Euroopa Liit
Euroopa Sotsiaalfond

Eesti
tuleviku heaks

Digitaalsete tõendite kasutamise võimaldamine

Jaanus Tehver
Kriminaalmenetluse revisjoni töörühma liige
Mai 2016

1. Lähteülesanne

Väljavõte hankedokumendist: Digitaalse kriminaalmenetluse osaks on ka digitaalsed tõendid, nende kogumine ja kasutamine kohtumenetluses. Digitaalseid tõendeid kogutakse kriminaalmenetlustes üha enam, kuid kehtiv õigus eraldi menetluskorda ja selliste tõendite kogumise põhimõtteid ei sätesta, mistõttu on seni lähtutud tavaliste tõendite kogumise ja uurimise regulatsioonist. Samas on füüsilised ja digitaalsed tõendid oma olemuselt põhimõtteliselt erinevad, mistõttu tekitab selline olukord praktikas segaseid olukordi (nt, kas ja kuivõrd on ruumi läbiotsimise käigus lubatud koguda selliseid digitaalseid tõendeid, mis asuvad ruumiliselt eraldatud andmekandjal, kuid millele on ligipääs läbi ruumis oleva seadme). Seetõttu on ka

Õiguskantsler juhtinud tähelepanu, et arvestades elektroonilise suhtluse laia kasutusala ning elektroonilistes andmekandjates sisalduva info teatavaks saamisega kaasnevat põhiõiguste riive ulatust, oleks asjakohane kaaluda, kas täpsem regulatsioon (koos vajalike menetlusgarantiidega) aitaks kaasa põhiõiguste ja -vabaduste paremale tagamisele.

2. Kehtiva õiguse analüüs

Kehtiv KrMS, sh seadusena vastuvõetud, kuid tulevikus (kuni 01.01.2017.a.) jõustuvad seaduse muudatused, praktiliselt ei sisalda erisätteid digitaalsete tõendite kohta. See 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. Allakirjutanule 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.

Samal ajal tuleb nentida, et juba aastaid on praktikas segadus erinevate digitaalsete tõendite kvalifitseerimisel KrMS § 63 lg 1 sätestatud tõendi liikide alla (asitõend, muu dokument, muu teabetalletus). Lisaks sellele võib olla problemaatiline teatud spetsiifiliste ja praktikas harva vahetult kasutatavate tõendi vormide lugemine tõendiks KrMS § 63 lg 1 järgi -- nimelt näivad antud normis loetletud relevantsed tõendi liigid ehk asitõend, muu dokument ja muu teabetalletus osutavat eelkõige mingisugusele andmekandjale *salvestatud* (ingl k *stored*) teabele, samal ajal kui tõendusteavet võib omada ka erinevate seadmete vahel *liikuv* (ingl k *transmitted*) digitaalne teave, mida kogutakse reaalajas[1].

Erisätete puudumine digitaalsete tõendite kohta tähendab praktika seda, et selliste tõendite kogumisel, käitlemisel, uurimisel ja esitamisel kohaldatakse norme, mis on algselt määratud teiste tõendiliikide reguleerimiseks ning mis sellest tulenevalt tekitavad mitmemõistetavusi ja rakendusprobleeme. Näiteks on reguleerimata andmekandjast tõendusväärtusliku koopia loomine ja seda toimingut käsitletakse enamasti vaatlusena ja vormistatakse vaatlusprotokolliga, kuigi toimingu sisu ja eesmärk ei vasta KrMS § 83 lg 1 toodud vaatluse mõistele. Selgus puudub ka küsimuses, millistel juhtudel on andmekandjalt või selle koopialt tõendusteabe leidmiseks ja fikseerimiseks vajalik läbi viia ekspertiis ning millal piisab vaatlusest. 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.

[1] Praktikas ei ole sellise teabe kasutamine tõendina osutunud problemaatiliseks seetõttu, et reeglina saab sellist teavet koguda vaid jälitustoiminguga ning tõend vormistatakse jälitustoimingu protokolli ja sellele käigus tehtud teabetalletuse kujul.

Oluline probleemide valdkond seondub asjaoluga, et kui nn teel olevate sõnumite (mis tänapäeval on valdavalt digitaalsed) puhul rakenduvad isikute õiguse kaitseks KrMS-i jälitustegevuse regulatsiooni menetlusgarantiid, siis andmekandjatele salvestatud teabe puhul need garantiid ei rakendu ning praktiliselt mitte mingeid tagatisi vältimaks kriminaalmenetluse käigus teabe äravõtmisega isikute õiguste ebaproportsionaalseid riiveid ei eksisteeri. Arvestades asjaolu, et praktikas hõlmab valdav enamik läbiotsimiseks antud lube õigust ära võtta ka andmekandjaid ning vähemalt sellistes kriminaalmenetlustes, mille käigus jõutakse kahtlustatava kindlakstegemiseni, on mitte ühegi andmekandja äravõtmine pigem erandlik olukord (kuivõrd peaaegu iga inimese igapäevases kasutuses on vähemalt üks oluline andmekandja telefoni näol), siis omab nn digitaalse privaatsuse kaitse järjest suuremat tähendust.

Eesti on ühinenud 23.11.2001.a. Arvutikuritegevusevastase konventsiooniga (nn Budapesti konventsioon), mille artiklites 14-21 sätestatud menetlusõiguste põhimõtete täiel määral järgmist kehtiv KrMS ei võimalda.

2013.a. valminud Tartu Ülikooli analüüs isikute põhiõiguste tagamisest ja eeluurimise kiirusest kriminaalmenetluses[2] leidis kokkuvõtlikult, et:

i) KrMS ei vasta digitaalsete tõendite kogumise ja jälitustoimingute tegemise osas digitaalsete tõendite erispetsiifikale ega järgi piisavalt digitaalkriminalistika põhiprintsiipe;

ii) mõistlik oleks kehtestada KrMS-is digitaalandmete kogumisele erikord;

iii) täiendusi vajab jälitustegevuse regulatsioon, mis ei järgi täies ulatuses digitaalsete tõendite valdkonnas levinud üldteoreetilisi seisukohti;

iv) Eesti ei täida Arvutikuritegevusvastase konventsiooni (23.11.2011) menetlusõiguslikke miinimumkohustusi.

Ma nõustun eelviidatud analüüsi järeldustega.

3. Eesmärk

Rakendatav menetlusõigus peab võimaldama kriminaalmenetluses koguda ja kasutada digitaalseid tõendeid nii, et maksimaalsel määral oleks tagatud tõendusteabe usaldusväärsus ning teave oleks esitatud viisil, mis võimaldaks seda kohtus sisuliselt uurida ja hinnata ning vajadusel kontrollida.

[2] http://www.kriminaalpoliitika.ee/et/analuus-isikute-pohioiguste-tagamisest-ja-eeluurimise-kiirusest-kriminaalmenetluses, vt analüüsi lk 155-156.

Samal ajal peab rakendatav menetlusõigus sätestama menetlusõiguslikud garantiid isikute (teabevaldajate) õiguste, eelkõige privaatsusõiguse ja konfidentsiaalse teabe kaitstuse, ebaproportsionaalsete riivete vältimiseks.

Digitaalsete tõendite kogumise, käsitlemise ja esitamise reeglid peavad toetama kriminaalmenetluse efektiivsust ja vältima nii menetlejate kui menetlussubjektide asjatut koormamist bürokraatiaga ning ühtlasi tagama kohtumenetluse poolte võrdsete relvade (*equality of arms*) põhimõtte rakendamise.

Kuivõrd analüüsi aluseks olev ülesande püstitus näeb ette eelkõige praktiliste lahenduste leidmist kehtiva menetlusõiguse üldiste põhimõtete raamides, siis otsin analüüsiga selliseid regulatsioonivõimalusi, mida on võimalik sobitada kehtiva (arvestades ka vastu võetud, kuid tulevikus jõustuvate muudatustega) KrMS põhimõtete, struktuuri ja üldmõistetega.

4. Probleemid ja lahendused

4.1. Digitaalsete andmete ja andmekandja koht rangete tõendiliikide süsteemis

KrMS on rajatud nn rangele tõendamismenetlusele ehk lubatud tõendiliikide ammendavale loetelule seaduses (KrMS § 63 lg 1). Kuna selle põhimõtte ümbervaatamise vajadus väljub analüüsi raamidest, siis ma eeldan KrMS § 63 lg 1 senisel kujul kehtimajäämist. Iseenesest ei takista KrMS § 63 lg 1 ka digitaalsete tõendite kasutamist kriminaalmenetluses, kuivõrd kõik võimalikud tõendamisväärtusega digitaalsed andmed ja vastavad andmekandjad on kvalifitseeritavad mõne antud normis loetletud tõendi liigi alla.

Eeltoodule vaatamata tuleb nentida, et digitaalsete andmete ja andmekandja koht rangete tõendiliikide süsteemis on mõneti ebaselge ja see tekitab nii õiguspoliitilisi (menetlusseaduse selgus ja arusaadavus) kui ka praktilisi probleeme.

Kehtiva seaduse kontekstis ei ole üheselt mõistetav, millisel juhul kvalifitseeruvad digitaalsed andmed ja vastavad andmekandjad kas (i) asitõendiks, (ii) dokumendiks või (iii) teabetalletuseks[3]. Riigikohtu praktikas on leitud[4], et *salvestised* (mille all peetakse eelduslikult silmas ka digitaalset teavet koos vastava andmekandjaga) saavad olla iseseisvad tõendid järgmistel juhtudel:

a) tegemist on uurimistoimingute käigus tehtud ning nende toimingute käiku ja tulemusi kajastavate salvestustega, mis kokkuvõttes vormistatakse vastava

[3] Kuni 31.12.2012.a. kasutas seadus terminit "teabesalvestis". Mõisted "teabetalletus" ja "teabesalvestis" on sisult laiemad kui digitaalsed andmed vastaval andmekandjal, kuivõrd need on tehnoloogianeutraalsed, s.t. hõlmatud on nii digitaal- kui analoogtehnoloogiat rakendades tehtud salvestised. Kriminaalmenetluses kasutatavate tõendite kontekstis on tänapäeval analoogtehnoloogial põhinevate salvestiste tähtsus marginaalne, mistõttu "teabetalletuse" all peetakse üldjuhul silmas nimelt digitaalselt salvestatud andmeid.

[4] Vt RKK otsus nr 3-1-1-21-09 p 9, RKK otsus nr 3-1-1-83-15 p 9 ja 10.

uurimistoimingu protokolli lisana ja mille seos kriminaalasjaga nähtub selle protokolli tekstist;

b) tegemist on jälitustoiminguga saadud salvestisega, mille juurde saab pöörduda jälitustoimingu protokolli kui tõendi kontrollimiseks;

c) tegemist on menetleja poolt isikutelt ära võetud või isikute poolt omal initsiatiivil menetlejale antud varem tehtud salvestistega, mis võivad olla nende sisust tulenevalt käsitletavad kas asitõendi või dokumendina ning mis peavad olema vormistatud KrMS III ptk 9. jao sätete kohaselt.

Riigikohtu seisukoha järgi ei ole mistahes muul salvestisel (peale eelkirjeldatute) kriminaalasjas tõenduslikku tähendust. Samas on Riigikohus leidnud ka, et "muu teabesalvestisena" on käsitletav näiteks telefonivestluse (heli)salvestis[5], kuigi sellise tõendi liigitamine kas asitõendiks või dokumendiks on küsitav. Probleemi komplitseerib tõsiasi, et kui asitõendi mõiste on määratletud (KrMS § 124 lg 1), siis dokumendi mõistet määratletud ei ole ning ühtlasi näeb seadus *expressis verbis* ette ka (eri)juhtumi, mil dokument on ühtlasi asitõend (KrMS § 123 lg 2).

Nii seadus kui Riigikohtu praktika on eelkõige just väljaspool uurimis- ja jälitustoiminguid tehtud teabetalletuste osas ebaselge ja segadust tekitav selles osas, kas ja millistel juhtudel on teabetalletus (digitaalne teave vastaval andmekandjal) iseseisev tõend *per se* ning millal tuleb seda käsitleda kui asitõendit või dokumenti. Sellest tulenevalt on ebaselge, millisel juhul on nõutav teabetalletuse käsitlemine kas uurimistoimingu protokollis või vaatlusprotokollis ning millisel juhul pole protokollimine nõutav (vt KrMS § 124 lg 2). Sellele lisandub Margus Kurmi poolt teema 4.5 analüüsi raames välja toodud probleem, et kehtiv KrMS ei erista ei dokumentide ega teabetalletuste kontekstis ühelt poolt tõendamiseseme asjaolusid vahetult kajastavaid ja teiselt poolt sisuliselt ütlusi sisaldavaid tõendeid.

Segadus tõendi liikide kohaldamisel digitaalsete andmete ja vastavate andmekandjate suhtes avaldub praktikas eelkõige selles, milliseid nõudeid on vaja järgida tõendi vormistamisel.

Lahendusena pean mõistlikuks viia KrMS-i sisse järgmised muudatused:

1) dokumendi mõiste määratlemine (vt Margus Kurmi analüüs teema 4.5 kohta) ehk KrMS § 123 lg 1 muutmine;

2) teabetalletuse mõiste määratlemine ja piiritlemine teistest tõendi liikidest, näiteks järgmisel viisil:

§ 124[1]. Teabetalletus

[5] Vt RKK otsus nr 3-1-1-5-09 ja 3-1-1-33-11

(1) Teabetalletus on andmekandja koos sellele salvestatud andmetega, mis võimaldavad tehnikavahendeid kasutades inimesele tajutaval kujul taasesitada kriminaalasjas tähtsust omavat teavet.

(2) Teabetalletus on dokument, kui sellel on käesoleva seadustiku § 123 lg 1 loetletud tunnused.

(3) Teabetalletus on asitõend, kui sellel on käesoleva seadustiku § 124 lg 1 loetletud tunnused.

(4) Teabetalletus, mis on loodud uurimis- või jälitustoimingu käigus, tuleb lisada uurimis- või jälitustoimingu protokollile.

4.2. Teabetalletuse koopia kasutamine tõendina

Kehtiv KrMS on segadust tekitav andmekandjale salvestatud teabest koopia tegemise ja sellise koopia tõendina kasutamise osas.

Teatavasti on üks digitaalkriminalistika põhimõtteid see, et kuivõrd digitaalsed andmed on väga kergesti manipuleeritavad, tuleks võimalusel alati luua algsest uurimisele allutatud andmekandjast nn tõendusväärtuslik koopia (ingl k *forensic copy*) ja edasised uurimistoimingud viia läbi koopia suhtes. Samast põhimõttest tulenevalt eeldatakse, et kui pole alust kahelda menetluse käigus loodud tõendusväärtusliku koopia autentsuses, on koopia kasutatav tõendina.

Iseenesest kehtiv KrMS regulatsioon ei välista koopiate kasutamist tõendina, kuivõrd ka kriminaalmenetluse käigus menetleja poolt loodud *forensic copy* on käsitletav "muu teabetalletusena" KrMS § 63 lg 1 tähenduses. Kuivõrd Riigikohus on väljendatud seisukohta, et KrMS § 123 lg 1 tähenduses dokumendi kvaliteet on nii originaaldokumendil kui koopial[6], siis ei ole ka teabetalletuste koopiate tegemist ja nende tõendina kasutamise lubatavust kahtluse alla seatud ning praktikas kasutatakse seda sageli.

Samas ei ole väljakujunenud praktika probleemideta ühitatav KrMS § 125 lg 5 sätestatud põhimõttega, mille kohaselt kui asitõendiks on dokument, mida selle omanikul on edaspidi vaja majandus- või ametitegevuses või muul olulisel põhjusel, teeb menetleja sellest omanikule koopia. Koopia vastavust originaalile kinnitab menetleja oma allkirjaga koopial. KrMS § 125 lg 6 kohaselt tuleks sama põhimõtet kohaldada digitaalseid andmeid sisaldavate andmekandjate suhtes, mis ei ole asitõendid. Kuivõrd andmekandjad on reeglina omanikule olulised, siis näeb kehtiv seadus justkui ette, et menetleja peaks tegema neist koopiad ja koopiad ka omanikule üle andma.

[6] Vt RKK otsus 3-1-1-46-10 p 8.3.1.

Andmekandjate käsitlemise praktika on KrMS § 125 lg 5 ja 6 sätestatuga võrreldes tegelikult risti vastupidine -- andmekandjatest tehakse üldjuhul tõendusväärtuslik koopia ja omanikule tagastatakse algne andmekandja, mitte koopia. Selline toimimisviis on ka loogiline ja põhjendatud, kuivõrd andmekandja tõendusväärtuslikku koopiat saab luua vaid spetsiifilises failiformaadis, mis on käsitsetav üksnes spetsiaalset riist- ja/või tarkvara kasutades, mistõttu koopia omanikule tagastamine ei teeniks sisuliselt omaniku huve (isikul oleks äärmiselt keeruline menetlejalt saadud koopiaga midagi peale hakata).

Arvestades seda, kuivõrd kergesti allub digitaalne teave mõjutustele ning kuivõrd keeruline on andmete manipuleerimise fakti tagantjärgi tuvastada, tuleks teabetalletuste koopiate loomise nõuded seaduses reguleerida. Kehtivas KrMS-is asjassepuutuvad sätted puuduvad.

Teabetalletuse koopia tõendina kasutamise võimaluse sätestamine peaks võimaldama ka rakendada andmekandja äravõtmise (ingl k *seizure*) alternatiivina teabekandjale juurdepääsu ja selle kopeerimist (ingl k *access and copy*), mis riivab teabevaldajate huve vähem intensiivselt.

Lahendusena pean mõistlikuks viia KrMS-i sisse järgmised muudatused:

1) KrMS täiendamine järgmise sättega:

§ 124^2. Teabetalletuse koopia tõendina

(1) Kriminaalmenetluse käigus loodud teabetalletuse koopia on tõend, kui on täidetud järgmised tingimused:

1) algse teabetalletuse oma valdusse või sellele juurdepääsu saamisel ning teabetalletuse käitlemisel on menetleja täitnud käesoleva seadustiku nõuded;

2) koopia on loodud viisil, mis tagab kopeeritud teabe identsuse, terviklikkuse ja muutmatul kujul säilimise;

3) koopia päritolu ja autentsust on võimalik kriminaalmenetluses usaldusväärselt kontrollida.

(2) Kui teabetalletuse omanik on menetlejale teada, peab menetleja andma omanikule või tema esindajale võimaluse viibida koopia tegemise juures.

(3) Teabetalletuse koopia loomine protokollitakse käesoleva seadustiku §-is 146 sätestatud korras.

2) kaaluda tuleks, kas digitaalseid andmeid sisaldavate andmekandjate äravõtmisel või muul viisil menetleja valdusse sattumisel peaks olema *kohustuslik* andmekandjast tõendusväärtusliku koopia loomine ning üksnes erandjuhul (kui koopia tegemine ei ole võimalik või pole otstarbekas) saaks sellest toimingust loobuda.

4.3. Andmekandjalt tõendusteabe otsimise tingimused

Eelkõige digitaalseid andmeid sisaldavate andmekandjate plahvatuslik levik ja nende ulatuslik kasutamine kõigi inimeste poolt, kusjuures andmeid salvestatakse pidevalt ja enamasti ilma inimese vahetu sekkumiseta, on kaasa toonud olukorra kus inimeste õigus privaatsusele (põhiseaduse § 26) vajab digitaalandmete kontekstis kõrgendatud tähelepanu.

Kehtiv KrMS ei sätesta mingeid tingimusi ega piiranguid kriminaalmenetluse käigus ära võetud või menetlejale üle antud andmekandjatele salvestatud andmete käitlemisele, sh tõendusteabe otsimisele ja teabe kasutamisele kriminaalmenetluses. Arvestades vastavate toimingutega kaasneva põhiõiguste riive intensiivsust, on vajalik täiendavate menetlusgarantiide sätestamine KrMS-is. Mõistlik on seaduses sätestada, et andmekandjalt tõendusteabe otsimisele kehtivad läbiotsimisega (KrMS § 91-92) analoogsed nõuded.

Kuivõrd kehtiv õigus ei reguleeri krüpteeritud või muul viisil vaatlemise eest kaitstud andmetele juurdepääsu saamise tingimusi, tuleks ka need seaduses sätestada. Lisaks on mõistlik ette näha nn kaugläbiotsimise võimalus ehk andmekandja läbiotsimine läbi kaugsidet pakkuva tehnilise lahenduse -- ka see aitab andmekandja äravõtmise alternatiivina (*access and copy* põhimõttest lähtuvalt) vältida ebaproportsionaalset teabevaldaja huvide riivet.

Vajalikud muudatused KrMS-is:

§ 92[1]. Andmekandja läbiotsimine

(1) Andmekandja läbiotsimise eesmärk on leida andmekandjalt kriminaalmenetluses tähtsust omavat teavet. Andmekandja läbiotsimist võib toimetada, kui esineb põhjendatud kahtlus, et otsitav teave on andmekandjale salvestatud.

(2) Andmekandja läbiotsimist võib toimetada:

1) andmekandja omaniku või muu isiku, kellel on põhjendatud huvi andmekandjale salvestatud teabe kaitstuse suhtes, kirjalikul loal; või

2) prokuratuuri taotlusel eeluurimiskohtuniku määruse või kohtumääruse alusel.

(3) Andmekandja läbiotsimise taotluses ja läbiotsimismääruses märgitakse:

1) läbiotsimise eesmärk;

2) läbiotsimise põhjendus;

3) läbiotsimisele kuuluva andmekandja identifitseerimist võimaldavad andmed.

(4) Kui läbiotsimine viiakse läbi käesoleva paragrahvi lõike 2 punktis 2 sätestatud alusel, tuleb läbiotsimismäärust tutvustada käesoleva paragrahvi lõike 2 punktis 1 nimetatud isikule enne läbiotsimise alustamist.

(5) Andmekandja läbiotsimisel tuleb tagada andmekandjale salvestatud andmete terviklikkus ja muutmatul kujul säilimine. Andmekandja läbiotsimine võib toimuda kaugühenduse teel tehnilise vahendi abil.

(6) Kui andmekandjale salvestatud andmed on krüpteeritud või muul viisil kaitstud selliselt, et andmete vaatlemiseks on vajalik krüpteerimisvõtme, salasõna või muu kasutajatunnuse sisestamine või muu andmete kaitsemeetme kõrvaldamine, on menetlejal õigus:

1) nõuda andmekandja omanikult või valdajalt andmete kaitsemeetme kõrvaldamiseks vajaliku krüpteerimisvõtme, salasõna või muu kasutajatunnuse avaldamist ning selgitusi andmekandja kaitsmise viisi kohta käesoleva seadustiku § 215 lg 1 sätestatud korras;

2) kasutada andmete vaatlemist takistava krüpteeringu või muu andmete kaitsmise meetme kõrvaldamiseks tehnikavahendeid või muust kui käesoleva paragrahvi lõike 5 punktis 1 nimetatud allikast pärinevat teavet.

(7) Andmekandja läbiotsimise kohta koostatakse protokoll, milles märgitakse:

1) viide käesoleva paragrahvi lõikes 2 nimetatud läbiotsimise alusele;

2) käesoleva paragrahvi lõike 5 ja 6 rakendamise asjaolud;

3) otsingute tingimused, käik ja tulemused;

4) leitud kriminaalasjas tähtsust omava teabe tunnused.

4.4. Jälitustoimingute dokumenteerimine

Kehtiva KrMS § 126^{10} ei näe ette kohustuslikke nõudeid jälitustoimingute dokumenteerimiseks selles osas, mis puudutab digitaalandmete kogumise protsessi ning andmete autentsuse ja terviklikkuse tagamise meetmete kirjeldamist. 2013.a. valminud Tartu Ülikooli analüüsis isikute põhiõiguste tagamisest ja eeluurimise kiirusest kriminaalmenetluses[7] leiti, et see muudab võimatuks hinnata hiljem kogutud tõendite usaldusväärsust.

Probleemi lahendamiseks tuleks KrMS-i täiendada jälitustoimingute dokumenteerimise nõuetega juhul, kui jälitustoiminguga kogutakse digitaalset teavet.

Vajalikud täiendused ja muudatused KrMS-is:

1) KrMS-is reegli sätestamine, et kui jälitustoimingu käigus luuakse teabetalletus, tuleb see lisada jälitustoimingu protokollile (vt käesoleva analüüsiga pakutud KrMS § 124^1 lg 4, vt analüüsi p 4.1);

[7] http://www.kriminaalpoliitika.ee/et/analuus-isikute-pohioiguste-tagamisest-ja-eeluurimise-kiirusest-kriminaalmenetluses, vt analüüsi lk 153.

2) KrMS § 126 lg 1 täiendamine järgmiste punktidega:

5[1]) jälitustoimingu protsessi ja kasutatud meetodite kirjeldus;

5[2]) kogutud teabe terviklikkuse ja autentsuse tagamise meetmed ja selle kontrollimist võimaldavad andmed;

3) KrMS § 126[10] lg 2 tekstist jäetakse välja sõnad "vajaduse korral".

4.5. Muud kaalumist vajavad küsimused

4.5.1. Menetleja korraldus andmete säilitamiseks ja esitamiseks

Budapesti konventsiooni artiklid 16, 17 ja 18 kohustavad konventsiooni osalisi kehtestama seadusandlikud meetmed selleks, et vajadusel oleks võimalik menetlejal anda teabevaldajale korraldus kriminaalmenetluses tähtsust omava teabe säilitamiseks teatud ajavahemiku jooksul (kuni 90 päeva) ja menetlejale üleandmiseks. Kehtiv KrMS võimaldab põhimõtteliselt selliseid meetmeid rakendada § 215 kaudu, kuid on küsitav, kas viidatud üldine regulatsioon on digitaalse teabe säilitamise ja kogumise võimalikkuse tagamiseks piisav või ei. Mitmed riigid (sh näiteks Soome) on Budapesti konventsiooni nõuete täitmiseks kehtestanud digitaalandmete säilitamise ja üleandmise nõudmiseks erikorra.

4.5.2. Läbiotsimise laiendamine

Kehtiv KrMS ei võimalda laiendada läbiotsimist sellistele seadmetele ja andmekandjatele, mis ei asu läbiotsimismäärusega kindlaksmääratud kohas, kuid mis on viimatinimetatud kohas asuvate arvutisüsteemidega ühenduses tehniliste vahendite kaudu. Näiteks Saksamaa StPO võimaldab sellisel juhul läbiotsimist laiendada ka sellistele ruumiliselt eraldatud seadmetele. Samas paljudes riikides (sh Soome, Sloveenia) Saksamaaga analoogne regulatsioon puudub. Mõistlik on kaaluda, kas Eestis on vajalik sellise läbiotsimise laiendamise võimaluse sätestamine või on praktilised olukorrad lahendatavad läbi uue läbiotsimismääruse väljastamise.

4.5.3. Ameti- või kutsesaladusega hõlmatud teabe kaitse

KrMS ei näe ette mitte mingeid garantiisid selleks, et andmekandjate käitlemisel, sh jälitustoimingute tegemisel või muul viisil tõendusteabe otsimisel ja fikseerimisel, ei riivataks ameti- või kutsesaladusega hõlmatud teabe puutumatust. Kaaluda tuleks, kas teistest seadustest tulenevad üldised ameti- ja kutsesaladuse kaitstuse nõuded tagavad piisaval määral selle, et kõnealused andmed ei muutuks kriminaalmenetluses uurimisobjektiks ja neid ei kasutataks tõendina olukorras, kus see läheks vastuollu saladuse kaitstuse põhimõttega. Kui ei, siis on vajalik KrMS täiendamine vastavate erisätetega.