada kindlasti isikusamasus ja veenduda, et ei kasutata süvavõltsingut. Näiteks kaugtõestamisel on kasutusel Veriffi teenus, mis tehnoloogia abil aitab süvavõltsingut tuvastada.

Riigikogu algatas 05.04.2021 KrMSi revisjoni eelnõu, millega tehti KrMSis mitmeid käesoleva magistritöö teemaga haakuvaid muudatusi. Suurima muudatusena luuakse KrMSi uue tõendi liigina dokumentaalne tõend. Selle tingis ka uue tõendite liigituse ümberkorraldamine, mille tulemusena on muudatuse kohaselt tõendiks kriminaalasjas ütlus, asitõend või dokumentaalne tõend. Seletuskirja kohaselt saab muudatuse kohaselt hakata eristama dokumentaalseid tõendeid nende andmekandjast. Dokumentaalsel tõendil ei pea olema füüsilist keha, mistõttu on edaspidi võimalik kategoriseerida kõik digitaalsed tõendid dokumentaalseteks tõenditeks. Kuna digitaalsed tõendid ei ole muudatuse kohaselt asitõendid, ei tule neid eraldi vaadelda ega koostada vaatlusprotokolli. Samuti on muudatus tehnoloogianeutraalne, võimaldades kasutada mitte ainult digitaalseid, vaid ka mõne tulevikutehnoloogiaga loodud andmeid tõenditena kriminaalmenetluses.

ABSTRACT

PERSPECTIVES OF THE USE OF INFORMATION TECHNOLOGY AND DIGITAL FORMS AS EVIDENCE IN CRIMINAL PROCEEDINGS

Many people's lives and activities are now influenced by information and communication technology (ICT), which affects them both at home and at work. Not only that, but ICT is also one of the most important pillars of the Estonian e-state, as it enables various state agencies to communicate with one another as well as with citizens and businesses, as well as to exchange data. The advancement of information technology has even reached the realm of legal proceedings. Court proceedings are more efficient, and litigants have better access to justice because of the use of ICT.

Two advanced information systems, which have been widely used in Estonia by both courts and participants in proceedings, are responsible for the efficiency, speed, and electronic communication. First, the court information system, which is a tool for the administration of justice and the administration of courts that directly reduces the workload of courts, the time required to perform procedural acts, and therefore the time required to meet procedural deadlines. As a second point, Estonia has an important and useful web-based information system known as the "e-file system," which allows participants in proceedings and their representatives to electronically submit procedural documents and to track the progress of the court proceedings that are related to them.

High-quality evidence is a critical pillar of criminal proceedings, as without it, a fair decision is impossible. Along with so-called traditional evidence, digital evidence now accounts for a growing portion of the evidence presented in court proceedings.

The concept of digital evidence is subject to a variety of interpretations. In its most basic definition, digital evidence is information that has been stored in digital form and that can be reproduced in a manner that is legally acceptable. Many times, the terms "electronic evidence" and "digital evidence" are used to refer to the same thing. This master's thesis makes extensive use of the term "digital evidence," which refers to any certificate in digital or electronic form that is stored on digital devices. This is done for the sake of consistency and clarity.

Digital evidence can be defined as data that must be viewed through an electronic device (in digital form) to be perceived by a person, or data that has been in digital form at some point. To be digital, data must be created, modified, or transmitted using an electronic device. Additionally, the proof factor is critical in the case of evidence: the data must be capable of proving the facts.

Because the concept of digital evidence has numerous definitions, it can also be classified in a variety of ways. For instance, digital evidence can be classified according to the sources from which it can be gathered: from electronic devices, network connections, and network applications. This means that one option is to associate digital evidence with its location rather than its creator. The second option is to categorize the digital evidence by its creator. First, there is content created by one or more people: user-generated content is admissible as evidence if it is credible and certain, that is, if it can be linked to a specific individual. Second, the content generated automatically by a computer or electronic device, such as data logs (and also metadata). Lastly, there is content that is created using a combination of computer and human. If content is created by both a human and a machine, both must be verified as trustworthy to use as a piece of evidence.

While oral and later written evidence have been used in court for centuries, courts have also grown accustomed to evidence that would have been unthinkable 50 years ago. There are numerous examples throughout history of courts disregarding reliable photographs (in 1899), sound recordings (1934), films, and Internet extracts (1999). Despite prior views, courts have begun to accept the possibility that digital evidence may still be reliable in some instances. The principle of reliability is qualitative in nature and encompasses two dimensions: reliability and authenticity. Credibility should demonstrate that something can substantiate the facts contained within. Authenticity is the state of being what something claims to be.

Digital evidence is easily altered, damaged, and destroyed, which distinguishes it from so-called conventional evidence. Additionally, digital evidence can exist in multiple locations simultaneously. Even if there is reasonable doubt about the reliability of digital evidence, this does not automatically render it inadmissible; rather, it reduces the weight accorded by the court. For instance, if there is a suspicion that the evidence was tampered with prior to collection, this suspicion may diminish the weight accorded to the evidence.

When digital evidence is used in court proceedings, it is also necessary to document how the evidence was handled. If there is a period during which digital evidence could have been misinterpreted or ended up in the hands of an unauthorized person, the evidence's integrity must be questioned. The integrity of data, including digital evidence, refers to the data being undamaged, accurate, complete, current, and authentic.

The integrity of digital evidence can be expressed in a variety of ways, most notably in digital forensics. To begin, there is the integrity of the data, which indicates that it has not been altered without proper authorization, either intentionally or unintentionally. Another type of digital certificate integrity is duplication integrity, which means that duplicating data does not alter the data in any way, whether intentionally or unintentionally, and that the duplicate is identical to a bit copy of the original data. The third critical type of integrity for a digital certificate is the integrity of the computer (including the integrity of the system), which means that the computer (or system) produces the correct results when used properly, as it did when the certificate was created. integrity of the hardware. The final type of digital evidence integrity is process integrity, which refers to adhering to legal requirements for evidence collection, retrieval, interpretation, and presentation. In summary, integrity documentation enables the assertion that digital evidence has not been tampered with since it was collected and analysed.

The origin of a common evidence can be determined by the author's handwriting and other evidence. However, the risk associated with digital evidence is that a digital file may be created with a false identity, making it nearly impossible to identify or trace the true author.

The submission of digital evidence may entail additional costs for the court or public prosecutor to dispel any doubts about the evidence's origin. Digital evidence may require the assistance of experts, as judges and prosecutors may lack sufficient technical knowledge, whereas traditional evidence enables the court to draw on its internal convictions and work practices to determine the viability of evidence.

The authenticity of digital evidence means that it accurately represents what it is supposed to represent and demonstrates what it is supposed to prove in a particular case. This indicates that the digital certificate has not been tampered with, altered, or falsified in any way. While the dangers of evidence tampering are not unique to digital evidence, there is a widespread belief that digital evidence is easier to alter and tamper with than physical evidence. As is the case with any piece of evidence, altering digital evidence can result in incorrect conclusions.

Digital evidence can be altered using a variety of freely available software, and certificate forgery or alteration is difficult to detect. This means that not only is digital evidence easily altered, but also that the alteration of the altered certificate is difficult to detect. The more primitive the method used to modify the digital certificate, the more easily the modification will be detected. For instance, it is quite simple to modify the content of an e-mail received from another user within the office software to forward it in a different format.

However, one of the most dangerous and significant threats to the integrity of digital evidence is the ever-evolving technology of deep fake, which creates significant difficulties for courts and pre-trial proceedings. As digital technology advances, it becomes increasingly difficult to distinguish genuine from counterfeit (audio and/or visual) media.

Deep fake technology has both a direct and indirect influence on legal proceedings. As a direct result, deep fake technology adds to the court's workload. These include cases involving deep fakes themselves, such as those in which a claim for damages is made against a deep fake video. However, deep fake has an indirect effect on the courts by assisting in the resolution of disputes that they did not cause. In these instances, the alleged deep fake is not the basis for the case, but rather serves as one piece of evidence in court proceedings in which video evidence has already been presented. With the increasing use of video recordings as evidence in criminal cases, the risk of deep fake becomes more real.

Even if a deep fake video is not used or even mentioned as evidence in a court proceeding, the existence of a deep fake as such creates difficulties in verifying the overall credibility of the evidence. For instance, the accused's counsel may argue that certain (de facto) evidence-based videos are blatantly fabricated. In this case, the prosecutor may have to rely on sophisticated technology to demonstrate that the video he submitted is still accurate and reliable. This can result in irrational resource expenditures.

Although the current Code of Criminal Procedure contains no specific provisions on digital evidence, the definition of evidence in the current law is broad, leaving room for consideration of whether it also encompasses digital evidence. The absence of specific provisions in the Code of Criminal Procedure does not preclude the use of digital evidence in establishing the circumstances surrounding the object of evidence, as the types of evidence listed in § 63 (1) of the Code of Criminal Procedure are sufficiently broad to encompass most of the digital

evidence. Digital evidence can theoretically be classified as so-called strict evidence, as defined in Code of Criminal Procedure § 63 (1), and not as so-called free evidence, as defined in Code of Criminal Procedure § 63 (2).

Digital evidence in the form of a file, such as photographs, videos, and e-mails, can be considered evidence within the meaning of Code of Criminal Procedure § 63 (1), and digital evidence can be classified as evidence in Estonian law based on case law. Metadata can also be considered digital evidence under Estonian law and has significant value for verification. However, they have not been considered sufficient to prove on their own, but rather in conjunction with other evidence.

Pursuant to § 61 (1) of Code of Criminal Procedure, no evidence has a predetermined force. This means that all admissible types of evidence specified in § 63 (1) of Code of Criminal Procedure, as well as all different specific evidence within the same type of evidence, are in principle of equal value.

To begin, the reliability of a piece of evidence must be determined. Assessing the relevance entails believing that it accurately reflects an essential aspect of the criminal offense that is the subject of the criminal proceedings and that it can be used to establish the fact to which the evidence pertains. Thus, the court must consider the relevance of the evidence in question before accepting it or declining to take it. If the evidence is irrelevant to the case, the court may refuse to accept it or may order its collection, as it is irrelevant to the case. In the case of digital evidence, it is necessary to determine the relevance of a particular piece of evidence in a criminal case. According to case law, there is no reason to evaluate the relevance of digital evidence in any other manner or to ask any additional questions during the evaluation process.

The admissibility of evidence relating to a criminal offense is contingent upon whether and to what extent the provisions of criminal procedure aimed at safeguarding fundamental rights were followed during the evidence collection process. This means, first and foremost, that evidence must be gathered in a manner that respects the person’s honour and dignity, does not jeopardize their life or health, and does not result in unjustified property damage. It is prohibited to obtain evidence by torturing or other forms of violence against a person, or by any other means that may impair a person's memory or degrade human dignity. The Code of Criminal Procedure does not provide for the admissibility of digital evidence, which is why it is permitted if the

collection of the evidence does not violate the requirements set forth in Code of Criminal Procedure § 64.

The credibility of a piece of evidence is determined by the weight assigned to it by the evidence assessor after comparison and analysis with other evidence gathered in the case. The issue of evidence's reliability typically arises in court only after the evidence has been accepted and published and has passed the relevance and admissibility tests. In case law, a piece of evidence's reliability is also justified by the way it rhymes with other pieces of evidence. While a rigged body of evidence increases the likelihood that it will be reflected in that body, rhyme is not a characteristic of evidence that increases its credibility.

The legislature has not established any universally applicable standards for determining the reliability of evidence. As a result, the Code of Criminal Procedure contains no specific provisions addressing the reliability of digital evidence. When it comes to digital evidence, a superficial analysis can quickly lead to the (false) conclusion that the digital evidence is reliable. Assessing a digital certificate's reliability requires a thorough understanding of the content and unique characteristics of this type of evidence in comparison to other types of evidence. Additionally, the assessor must understand how digital evidence can be subtly altered to give the appearance of being trustworthy when it is not. In case law, a piece of evidence's reliability is also justified by the way it so-called “rhymes” with other pieces of evidence.

The final value of a piece of evidence is an assessment of how critical it is for the court to consider (or refute) any fact contained in the piece of evidence. The court must make a final assessment of the evidence in the case of digital evidence after determining its relevance, admissibility, and reliability. The case law demonstrates that the court is not bound by existing regulation when assessing digital evidence, and thus the existing regulation of the Code of Criminal Procedure can be interpreted as allowing the court to assess digital evidence as well.

The Code of Criminal Procedure enables participation in court proceedings as well as testimony via video bridge. This possibility had been long overdue, and the amendments to the law, which were rushed through due to the unique circumstances, have enabled it, ensuring more flexible court proceedings for both processors and participants. While testimony given remotely may be used as evidence, the person conducting the proceedings must exercise extreme caution to ensure that the person on the other side of the screen during the interrogation is still a real person and not a fake.

On 1 April 2021, the Government of the Republic of Estonian presented a draft act of amending the Criminal Procedure Code to the Riigikogu. The draft's objective is to improve the evidence system by streamlining the classification of evidence and introducing the concept of documentary evidence. The draft replaces the current document-based language, which is based on traditional paper-based procedures, with a more neutral language that is independent of whether the information is stored electronically, on paper, or in any other format.

The draft does not establish a separate regulation for digital evidence; rather, the legislator has stated unequivocally that digital evidence should be classified as documentary evidence. This type of evidence classification is novel and has the potential to simplify the use of digital evidence in criminal proceedings. Appropriate training of processors following the draft's entry into force is critical to ensuring that changes are not misinterpreted.

KASUTATUD MATERJALID

KIRJANDUS

1. Casey, E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd Edition. 2011, lk 7.Mason, S., Seng, D. Electronic evidence. Fourth Edition. 2017.
2. Chih-ping, C. Knowledge Production from Social Networks Sites. Using Social Media Evidence in the Criminal Procedure. Studiorum Università di Bologna. Dottorato di ricerca in Law, science and technology, 29 Ciclo. 2018,
3. Craiger, P. Training and Education in Digital Evidence, Handbook of Digital and Multimedia Forensic Evidence. 2008.
4. Duranti, L. Rogers, C. Trust in digital records: An increasingly cloudy legal area. Computer Law & Security Review, Volume 28, Issue 5, 2012.
5. Goode, S. The Admissibility of Electronic Evidence. Review of Litigation, Vol. 29, Issue 1. 2009.
6. Kietzmann, J., Lee, L.W., McCarthy, I.P., Kietzmann, T.C. Deepfakes: Trick or treat? Business Horizons. 2020, 63.
7. Li, Y. Li, Chang, M.-C., Lyu, S. In Ictu Oculi: Exposing AI Generated Fake Face Videos by Detecting Eye Blinking. State University of New York, 2018. Li, Y., Lyu, S. Exposing DeepFake Videos By Detecting Face Warping Artifacts, Computer Science Department University at Albany, State University of New York, USA, 2019.
8. Lin. X. Introductory Computer Forensics. A Hands-on Practical Approach, Wilfrid Laurier University Waterloo, ON, Canada. 2018.
9. Lupo, G., Bailey J. Designing and Implementing e-Justice Systems: Some Lessons Learned from EU and Canadian Examples, Laws 2014, 3. 2014.
10. Maras, M-H., Alexandrou, A. Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos. The International Journal of Evidence & Proof. 2019, Vol. 23(3). 2019.
11. Nilsson, J.D, Digital Evidence in the Courtroom. Nova Science Publishers. 2010.
12. Pfefferkorn, R. “Deepfakes“ in the Courtroom. Boston University Public Interest Law Journal . Summer2020, Vol. 29 Issue 2, 2021.
13. Praust, V. Infoühiskond ja selle teetähised. Infotehnoloogia haldusjuhtimises. Aastaraamat 1998.

14. Schneider, J., Wolf, J., Freiling, F. Tampering with Digital Evidence is Hard: The Case of Main Memory Images. Forensic Science International: Digital Investigation, Volume 32. 2020.
15. Shah, M. S. M. B; Saleem, S., Zulqarnain, R. Protecting Digital Evidence Integrity and Preserving Chain of Custody, Journal of Digital Forensics, Security and Law: Vol. 12 , Article 12. 2017.
16. Westerlund, M. The Emergence of Deepfake Technology: A Review. Technology Innovation Management Review. November 2019 (Volume 9, Issue 11). 2019.
17. Whitcomb, C.M.. An Historical Perspective of Digital Evidence: A Forensic Scientist's View. International Journal of Digital Evidence, Spring 2002 Volume 1, Issue 1, 2002.

ÕIGUSAKTID

18. Elektroonilise side seadus - RT I, 27.02.2022, 3
19. Justiitsministri 25.01.2020 määrus nr 7 „Maa-, haldus- ja ringkonnakohtu kantselei kodukord", RT I, 08.12.2020, 16.
20. Justiitsministri 19.06.2009 määrus nr 23 „Notariaadimäärustik", RT I, 22.06.2021, 4.
21. Karistusseadustik – RT I, 03.03.2021, 3.
22. Kriminaalmenetluse seadustik - RT I, 20.12.2019, 7; RT I, 29.12.2020, 10; RT I 22.12.2021, 4.
23. Kohtute infosüsteemi põhimäärus – RT I, 09.10.2020, 6.
24. Tsiviilkohtumenetluse seadustik – RT I, 22.03.2021, 5.
25. Tõestamisseadus – RT I, 22.12.2020, 47

EELNÕUD JA VÄLJATÖÖTAMISKAVATSUSED

26. Abipolitseiniku seaduse ja teiste seaduste muutmise seadus (COVID-19 haigust põhjustava viiruse SARS-Cov-2 levikuga seotud meetmed) 170 SE. Arvutivõrgus kättesaadav https://www.riigikogu.ee/tegevus/eelnoud/eelnou/000826a5-0c93-407c-9fab-f173221748b4/ (28.02.2021).
27. Algoritmiliste süsteemide mõjude reguleerimise väljatöötamise kavatsus. Arvutivõrgus kättesaadav https://eelnoud.valitsus.ee/main/mount/docList/93ebe63d-de8c-4662-9908-3232aa7f987c (21.03.2021).
28. Justiitsministri 19.06.2009. a määruse nr 23 „Notariaadimäärustik" muutmise eelnõu ja seletuskiri https://adr.rik.ee/jm/dokument/7375024 (14.04.2021).

29. Kriminaalmenetluse seadustik 594 SE. Eelnõu algtekst. Arvutivõrgus kättesaadav https://www.riigikogu.ee/tegevus/eelnoud/eelnou/3cbbe022-95f6-32ec-be3c-9c4aa0001f34/Kriminaalmenetluse%20seadustik (28.02.2021).
30. Kriminaalmenetluse seadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seadus 599 SE seletuskiri. Arvutivõrgus kättesaadav https://www.riigikogu.ee/tegevus/eelnoud/eelnou/ab9521d9-5558-45b8-c93a-b5122208c53b/ (12.04.2021).
31. Kriminaalmenetluse seadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seadus (kriminaalmenetluse seadustiku revisjon) 367 SE. Arvutivõrgus kättesaadav https://www.riigikogu.ee/tegevus/eelnoud/eelnou/d10291ef-980a-4b1d-8852-bab30d7e25f3/Kriminaalmenetluse%20seadustiku%20muutmise%20ja%20sellega%20seonduvalt%20teiste%20seaduste%20muutmise%20seadus%20(kriminaalmenetluse%20seadustiku%20revisjon) (12.04.2021).
32. Kriminaalmenetluse seadustiku muutmise seadus 392 SE. Arvutivõrgus kättesaadav https://www.riigikogu.ee/tegevus/eelnoud/eelnou/69f4f636-076c-487f-93c2-3827044cfb50/Kriminaalmenetluse%20seadustiku%20muutmise%20seadus (06.04.2022).
33. Tsiviilkohtumenetluse seadustiku muutmise seaduse eelnõu väljatöötamise kavatsus. Arvutivõrgus kättesaadav https://adr.rik.ee/jm/dokument/7420901 (14.04.2021).
34. Tõestamisseaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seadus 719 SE. Arvutivõrgus kättesaadav https://www.riigikogu.ee/tegevus/eelnoud/eelnou/1ef1f0ea-7e3a-410c-b597-878a97191140 (06.04.2022).

RIIGIKOHTU LAHENDID

35. RKo 3-1-1-19-05, 18.04.2005.
36. RKKKo 3-1-1-157-05, 27.03.2006.
37. RKo 3-1-1-104-06, 24.10.2005.
38. RKKKo 3-1-1-105-06, 28.02.2007.
39. RKKKo 3-1-1-45-07, 15.10.2007.
40. RKKKo 3-1-1-5-09, 26.03.2009.
41. RKKKo 3-1-1-33-11, 04.05.2011.
42. RKKKo 3-1-1-82-11, 18.10.2011.

43. RKKKo 3-1-1-38-12, 03.05.2012.
44. RKKKo 3-1-1-89-12, 18.02.2013.
45. RKKKo 3-1-1-55-14, 04.12.2014.
46. RKKKo 3-1-1-77-15, 13.10.2015.
47. RKKKo 3-1-1-83-15, 29.10.2015.
48. RKKKm 3-1-1-24-16, 30.03.2016.
49. RKKKo 3-1-1-82-16, 21.11.2016.
50. RKKKo 3-1-1-104-16, 21.12.2016.
51. RKKKm 1-16-6179/85, 12.11.2018.
52. RKKKo 1-17-5210, 28.11.2019.
53. RKÜKo 1-17-2359, 03.03.2021.
54. RKKKo 1-20-1578, 21.05.2021.
55. RKKKo 1-16-6179/111, 18.06.2021.

ESIMESE JA TEISE ASTME KOHTULAHENDID

56. Harju Maakohtu kohtuotsus kriminaalasjas nr 1-15-5739 (29.09.2015).
57. Harju Maakohtu kohtuotsus kriminaalasjas nr 1-16-2605 (06.04.2016).
58. Harju Maakohtu kohtuotsus kriminaalasjas nr 1-17-2018 (03.07.2018).
59. Harju Maakohtu kohtuotsus kriminaalasjas nr 1-18-1038 (19.05.2020).
60. Harju Maakohtu kohtuotsus kriminaalasjas nr 1-18-5011 (06.02.20120).
61. Harju Maakohtu kohtuotsus kriminaalasjas nr 1-19-5800 (27.08.2019).
62. Harju Maakohtu kohtuotsus kriminaalasjas nr 1-19-883 (25.11.2019).
63. Harju Maakohtu kohtuotsus kriminaalasjas nr 1-20-98 (18.03.2020).
64. Pärnu Maakohtu kohtuotsus kriminaalasjas nr 1-10-90 (28.08.2013).
65. Pärnu Maakohtu kohtuotsus kriminaalasjas nr 1-19-2108 (27.09.2019).
66. Pärnu Maakohtu kohtuotsus kriminaalasjas nr 1-19-4150 (23.04.2020).
67. Tallinna Ringkonnakohtu kohtuotsus kriminaalasjas nr 1-14-1938 (15.07.2014).
68. Tallinna Ringkonnakohtu kohtuotsus kriminaalasjas nr 1-19-5662 (26.02.2020).
69. Tartu Ringkonnakohtu kohtumäärus kohtuasjas nr 1-20-3240 (08.06.2020).
70. Tartu Ringkonnakohtu kohtuotsus kriminaalasjas nr 1-17-6611 (31.01.2019).
71. Tartu Ringkonnakohtu kohtuotsus kriminaalasjas nr 1-18-10464 (30.04.2020).
72. Tartu Ringkonnakohtu kohtuotsus kriminaalasjas nr 1-18-4600 (03.12.2020).
73. Tartu Ringkonnakohtu kohtuotsus kriminaalasjas nr 1-21-3744 (30.06.2021).
74. Viru Maakohtu kohtuotsus kriminaalasjas nr 1-16-5757 (19.06.2017).

75. Viru Maakohtu kohtuotsus kriminaalasjas nr 1-19-4135 (09.01.2020).
76. Viru Maakohtu kohtuotsus kriminaalasjas nr 1-19-4802 (21.08.2020).
77. Viru Maakohtu kohtuotsus kriminaalasjas nr 1-19-7953 (16.09.2020).

VÄLISRIIKIDE KOHTULAHENDID

78. *Cunningham v. Fair Haven & Westville R. Co*, Supreme Court of Connecticut Third Judicial District, New Haven, June Term, Aug 1, 1899. Arvutivõrgus https://casetext.com/case/cunningham-admx-v-fair-haven-westville-r-co (27.04.2022).
79. *Regina v Weiner* [2011] EWCA Crim 1249, England and Wales Court of Appeal (Criminal Division), Apr 7, 2011. Arvutivõrgus https://www.casemine.com/judgement/uk/5a8ff70360d03e7f57ea5a58 (27.04.2022).
80. *St. Clair v. Johnny's Oyster & Shrimp, Inc*., US District Court for the Southern District of Texas - 76 F. Supp. 2d 773 (S.D. Tex. 1999). Arvutivõrgus https://law.justia.com/cases/federal/district-courts/FSupp2/76/773/2370358/ (27.04.2022).
81. *State v. Simon,* 174 A. 867, 872 (N.J. Sup. Ct. 1934). Arvutivõrgus https://casetext.com/case/state-v-simon-72 (27.04.2022).
82. Euroopa Kohtu otsus (suurkoda) 2. märtsil 2021 kohtuasjas C-746/18. Arvutivõrgus https://eur-lex.europa.eu/legal-content/et/TXT/?uri=CELEX:62018CJ0746 (27.04.2022).

MUUD ALLIKAD

83. Andmekaitse Inspektsioon, Metaandmed ja privaatsus Juhis organisatsioonidele1 ja kodukasutajale seaduse rakendamisel. 2015. Arvutivõrgus kättesaadav https://www.aki.ee/et/node/1661 (23.04.2022).
84. Doctored audio evidence used to damn father in custody battle. The Telegraph, 2020. Arvutivõrgus kättesaadav https://www.telegraph.co.uk/news/2020/01/31/deepfake-audio-used-custody-battle-lawyer-reveals-doctored-evidence/ (23.04.2022).
85. E4J University Module Series: Cybercrime. Module 4: Introduction to Digital Forensics. Digital evidence. 2019. Kättesaadav arvutivõrgus https://www.unodc.org/e4j/en/cybercrime/module-4/key-issues/digital-evidence.html- (23.04.2022).

86. Eesti rahvusvahelises julgeolekukeskkonnas 2021. Välisluureameti aastaraamat. 2021. Arvutivõrgus kättesaadav https://www.valisluureamet.ee/pdf/raport/2021-EST.pdf (23.04.2022).
87. E-toimik. Registrite ja Infosüsteemide Keskuse veebileht. Kättesaadav arvutivõrgus: http://www.rik.ee/et/e-toimik (23.04.2022).
88. Ettepanek: EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS, milles käsitletakse arvutipõhist süsteemi piiriüleste tsiviil- ja kriminaalmenetluste andmete vahetamiseks (e-CODEXi süsteem) ning millega muudetakse määrust (EL) 2018/1726. Arvutivõrgus kättesaadav https://eur-lex.europa.eu/legal-content/EN-ET/ALL/?uri=CELEX:52020PC0712 (23.04.2022).
89. Guess How Many Microsoft Office Documents Were Made Last Year. Business Insider, 2014. Arvutivõrgus kättesaadav https://www.businessinsider.com/how-many-microsoft-office-documents-were-made-last-year-2014-2 (23.04.2022).
90. Information society. Eurostat regional yearbook 2014. Arvutivõrgus kättesaadav https://ec.europa.eu/eurostat/documents/3217494/5786345/KS-HA-14-001-08-EN.PDF/d713d26a-2272-4500-aa67-cced7e73f2ff (23.04.2022).
91. Johnson, P. What are Deepfakes? And why should you care about them? Veriff, 2020. Arvutivõrgus kättesaadav https://www.veriff.com/blog/what-are-deepfakes (23.04.2022).
92. Justiitsministeeriumi programm aastateks 2020-2023 „Usaldusväärne ja tulemuslik õigusruum“. Arvutivõrgus kättesaadav https://www.just.ee/et/ministeerium-kontaktid/arengukavad-ja-tooplaanid (23.04.2022).
93. Justiitsministeeriumi programm aastateks 2022-2025. Arvutivõrgus kättesaadav https://www.just.ee/ministeerium-uudised-ja-kontakt/ministeeriumist-ja-minister/strateegilised-alusdokumendid (23.04.2022).
94. Justiitsministeeriumi valitsemisala arengukava aastateks 2018 – 2021. Arvutivõrgus kättesaadav https://www.just.ee/et/ministeerium-kontaktid/arengukavad-ja-tooplaanid (23.04.2022).
95. Keypoint Intelligence, Our Best Photos Deserve to Be Printed. 2018. Arvutivõrgus kättesaadav https://www.keypointintelligence.com/news/editors-desk/2018/september/our-best-photos-deserve-to-be-printed/ (23.04.2022).
96. Kurm, M. Tõendite kogumisel dubleerimise vältimine kohtu- ja kohtueelses menetluses. Analüüs. 2016. Arvutivõrgus kättesaadav https://www.just.ee/sites/www.just.ee/files/toendamine_m._kurm.pdf (23.04.2022).

97. Infosüsteemide kolmeastmelise etalonturbe süsteemi ISKE rakendusjuhend. Versioon 8.00. 2017. Arvutivõrgus kättesaadav https://www.ria.ee/et/kuberturvalisus/iske/juhendid-ja-materjalid.html (23.04.2022).
98. Number of sent and received e-mails per day worldwide from 2017 to 2025. Statista, 2021. Arvutivõrgus kättesaadav https://www.statista.com/statistics/456500/daily-number-of-e-mails-worldwide/ (23.04.2022).
99. Scientific Working Group on Digital Evidence (SWGDE). International Organization on Digital Evidence (IOCE). 2002. Arvutivõrgus kättesaadav https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm (23.04.2022)
100. Tehver, J. Digitaalsete tõendite kasutamise võimaldamine, mai 2016. Arvutivõrgus kättesaadav http://www.just.ee/sites/www.just.ee/files/digitaalsed_toendid_j._tehver.pdf (23.04.2022).
101. The 2020 EU Justice Scoreboard, European Commission, Luxembourg: Publications Office of the European Union, 2020. Arvutivõrgus kättesaadav https://ec.europa.eu/info/sites/info/files/justice_scoreboard_2020_en.pdf (23.04.2022).
102. Vabariigi Valitsus. Ülevaade Vabariigi Valitsuse tegevusprogrammi täitmisest 2020. aastal. Alapeatükk 3.3.3. Olulisemad hilinenud ja elluviidavad tegevused. 2020. Arvutivõrgus kättesaadav https://www.valitsus.ee/juri-ratase-ii-valitsuse-tegevusprogramm (23.04.2022).

INFORMATIIVSED ARTIKLID

103. Fitness tracking app Strava gives away location of secret US army bases. The Guardian, 2018. Arvutivõrgus kättesaadav https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases (23.04.2022).
104. Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case. The Wall Street Journal, 2019. Arvutivõrgus kättesaadav https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402 (23.04.2022).
105. Kohus mõistis väidetava rünnaku ohvri valeütluste andmises süüdi. Tartu Postimees, 2020. https://tartu.postimees.ee/6981555/kohus-moistis-vaidetava-runnaku-ohvri-valeutluste-andmises-suudi (23.04.2022).

VEEBILEHED

106. Eesti Keele kõnesünteesikeskkond: https://www.eki.ee/heli/.
107. E-CODEXi veebileht https://www.e-codex.eu/.
108. Overdubi Descrpiti veebilehel https://www.descript.com/overdub.
109. Deepfakesweb'i korduma kippuvad küsimused https://deepfakesweb.com/faq.
110. Washingtoni Ülikool süvavõltsingu tuvastamise veebileht https://www.spotdeepfakes.org/en-US.
111. Michigani Tehnoloogia Ülikooli süvavõltsingute veebileht https://detectfakes.media.mit.edu/.
112. ÜRO uimastite ja kuritegevuse büroo veebileht https://www.unodc.org/e4j/en/tertiary/index.html