TARTU ÜLIKOOL
ÕIGUSTEADUSKOND
Võrdleva õigusteaduse õppetool

Marit Konks

KRIMINAALMENETLUSES KOGUTUD ISIKUANDMETE KAITSE AVALIKU SEKTORI TEABE TAASKASUTAMISEL

Magistritöö

Juhendaja
dr iur. Mario Rosentau
Kaasjuhendaja
vandeadvokaat Mari Männiko

Tallinn
2014

SISUKORD

SISSEJUHATUS

Elame infoajastul, kus informatsioonist on saanud üks põhiressurss uute teenuste ja toodete loomiseks. Teenuseid ja rakendusi näiteks mobiiltelefonidele või interneti kasutajatele luuakse üleöö Garage 48[1] suunitlusega ettevõtluses. Paljude selliste teenuste loomise üheks eelduseks on andmebaasides või muudes infokogudes sisalduv teave. Senini on avalike andmekogude põhjal teenuste loojaks olnud esmajoones riik. Avaliku teabe taaskasutamise regulatsiooniga on aga võimalik avaliku sektori valduses olevat teavet välja anda erasektorile teenuste ja toodete väljaarendamiseks. Kui praktikas on avaliku sektori teabe taaskasutamine veel uus mõiste, siis esimene avaliku sektori teabe taaskasutamist reguleeriv direktiiv võeti Euroopa Liidu tasandil vastu juba 2003 aastal. Eesti seadusandlusesse implementeeriti direktiiv 2012. aasta detsembris, kui taaskasutamise regulatsioon sätestati Eesti avaliku teabe seaduses (AvTS).[2] AvTS §-i 8 täiendati lõikega 3, mis sätestab, et teabele juurdepääs hõlmab õigust seda teavet taaskasutada ning AvTS §-i 4 täiendati lõigetega 4^1-4^3, mis sätestavad avalikule teabele juurdepääsu tingimused ning juurdepääsutasu määramise ja suuruse põhimõtted. Järelikult on õiguslikult võimalik kasutada avaliku sektori valduses olevat teavet ka teistel elualadel ning selleks algselt mitte ettenähtud otstarbel.

Kuna tegemist on veel laialdaselt kasutamata regulatsiooniga, siis ei ole selge, kas selle rakendamine tagab alati isikuandmete kaitse. Nii on käesoleva magistritöö autor võtnud lähema uurimise alla isikuandmete kaitse teabe taaskasutamise ühes kõige sensitiivsemas valdkonnas – kriminaalmenetluses. Siit tulenevalt on sõnastatud ka magistritöö uurimisküsimus: kas avaliku sektori teabe taaskasutamise regulatsioon kaitseb kriminaalmenetluses kogutud isikuandmeid? Oma küsimusele vastuse leidmisel on autor arvestanud, et avalik sektor omab väga eripalgelist teavet riigis elavate isikute kohta. Paljud andmed ja neile ligipääs on kaitstud isikuandmete kaitse seadusega (IKS). IKS kohaldub paralleelselt AvTS-iga ning keelab delikaatsete isikuandmete avaldamise, sealhulgas teabe taaskasutamise eesmärgil. IKS-i kohaselt on delikaatsed andmed muuhulgas süüteo toimepanemise või selle ohvriks langemise kohta enne avalikku kohtuistungit või õigusrikkumise asjas otsuse langetamist või asja menetluse lõpetamist.[3] Seega väljuvad kriminaalmenetluses kogutud andmed delikaatsete andmete kaitsealast, kui kriminaalmenetlus on lõpetatud või isik mõistetud asjas õigeks. AvTS

[1] Garage 48 on ürituse formaat, kus ettevõtjad loovad teenused 48 tunni jooksul.
[2] Euroopa Komisjoni arvates ei olnud Eestis tagatud avaliku teabe taaskasutamisega seonduvad õigused ja puudus õigusselgus. Avaliku teabe seaduse muutmise seaduse eelnõu seletuskiri, lk 1
[3] IKS § 4 lg 2 p 8

kohaselt on teabevaldaja kohustatud tunnistama asutusesiseseks kasutamiseks mõeldud teabeks kriminaal- või väärteomenetluses kogutud teabe, välja arvatud vastavalt väärteomenetluse seadustikus ja kriminaalmenetluse seadustikus (KrMS) sätestatud tingimustel avaldatava teabe.[4] Seega saab kohaldada AvTS-i KrMS-s ettemääratud osas.

Eelpool öeldust tulenevalt on sõnastatud käesoleva magistritöö hüpotees: avaliku sektori teabe taaskasutamisel ei ole tagatud kriminaalmenetluses kogutud isikuandmete kaitse. Autor on hüpoteesi sõnastamisel lähtunud eeldusest, et uurimisasutustel on palju õigusi tõe väljaselgitamiseks.[5] Autor peab küsitavaks, kas sellise eriõigusega kogutud andmete puhul on nende taaskasutamine lubatav ja kas taaskasutuse regulatsioon on kehtivas seaduses piisav. Lähtudes andmete töötlemise ja kogumise eesmärgipärasuse printsiibist, ei saa avalikus sektoris ega erasektoris olemas olla muud huvi, mis vastaks nende andmete kogumise esialgsele eesmärgile. Andmete kogumine ja nende edaspidine kasutamine tulevikus muul eesmärgil läheb vastuollu minimaalsuse ja eesmärgipärasuse põhimõttega. Lisaks kehtib kriminaalmenetluses süütuse presumptsioon – kedagi ei tohi käsitada kuriteos süüdi olevana enne, kui tema kohta on jõustunud süüdimõistev kohtuotsus.[6] Autor on seisukohal, et kriminaalmenetluses kogutud andmete säilitamine ja kasutamine pärast kriminaalmenetluse lõppu ja juhul, kui puudub süüdimõistev kohtuotsus, rikub vähemalt kaudselt süütuse presumptsiooni põhimõtet. Seda põhjusel, et puudub alus kriminaalmenetluses tõe väljaselgitamise huvides kogutud andmete säilitamiseks ja kasutamiseks muul eesmärgil, kui tõde on juba selgunud ja seega esialgne andmete kasutamise eesmärk täidetud. Autori arvates saab kriminaalmenetluse puhul luua paralleeli haldusmenetlusega, kus teoreetiliselt saab kõneleda kahest peamisest ja vastandlikust menetluse eesmärgist. Neist esimeseks eesmärgiks on menetluse tulemuse õigsuse ja/või ratsionaalsuse tagamine ning teiseks menetluses osaleva isiku inimväärikuse austamine. Teist käsitlust on nimetatud ka menetlust tähtsustavaks eesmärgiks.[7] Kusjuures protseduurilist õiglust, mis peab kaitsma isikut ja tema inimväärikust, peetakse omaette eesmärgiks.[8] KrMS ja Vabariigi Valitsuse (VV) määrus "Kriminaaltoimiku arhiivimise kord ja toimiku säilitamise tähtajad pärast kriminaalmenetluse lõpetamist" ei käsitle, kuidas peaks toimima isiku toimikuga, kes mõisteti kriminaalmenetluses õigeks.

[4] AvTS § 35 lg 1 p 1
[5] Tõe väljaselgitamise eesmärk tuleneb KrMS §-st 9 lõikest 4 "Kriminaalmenetluses on isiku perekonna- või eraellu lubatud sekkuda vaid käesolevas seadustikus ettenähtud juhtudel ja korras kuriteo tõkestamiseks, kurjategija tabamiseks, kriminaalasjas tõe tuvastamiseks ja kohtuotsuse täitmise tagamiseks."
[6] Eesti Vabariigi Põhiseadus, § 22 lg 1
[7] Parrest, N. Hea halduse põhimõte Euroopa Liidu põhiõiguste hartas. Juridica I 2006, lk 24
[8] Lord Millett. The Right to Good Administration in European Law. Public Law, Sweet & Maxwell 2002 summer, lk 312

Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikkel 8 lg 2 alusel peab isikuandmete säilitamine toimuma seaduse alusel. Vastavalt AvTS §-le 35 saab sellekohase teabe tunnistada küll asutusesiseseks kasutamiseks, kuid puudub regulatsioon andmete säilitamise kohta ja on võimalik, et neid andmeid saab kasutada taaskasutamise eesmärgil. Paraku on oht, et selline andmete säilitamine ja taaskasutamine rikub isikute põhiõigust privaatsusele.

Rahvusvahelistest allikatest on isikuandmete kaitse seisukohalt olulisemad eelviidatud Euroopa inimõiguste ja põhivabaduste kaitse konventsioon (EIÕK) ja Euroopa Liidu põhiõiguste harta. EIÕK on Eesti Vabariigile siduv alates 16. aprillist 1996. Seda daatumit saab pidada *ratione temporis* piiriks, millest alates laienes Eesti elanikele konventsiooni kaitse ja riigile võetud kohustused. Konventsioon toob kaasa riigi vastutuse teiste selle lepingu osalisriikide ees[9], mida realiseeritakse Euroopa Nõukogu poliitiliste mehhanismide ja rahvusvahelise avalikkuse kaudu. Konventsiooni saab pidada tänu sõltumatule kohtulikule järelevalvele kahtlemata üheks tõhusaimaks regionaalseks inimõigusaktiks.[10] Konventsioon annab igaühele võimaluse väljuda siseriikliku jurisprudentsi ning suveräänsuse raamidest ning esitada kaebus oma riigi vastu, sealhulgas vaidlustada oma riigi kõrgema kohtu otsuseid. Kohtu otsus on siduv vaidluse poolte vahel, kuid kohtul puudub pädevus tühistada siseriiklikke õigusakte või toiminguid. Seda peab tegema riik ise ja nende tegematajätmisel riskeerib riik oma rahvusvahelise poliitilise ja lepingulise usaldusväärsuse kaotusega.[11]

EIÕK artikkel 8 sätestab privaatsusõiguse alljärgnevalt:

1. Igaühel on õigus sellele, et austataks tema era- ja perekonnaelu ja kodu ning korrespondentsi saladust.

2. Võimud ei sekku selle õiguse kasutamisse muidu, kui kooskõlas seadusega ja kui see on demokraatlikus ühiskonnas vajalik riigi julgeoleku, ühiskondliku turvalisuse või riigi majandusliku heaolu huvides, korratuse või kuriteo ärahoidmiseks, tervise või kõlbluse või kaasinimeste õiguste ja vabaduste kaitseks.

EIÕK artikkel 8 on olnud eeskujuks Eesti põhiseaduse (PS) § 26 sõnastamisel[12] ja see on käesoleva magistritöö kirjutamisel üheks fundamentaalseks õigusallikaks. Euroopa Liidu põhiõiguste harta kodifitseeris esimesena otsesõnu õiguse isikuandmete kaitsele. Nii on vastavalt harta artiklile 7 igaühel õigus sellele, et austataks tema era- ja perekonnaelu, kodu ja

[9] EIÕK konventsioon on välisleping põhiseaduse § 123 mõttes
[10] C. Ovey, R. C. A. White. European Convention of Human rights, 3rf ed. Oxford University Press 2002, lk 1
[11] R. Maruste. Konstitutsionalism ning põhiõiguste ja -vabaduste kaitse. Tallinn: Juura 2004, lk 236-237
[12] Eesti Vabariigi Põhiseadus – kommenteeritud väljaanne. Paragrahv 26. Kättesaadav: http://www.pohiseadus.ee/ptk-2/pg-26/ (20.02.2014)

edastatavate sõnumite saladust ja artikkel 8 kohaselt on igaühel õigus oma isikuandmete kaitsele ja selliseid andmeid tuleb töödelda asjakohaselt ning kindlaksmääratud eesmärkidel ja asjaomase isiku nõusolekul või muul seaduses ettenähtud õiguslikul alusel. Igaühel on õigus tutvuda tema kohta kogutud andmetega ja nõuda nende parandamist. Nende sätete täitmist kontrollib sõltumatu asutus.[13] Rahvusvahelisel tasandil on kehtestatud veel teisi üldakte isikuandmete kaitsest, kuid käesoleva töö raames autor nendel pikemalt ei peatu.[14]

Magistritöö on sisuliselt jaotatud kaheks osaks. Esimene osa keskendub avaliku teabe taaskasutamise regulatsioonile ja selle mõjule isikuandmete kaitsele. Autor analüüsib teabe taaskasutamise regulatsiooni vastavust isikuandmete kaitse põhimõtetele ning kas ja kuidas on Eesti seadustega tagatud isikuandmete kaitse teabe taaskasutamisel. Seejärel teeb autor vahekokkuvõtte, tuues esimese sisulise osa järel välja olulisemad järeldused isikuandmete kaitsest avaliku sektori teabe taaskasutamisel. Teine sisuline osa keskendub kriminaalmenetluses kogutud isikuandmete kaitsele ja võimalikule isikute privaatsusõiguse rikkumise ohule kriminaalmenetluses kogutud isikuandmete taaskasutamisel. Varasemalt on isikuandmete kaitset kriminaalmenetluses uurinud oma bakalaureusetöös Merje Jõgi.[15] Kuna eelnimetatud töö on kirjutatud aastal 2006, mil ei olnud veel kehtima hakanud IKS sellisel kujul nagu meie seda täna tunneme ja töö ei puudutanud teabe taaskasutamist, siis on käesolev magistritöö uudne ja asjakohane, sest teabe taaskasutamise valdkonda ei ole selliselt varem uuritud. Magistritöö lõpus esitab autor oma järeldused, kas kriminaalmenetluses kogutud isikuandmed on avaliku teabe taaskasutamisel kaitstud või mitte.

Magistritöös on kasutatud erinevaid uurimismeetodeid. Oma töös analüüsib autor erialakirjandust, õigusallikaid ja kohtupraktikat. Nii on kasutatud kvalitatiivset ja induktiivset meetodit teoreetilise kirjanduse analüüsimisel ja võrdlevat meetodit õigusallikate kirjeldamisel. Kohtupraktika analüüsil on kasutatud sünteesi üksikult üldisele.

Autor tänab oma juhendajaid Mario Rosentaud ja Mari Männikot magistritöö kirjutamisel osutatud abi ja väga hea koostöö eest.

[13] Euroopa Liidu põhiõiguste harta, artikkel 8 lg 3
[14] Organization for Economic Cooperation and Development: Guidelines governing the protection of privacy and transborder flows of personal data (OECD Guidelines 1980); Council of Europe: Convention for the Protection of Individuals with the regard to Automatic Processing of Personal Data (1981)
[15] Jõgi, M. Isikuandmete kaitse kriminaalmenetluses. Juhendaja Jaggo, O. 2006 Tartu Ülikool, õigusinstituut, avaliku õiguse instituut, kriminaalõiguse, kriminoloogia- ja kognitiivse psühholoogia õppetool

Töös on kasutatud järgmisi põhimõisteid:

Avalik teave – mis tahes viisil ja mis tahes teabekandjale jäädvustatud ja dokumenteeritud teave, mis on saadud või loodud seaduses või selle alusel antud õigusaktides sätestatud avalikke ülesandeid täites.[16]

Avaliku teabe taaskasutamine – füüsilise või juriidilise isiku poolt teabe kasutamine ärilisel või mitteärilisel eesmärgil, mis ei lange kokku algse eesmärgiga, mille jaoks see teave avalikke ülesandeid täites saadi või loodi. Teabevaldajatevaheline teabe vahetamine oma avalike ülesannete täitmiseks ei ole teabe taaskasutamine.[17]

Kriminaaltoimik – kriminaalmenetluse käigus kogutud andmik kõigi kriminaalasjas kogutud faktiliste asjaolude kohta.[18]

[16] AvTS § 3 lg 1
[17] AvTS § 3^1 lg 1
[18] Autori sõnastus

1. AVALIKU SEKTORI TEABE TAASKASUTAMINE

Teabe taaskasutamise regulatsioon on oma alguse saanud mitmel põhjusel. Ühelt poolt pidas Euroopa komisjon Euroopa informatsiooniturgu alaarenenuks ning oli mures, selle võimekuse pärast võistelda Ameerika Ühendriikidega. Komisjoni arvamust mõjutas asjaolu, et Ameerika Ühendriikides on avalik teave lihtsalt kättesaadav ja madalate kuludega.[19] Seepärast vajas Euroopa Liit vahendit, millega ergutada ettevõtluse arengut ja püsida maailma majanduses konkurentsis. Teiselt poolt tuleneb regulatsiooni vajalikkus Euroopa Liidu enda olemusest – Euroopa Liit on ajalooliselt selle liikmesriikide ühisturg. Seetõttu peab ka 2003. aasta teabe taaskasutamise direktiiv kõige olulisemaks eesmärgiks Euroopa Liidu asutamislepingus ette nähtud siseturu rajamist ning süsteemi sisseseadmist, mis tagaks siseturul moonutamata konkurentsi. Nii võimaldab avaliku sektori valduses oleva teabe laiem taaskasutamine Euroopa ettevõtetel ära kasutada selle teabe potentsiaali ning toetada majanduskasvu ja töökohtade loomist.[20]

Samas juba aastal 1999 on Euroopa Liidu andmekaitsevolinike assamblee *andmekaitse 29. töörühm*[21] tegelenud andmekaitse ja avalike registrite vahel valitseva vastuolulise suhtega.[22] Töörühma ajendas oma arvamust esitama rohelise raamatu ettevalmistamine, mis analüüsis teemade kaupa avaliku sektori teabe taaskasutamisest tulenevaid ohte ja kasu.[23] Esitatud arvamuses jõudis töörühm tõdemuseni, et avaliku sektori teabe hulka kuuluvad isikuandmed, mida avaldatakse mitmesugustele haldusorganitele. Kokkuvõtvalt jõudis töörühm järeldusele, et avalik juurdepääs andmetele ei tähenda kontrollimatut juurdepääsu: kõik liikmesriigid tuginevad oma õigusaktides sellele andmetele ligipääsu filosoofiale.[24] Lukas Gundermann on eelnimetatud töörühma järelduse võtnud kokku sõnadega, nagu oleks siseriiklikule seadusandjale esitatud õigusväline üleskutse, mitte ohverdada kodanike õigust privaatsusele ja

[19] K. Janssen, J. Dumortier. Towards a European framework for the re-use of public sector information: A long and winding road. International Journal of Law and Information Technology 2, 2003, pp 184-201
[20] Direktiiv 2003/98/EÜ, preambul punkt 5
[21] Töörühm on asutatud direktiivi 95/46/EÜ artikli 29 alusel. Sõltumatu Euroopa nõuandev kogu, kes tegeleb andmekaitse ja eraelu puutumatuse kaitsega. Töörühma ülesanded on kindlaks määratud direktiivi 95/46/EÜ artiklis 30 ja direktiivi 2002/58/EÜ artiklis 1. Töörühm on saanud nime andmekaitsedirektiivi artikli järgi, millega töörühm loodi.
[22] Working Party on the protection of individuals with regard to the processing the personal data. Opinion No. 3/99 WP 20 "Public sector information and the protection of personal data."
[23] Commission of the European Communities, Brussels 20.01.1999, "Public sector information – a key resource for Europe" COM (1998) 585 final
[24] "Public access to data does not mean unfettered access: all Member States base their legislation on this philosophy".

andmekaitsele täielikult avaliku sektori valduses oleva teabe kommertsliku realiseeritavuse altarile.[25]

Niisiis oli avaliku teabe taaskasutamise direktiivide loomisel Euroopa Liidus suured lootused, kuid veel rohkesti ebamäärast ning vaieldavat andmekaitse valdkonnas. Seda põhjusel, et näiteks juba eelviidatud *andmekaitse 29. töörühma* arvamus tõi välja viis eri teemat, mida peaks rohelises raamatus enam arvestama: näiteks andmetöötluse seaduslikkuse ja eesmärgipärasuse põhimõte, andmesubjekti teavitamine, iga üksikjuhtumi eraldi kaalumine ja otsustamine. Kusjuures neid teemasid tuleb arvestada mitte ainult olukorras, kus siseriiklikult on teabele ligipääs reguleeritud, vaid ka olukordades, kus see regulatsioon puudub.[26]

17. novembril 2003. aastal võeti vastu rohelise raamatu analüüsi tulemusena direktiiv 2003/98/EÜ avaliku sektori valduses oleva teabe taaskasutamise kohta. Põhjalikumad taaskasutamise eesmärgid leiame teabe taaskasutamise direktiivide 2003/98/EÜ ja 2013/37/EL preambulatest. Olgu veelkord öeldud, et 2013. aasta direktiiv ei asenda 2003. aasta direktiivi, vaid täiendab seda. Järgnevalt peatub autor 2003. aasta direktiivi eesmärkidel, sisul ja avaliku teabe taaskasutamise regulatsiooni rakendamisel tekkinud probleemkohtadel seoses isikuandmete kaitsega.

1.1. Direktiivi 2003/98/EÜ eesmärgid

2003. aasta direktiiv pidas oluliseks, et taaskasutus toimiks liikmesriikides ühtsetel alustel ja eeldas selleks õiglaste, proportsionaalsete ja mittediskrimineerivate tingimuste loomist.[27] Samuti peeti oluliseks kõikide avaliku sektori valduses olevate dokumentide kättesaadavaks tegemist – mitte üksnes poliitiliste, vaid ka seadusandlike ja haldusmenetluste osas, kuna see on oluliseks meetmeks laiendamaks õigust saada teavet, mis omakorda on demokraatia üks põhiprintsiipe. Sealjuures teabe saamise õigus kehtib nii kohaliku, riikliku kui rahvusvahelise tasandi institutsioonide puhul.[28] Käesoleva töö seisukohalt on oluline juhtida tähelepanu sellele, et direktiivi preambula punkti 21 kohaselt tuleks direktiivi kohaldada täielikus

[25] Gundermann, L. Euroopa Liidu andmekaitseõigus – andmekaitse ja andmetele avaliku juurdepääsu suhtest ning andmekaitse järelevalve olukorrast. Juridica VIII 2005, lk 515
[26] Working Party on the protection of individuals with regard to the processing the personal data, Opinion No. 3/99, WP 20 "Public sector information and the protection of personal data" p 11
[27] Direktiiv 2003/98/EÜ, peambul punkt 8
[28] *Ibid,* punkt 16

vastavuses isikuandmete kaitse põhimõtetega, mis on sätestatud Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiivis 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (*edaspidi* isikuandmete kaitse direktiiv).[29] Käesoleva töö autor peab 2003. aasta direktiivi eesmärke mõnevõrra ambitsioonikateks, sest need kõnelevad üheaegselt demokraatia põhiprintsiipidest, isikute põhiõiguste kaitsest ja andmete taaskasutamise majanduslikust kasust. Autori arvates saavad need eesmärgid olla mõneti vastandlikud, sest majanduslik kasu ja isikute põhiõiguste kaitse võivad taotleda vastupidiseid eesmärke. Näiteks on majandusliku kasu huvides saada ligipääs võimalikult paljudele isikuandmetele erisugustes andmebaasides, samas isiku huvides on võimalikult minimaalne teabe avaldamine ja privaatsuse kaitse. Nii on loodud olukord, kus tuleb kaaluda erinevaid huve. Euroopa Liidu huviks saab kindlasti pidada andmete taaskasutamisest tulenevat majanduslikku kasu. Avaliku sektori teabe taaskasutamist hinnatakse kõige suuremaks infoallikaks Euroopas ja selle ressursi turuväärtuseks vähemalt 32 miljardit eurot.[30] Huvide kaalukausi teises otsas on isikute põhiõiguste kaitse. Kuna isiku eraelu puutumatus on võõrandamatu inimõigus, siis juba eelduslikult ei ole võimalik selle põhiõiguse väärtust mõõta rahas. Inimõigused on hindamatud. Järgnevalt analüüsib autor nende huvide kaitset avaliku sektori teabe taaskasutamise 2003. aasta direktiivis.

1.2. Direktiiv 2003/98/EÜ sisu

Vastavalt direktiivi artiklile 1 on kehtestatud miinimumreeglid, et reguleerida liikmesriikide avaliku sektori valduses olevate dokumentide taaskasutamist ja nende taaskasutamist soodustavaid praktilisi abinõusid. Sealhulgas direktiivi ei kohaldata dokumentide suhtes, millele juurdepääs on liikmesriikide juurdepääsukorra kohaselt keelatud ja ei kahjusta ega mõjuta üksikisikute kaitset isikuandmete töötlemisel, nagu see on ette nähtud ühenduse ja siseriiklike õigusaktidega, ning eelkõige ei muuda see isikuandmete kaitse direktiivis sätestatud kohustusi ja õigusi. Lähtuvalt isikuandmete kaitse direktiivist mõistetakse isikuandmete all igasugust teavet tuvastatud või tuvastatava füüsilise isiku (*edaspidi* andmesubjekt) kohta. Tuvastatav isik on isik, keda saab otseselt või kaudselt tuvastada, eelkõige isikukoodi põhjal või ühe või mitme tema füüsilisele, füsioloogilisele, vaimsele, majanduslikule, kultuurilisele

[29] Euroopa Parlamendi ja nõukogu direktiiv 95/46/EÜ, 24. oktoober 1995, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta

[30] Digital Agenda for Europe. A Europe 2020 Initiative. Kättesadaav: http://ec.europa.eu/digital-agenda/en/pillar-i-digital-single-market/action-3-open-public-data-resources-re-use (25.02.2014)

või sotsiaalsele identsusele omase joone põhjal.[31] Tuvastatavus saab aga igas olukorras olla erinev. See sõltub mitmetest teguritest, nagu millised on meie isikutunnused (juuste värv, pikkus jne), aga näiteks ka sellest, kus me elame (väike küla või suur linn). Tallinnas oleks ilmselt pikk tumedapäine sale naisterahvas anonüümne, ent Veski külas Põlvamaal võib isiku nende andmete põhjal hetkega tuvastada ja isiku privaatsus ei oleks tagatud. Seega sõltub isikuandmete kaitse paljuski andmete hulgast, liigist ja kontekstist, kus need andmed parasjagu asetsevad. Isikuandmete kaitse direktiiv lubab isikuandmete töötlemist vaid seaduse alusel ja vastavalt direktiivi artiklile 1 peavad liikmesriigid tagama, et isikuandmete töötlemisel kaitstakse füüsiliste isikute põhiõigusi ja -vabadusi ning eelkõige nende eraelu puutumatust. Isikuandmete kaitse direktiiv sätestab andmete kaitsele järgnevad printsiibid:

- seaduslikkus – isikuandmeid kogutakse õiglaselt ja seaduslikult;
- proportsionaalsus – isikuandmete töötlemine peab olema vajalik ja isikuandmeid kogutakse täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel ega töödelda hiljem viisil, mis on vastuolus kõnealuste eesmärkidega. Täiendavat töötlemist ajaloo, statistika või teadusega seotud eesmärkidel ei peeta vastuolus olevaks tingimusel, et liikmesriigid kannavad hoolt vajalike tagatiste eest;
- vähesus – isikuandmed on piisavad, asjakohased ega ületa selle otstarbe piire, mille tarvis neid kogutakse ja/või hiljem töödeldakse;
- kvaliteet – andmed on täpsed ja vajaduse korral ajakohastatud; võetakse kõik mõistlikud meetmed, et kustutada või parandada andmete kogumise või hilisema töötlemise eesmärgi seisukohast ebaõiged või mittetäielikud andmed;
- säilitamiseaeg – isikuandmeid säilitatakse kujul, mis võimaldab andmesubjekte tuvastada ainult seni, kuni see on vajalik seoses andmete kogumise või hilisema töötlemise eesmärkidega.[32]

Arvestades eelnevat saab järeldada, et kui tegemist on isikuandmete taaskasutamisega, siis tuleb kohaldada nii isikuandmete kaitse kui ka avaliku teabe taaskasutamise direktiivi. Isikuandmete kaitse direktiivi sätted limiteerivad oluliselt isikuandmeid sisaldava teabe taaskasutamist. Avaliku teabe taaskasutamise direktiiv viitab isikuandmete kaitse direktiivile otsesõnu oma preambula punktis 21, artikli 1 lõikes 4 ja artikli 2 lõikes 5. Nii võiks teha järelduse, et tagatud on piisav kaitse ja selgus isikuandmete kaitsest teabe taaskasutamisel ja isikuandmete kaitse direktiiv on loonud selged raamid isikuandmete kaitsele.

[31] Direktiiv 95/46/EÜ, artikkel 2 a
[32] *Ibid*, artikkel 6

Tegelikkuses jättis 2003. aasta taaskasutamise direktiiv aga liikmesriigile laiema diskretsiooni õiguse, kas anda enda valduses olev teave[33] taaskasutusse või mitte. Mõnede arvamuste kohaselt reguleeribki teabe taaskasutamist ja andmetele ligipääsu vaid liikmesriigi seadusandlik diskretsiooniotsus juurdepääsukorra kehtestamisel.[34] Lähtudes avaliku teabe taaskasutamise direktiivi artiklist 1 lõikest 3 ei mõjutanud direktiiv liikmesriikide juurdepääsukordasid ja nende kohaldamist, kui vastavalt juurdepääsukorrale pidid kodanikud ja ettevõtted dokumentidele juurdepääsemiseks tõendama oma konkreetset huvi. Seega eksisteerib 2003. aasta teabe taaskasutamise direktiivi kohaselt konkurents avaliku sektori andmete taaskasutamise lubamise ja isikuandmete kaitse tagamise vahel. Kokkuvõttes loob selline olukord autori arvates ebakindlust nii avalikus sektoris, andmesubjektides kui võimalikes taaskasutajates, sest pole teada, mil viisil ja kuidas on isikuandmete taaskasutus ikkagi lubatud. Millal on olulisemad majanduslikud huvid ja millal kaalub isikute õigus privaatsusele ülesse võimaliku majandusliku kasu? Selle otsuse tegemine on jäetud liikmesriikide endi ja andmetele ligipääsu reguleerivate juurdepääsukordade kanda.

Praeguseks on Euroopa Kohtult olemas üks kohtulahend teabe taaskasutamisest, mis on seotud ka haldusorgani diskretsiooni rakendamisega. Kaasuses *Compass-Datenbank GmbH*[35] oli põhiküsimuse all see, kas avaliku võimu kandja on ettevõtja, kui ta salvestab andmebaasis selliseid andmeid, mille ettevõtjad peavad seadusest tuleneva kohustuse alusel esitama ja kui andmetega tutvumise ja/või väljavõtte tegemise eest nõutakse seaduse alusel tasu. Eesti mõistes on analoog vaidlusalusele andmebaasile meie äriregister. Antud kaasuses oli Austria Vabariik usaldanud mitmele ettevõtjale ülesande olla vahendusagentuuriks riikliku äriregistri *Firmenbuchi* ja lõppkasutaja vahel ning oma tegevuse tasustamiseks oli ettevõtjatel õigus nõuda lisaks riigilõivule, mis kantakse Austria Vabariigile, mõistliku suurusega lisatasu teenuse osutamise eest. Vahendusagentuuridel ja nende lõppklientidel oli keelatud luua oma andmekogusid, mis taasesitavad *Firmenbuchi* andmeid, ise neid andmeid pakkuda ja lisada andmete vahele või esitlusse reklaami. *Compass-Datenbank* ühe vahendusagentuurina soovis aga *Firmenbuchist* saada tasu eest taaskasutamiseks *Firmenbuchi* dokumente ja väljavõtteid ajalooliste andmetega. Euroopa Kohus asus kaasuse põhiküsimuses seisukohale, et avaliku võimu kandja ei ole kõnealuse tegevuse raames ettevõtja Euroopa Liidu toimimise lepingu artikli 102 tähenduses. Käesoleva töö seisukohalt peab autor olulisemaks aga kohtu väljendatud

[33] Direktiiv kasutab mõistet "dokument".
[34] K. Janssen. The influence of the PSI directive on open government data: An overview of recent developments. Government Information Quarterly 28, 2011, p 453
[35] European Court of Justice, Compass-Datenbank GmbH vs Austria 26.04.2012, C-138/11

arvamust, mille kohaselt avaliku võimu kandja võib siseriikliku õiguse sätetega arvestades õiguspäraselt keelata sellises andmebaasis (kõnealuses asjas äriregister) sisalduvate andmete taaskasutamise. Seda selleks, et kaitsta äriühingute ja muude õigussubjektide, kellele on seadusega pandud registrile teabe esitamise kohustus, huvi selle vastu, et neid puudutavaid andmeid ei taaskasutata väljaspool seda andmebaasi. Seega, kui isikul on seadusest tulenev kohustus oma andmeid riigile esitada, siis tulenevalt Euroopa Kohtu otsusest saab autori arvates laiendada seda õigustatud ootust ka füüsilistele isikutele, et nende andmeid ei taaskasutata väljaspool sellist andmebaasi ja muudel eesmärkidel.

Otseselt isikuandmete taaskasutamise kohta Euroopa Kohtu praktika praegu puudub. Ühelt poolt võiks eeldada, et see on positiivne, sest isikuõiguste rikkumisi ei ole toimunud. Teisalt võiks aga oletada, et võib-olla tulenevalt taaskasutamise direktiivi ebakindlast ja sisuliselt lahtivaidlemata isikuandmete kaitsega seonduvatest õigustest ja kohustustest, ei julge ega taha ettevõtjad avaliku sektori andmeid taaskasutada. Selline olukord saab omakorda viidata puudulikule regulatsioonile taaskasutamise direktiivis, sest direktiivi eesmärk on ennekõike soodustada avaliku teabe taaskasutamist ja seeläbi suurendada majanduslikku kasu. Sarnasele seisukohale on jõudnud M. de Vries, lisades, et juurdepääs andmetele ei tähenda alati veel seda, et neid andmeid saavad ettevõtjad taaskasutada. Vaid ligipääs andmetele ilma võimaluseta neid kasutada ei ole ettevõtjatele piisav.[36] Igal juhul on avalik sektor olukorras, kus teabenõude saamisel tuleb igat üksikjuhtumit eraldi hinnata ja kaaluda eri osapoolte huve.[37]

1.2.1. Euroopa andmekaitseinspektori arvamus

Nagu eelpool selgus, ei ole 2003. aasta direktiivis piisavalt selgelt sõnastanud isikuandmete kaitset puudutavavad õigused ja kohustused. Sellest tulenevalt on Euroopa andmekaitseinspektor Peter Hustinx 2012. aasta aprillis esitanud enda arvamuse ja järeldused direktiivi 2003/98/EÜ ja siis veel eelnõu staadiumis olnud direktiivi 2013/37/EL kohta.

[36] M. de Vries. Integrating Europe's PSI re-use rules – Demysrifying the maze. Computer Law & Security Review 27, 2011
[37] Article 29 Data Protection Working Party. Opinion 7/2003 on the re-use of public sector information and the protection of personal data – Striking the balance. WP/83, p 9

Andmekaitseinspektor juhib tähelepanu sellele, et isikuandmeid sisaldava avaliku sektori teabe taaskasutamine võib anda suuri eeliseid, ent sellega kaasnevad ka märkimisväärsed isikuandmete kaitsega seotud riskid. Seetõttu soovitab andmekaitseinspektor oma ettepanekuga uues direktiivis täpsemalt määratleda, millistes olukordades ja milliseid kaitsemeetmeid kohaldades võib nõuda isikuandmeid sisaldava teabe taaskasutamiseks kättesaadavaks tegemist, sealhulgas:

- kehtestada selgemalt, mil määral kohaldatakse avaliku sektori teabe direktiivi isikuandmete suhtes;
- nõuda, et enne, kui mis tahes isikuandmeid sisaldava avaliku sektori teabe tohib taaskasutamiseks kättesaadavaks teha, peab asjaomane avaliku sektori asutus teavet hindama;
- kui see on asjakohane, nõuda, et andmed on muudetud täielikult või osaliselt anonüümseks ning litsentsitingimustega on konkreetselt keelatud üksikisikuid uuesti identifitseerida ja taaskasutada isikuandmeid otstarbel, mis võib andmesubjekte individuaalselt mõjutada;
- nõuda, et alati, kui tegemist on isikuandmete töötlemisega, sisaldaksid avaliku sektori teabe taaskasutamise litsentsi tingimused andmekaitseklauslit;
- vajaduse korral võtta arvesse isikuandmete kaitsega seotud riske ning nõuda taotlejatelt tõendusmaterjali (andmekaitsealase mõju hindamise teel või muul viisil) selle kohta, et kõikidele isikuandmete kaitsega seotud riskidele on pööratud piisavalt tähelepanu ja et taotleja töötleb andmeid kooskõlas kohaldatavate andmekaitsealaste õigusaktidega;
- selgitada, et erandina üldpõhimõttest, mille kohaselt taaskasutamine on lubatud mis tahes ärilisel või mitteärilisel eesmärgil, võidakse seada taaskasutamine sõltuvusse selle otstarbest.

Lisaks leidis andmekaitseinspektor, et andmete töötlemiseelsed (nt digitaliseerimisega seotud), anonüümseks muutmise ja koostamise kulud peaks sisse nõudma litsentsiomanikelt, kui see on asjakohane ja soovitas komisjonil töötada välja täpsemad suunised, keskendudes andmete anonüümseks muutmisele ja litsentsimisele, ning konsulteerida selles *andmekaitse 29. töörühmaga*.[38]

[38] Euroopa Andmekaitseinspektori arvamuse kokkuvõte, mis käsitleb Euroopa Komisjoni avatud andmete paketti, sealhulgas ettepanekut võtta vastu direktiiv, millega muudetakse direktiivi 2003/98/EÜ avaliku sektori valduses oleva teabe taaskasutamise kohta, avatud andmeid käsitlevat teatist ning komisjoni otsust 2011/833/EL komisjoni dokumentide taaskasutamise kohta. Euroopa Liidu Teataja 2012/C 335/06, lk 8-9

Ka Euroopa Liidu töörühm *LAPSI* (*Legal Aspects of Public Sector Information*) on pidanud oluliseks ja teinud komisjonile ettepaneku, et uus direktiiv peab enam lahti seletama andmete kaitsega seotud kohustused ja õigused.[39] Andmete taaskasutamisel ei tohiks kindlasti erinevate avaliku sektori valduses olevates andmebaasides olevad andmed olla tuvastatavad ning andmebaasi avalikustamisel tuleks tagada andmebaasis olevate isikute anonüümsus.[40]

1.3. Direktiivi 2013/37/EL eesmärgid

Täiendav direktiiv võeti vastu kümme aastat pärast esialgsete miinimumreeglite kehtestamist avaliku teabe[41] taaskasutamisele. Vahepealsel ajal oli hüppeliselt kasvanud avalikus sektoris kogutavate andmete maht, nende kogumise viisid ning liigid. Seetõttu oli vajalik kaasajastada direktiivi, et kasutataks efektiivsemalt ära avalike andmete majanduslikud ja sotsiaalsed võimalused.[42] Direktiivi eesmärgina on peetud oluliseks kehtestada liikmesriikidele selge kohustus lubada kõikide dokumentide taaskasutamist, välja arvatud juhul, kui juurdepääs on piiratud või välistatud siseriiklike juurdepääsu reguleerivate eeskirjade alusel või kuulub muude sama direktiiviga kehtestatud erandite alla.[43] Üheks direktiivi põhimõtteks on, et isikuandmeid ei tohiks kogumise järgselt töödelda viisil, mis ei ole kooskõlas kõnealuste andmete kogumisel kindlaks määratud täpse, selge ja õiguspärase eesmärgiga ja direktiivi kohaselt peavad liikmesriigid kindlaks määrama isikuandmete seadusliku töötlemise tingimused.[44] Direktiiv peab oluliseks järgida Euroopa Liidu põhiõiguste hartas tunnustatud põhimõtteid ja õigust isikuandmete kaitsele (artikkel 8). Direktiivi ei tohi tõlgendada ega rakendada viisil, mis läheb vastuollu Euroopa inimõiguste ja põhivabaduste kaitsekonventsiooniga.[45]

2013. aasta direktiiv toob kasutusele uue mõiste "avatud andmepoliitika", mille eesmärgiks on soodustada minimaalsete või puuduvate õiguslike, tehniliste või rahaliste piirangutega avaliku sektori teabe laialdast kättesaadavust ja taaskasutamist ärilisel või mitteärilisel eesmärgil ning edendada teabe liikumist mitte ainult majanduselus osalejate, vaid ka kodanike huvides.

[39] C, dos Santos. On Privacy and Personal Data Protection as Regards Re-use of Public Sector Information (PSI). Masaryk University Journal of Law and Technology 6:3, 2012, p 339
[40] K. Janssen. The influence of the PSI directive on open government data: An overview of recent developments. Government Information Quarterly 28, 2011, p 448
[41] Direktiiv kasutab mõistet "dokument"
[42] Direktiiv 2013/37/EL, preambul punkt 5
[43] *Ibid.* punkt 8
[44] *Ibid.* punkt 11
[45] *Ibid.* punkt 34

Direktiiv toob välja, et see võib täita olulist rolli uute teenuste käivitamisel, mis põhinevad kõnealuse teabe uuenduslikel kombineerimis- ja kasutamisviisides, stimuleerida majanduskasvu ning edendada sotsiaalset kaasatust. Avatud andmepoliitika üheks eelduseks peab direktiiv taas dokumentide taaskasutamist liidu tasandil samadel tingimustel. Taaskasutamise lubamises nähakse lisaväärtuse loomise võimalust taaskasutajale, lõppkasutajale ja ühiskonnale tervikuna. Kuid ka avalikule asutusele endale, sest sellega edendatakse läbipaistvust ja vastutust ning saadakse taaskasutajalt ja lõppkasutajatelt tagasisidet, mille abil saab asjaomane avaliku sektori asutus parandada kogutud teabe kvaliteeti. [46] Direktiivi kõige olulisemaks eesmärgiks saab ilmselt pidada andmete taaskasutamise regulatsiooni kaasajastamist, sest kümne aasta möödumisega on muutunud maailmas eksisteerivate andmete hulk ja koguma on hakatud uusi andmeliike. Ka 2013. aasta direktiivi eesmärkidest kuvab enim läbi majanduslik ja sotsiaalne kasu, viitega kohustusele järgida õigust isikuandmete ja EIÕK-le ja Euroopa Liidu põhiõiguste hartale.

1.4. Direktiivi 2013/37/EL sisu

2013. aasta avaliku teabe taaskasutamise direktiiviga muudeti direktiivi kohaldamisala. Muudatuse järgi ei kohaldata direktiivi selliste dokumentide suhtes, millele juurdepääs on liikmesriikide juurdepääsukorra kohaselt keelatud, sealhulgas:

- dokumendid, millele juurdepääs on piiratud liikmesriikide juurdepääsukorraga, sealhulgas kui kodanikud ja ettevõtjad peavad tõendama oma konkreetset huvi juurdepääsuks dokumentidele;[47]
- dokumendid, millele juurdepääs on välistatud või piiratud juurdepääsukorraga isikuandmete kaitse tõttu ning dokumentide osad, mis on selle korra alusel juurdepääsetavad ning sisaldavad isikuandmeid, mille taaskasutamine on õiguslikult määratletud sellise õigusakti rikkumisena, millega reguleeritakse üksikisikute kaitset isikuandmete töötlemisel.[48]

Rohkemat täiendav direktiiv isikuandmete kaitsest ei reguleeri. Küll on uuendusena taaskasutamise reguleerimisala laiendatud raamatukogudele, sealhulgas ülikoolide raamatukogudele, muuseumidele ja arhiividele.[49]

[46] *Ibid.* punktid 3-4
[47] Direktiiv 2013/37/EL, artikkel 1 punkt ca
[48] *Ibid.* artikkel 1 punkt cc
[49] *Ibid.* preambul punkt 14

Kokkuvõtvalt saab öelda, et 2003. aasta direktiiv andis ette miinimumnõuded andmete taaskasutamisele ja viitelise kohustuse järgida isikuandmete kaitse direktiivis sätestatud õiguseid ja kohustusi. 2013. aasta direktiivilt oodati nende õiguste ja kohustuste täpsemat selgitamist. Täiendav direktiiv siiski endiselt ei anna täpsemaid juhiseid taaskasutajale, andmesubjektile ja avaliku sektori asutustele isikuandmete taaskasutamisel kehtivate konkreetsete õiguste ja kohustuste kohta. Taas sõltub ligipääs isikuandmetele ja nende taaskasutamise lubatavus liikmesriigi diskretsiooni otsusest ja liikmesriigi juurdepääsukorra regulatsioonist. Kui varasemalt viitas direktiiv vaid isikuandmete kaitse direktiivile, siis täiendav direktiiv viitab lisaks Euroopa Liidu põhiõiguste hartale ja direktiivi ei tohi tõlgendada ega rakendada viisil, mis läheb vastuollu EIÕK-ga. Praegusel kujul ei ole 2013. aasta direktiiv autori arvates arvestanud Euroopa andmekaitseinspektori ja *LAPSI* töörühma ettepanekuid, sest taaskord on viidatud taaskasutamise direktiivist väljapool asuvatele õigusaktidele ning direktiivis endas puudub endiselt konkreetne seisukoht isikuandmete taaskasutamise õiguste ja kohustuste kohta.

1.5. Direktiivide 2003/98/EÜ ja 2013/37/EL kooskõla direktiiviga 95/46/EÜ

Euroopa Liidus võeti üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta direktiiv vastu aastal 1995 ja direktiivi põhimõtted on kajastatud käesoleva töö peatükis 1.2. Isikuandmete kaitse direktiiv on konkreetne ja seniajani kehtinud isikuandmete kaitset puudutavatest regulatsioonidest kõige sügavama teema käsitlusega. Direktiiv kasutab rahvusvahelistes allikates nagu OECD juhend[50] ja Euroopa Nõukogu 1981. aasta konventsioon[51] kehtestatud mõisteid ja lähtub neis kehtestatud isikuandmete töötlemise põhimõtetest, reguleerides neist kõige üksikasjalikumalt isikuandmete kaitset.[52] Ühe eristuva ja olulise eesmärgina on isikuandmete kaitse direktiiv oma artiklis 1 lõikes 1 seadnud eesmärgiks, et liikmesriigid kaitsevad isikuandmete töötlemisel füüsiliste isikute põhiõigusi ja -vabadusi ning eelkõige nende õigust eraelu puutumatusele.[53] Seega on isikuandmete kaitse direktiiv otsesõnu seadnud oma eesmärgiks isikute privaatsuse kui ühe põhiõiguse kaitse.

[50] Organization for Economic Cooperation and Development: Guidelines governing the protection of privacy and transborder flows of personal data (OECD Guidelines 1980)
[51] Council of Europe: Convention for the Protection of Individuals with the regard to Automatic Processing of Personal Data (1981)
[52] Tikk, E. Nõmper, A. Informatsioon ja õigus. Tallinn: Juura 2007, lk 67
[53] Kattub IKS § 1 lõikega 1

Isikuandmete kaitse direktiiv tõlgendab terminit "isikuandmed" küllaltki avaralt. Nähtuvalt preambula punktist 26 tuleb kaitsmise põhimõtteid kohaldada igasuguse tuvastatud või tuvastatava isiku kohta käiva teabe suhtes ja isiku tuvastatavuse kindlakstegemisel tuleb arvesse võtta kõiki vahendeid, mida volitatud töötleja või keegi muu võib andmesubjekti tuvastamiseks kasutada.[54] Järelikult on isikuandmed igasugused andmed, mida saab konkreetse isikuga seostada ja pole tähtis, mis valdkonnas need andmed on kogutud. Seega peab andmete taaskasutamine arvestama nende isikuandmete kaitsega ja tagama isikute tuvastamatuse. Sealjuures on oluline andmete kogumise eesmärk. Nii on näiteks info maja väärtuse kohta, kui seda väärtust kasutatakse piirkonna kinnisvara hindade näitlikustamiseks, vaid info eseme kohta. Juhul, kui maja väärtuse alusel määratakse isiku maksekohustuse ulatust, siis tuleb käsitleda seda infot isikuandmetena.[55] Niisiis sõltub andmete kasutamise eesmärgist, kas tegemist on isikuandmetega või mitte.

Isikuandmete kaitse direktiivi reguleerimisala käsitlev artikkel 3 lõike 2 kohaselt ei kohaldata direktiivi isikuandmete töötlemise suhtes, kui see toimub sellise tegevuse käigus, mis on seotud avaliku korra, riigikaitse, riigi julgeoleku (sealhulgas riigi majanduslik heaolu, kui töötlemine on seotud riigi julgeoleku küsimustega) ja riigi toimingutega kriminaalõiguse valdkonnas. Direktiivi preambula kohaselt tuleb direktiivi kohaldada heli- ja pildiandmete töötlemisele, kui tegemist on automatiseeritud töötlemisega või kui andmed võetakse lihtsat juurdepääsu võimaldavast kataloogist või kantakse andmed sellisesse kataloogi. Heli- ja pildimaterjali sisaldavate andmete töötlemine (näiteks videovalve), ei kuulu andmekaitse direktiivi reguleerimisalasse, kui see on seotud riigi toimingutega kriminaalõiguse valdkonnas.[56]

2003. aasta teabe taaskasutamise direktiivi kohaselt tuleb direktiivi kohaldada ja rakendada täielikus vastavuses isikuandmete kaitse põhimõtetega[57] ja direktiiv ei kahjusta ega mõjuta üksikisikute kaitset isikuandmete töötlemisel ja ennekõike ei muuda see isikuandmete kaitse direktiivis sätestatud õigusi ja kohustusi.[58] Seega ei saa automaatselt eeldada, et igasugune andmete taaskasutamine on lubatud. Kui haldusorgani valduses olev teave sisaldab isikuandmeid, siis nende andmete taaskasutamise lubatavuse küsimus langeb koheselt isikuandmete kaitse direktiivi kaitse alla. Järelikult, kui teabe taaskasutamine hõlmab

[54] Seda järeldust toetab 20.06.2007 *andmekaitse 29 töörühma* arvamus 4/2007 isikuandmete mõiste kohta. Mille kohaselt "andmed käivad üksikisiku kohta, kui need viitavad tema isikule, omadustele või käitumisele või kui sellist teavet kasutatakse, et määrata või mõjutada seda, kuidas kõnealust isikut koheldakse või hinnatakse".
[55] *Ibid.* lk 9
[56] Direktiiv 95/46/EÜ, preambuli punktid 14-16
[57] Direktiiv 2003/98/EÜ, peambul punkt 21
[58] *Ibid.* artikkel 1 lg 1

isikuandmeid, siis haldusorgan ei saa tugineda teabe taaskasutamise regulatsioonile kui õiguspärasele vahendile nende andmete taaskasutamise automaatseks lubamiseks.

Andmekaitse 29. töörühm soovitab tungivalt, et enne isikuandmete taaskasutusse andmist tuleb läbi viia põhjalik analüüs nende isikuandmete taaskasutusse andmise mõjude kohta. Lisaks on töörühm andnud liikmesriikidele soovituse, et kaaluda võiks sellise mõjude analüüsi kohustuslikuks muutmist oma seadusandluses või edendada eeskuju mõjude analüüsi rakendamiseks. Igal juhul ja isegi kui see ei ole *expressis verbis* seaduses kirjas, peaks haldusorgan viima läbi põhjaliku analüüsi, et tuvastada, kas isikuandmeid võib anda taaskasutamiseks, ja kui see on lubatud, siis millistel tingimustel ja millistel isikuandmete kaitseks vajalike turvameetmetega on see taaskasutamine lubatav. Lisaks peaks mõjude analüüs võimalusel kaasama kõiki huvigruppe, sealhulgas isikuandmete volitatud töötlejat, teabenõudjat, andmesubjektide esindajat, kelle isikuandmete avalikustamist volitatud töötleja kaalub.[59] Seega on *andmekaitse 29. töörühm* näinud vajadust enne isikuandmete taaskasutusse andmist läbi viia põhjalik mõjude analüüs.[60] Autor nõustub *andmekaitse 29. töörühma* ettepanekuga ja peab vajalikuks selliste analüüside tegemise kohustuslikuks muutmist. Kui töörühm soovitas mõjude analüüsi muuta kohustuslikuks liikmesriikide tasandil, siis autori arvates peaks see kohustus olema kehtestatud direktiiviga Euroopa Liidu tasandil. Seda põhjusel, et liikmesriikide õiguskorrad ja isikuandmete kaitset puudutavad juurdepääsukorrad on liikmesriigiti erinevad ning seetõttu ei ole ühtsetel alustel üle liidu tagatud isikuandmete kaitse. Lisaks ei oleks selliselt tagatud võrdne konkurents andmete taaskasutamiseks saamiseks eri liikmesriikides, mis otseselt rikub vaba ja moonumata konkurentsi põhimõtet Euroopa Liidus.

Andmekaitse 29. töörühm on pidanud veel vajalikuks kehtestada seaduslikud meetmed, mis selgelt kirjeldaksid, milline teave on avalik ning millistel eesmärkidel ja tingimustel on selle taaskasutamine lubatud.[61] Konkreetseid kriteeriume teabe eesmärgipärase kasutamise hindamiseks on peetud vajalikuks, sest muidu on vaid õrn lootus, et teabe taaskasutamisel täidetakse eesmärgipärasuse põhimõtet. Väidet nagu "õigusraamistik peab olema kujundatud

[59] Article 29 Data Protection Working party. Opinion 06/2013 on open data and public sector information (PSI) reuse. WP 207, pp 6-7

[60] Näiteks on Suurbritannia *Information Commissioner's Office* loonud infoportaali riigiasutustele, kodanikele ja ettevõtjatele, mis annab konkreetsed juhised isikuandmete kaitseks ja kuidas muuta isikuandmeid anonüümseks. Kättesaadav: http://ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation (29.04.2014)

[61] Article 29 Data Protection Working party. Opinion 06/2013 on open data and public sector information (PSI) reuse. WP 207, p 10

selliselt, et ta võimalikult väldiks teabe teistsugust kasutamist" on peetud abituks.[62] Lukas Gundermann on seetõttu tõdenud, et õiguse võimet toimida juhtimisvahendina, on teabe eesmärgipärase taaskasutamise hindamisel selgelt üle hinnatud.[63] Autor nõustub siinkohal Gundermanni esitatud seisukohaga, sest kahtleb, kas õigusraamistikul saab ilma objektiivsete alusteta olla üldse kompetentsi, et hinnata laiapõhjaliselt teabe kasutamise eesmärke. Seega on konkreetsed kriteeriumid vajalikud, et tagada õiguspärane andmetöötlus.

Samas peab *andmekaitse 29. töörühm* võimalikuks, et isegi selliste kriteeriumite kehtestamisel ei saa olla alati kindel, et seda teavet võib teabe taaskasutamise direktiivi alusel taaskasutada. Seega tekib küsimus, kas isikuandmeid üldse saab taaskasutada? Tulenevalt *andmekaitse 29. töörühma* seisukohast on isikuandmete taaskasutamine lubatud, kui need on muudetud täiesti anonüümseks. Seda peetakse ka kõige efektiivsemaks lahenduseks, minimaliseerimaks riske isikuandmete tahtmatu avalikustamise eest. Samas on väljakutsuv ülesanne otsustada, millisel tasemel andmete liitmine oleks sobiv ja millist spetsiifilist anonüümseks muutmise meetodit tuleks kasutada.[64] Kuna isikuandmete kaitse direktiiv käsitleb mõistet "isikuandmed" avaralt, tuleb autori arvates isikuandmete anonüümseks muutmisel arvestada kõikvõimalike ohtudega, mis ka kaudselt annavad võimaluse isikuid identifitseerida ja taastuvastada. Küll aga saab asuda seisukohale, et kui isikuandmed on muudetud täiesti anonüümseks, siis isikuandmete kaitse direktiiv enam ei kohaldu ja teavet võib taaskasutada ilma isikuandmete kaitse direktiivist tulenevate piiranguteta.[65] Sellisel juhul ei saa aga enam rääkida isikuandmete taaskasutamisest, vaid lihtsalt andmete taaskasutamisest kui sellisest.

Teabe anonüümseks muutmist on aga peetud järjest keerulisemaks ülesandeks ja isikute äratundmine algselt anonüümseks muudetud allikates on saanud tõsiseks ohuks. Nii tõi *andmekaitse 29. töörühm* näitena välja ühe narkootikumide ja alkoholi kuritarvitamise, seksuaalse väärkohtlemise ja koolikohustuslikkuse kohta koolides läbiviidud uuringu. Uuring oli tehtud heas usus ja parimate kavatsustega, ent hoolikalt oli läbimõtlemata andmete alusel isikute taastuvastatavus. Uuringu andmetel oli 500 õpilasega koolis A aastal 2012 20% õpilasi (100 õpilast), kelle üks vanematest oli kas narko- või alkoholisõltlane. Nendest omakorda 8% (8 õpilast) oli seksuaalselt väärkoheldud. Uuringu kohaselt rohkem õpilasi koolis A ei olnud seksuaalselt väärkoheldud. Oluliselt vaeva heade hinnete saamisel koolis nägi 96% õpilastest,

[62] Gundermann, L. Euroopa Liidu andmekaitseõigus – andmekaitse ja andmetele avaliku juurdepääsu suhtest ning andmekaitse järelevalve olukorrast. Juridica VIII 2005, lk 515
[63] *Ibid.*
[64] Article 29 Data Protection Working party. Opinion 06/2013 on open data and public sector information (PSI) reuse. WP 207, pp 10-12
[65] Direktiiv 95/46/EÜ preambul p 26, artkkel 2 a

kelle vanemad olid alkohoolikud või narkosõltlased ja neist 50% olid õpilased, keda oli seksuaalselt väärkoheldud (4 õpilast). Kuna oli teada, et heade hinnetega ja muidu helge peaga õpilase C ema on alkohoolik, siis C klassikaaslased järeldasid, et õpilane C kuulub 50% õpilaste hulka, keda on kodus seksuaalselt väärkoheldud.[66] Seega antud juhul ei olnud täidetud isikuandmete kaitse direktiivist tulenev isiku tuvastamatuse nõue ja tagatud ei olnud isiku eraelu puutumatus. Eeltoodud näitest tulenevalt on autori arvates olemas väga lai hall ala, kus teabe väljaandja usub, et isikuid ei ole võimalik andmehulgast tuvastada, ent kolmandad osapooled saavad ikkagi vähemalt osa isikutest andmehulgast tuvastada, kasutades näiteks muud avalikku infot või muud infot, mis on kolmandale isikule kättesaadav. Nii pidas ka *andmekaitse 29. töörühm* üheks suurimaks ohuks järjest kasvavat internetivõrgus kättesaadavat teavet, mis ei piirdu vaid avalikult kättesaadava teabega. Töörühma hinnangul on juba väga suur hulk teavet erinevatel organisatsioonidel ja ettevõtjatel olemas ja isikuandmete taaskasutusse andmisega võib tõenäoliselt ilmneda, et algselt tuvastamata isikud saavad tuvastatuks ja seda tihti ilma andmesubjektide endi teadmata.[67] Seega järjest laiaulatuslikumaks muutuv isikuandmete kogumine ja töötlemine vähendab andmesubjekti kontrolli oma andmete käitlemise üle. Kuna info- ja kommunikatsioonitehnoloogiad võimaldavad isikuandmeid massiliselt koguda ja töödelda, siis kujutab selline tegevus ohtu üksikisiku eraelu puutumatusele ning üldisele isiksusõigusele: erinevaid andmeid kombineerides on võimalik luua võrdlemisi terviklik pilt isiku suhetest, harjumustest, omadustest, varalisest seisust ja muust sellisest ning seeläbi isikut nii öelda jälgida. Seepärast tuleb andmetöötlust piirata põhiseaduslike õiguste kaitseks, et iga isik saaks ise otsustada, kui palju ta end teistele isikutele ning laiemale avalikkusele nähtavaks teeb.[68]

2013. aasta teabe taaskasutamise direktiiv lisas uuendusena, et teabe taaskasutamine laieneb raamatukogudele ja arhiividele. Pärast teatud aja möödumist, kui dokumendid ei ole enam haldusorganile vajalikud või need on täitnud oma eesmärgi, viiakse läbi asutuses hindamisprotsess, mille tulemusena osa dokumente arhiivitakse kui ajaloolise väärtusega dokumendid. *Andmekaitse 29. töörühm* pidas sellise arhiivimise põhiküsimuseks seda, et millistel teistel eesmärkidel arhiivitud isikuandmeid üldse saab taaskasutada? Näiteks, kui Eesti Rahvusarhiivis arhiivitakse kriminaaltoimik, saab see jätkuvalt häbistada isikut ja tema

[66] Article 29 Data Protection Working party. Opinion 06/2013 on open data and public sector information (PSI) reuse. WP 207, p 16
[67] *Ibid.* pp 13-14
[68] Ilus, T. Andmesubjekti osaluse põhimõte Euroopa Nõukogu konventsioonide ning Euroopa Inimõiguste Kohtu lahendite valguses. Juridica VIII/2005, lk 522

rehabilitatsiooni ühiskonda, kuna toimik võib sisaldada väga delikaatseid isikuandmeid. Isegi, kui avalikkusel ei ole juurdepääsupiirangu tõttu ligipääsu kriminaaltoimikule, on avalikkusele teada ja kättesaadav fakt toimiku olemasolust. Arhiivitud dokumendid võivad sisaldada delikaatseid andmeid lisaks muudest valdkondadest, nagu informatsiooni raskest haigusest või muudest delikaatsetest katsumustest või sündmustest isiku elus. Seejuures juurdepääsupiirangud arhiivis on tähtajalised, mistõttu saavad need dokumendid millalgi avalikuks ja seega saavad otseselt mõjutada, kui mitte andmesubjekti ennast, siis andmesubjekti järeltulijaid ja sugulasi.[69] Eestis reguleerib arhiivimist arhiiviseadus ja arhiivieeskiri. Rahvusarhiivis säilitatavale arhivaalile on juurdepääs vaba, kui sellele ei laiene AvTS-s, IKS-s, riigisaladuse ja salastatud välisteabe seaduses (RSVS) või muus seaduses kehtestatud piirangud.[70] AvTS-i ei kohaldata aga juurdepääsu võimaldamisel arhivaalidele Rahvusarhiivis ja kohaliku omavalitsuse arhiivis arhiiviseaduses ja selle alusel sätestatud korras, välja arvatud juurdepääsupiirangute kehtestamise osas.[71]

Tulenevalt *andmekaitse 29. töörühma* seisukohast on teabe taaskasutamise direktiivid kooskõlas isikuandmete kaitse direktiiviga, kui taaskasutamiseks väljastatud isikuandmed on anonüümsed ja täiesti tuvastamatud. Autori arvates peaks Eesti Andmekaitse Inspektsioon (AKI) sarnaselt Suurbritannia isikuandmete kaitse ametile välja töötama konkreetsed juhised isikuandmete anonüümseks muutmise kohta.[72] Praegu konkreetselt seesugune juhis AKI-l puudub.[73] Küll aga kahtleb autor, kas arhiivides olevate dokumentide taaskasutusse andmise kord on kooskõlas isikuandmete kaitse direktiiviga. On üldine Euroopa Inimõiguste Kohtu (EIK) seisukoht,[74] et mida kauem aega on läinud mööda isikuandmete esialgsest kogumisest, seda enam saavad need andmed osaks isiku privaatsfäärist. Seetõttu ei ole autori arvates õiguspärane olukord, kus pikaajaliselt säilitatakse riiklikus arhiivis isikuandmeid sisaldavaid dokumente, millel teatud aja möödudes juurdepääsupiirang lõppeb ja dokumendid saavad avalikuks.

[69] Article 29 Data Protection Working party. Opinion 06/2013 on open data and public sector information (PSI) reuse. WP 207, p 24
[70] Arhiiviseadus § 10 lg 1
[71] AvTS § 2 lg p 2
[72] Anonymisation: managing data protection risk code of practice. Information Commissioner's Office. Kättesaadav: http://ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Practical_application/anonymisation-codev2.pdf (29.04.2014)
[73] AKI koduleht. Kättesaadav: http://www.aki.ee/et/juhised (02.05.2014)
[74] Näiteks EIKo 04.05.2000, 28341/95, Rotaru vs Romania, § 43; EIKo 13.11.2012, 24029/07, M.M vs United Kingdom

2. AVALIKU SEKTORI TEABE TAASKASUTAMISE REGULATSIOON EESTI ÕIGUSES

2.1. Avaliku teabe seadus

Avaliku teabe seadus on Eestis vastu võetud 2000. aastal ja eelkõige sellepärast, et isikutele oleks tagatud haldusdokumentidele juurdepääs, mis võimaldab ennetavalt kontrollida halduse tegevuse seaduslikkust (üldine ennetav õiguskaitse).[75] 2012. aasta detsembris täiendati AvTS-i avaliku sektori teabe taaskasutamist reguleerivate sätetega. AvTS muutmise seaduse eelnõu eesmärgiks oli avaliku teabe taaskasutatavaks tegemise abil stimuleerida uute toodete ja teenuste loomist erasektori poolt.[76] Seaduse muudatuse algatuse tingis Euroopa Komisjoni osutatud vajadus rikkumiste parandamiseks Eesti õiguskorras, sest Euroopa Komisjoni arvates ei olnud Eestis tagatud avaliku teabe taaskasutamisega seonduvad õigused ja puudus õigusselgus.[77] Seaduse muudatusega lisati AvTS-i § 3^1, mis sätestab avaliku teabe taaskasutamise mõiste ja AvTS §-i 8 täiendati lõikega 3, mis sätestab, et teabele juurdepääs hõlmab ka õigust seda teavet taaskasutada ning AvTS §-i 4 täiendati lõigetega 4^1-4^3, mis sätestavad avalikule teabele juurdepääsu tingimused ja juurdepääsutasu suuruse ning määramise põhimõtted.

Tulenevalt AvTS-i muudatustest on võimalik kasutada avaliku sektori valduses olevat teavet ka teistel elualadel ning selleks algselt mitte ettenähtud otstarbel. Erinevalt direktiividest ütleb AvTS põhimõttena välja, et teabele juurdepääsu võimaldamisel peab olema tagatud isiku eraelu puutumatus.[78] Seadus ei viita edasi teistele seadustele, vaid kohustab tagama isiku eraelu puutumatuse. Autor peab seda oluliseks ning mõnevõrra selgemaks teabe taaskasutamise direktiivide regulatsioonidest, mis viitavad isikuandmete kaitse direktiivi isikuandmete kaitse põhimõtetele ja liikmesriikide juurdepääsukordadele. Autori arvates peaks teabe taaskasutamise direktiiv vähemalt sama selgelt antud põhimõtte sätestama, sest see on konkreetne, kõigile arusaadav seisukoht ja annab edasi tugeva signaali, et isikuandmete kaitse peab tagama isikute eraelu puutumatuse. Seaduse muutmise seletuskirja kohaselt ei erine teabe taaskasutamine tavapärasest avaliku teabe avalikustamisest ning teabenõuete esitamisest.

[75] K. Merusk, R. Narits. Eesti konstitutsiooniõigusest. Tallinn: Juura 1998, lk 199
[76] Avaliku teabe seaduse muutmise seaduse seletuskiri, lk 1 Kättesaadav: http://www.riigikogu.ee/?op=ems&page=eelnou&eid=bd9d9bac-52dc-4549-a23c-ee4816e0a2af& (21.02.2014)
[77] *Ibid*, lk 2
[78] AvTS § 4 lg 3

Avaliku teabe taaskasutamist peetakse üheks teabe kasutamise viisiks ja seega kohaldub avaliku teabe taaskasutamisele AvTS kogu ulatuses alates põhimõtetest kuni järelevalveni.[79]

Nagu tõi autor välja käesoleva töö sissejuhatuse, siis on teabe taaskasutamine AvTS kohaselt füüsilise või juriidilise isiku poolt teabe kasutamine ärilisel või mitteärilisel eesmärgil, mis ei lange kokku algse eesmärgiga, mille jaoks see teave avalikke ülesandeid täites saadi või loodi. Seega lubab AvTS teabe taaskasutamist selle kogumise esialgsest eesmärgist erineval viisil. Autori arvates võib selline sõnastus seadust rakendavatele haldusorganitele ning teavet taaskasutada soovivatele kolmandatele isikutele luua väära arusaama, nagu võiks taaskasutada kogu haldusorgani valduses olevat teavet. Kuigi AvTS kohaldub paralleelselt IKS-ga, oleks õigusselguse mõttes tarvilik isikuandmete kaitse tagamiseks AvTS-s sätestada isikuandmete taaskasutamise keeld, nii nagu on see põhimõttena väljatoodud avaliku teabe seaduse muutmise seaduse seletuskirjas.[80]

Lisaks on oluline pöörata tähelepanu juba eelpool viidatud AvTS §-le 4, mis sätestab avalikule teabele juurdepääsu põhimõtted. Nende kohaselt on demokraatliku riigikorralduse tagamiseks ning avaliku huvi ja igaühe õiguste vabaduste ja kohustuste täitmise võimaldamiseks teabevaldajad kohustatud tagama juurdepääsu nende valduses olevale teabele seaduses sätestatud tingimustel ja korras. Teabele juurdepääs tuleb tagada igaühele võimalikult kiirel ja hõlpsal viisil ning tasuta, kui seadusega pole tasu ettenähtud. Igaühel on õigus vaidlustada teabele juurdepääsu piiramist, kui selline piirang rikub tema õigusi ja vabadusi. Seoses AvTS-i täiendamisega lisati isikuandmete kaitset puudutav põhimõte, et teabele juurdepääsu võimaldamisel peab olema tagatud isiku eraelu puutumatus ja autoriõiguste kaitse. Seega lubab AvTS justkui isikuandmeid kasutada selleks algselt mitteettenähtud eesmärgil, kui see ei riiva isikute eraelu puutumatust. Nii tekib magistritöö autori arvates siin hoolimata eraelu puutumatuse põhimõtte sätestamisest AvTS-s ebakõla AvTS-i, teabe taaskasutamise direktiivide ja rahvusvaheliste õigusallikate vahel isikuandmete kaitse tagamise kohta. Seda põhjusel, et tulenevalt rahvusvahelistes allikates kehtivatele põhimõtetele on isikuandmete kasutamine ja säilitamine selleks algselt mitteettenähtud eesmärgil keelatud. Teabe taaskasutamise regulatsioon AvTS-s on loonud aga oma tõlgenduse, mille kohaselt isikuandmete taaskasutamine on lubatud ja selleks algselt mitteettenähtud eesmärgil, kui

[79] Avaliku teabe seaduse muutmise seaduse seletuskiri, lk 4 Kättesaadav: http://www.riigikogu.ee/?op=ems&page=eelnou&eid=bd9d9bac-52dc-4549-a23c-ee4816e0a2af& (30.04.2014)
[80] *Ibid*. lk 6

tagatud on isikute eraelu puutumatus. Autor jätkab probleemi lahkamist järgmises peatükis, lisades analüüsi IKS-i.

2.2. Isikuandmete kaitse seadus

Üheks suurimaks andmetöötlejaks saab pidada riiki, sest riik haldab ja valdab oma kodanike andmeid ja töötleb neid andmeid oma ülesannete täitmiseks.[81] Samas isikuandmete töötlemise õigus ei tähenda töötleja absoluutset võimu andmete üle, andmesubjekt peab saama võimalikult palju oma isikuandmete töötlemist mõjutada, selles osaleda ja seda kontrollida.[82] Nii on paljud andmed ja neile ligipääs Eestis kaitstud IKS-ga, näiteks delikaatsed isikuandmed, nagu: poliitilisi vaateid, usulisi ja maailmavaatelisi veendumusi kirjeldavad andmed, välja arvatud andmed seadusega ettenähtud korras registreeritud eraõiguslike juriidiliste isikute liikmeks olemise kohta; etnilist päritolu ja rassilist kuuluvust kirjeldavad andmed; andmed terviseseisundi või puude kohta; andmed pärilikkuse kohta; biomeetrilised andmed (eelkõige sõrmejälje-, peopesajälje- ja silmaiirisekujutis ning geeniandmed); andmed seksuaalelu kohta; andmed ametiühingu liikmelisuse kohta; andmed süüteo toimepanemise või selle ohvriks langemise kohta enne avalikku kohtuistungit või õigusrikkumise asjas otsuse langetamist või asja menetluse lõpetamist.[83] IKS kohaldub paralleelselt AvTS-ga ning keelab delikaatsete isikuandmete avaldamise sealhulgas teabe taaskasutamise eesmärgil. Samuti ei tohi avalikustada teavet, mis oluliselt kahjustaks isiku eraelu puutumatust.[84]

Eestis on isikuandmete kaitse direktiiv harmoniseeritud IKS-ga. AvTS lubab isikuandmeid taaskasutada, kui sellega ei kaasne oluline eraelu puutumatuse riive, kuid IKS lubab isikuandmete töötlemise ainult kolmel juhul:

1. kui on olemas andmesubjekti nõusolek;
2. kui haldusorgan töötleb isikuandmeid avaliku ülesande täitmise käigus seaduse või välislepingu või Euroopa Liidu Nõukogu või Euroopa komisjoni otsekohalduva õigusaktiga ettenähtud kohustuse täitmiseks;
3. kui riigisaladusega seotud isikuandmete töötlemise tingimused ja korra kehtestab Vabariigi Valitsus määrusega.[85]

[81] Andmete omanikuks on andmesubjektid, kelle nõusolekut riik vajab andmete töötlemiseks.
[82] Ilus, T. Andmesubjekti osaluse põhimõte Euroopa Nõukogu konventsioonide ning Euroopa Inimõiguste Kohtu lahendite valguses. Juridica VIII/2005, lk 522
[83] IKS § 4 lg 2
[84] AvTS § 35 lg 1 p 12
[85] IKS § 10

Seetõttu ei tohi haldusorgan näiteks dokumendiregistris avaldada ühegi eraisiku nime ilma tema nõusolekuta või igal üksikjuhtumil kontrollitud selgelt ülekaaluka vajaduseta. Põhiõigustesse otsesema või kaudsema sekkumise oht eksisteerib alati, kui jutt käib üheselt tuvastatava isiku kohta käivate andmete töötlemisest. Ivo Pilving on esitanud arvamuse, et need õigused oleks paremini tagatud, kui tunnustada iseseisva põhiõigusena õigust kõikide isikut identifitseerida võimaldavate andmete kaitsele.[86] Järgmisena vaatame isikuandmete töötlemisele kohalduvaid põhimõtteid.

Isikuandmete töötlemise põhimõtted tulenevad isikuandmete kaitse direktiivi artiklist 6. IKS on sarnaselt direktiivile sätestanud isikuandmete töötlemise põhimõtted IKS §-s 6. Täiendavalt direktiivile sõnastab IKS veel kolm põhimõtet, mida isikuandmete töötlemisel peab järgima. Esiteks kasutuse piiramise põhimõte, mille kohaselt isikuandmeid võib koguda vaid ulatuses, mis on vajalik määratletud eesmärkide saavutamiseks. Teiseks turvalisuse põhimõte, mille järgi isikuandmete kaitseks tuleb rakendada turvameetmeid, et neid kaitsta tahtmatu või volitamata töötlemise, avalikuks tuleku või hävimise eest. Kolmandaks individuaalse osaluse põhimõte, mille kohaselt andmesubjekti tuleb teavitada tema kohta kogutavatest andmetest, talle tuleb võimaldada juurdepääs tema kohta käivatele andmetele ja tal on õigus nõuda ebatäpsete või eksitavate andmete parandamist. Seega on IKS täpsemalt reguleerinud isikuandmete töötlemisele kohalduvaid põhimõtteid ja lisatud on individuaalse osaluse, turvalisuse ja kasutuse piiramise põhimõtted.

Avaliku teabe seaduse muutmise seaduse seletuskirja kohaselt ei ole isikuandmete töötlemise põhimõtetega kooskõlas erinevaid isikuandmeid sisaldavate andmebaaside kopeerimine ja taaskasutatavaks tegemine, sest sellega kaasneks tõenäoliselt andmesubjekti õiguste oluline riive. Nii on näiteks AKI teinud Lasnamäe Linnaosavalitsusele ettekirjutuse, milles kohustati linnaosavalitsust kustutama rahvastikuregistrist saadud andmete põhjal koostatud eraldiseisev andmebaas, mis sisaldas ja kajastas 19 708 täisealise mittekodaniku andmeid.[87]
Samas avalikustatud isikuandmete kohta üksikpäringute tegemine on lubatav, sest mahukale isikuandmete töötlemisele on seatud tõke – üksikpäringu vorm. Nii ei pidanud seadusandja avaliku teabe seaduse muutmise seaduse seletuskirja kohaselt üksikpäringut, näiteks kinnistusraamatust, isiku eraelu puutumatust ülemäära riivavaks. Seda põhjusel, et päringu tegemise huvi kaalub üles eraelu puutumatuse, näiteks külgnevate kinnisasjade omanike kindlakstegemisel. Kahjustavaks peetakse aga masspäringute tegemist, sest see võimaldab

[86] Pilving, I. Õigus isikuandmete kaitsele. Juridica VIII/2005, lk 535
[87] AKI 27.05.2013 ettekirjutus-hoiatus Lasnamäe Linnaosavalitsus, isikuandmete kaitse asjas

erinevate andmebaaside võrdlemisel kombineerida isiku kohta käivat teavet. Seletuskiri toob välja olulise järelduse, et hoolimata avalike andmekogude olemasolust (näiteks kinnistusraamat, asutuse dokumendiregister, karistusregister), ei ole isikuandmete kaitse mõttega kooskõlas isikuandmete taaskasutatavaks tegemine. Taaskasutatavad saavad olla avalike andmekogude andmed isikustamata kujul.[88] Paraku on see põhimõte jäänud vaid seletuskirja ja pole samal kujul jõudnud edasi seadusesse.

AvTS kaitseb IKS-is sätestatud delikaatseid isikuandmeid. Eelmises peatükis jõudis autor järeldusele, et AvTS on loonud tõlgenduse, mille kohaselt on isikuandmete taaskasutamine lubatud ja ka selleks algselt mitteettenähtud eesmärgil, kui tagatud on isikute eraelu puutumatus. Kuigi AvTS kaitseb IKS-is sätestatud delikaatseid isikuandmeid, siis ei laiene see kaitse justkui kõikidele isikuandmetele ja AvTS lubab isikuandmete avaldamise juhul, kui selline teabe avaldamine ei kahjusta oluliselt andmesubjekti eraelu puutumatust.[89] Seega on seadusandja jätnud kolmandatele isikutele isikuandmete avaldamise haldusorgani diskretsiooniotsuseks. Diskretsiooni põhieesmärgiks on ennekõike tagada üksikjuhtumi õiglane lahendamine ja selle teostamisel on haldusorgan olukorras, kus ta peab ühelt poolt arvestama seaduse eesmärki *ratio legis*'t ja teiselt poolt konkreetseid elulisi asjaolusid, et leida üksikjuhtumile sobiv ja õiglane lahendus. Diskretsiooniotsuses põimuvad nii otstarbekus kui õiglus.[90] Antud juhul peab haldusorgan suutma hinnata, kas tegemist on isikuandmetega[91] ja, millisel eesmärgil on need andmed kogutud ning kas ja millisel eesmärgil on õigus neid andmeid kasutada tulevikus.[92] Tulenevalt AvTS-st peab haldusorgan suutma hinnata, kas isikuandmete väljastamisega rikutakse eraelu puutumatust oluliselt. Mis omakorda saab autori arvates tähendada seda, et eraelu puutumatuse riive või oht eraelu puutumatust riivata on juba AvTS-i sisse kirjutatud, sest AvTS ei välista sellise riive võimalikkust.

Ivo Pilving on esitanud seisukoha, mille kohaselt iseseisva põhiõiguste riivena on käsitatav iga isikuandmetega tehtav toiming. See ei tähenda, et isikuandmete töötlemine oleks keelatud, kuid see töötlemine peab olema seadusega piisaval määral reglementeeritud, riik peab olema kaalunud töötlemise vajalikkust ning töötlemise suhtes peab olema tagatud sõltumatu järelevalve ja kohtulik kaitse. Samas abstraktselt ei ole võimalik määrata, kas avalikkuse

[88] Avaliku teabe seaduse muutmise seaduse seletuskiri, lk 4-6 Kättesaadav: http://www.riigikogu.ee/?op=ems&page=eelnou&eid=bd9d9bac-52dc-4549-a23c-ee4816e0a2af&, (30.04.2014)
[89] AvTS § 35 lg 1 p 12
[90] Merusk. K. Admnistratsiooni diskretsioon ja selle kohtulik kontroll. Tallinn: Juura Õigusteabe AS 1997, lk 64
[91] Isikuga saab seostada ka andmeid, mis otseselt ei viita isikule, kuid saab isikuga seostada, näiteks andmed kinnisvara kohta, vt p 1.3
[92] Isikuandmete kasutusse andmise üle otsustamisel peab arvestama IKS §-s 6 ja direktiivis 95/46/EÜ artiklis 6 kehtestatud põhimõtteid

juurdepääs näiteks perekonnaseisuaktidele kahjustab alati lubamatul määral eraelu või ei kahjusta seda üldse. Riigikohus on leidnud, et reeglina ei pruugi perekonnaseisuaktide kättesaadavus eraelu kahjustada, kuid kuna erandite esinemise võimalus on reaalne, tuleb igasse teabenõudesse suhtuda tõsiselt ja ettevaatlikult, küsides enne teabe avalikustamist asja kohta andmesubjekti arvamust. Igal juhul on väär saavutada efektiivsus teabenõudja huvides teise isiku õiguste raskema rikkumise arvel.[93] Autor nõustub Ivo Pilvinguga ja on arvamusel, et eraelu efektiivsemaks kaitseks võiks enne teabenõudjale vastamist küsida andmesubjekti arvamust. Selline andmetöötleja kohustus tagaks andmesubjektile efektiivsema põhiõiguste kaitse ja oht andmesubjekti eraelu riiveks oleks väiksem.

Eesti seadusandja saabki autori arvates haldusorgani tööd muuta lihtsamaks ja selgemaks, võttes eeskuju Saksa Liidukonstitutsioonikohtu seisukohast, mille kohaselt seadusandja peab määrama kindlaks eesmärgid, milleks isikuandmeid kasutada tohib, ning andmetöötlemisel on need eesmärgid põhimõtteliselt siduvad.[94] Sealjuures selle eesmärgi muutmiseks on vaja seaduslikku alust. Muudatus peab olema esialgse eesmärgiga kooskõlas, õigusselgelt sätestatud ning põhiõiguslikult kaitstud huvidega võrreldes ülekaalukate üldiste huvidega õigustatud.[95] Peale selle tuleb olenevalt olukorrast sätestada korralduslikud ja menetluslikud või tehnilised kaitseabinõud.[96]

VAHEKOKKUVÕTE

Eelnevast tulenevalt on käesoleva töö autor seisukohal, et teoreetiline ja praktiline käsitlus teabe taaskasutamise ja isikuandmete kaitse kohta ei kattu. Andmete taaskasutamise direktiivide ja Eesti seadusandlusega oleks teoreetiliselt justkui isikuandmete kaitse tagatud. Samas on esitatud mitmeid vastupidiseid arvamusi ja esitatud ettepanekuid, et tagada isikuandmete efektiivsem kaitse. Avaliku teabe seaduse muutmise seletuskirja kohaselt ei ole isikuandmete taaskasutatavaks tegemine kooskõlas isikuandmete kaitse põhimõttega. Samas AvTS ei sätesta, et isikuandmeid ei tohi taaskasutada. Lisaks seaduste regulatsioonidele on isikuandmete avaldamine seatud sõltuvusse avaliku sektori asutuste juurdepääsukordadest. Nii langeb teabe

[93] Pilving, I. Õigus isikuandmete kaitsele. Juridica VIII/2005, lk 533
[94] Albers, M. Isikuandmete kaitsepõhiõiguslik alus: kas õigus informatsioonilisele enesemääramisele ja/või eraelu austamisele? Juridica VIII 2005, lk 540 viide nr 18 BVerfGE 65. kd , lk 46; GrundgesetZ'i artikkel 10 kohta: BVerfGE 100 kd., lk 359 jj; Grundgesetz'i artikkel 13 kohta: BVerfGE 109. kd, lk 375 jj
[95] *Ibid*, viide nr 19 BVerfGE 65. kd, lk 1 (61 jj); 100. kd, lk 360; 109. kd, lk 375 jj; 110. kd, lk 69
[96] *Ibid*, viide nr 20 BVerfGE 65. kd, lk 46

taaskasutamise direktiivide ja siseriiklike seaduste alusel tegelik otsustusruum ja vastutus konkreetsele haldusorganile, kes isikuandmeid haldab.

Isikuandmete töötlemisele kohalduvad printsiibid, mida tuleb arvestada iga üksikjuhtumi hindamisel. Neist tähtsaimaks peab autor siinkohal eesmärgipärasuse põhimõtet, mille kohaselt ei tohi isikuandmeid töödelda viisil, mis läheb vastuollu nende andmete esialgse kogumise ja töötlemise eesmärgiga. Autor on seisukohal, et Eesti õigusraamistik peab sätestama selgemad kriteeriumid ja juhised, mille alusel haldusorgan saaks hinnata, kas teavet kasutatakse eesmärgipäraselt või mitte. Eeskujuks seadusandjale saavad siin olla Saksa Liidukonstitutsioonikohtu antud juhised. Nii võiks Eesti seaduse tasandil määrata kindlaks eesmärgid, milleks isikuandmeid kasutada tohib ja kehtestada teabe taaskasutamisele korralduslikud, menetluslikud või tehnilised kaitseabinõud. Seejuures tuleb arvestada, et vastavalt isikuandmete kaitse direktiivile on isikuandmete taaskasutamine lubatud vaid juhul, kui andmed on muudetud anonüümseks ja täiesti tuvastamatud.

Kuigi riik on üheks suurimaks andmetöötlejaks, ei tähenda see veel seda, et andmed kuuluvad alati vaid riigile. Isikuandmed kuuluvad andmesubjektile, kelle nõusolekut riik vajab nende andmete töötlemiseks. Andmesubjektil omakorda peab olema võimalik kontrollida oma andmete kasutamist ja töötlemist riigi poolt. Kuigi Euroopa Liit on kehtestanud andmete taaskasutamise regulatsiooni, mis lubab riigi poolt kogutud andmeid kasutada selleks algselt mitte ettenähtud eesmärkidel, ei tohi riik kahjustada isikute eraelu puutumatust. Nagu on öelnud Robert Alexy: kaitsev riik on aktiivne riik.[97] Eesti seadusandlus peab olema selge ja üheselt mõistetav ning puudujääkide avastamisel on riigi ülesanne tegutseda, et tagada isikute põhiõiguste kaitse.

Autor teeb siinkohal kolm järeldust:

1. Isikuandmete kaitse on tagatud, kui haldusorgani juurdepääsukord ja diskretsiooniotsus seda garanteerivad.
2. Isikuandmete taaskasutamine on lubatud, kui need andmed on kogutud seaduslikul alusel ja eesmärgil ning andmed on muudetud anonüümseks.
3. Teabe taaskasutamise regulatsiooni efektiivseks ja eesmärgipäraseks kasutamiseks peab seadusandja kehtestama selgemad juhised isikuandmete kasutamise eesmärgipärasuse hindamiseks ja anonüümseks muutmiseks.

[97] Alexy, R. Põhiõigused Eesti põhiseaduses. Eriväljaanne. Juridica 2001, lk 70

3. ISIKUANDMETE KAITSE KRIMINAALMENETLUSES

Kriminaalmenetluses on isiku perekonna- või eraellu lubatud sekkuda vaid KrMS-s ettenähtud juhtudel ja korras kuriteo tõkestamiseks, kurjategija tabamiseks, kriminaalasjas tõe tuvastamiseks ja kohtuotsuse täitmise tagamiseks.[98] Kriminaalmenetluse läbiviimisel koostatakse kriminaaltoimik, mis sisaldab kõiki faktilisi asjaolusid kriminaalmenetluses kogutud andmete kohta. Seega sisaldab toimik sealhulgas isikuandmeid nii süüdistatava, kannatanu, tunnistajate ja teiste asjaga seotud isikute kohta. Eraelu saab riivata iga kaitseala ebasoodus mõjutamine riigi poolt, aga ka riigi kaitsekohustuse täitmata jätmine. Nii saab füüsilist ja vaimset puutumatust riivata isiku läbivaatus (KrMS § 188) ja läbiotsimine (KrMS § 91), võrdlusmaterjali võtmine (KrMS § 100), sunniviisiline sõrmejälgede ja DNA-proovide võtmine, sundvaktsineerimine, toimingud isiku vaba ja teadliku nõusolekuta meditsiini ja bioloogia valdkonnas ning isiku jälgimine ja jälitamine.[99]

IKS-i kohaselt on seadusega kaitstud delikaatsed isikuandmed, sealhulgas andmed süüteo toimepanemise või selle ohvriks langemise kohta enne avalikku kohtuistungit või õigusrikkumise asjas otsuse langetamist või asja menetluse lõpetamist.[100] Seega pärast avalikku kohtuistungit, asjas otsuse langetamist ja asja menetluse lõpetamist väljuvad andmed delikaatsete isikuandmete kaitsealast. Samas ei tähenda see, et tegemist ei oleks enam üldse isikuandmetega ja et neid andmeid enam üldse ei kaitsta.[101]

Kriminaalmenetluse kulgemise ajal reguleerib kohtueelses menetluses kogutud andmete avaldamist KrMS § 214. Nõnda võib kohtueelses menetluses andmeid avaldada vaid prokuratuuri loal ja prokuratuuri määratud ulatuses sama paragrahvi lõikes 2 sätestatud tingimustel. Sealjuures kohtueelse menetluse andmete avaldamine on lubatud kriminaalmenetluse, avalikkuse või andmesubjekti huvides, kui see ülemäära ei kahjusta andmesubjekti ega kolmandate isikute õigusi, eriti delikaatsete isikuandmete puhul.[102] KrMS § 214 on erinormiks IKS-is kehtestatud eeldustele isikuandmete töötlemisel, sest vastavalt IKS § 2 lg 2 kohaldatakse IKS-i kriminaalmenetlusele ja kohtumenetlusele menetlusseadustikes sätestatud erisustega. See ei vabasta aga kohtueelses menetluses andmete avaldamisel ja kui

[98] KrMS § 9 lg 4
[99] Eesti Vabariigi Põhiseadus – kommenteeritud väljaanne. Paragrahv 26, punktid 9, 9.1. Kättesaadav: http://www.pohiseadus.ee/ptk-2/pg-26/ (09.04.2014)
[100] IKS § 4 lg 2 p 8
[101] RKHKo 3-3-1-3-12, p 19; IKS § 4 lg 1
[102] KrMS § 214 lg 2 p 4

need andmed sisaldavad isikuandmeid, arvestamast IKS §-s 6 sätestatud isikuandmete töötlemise põhimõtetega.[103] AvTS § 2 lg 2 p 4 kohaselt ei rakendu AvTS juurdepääsupiirangute, juurdepääsu eritingimuste, korra ja viiside osas, juhul kui need on eriseaduses või välislepingus sätestatud teisiti. Autor on seisukohal, et kui KrMS on eriseaduseks IKS-i suhtes, siis on KrMS eriseaduseks ka AvTS-i suhtes, sest isikuandmete kaitsmisel kohaldatakse nii IKS-i kui AvTS-i koos.

Juhul, kui kriminaalmenetlus lõpetatakse KrMS §-des 200-205[1] sätestatud alustel, siis antakse kriminaaltoimik üle arhiivi. Nendeks kriminaalmenetluse lõpetamise alusteks on, kui ilmeb kriminaalmenetlust välistav asjaolu; kuriteo toimepannud isik on tuvastamatu; kuriteo on toimepannud süüvõimetu alaealine; kriminaalmenetluse lõpetatamine avaliku huvi puudumise tõttu ja süü ei ole suur; kriminaalmenetluse lõpetamine karistuse ebaotstarbekuse tõttu; kriminaalmenetluse lõpetatamine leppimise tõttu; kriminaalmenetluse lõpetatamine välisriigi kodaniku toimepandud kuriteos või välisriigis toimepandud kuriteos; kriminaalmenetluse lõpetatamine seoses isikult tõendamiseseme asjaolude väljaselgitamisel saadud abiga; kriminaalmenetluse lõpetamine konkurentsialase kuriteo puhul; kriminaalmenetluse lõpetatamine seoses mõistliku aja möödumisega. Üldmenetluses kohtusse saadetud kriminaalasjas antakse kriminaaltoimik arhiivi kohtulahendi jõustumisel.[104] Järelikult arhiivitakse kriminaalmenetluse lõpetamise järgselt kõik kriminaaltoimikud. Kriminaaltoimiku arhiivimise korra ja toimiku säilitamise tähtajad on määratud VV määrusega nr 261 ja selle järgi arhiivitakse uurimisasutustes toimikud uurimisasutuse arhiivihalduse korra kohaselt.[105]

Süütuse presumptsioon on eelkõige kriminaalmenetluslik printsiip, mis on üks ausa kohtumenetluse garantiisid.[106] Isikuandmete kaitse seisukohalt on peetud peamiseks küsimuseks, kas, ja kui, siis millises ulatuses piirab süütuse presumptsioon isikuandmete avaldamist isiku poolt kuriteo toimepanemise või sellekohase kahtluse kohta väljaspool süütuse presumptsiooni kriminaalmenetluslikke eesmärke.[107] Süütuse presumptsiooni põhieesmärgiks ei ole isikuandmete kaitse, kuid seda loetakse siiski osaks isiku mainega. Ehk süütuse presumptsiooni isiku mainega seotud poole eesmärgiks on kaitsta isiku mainet kui süütut ehk konkreetses kuriteos mitte süüdiolevat.[108] Euroopa Inimõiguste Kohus (EIK) on tauninud

[103] Männiko, M. Õigus privaatsusele ja andmekaitse. Tallinn: Juura 2011, lk 214
[104] KrMS § 209 lg 1[1]
[105] VV määrus nr 261, § 4 lg 9
[106] Kergandberg, E., Sillaots, M. Kriminaalmenetlus. Tallinn: Juura 2006, lk 51
[107] Männiko, M. Õigus privaatsusele ja andmekaitse. Tallinn: Juura 2011, lk 210
[108] *Ibid*, lk 210-211

olukorda, kus kriminaalmenetluses õigeks mõistetud isikuid koheldakse samal viisil kui süüdimõistetud isikuid.[109] EIK on leidnud, et süütuse presumptsioon sisaldab üldist reeglit, mille kohaselt pärast isiku õigeksmõistmist ei tohi mingilgi viisil levitada või anda alust vastupidiseks arvamuseks.[110]

Kuigi EIK on pidanud teatud juhtudel lubatavaks erallu sekkumist, näiteks kuritegude preventatsiooniks ja seda kriminaalmenetluse käigus[111] ei ole tegemist kestva õigusega juhul kui kriminaalmenetlus lõpetatakse või isik mõistetakse kriminaalasjas õigeks.[112]

EIÕK artikkel 8 ja isikuandmete kaitse seisukohalt on oluline küsimus, kas, ja kui, siis millises ulatuses on riik õigustatud säilitama kriminaalmenetluses kogutud isikuandmeid, kui kuriteo toimepanemises kahtlusalustavat isikut ei ole süüdi mõistetud. Kõnealust küsimust on vaaginud EIK oma lahendis *S and Marper*.[113]

Eelnimetatud lahendis oli Suurbritannia säilitanud pärast kriminaalmenetluse lõppu määramata ajaks avaldajate sõrmejäljed, rakunäidised ja DNA-profiilid eesmärgiga kasutada neid tulevikus kuritegevuse ennetamiseks ja avastamiseks. Kusjuures esimene avaldaja S, kes ühtlasi oli alaealine, oli mõistetud kriminaalasjas õigeks ja teise avaldaja osas lõpetati kriminaalmenetlus enne süüdistuse esitamist. Kuigi Suurbritannia oli nende andmete säilitamise kehtestanud seadusega ja andmetel oli seadusega ette nähtud eesmärk (kuritegude ennetamine ja avastamine), ei pidanud EIK neid eesmärke demokraatlikus ühiskonnas vajalikuks. Nii kritiseeris EIK Inglismaa ja Walesi seadusi, sest need ei arvesta sõrmejälgede, rakunäidiste ja DNA-profiilide säilitamisel piisavalt isiku vanuse aspektiga ning süüteo liigi ja raskusega, mille menetlemise raames need andmed võeti. Inglismaa ja Walesi seadustes oli ette nähtud eelviidatud andmete kustutamise alused, kuid need katsid väga erandlikke asjaolusid, nagu algupärane andmete kogumise õigusvastasus või kuriteo toimepanemise puudumise fakti kindel tuvastamine. Nii leidis EIK, et puudub tasakaal era- ja avalike huvide vahel, sest riik on ebaproportsionaalselt sekkunud isiku privaatsusesse ja tema erallu. Olenemata sellest, et EIK käsitles kaasuses kitsamalt küsimust sõrmejälgede, rakunäidiste ja DNA-profiilide säilitamise kohta pärast kriminaalmenetlust, kus süüdimõistmist ei järgnenud, pidas EIK vajalikuks siseriiklikult rakendada sarnaseid meetmeid ka teistele sarnastele andmetele. EIÕK artiklis 8

[109] Eesti õigusterminoloogias võib mõiste "süüdimõistev otsus" suunata arusaamisele, et see erand seondub ainult kriminaalmenetlusega. See ei ole nii. EIÕK järelevalveorganid kasutavad sisulist lähenemist, hinnates ka rakendatava sanktsiooni iseloomu ja raskust. Seetõttu võib Eestis haldusõigusrikkumisena käsitletav delikt olla EIÕK seisukohalt (kriminaal)süütegu. Vaata lähemalt: Maruste. R. Isikuvabadus- ja puutumatus. Lk 115 – Lõhmus, U. (koost). Inimõigused ja nende kaitse Euroopas. Tartu: Sihtasutus Iuridicum 2003, lk 115

[110] EIKo 21.03.2000, 28389/95, Rushiti vs Austria

[111] EIKo 25.02.1997, 22009/93, Z vs Finland

[112] EIKo 10.12.2008, 30562/04 and 30566/04, S and Marper vs United Kingdom

[113] *Ibid.*

lõikes 2 sätestatud seadusega kooskõla nõue tähendab, et meetmel ei saa olla lihtsalt "mingisugune" alus kehtivas õiguses, vaid see peab olema ka ette ennustatav "koos kõikide tagajärgedega".[114] Eraelu on EIK käsitluse kohaselt lai mõiste, millel puudub ammendav definitsioon. See katab nii isiku füüsilise kui ka psühholoogilise terviklikkuse[115] ja mitmeid aspekte isiku füüsilisest ja sotsiaalsest identiteedist.[116] EIK seisukoha järgi kuuluvad EIÕK artikli 8 kaitsealasse lisaks isiku sugu, nimi, seksuaalne orientatsioon, seksuaalelu, terviseseisund ja etniline kuuluvus.[117] Kui Euroopa Nõukogu 1981. aasta konventsioon määratleb kitsamalt isikuandmeteks näiteks andmed, mis paljastavad isiku etnilise päritolu ja seda spetsiaalses kategoorias, koos muude delikaatsete isikuandmetega,[118] siis EIÕK artikkel 8 kaitseb lisaks kitsastele kategooriatele isiku õigust enda arendamisele, õigust rajada ja arendada suhteid teiste isikutega ja välismaailmaga.[119] Nii sisaldab mõiste eraelu veel enam isiku õigust ka oma kuvandile.[120]

Eesti õigus ei reguleeri, kuidas säilitada õigeksmõistva kohtuotsuse jõustumise järgselt kriminaalmenetluses kogutud andmeid. Kuna EIÕK artikkel 8 lg 2 kohaselt tuleb andmeid säilitada vaid "seaduse alusel", siis on olemas otsene ja potentsiaalne isikute privaatsusõiguse rikkumine EIÕK artikkel 8 lg 2 mõttes. EIK on lahendis *S and Marper* otsesõnu viidanud isikuandmete töötlemise põhimõtetele ja et kogutud andmeid võib töödelda ja säilitada vaid eesmärgipäraselt. Seega, kui eesmärk on saavutatud, siis puudub vajadus nende andmete edaspidiseks kasutamiseks ja säilitamiseks. Autor on lisaks seisukohal, et *S and Marperi* kaasuses väljatoodud isikuandmete kaitse eesmärgipärase kasutamise ja säilitamise põhimõte toetab süütuse presumptsiooni põhimõtte kehtimist kõigile kriminaalmenetluses osalevatele ja osalenud isikutele.

Eesti PS on EIÕK artikkel 8 eeskujul sõnastanud perekonna- ja eraelu puutumatuse põhimõtte §-s 26. Sama sätte teise lause kohaselt ei tohi riigiasutused, kohalikud omavalitsused ja nende ametiisikud sekkuda kellegi perekonna- ja eraellu muidu, kui seaduses sätestatud juhtudel ja korras tervise, kõlbluse, avaliku korra või teiste inimeste õiguste ja vabaduste kaitseks, kuriteo tõkestamiseks või kurjategija tabamiseks. Nii on PS § 26 üheks oluliseks valdkonnaks

[114] EIKo 04.05.2000, 28341/95, Rotaru vs Romania
[115] EIKo 29.02.2002, 2346/02, Pretty vs United Kingdom, § 61; EIKo 22.07.2003, 24209/94, Y.F. vs Turkey, § 33
[116] EIKo 07.02.2002, 53176/99, Mikulic vs Croatia, § 53
[117] EIKo 10.12.2008, 30562/04 and 30566/04, S and Marper vs United Kingdom, § 66
[118] Council of Europe: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Article 6
[119] European Commission of Human Rights. Report of the Commission. Burghartz vs Switzerland 21.10.1992, § 47; European Commission of Human Rights. Report of the Commission. Friedl vs Austria 31.01.1995, § 44
[120] EIKo 11.01.2005, 50774/99, Sciacca vs Italy, § 29

isikuandmete kaitse ja eraelu puutumatuse riivena käsitatakse muuhulgas isikuandmete kogumist, säilitamist, kasutamist ja avalikustamist.[121] EIK on oma praktikas seisukohal, et isikuandmete säilitamine ja kasutamine võib riivata õigust eraelu puutumatusele ja privaatsusõiguse riive on lubatud vaid seadusliku aluse olemasolul.[122] Juhul, kui isikuandmeid kogutakse ilma seadusliku aluseta ja andmesubjekti nõusolekuta on see vastuolus EIÕK artikliga 8, sealjuures ei saa andmete töötlemise vajadust põhjendada riikliku julgeoleku tagamise vajadusega.[123]

PS kommentaaridest tuleneb, et EIÕK artikkel 8 lg 2 on niivõrd avaralt sõnastatud, et võimaldab riivata perekonna- ja eraelu puutumatust peaaegu igal mõeldaval põhjusel.[124] Nii leidis põhiseaduse ekspertiisikomisjon põhiseaduse kommentaare koostades, et PS § 26 teises lauses ettenähtud piiramisvõimalused on osutunud liiga kitsaks, kuna loetelu ei võimalda eraelu riiveid, mis on vajalikud politsei- ja korraõiguses ning kriminaalmenetluses (nt kriminaaltäitemenetluses, vangistusest vabanenud isikute resotsialiseerimiseks või riikliku julgeoleku tagamiseks). Nii esitas ekspertiisikomisjon ettepaneku PS § 26 sõnastuse üldisemaks muutmiseks, sest mida üldisem on säte oma kaitseala poolest, seda üldisemalt peaks olema sõnastatud ka piirangu klausel ja ka lihtne seadusereservatsioon võimaldab põhiõigusi tõhusalt kaitsta.[125] Seega tegi komisjon ettepaneku laiendada avaliku võimu diskretsiooni ning anda enam võimalusi ja vabadust rohkemate isikuandmete töötlemiseks. Autor nõustub siinkohal ekspertiisikomisjoniga, et PS peaks olema sõnastatud sama avaralt kui EIÕK artikkel 8, ent autor on ka seisukohal, et sellisel juhul tuleb mõistet "eraelu" sisustada sarnaselt EIK praktikale. Selleks, et teada saada, kas kriminaalmenetluses on tagatud isikuandmete kaitse, analüüsib autor töö järgnevates osades Eesti uurimisasutustes, maakohtutes ja e-toimiku infosüsteemis kehtestatud juurdepääsupiiranguid ja säilitamistähtaegu. Autor peab oluliseks lisaks juurdepääsupiirangutele analüüsida säilitustähtaegade regulatsiooni, sest mida kauem avalik sektor andmeid säilitab, seda pikemal perioodil on võimalik neid andmeid taaskasutada.

[121] RKHKo 3-3-1-3-12, p 19
[122] EIKo 26.03.1987, 9248/81, Leander vs Sweden
[123] EIKo 16.02.2000, 27798/95, Amann vs Switzerland
[124] Eesti Vabariigi Põhiseadus. Kommenteeritud väljaanne. § 26, p 11.2 Kättesaadav: http://www.pohiseadus.ee/ptk-2/pg-26/ (30.04.2014)
[125] *Ibid*, p 11.3; Eesti Vabariigi Põhiseaduse ekseprtiisikomisjoni lõpparuanne. Põhiseaduse analüüs. Kättesaadav: http://www.just.ee/10725 (14.03.2014)

3.1. Isikuandmete säilitamine ja kaitse Vabariigi Valitsuse määruses nr 261

Uurimisasutused Eestis on Politsei- ja Piirivalveamet (PPA), Kaitsepolitseiamet (KAPO) ja Riigiprokuratuur.[126] Nagu öeldud, reguleerib kriminaaltoimikute arhiveerimist VV määrus nr 261 "Kriminaaltoimiku arhiveerimise kord ja säilitamise tähtajad". Kriminaaltoimik selle määruse tähenduses on KrMS §-des 200-205^2 sätestatud alustel lõpetatud kriminaalasja toimik ja üldmenetluse kriminaaltoimiku materjalid, mida ei ole lisatud kohtutoimikusse.[127] Nii arhiivitakse kriminaaltoimik kõikides KrMS §-des 200-205^2 nimetaud menetlustes ja määruses kehtestatud arhiivi üleandmise tähtaegade kohaselt. Sealjuures kriminaaltoimikud arhiivitakse uurimisasutuse arhiivihalduse korra kohaselt [128] ja üldmenetluses otsuse jõustumisel arhiivitakse kriminaaltoimik prokuratuuris prokuratuuri arhiivihalduse korra kohaselt.[129] Järgnevalt analüüsib autor uurimisasutustes kehtestatud arhiivihalduse kordasid, arvestades VV määruses nr 261 kehtestatud kriminaaltoimikute säilitamise tähtaegu.

Tulenevalt VV määruse nr 261 §-st 6 säilitatakse pärast kriminaalmenetluse lõpetamist KrMS §-des 200, § 201 lg 2, §-des 203, 203^1 , 204, 205, 205^1, 205^2 ja 274^2 sätestatud alustel kriminaaltoimikut 10 aastat alates kriminaalmenetluse lõpetamise määruse koostamisest või kohtumääruse jõustumisest. KrMS § 200^1 sätestatud alustel säilitatakse esimese astme kuriteo kriminaaltoimikut 15 aastat alates kriminaalmenetluse lõpetamise määruse koostamisest. Üldmenetluses otsuse jõustumisel säilitatakse kriminaaltoimikut 10 aastat alates kohtulahendi jõustumisest. Kriminaaltoimikud süüteos inimsuse vastu, sõjasüüteos või süüteos, mille toimepanemise eest on karistusseadustikus ette nähtud eluaegne vangistus säilitatakse alaliselt. Uurimisasutuse, maakohtu ja prokuratuuri arhiivis säilitatakse arhivaale hävitamiseni nende säilitustähtaja möödumisel või üleandmiseni avalikku arhiivi. Kuna selgus, et Eestis arhiivitakse kõik alaealiste komisjoni tehtud otsused 10 aastaks, siis peab autor kaheldavaks, kas seesugune regulatsioon on proportsionaalne ja kas see arvestab isiku vanuse aspektiga nii, nagu EIK on seda ette näinud oma lahendis *S and Marper*.

[126] KrMS § 31 lg 1 kohaselt on uurimisasutusteks on veel Maksu- ja Tolliamet, Konkurentsiamet, Sõjaväepolitsei, Keskkonnainspektsioon ning Justiitsministeeriumi vanglate osakond ja vangla, kes täidavad uurimisasutuse ülesandeid vahetult või nende hallatavate või kohalike asutuste kaudu. KrMS. Käesolevas magistritöös on autor ennekõike keskendunud politsei- ja julgeolekuasutustele.
[127] VV määrus nr 261 "Kriminaaltoimikute arhiivimise kord ja säilitamise tähtajad", § 3
[128] *Ibid.* § 4 lg 9
[129] *Ibid*. § 4^1

3.1.1. Kaitsepolitseiamet

KAPO lähtub kriminaal- ja väärteomenetluses kogutud teabe menetlusjärgsel avaldamisel ja isikuandmete kaitsmisel AKI ja Riigiprokuratuuri ühiskirjast uurimisasutustele ja väärtegude kohtuvälisele menetlejale. Kirja kohaselt ei reguleeri alates toimiku arhiveerimisest toimikumaterjalide avaldamist enam menetlusseadustik ja aluseks tuleb esmajoones võtta arhiiviseadus koosmõjus AvTS-ga. Nii otsustab arhiveeritud toimikumaterjalide juurdepääsupiirangute ja andmete väljastamise üle ja nende õiguspärasuse eest teabevaldaja, see tähendab asutus, kus arhiveeritud toimik asub. Juurdepääsupiirangud kehtestatakse arhiivitoimikus sisalduvale teabele tulenevalt AvTS §-st 35 ning eriseadustest. Sealjuures sõltuvalt piirangu alusest kehtestatakse erinevad tähtajad (AvTS § 40). Isikuandmeid sisaldavale teabele on juurdepääsupiirang selle saamisest või dokumenteerimisest alates 75 aastat või isiku surmast alates 30 aastat, või kui surma ei ole võimalik tuvastada, siis 110 aastat isiku sünnist. Isikuandmeid sisaldavale teabele juurdepääsu lubamisel lähtutatakse AvTS-s sätestatud juurdepääsupiirangutest. AKI ja Riigiprokuratuuri ühiskirjast tulenevalt on IKS § 14 lg 2 alusel kolmandatele isikutele (sh arhiivitoimikus olevate isikuandmete) edastamine või nendele juurdepääsu võimaldamine lubatud andmesubjekti nõusolekuta:

1) kui kolmas isik, kellele andmed edastatakse, töötleb isikuandmeid seaduse, välislepingu või Euroopa Liidu nõukogu või Euroopa Komisjoni otsekohalduva õigusaktiga ettenähtud ülesande täitmiseks;
2) üksikjuhtumil andmesubjekti või muu isiku elu, tervise või vabaduse kaitseks, kui andmesubjektilt ei ole võimalik nõusolekut saada;
3) kui kolmas isik taotleb teavet, mis on saadud või loodud seaduses või selle alusel antud õigusaktides sätestatud avalikke ülesandeid täites (seega süüteomenetluse käigus kogutud teave) ja taotletav teave ei sisalda delikaatseid isikuandmeid ning sellele ei ole muul põhjusel kehtestatud juurdepääsupiirangut.

Arhiveeritud toimikumaterjalide mittetutvustamise otsuse peale kaebamist reguleerib eelkõige AvTS § 46, mis võimaldab pöörduda vaidega AKI poole või teabevaldaja kõrgemalseisva organi poole või kaebusega halduskohtusse. Sarnane võimalus sisaldub IKS §-s 22.[130] Kriminaaltoimikute säilitamistähtaegu autorile teabenõude alusel KAPO ei avalikustanud. KAPO tugines oma vastuses RSVS-st tulenevale KAPO arhiivi juhendile ja dokumentide loetelule kehtestatud juurdepääsupiirangule.[131]

[130] Juhend kriminaal- ja väärteomenetluses kogutud teabe avaldamiseks pärast menetluse lõpetamist. Kättesaadav: https://www.kapo.ee/est/avalik-teave/isikuandmete-kaitse (13.03.2014)
[131] KAPO vastus, magistritöö lisa nr 1

Autori valduses on KAPO vastus eraisiku esitatud küsimusele: "Kas süütuks osutunud isiku kohta ning sealhulgas isiku kohta, kelle suhtes on kriminaalmenetlus lõpetatud, koostatud toimik või selle erinevad osad on avalikult kättesaadavad igale soovijale?"[132]

KAPO tugines oma vastuses eraisikule AvTS §-le 3 lg 1, mille kohaselt on avalik teave mis tahes viisil ja mis tahes teabekandjale jäädvustatud ja dokumenteeritud teave, mis on saadud või loodud seaduses või selle alusel antud õigusaktides sätestatud avalikke ülesandeid täites. Arhiveeritud kriminaalasjade materjalidega tutvumist reguleerib arhiiviseadus koosmõjus AvTS-i ja IKS-ga. KAPO selgitas, et tulenevalt IKS §-dest 14 ja 16 ning arhiiviseaduse §-st 42 on isikuandmete edastamine või kolmandatele isikutele lubatud andmesubjekti nõusolekuta kui kolmas isik taotleb teavet, mis on saadud või loodud seaduses või selle alusel antud õigusaktides sätestatud avalikke ülesandeid täites ja taotletav teave ei sisalda isikuandmeid ning sellele ei ole muul põhjusel kehtestatud juurdepääsupiirangut. Isikuandmete saamise õigus tuleneb IKS § 14 lg-st 2. Nii lubas KAPO kolmandal isikul tutvuda kriminaalasja materjalidega KAPO-s ja talle võimaldati osaline juurdepääs kriminaalasja materjalidele, arvestades seaduses nimetatud juurdepääsupiiranguid.[133] Kusjuures KAPO ütles oma vastuses, et küsitud kriminaalasja toimiku andmetest enamus ei sisalda delikaatseid isikuandmeid. Autori arvates ei tähenda viimati mainitu aga seda, et toimik ei sisalda üldse isikuandmeid ning neid ei peaks üldse juurdepääsupiiranguga kaitsma. Tulenevalt isikuandmete kaitse direktiivist ei tähenda asjaolu, et dokument ei sisalda konkreetselt (delikaatseid) isikuandmeid must-valgelt kirjutatuna, ei tähenda see, et muudest dokumendis sisalduvatest andmetest, kirjeldustest või muust infost ei oleks võimalik isikut tuvastada või neid andmeid tuvastamiseks tuletada. Autor tugineb siin sealjuures *andmekaitse 29. töörühma* seisukohale, mille kohaselt isegi anonüümseks muudetud isikuandmeid on võimalik tuvastada, kui seda võimaldab andmete asumise kontekst. Seetõttu ei pruugi autori arvates osaline juurdepääsu võimaldamine kriminaaltoimikutele tagada andmesubjekti eraelu kaitset piisavas ulatuses ja isikuandmed saavad kolmandatele isikutele olla tuvastatavad.

Kõige suurem vastuolu kirjeldatud KAPO vastuses tuleneb autori arvates aga vastuses viidatud ja eelpool juba mainitud KAPO ja AKI ühiskirjas esitatud põhimõttest, mille kohaselt kolmandatele isikutele võib süüteomenetluses kogutud teavet jagada, kui see teave on loodud või saadud seaduse alusel. Autori arvates eeldab nimetatud punkti kohaldamine, et avalikult jagatav teave peab olema ka kogutud ja säilitatud seaduslikul alusel. See on eeldus, et

[132] Väljavõte KAPO vastusest eraisikule, mis kajastab IKS-i, AvTS-i ja arhiiviseaduse rakendamist. Magistritöö lisa nr 2

[133] Sarnast praktikat kasutab AKI, kohustades uurimisasutusi võimaldama osalist juurdepääsu kriminaaltoimikutele, vt AKI 25.02.2014 vaideotsus eraisik/Politsei- ja Piirivalveamet

haldusorgan saaks üldse teavet jagada. Antud juhul KAPO-l seaduslik alus kriminaalasjas õigeksmõistetud isiku kriminaaltoimiku säilitamiseks puudus. Kuna seaduslik alus kriminaalasjas õigeksmõistetud isiku kriminaaltoimiku säilitamiseks puudub, ei saa KAPO-l olla legitiimset alust kriminaaltoimiku andmete taaskasutamiseks andmiseks kolmandatele isikutele.

3.1.2. Prokuratuurid

Prokuratuurides arhiivihalduse korda eraldi kehtestatud ei ole ja arhiveerimine on asjaajamiskorra üks osa. Asjaajamiskord on kõikidel prokuratuuridel ühtne. Nähtuvalt asjaajamiskorrast registreeritakse kriminaalmenetluse materjalid e-toimikus. Kõikidele kriminaaltoimikutele kehtib juurdepääsupiirang, mille määramisel lähtutakse AvTS-st ja menetlusosaliste andmete kaitset reguleerivates seadustes sätestatust. Kriminaalmenetluse lõpetamisel edastatakse kriminaaltoimik pärast kaebetähtaja möödumist arhiivimiseks kohtueelse menetluse lõpuleviinud uurimisasutusele, välja arvatud juhul, kui uurimist teostas ainuisikuliselt prokuratuur. Sellisel juhul edastatakse kriminaaltoimik Riigiprokuratuuri arhiivi, kus neid säilitatakse menetluse lõpetamisest 25 aastat. Avalikkust huvitavad või eeldatavalt ajaloolist väärtust omavad kriminaalasjad jäetakse alatisele säilitamisele ja antakse üle avalikku arhiivi. Üldmenetluses otsuse jõustumisel arhiivitakse kriminaaltoimik koos eraldatud materjalidega prokuratuuris ja toimikut säilitatakse 10 aastat alates kohtulahendi jõustumisest. Sealjuures vajaduse möödumisel annab ringkonnaprokuratuur toimiku akti alusel edasiseks säilitamiseks või toimikule alatise säilitustähtaja määramiseks üle Riigiprokuratuuri arhiivi. Kriminaaltoimikust võetakse enne hävitamist välja isikut tõendavate dokumentide originaalid, mis säilitatakse prokuratuuri arhiivis 50 aastat või väljastatakse need allkirja vastu dokumendi omanikule. Juurdepääsu prokuratuuri arhiveeritud lõpetatud kriminaaltoimikule otsustab menetlust juhtiv või kõrgemalseisev prokurör. Üle 10-aastase säilitustähtajaga digitaaldokumendid, mis arhiiviväärtust ei oma, võib anda säilitamiseks rahvusarhiivi. Kehtivaid juurdepääsupiiranguid sisaldavaid arhivaale ei laenutata. Kolmandatele isikutele võimaldatakse juurdepääs ainult andmesubjekti kirjalikul nõusolekul. Pärast andmesubjekti surma on tema isikuandmeid sisaldavale arhivaalile juurdepääs andmesubjekti pärijal, abikaasal, lähisusgulasel või nende nõusolekul kolmandal isikul. Nõusolekut ei ole vaja, kui

andmesubjekti surmast on möödunud 30 aastat või arhivaalis sisalduvateks isikuandmeteks on üksnes andmesubjekti nimi, sugu, sünni- ja surmaaeg ning surma fakt.[134]

3.1.3. Politsei- ja piirivalveamet

PPA kodulehelt leiab isikuandmete töötlemise üldpõhimõtted. [135] Nende kohaselt rakendab PPA isikuandmete kaitstuse ja õiguspärase töötlemise tagamiseks organisatsioonilisi, füüsilisi kui infotehnilisi turvameetmeid. PPA teenistujad, kes vastutavad teenistuskohustuste täitmisel isikuandmete töötlemisele kehtestatud põhimõtete järgimise eest, läbivad vastava koolituse ning PPA teostab nendest põhimõtetest kinnipidamise üle järelevalvet. PPA väljastab ja edastab kolmandatele isikutele isikuandmeid, kui vastav kohustus tuleneb seadusest või on selleks olemas andmesubjekti luba. PPA kriminaaltoimikute arhiveerimise juhendi kohaselt antakse toimik üle arhiivi pärast kriminaalmenetluse lõpetamist uurimisasutuses või prokuratuuris ja toimikus peab sisalduma menetluse lõpetamise määrus. Kui pärast 01.01.1991 lõpetatud kriminaalasi puudutas avalikkuse erilist tähelepanu pälvinud sündmust või kriminaalasja menetlemisega kaasnes avalik huvi, siis koostab menetleja asutusesesisese kirja kriminaalasjale arhiiviväärtuse omistamise kohta, kooskõlastab selle vahetu juhi ja vastavalt keskkriminaalpolitsei või kriminaalbüroo juhiga ja märgib pärast kooskõlastuse saamist lõpetatud toimiku kaanele säilitustähtaja järele "AV".[136] Arhiivis asuvate lõpetatud toimikutega on õigus tutvuda ja saada toimikuid ajutiseks kasutamiseks seoses teenistusülesannete täitmisega kirjaliku taotluse alusel, mis on registreeritud dokumendihaldussüsteemis või allkirja vastu politseiasutuse teenistujal või kohtu-, prokuratuuri- ja justiitsministeeriumi teenistujatel. Politseiasutuse teenistujale, prokuratuurile väljastatakse toimik üldjuhul 30 kalendripäevaks ja kohtule 90 kalendripäevaks. Füüsiliste ja juriidiliste isikute taotlused toimiku väljastamiseks edastatakse kriminaalasja menetlenud struktuuriüksusele, toimiku tutvustamiseks annab loa vastava struktuuriüksuse juht. Toimikut tutvustab kriminaalasja menetlenud politseiametnik või struktuuriüksuse juhi poolt määratud teenistuja. Toimikud, välja arvatud märkega "AV", hävitatakse Rahvusarhiivi otsuse alusel vastavalt dokumendihalduskorra nõuetele, hävitamisaktile lisatakse hävitatud kriminaalasjade nimekiri.[137] AKI menetluspraktikas leiab

[134] Väljavõte prokuratuuride asjaajamiskorrast. Magistritöö lisa nr 3
[135] PPA isikuandmete töötlemise üldpõhimõtted. Kättesaadav: https://www.politsei.ee/et/organisatsioon/isikuandmete-tootlemise-uldpohimotted.dot (13.03.2014)
[136] Toimikud märkega "AV" säilitatakse politseiasutuse arhiivihoidlas ja antakse avalikku arhiivi arhiivieeskirjas kehtestatud tähtaegadel ja korras.
[137] PPA, Kriminaaltoimikute arhiveerimise juhend. Magistritöö lisa nr 4

vaideotsuse, milles kohustatakse PPA-d teabenõudjale teavet jagama või toimikut tutvustama osas, milles see ei sisalda juurdepääsupiiranguga teavet.[138] Käesoleva töö autor esitas PPA-le teabepäringu teadasaamaks PPA poolt kriminaaltoimikutele määratud säilitustähtaegu. Pärast mitmekordset kirjavahetust sai autor vastuse, et "kriminaaltoimikute säilitustähtajad on määratud PPA dokumentide loeteluga. Dokumendi säilitustähtaja määramise aluseks asutuse dokumentide loetelus võib olla õigusakt või selle puudumisel praktiline vajadus."[139] Seega ei ole üheselt selge, millised säilitamise tähtajad PPA-s kriminaaltoimikutele määratakse ja kuidas ning millise vajaduse tekkimisel PPA-s säilitamistähtaegu muudetakse.

3.1.4. Uurimisasutustes kehtestatud juurdepääsupiirangute ja säilitamistähtaegade kooskõla kehtiva õigusega

Juurdepääsu piirangud kriminaalmenetluses kogutud andmetele on uurimisasutustes reguleeritud tulenevalt AvTS-ist. Siiski on uurimisasutuste juurdepääsukorrad teatud juhtudel laiendanud kriminaaltoimikutele ligipääsu, näiteks PPA-s pääseb teenistusülesannete täitmiseks kriminaaltoimikule ligi politseiasutuse teenistuja, kohtu-, prokuratuuri- ja justiitsministeeriumi teenistujad. Tulenevalt uurimisasutustes kehtestatud juurdepääsu kordadest saab öelda, et uurimisasutused arvestavad üldiselt AvTS-st tulenevaid juurdepääsupiiranguid. Võrreldes VV määruses nr 261 ja uurimisasutustes kehtestatud arhiivihalduse kordasid jääb silma, et Riigiprokuratuuris säilitatakse kriminaaltoimikuid veel 25 aastat pärast menetluse lõppu, kuigi määruse järgi on säilitamistähtaeg vastavalt kas 10 või 15 aastat ja alaliselt säilitatakse kriminaaltoimikud süüteos inimsuse vastu, sõjasüüteos või süüteos, mille toimepanemise eest on karistusseadustikus ette nähtud eluaegne vangistus. Samuti säilitatakse alaliselt avalikkust huvitavad või eeldatavalt ajaloolist väärtust omavad kriminaalasjad mida võib üle anda avalikku arhiivi. VV määrus nr 261 § 4 lg 10 kohaselt arhiivib prokuratuur kriminaaltoimiku samas paragrahvis kehtestatud tähtaegadel. Seega ei vasta Riigiprokuratuuris kehtestatud säilitustähtajad VV määruses nr 261 § 10 lg 4 nõuetele.

Üldmenetluses otsuse jõustumisel arhiivitakse prokuratuuris kriminaaltoimik 10 aastaks ja ringkonnaprokuratuuril on võimalik pikendada säilitamistähtaega või määrata alatine säilitustähtaeg. Kusjuures ka PPA on jätnud endale võimaluse säilitustähtaja pikendamiseks ja

[138] Andmekaitse Inspektsioon 25.02.2014 vaideotsus Politsei- ja Piirivalveamet/eraisik
[139] PPA vastus. Magistritöö lisa nr 5

tuginedes sealjuures "praktilisele vajadusele". Autor on seisukohal, et prokuratuurides ja PPA-s seesugusel kujul kriminaaltoimikute säilitamise praktika ei vasta VV määruses nr 261 kehtestatud nõuetele ja arvestades EIK lahendit *S and Marper* on olemas potentsiaalne EIÕK artikli 8 lg 2 rikkumine.

Küll peab autor oluliseks, et PPA on väljatoonud oma koduleheküljel teenistujate andmekaitsealase koolitamise vajaduse. Seda eriti tulenevalt esimeses töö osas tehtud järeldusest, et isikuandmete kaitse sõltub oluliselt haldusorgani diskretsiooniotsusest, mis lõpuks saab taanduda ühe ametniku diskretsiooniks. Nii saab inimene (ametnik) olla nõrgim lüli isikuandmete kaitse tagamise süsteemis. Paraku on kohtupraktika põhjal PPA-l uurimisasutustest enim kogemust ametnike poolt isikuandmete väärkasutamise kohta.

3.2. Riigikohtu lahendid 3-1-1-25-12 ja 3-1-1-81-08

Ilmselt kõige tuntum PPA kaasus isikuandmete kaitse nõuete rikkumisest on juhtum, kui Põhja Politseiprefektuuri analüüsi- ja planeerimisbüroo komissar A. Järvet edastas kolmandate isikute isikuandmeid oma elukaaslasele. A. Järvet edastas isikuandmeid kriminaalpolitsei infosüsteemist KAIRI, mille pidamise ja kasutamise kohta on politseiameti peadirektor kehtestanud eraldi korra. Kuna kord ei ole seadus, siis möönis Riigikohus oma lahendis 3-1-1-25-12, et kuigi politseiameti peadirektori pädevusse võib kuuluda haldusorgani siseselt teabesüsteemide ja andmekogude pidamise korda puudutavate küsimuste lahendamine ning selleks käskkirjade andmine, siis ei ole nende õigusaktide rikkumine aluseks isikute kriminaalvastutusele võtmiseks KarS § 157 alusel. Nii on Riigikohtu kriminaalkolleegiumi praktika kohaselt süüditunnistamist konkretiseerimata süüdistuses loetud kaitseõiguse eiramiseks ja kriminaalmenetlusõiguse oluliseks rikkumiseks KrMS § 339 lg 2 tähenduses, sest isik peab aru saama, milles teda süüdistatakse ning kohaldatava õigusakti säte ei tohi olla tema jaoks üllatuslik.[140]

A. Järveti kaasusega sarnases kriminaalasjas edastas Põhja Politseiprefektuuri kriminaalosakonna varavastaste kuritegude politseivaneminspektor J. Prii kolmandate isikute isikuandmeid teabenõudjale R. Pentile infosüsteemist KAIRI. Riigikohus jõudis oma otsuses 3-1-1-81-08 järeldusele, et KarS § 157 rakendamine on õigustatud, sest J. Priile said

[140] RKKKo 3-1-1-25-12, punktid 10 ja 11

isikuandmed teatavaks tema ametitegevuses. Karistusõigusliku vastutuse eelduseks on, et eraelu puudutav teave on saanud teatavaks just ameti- või kutsetegevuses ja ilma vastavat ametiseisundit omamata ning kasutamata poleks teave olnud kättesaadav.[141] Ka selles kaasuses oli vastutusele võtmise aluseks politseiameti peadirektori poolt kehtestatud infosüsteemi KAIRI pidamise ja kasutamise kord, ent süüdistuses oli lisaks sellele ära nädatud ka politseiseaduse §-st 5 lg-st 2 tulenev alus, mille kohaselt avalikustamisele ei kuulu eraelu puudutavad andmed ja sama paragrahvi lg 4 kohaselt on politseiametnikel keelatud andmete esitamine teiste isikute kohta.

Seega on Riigikohus teinud sisult sarnaste rikkumiste pinnalt kaks erinevat otsust. Nii A. Järvet kui ka J. Prii olid ametiisikud, kes edastasid infosüsteemist KAIRI kolmandatele isikutele isikuandmeid ja teave sai neile teatavaks nende ametitegevuses. Kui J. Prii kaasuses leidis Riigikohus, et KarS § 157 rakendamise koosseis on täidetud, siis A. Järveti kaasuses ei pidanud Riigikohus seda põhjendatuks, kuna kohtulikul arutamisel oli jäänud välja selgitamata, millise seaduse nõudeid süüdistatav lisaks infosüsteemi KAIRI pidamise ja kasutamise korrale rikkus ning millest KarS §-s 157 sätestatud kuriteokoosseisu mõttes tulenes tema kohustus süüdistuses kirjeldatud teavet saladuses hoida.[142] EIÕK artikkel 13 kohaselt on igaühel, kelle konventsioonis sätestatud õigusi ja vabadusi on rikutud, õigus tõhusale menetlusele ka siis, kui rikkumise pani toime ametiisik.[143] Riigikohtu praktikast tulenevalt teeb autor siinkohal järelduse, et isikuandmete kaitse seisukohalt on oluline, et kohustus ja vastutus infosüsteemides ja andmebaasides olevate andmete kaitse tagamise eest peab tulenema igal juhul seadusest ja mitte haldusorgani kehtestatud korrast. Seda põhjusel, et vaid nii on tagatud KarS § 157 rakendamine ametiisikute vastutusele võtmiseks kolmandatele isikutele isikuandmete edastamise eest. Seaduses sätestatud konkreetne kohustus on vajalik meede isikuandmete ja eraelu kaitseks.

3.3. Euroopa Ühenduste Komisjoni ettepanek nr KOM(2005) 475

Euroopa Ühenduste Komisjon on vastu võtnud raamotsuse politsei- ja õigusalase koostöö raames töödeldavate isikuandmete kaitse kohta.[144] Raamotsuse eesmärgiks oli Euroopa Liidu

[141] RKKKo 3-1-1-81-08, punkt 14.2
[142] RKKKo 3-1-1-25-12, p 10.4
[143] RKÜKo 3-3-1-85-09, p 73
[144] Euroopa Ühenduste Komisjoni ettepanek nr KOM (2005) 475 kriminaalasjadega seotud politsei- ja õigusalase koostöö raames töödeldavate isikuandmete kaitse kohta.

liikmesriikide vahel kriminaalasjadega seotud politsei- ja õigusalase koostöö käigus töödeldavate isikuandmete kaitse efektiivsem tagamine, samal ajal tõhustades terrorismi vastu võitlemise alast koostööd. Raamotsus viitab korduvalt isikuandmete kaitse direktiivile 95/46/EÜ ja seal kehtestatud seaduslikkuse ja eesmärgipärase andmetöötluse rakendamise olulisusele. Lisaks näevad liikmesriigid raamotsuse alusel ette, et isikuandmeid töödeldakse ainult siis, kui tuvastatud asjaolude põhjal on põhjust arvata, et asjaomased andmed võimaldaksid, lihtsustaksid või kiirendaksid kuriteo ennetamist, uurimist, avastamist ja kuriteo eest vastutusele võtmist, puuduvad muud andmesubjekti vähem mõjutavad meetmed ja andmete töötlemine ei ole ulatuslikum, kui kuriteo uurimiseks vaja.[145] Liikmesriikidel tuleb selgelt eristada isik, kes on kuriteos süüdi mõistetud.[146] Raamotsuse artikli 5 kohaselt peavad liikmesriigid ette nägema, et pädevad asutused tohivad isikuandmeid töödelda ainult siis, kui seadusega on ette nähtud, et selline töötlemine on vajalik asjaomase ametiasutuse õiguspäraste ülesannete täitmiseks ja kuritegude ennetamiseks, avastamiseks ja kuritegude eest vastutusele võtmiseks. Seega on raamotsus läinud isikuandmete kaitse direktiivist täpsemaks ning reguleerib konkreetsemalt kriminaalmenetlustes kogutud isikuandmete kaitset ja nende andmete töötlemist. Sealjuures lubab raamotsus isikuandmete töötlemise, kui see on vajalik kuritegude ennetamiseks.

3.4. Kohtutoimikule ligipääsu regulatsioon KRMS-s

Vastavalt VV määrusele nr 261 arhiivitakse kriminaaltoimikud pärast kriminaalmenetluse lõpetamist kohtuistungil maakohtu arhiivihalduse korra kohaselt.[147] Tulenevalt autori poolt esitatud teabepäringutele Eesti maakohtutele eraldi arhiivihalduse korda maakohtutel olemas ei ole. Kohtu arhiiv juhindub oma töös arhiiviseadusest ning arhiivieeskirjast ja maa-haldus- ja ringkonnakohtu kantselei kodukorrast, mis on kehtestatud justiitsministri 22.12.2005 aasta määrusega nr 57. Viimati nimetatus on muuhulgas sätestatud toimikute väljaandmise kord ja säilitamistähtajad. Nii otsustavad kohtutoimikutele ligipääsu protsessis mitteosalenud isikutele kohtu esimees või kohtumaja juht.[148] Kodukorra kohaselt määratakse säilitustähtajad vastavalt kas 3, 5, 10 või 15 aastat ning eriti rasked kuriteod nagu süüteod Eesti Vabariigi vastu, terrorismis ja mõrvas säilitatakse alaliselt. Seega vastavad kohtutoimikutele kohtute poolt

[145] *Ibid*, artikkel 4 lg 1 punkt e
[146] *Ibid*, artikkel 4 lg 3
[147] VV määrus nr 261, § 5
[148] Justiitsministri 22.12.2005 aasta määrus nr 57 "Maa-, haldus- ja ringkonnakohtu kantselei kodukord." Lisa 5

määratavad säilitustähtajad osaliselt VV määrusele nr 261. Erinevalt VV määrusest nr 261 on kohtute kodukorras ette nähtud võimalus säilitada mõnede kuritegude puhul, nagu näiteks süüteod alaealise või omandi vastu kriminaaltoimikuid 3 aastat. Kui VV määrus nr 261 kehtestas toimikute säilitamistähtajad vastavalt kriminaalmenetluse lõpetamise alusele, siis justiitsministri määrus nr 57 kehtestab kriminaaltoimikute säilitamistähtajad sõltuvalt kuriteo raskusest. Seega arvestab kohtute kodukord enam alaealiste õigustega ja hindab proportsionaalsemalt andmete säilitamise vajalikkust, kui seda teeb VV määrus nr 261 ja uurimisasutustes kehtestatud korrad. Siiski arhiivib ka maakohus õigeksmõistva kohtuotsuse ja lõpetatud kriminaalasjade toimikud ilma seadusliku aluseta ning olemas on EIÕK artikli 8 lg 2 riive võimalus.

Vastavalt AvTS § 28 lg 1 p 29 on kohus teabevaldajana kohustatud avalikustama jõustunud kohtulahendid seadusest tulenevate piirangutega. Kohtuotsus jõustub, kui selle edasikaebamise tähtaeg on möödunud või kui seda ei saa enam vaidlustada muul viisil kui teistmismenetluses.[149] Järgnevalt peatub autor AKI 29.01.2010 aastal tehtud vaideotsusel[150], milles AKI kohustab Tartu Ringkonnakohut väljastama menetlusvälisele isikule kriminaalasjas tehtud kohtulahendi enne selle jõustumist.[151] Antud asjas oli Tartu Ringkonnakohus keeldunud isikule kohtulahendit väljastamast, tuginedes AvTS §-le 28 lg 1 p-le 29 ja KrMS § 408’ lg-le 1, mille kohaselt avalikustatakse jõustunud kohtuotsus selleks ettenähtud kohas arvutivõrgus, välja arvatud juhul, kui kriminaalasjas, milles kohtumäärus tehti jätkub kohtueelne menetlus ja KrMS §-le 317 lg 1, mille kohaselt võib pärast kohtuotsuse kuulutamist või teatavaks tegemist sellega tutvuda kohtus ja kohtumenetluse poole soovil antakse talle kohtuotsuse koopia. Tartu Ringkonnakohus leidis, et ükski seadus ei sätesta jõustumata kohtulahendite avalikkust isikute osas, kes ei ole kohtumenetluse pooled. Samuti oli kriminaalasjas esitatud kassatsioon. AKI leidis aga enda vaideotsuses, et piirata ei tohi kohtuotsuse kättesaadavust, kui selles on nimed asendatud tähtedega ja sellisel juhul on tegemist üldiseks kasutamiseks levitatava informatsiooniga PS § 44 lg 1 tähenduses. Lisaks tõi AKI välja, et KrMS ei ole AvTS-i suhtes jõustumata kohtuotsustele juurdepääsu osas tervikuna eriseaduseks ja nii tuleb päringuid, millega taotletakse juurdepääsu kohtuotsustele, sealhulgas ka jõustumata kohtuotsustele menetleda AvTS-s sätestatud korra kohaselt. Juurdepääsupiirangu aluseks ei saa olla AvTS § 28 lg 1 p 29 ning KrMS § 408’ lg 1, mis paneb teabevaldajale kohustuse avalikustada jõustunud

[149] KrMS § 408’ lg 1
[150] AKI 29.01.2010 vaideotsus eraisik/Tartu Ringkonnakohus. Magistritöö lisa nr 7
[151] AKI praktika eri kohtumenetlustes kohtutoimiku ja kohtuotsuse väljastamise kohta ei ole ühtne, sest erinevalt KrMS-st on näiteks halduskohtumenetluse seadustikus (HKMS) sätestatud kohtuotsuse avaldamise erikord HKMS §-s 175 ja §-s 89 sätestatud tingimustel. Vt 27.12.2013 vaideotsus AS PR Põhjarannik/Tallinna Halduskohus

kohtuotsused oma võrgulehel. KrMS § 317 lg 1 sätestab aga kohtumenetluse poolte õigused, mitte kolmandate isikute õigused. Seega, kui eriseadus ei sätesta kolmandate isikute õigusi, tuleb AKI seisukoha järgi lähtuda AvTS-st. AKI viitas vaideotsuses sealhulgas kohtute haldamise nõukoja seisukohale, mille järgi jõustumata lahendid on kõigile kättesaadavad avaliku teabe seaduses ettenähtud teabenõude korras.[152] Autori tähelepanu köitis AKI vaideotsuses esitatud seisukoht, et kui kohtuotsus kuulutatakse välja avalikult ja ilma piiranguteta, siis loob see justkui eelduse, et ka muudel isikutel on juurdepääsuõigus kohtuotsusele. Autor ei nõustu AKI seisukohaga, sest kohtuotsuse avalikul kuulutamisel ei loeta alati kohtuniku poolt ette kogu kohtuotsust tervikuna vaid resolutiivosa. Seda seisukohta toetab ka KrMS § 315 lg 4, mille kohaselt võib kohus kuulutada üksnes kohtuotsuse resolutiivosa, selgitades selle kuulutamisel suuliselt kohtuotsuse olulisemaid põhjendusi. Resolutiivosa kuulutamine on üks kohtuotsuse kuulutamise viisidest.[153] Seega kohtuotsuse avalik kuulutamine ei ole võrdsustatav kohtuotsuse edastamisega kolmandatele isikutele, sest avalikul kohtuotsuse kuulutamisel ei avalikustata alati kogu asjas otsuse tegemise aluseks olnud teavet.

Seega on antud vaideotsuses AKI lubanud ja Tartu Ringkonnakohut kohustanud kohtuotsust väljastama kolmandatele isikutele juhul, mil kohtuotsuse edasikaebamise tähtaeg ei ole möödunud ja kohtuotsus ei ole veel jõustunud. Autori arvates peitub siin oht, et jõustumata kohtulahendite väljastamine kolmandatele isikutele riivab süütuse presumptsiooni põhimõtet.[154] Seda näiteks olukorras, kus maakohus on teinud küll esimeses astmes isiku kohta süüdimõistva kohtuotsuse, kuid isik soovib otsust edasi kaevata ja pole välistatud, et ringkonnakohus mõistab isiku kriminaalasjas õigeks. AKI vaideotsusest nähtuvalt on kolmandatel isikutel aga õigus saada see mittejõustunud maakohtu otsus enda valdusesse. Sisuliselt saab nii kolmandatele isikutele võimalikuks anda oma hinnang isiku mainele ja seda enne kohtuotsuse kehtima hakkamist. Autori arvates rikub seetõttu jõustumata kohtulahendite väljastamine kohtualuse põhiõigust privaatsusele ja ennekõike saab kahjustada isiku mainet. EIÕK artikkel 6 lg 2 järgi on isik süütu seni, kuni seaduse kohaselt ei ole süü tõendatud. Süü leiab aga tõendamist jõustunud kohtuotsusega.

[152] Kohtute haldamise nõukoda. Õigusemõistmise avalikkus versus isiku õigus eraelu puutumatusele. Kättesaadav: http://www.riigikohus.ee/?id=329 (20.03.2014)
[153] Kergandberg, E. jt. (koost). Kriminaalmenetluse seadustik. Kommenteeritud väljaanne. Tallinn: Juura 2012, lk 723
[154] Autor on seisukohal, et sellise konkreetse teabenõude esitamisega kohtule teabe saamiseks saab eeldada ka, et kolmas isik teab või on juba tuvastanud andmesubjekti. Lisaks ei saa välistada, et võimalik on andmesubjekti tuvastada anonüümseks muudetud kohtuotsusest. Vt sellest lähemalt: Hansen, T. Õigus eraelu puutumatusele vs. kohtulahendi avalikustamine. Magistritöö. Juhendajad Ernits, M. Aaviksoo, B. Tartu Ülikool, õigusteaduskond, riigi- ja haldusõiguse õppetool. 2012

Siinkohal on autori arvates taas asjakohane seisukoht, et menetluslik korrektsus ja õiglus ei ole mitte üksnes tõhusa halduse kõrvalprodukt, vaid eesmärk omaette.[155] Autor on seisukohal, et isiku privaatsusõiguse tagamiseks kriminaalmenetluses tehtavad toimingud peaks tagama, et isikuga ei saaks seostada veel mitte kehtivat informatsiooni. Kohtumenetluses on õiglus ja menetluslik korrektsus üheks peamiseks eesmärgiks ja autori arvates ei ole õiglane enne lõplikku ja jõustunud kohtuotsust väljastada kolmandatele isikutele kriminaalmenetluses tehtud kohtulahendeid, mis otseselt saavad kahjustada kohtualuste isikute mainet.[156] Veelgi enam, kui vaadata maa-, haldus- ja ringkonnakohtu kantselei kodukorda, siis vastavalt selle §-le 69 antakse toimikuid ja muid dokumente tutvumiseks kolmandatele isikutele pärast kohtuotsuse jõustumist kohtumenetluse seaduses ja menetlusosaliste andmete kaitset reguleerivates seadustes sätestatud korras ja vastavalt §-le 72 avalikustatakse jõustunud lahend menetlusseadustes sätestatu kohaselt. Autori arvates toetab seda ka KrMS § 315 lg 5 p 1, mille kohaselt teatab kohus kohtuotsuse resolutiivosa kuulutades päeva, millal kohtuotsus on kohtumenetluse pooltele kohtus tutvumiseks kättesaadav.[157] Ehk KrMS reguleerib vaid olukorda, milles lubatakse kohtuotsusega tutvuda menetlusosalistel ja mitte kolmandatel isikutel. Seega on kohtuotsuse avalikustamise tingimused ette nähtud eelkõige menetlusseaduses ja mitte AvTS-s. Seega KrMS kohaselt ja mitte AvTS-i eriseadusena rakendades.

Sarnaselt PPA-le tehtud vaideotsusele on AKI kohustanud oma vaideotsusega ka Pärnu maakohut tutvustama kolmandale isikule kohtutoimikut osas, milles see ei sisalda juurdepääsupiiranguga teavet.[158] Nimelt oma esialgse otsusega Pärnu maakohus keeldus toimikut tutvustamast kolmandatele isikutele, põhjendades seda asjaoluga, et toimik sisaldab delikaatseid isikuandmeid kolmandate isikute kohta. Erinevalt PPA-le tehtud vaideotsusest lubab antud vaideotsus Pärnu maakohtul keelduda teabenõudjale ka osalist tutvumist toimiku materjalidega. Seda tingimusel, et Pärnu maakohus põhjendab oma vastavat otsust arusaadavalt teabenõudjale. Paraku vaideotsus ei ütle otsesõnu ja ka kaude jääb arusaamatuks, miks Pärnu maakohtul on õigus keelduda osalisest toimikuga tutvumiseks andmisest, kuid PPA-l selline õigus puudub.

[155] Lord Millett. The Right to Good Administration in European Law. public law, Sweet & Maxwell 2002 summer, p 312
[156] Trechsel, S. Human Rights In Criminal Proceedings. Oxford: Oxford University Press 2007, lk 164
[157] Kergandber, E. jt. (koost). Kriminaalmenetluse seadustik. Kommenteeritud väljaanne. Lk 727
[158] AKI 04.03.2011 vaideotsus eraisik/Pärnu maakohus. Magistritöö lisa nr 8

3.5. E-toimik

E-toimiku menetlemise infosüsteem on kriminaalmenetluses menetlusandmete ja isikuandmete töötlemiseks peetav riigi infosüsteemi kuuluv andmekogu.[159] KrMS § 210 lg 1 punktides 1-5 on sõnastatud e-toimiku eesmärgid, mis on:

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

Sama paragrahvi lõikest 2 nähtub, et andmekogusse kantakse andmed menetluses olevate, alustamata jäetud ja lõpetatud kriminaalasjade kohta. Seega on e-toimikus kajastatud lisaks alustamata jäetud ja lõpetatud kriminaalasjad, kusjuures ei ole täpsustatud, kas andmekogus säilitatakse näiteks kriminaalasjas õigeksmõistetud isikute andmeid. Seetõttu tuleks seda pigem jaatada, kuna puudub täpsem regulatsioon ja neid kriminaalasju saab pidada lõpetatud kriminaalasjade hulka kuuluvateks.

Lisaks kantakse andmekogusse andmed kriminaalmenetluse käigus tehtud toimingute kohta, KrMS-s sätestatud juhtudel digitaalsed dokumendid (sealhulgas filmi, heli ja videosalvestised) ja andmed menetleja, menetlusosalise, süüdimõistetu, eksperdi, asjatundja ning tunnistaja kohta ja kohtulahend. KrMS § 16 lg 1 kohaselt on kriminaalasja menetlejaks kohus, prokuratuur ja uurimisasutus. Menetlusosalisteks on sama paragrahvi lg 2 kohaselt kahtlustatav, süüdistatav ning nende kaitsjad, kannatanu, tsiviilkostja ja kolmas isik. Järelikult talletatakse e-toimikus kõik kriminaalasjad, sealhulgas alustamata jäetud ja lõpetatud kriminaalasjad ning kogu info menetlusosaliste kohta. Autori teabepäringule Registrite- ja Infosüsteemide Keskusele küsimusega, milliste tähtaegadega ja mille alusel kriminaalmenetluse materjale e-toimikus säilitatakse, sai autor vastuseks, et "andmeid säilitatakse igavesti."[160] Autor on seisukohal, et sellisel kujul andmekogu pidamine ei ole õiguspärane. Lähtuvalt eelviidatud EIK lahendist *S and Marper* ei ole EIÕK artikliga 8 kooskõlas, kui säilitatakse isikuandmeid kriminaalasjas, kus isik mõisteti õigeks või menetlus lõpetati. EIK leidis selles lahendis, et siseriiklik õigus peab tagama piisavad ja sobivad garantiid, et säilitatud isikuandmed on efektiivselt kaitstud

[159] KrMS § 210 lg 1
[160] Registrite- ja Infosüsteemide keskuse vastus. Magistritöö lisa 6

nende väär- ja kuritarvituse eest. Eriti oluliseks pidas kohus seda andmete puhul, mis on seotud DNA ja teiste isiku geneetiliste andmetega, mille põhjalt saab tuletada isiku põlvnemist. Kohus võtab sellised andmed kokku mõistega kui "eriti privaatse iseloomuga andmed" (*the intrinsically private character of this information*), mistõttu kohus uuris selliste andmete kasutamist ja säilitamist antud kriminaalmenetluses eriti hoolikalt, ja arvestades, et isiku nõusolek tema andmete töötlemiseks puudub.[161] Nagu selgus on e-toimikus need andmed talletatud lõpmatuseni. Kuigi õigeksmõistva kohtuotsuse resolutsioonis esitatakse riiklikus sõrmejälgede registris ja riiklikus DNA-registris sisalduvate andmete kustutamine[162], ei ole reguleeritud andmete kustutamine e-toimikust. Lisaks ei ole reguleeritud nende andmete kustutamine olukorras, kus isiku kohta on need andmed küll kogutud, ent menetlus on lõpetatud ilma õigeksmõistva kohtuotsuseta. Kuna e-toimiku infosüsteemis talletatakse eranditult kõik kriminaalasjad tähtajatult ja ilma seadusliku aluseta, on tõenäoliselt tegemist EIÕK artikli 8 lg 2 rikkumisega. E-toimiku infosüsteem rikub potentsiaalselt kõikide infosüsteemis menetlusosalistena kajastatud andmesubjektide isikuõigusi, sest nende andmete säilitamine toimub seadusliku aluseta.

Tuleb arvestada, et e-toimiku andmekogus on salvestatud ka kolmandate isikute ja kannatanu isikuandmed. Eriti tuleks autori arvates tähelepanu pöörata siinkohal kannatanu isikuõiguste kaitsele, sest faktoloogia, mida kannatanu kohta kriminaalasjas alles hoitakse võib sisaldada vägagi delikaatseid ja isiku privaatsuse kaitset silmas pidades olulist teavet. Nii tuleks autori arvates kustutada lisaks kriminaalasjas õigeksmõistetule kolmandate isikute isikuandmed, kui kriminaalasjas on jäänud süüdistatava süü tõendamata või menetlus lõpetatud. Praegu seesugune regulatsioon Eesti seadusandluses puudub. Autor nõustub, et õigustatud on kannatanu andmete säilitamine teatud aja jooksul, kui süüdistatava süü on leidnud tõendamist, ent kas on õigustatud hoida alles kannatanu andmeid, kui kriminaalasi näiteks lõpetatakse või isik mõistetakse piisavate tõendite puudumise tõttu õigeks? Autor peab sellise tegevuse õigsust kaheldavaks, sest kui juba kriminaalasjas õigeks mõistetud isiku või muul põhjusel menetluse lõpetamise puhul kahtlustatava andmete seadusliku aluseta säilitamine läheb vastuollu EIÕK artikliga 8 lg 2, siis võiks öelda, et kannatanu võib nii mõnelgi juhul olla veelgi nõrgemal positsioonil ja tema isikuõiguste riive vähemalt sama suur.

[161] EIKo 10.12.2008, 30562/04 and 30566/04, S and Marper vs United Kingdom, §-d 103-104
[162] KrMS § 314 lg 5^1

Nagu selgus, sisaldab e-toimik andmekoguna olulisel hulgal kriminaalmenetluses kogutud isikuandmeid. See viib käesoleva töö autori järgmise küsimuseni: kellel ja mille alusel on ligipääs e-toimikus olevatele isikuandmetele? Ligipääsu e-toimikule reguleerib VV 03.07.2008 aasta määrus nr 111 "E-toimiku süsteemi asutamine ja e-toimiku süsteemi pidamise põhimäärus" (edaspidi e-toimiku põhimäärus). Vastavalt e-toimiku põhimääruse §-le 3 esitavad e-toimiku süsteemi andmeid väärtegude kohtuvälised menetlejad, uurimisasutus, prokuratuur, kohus, menetlusosalised ja teised menetluses osalevad isikud. E-toimiku vastutavaks töötlejaks on justiitsministeerium.[163] Volitatud töötlejateks on kohtud, prokuratuur, politseiasutused, KrMS §-s 31 nimetatud uurimisasutused[164], väärteomenetluse seadustiku §-s 9 nimetaud kohtuvälised menetlejad[165] ja julgeolekuasutused. Lisaks põhimääruses sätestatule on KrMS-st tulenevalt volitatud töötleja justiitsministeeriumi poolt määratud isik.[166] Seega on justiitsministeeriumil õigus määrata volitatud töötlejaks veel muid isikuid. Vastutav töötleja võimaldab volitatud töötlejale juurdepääsu e-toimiku süsteemi andmetele ja juurdepääsu ulatus ning piirangud on sätestatud e-toimiku põhimääruse §-des 16-18[1].[167] E-toimiku süsteemis kannete ja päringute tegemise õigus on volitatud töötlejal üksnes tema seadusest ja teistest õigusaktidest tulenevate ülesannete täitmiseks.[168] E-toimiku avaliku liidese kasutajatel on e-toimiku süsteemi kannete ja päringute tegemise õigus seaduses lubatud juhtudel ja mahus.[169] Vastutaval töötlejal on õigus kontrollida kannete ja päringute vastavust seadusele. Väärkasutuse avastamine võib olla aluseks e-toimiku süsteemi kasutusõiguse piiramiseks, peatamiseks või lõpetamiseks. Andmed e-toimiku süsteemis saavad olla kas avalikud, piiratud juurdepääsuga või salastatud.[170] Salastatuse astme määrab andmeid sisestav volitatud töötleja, lähtudes seadusest ja andmete iseloomust. Autor on seisukohal, et salastatuse astme määramisel peab arvestama isikuandmete kaitse direktiivis toodud isikuandmete mõiste laia tõlgendusega ja andmete iseloomu hindamine peab tagama, et nende andmete põhjal ei ole võimalik isikut tuvastada.

[163] VV määrus nr 111, § 4 lg 1
[164] Uurimisasutused oma pädevuse piires on Politsei- ja Piirivalveamet, Kaitsepolitseiamet, Maksu- ja Tolliamet, Konkurentsiamet, Sõjaväepolitsei, Keskkonnainspektsioon ning Justiitsministeeriumi vanglate osakond ja vangla, kes täidavad uurimisasutuse ülesandeid vahetult või nende hallatavate või kohalike asutuste kaudu.
[165] Kohtuväline menetleja on seadusega sätestatud juhul:
1) täidesaatva riigivõimu volitustega asutus;
2) valla- ja linnavalitsus.
[166] KrMS § 210 lg 4 teine lause
[167] VV määrus nr 111, § 15
[168] *Ibid*. § 15 lg 3
[169] *Ibid.* lg 4
[170] *Ibid.* § 16 lg 1

Avalikel andmetel puuduvad juurdepääsupiirangud ja neid näevad kõik volitatud töötlejad.[171] Seega peab volitatud töötleja oskama hinnata, kas teabele kehtivad juurdepääsupiirangud ja eelkõige, kas tegemist on isikuandmetega või mitte. Kuid nagu selgus käesoleva magistritöö esimeses osas, siis ei ole isikuandmete tuvastamine lihtne ülesanne. Piiratud juurdepääsuga andmetel on e-toimikus osaline juurdepääsupiirang. Piiratud juurdepääsuga andmeid näeb piisavate õiguste ja olemasolu korral see volitatud töötleja, kes asja menetleb või kes on asja menetlenud. Muud volitatud töötlejad näevad piisavate õiguste olemasolu korral järgmisi piiratud juurdepääsuga andmeid:

1) kriminaalmenetluses VV määruse nr 111 §-s 17 lg 2 loetletud andmed (kriminaalasja number, kriminaalmenetluse number ehk kohtuasja number, kriminaalasja alustamise kuupäev, kriminaalasja menetlev asutus, kriminaalasja aktiivselt menetlev isik, kriminaalasja staadium, kriminaalasja seis, kahtlustatava või süüdistatava teo kvalifikatsioon, kahtlustatava või süüdistatava nimi).
2) väärteomenetluses VV määrus nr 111 §-s 18 lg 2 loetletud andmeid (menetlusalune isik, kelle karistamise kohta on jõustunud kohtuvälise menetleja otsus või kohtuotsus, on süüdlane)

E-toimiku süsteemi avaliku liidese kaudu näeb piiratud juurdepääsuga andmeid üksnes see isik, kelle kohta need andmed on kogutud, kui nende andmete vaatamiseks ei ole seatud talle piirangut. [172] Salastatud andmetele on täiendavad juurdepääsupiirangud, millest tulenevalt näevad neid vaid e-toimiku põhimääruse §-des 17-18[1] nimetatud isikud.[173]
Nii näevad e-toimikus kriminaalmenetluses salastatud andmeid:

1) aktiivne menetleja, sealhulgas kohtute infosüsteemis menetlusgrupi liige, kes menetleb kriminaalasja, milles need andmed asuvad;
2) uurimisasutuses viimasena kriminaalasja menetlenud ametnik ehk menetlejast uurija, kui salastatud, kui salastatud kriminaalasi on prokuratuuris;
3) nendele andmetele juurdepääsu saanud kasutaja vahetu ülemus ja vahetu ülemuse ülemus tulenevalt põhisüsteemi kasutusõiguste hierarhiast;
4) selle põhisüsteemi haldurid ja administraatorid, kus salastatud kriminaalasi asub, välja arvatud kohtute infosüsteemi haldurid ja administraatorid;
5) kohtute infosüsteemis selle kohtu esimees ja kantseleijuhataja, kus kriminaalasja menetletakse;

[171] *Ibid.* § 16 lg 3
[172] *Ibid.* § 18 lg 4[1]
[173] *Ibid.* § 18 lg 5

6) põhisüsteemi poolt määratud aktiivsed vaatlejad konkreetses kriminaalasjas;
7) järelevalve õigustega isikud, kes näevad andmeid oma põhisüsteemi kaudu.

Järelikult on väga paljudel isikutel ligipääs kriminaalmenetluses kogutud ja salastatud andmetele. Juhul kui täiendav juurdepääsupiirang on tervel kriminaalasjal, siis on eelnevalt nimetamata kasutajatele nähtavad ainult järgmised põhiandmed:

1) kriminaalasja number
2) kriminaalmenetluse number ehk kohtuasja number;
3) kriminaalasja alustamise kuupäev;
4) kriminaalasja menetlev asutus;
5) kriminaalasja aktiivselt menetlev isik;
6) kriminaalasja staadium;
7) kriminaalasja seis;
8) kahtlustatava või süüdistatava teo kvalifikatsioon;
9) kahtlustatava või süüdistatava nimi.

E-toimik on infoallikas, mille põhjal iga aasta 1. märtsiks avaldab justiitsministeerium aruande eelmise aasta kuritegevuse kohta ja avaldab kuritegevuse statistikat.[174] Justiitsministeerium võib õigusaktides ettenähtud juhtudel väljastada e-toimiku süsteemi andmeid statistilistel eesmärkidel kasutamiseks. Andmed väljastatakse kujul, mis ei võimalda isikuid identifitseerida.[175]

KrMS § 210 lg 8 kohaselt kehtestab kriminaalstatistika avaldamise korra Vabariigi Valitsus. VV 25.09.2008 aasta määrus nr 145 "Kriminaalstatistika avaldamise kord" § 2 kohaselt on kriminaalstatistika liigid kuritegevuse statistika: kuritegude ja kuritegudega seotud isikute andmed; menetlusstatistika: menetlustoimingute, lõplike menetlusotsuste, kriminaalasjade ja kriminaalmenetluse kestuse andmed; sanktsioonide statistika: karistuste, kohustuste, mõjutusvahendite, menetluse tagamise vahendite, menetluse käigus kohaldatud arestide ja trahvide andmed; karistuse täitmise statistika: kriminaalhoolduse, vangistuse ja täitemenetluse andmed. Sama määruse § 1 avab määruses kasutatavate mõistete sisu ja selle kohaselt on kriminaalstatistika kriminaalmenetluse käigus ja tulemusena e-toimiku menetlemise infosüsteemi koondatud ja töödeldud andmete kogum. Lõplikult lahendatud kuritegu on jõustunud süüdimõistva kohtulahendiga kuritegu ja kuritegu, mille menetlemine on KrMS §-de 201-205 alusel lõpetatud.

[174] KrMS § 210 lg 6, lg 7
[175] VV määrus nr 111, § 19

3.6. Delikaatsed isikuandmed kriminaalmenetluses

Isikuandmed on kriminaalmenetluses delikaatsed enne avalikku kohtuistungit, õigusrikkumise asjas otsuse langetamist või asja menetluse lõpetamist.[176] Samas nende andmete sisu ei muutu õigeksmõistva otsuse või asjas menetluse lõpetamise puhul. Seetõttu peab autor küsitavaks, miks need andmed väljuvad delikaatsete isikuandmete kaitsealast? Autor on seisukohal, et pärast õigeksmõistvat kohtuotsust või kriminaalasjas menetluse lõpetamist peaksid asjaga seotud andmed endiselt olema kaitstud IKS-s ja AvTS-s kehtestatud delikaatsetele isikuandmetele kehtestatud juurdepääsupiiranguga. Kuigi õigeksmõistvad kohtuotsused avalikustatakse umbisikuliselt, kahtleb autor, kas kohtuotsust või kohtutoimikut on üldse võimalik muuta umbisikuliseks. Autor tugineb siin magistritöö esimeses osas tehtud järeldusele, mille kohaselt umbisikustamine ei täida oma eesmärki, kui andmete asumise kontekst ei võimalda tagada isiku anonüümsust ja isik on endiselt tuvastatav. Saksa Liidukonstitutsioonikohus on mõistet "eraelu" defineerinud kui "isikliku elu kujundamise kitsam sfäär". See kitsam sfäär hõlmab individuaalse tagasitõmbumise sfääri, kus isik saab olla üksi. *Right to be let alone*, nagu see on tuntud Ameerika diskussioonist.[177] Autor on seisukohal, et kohtuotsuste ja kohtutoimikute umbisikustamine ei pruugi piisavalt tagada isiku privaatsfääri kaitset, sest kui isikustamata andmeid on võimalik tulenevalt kontekstist seostada konkreetse isikuga või kaudselt tuvastada, siis rikutakse isiku õigust olla üksi. Seetõttu peab autor õiguspäraselt kaheldavaks praktikat, mille kohaselt uurimisasutused ja AKI lubavad kolmandatel isikutel tutvuda kriminaal- ja kohtutoimikutega osas, mis ei ole kaetud juurdepääsupiiranguga.

KarS § 157^1 sätestab vastutusele võtmise aluse delikaatsete isikuandmete ebaseadusliku avalikustamise, andmetele juurdepääsu võimaldamise või andmete edastamise eest omakasu eesmärgil või kui sellega on tekitatud oluline kahju teise isiku seadusega kaitstud õigustele ja huvidele. Käesoleva töö autor on läbi vaadanud maakohtute, ringkonnakohtute ja Riigikohtu praktika ja jõudnud tõdemuseni, et KarS § 157^1 ei ole kriminaalkorras vastutusele võtmiseks praeguseni kasutatud. Rakendamist on leidnud KarS § 157 kutse- ja ametitegevuses teatavaks saanud saladuse hoidmise kohustuse rikkumise kohta ja Kars § 157^2 teise isiku identiteedi ebaseadusliku kasutamise eest. Autori hinnangul saab siiski olulise järelduse teha Riigikohtu lahendist 3-1-1-56-13. Antud lahendis heideti isikule Kars § 157 järgi ette seda, et ta rikkus IKS

[176] IKS § 4 lg 2 p 8
[177] Albers, M. Isikuandmete kaitsepõhiõiguslik alus: kas õigus informatsioonilisele enesemääramisele ja/või eraelu austamisele? Juridica VIII 2005, lk 538

§-s 26 sisalduvat kohustust hoida talle tööülesannete täitmisel teatavaks saanud isikuandmeid saladuses. Riigikohus ütles selles lahendis välja, et viidatud sättest ei tulene, et see kohustus laieneb vaid delikaatsetele isikuandmetele.[178] Seega laieneb IKS § 26 kõikidele isikuandmetele. Tulenevalt IKS §-dest 42-43 kohaldatakse teatud juhtudel delikaatsete isikuandmete töötlemisnõuete rikkumise[179] ja isikuandmete kaitse turvameetmete ja isikuandmete töötlemise nõuete rikkumise eest KarS-i üldosa ja väärteomenetluse seadustiku sätteid. Kuna pärast kriminaalmenetluse lõppu väljuvad andmed delikaatsete isikuandmete kaitsealast, siis vastutus nende andmete väärkasutamise eest kvalifitseerub väärteoks. Autor on arvamusel, et isikukahju ja põhiõiguste riive on võimalik igasuguste isikuandmete väärkasutamisel. Seetõttu tuleks autori arvates kaaluda seoses teabe taaskasutamise regulatsiooni kehtestamisega AvTS-is IKS-s kehtestatud vastutusele võtmise regulatsiooni üle vaatamist ja vajadusel ajakohastamist. Näiteks on hetkel võimalik IKS § 42 lg 1 kohaselt delikaatsete isikuandmete kaitse turvameetmete rikkumise eest trahvida füüsilist isikut kuni 300 trahviühikuga ehk kuni 1200 euroga ja juriidilist isikut kuni 32 000 euroga.[180] Arvestades, et avaliku sektori valduses olev teave on hinnatud majanduslikult oluliseks ressursiks ja isikukahju ning põhiõiguste riive on võimalik igasugusel isikuandmete kasutamisel, siis võiks autori hinnangul analüüsida praeguses IKS-is kehtestatud trahvimäärade vastavust võimalike rikkumiste intensiivsusele. Isikute põhiõigus privaatsusele on hindamatu ja riigil on positiivne kohustus need põhiõigused efektiivselt tagada.

Juhul, kui riik on isiku privaatsusõigust rikkunud on õigus nõuda riigilt kahju hüvitamist riigivastutuse seaduse alusel.[181] EIÕK artikkel 13 kohaselt on igaühel, kelle konventsioonis sätestatud õigusi ja vabadusi on rikutud, õigus tõhusale menetlusele enda kaitseks, sealhulgas kui rikkumise pani toime ametiisik. EIÕK on Eesti õiguskorra lahutamatu osa.[182] PS § 25 kohaselt on igaühel õigus nõuda talle ükskõik kelle poolt õigusvastaselt tekitatud moraalse ja materiaalse kahju hüvitamist. Õigus nõuda kahju hüvitamist tuleneb PS § 25-st juhul, kui kahju on tekitatud õigusvastaselt – rikutud on kahjukannatanud isiku mõnda seadusest, põhiseadusest või välislepingust tulenevat õigust.[183]

[178] RKKKo 3-1-1-56-13, p 14.1
[179] IKS § 42 reguleerib vastutusele võtmist delikaatsete isikuandmete töötlemise registreerimiskohustuse ja isikuandmete välisriiki edastamise nõuete ning andmesubjekti teavitamise kohustuse rikkumisel
[180] KarS § 47 lg 1, 2
[181] RKÜKo 3-3-1-85-09, p 106
[182] *Ibid*. p 73
[183] *Ibid*. p 76

3.7. EIK lahendid

M.K versus Prantsusmaa

Vaadeldavas kohtulahendis oli isiku M.K suhtes toimunud kaks kriminaaluurimist kahtlusega vargustes. Mõlema uurimise käigus võeti M.K-lt sõrmejäljed. Esimeses menetluses mõisteti M.K õigeks ja teises asjas kriminaalmenetlus lõpetati. Kui õigeksmõistva otsusega sõrmejäljed kustutati andmebaasist, siis teise menetluse järel keeldusid ametivõimud ja kohtud sõrmejälgi andmebaasist kustutamast. Prantsusmaa seaduste kohaselt kuulusid sõrmejäljed säilitamisele 25 aastaks. EIK leidis siin lahendis, et Prantsusmaa ei ole austanud isiku eraelu. Isikuandmete säilitamisel peab arvestama meetme vajalikkust ja kestvust. Autori arvates oli antud kaasuses huvitav Prantsusmaa väide, et sõrmejälgede säilitamine oli vajalik, et kaitsta M.K-d identiteedi varguse eest. EIK selle põhjendusega ei nõustunud ja leidis, et sel juhul on võimalik põhjendada kogu Prantsusmaa elanikkonnalt sõrmejälgede võtmist ja säilitamist. Prantsusmaa seadus ei sätestanud, millistel asjaoludel on lubatud säilitada isikute sõrmejälgi. Lisaks jõudis EIK järeldusele, et 25 aastane säilitustähtaeg tähendab sisuliselt andmete tähtajatut säilitamist. Kokkuvõtvalt leidis EIK, et demokraatlikus ühiskonnas ei ole Prantsusmaa kehtestatud pikaajaline sõrmejälgede säilitamise periood põhjendatud ja rikutud on EIÕK artiklit 8.[184]

M.M versus Ühendkuningriik

Selles lahendis oli tehtud M.M-le hoiatus perekonnatüli käigus lapse äraviimise katses. Sel ajal Ühendkuningriigis kehtinud regulatsiooni kohaselt oleks see hoiatus pidanud kustuma kolme aasta möödumisel ning M-M-le oli antud ka vastav teave. Pärast M-M-le hoiatuse kohaldamist muudeti aga seadust ning tema hoiatus kanti karistusregistrisse viieks aastaks. M.M leidis, et tegemist on tema eraelu riivega EIÕK artikkel 8 tähenduses, kuna andmete olemasolu karistusregistris mõjutab tema võimalikke tööandjaid ja kitsendab karjääri võimalusi. EIK leidis, et isiku kohta info kogumine on otseselt EIÕK artikkel 8 kaitsealas. Isiku õigusvastase käitumisega seotud informatsioon on eriti tundlik isiklik teave ja mida kaugemale ajas jääb õigusvastane käitumine, seda enam muutub see isiku eraelu osaks. EIÕK asus seisukohale, et teatud aja möödudes tuleneb eraelu austamise nõudest, et isik peab andma oma nõusoleku teda puudutava ja õigusvastast käitumist sisaldava teabe avaldamiseks. Kuna sel ajal puudus

[184] EIKo 18.04.2013, 19522/09, Affaire M.K vs France

Ühendkuningriigi õiguses selge regulatsioon politsei pädevusest avaldada tööandjatele teavet isiku õigusvastase käitumise kohta, siis ei olnud sellise teabe säilitamine kooskõlas seadusega ja eraelu riive vajalikkus demokraatlikus ühiskonnas. EIK rõhutas, et seadusest peab tulenema detailne regulatsioon, kuna avalikult kättesaadav teave isiku varasema õigusvastase käitumise kohta saab negatiivselt mõjutada isiku tööandjaid ja pole välistatud "noahoop isiku mainele". EIK tuvastas artikkel 8 riive. [185]

Peruzzo and Martens versus Germany

EIK jõudis järeldusele, et antud lahendis ei ole relevantne viidata EIK lahendile *S and Marper*, kuna erinevad faktilised asjaolud. Esiteks erinevalt *S and Marperi* kaasusest oli siin DNA analüüsid võetud ja säilitatud isikutelt, kes olid kriminaalkorras süüdi mõistetud, andmete säilitamine oli ettenähtav ja olemas oli legitiimne alus – võitlus kuritegevuse vastu. Saksamaal oli kehtestatud täpne regulatsioon, mis nägi ette, et DNA andmeid kasutatakse vaid DNA profiili loomisel ja ekspertidele esitatakse DNA proovid anonüümselt. Kui DNA profiil on loodud, siis selle algmaterjal hävitatakse, kuna eesmärk on täidetud. DNA profiili maksimaalset säilitamistähtaega 10 aastat, pidas EIK mõistlikuks säilitamistähtajaks. EIK ei võtnud avaldust vastu.[186]

[185] EIKo 13.11.2012, 24029/07, M.M vs United Kingdom
[186] EIKo 04.06.2013, 7841/08 and 57900/12, Peruzzo and Martens vs Germany

KOKKUVÕTE

Avaliku sektori teabe taaskasutamisele on seatud kõrged majanduslikud ootused. Teabe taaskasutamist peetakse üheks seni efektiivselt kasutamata tuluallikaks Euroopa Liidus ja selle turuväärtuseks vähemalt 32 miljardit eurot. Euroopa Liidu eesmärgiks avaliku sektori teabe taaskasutamise direktiivide kehtestamisel on olnud ettevõtlusarengu ergutamine ja maailma majanduses konkurentsis püsimine. Avaliku sektori teabe taaskasutamise direktiividelt oodatakse liikmesriikides avaliku teabe kättesaadavuse ühtlustumist ning seeläbi moonutamata konkurentsi arengut liidus. Ühtlasi toetab avaliku sektori valduses olevate dokumentide ja teabe kättesaadavaks tegemine läbipaistva halduse põhimõtet ja on demokraatia üks põhiprintsiipe. Teabe taaskasutamise direktiividega on seatud eesmärgiks kõigi avaliku sektori valduses olevate dokumentide kättesaadavaks tegemine ja 2013. aasta teabe taaskasutamise direktiiv laiendas seda õigust avaliku sektori asutustelt arhiividele, ülikoolidele ja muuseumidele. Kuigi teabe taaskasutamise direktiivid viitavad isikuandmete kaitse direktiivile ja seal kehtestatud isikuandmete kaitse põhimõtetele, ei ole direktiivid otsesõnu isikuandmete kasutamist avaliku sektori teabe taaskasutamisel reguleerinud. Seetõttu on direktiivide osaks saanud kriitika, mille kohaselt ei anna direktiivid piisavaid ja täpseid juhiseid, kas ja kuidas on isikuandmete taaskasutamine lubatud.

Käesoleva magistritöö eesmärgiks oli leida vastus küsimusele, kas avaliku sektori teabe taaskasutamise regulatsioon kaitseb kriminaalmenetluses kogutud isikuandmeid. Kuna teabe taaskasutamise regulatsioon on praktikas uus, siis analüüsis autor esmalt avaliku sektori teabe taaskasutamise direktiive ning nende vastavust isikuandmete kaitse direktiivile ja isikuandmete kaitse põhimõtetele. Seejärel analüüsis autor avaliku sektori teabe taaskasutamise regulatsiooni Eesti õiguses ning tegi magistritöös vahekokkuvõtte, mille põhjalt teeb autor täiendavad järeldused käesolevas kokkuvõttes. Magistritöö kolmandas peatükis analüüsis autor isikuandmete kaitset kriminaalmenetluses ja küsimust, kas kriminaalmenetluses kogutud isikuandmed on teabe taaskasutamisel kaitstud. Autor arvestas analüüsi tehes, et tulenevalt AvTS §-st 8 lõikest 3 hõlmab teabele juurdepääs õigust seda teavet taaskasutada.

Magistritöö lõpuks on autor analüüsi käigus jõudnud järgmistele järeldustele:

Isikuandmete definitsioon on väga avar. Isikuandmed on igasugused andmed, mida saab konkreetse isikuga seostada ja pole oluline, mis valdkonnas need andmed on kogutud. Isikuandmed on osa isiku eraelust ja privaatsfäärist, mida kaitseb EIÕK artikkel 8. Tulenevalt EIK praktikast kuulub eraelu kaitse alla inimese füüsiline ja vaimne terviklikkus, füüsiline ja sotsiaalne identiteet, isiku sugu, nimi, seksuaalne orientatsioon, seksuaalelu, terviseseisund, etniline kuuluvus, isiku õigus enda arendamisele, õigust rajada ja arendada suhteid teiste inimestega ja välismaailmaga ja isiku õigust oma kuvandile. EIK on öelnud, et eraelu mõiste on määratlemata õigusmõiste ja seda ei saa ammendavalt kirjeldada. Isikuandmete kaitse peab tagama eraelu puutumatuse ja isiku privaatsfääri säilimise.

Kõige selgem juhis isikuandmete taaskasutamise kohta pärineb *andmekaitse 29. töörühmalt*. Selle juhise kohaselt on isikuandmete taaskasutamine lubatud vaid juhul, kui need andmed on muudetud täiesti anonüümseks ja nende isikuseos on tuvastamatu. Mis omakorda tähendab seda, et pärast isikuandmete anonüümseks muutmist ei saagi me enam rääkida isikuandmete taaskasutamisest kui sellistest, vaid lihtsalt andmete taaskasutamisest. Seega senikaua, kuni isikud on andmete hulgast tuvastatavad, on tegemist isikuandmetega ja nende andmete kasutamisele kohaldub isikuandmete kaitse direktiiv. Kui andmete isikuseos on muudetud täiesti tuvastamatuks ja isikuid ei ole võimalik identifitseerida, siis saab kohaldada teabe taaskasutamise direktiive.

Isikuandmete kaitse direktiiv kohaldub, kui isikuandmed on kas või kaudselt tuvastatavad, isegi siis, kui avalik sektor on enda teada muutnud need andmed andmekogus anonüümseks. Isikuandmete kaitse direktiivi kohaselt kogutakse isikuandmeid vaid täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel ja isikuandmeid ei töödelda hiljem viisil, mis on vastuolus nende kogumise esialgse eesmärgiga. Järelikult on igasugune isikuandmete taaskasutamine algselt mitte ettenähtud eesmärkidel keelatud.

Õigusselguse ja moonutamata konkurentsi tagamiseks peaks isikuandmete taaskasutamise keeld tulenema avaliku sektori teabe taaskasutamise direktiivist. Nagu selgus eri õigusaktide analüüsimisel, on isikuandmete taaskasutamise keeld tuletatav praegu erinevatest õigusaktidest. Seetõttu on autor seisukohal, et õigusselguse tagamiseks peaks see keeld tulenema avaliku sektori teabe taaskasutamise direktiividest endast. Nii kanduks see keeld ühtse põhimõttena kõikide Euroopa Liidu liikmesriikide seadustesse ning isikuandmetele ligipääs ei

sõltuks enam igas liikmesriigis asuvate haldusorganite teabele juurdepääsukordadest. Lisaks toetab ühtse põhimõtte kehtestamine direktiivi tasandil võrdse konkurentsi loomist teabe taaskasutamise turul Euroopa Liidus.

Õigusselguse ja isikuandmete kaitse põhiõiguse tagamiseks [187] peaks isikuandmete taaskasutamise keeld olema sätestatud seaduses. Eestis on avaliku sektori teabe taaskasutamine reguleeritud AvTS-s. Nagu selgus, lubavad AvTS ja teabe taaskasutamise direktiivid kasutada avalikus sektoris kogutud teavet mistahes muul eesmärgil, mis ei lange kokku algse eesmärgiga, mille jaoks see teave avalikke ülesandeid täites saadi või loodi. Autor peab sellist sõnastust mõnevõrra eksitavaks, sest tulenevalt IKS-s ja isikuandmete kaitse direktiivis kehtestatud isikuandmete töötlemise põhimõtetest on igasugune isikuandmete esialgsest eesmärgist erinev töötlemine keelatud. Isikuandmete taaskasutamise keeld on põhimõttena kirjas AvTS eelnõu seletuskirjas, kuid see põhimõte ei ole jõudnud samal kujul seadusesse. Seetõttu on autor arvamusel, et lisaks direktiivile tuleks isikuandmete taaskasutamise keeld sätestada sarnaselt AvTS-is. Autori arvates lihtsustaks see muudatus muuhulgas diskretsiooni teostajate tööd ning vähendaks teabe taaskasutamisel ebakindlust nii teabe taaskasutajates, avalikus sektoris kui ka andmesubjektides.

Tulenevalt AvTS §-st 8 lg 3 hõlmab juurdepääs teabele õigust seda teavet taaskasutada. Muuhulgas on teabe taaskasutamiseks teabe kasutamine mistahes muul viisil ja eesmärgil, kui oli teabe esialgne kogumise ja kasutamise eesmärk. Seega, kui isikul on juba juurdepääs teabele, on tal õigus seda teavet taaskasutada. IKS sätestab, et isikuandmeid ei tohi kasutada eesmärgil, mis ei ole andmetöötluse eesmärkidega kooskõlas, kuid nagu selgus magistritöö esimeses osas, siis puudub õigusraamistikul objektiivne võimekus isikuandmete eesmärgipärase kasutamise hindamiseks. Praegu on seadusandja jätnud isikuandmete kolmandatele isikutele avaldamise haldusorgani diskretsiooniotsuseks. Seejuures haldusorgan peab suutma hinnata, kas tegemist on isikuandmetega, millisel eesmärgil on need andmed kogutud ning kas ja millisel eesmärgil on kellegil õigus neid andmeid kasutada tulevikus. Lisaks peab haldusorgan suutma AvTS-st tulenevalt hinnata, kas isikuandmete väljastamisega rikutakse oluliselt eraelu puutumatust. Järelikult on haldusorganitel suur vastutus, sest kui teave on läinud avalikust sektorist juba üle kolmandatele isikutele, siis puudub kontroll selle teabe eesmärgipärase kasutamise üle. Juhul kui selleks teabeks on isikuandmed ja neid on kasutatud

[187] Ivo Pilving on öelnud, et informatsioonilise enesemääramise õiguse asemel peaks kõnelema isikuandmete kaitse põhiõigusest, nii nagu teeb seda Euroopa põhiõiguste harta, vt Pilving, I. Õigus isikuandmete kaitsele. Juridica VIII 2005, lk 535

esialgsetest eesmärkidest erinevalt on isikukahju juba tekkinud. Seetõttu peaks teabe taaskasutamise regulatsiooni efektiivseks ja eesmärgipäraseks kasutamiseks seadusandja kehtestama selgemad juhised isikuandmete kasutamise eesmärgipärasuse hindamiseks ja isikuandmete anonüümseks muutmise kohta.

On üldine seisukoht, et mida rohkem aega on möödunud isikuandmete esialgsest kogumisest, seda enam saavad need osaks isiku privaatsfäärist. Seetõttu ei ole autori arvates õiguspärane olukord, et riiklikus arhiivis säilitatakse pikaajaliselt isikuandmeid sisaldavaid dokumente, mille juurdepääsupiirang teatud aja möödudes lõppeb ja need saavad avalikuks. Näiteks juba fakt, et Rahvusarhiivis säilitatakse isiku kohta kriminaaltoimikut, võib isikut jätkuvalt häbistada ja takistada tema rehabilitatsiooni ühiskonda. Lisaks võivad arhiivitud dokumendid sisaldada delikaatseid isikuandmeid, nagu näiteks informatsiooni raskest haigusest või muudest delikaatsetest sündmustest isiku elus. Pärast juurdepääsupiirangu lõppemist ja dokumentide avalikuks saamist võib see teave otseselt mõjutada nii andmesubjekti ennast kui ka tema järeltulijaid ja sugulasi.

KarS § 157 sätestab vastutusele võtmise kutse- ja ametitegevuses teatavaks saanud saladuse hoidmise kohustuse rikkumise eest. Tulenevalt Riigikohtu praktikast peab KarS § 157 rakendamiseks aga kehtima lisaks seadusest tulenev keelunorm, mis otsesõnu keelab teatud kutse- ja ametitegevuses teatavaks saanud teabe avalikustamise. KarS § 157^1 võimaldab määrata karistuse delikaatsete isikuandmete ebaseadusliku avaldamise eest. Kuna pärast kriminaalmenetluse lõppu väljuvad kriminaalmenetluses kogutud andmed delikaatsete isikuandmete kaitsealast ja on võimalik, et teabe taaskasutaja ei ole neid andmeid saanud teada kutse- ega ametitegevuses, siis on sellisel juhul tegemist väärteoga. Kuivõrd kriminaalmenetluses kogutud andmete sisu ei muutu pärast kriminaalmenetluse lõppu, siis võiks autori arvates kaaluda IKS-i delikaatsete isikuandmete loetelu muutmist selliselt, et kriminaalmenetluses kogutud andmed jäävad delikaatseks ka pärast menetluse lõppu.

Autori arvates peaks analüüsima IKS-is kehtestatud väärtegude karistusmäärade põhjendatust ja nende eesmärgipärasust. Seda põhjusel, et praegu kehtivas IKS-s kehtestatud karistusmäärad on jõustatud enne avaliku teabe taaskasutamise regulatsiooni kehtestamist AvTS-is. Avaliku sektori valduses olevat teavet on hinnatud majanduslikult oluliseks ressursiks ning isikukahju ja põhiõiguste riive on võimalik igasugusel isikuandmete kasutamisel. Seetõttu peaksid IKS-s kehtestatud trahvimäärad vastama võimalikule avaliku teabe taaskasutamise regulatsioonist

tulenevale rikkumise intensiivsusele. Isikute põhiõigus privaatsusele on hindamatu ja riigil on positiivne kohustus need põhiõigused efektiivselt tagada.

EIK praktikast tulenevalt ei ole demokraatlikus ühiskonnas vajalik säilitada kriminaalmenetluses õigeksmõistetud isiku andmeid ja andmeid isikute kohta, kelle suhtes kriminaalmenetlus on lõpetatud. Süütuse presumptsioon sisaldab üldist reeglit, mille kohaselt pärast isiku õigeksmõistmist (süü puudumist) ei tohi mingilgi viisil levitada või anda alust vastupidiseks arvamuseks. Kui isikut ei ole süüdi mõistetud, siis puudub alus tema andmete säilitamiseks. Andmete säilitamine on aga põhiline eeldus, et neid saaks taaskasutada. Analüüsist selgus, et Eestis on kehtestatud kriminaaltoimikutele säilitamistähtajad pärast kriminaalmenetluse lõppu VV määrusega nr 261. Nimetatud määrus aga ei reguleeri, kuidas säilitada õigeksmõistva kohtuotsuse jõustumise järgselt kriminaalmenetluses kogutud andmeid. Kuna EIÕK artikkel 8 lg 2 kohaselt tuleb andmeid säilitada "seaduse alusel", siis on olemas otsene ja potentsiaalne isikute privaatsusõiguse rikkumine EIÕK artikkel 8 lg 2 mõttes.

Tulenevalt VV määrus nr 261 § 4 lg-st 2 ja § 6 lg-st 1 säilitatakse alaealiste komisjonis tehtud otsused veel 10 aastat pärast kriminaalmenetluse lõpetamise määruse koostamist või kohtumääruse jõustumist. Autor peab kaheldavaks, kas seesugune regulatsioon on proportsionaalne ja kas see arvestab isiku vanuse aspektiga nii, nagu EIK on seda ette näinud oma lahendis *S and Marper*.

Selleks, et avaliku sektori valduses olevat teavet saaks taaskasutada, peab see teave olema säilitatud seaduslikul alusel. EIÕK artikliga 8 ei ole kooskõlas, kui isikuandmeid säilitatakse seadusliku aluseta ja ebaproportsionaalselt pikkade tähtaegadega. EIK on oma lahendis M.K vs Prantsusmaa öelnud, et 25 aastane säilitustähtaeg on sisuliselt võrdne andmete tähtajatu säilitamisega. Eesti uurimisasutustest säilitab Riigiprokuratuur pärast kriminaalmenetluse lõppu kriminaaltoimikuid veel 25 aastat, mis ei ole kooskõlas VV määruses nr 261 kehtestatud tähtaegadega ning on ebaproportsionaalselt pikk tähtaeg tulenevalt EIK praktikast.

Tulenevalt VV määrusest nr 261 §-st 4 on kriminaaltoimikute säilitamistähtajad vastavalt kas 10 või 15 aastat ja alaliselt säilitatakse kriminaaltoimikuid süüteos inimsuse vastu, sõjasüüteos või süüteos, mille toimepanemise eest on KarS-s ette nähtud eluaegne vangistus. VV määrus nr 261 § 4 lg 10 kohaselt arhiivib prokuratuur kriminaaltoimiku samas paragrahvis kehtestatud tähtaegadel. Seega ei vasta Riigiprokuratuuris kehtestatud säilitustähtajad VV määruses nr 261 § 4 nõuetele.

Ringkonnaprokuratuuril on võimalik pikendada kriminaaltoimikute säilitamistähtaega või määrata alatine säilitustähtaeg. PPA on jätnud endale võimaluse kriminaaltoimikute säilitamistähtaegade pikendamiseks tuginedes "praktilisele vajadusele". Autor on seisukohal, et prokuratuurides ja PPA-s ei vasta kriminaaltoimikute säilitamine sellisel kujul VV määruses nr 261 kehtestatud nõuetele, sest pole selge, millised säilitamise tähtajad kriminaaltoimikutele määratakse ja kuidas ning millise vajaduse tekkimisel säilitamistähtaegu muudetakse. Seetõttu on tulenevalt EIK lahendist *S and Marper* olemas potentsiaalne EIÕK artikkel 8 lg 2 rikkumine.

Eesti kohtud arvestavad võrreldes uurimisasutustega kõige enam kriminaaltoimikutele säilitamistähtaegade määramisel proportsionaalsuse põhimõttega. Säilitamistähtajad on määratud maa,- haldus- ja ringkonnakohtu kantselei kodukorra lisas 5. Erinevalt VV määrusest nr 261 võimaldab kodukord säilitada teatud süütegude puhul kriminaaltoimikud ka 3 ja 5 aastat ning säilitamistähtaja määramisel on arvestatud kuriteo raskusega. Nii säilitatakse näiteks süütegudes alaealise või omandi vastu kriminaaltoimikuid 3 aastat. Seega arvestab kohtute kodukord enam alaealiste õigustega ja hindab proportsionaalsemalt andmete säilitamise vajalikkust kui uurimisasutustes kehtestatud korrad ja VV määrus nr 261. Siiski arhiivib ka maakohus õigeksmõistva kohtuotsuse ja lõpetatud kriminaalasjade toimikud ilma seadusliku aluseta ning olemas on potentsiaalne EIÕK artikkel 8 lg 2 riive.

KrMS-s oleks vaja analoogselt HKMS §-de 89 ja 175 alusel sätestada konkreetsemad kohtuotsusele juurdepääsutingimused. Praegu on AKI lubanud kolmandatele isikutele juurdepääsu kriminaalmenetluses veel jõustumata kohtulahenditele. AKI on viidanud asjaolule, et kuna KrMS-s puudub regulatsioon kohtuotsuse väljastamiseks, siis tuleb AvTS-i kohaldada eriseadusena KrMS suhtes. Autor ei nõustunud magistritöös AKI väitega ja on seisukohal, et tulenevalt KrMS-st ning maa-, haldus- ja ringkonnakohtu kantselei kodukorrast on KrMS eriseadus AvTS-i suhtes. Autor on seisukohal, et õigusselguse paremaks tagamiseks tuleks kohtuotsusele juurdepääsutingimused sõnaselgemalt kehtestada KrMS-s.

E-toimiku infosüsteemis säilitatakse väga palju erisuguseid (isiku)andmeid. Analüüsist selgus, et e-toimiku infosüsteemis säilitatakse kõik kriminaalasjade materjalid tähtajatult ja ilma seadusliku aluseta. Seetõttu on olemas potentsiaalne EIÕK artikkel 8 lg 2 rikkumine. Lisaks rikub e-toimiku infosüsteem potentsiaalselt kõikide infosüsteemis menetlusosalistena kajastatud andmesubjektide isikuõigusi, sest nende andmete säilitamine infosüsteemis toimub ilma seadusliku aluseta.

Piiratud juurdepääsuõigus kriminaaltoimikule ja kohtuotsusele ei pruugi piisavalt tagada isiku privaatsfääri kaitset. Isegi kui osaliselt kinni katta kriminaaltoimikus delikaatsed isikuandmed või muul viisil neid umbisikustada, siis nende andmete asumise kontekst võib isiku paljastada ja isik on endiselt tuvastatav. Kohtuotsuste ja kriminaaltoimikute umbisikustamine ei pruugi piisavalt tagada isiku privaatsfääri kaitset, sest isikustamata andmeid on võimalik tulenevalt kontekstist seostada konkreetse isikuga või kaudselt tuvastada ja see rikub isiku õigust olla üksi. Autori arvates ei ole see vastavuses isikuandmete kaitse direktiivist tuleneva isiku tuvastamatuse põhimõttega, sest hoolimata osalise info edastamisest kolmandatele isikutele, saab taaskasutamiseks antud info põhjalt luua seoseid ja tuletada infot, mis võib olla delikaatne ja ei tohiks olla kättesaadav. Andmekaitse 29. töörühm on tauninud sellise olukorra tekkimist ja soovitanud liikmesriikidel eraldi viia läbi põhjalikud analüüsid hindamaks, kas anonüümseks muudetud teabe põhjal on isikud tuvastatavad.

Eelnevast tulenevalt teeb autor järgnevad ettepanekud:

1. Teabe taaskasutamise direktiivides tuleks sätestada isikuandmete taaskasutamise keeld.
2. AvTS-i tuleks täiendada põhimõttega, mis keelab isikuandmete taaskasutamise.
3. Seadusandja või AKI peaks teabe taaskasutamise regulatsiooni efektiivseks ja eesmärgipäraseks kasutamiseks kehtestama selged juhised haldusorganitele, mille järgi need saaks hinnata isikuandmete kasutamise eesmärgipärasust ja vajadusel muuta isikuandmed anonüümseks.
4. Muuta IKS-is kehtestatud delikaatsete isikuandmete loetelu selliselt, et pärast kriminaalmenetluse lõppu jäävad menetluses kogutud andmed delikaatseks. Avaldada võib süüdimõistetud isiku andmeid.
5. Juurdepääsupiirangute lõppemine arhiivis säilitatavatele isikuandmetele ei tohiks kahjustada andmesubjektide ja nende järeltulijate privaatsfääri.
6. Seadusandja peaks üle vaatama IKS-s kehtestatud isikuandmete väärkasutamise eest vastutusele võtmise alused, arvestades sealjuures võimalikku ohtu isiku põhiõigustele teabe taaskasutamisel.
7. Täiendada tuleb VV määrust nr 261 ja lisada säte, mis reguleerib õigeksmõistva kohtuotsuse järgselt kriminaalmenetluses kogutud andmete säilitamist, et kriminaaltoimikute säilitamine vastaks EIÕK artikkel 8 lg-le 2. Seejuures arvestades, et kriminaalmenetluses isikuandmete kogumise eesmärk on täidetud ja nende andmete säilitamine ja kasutamine teistel eesmärkidel on keelatud. Täiendav säte peaks laienema nii uurimisasutustele kui kohtutele.

8. Seadusandja võiks üle vaadata alaealiste komisjonis tehtud otsuste säilitamistähtajad ja kaaluda nende lühendamist. Eelkõige lähtudes EIK praktikas väljatoodud proportsionaalsuse printsiibist.
9. Riigiprokuratuur peaks viima kriminaaltoimikute säilitamistähtajad kooskõlla VV määruses nr 261 sätestatud tähtaegadega.
10. Prokuratuurid ja PPA peaksid sätestama selged alused, mille järgi kriminaaltoimikute säilitamistähtaegu muudetakse. Tähtajad peavad olema kooskõlas VV määruses nr 261 säilitamistähtaegadega ja EIK praktikaga.
11. Kehtestada tuleks KRMS-s analoogselt HKMS-iga konkreetne kohtuotsusele juurdepääsukord kolmandatele isikutele.
12. Seadusandja peaks kehtestama e-toimiku infosüsteemis olevatele andmetele konkreetsed säilitamistähtajad.
13. Haldusorgan peab enne teabe taaskasutatavaks tegemist põhjalikult hindama, kas anonüümseks muudetud teabe põhjal on isikud tuvastatavad või on võimalik teabe põhjal isikuid kaudselt identifitseerida. Eriti oluline on see piiratud juurdepääsu võimaldamisel kriminaaltoimikutele.

Kokkuvõtvalt on autor jõudnud tõdemuseni, et magistritöö alguses esitatud hüpotees on leidnud kinnitust – avaliku sektori teabe taaskasutamisel ei ole tagatud kriminaalmenetluses kogutud isikuandmete kaitse. Kehtiv praktika ja õigusraamistik ei kaitse piisavalt selgelt isikuandmeid teabe taaskasutamisel ja ei taga isikuandmete taaskasutamisele kehtestatud teabe anonüümsuse nõudeid. Lisaks ei säilitata Eestis kõiki kriminaalmenetluses kogutud isikuandmeid seaduse alusel, mis otseselt riivab isikute õigust eraelu puutumatusele ja pole kooskõlas isikuandmete töötlemise põhimõtetega.

SUMMARY

Protection of personal data collected in criminal proceedings on re-use of public sector information

The European Union (EU) has set a goal to improve internal market by validating the re-use of public sector information (PSI). PSI is seen as an opportunity to expand economy, increase employment and improve public sector transparency. Therefore the EU has implemented directives 2003/98/EC and 2013/37/EU on the re-use of PSI. As it is not certain, if the re-use of PSI regulation secures protection of personal data this master's thesis analyses protection of personal data in the most delicate sphere – criminal proceedings.

Re-use of PSI is a new legal instrument in Estonian legislature. On account of this, the master's thesis is divided into two sections. In the first section, the author analyses re-use of PSI directives and their adequacy to ensure protection of personal data and how the regulation has been implemented in Estonian legislature. In the end of the first section, the author makes a short compendium with three conclusions:

1. Protection of personal data is guaranteed when public sector institution access regime and discretion assures it.
2. Re-use of personal data is allowed only if this data is collected lawfully and on legitimate purposes, and personal data has been made completely anonymous.
3. To ensure effectiveness of the re-use of PSI, legislator should give clear and objective instructions on how to evaluate the character of the information and its purposes.

In the second section of the master's thesis the author analyses protection of personal data in criminal proceedings and how it is guaranteed by Estonian legislature and personal data processors who carry out criminal proceeding and retain criminal proceeding files. Final conclusions are added in the end of this chapter.

The main part of this master's thesis has opinions and recommendations given by Article 29 Working Party, Directive 95/46/EC, judgements of European Court of Human Rights (ECHR) and Estonian regulations of retaining criminal proceeding files and access regimes to personal data.

The hypothesis of the master's thesis is the claim that the protection of personal data obtained in criminal proceedings in re-use of PSI is not guaranteed. The author has based the claim on

the fact, that in criminal proceedings data processors have extensive rights in order to find out the truth.

Presumption of innocence must be guaranteed in every level of justice system but also after the criminal proceedings have come to an end. Retained files of criminal proceedings after the person has not been assumed to be guilty, or the criminal investigation has been finished, personal data must be destroyed. This is because the initial aim of collecting this information has been fulfilled and there is no other objective purpose to retain this information. Deleting files of criminal proceedings is a premise that this data cannot be re-used in the future. This is an important warranty so as to secure the right to privacy.

Final conclusions:

The term *personal data* is wide and incorporates all kinds of data we can associate with a certain person. Therefore, protection of this data can be rather difficult as we live in an information age and there is already all kinds of information available on the internet, within corporations, owned by the employers etc. Due to this it is significant that the personal data that the State gives access to for re-use is completely anonymous. This also means, that the State should have the competence to evaluate the information in terms of whether it contains personal data or not. It follows that the State should give public sector institutions guidelines in order for them to evaluate such information. The re-use of personal data is only allowed when it has been made fully anonymous.

The most definite instructions about re-use of personal data, are given by Article 29 Working Group. According to these instructions, re-use of PSI directives are implemented only implement when data does not include personal data, and data is completely anonymous. In case the data includes personal information, directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data is implemented.

Re-use of personal data for other purposes than for which the data was initially obtained for is prohibited.

In order to avoid distorted internal market in the EU, the prohibition of re-use of personal data should be written in the directives of re-use of PSI. This would support equal competition in the market of re-use of PSI in the EU and clarify legal rights and duties.

For legal clarity, the prohibition to re-use personal data should be written in the Estonian Public Information Act. This would make administrative institution's work unequivocal and give more assurance for the PSI re-users, persons and administration institutions.

Therefore, to ensure legal liability, the ground for taking public servants responsible for misuse of personal data according to the State Court of Estonia must come from the law. Stating public servant's obligations in administrative institution internal regulations is not enough.

After access restriction has come to an end, archived personal data should not become public. It is general standpoint that the sensitivity of data will decrease with the passage of time. However, the inappropriate release of many decades old records could still have a severely detrimental effect on the individual directly concerned but also on other individuals, such as his/her family members or descendants.

The legal liability part of the Personal Data Protection Act should be revised in order to guarantee effective protection from improper use of personal data. Given penalties should be in accordance with possible violations coming from the PSI re-use regulation in the Public Information Act.

According to the ECHR there is no democratic need to retain personal data about the person who has been acquitted or about the person whose criminal proceeding has been finished.

Estonia lacks regulation on retaining criminal proceeding files and personal data when the person has not been convicted. For this reason, it is potential threat and infringement of European Convention of Human Rights article 8 (2).

The author doubts if the Estonian decree about retaining files of criminal proceeding is proportional and takes into consideration juvenile rights as does the ECHR in its decision S and Marper. Estonia retains juvenile criminal proceeding files for 10 years after the end of the proceeding.

As it turned out in the analyses, Estonian criminal proceeding data processors lack lawful ground for retaining data collected in criminal proceedings. The Office of the Prosecutor General retains criminal proceeding files for 25 years after the end of the proceeding. However, the ECHR has stated that retention period of 25 years is equal to permanent retention. According to the Estonian decree about retaining files of criminal proceeding, designated time limits can be 10 or 15 years, or permanent in some cases as war crimes or crimes against humanity permanent. Therefore, this kind of long retention time period is disproportionate and is in accordance with Estonian decree no 261 about criminal proceeding data retention time limits. The Police and Border Guard Board (PBGB) and District Prosecutor's Office have possibility to change criminal proceeding files retention time limits relying on "practical need". This creates uncertainty of how and under which criteria retention time limits are changed. For this reason it is potential infringement of the European Convention of Human Rights article 8 (2).

Estonian courts reckon with the most of proportionality principle. Court's rules of procedure allow certain criminal proceeding files to be retained for lesser period of time than set out on the decree no 261. For example, in some cases it is allowed to retain files for 3 or 5 years. However, courts still courts retain criminal proceeding files on person who has been found not guilty, or when the proceeding has been ended. For this reason, it is potential infringement of the European Convention of Human Rights article 8 (2). The author has made a suggestion the Estonian Code of Criminal Procedure should be more concrete enacting access regimes to court decisions. The author has suggested to follow the example of the Estonian Code of Administrative Court Procedure.

Estonian database *E-toimik* retains all kinds of personal data with no time limits. Thus it is a potential infringement of the European Convention of Human Rights article 8 (2).

Partial access regime to criminal proceeding files does not provide enough protection to the right to privacy. Even though some information in criminal proceeding files has been covered as censored, it is still possible to identify personal data. Therefore, exhaustive analysis must be carried out before giving access to third parties.

The final conclusion, as already stated above, is that the protection of personal data obtained for criminal proceeding in re-use of PSI is not guaranteed. Valid practice and legal right does not protect personal data enough for the re-use of data and does not meet the anonymity

standards of personal data. Additionally, Estonia does not retain all criminal proceeding files lawfully, which directly violates the right to privacy and is not in accord with personal data processing principles.

KASUTATUD LÜHENDID

AKI	Andmekaitse Inspektsioon
andmekaitse 29. töörühm	direktiivi 95/46/EÜ artikli 29 alusel loodud töörühm. Sõltumatu Euroopa nõuandev kogu, kes tegeleb andmekaitse ja eralu puutumatuse kaitsega.
AvTS	avaliku teabe seadus
e-toimiku põhimäärus	Vabariigi Valitsuse määrus nr 111 "E-toimiku süsteemi asutamine ja e-toimiku süsteemi pidamise põhimäärus
ECHR	*European Court of Human Rights*
EIK	Euroopa Inimõiguste Kohus
EIÕK	Euroopa inimõiguste ja põhivabaduste kaitse konventsioon
HKMS	halduskohtumenetluse seadustik
IKS	isikuandmete kaitse seadus
isikuandmete kaitse direktiiv	24.10.1995 a direktiiv 95/46/EÜ
KAPO	Kaitsepolitseiamet
KaRS	karistusseadustik
KrMS	kriminaalmenetluse seadustik
LAPSI	*Legal Aspects of Public Sector Information*
nr	number
PBGB	*Police and Border Guard Board*
PPA	Politsei- ja Piirivalveamet
PS	Eesti Vabariigi põhiseadus
PSI	*public sector information*
RSVS	riigisaladuse ja salastatud välisteabe seadus
vs	versus
vt	vaata
VV	Vabariigi Valitsus

KASUTATUD KIRJANDUS

1. Albers. M. Isikuandmete kaitsepõhiõiguslik alus: kas õigus informatsioonilisele enesemääramisele ja/või eraelu austamisele? Juridica VIII 2005, lk 537-543.
2. Alexy. R. Põhiõigused Eesti põhiseaduses. Eriväljaanne. Juridica 2001, lk 5-96.
3. Avaliku teabe seaduse muutmise seaduse eelnõu 263 SE seletuskiri, kättesaadav: http://www.riigikogu.ee/?op=ems&page=eelnou&eid=bd9d9bac-52dc-4549-a23c-ee4816e0a2af& (14.04.2014).
4. C, Ovey; R. C. A. White. European Convention of Human Rights. 3rf edition Oxford University Press 2002
5. C. dos Santos. On privay and personal Data Protection as Regards Re-use of Public Sector Information (PSI). masaryk University Journal of Law and Technology, 6:3, 2012, pp 337-352.
6. Eesti Vabaiigi Põhiseaduse ekspertiisikomisjoni lõpparuanne. Põhiseaduse analüüs. Kättesaadav: http://www.just.ee/10725 (15.04.2014).
7. Eesti Vabariigi põhiseadus – kommenteeritud väljaanne. Kättesaadav: http://www.pohiseadus.ee/ (14.04.2014).
8. Gundermann. L. Euroopa Liidu andmekaitseõigus – andmekaitse ja andmetele avaliku juurdepääsu suhtest ning andmekaitse järelevalve olukorrast. Juridica VIII 2005, lk 511-518.
9. Ilus. T. Andmesubjekti osaluse põhimõte Euroopa Nõukogu konventsioonide ning Euroopa Inimõiguste Kohtu lahendite valguses. Juridica VIII 2005, lk 519-531.
10. Information Commissioner's Office. Anonymisation: managing data protection risk code of practice. Kättesaadav: http://ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Practical_application/anonymisation-codev2.pdf (29.04.2014).
11. Jõgi. M. Isikuandmete kaitse kriminaalmenetluses. Bakalaureusetöö, juhendaja Jaggo, O. Tartu Ülikool, õigusinstituut, avaliku õiguse instituut, kriminaalõiguse, kriminoloogia- ja kognitiivse psühholoogia õppetool 2006
12. K. Janssen, J. Dumortier. towards a European framework for re-use of public sector information: A long and winding road. international Journal of Law and information Technology, Vol 11, No 2, 2003, pp 184-201.
13. K. Janssen. The influence of the PSI directive on open government data: An overview of recent developments. Government Information Quarterly, 28, 2011, pp 446-456.

14. Kergandberg, E. Pikamäe, P. Kriminaalmenetluse seadustik. Kommenteeritud väljaanne. Tallinn Juura 2012
15. Kergandberg. E, Sillaots. M. Kriminaalmenetlus. Tallinn Juura 2006
16. Lord Millett. The Right to Good Administration in European Law. Public Law, Sweet & Maxwell 2002 summer, pp 309-322.
17. Lõhmus, U. Inimõigused ja nende kaitse Euroopas. Tartu: Sihtasutus Iuridicum 2003
18. M. de Vries. Integrating Europe's PSI re-use rules – Demystifying the maze. Computer Law & Security Review, 27, 2011, pp 68-74.
19. Merusk, K. Administratsiooni diskretsioon ja selle kohtulik kontroll. Juura Õigusteabe AS 1997
20. Merusk. K, Narits. R. Eesti konstitutsiooniõigusest. Tallinn Juura 1998
21. Männiko. M. Õigus privaatsusele ja andmekaitse. Tallinn Juura 2011
22. Parrest. N. Hea halduse põhimõte Euroopa Liidu põhiõiguste hartas. Juridica I 2006, lk 24-33.
23. Pilving. I. Õigus isikuandmete kaitsele. Juridica VIII 2005, lk 532-536.
24. R. Maruste. Konstitutsionalism ning põhiõiguste ja -vabaduste kaitse. Tallinn: Juura 2004
25. Tikk. E, Nõmper. A. Informatsioon ja õigus. Tallinn Juura 2007
26. Trechsel, S. Human Rights In Criminal Proceedings. Oxford: Oxford University Press 2007

KASUTATUD NORMATIIVAKTID

27. Arhiiviseadus. 17.02.2011. – RT I, 21.03.2011, I
28. Avaliku teabe seadus. 15. november 2000. – RT I 2000, 92, 597 ... RT I, 19.12.2012, 5
29. Council of Europe: Convention for the Protection of Individuals with the regard to Automatic Processing of Personal Data (1981).
30. E-toimiku süsteemi asutamine ja e-toimiku süsteemi pidamise põhimäärus. VVm 03.07.2008 nr 111. – RT I 2008, 31, 197 ... RT I, 17.11.2011, 5
31. Eesti Vabariigi põhiseadus. 28. juuni 1992. – RT 1992, 26, 349 ... RT I, 27.04.2011, 2
32. Euroopa inimõiguste ja põhivabaduste kaitse konventsioon. 4. november 1950.
33. Euroopa Liidu põhiõiguste harta. 7. detsember 2000.
34. Euroopa Parlamendi ja nõukogu 17.11.2003. a direktiiv 2003/98/EÜ avaliku sektori valduses oleva teabe taaskasutamise kohta. – ELT L 345, 31.12.2003, lk 1-6.
35. Euroopa Parlamendi ja nõukogu 23.07.2013. a direktiiv 2013/37/EL, millega muudetakse direktiivi 2003/98/EÜ avaliku sektori valduses oleva teabe taaskasutamise kohta. – ELT L 175, 27.06.2013, lk 1-8.
36. Euroopa Parlamendi ja nõukogu 24.10.1995. a direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. – ELT L 281, 23.11.1995, lk 1-19.
37. Isikuandmete kaitse seadus. 15. juuni 2007. – RT I 2007, 24, 127 ... RT I, 30.12.2010, 11
38. Karistusseadustik. 06. juuni 2001. – RT I 2001, 61, 364 ... RT I, 26.02.2014, 6
39. Kriminaalmenetluse seadustik. 12. veebruar 2003. – RT I 2003, 27, 166 ... RT I, 26.02.2014, 8
40. Kriminaaltoimiku arhiivimise kord ja säilitamise tähtajad. VVm 30.07.2004 nr 261. – RT I 2004, 60, 430 ... RT I, 02.09.2011, 5
41. Maa-, haldus- ja ringkonnakohtu kantselei kodukord. JMm 22.12.2005 nr 57. – RTL 2005, 124, 1973 ... RT I, 29.11.2013, 15

KASUTATUD KOHTUPRAKTIKA

42. ECJ Compass Case, C-138/11, *Compass Datenbank GmbH versus Austria.*
43. EIKo 26.03.1987, 9248/81 *Leander versus Sweden.*
44. EIKo 25.02.1997, 22009/93 *Z versus Finland.*
45. EIKo 16.02.2000, 27798/95 *Amann versus Switzerland.*
46. EIKo 21.03.2000, 28389/95 *Rushiti versus Austria.*
47. EIKo 04.05.2000, 28341/95 *Rotaru versus Romania.*
48. EIKo 29.04.2002, 2346/02 *Pretty versus United Kingdom.*
49. EIKo 07.02.2002, 53176/99 *Mikulic versus Croatia.*
50. EIKo 22.07.2003, 24209/94 *Y.F. versus Turkey.*
51. EIKo 11.01.2005, 50774/99 *Sciacca versus Italy.*
52. EIKo 10.12.2008, 30562/04 *and* 30566/04 *S and Marper versus United Kingdom.*
53. RKHKo 12.06.2012, 3-3-1-3-12.
54. RKKKo 05.04.2012, 3-1-1-25-12.
55. EIKo 13.11.2012, 24029/07 *M.M. versus United Kingdom.*
56. EIKo 04.06.2013, 7841/08 and 57900/12 *Peruzzo and Martens versus Germany.*
57. EIKo 18.04.2013, 19522/09 *M.K. versus France.*
58. RKÜKo 22.03.2011, 3-3-1-85-09.
59. RKKKo 23.02.2009, 3-1-1-81-08.

MUUD MATERJALID

60. Article 29 Data Protection Working Party. Opinion 4/2007 on the concept of personal data. 20.06.2007 WP 136 pp 1-26. Kättesaadav: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf (04.05.2014).
61. Article 29 Data Protection Working Party. Opinion 6/2013 on open data and public sector information (PSI) reuse. 05.06.2013 WP 207 pp 1-28. Kättesaadav: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp207_en.pdf (04.05.2014).
62. Article 29 Data Protection Working Party. Opinion 7/2003 on the re-use of public sector information and the protection of personal data – Striking the balance. 12.12.2003 WP 83 pp 1-11. Kättesaadav: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp83_en.pdf (05.05.2014).
63. Commission of the European Communities, Brussels 20.01.1999. Public sector information – a key resource for Europe. COM (1998) 585 final.
64. Digital Agenda for Europe. A Europe 2020 Initiative. Kättesaadav: http://ec.europa.eu/digital-agenda/en/pillar-i-digital-single-market/action-3-open-public-data-resources-re-use (14.04.2014).
65. Euroopa Andmekaitseinspektori arvamuse kokkuvõte, mis käsitleb Euroopa Komisjoni avatud andmete paketti, sealhulgas ettepanekut võtta vastu direktiiv, millega muudetakse direktiivi 2003/98/EÜ avaliku sektori valduses oleva teabe taaskasutamise kohta, avatud andmeid käsitlevat teatist ning komisjoni otsust 2011/833/EL komisjoni dokumentide taaskasutamise kohta. ELT C 335, 01.11.2012, lk 8-9.
66. Euroopa Ühenduste Komisjon. Nõukogu raamotsus. Ettepanek nr KOM (2005) 475 kriminaalasjadega seotud politsei- ja õigusalase oostöö raames töödeldavate isikuandmete kaitse kohta. Lk 1-39.
67. European Commission of Human Rights. Report of the Commission. 21.10.1992, 16213/90, *Burghartz versus Switzerland.*
68. European Commission of Human Rights. Report of the Commission. 31.01.1995, 15225/89, *Friedl versus Austria.*
69. Hansen, T. Õigus eraelu puutumatusele vs. kohtulahendi avalikustamine. Magistritöö. Juhendajad Ernits, M. Aaviksoo, B. Tartu Ülikool, õigusteaduskond, riigi- ja haldusõiguse õppetool. 2012.

70. Juhend kriminaal- ja väärteomenetluses kogutud teabe avaldamiseks pärast menetluse lõpetamist. Kättesaadav: https://www.kapo.ee/est/avalik-teave/isikuandmete-kaitse (15.04.2014).
71. Kaitsepolitseiamet. 25.03.2014 vastus teabepäringule. Magistritöö lisa nr 1.
72. Kohtute haldamise nõukoda. Õigusemõistmise avalikkus versus isiku õigus eraelu puutumatusele. Kättesaadav: http://www.riigikohus.ee/?id=329 (15.04.2014).
73. Organization for Economic Cooperation and Development: Guidelines governing the protection of privacy and transborder flows of personal data (OECD Guidelines) 1980.
74. Politsei- ja Piirivalveamet. 20.03.2014 vastus teabepäringule. Magistritöö lisa nr 5.
75. Politsei- ja Piirivalveamet. Isikuandmete töötlemise üldpõhimõtted. Kättesaadav: https://www.politsei.ee/et/organisatsioon/isikuandmete-tootlemise-uldpohimotted.dot (15.04.2014).
76. Politsei- ja Piirivalveamet. Kriminaaltoimikute arhiveerimise juhend. Magistritöö lisa nr 4.
77. Registrite- ja Infosüsteemide Keskus. 29.04.2014 vastus teabepäringule. Magistritöö lisa nr 6.
78. UK Information Commissioner's Office web page. Data protection. Kättesaadav: http://ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation (29.04.2014).
79. Working Party on the protection of individuals with regard to the processing of personal data. Opinion No 3/99 on Public Sector information and the protection of personal data. 03.05.1999 WP 20 pp 1-12.
    Kättesaadav:
    http://ec.europa.eu/justice/dataprotection/article29/documentation/opinion-recommendation/files/1999/wp20_en.pdf (04.05.2014).
80. Väljavõte Kaitsepolitseiameti vastusest eraisikule. Magistritöö lisa nr 2.
81. Väljavõte prokuratuuride asjaajamiskorrast. Magistritöö lisa nr 3.

Andmekaitse inspektsiooni lahendid

82. Andmekaitse inspektsiooni 29.01.2010 vaideotsus eraisik/Tartu Ringkonnakohus. Magistritöö lisa nr 7.
83. Andmekaitse inspektsiooni 04.03.2011 vaideotsus eraisik/Pärnu Maakohus. Magistritöö lisa nr 8.
84. Andmekaitse inspektsiooni 27.05.2013 ettekirjutus-hoiatus Lasnamäe Linnaosavalitsus, isikuandmete kaitse asjas. Kättesaadav: http://www.aki.ee/et/ettekirjutused-2013 (05.05.2014).
85. Andmekaitse inspektsiooni 27.12.2013 vaideotsus AS PR Põhjarannik/Tallinna Halduskohus. Kättesaadav: http://www.aki.ee/et/vaideotsused-2013 (05.05.2014).
86. Andemkaitse inspektsiooni 25.02.2014 vaideotsus eraisik/Politsei- ja Piirivalveamet. Kättesaadav: https://www.aki.ee/et/vaideotsused-2014 (05.05.2014).

LISAD

Lisa 1

Marit Konks	Teie 19.03.2014 nr	
marit.konks@gmail.com	Meie 25.03.2014	nr 10-AT

Vastus

Kaitsepolitseiameti arhiivi juhendi järgi peavad arhiivi antavad kriminaaltoimikud vasta justiitsministri 16.07.2008.a. määruse nr 39 "Kriminaalasja kohtueelse menetluse dokument näidisvormide kehtestamine" nõuetele. Kriminaaltoimikute säilitamise tähtajad on kehtestatud dokumentide loeteluga. Riigisaladuse ja salastatud välisteabe seadusest tulenevalt on kehtestatud juurdepääsupiira Kaitsepolitseiameti arhiivi juhendile ja dokumentide loetelule.

Lugupidamisega /allkirjastatud digitaalselt/ Eha Prunt
büroojuht

Lisa 2

KAITSEPOLITSEIAMET

Teabenõudele vastus

Kriminaalmenetluses kogutud teabe pärast kriminaalmenetluse lõppu avaldamise praktika ühtlustamiseks on 2009.a koostanud Andmekaitse Inspektsioon ja Riigiprokuratuur ühise selgituse uurimisasutustele ning väärtegude kohtuvälistele menetlejatele, mis on leitav aadressil: http://www.aki.ee/est/?part=html&id=125.

1. Teie küsimusele kas süütuks osutunud isiku kohta ning sealhulgas isiku kohta kelle suhtes on kriminaalmenetlus lõpetatud koostatud toimik või selle erinevad osad on avalikult kättesaadavad igale soovijale vastame, et:

-Demokraatliku riigikorralduse tagamiseks ning avaliku huvi ja igaühe õiguste, vabaduste ja kohustuste täitmise võimaldamiseks on teabevaldajad kohustatud tagama juurdepääsu nende valduses olevale teabele seaduses sätestatud tingimustel ja korras.

-Vastavalt AvTS-i §-le 3 lg 1 on avalik teave mis tahes viisil ja mis tahes teabekandjale jäädvustatud ja dokumenteeritud teave, mis on saadud või loodud seaduses või selle alusel antud õigusaktides sätestatud avalikke ülesandeid täites.

- Arhiveeritud kriminaalasjade materjalidega tutvumist reguleerib arhiiviseadus (ArhS) koosmõjus avaliku teabe seaduse (AvTS) ja isikuandmete kaitse seadusega(IKS).

- Kriminaalasi nr [redacted] on arhiveeritud Kaitsepolitseiametis. Kriminaalasja toimiku andmetest enamus ei sisalda delikaatseid isikuandmeid.

- Kriminaalasjas nr [redacted] arhiveeritud juurdepääsupiiranguga teabele on teabenõude alusel võimaldatud osaline juurdepääs avaliku teabe seaduses sätestatud korras arvestades isikuandmete kaitse seaduse nõudeid ning Andmekaitse Inspektsioon ja Riigiprokuratuur ühist selgitust. Kriminaalasjas nr [redacted] ei ole avalikustatud delikaatseid isikuandmeid.

- Kordame, et isikuandmete (ArhS § 42, IKS §§ 14, 16) edastamine või nendele juurdepääsu

võimaldamine andmete töötlemiseks kolmandale isikule on lubatud andmesubjekti nõusolekuta kui kolmas isik taotleb teavet, mis on saadud või loodud seaduses või selle alusel antud õigusaktides sätestatud avalikke ülesandeid täites ja taotletav teave ei sisalda delikaatseid isikuandmeid ning sellele ei ole muul põhjusel kehtestatud juurdepääsupiirangut. Kui otsustatakse lubada juurdepääs asutusesiseseks tunnistatud teabele, siis isikuandmete saamise õigus ilma andmesubjekti teavitamata tuleneb IKS § 14 lõikest 2.

2. Kaitsepolitseiamet vastab talle esitatud küsimustele vastavalt seaduses ettenähtud nõuetele ja piirangutele.

3. Teil on võimalik tutvuda kriminaalasja nr [redacted] materjalidega kokkuleppel Kaitsepolitseiametiga, (tel 6121400, 6121455) ning Teile võimaldatakse osaline juurdepääs kriminaalasja materjalidele arvestades seadustes nimetatud juurdepääsupiiranguid.

Lisa 3

V Ä L J A V Õ T E
Prokuratuuri asjaajamiskord

IX. KRIMINAALMENETLUSE MATERJALIDE ARVESTUS JA HOIDMINE

160. Kriminaalmenetluse materjalid registreeritakse e-toimiku süsteemis. Saatekirjade skaneerimine ja dokumendihaldusesse salvestamine ei ole kohustuslik, kui menetlust juhtiv prokurör ei otsusta teisiti. Vajadusel tehakse vastav märge dokumendihaldussüsteemis ja saadetakse prokurörile menetlus. Kantselei teeb saabumis- või väljastusmärke toimiku esilehe siseküljele ja edastab materjali koos asitõenditega tööjaotuskava-järgsele prokurörile, uurimisasutusele või kohtule.

160.[1] Kõikidel kriminaaltoimikutel on juurdepääsupiirang, mille määramisel lähtutakse avaliku teabe seadusest ja menetlusosaliste andmete kaitset reguleerivates seadustes sätestatust.
160.[2] Menetlust juhtiva prokuröri otsusega Kriminaalmenetluse seadustiku § 223 lg 2 alusel kriminaalasjast välja võetud toimikut või originaaldokumenti säilitatakse kümme aastat alates kohtulahendi jõustumisest. Säilitustähtaja möödumisel hävitatakse eraldatud dokumendid vastavalt arhiivieeskirja nõuetele. Kriminaalasjast tervikköite eraldamisel lisatakse kriminaaltoimikusse eraldatud toimiku sisukorra koopia, eraldamisotsuse teinud prokuröri andmed ja kuupäev. Üksikdokumendi eraldamisel tehakse vastav märge kriminaaltoimiku sisukorda; vajadusel lisatakse toimikusse õiend, kuhu märgitakse eraldatud dokumendi pealkiri, leheküljenumbrid, eraldamisotsuse teinud prokuröri andmed ja eraldamise kuupäev.
160.[3] Kriminaalasjade arhiivtehnilise arvestuse huvides viiakse Riigiprokuratuuri dokumentide loetelus sisse sari/sarjad kriminaalmenetluse materjalide hoidmiseks ja säilitamiseks (nt „Kriminaalasjast eraldatud materjalid“, „Prokuratuuris uuritud ja lõpetatud kriminaalasjad“ vms). Ringkonnaprokuratuuridel on soovitav sisse viia vahesarjad, mille raames hoida materjale kuni hävitamiseni või üleandmiseni Riigiprokuratuuri arhiivi.

161. Kabinetist lahkudes ja töövälisel ajal hoitakse kriminaalmenetluse materjale ja nende koopiaid kõrvalistele isikutele kättesaamatus kohas lukustatud kapis. Kriminaalasja juurde kuuluvaid asitõendeid hoitakse õigusaktidega kehtestatud korras. Passe, töötõendeid, juhilubasid jm dokumente hoitakse kriminaaltoimikusse lisatud pitseeritud ümbrikus.

162. Menetlust juhtiv prokurör võib komplekteerida endale tööalaseks kasutamiseks nn kontrollmaterjalid ja koondada need eraldi kiirköitjasse. Kontrollmaterjale säilitamise vajaduse ja säilitusaja pikkuse otsustab kriminaalmenetlust juhtinud prokurör. Avalikkust huvitavad kontrollmaterjalid võib jätta alatiseks säilitamiseks, saates need koos selgitava taotlusega arhiivimiseks Riigiprokuratuuri üldtalitusele.

163. Kriminaalmenetluse materjale edastatakse käsi-, kuller- või tähtpostiga. Kriminaalasja saatekirjade trükkimine suhtluses eestisiseste tüüpadressaatidega (politsei, kohus, prokuratuur) ei ole kohustuslik. Saatekirjaga edastatakse toimikuid juhul, kui on vaja anda täiendavaid selgitusi, juhiseid vms.

164. Kriminaalmenetluse lõpetamisel edastatakse kriminaaltoimik pärast kaebetähtaja möödumist arhiivimiseks kohtueelse menetluse lõpuleviinud uurimisasutusele, v.a juhul, kui uurimist teostas ainuisikuliselt Prokuratuur.

164.[1] Täies mahus prokuratuuri poolt uuritud kriminaalmenetluse materjalid edastatakse arhiivimiseks Riigiprokuratuuri arhiivi, kus neid säilitatakse lõpetamisest 25 aastat. Avalikkust huvitavad või eeldatavalt ajaloolist väärtust omavad kriminaalasjad jäetakse alatisele säilitamisele ja antakse üle avalikku arhiivi.

164.[2] Üldmenetluses otsuse jõustumisel arhiivitakse kriminaaltoimik koos eraldatud materjalidega prokuratuuris ja toimikut säilitatakse kümme aastat alates kohtulahendi jõustumisest. Vajaduse möödumisel annab ringkonnaprokuratuur toimiku akti alusel edasiseks säilitamiseks või toimikule alatise säilitustähtaja määramiseks üle Riigiprokuratuuri arhiivi.
164.[3] Kriminaaltoimikust võetakse enne hävitamist välja isikut tõendavate dokumentide originaalid, mida säilitatakse prokuratuuri arhiivis 50 aastat või väljastatakse need allkirja vastu dokumendi omanikule.

164.[4] Juurdepääsu prokuratuuris arhiveeritud lõpetatud kriminaaltoimikule otsustab menetlust juhtiv või kõrgemalseisev prokurör.

VII. DOKUMENTIDE ARHIIVTEHNILINE VORMISTAMINE, HOIDMINE, ÜLEANDMINE JA HÄVITAMINE

1. Arhivaalide loetelu koostamine ja elektroonilise registri pidamine

126. Toimikud, millega seotud asjaajamine on lõppenud, valmistatakse ette säilitamiseks DL-s neile kinnitatud tähtaegade alusel.

127. Olemi kindlakstegemise ning juurdepääsu tagamise vahendiks arhiivis on arhivaalide loetelud (lisa 19) ja nende alusel koostatud ühtne Prokuratuuri arhiiviregister. Arhivaalide loetelud koostatakse ringkonnaprokuratuuride kõikides struktuurüksustes igal aastal moodustunud arhivaalide kohta. Arhivaalide loetelu esitatakse Riigiprokuratuuri üldtalitusele elektrooniliselt 15. märtsiks.

128. Arhivaalid, failid ja muud üksused võetakse registris arvele kolme kuu jooksul pärast asjaajamisperioodi lõppu. Riigiprokuratuuri haldusosakonna üldtalituse arhivaar kannab kõik Prokuratuuri tegevuse käigus saadud ja loodud arhivaalid, failid ja muud üksused Prokuratuuri arhivaalid ühtsesse elektroonilisse registrisse ja esitab 01.aprilliks koondaruande arhivaalide liikumise kohta Riiklikule Arhiiviregistrile.

129. Arhivaalide loetelus loetletakse arhivaalid, failid või muud üksused dokumentide loetelus kehtestatud sarjade kaupa.
Arhivaalide loetelusse kantakse:
129.1 prokuratuuri ja struktuurüksuse nimetus ja tähis;
129.2 sarja tähis ja nimetus (dokumentide loetelu järgi);
129.3 toimiku või muu üksuse järjekorranumber ja pealkiri;
129.4 toimikute või muude üksuste hulk;
129.5 arhivaali või faili piirdaatumid;
129.6 märkuste lahtrisse kantakse kõik arhivaali või failiga tehtud toimingud (näit säilitamine failina, paberkandjal jne. Kui arhivaalid on hävitatud, märgitakse hävitamiseks eraldamise akti hindamisotsuse kuupäev, number ja hävitamise aeg).
=

2. Paberkandjal arhivaalide ettevalmistamine üleandmiseks ja säilitamiseks

130. Arhivaalid ja muud üksused, mille säilitustähtaeg ei ületa kümmet aastat, hoitakse ringkonnaprokuratuuri struktuuriüksuses dokumentide loeteluga vastavuses kuni hävitamiseks eraldamiseni. Arhivaalide hävitamiseks või üleandmiseks eraldamise korral tehakse arhiiviregistris märge arhivaalide väljumise kohta koos viitega hävitamis- või üleandmis-vastuvõtmisaktile. Arhivaalide hävitamiseni või Rahvusarhiivi üleandmiseks eraldamiseni hoitakse need arhiivis vastavuses arhiiviregistri ja arhivaalide loeteluga.

131. Arhiiviväärtusega ehk alatise ja pikaajalise säilitustähtajaga (üle 10 aasta) arhivaalid valmistatakse arhiivitehniliselt ette järgmiselt:
131.1 dokumendid võetakse registraatoritest, kiirköitjast või muust säilitamiseks mittesobivast ümbrisest välja;
131.2 liigsed koopiad ja mittearhiiviaines eraldatakse ning eemaldatakse metallkinnistid;
131.3 arhivaalid süstematiseeritakse kronoloogiliselt, tähestiku või kuupäevade järgi;
131.4 arhivaalid paigutatakse säilitamiseks sobivasse ümbrisesse ja kinnitatakse nii, et säiliks arhivaalide terviklikkus. Ümbris tähistatakse;
131.5 säiliku lehtede soovituslik arv toimikus on kuni 250 lehte;
131.6 säiliku esimene leht on säilikus olevate dokumentide nimestik. Viimasele lehele märgitakse lehtede arv säilikus, kuupäev ja säiliku koostaja nimi ning allkiri. Säilikud tähistatakse;
131.7 avaliku arhiivi nõudel lehed nummerdatakse;

132. Tähistamiseks märgitakse toimikule, karbile vm ümbrisele vähemalt järgmised andmed:
132.1 arhiivimoodustaja, struktuuriüksuse ja sarja nimi - kui nimetus on aasta kestel muutunud, kantakse säiliku kaanele mõlemad nimetused.
132.2 asjaajamisindeks või -tähis;
132.3 pealkiri;
132.4 säiliku piirdaatumid;
132.5 tähis arhivaalide loetelu järgi (selle märgib Riigiprokuratuuri arhivaar).

3. Paberkandjal arhivaalide üleandmine avalikku arhiivi

133. Arhiiviväärtusega ja pikaajalisele säilitamisele kuuluvad arhiivitehniliselt ettevalmistatud säilikud antakse hiljemalt seitsme aasta jooksul pärast toimikute lõpetamist asjaajamises üle Riigiprokuratuuri arhiivi. Korrastusüksuste valikul ja nendevaheliste seoste kindlaksmääramisel arhiiviskeemis lähtutakse Prokuratuuri struktuurist, Prokuratuurile pandud ülesannetest ning arhiivi suurusest ja koosseisust.

134. Arhiiviväärtusega arhivaalide Rahvusarhiivi üleandmise kohustus tekib 20 aastat pärast arhiiviväärtusega arhivaali tekkimist ja temaga seotud asjaajamise lõppemist. Üleandmine toimub viie aasta jooksul pärast üleandmise kohustuse tekkimist poolte kokkuleppel kindlaksmääratud tähtajal. Prokuratuuri põhjendatud taotluse alusel võib riigiarhivaar pikendada asutuse ülesannete täitmiseks vajalike arhivaalide üleandmise tähtaega kuni 20 aastat.

135. Arhivaalide Rahvusarhiivi üleandmiseks ettevalmistamisel koostab Riigiprokuratuuri arhivaar arhivaalide korrastamiseks ja kirjeldamiseks arhiiviskeemi. Arhiiviskeem kooskõlastatakse Rahvusarhiiviga.

Arhiiviskeem täpsustab või määrab kindlaks arhivaalide rühmitamise arhiivideks, sarjadeks ja nende alljaotusteks. Arhiiviskeemi tegemisel lähtutakse nii dokumentide kui arhivaalide loetelust, arvestades tegelikult ladestunud arhiiviväärtuslikuks hinnatud sarju.
Arhiivi tervikkirjeldus koostatakse kolmeosalisena:
135.1 arhiivimoodustaja kirjeldus
135.1.1 moodustaja nimi või nimed
135.1.2 tegevusaeg ja koht
135.1.3 staatus, ülesanded ja tegevusalad
135.1.4 struktuur
135.1.5 kirjelduse andmed

136.2 arhiivi ja selle koostisosade kirjeldus sarjatasandini – ülevaate andmine asutuse käigus tekkivate arhivaalide kogumi kohta.
136.2.1 tähis ja pealkiri
136.2.2 piirdaatumid
136.2.3 kogus
136.2.4 moodustaja
136.2. 5 hoiustaja ajalugu
136.2.6 sisu ja teema
136.2.7 hindamine ja hävitamine
136.2.8 korrastamissüsteem

136.3 sarja, säiliku ja arhivaali kirjeldamine

137. Arhivaalide üleandmiseks Rahvusarhiivi esitab Riigiprokuratuuri haldusosakonna üldtalitus taotluse, kus on märgitud viide arhivaalide üleandmise aluseks olevale seadusesättele, arhiivimoodustaja nimi, arhivaalide tüüp ja liik, säilikute arv, kehtivad juurdepääsupiirangud, muu dokumentatsioon.

138. Rahvusarhiivi antakse arhivaalid üle Riigiprokuratuuris koostatud üleandmise-vastuvõtmise aktiga (lisa 20). Enne arhivaalide üleandmist teostatakse olemikontroll. Arhiiviväärtusega arhivaalid antakse Rahvusarhiivile üle nimistu (lisa 21) alusel. Nimistu on säilikute süstematiseeritud loetelu koos säiliku järjekorranumbri, indeksi, pealkirja, lehtede arvu ning piirdaatumitega. Nimistu kohustuslikud osad on tiitelleht, sisukord, lühendite nimekiri, moodustaja kirjeldus, arhiivi ja selle osade kirjeldused ning nimistuplangid.
Nimistu allkirjastavad Riigiprokuratuuri haldusosakonna üldtalituse juhataja ja arhivaar ning selle kinnitab Rahvusarhiiv.

4. Digitaaldokumentide säilitamine

139. Digitaalselt hoitava dokumendi puhul peab olema määratud sari, millesse dokument vastavalt dokumentide loetelule kuulub. Digitaaldokumendid salvestatakse säilivuskindlale kandjale ja formaadis, mis tagab säilimise ja autentsuse vähemalt dokumendiliigile kehtestatud säilitustähtaja jooksul.

140. Üle 10-aastase säilitustähtajaga digitaaldokumendid, mis arhiiviväärtust ei oma, võib anda säilitamiseks Rahvusarhiivi.

141. KEHTETU (02.11.2010 RP-1-2/10/45)

142. Enne dokumentide ainult digitaalsele säilitamisele üleminekut peavad olema tagatud dokumentide arhiveerimiseks ja säilitamiseks vajalikud tingimused neile kehtestatud tähtaja jooksul.

5. Digitaalarhivaalide üleandmine avalikku arhiivi

143. Digitaalarhivaalid antakse avalikku arhiivi elektrooniliselt loetaval kandjal, milleks on ühekordseks salvestamiseks mõeldud kompaktplaat (*CD).* Avaliku arhiivi nõudmisel esitatakse arhivaalid ka paberile väljatrükituna. Digitaalarhivaalid antakse avalikku arhiivi üle tihendamata ja krüpteerimata kahe identse eksemplarina.

144. Digitaalarhivaal antakse avalikku arhiivi tarkvaraplatvormist ja kindlast rakendustarkvarast sõltumatus või avatud vormingus. Vajaduse korral viiakse arhivaalid sobivasse vormingusse enne üleandmist. Vormingu tüüp ja konverteerimisprotseduurid otsustab avalik arhiiv kooskõlastatult prokuratuuriga.

145. Üleantav digitaalarhivaal peab olema ühes järgmistest vormingutest:

145.1 Standard Generalized Markup Language (SGML), sealhulgas World Wide Web Consortium'i (W3C) soovitustele vastav Extensible Markup Language (XML);

145.2 Portable Document File Format (PDF);

145.3 standarditele vastav lihttekst - üleantavates tekstifailides kasutatakse 8-bitiseid märgikoode *Latin-1 ISO 8859-1* või *Latin-9 ISO 8859-15*. Mitte-eestikeelsete tekstide puhul on lubatud kasutada *UTF-8 (Unicode) ISO 10646* märgikoodi.

145.4 Tagged Image File Format (TIFF);

145.5 Portable Networks Graphics (PNG).

146. Tabelid konverteeritakse andmevälja varieeruva pikkusega (kuni 2048 sümbolit) lihttekstiks koos andmevälja eraldajaga, milleks on etteantud sümbol. Üldjuhul salvestatakse andmebaaside tabelitevahelised seosed säilitamiseks *Structured Query Language*'is (SQL) ja lihtteksti kujul. Erandid kooskõlastatakse avaliku arhiiviga.

6. Arhivaalide kasutamine

147. Prokuratuuri ametnikel on õigus oma teenistusülesannete täitmiseks laenutada arhivaale ja muid dokumente (v.a õigusaktide originaalid, millega saab tutvuda kohapeal). Laenutamine registreeritakse. Eraisikutele arhivaale ja muid originaaldokumente ei laenutata. Vajadusel väljastab kantseleitöötaja tõestatud koopiad või võimaldatakse materjaliga tutvuda kohapeal. Toimikust laenutamiseks väljavõetava dokumendi asemele pannakse selle tõestatud koopia. Kui originaaldokument tagastatakse, pannakse see toimikusse oma kohale ja koopia hävitatakse.

148. Teiste riigiasutuste või juriidiliste isikute nõudmisel väljastatakse arhivaale ja muid dokumente kirjaliku taotluse alusel. Nõutud arhivaalid või muud dokumendid väljastatakse kaaskirjaga, kus märgitakse materjali tagastamise tähtaeg ja dokumendi/arhivaali identifitseerimiseks vajalikud andmed (indeks, pealkiri, piirdaatumid). Laenutatud arhivaalid edastatakse adressaadile tähitult või käsiposti teel.

149. Salastatud teabekandjaid ja kehtivaid juurdepääsupiiranguid sisaldavaid arhivaale ei laenutata. Selliste dokumentide kohta tehtud päringutele vastab ainult selleks volitatud töötaja. Isikuandmeid sisaldavale arhivaalile võimaldatakse kolmandal isikul juurdepääs ainult andmesubjekti kirjalikul nõusolekul. Pärast andmesubjekti surma on tema isikuandmeid sisaldavale arhivaalile juurdepääs andmesubjekti pärijal, abikaasal, lähisugulasel või nende

nõusolekul kolmandal isikul. Mitme õigustatud isiku olemasolul on andmesubjekti isikuandmeid sisaldavale arhivaalile juurdepääs lubatud neist ükskõik kelle nõusolekul, kuid igaühel neist on õigus nõusolek tagasi võtta. Nõusolekut ei ole vaja, kui andmesubjekti surmast on möödunud 30 aastat või arhivaalis sisalduvateks isikuandmeteks on üksnes andmesubjekti nimi, sugu, sünni- ja surmaaeg ning surma fakt.

150. Kantselei väljastab arhiivis säilitavate arhivaalide ja muude dokumentide alusel vastavalt päringutele teatisi või dokumentide tõestatud koopiaid. Teatisele kirjutab alla struktuuriüksuse juht ning vajaduse korral tõestatakse teatis kantselei pitseriga.

7. Arhivaalide hävitamiseks eraldamine ja hävitamine

151. Säilitustähtaja ületanud arhivaalide hävitamiseks eraldamise ettevalmistamisel koostab struktuuriüksuse kantselei arhivaalide hävitamiseks eraldamise akti (lisa 22) kavandi ja esitab selle Riigiprokuratuuri üldtalitusele. Arhivaalide hindamiseks läbiviimiseks esitab Riigiprokuratuuri arhivaar selle Rahvusarhiivile kooskõlastamiseks. Enne arhivaalide hävitamiseks eraldamist hindab Rahvusarhiivi vastava ala spetsialist kõiki Riigiprokuratuuri registris olevaid arhivaale (v.a Rahvusarhiivi poolt eelhinnatud dokumendid hindamisotsuse alusel).

152. Arhivaalide hävitamiseks eraldamise aktis märgitakse vähemalt järgmised andmed:
152.1 tähis dokumentide loetelu või muu arhiivi kooseisu loetleva dokumendi järgi;
152.2 sarja või arhivaalide nimetus või pealkiri;
152.3 piirdaatumid;
152.4 arhivaalide või muude üksuste hulk (kantakse hävitamiseks eraldamise akti summaarselt;
152.5 arhivaalide säilitustähtaeg;
152.6 viide õigusaktile, mis reguleerib arhivaalide säilitamist või hävitamist;
152.7 märge arhivaalide hävitamise aja, koha, hävitamise viisi ning hävitaja kohta;
152.8 Asjaajamise eest vastutava ametniku ning akti koostaja allkirjad.

153. Arhivaalide hävitatakse ühe kuu jooksul pärast hindamisotsuse saamist Rahvusarhiivist. Dokumentide loetelusse kantud arhivaale ilma hindamisotsuseta hävitada ei tohi. Kui ringkonnaprokuratuuril puudub võimalus arhivaale kohapeal hävitada, tuuakse need hävitamiseks Riigiprokuratuuri. Arhivaal hävitatakse teabekandja tüüpi ja arhivaalile kehtestatud juurdepääsupiiranguid arvestades kas füüsilise hävitamise teel (purustamine või põletamine) või teabe kustutamisega selle kandjalt.

154. Arhivaalide hävitamise ja Rahvusarhiivile üleandmise akte ja arhiivinimistuid säilitatakse alatiselt. Arhivaalide loetelusid säilitatakse arhivaalide hävitamiseni või üleandmiseni avalikku arhiivi.

Lisa 4

KINNITATUD
Politsei- ja Piirivalveameti
peadirektori 22.10. 2012. a.
käskkirjaga nr 377
Lisa 1

Politsei- ja Piirivalveameti
peadirektori 29. detsembri 2011
käskkiri nr 488
Lisa 1

Kriminaaltoimikute arhiveerimise juhend

1. Juhend kehtib kriminaaltoimiku (edaspidi toimik) arhiveerimisel (sarja tähis dokumentide loetelus 3.2-1).

2. Toimiku valmistab arhiivi üleandmiseks ette kas kriminaalasja menetlenud politseiametnik või vahetu juhi poolt selle ülesande saanud teenistuja.

3. Toimiku juurde võivad jääda paberalusel asitõendid, muude asitõendite säilitamine ja hävitamine toimub vastavalt kehtivale korrale, mis reguleerib asitõendite ja teiste ära võetud esemete ning konfiskeeritud vara käitlemist.

4. Toimik antakse arhiivi üle pärast kriminaalmenetluse lõpetamist uurimisasutuses või prokuratuuris. Toimikus peab olema menetluse lõpetamise määrus.

5. Toimik antakse arhiivi üle pärast kaebetähtaja möödumist, kuid mitte hiljem kui 6 kuu möödumisel pärast määruse koostamist ning see peab vastama justiitsministri määrusega kehtestatud nõuetele.

6. Kui pärast 01.01.1991 lõpetatud kriminaalasi puudutas avalikkuse erilist tähelepanu pälvinud sündmust või kriminaalasja menetlemisega kaasnes avalik huvi, siis menetleja:
6.1 koostab asutusesisese kirja (mis registreeritakse sarja 1.7-6) kriminaalasjale arhiiviväärtuse omistamise kohta;
6.2 kooskõlastab selle vahetu juhi ja vastavalt keskkriminaalpolitsei või kriminaalbüroo juhiga;
6.3 märgib pärast kooskõlastuse saamist lõpetatud toimiku kaanele säilitustähtaja järele „AV".

7. Arhiivi antakse dokumendid üle dokumendihaldussüsteemis (edaspidi DHS) registreeritud üleandmis-vastuvõtmisakti alusel.

8. Kriminaalasjade üleandmis-vastuvõtmisakti koostab üleandja. Aktis peab olema toimikuid üleandva struktuuriüksuse nimetus, üleantavate kriminaalasjade numbrid ja köidete arv, KrMS § 200[1] alusel lõpetatud kriminaalasja kuriteo raskusaste, avaldaja nimi, üleandja ja vastuvõtja nimi, ametinimetus, allkiri ning üleandmise kuupäev, vajadusel arhiiviväärtuse omistamise kirja registreerimisnumber. Akti võib täiendada muude vajalike andmetega.

9. Akt edastatakse DHSis arhiivitalituse teenistujale, akti number teatatakse toimikute üleandmisel vastuvõtjale.

10. PPA keskkriminaalpolitsei menetlusbüroo või prefektuuri kriminaalbüroo juht või nende poolt määratud teenistuja kannab toimiku kaane paremasse ülaserva märke AK, viidates AvTS § 35 lg 1 vastava(te)le punkti(de)le.

11. Arhiivis asuvate lõpetatud toimikutega on õigus tutvuda ja saada toimikuid ajutiseks kasutamiseks seoses teenistusülesannete täitmisega kirjaliku taotluse alusel, mis on registreeritud DHSis (sari 3.2-9) või allkirja vastu:
11.1 politseiasutuse teenistujatel;
11.2 kohtu-, prokuratuuri- ja Justiitsministeeriumi teenistujatel.

12. Politseiasutuse teenistujale väljastatakse toimik 30 kalendripäevaks. Kui toimikut on vaja pikemaks perioodiks, tuleb sellest arhiivi teatada enne tagastamistähtaja möödumist. Uus tagastamistähtaeg märgitakse nõudelehele/arhiivihalduspro grammi väljale „laenutustähtaeg".

13. Prokuratuurile väljastatakse toimik üldjuhul (kui tagastamistähtaeg ei ole määratud) 30 ja kohtule 90 kalendripäevaks. Kaaskirjas teatatakse säiliku tagastamistähtaeg, tagastamistähtaja pikendamise ning säiliku arhiiviarvelt äravõtmise tingimused.

14. Füüsiliste ja juriidiliste isikute (va p 10 toodud teenistujad) taotlused edastatakse kriminaalasja menetlenud struktuuriüksusele, toimiku tutvustamiseks annab loa vastava struktuuriüksuse juht. Toimikut tutvustab kriminaalasja menetlenud politseiametnik või struktuuriüksuse juhi poolt määratud teenistuja.

15. Toimik võetakse arhiivi arvelt ära DHSis (sari 3.2-7) registreeritud menetlustoimingute jätkamise kirjaliku teate alusel, mis on edastatud arhiivitalituse teenistujale. Saabunud teate alusel sisestatakse arhiivihalduspro grammi akti registreerimise lehele viide säiliku arhiivi arvelt äravõtmise kohta (asutuse nimetus, teatise registreerimise kuupäev ja number).

16. Toimikud (va punkt 6s toodud juhtudel) hävitatakse Rahvusarhiivi 07.10.2010 hindamisotsuse nr 418 alusel vastavalt dokumendihalduskorra nõuetele. Hävitamisaktile lisatakse hävitatud kriminaalasjade nimekiri.

17. Toimikuid märkega „AV" säilitatakse politseiasutuse arhiivihoidlas ja antakse avalikku arhiivi arhiivieeskirjas kehtestatud tähtaegadel ja korras.

Elvi Kopti
dokumendihaldusbüroo
arhiivitalituse juhtivspetsialist

Lisa 5

Politsei- ja Piirivalveamet
Administratsioon

Marit Konks

marit.konks@gmail.com

Teie 20.03.2014 nr

Meie 20.03.2014 nr 1.7-2/45332-6

Kriminaaltoimikute säilitustähtajad

Küsisite, millise korra, juhendi või muu dokumendiga on Politsei- ja Piirivalveametis määratud kriminaaltoimikute säilitustähtajad. Dokumentide/toimikute säilitustähtajad on määratud asutuse dokumentide loeteluga. Kehtiv Politsei- ja Piirivalve dokumentide loetelu on kinnitatud peadirektori 31.10.2012 käskkirjaga nr 396. Dokumendi säilitustähtaja määramise aluseks asutuse dokumentide loetelus võib olla õigusakt või selle puudumisel dokumendi kasutamise praktiline vajadus.

Juurdepääsupiirang AvTS § 35 lg 1 p 12 alusel on kehtestatud Teie päringule ja meie vastusele, et vältida Teie kui eraisiku e-posti aadressi avalikustamist.

Lugupidamisega

(allkirjastatud digitaalselt)

Elvi Kopti
administratsioon, dokumendihaldusbüroo, arhiivitalitus
juhtivspetsialist

Elvi Kopti 6123039; elvi.kopti@politsei.ee

Lisa 6

Tere

E-Toimiku pidamise põhimäärus asub siin https://www.riigiteataja.ee/akt/117112011005

Toon Teile välja mõne punktid

§ 13. E-toimiku süsteemi andmete säilitamise tähtajad

E-toimiku süsteemi sisestatud andmeid säilitatakse menetlusseadustikes ja nende alusel antud õigusaktides sätestatud korras.

Hetkeseisuga tähendab see seda, et menetlusandmed säilitatakse igavesti.

§ 22. E-toimiku süsteemi logid ja nende hoidmine

(1) Iga e-toimiku süsteemi tehtud päringu või kande kohta säilitatakse vähemalt järgmised andmed:
1) kasutaja ees- ja perekonnanimi ning isikukood;
2) põhisüsteem;
[RT I 2009, 40, 269 - jõust. 26.07.2009]
3) kuupäev ja kellaaeg.

(2) Logitud andmeid konkreetse menetluse kohta säilitatakse menetluse lõppemiseni, kui seadusest ei tulene teisiti. Muid logisid säilitatakse kolm aastat päringu või kande tegemisest arvates.

Tervitades

Lisa 7

KINNITAN
" " jaanuar 2010

Viljar Peep
Andmekaitse Inspektsiooni
peadirektor

Vaideotsus

29.01.2010, Tallinnas

Lähtudes avaliku teabe seaduse (edaspidi AvTS) § 45 lg-st 2 ja haldusmenetluse seaduse (edaspidi HMS) §-st 83, vaatas Andmekaitse Inspektsiooni (AKI) II järelevalveosakonna peainspektor Elve Adamson läbi eraisiku vaide Tartu Ringkonnakohtu (Kalevi 1, 50050 TARTU) tegevuse peale teabenõudele vastamisel.

Vaide esitaja põhjendused ja nõue

xx.xx.2009 esitas eraisik Tartu Ringkonnakohtule teabenõude, milles palus väljastada kriminaalasja 1-07-10625 otsuse xxxx ja xxxxx kriminaalasjas.

Vaide kohaselt edastas Tartu Ringkonnakohus xx.xx.2009 vastuse, milles teatas, et Viru Ringkonnaprokuratuur on esitanud kassatsiooniõiguse kasutamise soovi. Samal päeval edastas vaide esitaja uue teabenõude, milles märkis, et kuna kriminaalmenetlus oli avalik, siis peavad ka kõik kohtuotsused ja määrused olema avalikud.

Peale teabenõude täpsustamist selgitas Tartu Ringkonnakohus vastuses teabenõudele, et jõustumata kohtuotsuse koopia antakse kriminaalmenetluse seadustiku (KrMS) §-st 317 tulenevalt ainult kohtumenetluse poolele, kelleks KrMS § 17 lõike 1 kohaselt on prokuratuur, süüdistatav ja tema kaitsja ning kannatanu. Kuna vaide esitaja ei ole kohtumenetluse pool, siis tekib tal kohtuotsusega tutvumise õigus peale kohtuotsuse jõustumist ja avalikustamist KrMS § 408^1 sätestatud korras.

Vaide esitaja leiab, et KrMS §317 käsitleb menetlusosaliste teavitamist ja ei reguleeri teabenõuetele vastamist.

Vaide esitaja palub teha Tartu Ringkonnakohtule ettekirjutus Tartu Ringkonnakohtu otsuse 1-07-10625 väljastamiseks vaide esitaja elektronposti aadressile eraisik@xxxx.ee.

Tartu Ringkonnakohtu selgitused:

Tartu Ringkonnakohtu selgituste kohaselt palus eraisik teabenõude korras väljastada talle kohtulahend kriminaalasjas 1-07-10625, kuna tal ei olevat võimalik vastava lahendiga tutvuda kohtulahendite registris (KIS-s).

Tartu Ringkonnakohus keeldus tulenevalt KrMS § 317 lg 1 teabenõudjale märgitud lahendit väljastamast, kuna eraisik ei ole nimetatud kohtuasjas menetlusosaline.

Tartu Ringkonnakohus on selgitanud, et soovitud kohtulahendile on kehtestatud juurdepääsupiirang vastavalt AvTS § 28 lg 1 p-le 29 ja KrMS § 408' lg 1 alusel nende vastastikuses koostoimes. Eelpoolmainitud sätete kohaselt on teabevaldaja kohustatud avalikustama jõustunud kohtulahendid seadusest tulenevate piirangutega. Kuna käesoleva teabenõude puhul oli tegemist jõustumata kohtulahendiga, siis ei olnud märgitud lahend avalikustatud ka kohtulahendite registris ja teabenõudena talle juurdepääsuõigust ei olnud tekkinud.

Tartu Ringkonnakohus leiab, et ükski seadus ei sätesta jõustumata kohtulahendite avalikkust isikute osas, kes ei ole kohtumenetluse pooled. KrMS § 315 lg 5 p 1 ja § 317 lg 1 sätestavad üheselt ainult kohtumenetluse pooltele kohtuotsuse juurdepääsu korra ja viisi. KrMS § 408 [1] lg 1 näeb ette, et vaid jõustunud kohtulahendid avalikustatakse selleks ettenähtud kohas arvutivõrgus. Ka AvTS § 28 lg 1 p 29 kohaselt on teabevaldaja kohustatud avalikustama vaid jõustunud kohtuotsused seadusest tulenevate piirangutega. Seega ei ole teabevaldaja kohustatud väljastama jõustumata kohtulahendeid isikutele, kes ei ole kohtumenetluse pooled.

Huvi kohtulahendite suhtes saab liigitada avalikkuse huviks ja isiklikuks huviks. Meediaväljaannete roll on esindada avalikkuse huvi. Kuna avalikust internetist on kättesaadavad vaid jõustunud kohtulahendid, siis jõustumata kohtulahendid eeldavad kättesaamiseks teabevaldaja poolt teabe väljastamist. Ainsaks AvTS-st tulenevaks motiiviks (kuid siiski mitte kohustuseks) jõustumata lahendi väljastamiseks saab olla avalikkuse huvi. AvTS § 30 lg 4 kohaselt on riigi- ja kohaliku omavalitsuse asutused kohustatud edastama ringhäälinguorganisatsioonidele või trükiajakirjandusele avalikustamiseks nende valduses oleva teabe sündmuste ja faktide kohta, mille puhul on eeldada avalikkuse huvi.

Põhiseaduse § 24 järgi on kohtuistungid üldjuhul avalikud ja kohtuotsused kuulutatakse avalikult, välja arvatud juhud, kui alaealise, abielupoole või kannatanu huvid nõuavad teisiti. See tähendab, et üldjuhul saavad kohtuistungitel viibida nii ajakirjanikud kui ka teised isikud. Kohtuistungite avalikkuse printsiip ei ole siiski samastatav jõustumata kohtulahendite dokumendina väljastamise kohustusega.

Kohtute Haldamise Nõukoja kinnitatud soovitused kohtute meediasuhtluseks ei ole kohustuslik regulatsioon, vaid soovituslik. Nimetatud dokument annab kohtutele soovitused suhtluseks ainult avalikkuse huvi esindavate ajakirjanikega, mitte aga kõigi isikutega. Oluline on siinkohal rõhutada, et praktilises kohtute meediasuhtluses väljastavad pressinõunikud üldjuhul ja valdavalt kokkuvõtlikku infot kohtumenetluse- ja lahendite, sh jõustumata kohtulahendite kohta. Jõustumata kohtulahendite, eriti motiveeritud terviklahendite seadusest tulenevate piirangutega dokumentidena väljastamine on kahtlemata kohtute meediasuhtluses oluliselt väiksema osakaaluga. Jõustumata kohtulahendite väljastamine ajakirjanikele kohtu poolt eeldab seda, et nad esindavad põhjendatud avalikkuse huvi, mitte isiklikku huvi.

Vastavalt PS §-le 149 on EV-s kehtiv kohtusüsteem kolmeastmeline.
Menetlusseadused annavad menetlusosalistele õiguse vaidlustada esimeses või teises kohtuastmes tehtud lahend. Igas kohtuastmes toimuv on küll iseseisev menetlus, mille tulemuseks on vastav kohtulahend, ometi ei ole see kohtuotsus või kohtumäärus käsitletav veel teabena, mis oleks avalikkusele mõeldud kasutamiseks vastavate kohturegistrite kaudu ning mittemenetlusosalistele kasutatav teabenõude korras ja seda seni, kuni kohtulahend on jõustunud.

Asjaolu, et lahend selle kuulutamisega koheselt ei jõustu, ei tähenda, et avalikkusel ei oleks õigust saada infot kohtus toimunust läbi meediakanalite. Küll on aga seadusandja piiranud kohute tegevust jõustumata kohtulahendite avalikustamisel mittemenetlusosalistele ja nende avalikustamisel kuni jõustumiseni vastavates registrites.

Kriminaalasjas 1-07-10625 esitas Viru Ringkonnaprokuratuuri 24.11.2009 teatise kassatsiooniõiguse kasutamise kohta ning kassatsiooni 22.12.2009, millest kohus on eraisikut ka informeerinud.

Tutvunud kogutud materjalidega leidis Andmekaitse Inspektsioon

Põhiseaduse § 44 sätestab igaühe õiguse saada vabalt üldiseks kasutamiseks levitatavat informatsiooni ja riigiasutuste, kohalike omavalitsuste ning nende ametiisikute kohustuse anda seaduses sätestatud korras Eesti kodanikule tema nõudel informatsiooni oma tegevuse kohta. Avalikule teabele juurdepääsu tingimused, kord ja viisid, juurdepääsust keeldumise ja juurdepääsu piiramise alused on sätestatud AvTS-is.

AvTS § 3 lg 1 kohaselt on avalik teave mis tahes viisil ja mis tahes teabekandjale jäädvustatud ja dokumenteeritud teave, mis on saadud või loodud seaduses või selle alusel antud õigusaktides sätestatud avalikke ülesandeid täites. AvTS eesmärgiks on tagada üldiseks kasutamiseks mõeldud teabele avalikkuse ja igaühe juurdepääsu võimalus, lähtudes demokraatliku ja sotsiaalse õigusriigi ning avatud ühiskonna põhimõtetest, ning luua võimalused avalikkuse kontrolliks avalike ülesannete täitmise üle. Seega peab teave, mille avalikustamist on igaühel AvTS alusel õigus nõuda, olema oma sisult ja olemuselt teabeks, mis on mõeldud üldiseks kasutamiseks. Teiseks iseloomujooneks nimetatud teabele on, et sellega tutvumise kaudu on avalikkusel võimalik kontrollida teabevaldajate poolt avalike ülesannete täitmist. Eeltoodust tulenevalt on teabevaldajad kohustatud demokraatliku riigikorralduse tagamiseks ning avaliku huvi ja igaühe õiguste, vabaduste ja kohustuste täitmise võimaldamiseks tagama juurdepääsu nende valduses olevale teabele seaduses sätestatud tingimustel ja korras (AvTS § 4 lg 1).

Juurdepääs teabele võimaldatakse teabevaldaja poolt vastavalt AvTS §-le 8, kas teabenõude täitmisega või teabe avalikustamisega. Teabenõue loetakse AvTS § 20 kohaselt täidetuks, kui teave on teabenõudjale seaduses sätestatud viisil edastatud või on selgitatud võimalust tutvuda avalikustatud teabega, samuti juhul, kui teabenõue on edastatud vastavalt kuuluvusele ja sellest on teabenõudjale teatatud.

AvTS näeb ette ka avalikule teabele juurdepääsu piiramise seaduses sätestatud korras. AvTS § 34 lg 1 kohaselt on piiratud juurdepääsuga teabeks teave, millele juurdepääs on seadusega kehtestatud korras piiratud, samas sätestab AvTS § 35 alused teabe asutusesiseseks kasutamiseks tunnistamiseks. AvTS § 38 lg 2 sätestab osalise teabe väljastamise võimaluse. Kui teabele juurdepääsu võimaldamine võib põhjustada juurdepääsupiiranguga teabe avalikuks tulemise, siis tagatakse juurdepääs üksnes sellele osale teabest või dokumendist, mille kohta juurdepääsupiirangud ei kehti (§ 38 lg 2).

AvTS-i kui üldseaduse tõlgendamisel tuleb teabele juurdepääsu võimaldamisel lähtuda ka eriseadustes sätestatud piirangutest. AvTS § 2 lg 2 p 4 sätestab üheselt, et AvTS-i ei kohaldata teabele juurdepääsupiirangute, juurdepääsu eritingimuste, korra ja viiside osas, juhul kui need on eriseaduses või välislepingus sätestatud teisiti. Käsitletava juhtumi puhul on

vaidemenetluse esemeks kriminaalmenetluses jõustumata kohtuotsus. Seega tuleb siinkohal vaadelda kriminaalmenetluse seadustiku sätteid (KrMS), milles on reguleeritud kuritegude kohtueelse menetluse ja kohtumenetluse kord ning kriminaalasjas tehtud lahendi täitmisele pööramise kord.

Põhiseaduse § 24 kohaselt on kohtuistungid avalikud. Kohus võib seaduses sätestatud juhtudel ja korras oma istungi või osa sellest kuulutada kinniseks. Kohtuotsus kuulutatakse avalikult, välja arvatud juhud, kui alaealise, abielupoole või kannatanu huvid nõuavad teisiti. Nimetatud põhiseaduse paragrahvis sisalduv väärtuste loetelu on kattuv KrMS §§-des 11 ja 12 toodud kohtuistungi ja kohtulahendi kuulutamise avalikkuse piiramise juhtude loeteluga. KrMS § 11 lg 2 kohaselt toimib avalikkuse põhimõte kohtulahendi kuulutamisel piiranguta, välja arvatud juhul, kui selle kuulutamist kinnisel kohtuistungil nõuavad alaealise, abielupoole või kannatanu huvid.

Põhiseaduse § 24 lg 4 lause teine pool sisaldab kataloogi põhjustega, millal tohib kohtuotsuse jätta avalikult kuulutamata. Siin on piiramisvõimalus tunduvalt kitsam, kuna kohtuotsuse tohib jätta avalikult kuulutamata ainult alaealise, abielupoole või kannatanu huvides. Need põhjused hõlmavad ainult kohtuotsuse kuulutamise kohtuistungil, milles mainitakse vastavaid isikuid nimeliselt. Piirata ei tohi aga kohtuotsuse kättesaadavust, kui selles on nimed asendatud tähtedega. Säärasel juhul kujutab kohtuotsus endast üldiseks kasutamiseks levitatavat informatsiooni põhiseaduse § 44 lg 1 tähenduses.

Vaide esitaja poolt teabenõudes taotletud kohtuotsus kuulutati vaide kohaselt välja piiranguteta. Kuigi KrMS § 315 lg 5 p 1 ja § 317 lg 1 sätestavad üheselt ainult kohtumenetluse pooltele kohtuotsusele juurdepääsu korra ja viisi, ei tähenda mainitud sätted veel automaatselt, et muudel isikutel puudub kohtuotsusele juurdepääsuõigus.

AvTS § 28 sätestab loetelu teabest, millise on teabevaldaja, tulenevalt AvTS § 29 lg-st 1, kohustatud aktiivses korras asutuse võrgulehel avalikustama. Tulenevalt AvTS § 28 lg 2 p-st 29 kuuluvad võrgulehel avalikustamisele jõustunud kohtuotsused. AvTS § 28 lg-s 1 toodud loetelu on vaid üks osa avalikust teabest, mille teabeavaldaja on kohustatud niiöelda omal initsiatiivil avalikustama. Ka KrMS § 408^1 lõige 1 sätestab jõustunud kohtulahendite avalikustamise nõuded, mitte teabenõuetele vastamise korra. Igaühe õigus üldiseks kasutamiseks mõeldud teabele ei piirdu ainult võrgulehel avalikustatud teabega tutvumisel. Igaühel on õigus nõuda juurdepääsu veel avalikustamata andmetele teabenõude täitmise kaudu. Teabe avalikustamine on teabevaldaja poolt seadusega sätestatud korras teabele juurdepääsu võimaldamine, ilma et selleks peaks teabenõuet esitama. Kui tegemist on informatsiooniga, mis on asutuse või ametiisiku valduses oleval infokandjal juba olemas, saab isik esitada teabenõude, mida menetletakse vastavalt AvTS-s sätestatud korrale.

Andmekaitse Inspektsioon leiab, et igaühe õigus üldiseks kasutamiseks mõeldud teabele ei piirdu ainult jõustunud kohtuotsuste avalikustamisega võrgulehel. KrMS ei ole AvTS-i suhtes jõustumata kohtuotsustele juurdepääsu osas tervikuna eriseaduseks. Seega tuleb päringuid, milles taotletakse juurdepääsu kohtuotsustele, sealhulgas ka jõustumata kohtuotsustele, menetleda AvTS-s sätestatud korra kohaselt- AvTS-is sätestatud tähtaja jooksul ja arvestades teabenõudja poolt märgitud teabe väljastamise viisi. Ka ei saa juurdepääsupiirangu aluseks olla AvTS § 28 lõige 1 punkt 29 ning KrMS 408^1 lõige 1, mis paneb teabevaldajale kohustuse avalikustada jõustunud kohtuotsused oma võrgulehel. KrMS § 317 lõige 1 sätestab aga kohtumenetluse poolte õigused, mitte kolmandate isikute õigused. Seega kui eriseadus ei sätesta kolmandate isikute õigusi, tuleb lähtuda AvTS-ist.

Riigikohus on avalikustanud oma võrgulehel http://www.nc.ee/?id=329 Kohtute Haldamise Nõukoja arvamuse „Õigusemõistmise avalikkus versus isiku õigus eraelu puutumatusele“, milles rõhutab, et jõustumata lahendid on kõigile kättesaadavad avaliku teabe seaduses ettenähtud teabenõude korras.

Eeltoodust lähtudes on Andmekaitse Inspektsioon seisukohal, et teabevaldaja on kehtestanud kohtuotsusele ebaseadusliku juurdepääsupiirangu ning on keeldunud ebaseaduslikult vaide esitaja xx.xx.2009 teabenõude täitmisest, rikkudes oma tegevusega AvTS § 9 lõige 2 punktis 1 sätestatud nõuet sellega, et ei võimaldanud juurdepääsu tema valduses olevale dokumendile, millele teabenõudjal oli juurdepääsuõigus.

Eeltoodut arvestades ning lähtudes HMS § 85 punktist 2, Andmekaitse Inspektsioon

otsustab:

1. **vaie rahuldada;**
2. **teha Tartu Ringkonnakohtule ettekirjutus – väljastada vaide esitaja e-posti aadressile Tartu Ringkonnakohtu otsus nr 1-07-10625, arvestades seadusest tulenevate piirangutega (KrMS § 408[1] lõiked 2-4).**

Ettekirjutuse täimise tähtaeg on 10.02.2010.

Vaideotsus teha teatavaks vaide esitajale ja Tartu Ringkonnakohtule
Järelevalvetulemus avalikustada Andmekaitse Inspektsiooni veebilehel.

Käesolevat vaideotsust on võimalik vaidlustada halduskohtumenetluse seadustikus sätestatud tingimustel ja korras halduskohtus.

Elve Adamson
peainspektor

Lisa 8

KINNITAN
" " märts 2011

/allkirjastatud digitaalselt/
Viljar Peep
Andmekaitse Inspektsiooni
peadirektor

Vaideotsus
04.03.2011, Tallinnas

Lähtudes avaliku teabe seaduse (edaspidi AvTS) § 45 lg-st 2 ja haldusmenetluse seaduse (edaspidi HMS) §-st 83, vaatas Andmekaitse Inspektsiooni (AKI) II järelevalveosakonna peainspektor Elve Adamson läbi eraisiku I (e-post: XXXX.XXXX@gmail.com) vaide Pärnu Maakohtu (Kuninga 22, 80099 Pärnu) Paide kohtumaja (Tallinna 18, 72711 Paide) tegevuse peale teabenõudele vastamisel.

RESOLUTSIOON:

Juhindudes haldusmenetluse seaduse § 85 punktist 2 ja 4 otsustas Andmekaitse Inspektsioon:

1. **Rahuldada vaie osas, mis puudutab kriminaalasja nr 1-213/1995 toimikuga tutvumisest keeldumise põhjendamist.**
2. **Teha Pärnu Maakohtule ettekirjutus – kohustada Paide kohtumaja üle vaatama kriminaaltoimikus 1-213/1995 olevad dokumendid ning võimaldada teabenõudjal tutvuda toimikuga selles osas, mis ei sisalda juurdepääsupiiranguga teavet. Juhul, kui toimik sellist teavet ei sisalda, siis põhjendada teabenõudjale arusaadavalt, miks ei ole võimalik ühegi toimikus oleva dokumendiga tutvuda ka osaliselt.**
3. **Jätta vaie rahuldamata teabenõudele vastamata jätmise osas, kuna menetluse käigus on Paide kohtumaja teabenõudjale vastanud.**
4. **Vaideotsus tehakse teatavaks vaide esitajale, Pärnu Maakohtule ja Pärnu Maakohtu Paide kohtumajale ning avalikustatakse Andmekaitse Inspektsiooni veebilehel.**

EDASIKAEBAMISE KORD:

Käesolevat vaideotsust on võimalik vaidlustada halduskohtumenetluse seadustikus sätestatud tingimustel ja korras halduskohtus.

Vaide esitaja põhjendused ja nõue

Vaide kohaselt edastas eraisiku I xx.xx.2010 Pärnu Maakohtule teabenõude, milles soovis tutvuda eraisik II tapmise kriminaaltoimiku ning kohtuotsusega. Xx.xx.2010 keeldus Pärnu Maakohtu Paide kohtumaja kriminaalasja toimikuga tutvumiseks võimaluse andmisest, kuna toimik sisaldab delikaatseid isikuandmeid kolmandate isikute kohta.

xx.xx.2010 edastas vaide esitaja Pärnu Maakohtu Paide kohtumajale täiendava teabenõude kriminaalasja toimikuga tutvumiseks, või kui keeldutakse kogu toimikuga tutvumise võimaldamisest (ka selle teabe osas, millele juurdepääsupiiranguid kehtestada ei saa), siis palus vaide esitaja keeldumist põhjendada.

Kuna xx.xx.2011 ei olnud xx.xx.2010 esitatud teabenõudele vastatud, siis edastas vaide esitaja samal päeval Pärnu Maakohtu Paide kohtumaja kantselei juhatajale ning kohtumaja juhile meeldetuletuse teabenõudele vastamata jätmise kohta koos koopiaga xx.xx.2010 esitatud teabenõudest. Kuni vaide esitamiseni ei ole Pärnu Maakohtu Paide kohtumaja vaide esitaja xx.xx.2010 ja xx.xx.2011 täiendavale teabenõudele vastanud.

Vaide esitaja leiab, et Pärnu Maakohtu Paide kohtumaja on rikkunud teabenõuete menetlemise korda, jättes teabenõuetele vastamata seaduses sätestatud tähtaja jooksul.

Vaide esitaja palub teha Andmekaitse Inspektsioonil Pärnu Maakohtu Paide kohtumajale ettekirjutus xx.xx.2011 esitatud teabenõude täitmiseks.

Pärnu Maakohtu selgitused:

Pärnu Maakohtu selgituste kohaselt ei vastanud Paide kohtumaja vaide esitaja xx.xx.2010. a teabenõudele, kuna eraisik I poolt oli Paide kohtumajale samasisuline teabenõue juba esitatud xx.xx.2010 ning teabenõudele vastati xx.xx.2010. Teabenõue täideti Paide kohtumaja arhivaari poolt xx.xx.2010 eraisikule I kohtuotsuste edastamisega posti teel. Pärnu Maakohus leiab, et kogu toimiku juurepääsupiirangut ei pea teabevaldaja põhjendama ning vastavasisulist põhjendust ei oleks pädev esitama kantselei juhataja, kellele xx.xx.2010. a eraisiku I e-kiri on adresseeritud. Sisuliselt oli xx.xx.2010. a eraisiku I kirja näol tegemist selgitustaotlusega, mitte teabenõudega AvTS § 14 tähenduses.

Vastavalt Pärnu MK Paide kohtumaja kantselei juhatajalt saadud selgitustele registreeriti xx.xx.2010. a Pärnu Maakohtu Paide kohtumajas sissetuleva dokumendina elektrooniline eraisiku I teabenõue 2-8/2/xxxx-xx, millega taotleti kriminaalasja kohtuotsusega ja toimikuga tutvumist. Vaatamata asjaolule, et nimetatud teabenõue ei vastanud avaliku teabe seaduse (edaspidi AvTS) §-s 14 sätestatud nõuetele (kohtule esitati ainult kannatanu nimi) asuti isikut abistama teabe saamisel.

Kohtul puudus 1995. a aastal elektrooniline andmebaas, kuid kohtutel oli kohustus pidada süüdistatavate nimeregistrit. Seetõttu otsiti läbi 1995. a nimeregister, otsides tapmise paragrahve, arhivaar sirvis läbi kõik kriminaaltoimikud ning leidis eraisiku I poolt küsitava.

Eraisiku I teabe saamise eesmärk tulenes vanavanaisa perekonnaloo uurimisest ning kuna eraisiku I näol on tegemist menetluses mitteosalenud isikuga, siis pöördus Paide kohtumaja kantselei juhataja xx.xx.2010. a teabenõudega loa saamiseks kohtuasja menetlenud kohtuniku poole, kuna menetluses mitteosalenud isiku juurdepääsu kohtutoimikule otsustab kohtu esimees, kohtudirektor või asja menetlenud kohtunik. Kohtunik kirjutas teabenõudele resolutsiooni xx.xx.2010. a, et lubab tutvuda kohtuotsusega.

xx.xx.2010.a. vastas Paide kohtumaja kantseleijuhataja eraisikule I elektrooniliselt, et kohtuasja menetlenud kohtunik otsustas anda võimaluse tutvuda kohtuotsusega kriminaalasjas nr 1-213/1995, kuid mitte toimikuga, kuna toimik sisaldab delikaatseid isikuandmeid kolmandate isikute kohta. Xx.xx.2010. a on posti teel saadetud arhivaari poolt eraisikule I nii Järva Maakohtu otsus, kui Tallinna Ringkonnakohtu otsus soovitud kriminaalasjas. Pärnu Maakohtu selgituste kohaselt luges Paide kohtumaja kohtuotsuse edastamisega teabenõude täidetuks.

xx.xx.2010. a registreeris Paide kohtumaja eraisiku I teabenõude nr 2-8/2/xxxx-xx, milles esitati sama taotlus kui xx.xx.2010. a teabenõudes. Kirja saabumise ajaks oli Paide kohtumaja poolt kohtuotsused eraisiku I aadressile postitatud, kuid arvestati asjaoluga, et xx.xx.2010. a e-kirja saatmise ajaks ei olnud posti teel saadetud otsused veel isikule kätte toimetatud.

Pärnu Kohtumaja märgib, et xx.xx.2010. a e-kiri on edastatud Paide kohtumaja kantselei juhataja tööalasele e-posti aadressile ja adresseeritud nimeliselt kantselei juhatajale ning vaatamata e-kirja teemas toodud märkele „teabenõue“, ei vasta kiri AvTS §-s 14 sätestatud nõuetele. Kiri sisaldab rohkelt viiteid avaliku teabe seadusele ning hõlmab isiku subjektiivseid arvamusi ja seisukohti. Kirja eelviimases lõigus toodud küsimustele vastamine ei mahu kantselei juhataja pädevusalasse. Seega on xx.xx.2010. a eraisiku e-kirja näol tegemist eelkõige selgitustaotlusega, millega isik soovib asutuse seisukohta või hinnangut.

Pärnu Kohtumaja leiab, et vastavalt AvTS § 45 lg-le 1 teostab Andmekaitse Inspektsioon teabevaldajate üle riiklikku järelevalvet nende poolt teabenõuete täitmisel ja teabe avalikustamisel. Kuna eraisiku I xx.xx.2010. a kirja näol ei ole tegemist teabenõudega avaliku teabe seaduse tähenduses, ei kuulu eraisiku I esitatud vaide lahendamine Andmekaitse Inspektsiooni pädevusalasse.

Täiendavalt on Pärnu maakohus selgitanud, et Pärnu MK kohtudirektori 06.02.2006. a käskkirja nr 1-6/15 „Pärnu Maakohtu dokumentide loetelu“ kohaselt on seatud kõigile kohtutoimikutel juurdepääsupiirang. Eeltoodust tulenevalt kehtib kõigi kohtutoimikute sh kriminaalasja nr 1-213/1995 toimiku osas juurdepääsupiirang, millest tulenevalt ei võimaldatud ka eraisikule I juurdepääsu kriminaalasja toimikule. Lisaks eeltoodule on küsitud ka täiendavalt luba kriminaalasja menetlenud kohtunikult, kes otsustas xx.xx.2010. a lubada tutvuda vaid kohtuotsusega, mitte kohtutoimikuga. Vastavasisulise loa andmise või loa andmisest keeldumise põhjendamine ei ole kohustuslik. Paide kohtumaja kantselei xx.xx.2010 a e-kirja kohaselt on kohtunik keeldunud toimikuga tutvumiseks loa andmisest, kuna toimik sisaldab delikaatseid isikuandmeid kolmandate isikute kohta. Nimetatud seisukoht ei olnud muutunud ka xx.xx.2010.a.

Pärnu Maakohtu Paide kohtumaja selgitused:

Pärnu Maakohtu Paide kohtumaja selgituste kohaselt ei tõlgendanud kohtumaja vaide esitaja xx.xx.2010.a. e-kirja teabenõudena, vaid kui teabenõude osalisest täitmisest keeldumisele järgnenud reageeringut kodaniku poolt, millega isik püüdis keeldumise üle järgi mõelda.

Kohtumaja täitis vaide esitaja teabenõude osaliselt xx.xx.2010.a. kohtuotsuse saatmisega posti teel, teabenõue oli esitatud xx.xx.2010.a., samal päeval saime kohtumaja juhilt ja ühtlasi kohtunikult, kes menetles antud kriminaalasja, loa teabenõuet täita sel moel, et isikul lubatakse tutvuda kohtuotsusega, mitte aga kriminaalasja toimikuga, kuna tegemist oli probleemse kohtualusega ja asjaoludega, mis ei kuulu kommenteerimisele. Kohtunik andis suulise kommentaari keeldumisele, tema sõnade kohaselt piisas antud teabenõude täitmiseks kohtuotsusest, kuna kõik antud kriminaalasja puudutavad asjaolud on kohtulahendis kirjas. Sellest tulenevalt pidas kohtumaja teabenõude täidetuks, xx.xx.2010 kohtuotsuse saatmisega.

Paide Kohtumaja selgituste kohaselt on eraisik I xx.xx.2010.a. pöördumine registreeritud dokumendiregistris teabenõudena, kuna antud elektronkirjal oli selline pealkiri. Hilisemal asjasse süvenemise selgus, et tegemist oli samasisulise nõudega, mis oli juba täidetud, kuna kohtuotsus saadeti teabenõudjale xx.xx.2010.a. Pärnu Maakohtu Paide kohtumajast välja. Toimikuga tutvumise nõudest kohus keeldus ja teavitas sellest ka kodanikku.

Kohtumaja keeldumine oli juba edastatud xx.xx.2010.a. meiliga eraisiku I meiliaadressile. Keeldumise kohtutoimikuga tutvumise kohta tegi Eesti Vabariigi kohtunik, mitte kantseleiametnik, mis aga tähendab, et kohtuniku arvamus on lõplik.

xx.xx.2010.a meili uue teabenõudena ei käsitlenud, kuigi meil kandis sellist pealkirja, kuna tegemist oli isiku täiendavate viidetega avaliku teabe seadusele ja ligipääsu võimaldavatele sätetele. Eraisik I saatis

järjekordse kirja xx.xx.2011 e-posti teel kantselei juhata meiliaadressile ja kohtuniku meiliaadressile, kus ta teatas, et on pöördunud AKI poole ning kirja lõppu oli kopeeritud ka xx.xx.2010.a e-kiri.

Paide kohtumaja selgituste kohaselt ei olnud kohtu arvates xx.xx.2011 pöördumise puhul tegemist teabenõudega, kuna:
-ei olnud teabenõudena esitatud;
-kodanik viitas jällegi sellel osale teabenõudest, mille osas täitmisest oli keeldutud kohtuniku poolt.
Kohus lähtus kohtuniku otsustusest keelduda toimikule ligipääsu võimaldamisest ning leidis, et pidevate ühesisuliste taotlustega püüdis teabenõudja mõjutada kohtuniku arvamust, mille ta oli andnud xx.xx.2010.a. Kohus täitis teabenõude lubatud piirides juba xx.xx.2010.a. ning samasisulisi e-kirju ei käsitlenud teabenõudena. Xx.xx.2010.a. meiliga andis kohtumaja teada, millises osas on nõue täidetav.

Paide kohtumaja on täiendavalt teavitanud, et registreeris xx.xx.2011.a., xx.xx.2011.a.saadetud elektronkirja tagantjärgi dokumendiregistris, kuid saabudes ei pidanud seda vajalikuks, kuna tegemist oli järjekordse e-kirjaga, mis ei ole esitatud teabenõudena, vaid eraisik I on oma eelnevad kirjad kokku kleepinud ning saatnud kohtuametnike nimelistele meiliaadressidele.

xx.xx.2011.a. edastas Paide kohtumaja täiendava selgituskirja asjaolude kohta eraisiku I meiliaadressile. Kriminaalasja toimik on KrMS § 160 alusel kriminaalasjas kogutud dokumentide kogum, mis tõendavad kohtualuse süüd, tegemist ei ole ühegi isiku ajalooliste elulooandmete kogumiga. Kohtuasja menetlenud kohtunik on leidnud, et teabenõude täitmiseks piisab kohtuotsuse saatmisest kodanikule, kuna otsus annab igakülgse ülevaate teo asjaoludest ja tõendite analüüsist. Teabenõude esitanud kodanik ei olnud kriminaalasja menetlusosaline, vaid väidetavalt kannatanu kaugelt sugulane, kes uurib oma sugupuud.

Kohtutoimikule ligipääsu võimaldamisest kohtunik keeldus ning see on lõplik kohtuniku seisukoht.

xx.xx.2011 on Paide kohtumaja edastanud täiendava selgituse Andmekaitse Inspektsioonile ja koopia vaide esitajale, milles märgib, et soovitud teabele kehtivad juurdepääsupiirangud ning teabenõudjal ei ole taotletavale teabele juurdepääsuõigust. Samuti on teabevaldaja selgitanud, et AvTS § 23 lõike 2 kohaselt on teabevaldajal õigus keelduda teabenõude täitmisest, kui füüsiliselt isikult taotletav teave ei käsitle avalike ülesannete täitmist.

Tutvunud kogutud materjalidega leidis Andmekaitse Inspektsioon

1. AvTS § 3 lg 1 kohaselt on avalik teave mis tahes viisil ja mis tahes teabekandjale jäädvustatud ja dokumenteeritud teave, mis on saadud või loodud seaduses või selle alusel antud õigusaktides sätestatud avalikke ülesandeid täites. Seega on kriminaalmenetluse käigus kogutud teave avalik teave ning teabele juurdepääsu võimaldamisel tuleb juhinduda peale otsuse jõustumist avaliku teabe seadusest, isikuandmete kaitse seadusest ja arhiiviseadusest.

AvTS § 35 lõige 1 punkti 1 kohaselt on teabevaldajad kohustatud tunnistama asutusesiseseks kasutamiseks mõeldud teabeks kriminaal- või väärteomenetluses kogutud teabe, välja arvatud vastavalt väärteomenetluse seadustikus ja kriminaalmenetluse seadustikus avaldatava teabe. Kuna kriminaal- ja väärteomenetluse seadustik reguleerivad teabele juurdepääsu õigusi ja võimalusi menetluse käigus kuni otsuse jõustumiseni, siis saab eeltoodud sätte alusel kehtestada juurdepääsupiirangu kuni otsuse jõustumiseni.

Tähelepanu väärib ka asjaolu, et avaliku teabe seaduse alusel on võimalik teabele kehtesta juurdepääsupiirang maksimaalselt 10 aastaks (AvTS § 40 lg 1) v.a eraelulise- ja delikaatsed isikuandmed (AvTS § 40 lg 3). Antud juhul on otsuse jõustumisest möödunud 15 aastat ning avaliku teabe seaduse jõustumisest 10 aastat. Seega saab juurdepääsupiirang käesoleval ajal üldjuhul olla vaid

isikuandmetele, mis kahjustavad oluliselt eraelu puutumatust või mida loetakse delikaatseteks isikuandmeteks.

Pärnu Maakohus on selgitanud, et Pärnu MK kohtudirektori 06.02.2006. a käskkirja nr 1-6/15 „Pärnu Maakohtu dokumentide loetelu“ kohaselt on seatud kõigile kohtutoimikutel juurdepääsupiirang. Eeltoodust tulenevalt kehtib kõigi kohtutoimikutele sh kriminaaltoimikutele juurdepääsupiirang.

AvTS § 41 lõike 1^1 sätestab, et asutuse juht kehtestab dokumentide loetelus sarjad, milles sisalduvatele dokumentidele võib juurdepääsupiirangud kehtestada. Konkreetsetele dokumentidele juurdepääsupiirangu kehtestamise otsustab asutuse juht või tema poolt määratud isik lähtudes dokumendi sisust ja juurdepääsupiirangu eesmärgist. Asutuse juht saab küll märkida dokumentide loetelus, et kohtutoimikud on juurdepääsupiiranguga, kuid lisada tuleb ka alused, mille alusel juurdepääsupiirangud kehtestatakse. Toimikutele juurdepääsupiirangute kehtestamine ei tähenda aga seda, et kõik toimikus olevad dokumendid on automaatselt juurdepääsupiiranguga. Juurdepääsupiiranguga saab olla siiski vaid teave, millel on piirangu kehtestamiseks alus. Seega tuleb teabenõude saamise korral toimik üle vaadata ning hinnata, millistele dokumentidele ja mis mahus piirang kehtib. Arvestada tuleb ka asjaoluga, et kuna antud juhul on kannatanu nimi teada, siis ei ole juurdepääsupiiranguga teabeks mitte ainult isiku nimi, vaid ka sündmusi kirjeldavad asjaolud, millest nähtuvad näiteks isiku kannatused. Samuti on juurdepääsupiiranguga teabeks teave, mille kaudu on võimalik teisi isikuid tuvastada.

Juurdepääsupiirangu alused on ära toodud AvTS § 35 ning valdkondade eriseadustes. Seega saab juurdepääsupiirangu kehtestada üksnes sellele osale teabest, millel on seadusest tulenev alus. Võib eeldada, et iga kriminaaltoimik sisaldab nii kannatanute, kui ka kolmandate isikute juurdepääsupiiranguga isikuandmeid, kuid see ei tähenda seda, et toimikuga ei oleks võimalik üldse tutvuda, kui toimik sisaldab dokumente, mida on võimalik osaliselt väljastada (kas kattes kinni juurdepääsupiiranguga teabe või kui mõni dokument ei sisalda isikuandmeid), siis tuleb see ka väljastada. AvTS § 38 lõike 2 kohaselt, kui teabele juurdepääsu võimaldamine võib põhjustada juurdepääsupiiranguga teabe avalikuks tulemise, siis tagatakse juurdepääs üksnes sellele osale teabest või dokumendist, millele juurdepääsupiirangud ei kehti. Seega on kohtul kohustus enne teabenõude täitmist teavet redigeerida. Juhul, kui ei ole võimalik ühelegi dokumendile juurdepääsu võimaldada (näiteks ka nimede kinni katmisel on muu teabe kaudu isikud tuvastavad), siis tuleb seda ka teabenõudjale arusaadavalt põhjendada. Põhjenduseks ei saa olla ainult, et toimik sisaldab juurdepääsupiiranguga isikuandmeid, kuna sellisest põhjendusest ei ole võimalik aru saada, miks ei väljastata teavet osaliselt, millele teabenõudja on ka viidanud.

Andmekaitse Inspektsioon ei nõustu Pärnu Maakohtu seisukohaga, et kogu toimikule juurdepääsupiirangut ei pea põhjendama. Kuna antud juhul oli tegemist teabenõudega, siis AvTS § 23 lõikest 3 tulenevalt peab teabevaldaja teabenõude täitmisest keeldumise koos põhjendusega teabenõudjale teatavaks tegema viie tööpäeva jooksul.

Tulenevalt eelnevast ei ole teabenõudjale edastatud vastustest arusaadav, mis põhjusel ei võimaldata soovitud toimikuga tutvuda selles osas, mis ei sisalda juurdepääsupiiranguga teavet, mida teabenõudja on oma teabenõudes ka selgesõnaliselt soovinud. Ka juhul, kui teabenõude täitmise üle otsustab kohtunik või kohtumaja juht, saab ta teabenõude täitmisest keeldumisel lähtuda ainult seadusest. Kuna antud juhul ei ole ühestki vastusest välja loetav, miks ei võimaldata toimikuga tutvuda ka osaliselt, siis ei saa Andmekaitse Inspektsioon anda hinnangut, kas toimikuga tutvumisest keeldumine oli kooskõlas seadusega või mitte.

2. Avaliku teabe seaduse kohaselt võib teabenõude esitada igaüks. Teabevaldaja ei saa eeldada, et teabenõudja teaks alati väga täpselt konkreetseid dokumentide andmeid, mida ta soovib. Avaliku teabe seaduse § 15 sätestab teabevaldaja kohustused teabenõudja abistamisel, et välja selgitada teabenõudja poolt soovitud teave, mida Paide kohtumaja on ka teinud. Õiguspärane ei ole aga vaide esitaja poolt xx.xx.2010 ja xx.xx.2011 edastatud pöördumistele vastamata jätmine ning xx.xx.2011 pöördumise

registreerimata jätmine. Kui kodanik edastab pöördumise, mitte asutuse üldisele e-posti aadressile, vaid ametniku e-posti aadressile, siis vastutab konkreetne ametnik pöördumise registreerimise ja vastamise eest. Ka juhul, kui Paide kohtumaja luges vaide esitaja täiendavaid pöördumisi selgitustaotluseks või oli seisukohal, et soovitud teave on teabenõudjale edastatud, ei anna see alust pöördumistele vastamata jätta. AvTS § 12 lõige 1 punkti 1 kohaselt tuleb kõik asutusse saabunud kirjad registreerida. Sama seaduse § 23 lõige 2 punkti 1 kohaselt võib teabevaldaja teabenõude täitmisest keelduda, taotletud teave on juba edastatud või kui tegemist on selgitustaotlusega (p 5). See aga eeldab isiku pöördumisele vastamist. Seadus ei anna võimalust jätta isikute pöördumised tähelepanuta ja vastuseta.

Ka juhul kui xx.xx.2010 edastatud pöördumise puhul oli teabevaldaja veendumisel, et soovitud teave ei ole teabenõudjani veel jõudnud, siis xx.xx.2011 edastatud meeldetuletuse puhul, millele oli lisatud ka xx.xx.2010 edastatud teabenõue, oli selgelt arusaadav, et isik soovis jätkuvalt kogu toimikuga tutvuda. Samuti palus teabenõudja, juhul kui toimikuga tutvuda ei võimaldata, keeldumist põhjendada, milleks kohustab ka seadus (AvTS § 23 lg 3).

Andmekaitse Inspektsioon ei saa ka nõustuda Pärnu Maakohtu seisukohaga, et tegemist ei olnud teabenõudega ning seega ei kuulu vaide lahendamine inspektsiooni pädevusse. Nii xx.xx.2010 kui xx.xx.2011 edastatud pöördumisest on selgelt arusaadav, et kohtuotsuste edastamine ei rahuldanud teabenõudjat. Samuti oli ka algses teabenõudes soov tutvuda kogu toimikuga. Teabenõudja on juhtinud kohtu tähelepanu asjakohastele seaduse sätetele ning palunud veelkord toimiku läbi vaadata ning teabenõue täita. Seega on selgelt arusaadav, et isik soovis jätkuvalt toimikuga (dokumenteeritud teabega) tutvuda, mis on käsitletav teabenõudena avaliku teabe seaduse mõistes.

Nii Õiguskantsler, kui Riigikohus on oma otsustes mitmel korral rõhutanud vajadust järgida hea halduse tava, mille kohaselt uurimisprintsiibist lähtudes tuleb taotluse, avalduse, kaebuse, pöördumise või muu tahteavalduse kvalifitseerimisel arvestada isiku tegeliku tahtega. Samamoodi tuleb talitada iga avaldusega, mille isik haldusorganile esitab: selgitada, kas sisuliselt on tegemist selgitustaotluse, märgukirja, teabenõude, vaide või taotlusega. Vajadusel tuleb pöörduda taotluse esitaja poole taotluse täpsustamiseks või püüda avaldusest enesest välja lugeda, mis eesmärgil isik avalduse esitas. Iga taotlust tuleb menetleda vastavalt selle tegelikule sisule ja eesmärgile, mida antud juhul tehtud ei ole.

Paide Kohtumaja on täiendavalt xx.xx.2011 ja xx.xx.2011 selgitanud toimikuga tutvumisest keeldumist. Nimetatud keeldumistest aga ei nähtu, miks ei ole võimalik toimikuga tutvuda selles osas, mis juurdepääsupiiranguga teavet ei sisalda või mille juurdepääsupiirang ei kehti, kattes eelnevalt kinni selle osa teabest, millele kehtib juurdepääsupiirang. Paide Kohtumaja on märkinud ka keeldumise aluseks AvTS § 23 lõige 2 punkti 2, mille kohaselt on teabevaldajal õigus keelduda teabenõude täitmisest, kui füüsiliselt ja eraõiguslikult juriidiliselt isikult taotletav teave ei käsitle avalike ülesannete täitmist. Andmekaitse Inspektsioon ei nõustu antud alusel teabenõude täitmisest keeldumisega, kuna antud juhul ei ole teabevaldajaks füüsiline ega eraõiguslik juriidiline isik, vaid kohus, mis on avalik-õiguslik juriidiline isik. Samuti on kohtutoimik koostatud avalikke ülesandeid täites ning toimikus sisalduv teave on avalik teave, millele saab juurdepääsupiiranguid kehtestada üksnes seadusest tulenevatel alustel. AVTS § 23 lõige 2 punkt 2 annab õiguse teabenõude täitmisest keelduda füüsilistel ja eraõiguslikel juriidilistel isikutel, kes täidavad avalikke ülesandeid, teabe osas, mis ei puuduta avalike ülesannete täitmist.

Tulenevalt eelnevast on Paide kohtumaja küll vaidlusalusele teabenõudele vastanud, kuid ei ole teabenõudjale arusaadavalt selgitanud toimikuga tutvumisest (ka osalise) keeldumise põhjuseid.

/*allkirjastatud digitaalselt*/

Elve Adamson
II järelevalveosakonna peainspektor

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, **Marit Konks,**
(*autori nimi*)

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose

Kriminaalmenetluses kogutud isikuandmete kaitse avaliku sektori teabe taaskasutamisel,
(*lõputöö pealkiri*)

mille juhendajad on **dr iur. Mario Rosentau ja Mari Männiko**,
(*juhendaja nimi*)

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

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

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

Tallinnas, **05.05.2014**