TARTU ÜLIKOOL

ÕIGUSTEADUSKOND

Avaliku õiguse instituut

Kriminaalõiguse, kriminoloogia ja kognitiivse psühholoogia õppetool

Julia Antonova

ISIKUANDMETE KAITSE KOHTUEELSES KRIMINAALMENETLUSES EESTIS

Magistritöö

Juhendaja: *MA* Sandra Mikli

Kaasjuhendaja: prof Jaan Sootak

Tartu

2015

SISUKORD

SISSEJUHATUS

Kriminaalmenetlus ja õigus privaatsusele - esmapilgul näib, et need kaks mõistet ei käi kokku. Üldteada fakt on, et kriminaalmenetluse raames sekkutakse ulatuslikult isikute erasfääri. Läbiotsimine, sõrmejälgede võtmine, jälitustoimingud on vaid mõned kriminaalmenetluses kasutatavad toimingud, mis on juba oma olemuselt riivavad intensiivselt privaatsust. Samal ajal näeb Eesti Vabariigi põhiseaduse[1] (*edaspidi PS)* § 26 ette igaühe õiguse perekonna- ja eraelu puutumatusele. Sarnase sätte leiab ka Euroopa Inimõiguste ja põhivabaduste kaitse konventsiooni[2] artiklist 8.

Tänapäeva kiiresti arenev digitaalmaailm annab isikule juurdepääsu piiramatule teabehulgale ning võimaldab erinevate tehnoloogiate abil teostada mistahes toiminguid ja tehinguid. Ühtlasi on oluliselt avardunud ka riigi võimalused hankida vajalikku teavet üksikisiku kohta ning uute tehnoloogiate kasutuselevõtt võimaldab õiguskaitseasutustel töödelda isikuandmeid kiiresti ning senisest oluliselt suuremas mahus. 2013. a suvel lahvatanud niinimetatud PRISM-programmiga seotud skandaal[3] tõi taas päevakorda arutelu selle üle, kuivõrd lihtne on riigil sekkuda isiku eraellu ning kuivõrd habras on piir õigustatud ja õigustamatu sekkumise vahel. Viimastel aastatel on isikuandmete kaitse valdkond olnud pidevalt fookuses ning valdkonnas on käimas mitmeid olulisi reforme. 2012. a jaanuaris avaldas Euroopa Komisjon kaks õigusakti ettepanekut, millega reformitakse Euroopa Liidus (*edaspidi EL*) seni kehtinud andmekaitsereeglid.[4] Muuhulgas hõlmab reform ka isikuandmete töötlemist kriminaalmenetluse valdkonnas[5] ning läbirääkimised vastava õigusakti ettepaneku üle ei ole

[1] Eesti Vabariigi Põhiseadus. - RT 1992, 26, 349 … RT I, 27.04.2011, 2.
[2] Inimõiguste ja põhivabaduste kaitse konventsioon. - RT II 2000, 11, 57.
[3] PRISM on Ameerika Ühendriikide (*edaspidi USA*) Riikliku Julgeoleku Agentuuri (NSA) andmehanke programm, mille kohaselt sai NSA piiramatu juurdepääsu selliste USA infotehnoloogiaettevõtete nagu Apple, Google, Facebook jt serverites asuvatele andmetele, sh näiteks isikuandmetele, kirjavahetusele, edastatud dokumentidele jm. PRISM-programmi avalikuks tuleks tekitas pahameelelaine nii USA-s kui EL-is, kuivõrd programm võimaldas NSA-l juurdepääsu ka EL-is asuvate andmesubjektide andmetele. Näiteks: NSA slides explain the PRISM data-collection program. - Washington Post, 10.07.2013.a Arvutivõrgus: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ (04.05.2015).
[4] Ülevaade EL andmekaitsereformist Euroopa Komisjoni veebilehel. Arvutivõrgus: http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm (04.05.2015).
[5] Euroopa Komisjon, 25.01.2012, COM (2012) 10 lõplik. Ettepanek: Euroopa Parlamendi ja Nõukogu direktiiv üksikisikute kaitse kohta seoses pädevates asutustes isikuandmete töötlemisega kuritegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumise kohta. Arvutivõrgus: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:ET:PDF (04.05.2015).

veel lõppenud.[6] Samuti on juba mitu aastat kestnud ning peatselt lõpusirgele jõudmas ka Euroopa Nõukogu andmekaitse konventsiooni[7] moderniseerimine.[8] Sellega seoses on isikuandmete kaitse temaatika viimasel ajal väga aktuaalne.

Riigi ülesanne on PS § 14 kohaselt tagada isikute põhiõiguste kaitse, sätestades selleks kohased menetlused ja õigusnormid. Muuhulgas on ka kriminaalmenetlus üks viise isikute põhiõiguste kaitseks. Kriminaalmenetluse kaudu teostavad pädevad asutused riiklikku sundi kuritegude uurimisel ja nende eest vastutusele võtmisel. Siinkohal põrkuvad kaks põhiõigust - PS §-is 26 sätestatud õigus eraelu puutumatusele ja PS §-s 13 reguleeritud õigus seaduse kaitsele. Põhiõiguste kollisioon on vältimatu, kuivõrd riigil on ühest küljest kohustus igaühele tagada seaduse kaitse, kuid teisest küljest hoiduda sekkumisest isiku eraellu.

PS §-st 26 tulenevalt on õigus eraelu puutumatusele igaühe õigus ning kriminaalmenetluse kontekstis peab eraelu puutumatus olema tagatud kõigile menetlusosalistele - nii kahtlustatavale, süüdistatavale, kannatanule, tsiviilkostjale kui kolmandale isikule. Ühtlasi võivad kriminaalmenetluses läbiviidavad toimingud riivata ka muude isikute õigusi, olgu selleks tunnistajad või kahtlustatavate perekonnaliikmed. Vaatamata sellele, milline on isiku menetlusõiguslik staatus, peavad pädevad asutused tagama isiku põhiõigusi, sh õiguse isikuandmete kaitsele.

Vastavalt PS §-le 11 ei ole põhiõigused üldjuhul absoluutsed. Põhiõiguste piiramisel on peamiseks mõõdupuuks vajalikkus demokraatlikus ühiskonnas. Teisalt ei tohi piirangud moonutada piiratavate õiguste ja vabaduste olemust.

Eelduslikult ei ole kohane vaidlus selle üle, kas riigil on vaja koguda üksikisikute kohta infot ning kas isikuandmeid on tarvis kasutada ka kriminaalmenetluses. Seega keskendub autor käesolevas töös sellele, kuidas on kriminaalmenetluses riigipoolne info töötlemine, sealhulgas info kogumine, ja säilitamine Eestis reguleeritud ning kas õiguslik regulatsioon on piisav, et tagada põhiseaduses sätestatud eraelu puutumatuse kaitse ning kooskõla Euroopa Liidu õigusest ja rahvusvahelistest kohustustest tulenevate nõuetega.

Tuginedes oma senistele teadmistele ning töökogemusele isikuandmete kaitse valdkonnas püstitab autor hüpoteesi, et üksikisiku õigus isikuandmete kaitsele ei ole kriminaalmenetluses

[6] Arvestades menetluse hetkeseisu võib eeldada, et direktiivi eelnõu läbirääkimised kestavad veel ligikaudu aasta. Vastuvõtmise järgselt jääb liikmesriikidele täiendavalt mitu aastat direktiivi ülevõtmiseks oma õigusesse ning seega direktiiv jõustub eelduslikult ligikaudu 3-4 aasta pärast.

[7] Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon. - RT II 2001, 1, 3.

[8] Teave Euroopa Nõukogu kodulehelt. Arvutivõrgus: http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp (04.05.2015) ning http://www.coe.int/t/dghl/standardsetting/dataprotection/Cahdata_en.asp (04.05.2015).

piisavalt tagatud ning eraelu puutumatuse riive proportsionaalsus on küsitav. Hüpoteesi kinnitamiseks või ümberlükkamiseks analüüsib autor asjakohaseid Eesti, rahvusvahelise õiguse norme, teiste riikide õigust ning erialakirjanduses välja toodud seisukohti. Kõigepealt analüüsib autor andmekaitseõiguse üldisi lähteallikaid, sisu ning õigusraamistikku. Seejärel keskendutakse töös konkreetselt Eesti kriminaalmenetluses isikuandmete töötlemisele, analüüsides andmekaitsealaste reeglite kohaldumist kriminaalmenetluse valdkonnas ning vastavaid Eestis kehtivaid õigusnorme. Teoreetilise käsitluse näitlikustamiseks analüüsib autor õiguslikku regulatsiooni kolme peamiselt isikuandmete töötlemisele suunatud menetlustoimingu puhul. Analüüsi tulemusena soovib autor leida hüpoteesile kinnituse või lükata see ümber. Autor loodab, et töös väljatoodud seisukohad leiavad praktilise rakenduse Eesti õiguses.

Käesolev magistritöö koosneb kahest peatükist. Esimeses peatükis annab autor ülevaate kehtivast Eesti ja rahvusvahelisest õigusraamistikust isikuandmete kaitse valdkonnas ning isikuandmete käsitlusest läbi kriminaalmenetluse prisma. Teises peatükis hindab autor, kas Eesti kehtiv regulatsioon tagab isikule piisava õiguse isikuandmete kaitsele ning näeb ette kohaseid piiranguid põhiõigustesse sekkumiseks.

Arvestades magistritöö olemust ning mahupiiranguid keskendub autor käesolevas töös üksnes isikuandmete töötlemisele kohtueelses kriminaalmenetluses. Töö põhirõhk on konkreetselt isikuandmete töötlemisega seotud põhiõigustel ning autor jätab käesoleva töö raames käsitlemata muud eraelu puutumatuse riivega seonduvad õigused, näiteks sõnumi saladus (PS § 43) ja kodu puutumatus (PS § 33). Kuigi andmekaitsealased küsimused tõusetuvad teravalt kindlasti ka kriminaalmenetlusega piirnevates valdkondades, näiteks süütegude ennetamine, isikute profileerimine, avaliku korra tagamine või teabehange, jätab autor need aspektid käesolevas töös käsitlemata. Samuti jääb käesoleva töö teemakäsitlusest välja isikuandmete kaitse kohtumenetluses ning pärast kohtuotsuse jõustumist, sealhulgas kohtuistungi läbiviimise, kohtulahendi avalikustamise ning karistusregistrisse kantud andmete avalikkusega seonduvad probleemid. Autor leiab, et ka need valdkonnad vajavad edaspidi põhjalikku käsitlemist ning autorile pakub huvi teema edasine põhjalikum ning ulatuslikum uurimine.

Autor on tänulik oma juhendajatele, kelle soovitused ja nõuanded olid abiks käesoleva magistritöö valmimisel.

1 ISIKUANDMETE KAITSE OLEMUS NING ÕIGUSLIK REGULATSIOON

Käesolevas peatükis käsitleb autor isikuandmete kaitsega seotud õigusraamistikku, sealhulgas vaadeldakse lähemalt kriminaalmenetluse valdkonnas töödeldavate isikuandmete kaitse õiguslikku regulatsiooni.

1.1 Isikuandmete tähtsus kriminaalmenetluse kontekstis

Nagu juba sissejuhatuses märgitud, on isikuandmetel tänapäevases ühiskonnas oma suur hind. Kuigi üldjuhul mõeldakse andmete väärtusest rääkides rahalist väärtust ning kasu, mida eraettevõtted teenivad suuremahulise andmetöötluse tulemusena,[9] saab andmete väärtusest rääkida ka kriminaalmenetluse kontekstis. Mida kiirem ja ulatuslikum on õiguskaitseasutuste juurdepääs erinevatele andmetele, seda tõhusamalt on neil võimalik oma ülesandeid täita. Teiselt poolt aga suureneb seeläbi ka isikute põhiõiguste riive ulatus, väärkasutamise risk ning kasvavad potentsiaalsed ohud üksikisiku õigustele. Enne isikuandmete kaitse regulatsiooni analüüsimist oleks eelkõige vaja piiritleda, mida hõlmab isikuandmete mõiste all ning milline on isikuandmete kaitse olemus ja ulatus tänapäeva õigusruumis. Kuigi kriminaalmenetlust reguleerib Eestis eeskätt kriminaalmenetluse seadustik (*edaspidi KrMS*),[10] tuleb isikuandmete ning isikuandmete kaitse mõistete sisustamiseks pöörduda teiste õigusnormide poole.

EIÕK ega PS ei kasuta mõistet "isikuandmete kaitse", vaid terminit "eraelu puutumatus", mis on oma olemuselt laiem. Eraelu mõiste areng on mõjutatud anglosaksi privaatsuse doktriinist ning juba 19. sajandil sisustati privaatsuse kui "õiguse olla üksi".[11] Euroopa Nõukogu Parlamentaarse Assamblee 1970. a resolutsiooni "Deklaratsioon masskommunikatsioonimeedia ja inimõiguste kohta"[12] punktis 15 on õigus eraelu puutumatusele määratletud kui õigus elada omaenda elu minimaalse sekkumisega. Resolutsiooni põhifookuses on sekkumine isiku eraellu ajakirjanduse poolt, kuid põgusalt leiab käsitlust ka vajadus kaitsta privaatsust laiemalt. Resolutsiooni punkti 20 kohaselt tuleks EIÕK

[9] J.-L. Gómez-Barroso, C. Feijóo-Gonzalez. Información personal: la nueva moneda de la economia digital. - El profesional de la información 2013 / 4, lk 292.
[10] Kriminaalmenetluse seadustik. - RT I 2003, 27, 166 ... RT I, 19.03.2015, 21.
[11] K. Jaanimägi, U. Lõhmus. PS § 26/6.1 - Ü. Madise jt (toim). Eesti Vabariigi Põhiseadus. Komm vlj. 3. tr. Tallinn: Juura 2012.
[12] Euroopa Nõukogu Parlamentaarse Assamblee resolutsioon 428 (1970) "Declaration on mass communication media and Human Rights". Arvutivõrgus: http://assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewPDF.asp?FileID=15842&lang=en (04.05.2015).

artikli 8 kohaldatavust vaadelda mitte üksnes kaitsena riigiasutuste tegevuse eest, vaid ka eraisikute, sealhulgas massimeedia sekkumise eest.

Aja möödudes ning tehnoloogia arenedes hakkas vajadus isiku privaatsust kaitsta aina rohkem päevakorda kerkima. Uued tehnoloogiad võimaldasid laiaulatuslikku andmete kogumist, töötlemist ja säilitamist, suurendades seeläbi ka isikut käsitleva info kasutamist nii riigi kui eraisikute poolt. Tekkis võimalus luua mahukaid andmebaase, mis said töödelda väga suurt hulka isikuandmeid. Ühelt poolt lihtsustas tehnoloogia areng kogutud andmete kasutamist erinevatel eesmärkidel, kuid samal ajal kasvas märkimisväärselt ka andmete väärkasutamise risk.[13]

Arvestades automatiseeritud töötlemise kiiret kasvu ning potentsiaalseid andmete väärkasutamisega kaasnevaid riske pidi seadusandja asuma täpsemalt reguleerima andmete kasutamist. Maailma esimese andmekaitset reguleeriva õigusakti võeti vastu Saksamaa Föderatiivses Vabariigis Hesseni liidumaal 1970.a.[14]

1980.a võttis Majanduskoostöö ja Arengu Organisatsioon (OECD) vastu resolutsiooni, millega kehtestati juhised privaatsuse kaitse ja isikuandmete piiriülese edastamise kohta (*Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*).[15] Juhiste art 1 p c annab isikuandmete definitsiooni: "isikuandmed on andmed tuvastatud või tuvastatava isiku kohta (andmesubjekt)". Sarnase definitsiooni annab ka 1981.a vastu võetud Euroopa Nõukogu konventsioon nr 108 isikuandmete automatiseeritud töötlemisel isikuandmete kaitse kohta (*edaspidi konventsioon 108* või *andmekaitsekonventsioon*) (art 2 p a) ning ka EL-is 1995.a vastu võetud direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta[16] (*edaspidi direktiiv 95/46/EÜ* või *andmekaitsedirektiiv*) (art 2 p a). Eesti võttis definitsiooni samuti omaks ning seda on kasutatud isikuandmete kaitse seaduse[17] (*edaspidi IKS*) § 4 lg-s 1 antud määratluses.

[13]H. Johlen. Artikel 8 Grundrechtecharta. Kölner Gemeinschaftskommentar zur Europäichen Grundrechte-Charta. BeckVerlag, München, 2006, art 8/1. Simitis, "S. Bundesdatencshutzgezetz" commentary. NomosVerlag, Baden-Baden, 2006, lk 64 (viidatud: Boehm, F. Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Springer Verlag, Berlin Heidelberg, 2012, lk 19-20).

[14] F. Boehm. Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Springer Verlag, Berlin Heidelberg, 2012, lk 20.

[15] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Arvutivõrgus: http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (04.05.2015).

[16] Euroopa Parlamendi ja nõukogu direktiiv 95/46/EÜ, 24.10.1995, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. - ELT L 281, 23.11.1995, lk 31-50.

[17] Isikuandmete kaitse seadus. - RT I 2007, 24, 127 ... RT I, 12.07.2014, 51.

Isikuandmete definitsioon Euroopa kehtivas õiguskorras on üsna lai. Nii konventsioonis 108 kui ka direktiivis 95/46/EÜ on isikuandmed defineeritud kui "mistahes informatsioon tuvastatud või tuvastatava isiku kohta (andmesubjekt)". Mõlemas õigusaktis antud mõiste on väga abstraktne, jättes suure tõlgendamisruumi. Definitsioonist nähtub seadusandja soov isikuandmete mõistele võimalikult laia kohaldamisala, kuivõrd terminis sisalduv ühend "mistahes informatsioon" võib üheaegselt viidata nii kindlatele faktidele isiku kohta, nagu näiteks isikukood, kui ka hinnangulistele kriteeriumitele, näiteks hinnang isiku krediidivõimekuse kohta. Seega selleks, et informatsioon oleks käsitatav isikuandmetega, ei pea see olema tõene või ümberlükkamatute tõenditega kinnitatav, vaid saab olla ka subjektiivne arvamus, millega omistatakse isikule teatud tunnuseid või omadusi. Oluline, et oma sisult annaks informatsioon edasi teavet isiku kohta, sõltumata teabe vormist. Nii on isikuandmeteks näiteks isiku fotod, kujutised, helilised salvestised.[18]

Isikuandmete definitsiooni kontekstis on tähelepanuväärne asjaolu, et isiku tuvastamist võimaldav teave võib teatud juhtudel olla ka selline informatsioon, mida üldjuhul oleks raske isikuandmeteks nimetada. Direktiivis 95/46/EÜ on isikuandmete mõiste mõneti täpsustatud ning kitsendatud. Direktiivi kohaselt on isik "tuvastatav" juhul, kui teda saab otseselt või kaudselt tuvastada eelkõige isikukoodi põhjal, samuti ühe või mitme tema füüsilisele, füsioloogilisele, vaimsele, majanduslikule, kultuurilisele või sotsiaalsele identiteedile omase tunnuse põhjal (art 2 p a). Isiku otsese tuvastamise all peetakse üldjuhul silmas isiku nime kasutamine. Kaudselt aga võimaldab isikut tuvastada mistahes muu info, nagu näiteks isikukoodi numbrikombinatsioon, sõrmejälje kujutis,[19] aga ka näiteks telefoninumber ja isegi töötingimused.[20] Tänapäeva asjaoludes loetakse isikuandmeteks sageli isegi veebiidentifikaatorit (IP-aadressi). Artikkel 29 töögrupp on pidanud IP-aadressi isikuandmeteks juba mõnda aega, eriti kui IP-aadressi töötlemine toimubki andmesubjekti tuvastamise eesmärgil, näiteks autoriõiguste kaitse kontekstis.[21] Nüüdseks on selline tõlgendus üle võetud ka Euroopa Kohtu poolt, kui kohus oma 2011.a tehtud otsuses selgelt sedastas, et IP-aadressid on isikuandmetena kaitstavad, kuivõrd need võimaldavad kasutaja täpset identifitseerimist.[22] Arvestades digimajanduse arengut ja e-teenuste kasutamise kasvu ei saa välistada, et lähiajal jõuab IP-aadressi käsitamine isikuandmetena ka *expressis verbis* ELi

[18] Article 29 Data Protection Working Party, 20.06.2007, Opinion 4/2007 on the concept of personal data, lk 6-7. Arvutivõrgus: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf (04.05.2015).
[19] *Ibid*, lk 14.
[20] EKo 06.11.2003, C-101/01, *Rootsi vs Lindqvist,* p 27.
[21] Article 29 Data Protection Working Party. Opinion 4/2007, lk 16-17.
[22] EKo 24.11.2011, C-70/10, *ScarletExtended SA vs Sociétébelgedesauteurs, compositeurs et éditeurs SCRL (SABAM),* p 51.

õigusesse, sest käimasoleva EL andmekaitse reformi raames soovitakse selgelt loetleda IP-aadress kui isiku tuvastamist võimaldavat teavet.[23]

Näiteks on üsna selge, et auto mudel või maja väärtus ei ole üldiselt käsitatavad isikuandmetega, vaid tegemist on kindlaid objekte kirjeldava informatsiooniga. Siiski teatud juhtudel võib isegi selline teave osutuda isikuandmeteks, kuivõrd võimaldab teha teatud järeldusi isiku omaduste kohta. Sellisteks omadusteks võib olla toodud näidete puhul muuhulgas isiku ostuvõime ja majanduslik seisund (teatud automudelid on kallimad kui teised, maja väärtus on kõrge), aga ka isiku otsene maksukoormus (maja väärtuse pinnalt tasutav maks). Toodud olukordades on ilmne, et objekte kirjeldav teave langeb isikuandmete definitsiooni alla.[24]

Eesti õiguses on isikuandmete defineerimisel lähtutud eelkõige konventsioonis 108 toodud laiemast definitsioonist ning IKS ei sisalda andmekaitsedirektiivi art 2 p-s a toodud kitsendust. Direktiivi kohaselt tuleks isikuandmetena käsitleda üksnes selliseid andmeid, mis iseloomustavad konkreetset isikut ning eristavad teda teistest isikutest. Seega võib öelda, et Eestis on isikuandmete mõistele antud laiem tähendus kui andmekaitsedirektiivis.[25] Mõiste laiem tähendus avardab ka kehtestatud reeglite kohaldamisala, kuivõrd isikuandmetena tuleb kaitsta suurem hulk teavet.

Tuleb tõdeda, et isikuandmete definitsioon on väga lai, hõlmates põhimõtteliselt kogu teavet, mida võib isikuga kas otseselt või isegi väga kaudselt seostada. Mõneti on selline laiaulatuslik kaitse põhjendatud, arvestades tänapäeval informatsiooni kättesaadavuse lihtsust ja ulatust. Samas on autori hinnangul küsitav, kas isikuga väga kaudselt seonduvate subjektiivsete arvamuste kaitse isikuandmetena ei too kaasa liigset ülereguleerimist ega pidurda infoühiskonna arengut. Autori hinnangul ei saa olla soovitav olukord, kus kokkuvõttes võib isikuandmeteks kvalifitseerida igat infokildu.

Arvestades kriminaalmenetluse olemust ning menetluse raames töödeldavate andmete iseloomu võib eeldada, et selliste andmete õigustamatu töötlemine võib tuua andmesubjektile suurema kahju kui pelgalt tema nime või isikukoodi töötlemine. Vähendamaks andmesubjektile kaasnevaid riske vajavad kriminaalmenetluses töödeldavad andmed rangemat kaitset. Nii konventsioon 108 kui ka direktiiv 95/46/EÜ põhinevad eeldusel, et teatud andmekategooriad

[23] Euroopa Komisjon. Ettepanek: Euroopa Parlamendi ja nõukogu määrus üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (isikuandmete kaitse üldmäärus), KOM (2012) 11 lõplik, 25.01.2012, art 4 p 1. Arvutivõrgus: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_et.pdf (04.05.2015).
[24] Article 29 Data Protection Working Party. Opinion 4/2007, lk 9.
[25] S. Mikli. Kui kauge Euroopa Liidu õigus saab järsku igapäevatöö osaks: probleeme Euroopa Liidu õiguse ülevõtmisel ja rakendamisel õiguskindluse põhimõtte kontekstis. - Juridica 2015 / 2, lk 106.

vajavad erilist kaitset ning neid võib töödelda ainult eritingimustel.[26] Seejuures võib leida mitmeid kriteeriume, mille järgi tuleb otsustada selle üle, milliseid andmeid tuleks kaitsta tugevamini. Kehtivas õiguses on võetud lähtekohaks, et teatud andmed võivad mõjutada ja kahjustada isiku põhiõigusi oluliselt rohkem kui teised. Selliseid andmeid on liigitatud isikuandmete erikategooriateks (*special categories of data*), Eesti õiguses on juurdunud termin "delikaatsed isikuandmed". Erialases kirjanduses on ühtlasi sageli kasutusel termin "tundlikud andmed" (*sensitive data*).

Konventsiooni 108 artikkel 6 sätestab keelu töödelda automatiseeritud viisil ilma kohaste tagatisteta teavet, mis puudutab isiku rassilist päritolu, poliitilisi arvamusi, usulisi või muid tõekspidamisi, tervist, seksuaalelu ning süüdimõistmisi kuritegudes.[27] Direktiivi 95/46/EÜ art 8 lõige 1 laiendab konventsioonis esitatud nimekirja ning keelab selliste andmete töötlemist, mis paljastavad isiku rassilist või etnilist päritolu, poliitilisi arvamusi, usulisi või filosoofilisi tõekspidamisi, ametiühingusse kuulumist, samuti andmeid tervise ja seksuaalelu kohta. Direktiivi sõnastus süüdimõistmisi käsitavas osas on konventsioonist mõnevõrra erinev, kuid oma sisult väga sarnane. Nimelt direktiivi art 8 lg 5 näeb ette, et süütegusid, kuritegudes süüdimõistmisi ning turvameetmeid puudutavat teavet tohib töödelda ainult pädeva asutuse järelevalve all ning kohaste tagatiste olemasolul. Kriminaalõiguse aspektist on aga oluline asjaolu, et direktiivi kohaselt loetakse tundlikeks andmeteks lisaks süüdimõistmistele ka teavet süütegude toimepanemise kohta. Eesti isikuandmete kaitse seadus võtab küll üle direktiivi 95/46/EÜ[28] ja peaks olema kooskõlas ka konventsiooniga 108,[29] kuid sisaldab samas mõlemast rahvusvahelise õiguse instrumendist mõnevõrra erinevat delikaatsete isikuandmete nimekirja, seejuures on väga erinev lähenemine süüteomenetlusega seotud andmetele.

---

[26] Article 29 Working Party. 20.04.2011. Advice paper on special categories of data ("sensitive data"), lk 4. Arvutivõrgus: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf (04.05.2015).

[27] Inglise keeles on kasutusel väljend *criminal convictions*, prantsuse keeles *condamnations pénales*, hispaania keeles *condenas penales*. Eestikeelses versioonis kasutatakse mõistet "süüdimõistmised toimepandud kriminaalkuritegudes". Siinkohal on vaieldav, mida "kriminaalkuriteod" hõlmavad. Vaadates kehtivat Eesti õigust, võiks asuda seisukohale, et viidatakse ainult karistusseadustikus kuriteona karistatavatele tegudele. Siiski on EIK mitmel korral leidnud (nn Engeli kriteeriumid, nt EIKo 08.06.1976, Engel ja teised *vs* Holland*;* EIKo 18.10.2011, Tomasovič *vs* Horvaatia), et EIÕK art 6 mõttes on kriminaalkuritegude määratlusel oluline arvestada õigusrikkumise kvalifikatsiooni siseriikliku õiguse järgi, õigusrikkumise olemust ning oodatava karistuse iseloomu ja raskust. Muuhulgas on kehtiva jaotuse kohaselt ka Eesti õiguses tuntud väärteod liigitatud "kriminaalkuritegudeks", sest tegemist on karistusseadustiku kohaldamisalasse kuuluvate tegudega. Seega kuigi ametlikult kasutatav termin on "kuritegu", tuleks seda Eesti õiguse kohaselt laiendada kõigile süütegudele.

[28] Redaktsiooniline märkus Riigi Teatajas.

[29] Eesti on konventsiooni ratifitseerinud 2000.a ning see jõustus 2002.a. Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni ratifitseerimise seadus. - RT II 2001, 1, 3.

IKS § 4 lg 2 p 8 kohaselt loetakse delikaatseteks isikuandmeteks andmed süüteo toimepanemise või selle ohvriks langemise kohta enne avalikku kohtuistungit või õigusrikkumise asjas otsuse langetamist või asja menetluse lõpetamist. Seletuskirja kohaselt kaitseb IKS § 4 lg 2 p 8 enne avalikku kohtuistungit, otsuse tegemist või asja menetluse lõpetamist nii süüteo (väärteo või kuriteo) sooritajat (süütuse presumptsiooni põhimõte) kui ka selle ohvrit selliselt, et andmed süüteo toimepanemise või selle ohvriks langemise kohta on delikaatsed isikuandmed.[30] Seaduse koostajad on võtnud lähtekohaks põhimõtte, et isikuandmed on delikaatsed senikaua, kuni asja kohta pole võimalik saada informatsiooni muul moel (avaliku kohtuistungi külastamine) või kuni asjas pole lõplikku selgust (kohtuotsust või menetluse lõpetamise määrust). Arvestades, et Eestis on näiteks karistusregistrisse kantud andmed üldjuhul avalikud[31] ning kohtulahendid on samuti suures osas avalikud (KrMS § 408[1]), võib tõusetuda küsimus Eesti õiguse kooskõlast siduvate rahvusvaheliste õigusaktidega ning väljakujunenud õiguspraktikaga.[32] Kuigi kõnealune küsimus väljub antud magistritöö raamest, väärib teema kindlasti edasist käsitlust.

Töö autori hinnangul on märkimisväärne pöörata tähelepanu asjaolule, et kehtivas IKS-is ei ole sätestatud eraldi reegleid delikaatsete isikuandmete töötlemisele. Direktiivi 95/46/EÜ art 8 lg 1 näeb ette üldise keelu töödelda delikaatseid isikuandmeid, sama artikli lg 2 sätestab kindlad olukorrad, millal delikaatsete isikuandmete töötlemine võib olla erandina lubatud. Eestis on seadusandja valinud lähenemise, mille kohaselt kehtib delikaatsete isikuandmete töötlemise korral põhimõtteliselt sama õiguskord mis nn tavaliste andmete töötlemisel. Erandiks on IKS viiendas peatükis sätestatud delikaatsete isikuandmete töötlemise registreerimise nõue, kuid muus osas ei erine delikaatsete isikuandmete töötlemisele esitatavad töötlemisenõuded ega turvameetmed muude andmete töötlemisel kehtivast korrast. Ka kriminaalmenetluse seadustikust ei tulene täiendavaid nõudeid isikuandmete töötlemisele.

1.2 Õigus isikuandmete kaitsele põhiõiguste kontekstis

[30] Isikuandmete kaitse seaduse seletuskiri. Arvutivõrgus: http://www.aki.ee/et/eraelu-kaitse/oigusaktid (04.05.2015).
[31] Karistusregistri seadus. - RT I, 21.03.2011, 3 ... RT I, 05.12.2014, 15, § 7.
[32] Näiteks EIK on oma 13.11.2012 otsuses nr 24029/07 *M.M. vs Ühendkuningriik (*p 200*)* märkinud, et karistusregistriga seoses on esmatähtis määratleda mh kindlad kolmandatele isikutele avalikustamise reeglid, mis kaitseksid andmeid meelevaldse ning liigse kasutamise eest.

Kriminaalmenetlus on valdkond, kus põrkuvad vastandlikud huvid. Ühelt poolt ootab ühiskond õiguskaitseasutustelt turvalisuse ning rahu tagamist, teiselt poolt võib aga selle eesmärgi saavutamine tähendada kriminaalmenetlusele allutatud (või sellega seotud) üksikisiku põhiõiguste tugevat piiramist. Demokraatlikus ühiskonnas ei ole kriminaalmenetlus suunatud üksnes karistamisele, vaid selle funktsiooniks on ka õigusriigi põhimõtetele tugineva menetluse ja õigusemõistmise tagamine.[33]

PS § 3 kohaselt teostatakse riigivõimu üksnes põhiseaduse ja sellega kooskõlas olevate seaduste alusel. Tegemist on õigusriigi aluspõhimõtte keskse sättega, millega sisustatakse seaduslikkuse ehk legaalsuse põhimõtte. Seaduslikkuse põhimõtte kohaselt toimivas riigis ei ole kohta nn politseiriiklusele ega omavolile ning kõik avalik-õiguslikud aktid peavad olema allutatud põhiseadusele.[34] Kõige olulisemat osa riigivõimust nimetatakse riigi tuumikülesanneteks ehk tuumikfunktsiooniks. Riigikohtu üldkogu on leidnud, et tuumikülesanded on need ülesanded, „mida on põhiseaduse mõtte kohaselt kohustatud täitma riigivõim". Süüteomenetlused (sh kriminaalmenetlus) on riigi tuumikfunktsiooni osiseid.[35] Sellest tulenevalt on ka kriminaalmenetlus allutatud PS §-s 3 sätestatule ning kriminaalmenetluse läbiviimine peab olema kooskõlas nii PS endaga kui ka teiste seadustega. Riigi kohustus tagada õigused ja vabadused tuleneb ka PS §-st 14. Kuivõrd kuritegevuse tulemusena seatakse ohtu või riivatakse erinevaid üksikisikute õigusi (näiteks vargus kahjustab isiku õigust omandile, tapmine õigust elule jne), on põhiseadusest tulenevalt riigil kohustus võtta tarvitusele meetmed selliste riivete takistamiseks.[36] Kriminaalmenetluses kehtib riiklikkuse põhimõte, mille kohaselt alustatakse ja toimetatakse kriminaalmenetlus Eesti Vabariigi nimel (KrMS § 5). Kohtueelset kriminaalmenetlust juhib prokuratuur, kelle ülesandeks on menetluse seaduslikkuse ja tulemuslikkuse tagamine ning kohtus riikliku süüdistuse esindamine (KrMS § 30 lg 1). Prokuratuur kui täitevvõimu asutus[37] allub PS-is ning selle alusel kehtestatud õigusaktides sätestatud põhimõtetele.

Õigusriigi mudel eeldab avaliku võimu poolt mistahes läbiviidavate toimingute kooskõla põhiseaduse ja seadusega. PS ei sätesta eraldi õigust isikuandmete kaitsele. Küll aga on PS § 26 kohaselt igaühel õigus perekonna- ja eraelu puutumatusele. PS § 26 eeskujuks on Euroopa

[33] U. Lõhmus. Põhiõigustest kriminaalmenetluses. 2.tr. Tallinn: Juura 2014, lk 15.
[34] E. Talvik. Legaalsuse põhimõte Eesti Vabariigi põhiseaduse tekkimises, muutmises ja muutmiskavades. Tartu 1991, lk 12 jj (viidatud: T. Annus, M. Ernits jt. PS § 3 /2).
[35] RKÜKo 3-1-1-86-07, p 26.
[36] J. Antonova. Leenureisijate broneeringuinfo kasutamine õiguskaitse eesmärkidel Eestis. Tallinn: 2013, lk 23.
[37] Prokuratuuriseadus. - RT I 1998, 41, 625 ... RT I, 10.03.2015, 17, § 1 lg 1.

Inimõiguste ja Põhivabaduste kaitse konventsiooni (*edaspidi EIÕK*) artikkel 8[38], mille esimene lõige sätestab igaühe õiguse era- ja perekonnaelu ning kodu ja korrespondentsi saladuse austamisele.[39] Uno Lõhmus, võttes kokku dr Nicole Morehami esitatud seisukohti,[40] kirjeldab alljärgnevat EIÕK art 8 kaitstavate õiguste jaotust:

- vabadus sekkumisest kehalisse ja vaimsesse terviklikkusesse (sh nt läbiotsimine, jälgimine, pealtkuulamine jt);

- isikuandmete kogumine, töötlemine ja avalikustamine;

- elukeskkonna kaitse;

- õigus identiteedi kaitsele;

- õigus personaalautonoomiale.[41]

Dr Morehami kohaselt on ilmne, et EIK lahendid liigitavad isikuandmete kogumist, töötlemist ning avalikustamist EIÕK art 8 kohaldamisalasse. Seega on isik kaitstud soovimatu ligipääsu eest teda puudutavale informatsioonile ning seeläbi ka soovimatust teabe kogumisest ja säilitamisest, isiklikku informatsiooni sisalduva lugemisest ning erakirjavahetusse sekkumisest. Informatsiooni kogumist võib jaotada kaheks - sekkuv ning mittesekkuv. Sekkuvaks teabekogumiseks on näiteks isiku jälitamine, kirjavahetuse lugemist võimaldava seaduse vastuvõtmine või tööalase telefoni pealtkuulamine. Mittesekkuvat teabekogumist on EIK käsitlenud muuhulgas selliselt, et isikut küsitleti tema kohta käivate andmete osas ning seejärel kirjutati kuuldu üles. Informatsiooni säilitamine kujutab endast teist võimalust sekkuda isiku õigusesse andmete kaitsele. Muuhulgas rikub EIÕK art 8 sätestatud õigust politsei poolt salaja peetav andmebaas ning seda ka juhul, kui vastav info oleks avalikult kättesaadav. Viimaks kahjustab isiku õigust andmete kaitsele eraelu puudutava teabe avalikustamine.[42] PS § 26 on peamisi sätteid, mis reguleerib eraelu puutumatust ja sellega haakuvat isikuandmete kaitset, kuid seonduvaid sätteid on teisigi. Nii näiteks sätestab PS § 18 õigust au ja hea nime kaitsele, § 33 õigust kodu puutumatusele, § 43 õigust sõnumi saladusele. Perekonna- ja eraelu üksikud tahud võivad kuuluda ka teiste PS sätete kaitsealasse.[43] PS §-st 26 laiema kohaldamisalaga on PS § 19, mis sätestab üldise enesemääramise ja enesekujutamise õiguse. PS § 19 võib samuti

[38] K. Jaanimägi, U. Lõhmus. PS § 26/2.
[39] Euroopa Inimõiguste ja põhivabaduste kaitse konventsioon. - RT II 1996, 11, 34.
[40] N.A. Moreham. The Right to Respect for Private Life in the European Convention on Human Rights: A Re-Examination. - European Human Rights Law Review, nr 1, 2008, lk 44-79.
[41] U. Lõhmus. Põhiõigused kriminaalmenetluses, 2014, lk 307.
[42]N.A. Moreham, 2008, lk 44-79.
[43] K. Jaanimägi, U. Lõhmus. PS § 26/3.

teatud ulatuses seostuda eraelu kaitsega. Kuivõrd EIÕK ei sisalda PS §-ga 19 sarnast laia sätet, paigutab EIK oma praktikas enamuse enesemääramisõiguse ja enesekujutamise õigusega seotud küsimusi EIÕK art 8 kaitsealasse. PS sätete analüüsimise tõusetub paratamatult küsimus, milline on PS § 19 esemeline kaitseala eraelu puutumatuse osas. Arvestades PS § 26 kohaldamisalale antud tõlgendust EIK praktikas, võib asuda seisukohale, et PS § 19 kaitsealasse jäävad kõik need eraelu aspektid, mis ei ole hõlmatud PS § 26 kaitsealaga.[44]

Nii EIÕK-s ning Eesti põhiseaduses sätestatud õigus eraelu puutumatusele on küllaltki laia kohaldamisalaga ning hõlmavad ka õigust isikuandmete kaitsele. Riigikohus on tõlgendanud PS §-s 26 sätestatud õigust eraelu puutumatusele ning asus muuhulgas seisukohale, et õigus isikuandmete kaitsele on üks olulisemaid osi eraelu kaitse juures.[45] Euroopa Inimõiguste Kohus on samuti analüüsinud seoseid isikuandmete kaitse ning eraelu puutumatuse vahel ja sedastas juba oma 1987.a tehtud otsuses *Leander vs Rootsi*[46] esmakordselt, et isikuandmete säilitamine ja kasutamine võib riivata õigust eraelu austamisele EIÕK art 8 tähenduses.[47] Otsuses *Amann vs Šveits* asus EIK seisukohale, et avaliku võimu kandja poolt isikute eraelu käsitlevate andmete kogumine ning säilitamine on oma olemuselt EIÕK artikli 8 mõjusfääris.[48] Sama seisukohta on kohus sisuliselt korrutanud ka mõned kuud hiljem tehtud otsuses *Rotaru vs Rumeenia*, kus kohus sedastas, et isiku eraelu puudutavate andmete säilitamine salajases andmebaasis kuulub EIÕK art 8 kohaldamisalasse.[49] Oma otsuses *M.S. vs Rootsi* rõhutas EIK, et isikuandmete kaitse on fundamentaalse tähtsusega võimaldamaks isikul kasutada õigust era- ja perekonnaelu austamisele nagu see on tagatud EIÕK artiklis 8.[50] Siiski tuleb nentida, et sarnaselt paljude teiste PS-is sätestatud põhiõigusega ei ole ka §-s 26 käsitletud õigus eraelu puutumatusele absoluutne. Üldised tingimused põhiseaduslike õiguste piiramiseks tulenevad PS §-st 11, mille kohaselt tohib õigusi ja vabadusi piirata üksnes kooskõlas põhiseadusega. Seejuures peavad kehtestatavad piirangud olema demokraatlikus ühiskonnas vajalikud ega tohi moonutada piiratavate õiguste ja vabaduste olemust. Riive põhiseaduspärasuse hindamisel tuleb esiteks arvestada nii formaalset kui materiaalset põhiseaduspärasust.[51] Formaalne põhiseaduspärasus tähendab, et põhiõigusi piirav õigustloov akt peab vastama pädevus-, menetlus- ja vorminõuetele ning määratuse ja seadusereservatsiooni põhimõtetele. Pädevus-, menetlus- ja

[44] K. Jaanimägi, U. Lõhmus. PS § 26/4.
[45]RKHKo 3-3-1-3-12, p 19.
[46]EIKo 26.03.1987, 9248/81, *Leander vs Rootsi*, p 48.
[47] O. Diggelmann, L. Wildhaber. Euroopa inimõiguste konventsioon ja eraelu kaitse. Uuemad arengusuunad. - Juridica 2007 / 1, lk 5-6.
[48]EIKo 16.02.2000, 27798/95, *Amann vs Šveits*, p 65 - 67.
[49] EIKo 04.05.2000, 2834/95, *Rotaru vs Rumeenia*, p 43.
[50]EIKo 27.08.1997, 20837/92, *M.S. vs Rootsi*, p 41.
[51] R. Alexy. Põhiõigused Eesti põhiseaduses. - Juridica 2001/1, lk 5-96.

vorminõuete kohaselt peab akt olema antud selleks pädeva organi poolt, järgides kõiki menetlus- ja vormireegleid.[52] Hinnates riive materiaalset kooskõla põhiseadusega tuleb kontrollida, kas põhiõigust riivav õigusakt on kehtestatud põhiseadusega lubatava eesmärgi saavutamiseks ning on selle saavutamiseks proportsionaalne abinõu.[53]

Teiseks peab riive olema vajalik demokraatlikus ühiskonnas. Kuigi kõnealune kriteerium pärineb EIÕK, on EIK oma lahendites andnud sellele ka proportsionaalsuse mõõtme.[54] Kohtuasjas *Z vs Soome* hindab kohus riive vajalikkust selle järgi, kas riive põhjused olid asjakohased ja piisavad ning kas tarvitusele võetud meetmed olid eesmärgi suhtes proportsionaalsed.[55] Eesti õigusesse tuli proportsionaalsuse põhimõte esmakordselt 1997. a, kui Riigikohus kasutas seda oma otsuses kohtuasjas 3-4-1-3-97.[56] Proportsionaalsuse hindamisel lähtutakse kolmeastmelisest proportsionaalsuse testist, mille raames hinnatakse riive sobivust, vajalikkust ning mõõdukust (ehk proportsionaalsust kitsamas tähenduses).[57] Riigikohus rakendas proportsionaalsuse kolmeastmelist hindamist esmakordselt 2000.a ning sellest on praeguseks välja kujunenud Eesti õiguse järjekindel praktika. Proportsionaalsuse põhimõte on õigusriigi üks aluspõhimõtteid ning sellest peavad lähtuma kogu riigivõim, st nii seadusandliku, täidesaatva kui kohtuvõimu esindajad. Proportsionaalsuse põhimõtet võib kokku võtta kui ülemäärase sekkumise keeldu ning riigi kohustust hoiduda isiku vabadustesse sekkumisest üldistes huvides kui see ei ole möödapääsmatu.[58] PS §11 sätestatud kolmas tingimus, mille kohaselt ei tohi riive moonutada piiratavate õiguste ja vabaduste olemust, võib käsitleda kui proportsionaalsuse põhimõtte sünonüümina.[59]

PS § 26 täpsustab olukordi, millal eraelu puutumatuse riive on õigustatud. PS § 26 teise lause kohaselt võib isiku perekonna- ja eraellu sekkuda seaduses sätestatud juhtudel ja korras tervise, kõlbluse, avaliku korra või teiste inimeste õiguste ja vabaduste kaitseks, kuriteo tõkestamiseks või kurjategija tabamiseks. Arvestades PS §-des 11 ning 26 sätestatud tingimusi võib järeldada, et eraelu puutumatuse riive on lubatud, kui

- sekkumise võimalus on sätestatud põhiseadusega kooskõlas olevas seaduses;

- sekkumine leiab aset seaduses sätestatud korras;

[52] RKPJKo 3-4-1-5-05, p 8.
[53] RKPJKo 3-4-1-16-08, p 28.
[54] M. Ernits. PS § 11/ 3.
[55] EIKo 25.02.1997, 22009/93 , Z *vs Soome*, p 94 - 113.
[56] RKPJKo 3-4-1-3-97, p I.
[57] R. Alexy. 2001, lk 5-96.
[58] M. Ernits. PS § 11/ 3.
[59] M. Ernits. PS § 11/ 4.3.

- sekkumine on vajalik tervise, kõlbluse, avaliku korra või teiste inimeste õiguste ja vabaduste kaitseks, kuriteo takistamiseks või kurjategija tabamiseks;

- sekkumine on proportsionaalne.

U. Lõhmus märgib, et PS-s on erinevate põhiõiguste juures kasutatud piiranguklauslite sätestamisel erinevat sõnastust, mis võib luua ettekujutuse erinevast kasutusalast. Näiteks on PS §-s 43, mis käsitleb õigust sõnumi saladusele, lubatakse selgelt sekkuda nimetatud põhiõigusesse kuriteo tõkestamiseks ja kriminaalmenetluses tõe väljaselgitamiseks.[60] PS §-is 26 sätestatud seaduse reservatsioon on kvalifitseeritud, võimaldades vastava põhiõiguse piiramist üksnes samas sättes täpselt sõnastatud eesmärkidel.[61] Sellest lähtuvalt tekib küsimus, kas PS §-is 26 ette nähtud õigust eraelu puutumatusele ei tohiks piirata kriminaalmenetluses tõe väljaselgitamiseks (erinevalt nt PS §-ist 19).

PS § 26 seadusereservatsiooni sõnastus on tekitanud ebaselgust varemgi. Põhiseaduse ekspertiisikomisjon leidis, et eraelu puutumatuse riivet võimaldavad eeldused on liialt kitsad. PS §-is 26 sätestatud loetelu ei võimalda eraelu riiveid, mis on vajalikud politsei- ja korraõiguses ning kriminaalmenetluses, sh nt kriminaaltäitemenetluses, vangistusest vabanenud isikute resotsialiseerimiseks või riikliku julgeoleku tagamiseks. Ekspertiisikomisjon tegi ettepaneku muuta § 26 lihtsa põhiseaduse reservatsiooniga põhiõiguseks, kuivõrd lähtuvalt üldistest põhiõiguste piiramise reeglitest, eelkõige proportsionaalsuse põhimõttest, oleks ka lihtsa seadusereservatsiooni korral võimalik tagada tõhus isikute õiguste kaitse.[62]

Hetkel pole siiski põhiseadust muudetud. Kuigi tuleb tunnistada, et põhiõiguste piiramise tingimuste erinev sõnastus võib tekitada väärarusaama, et õigust eraelu puutumatusele ei tohiks piirata kriminaalmenetluses tõe väljaselgitamiseks, leiab käesoleva töö autor, et selline arusaam poleks siiski korrektne. PS § 26 teine lause võimaldab piirata õigust eraelu puutumatusele nii kurjategija tabamiseks kui ka teiste isikute õiguste ja vabaduste kaitseks. Arvestades kriminaalmenetluse ülesandeid ning eesmärke on autori hinnangul ilmne, et vaatamata selgelt sõnastatud eesmärgi puudumisele ei takista PS sekkumist õigusesse eraelu puutumatusele juhul, kui see on vajalik kriminaalmenetluses. Mõistagi tuleb lähtuda kehtivatest põhiõiguste piiramise reeglitest (sh PS §-st 11).

Kriminaalmenetluse kontekstis on kindlasti võimalik eraelupuutumatuse mistahes väljendusvormi riive ning erandiks pole ka õigus isikuandmete kaitsele. Näiteks võib tuua nii

[60] U. Lõhmus, 2014, lk 309-310.
[61] K. Jaanimägi, U. Lõhmus. PS § 26/11.
[62] K. Jaanimägi, U. Lõhmus. PS § 26/11.3.

sõrmejälgede ja DNA-proovi võtmist (KrMS § 99[1]), andmete nõudmist sideettevõtjalt (KrMS § 90[1]), jälitustegevust (KrMS 3[1]. peatükk), läbiotsimist (KrMS § 91), isiku läbivaatust (KrMS §88) kui ka mitmeid teisi KrMS-s sisalduvaid menetlustoiminguid. Nii põhiseadus kui ka EIÕK näevad ette avaliku võimu teostajate positiivset kohustust tagada isikuandmete kaitse ning negatiivset kohustust hoiduda õigustamata sekkumisest. Seeläbi on loodud selged piirid, mille raames saavad riigiasutused tegutseda, kahjustamata eraisiku põhiõigust eraelu puutumatusele, sh tema kohta käivate andmete kaitsele.

Erinevalt EIÕK-st ja Eesti põhiseadusest eristab Euroopa Liidu põhiõiguste harta[63] (*edaspidi harta*) eraldi õiguse era- ja perekonnaelu puutumatusele (art 7) ning ka õiguse isikuandmete kaitsele (art 8). Kui harta art 7 põhineb EIÕK art-l 8, siis harta art 7 sätestab õiguse isikuandmete kaitsele kui autonoomse põhiõiguse.[64] Harta art 8 kohaselt on igaühel õigus oma isikuandmete kaitsele ning selliseid andmeid tuleb töödelda asjakohaselt, kindlaksmääratud eesmärkidel, puudutatud isiku nõusolekul või seaduses sätestatud õiguslikul alusel. Lisaks sätestab harta sõnaselgelt igaühe õiguse tutvuda tema kohta kogutud andmetega ning nõuda nende parandamist. Viimaks kehtestab harta nõude, et eespool nimetatud tingimuste täitmist peab kontrollima sõltumatu asutus. Rääkides õigusest eraelu puutumatusele ning õigusest andmekaitsele ja nende õiguste kaitseala eristamisest harta valguses võib nentida, et õigus eraelu puutumatusele annab isikule nö staatilise, negatiivse kaitse - teised isikud peaksid hoiduma õigustamata sekkumisest. Õigus isikuandmete kaitsele on aga justkui dünaamiline, see käib töödeldavate andmetega kaasas, seades igale töötlemistoimingule kindlad tingimused.[65] Õigus isikuandmete kaitsele ei keela andmete töötlemist ega kaitse isikut andmetetöötluse eest, vaid kaitseb ebaseadusliku ja / või ebaproportsionaalse andmete töötlemise eest.[66]

Hartas sätestatu kuulub EL õigusesse ning Euroopa Liidu lepingu[67] art 6 lg 1 annab hartale EL aluslepingutega samaväärse õigusjõu. Seega kuigi harta sätted ei ole sõnaselgelt kirjutatud EL aluslepingutesse, on nii EL institutsioonidel kui liikmesriikidel kohustus lähtuda harta põhimõtetest. Liikmesriikidele laieneb see kohustus niivõrd, kuivõrd nad tegutsevad EL õiguse rakendamise raames (art 51 lg 1). Kuivõrd praeguseks on EL õigus ja liikmesriikide õigus väga tihedalt kokku põimunud, võib harta art 51 lg 1 täitmine praktikas olla problemaatiline.

---

[63] Euroopa Liidu Põhiõiguste Harta, ELT C 83, 30.03.2010, lk 389-403.
[64] S. Rodota. Data Protection as a Fundamental Right. - Gutwirth, S. jt (toim). Reinventing Data Protection? Springer Science+Business Media B.V., 2009, lk 79.
[65] *Ibid*, lk 79.
[66] P. De Hert, P., S. Gutwirth. Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action. - Gutwirth, S. jt (toim). Reinventing Data Protection? Springer Science+Business Media B.V., 2009, lk 3.
[67] Euroopa Liidu leping. - ELT C 115, 09.05.2008, lk 13 – 45.

Kokkuvõttes võib öelda, et õigus isikuandmete kaitsele on leidnud kajastuse nii EIÕK-s, PS-s kui ka EL põhiõiguste hartas ning selle õiguse tähtsust tänapäeva tehnoloogiaajastul on raske üle hinnata.

1.3 Isikuandmete kaitse valdkonda reguleerivad õigusnormid

Kuivõrd Eesti kriminaalmenetluses ei ole kehtestatud eraldi isikuandmete kaitset reguleerivat õigusakti ning ka KrMS ei sisalda vastavat regulatsiooni, eeldab käesolevas töös püstitatud ülesande lahendamine valdkonnale kohaldatava andmekaitseõiguse laiemat tundmist ning selle analüüsi. Alljärgnevalt käsitleb autor käesoleva töö seisukohalt olulisi õigusakte.

Nagu eespool käsitletud, on õigus isikuandmete kaitsele hõlmatud EIÕK art-ga 8. Siiski EIÕK üksinda ei ole piisav andmekaitse valdkonna reguleerimiseks, mistõttu töötati välja konventsioon, milles sõnastatakse selged isikuandmete töötlemise reeglid ja tingimused. Euroopa Nõukogu 1981.a isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon põhineb EIÕK artiklil 8. Konventsiooni väljatöötamise põhjuseks oli arusaam, et isiku õiguste tõhusaks kaitseks on vaja täpsemaid ja süstemaatilisi sätteid kui seda leiab EIÕK artiklist 8.[68] Konventsioon koostoimes seda tõlgendanud ja täiendanud kohtupraktikaga kohustab liikmesriike kehtestama reeglid, millega tagatakse isikute õigused isikuandmete töötlemise osas. Konventsiooniga kehtestatakse viis andmekaitsepõhimõtet, mida riigid peaksid võtma aluseks andmetöötluse reguleerimisel. Need põhimõtted on sätestatud konventsiooni artiklis 5:

- andmed peavad olema kogutud ja töödeldud seaduslikult ja ausalt (seaduslikkuse põhimõte);

- andmed peavad olema säilitatud ainult selgelt piiritletud ja seaduslikel eesmärkidel ning ei tohi olla töödeldavad sellisel otstarbel, mis ei sobi algsete eesmärkidega (eesmärgikohasuse ning kasutuse piiramise põhimõte);

- andmed peavad olema vajalikud, kohased ega tohi olla üleliigsed säilitamise eesmärgi suhtes (minimaalsuse põhimõte);

- andmed peavad olema korrektsed ning vajadusel ajakohastatud (andmete kvaliteedi põhimõte);

[68]Data Protection. Complilation of Council of Europe texts. Strasbourg: Council of Europe, 2010, lk 7.

- andmeid tuleb säilitada viisil, mis välistab andmesubjekti identifitseerimise pärast säilitamise eesmärgi kadumist.

Konventsioon näeb ette ka andmesubjekti tutvuda tema kohta kogutud andmetega ning teatud juhtudel taotleda andmete parandamist ning kustutamist (individuaalse osaluse põhimõte). Samuti nähakse konventsioonis ette reeglid piiriüleseks andmevahetuseks.

Konventsiooni art 3 lg 1 kohaselt kohaldub konventsioon automatiseeritud andmetöötlusele nii era- kui avalikus sektoris ning liikmesriikidel on võimalik art 3 lg 2 alusel teha konventsiooni kohaldamisest erandeid. Võimalikud erandid ei sisalda aga võimalust välistada kohaldamisalast andmete töötlemine kriminaalmenetluses. Seega võib järeldada, et konventsioon 108 on kohaldatav ka kriminaalmenetluse raames toimuva andmetöötluse suhtes. Kuigi üldjuhul ei ole konventsiooni võtmesätetest[69] erandite tegemine lubatud, võimaldab konventsiooni art 9 lg 2 riikidel siiski teha sellest üldreeglist erandeid ning kitsendada kohaldamist teatud valdkondades. Art 9 lg 2 annab osalisriikidele võimaluse teha konventsiooni teatud sätetest erandeid, kui see on vajalik riigi julgeoleku, avaliku korra, riigi rahaliste huvide kaitseks või kuritegevuse vastases võitluses (p a) või kui erand on vajalik andmesubjekti või muu isiku õiguste kaitseks (p b). Seejuures on oluline, et erandite tegemine peab olema siseriiklikus õiguses täpselt reguleeritud ning piiritletud. Konventsiooni art 9 lg 2 kohaselt on erandi tegemine lubatud üksnes kui "see on lubatud osalisriigi õiguses ning on demokraatlikus ühiskonnas vajalik meede". Konventsiooni peetakse jätkuvalt fundamentaalse tähtsusega õigusaktiks seoses andmetöötlusega kriminaalõiguse valdkonnas.[70] Autor käsitleb erandi kohaldamist Eesti õiguses käesoleva töö järgmises peatükis.

Arvestades kriminaalmenetluse ja politseitöö eripärasid ja asjaolu, et nendes valdkondades toimub väga ulatuslik isikuandmete töötlemine, võttis ministrite nõukogu 1987.a soovituse nr 15[71], millega reguleeritakse isikuandmete kasutamist politsei valdkonnas. Soovituse eesmärk on kehtestada kindlad andmekaitsereeglid politseiülesannete täitmises, arvestades seejuures valdkonna spetsiifikat ning kohendades reeglid vastavalt.[72] Kuigi soovitus ei ole oma olemuselt

[69] Siinkohal viidatakse konventsiooni artiklile 5 (andmetöötluse üldpõhimõtted), art 6 (andmete eriliikide töötlemine) ja art 8 (andmesubjekti õigused).
[70] D. Alonso Blas. First and Third Pillar: Need for a Common Approach on Data Protection? - Gutwirth, S. jt (toim). Reinventing Data Protection? Springer Science+Business Media B.V., 2009, lk 227.
[71] Recommendation No R (87) 15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector. Arvutivõrgus: https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2196553&SecMode=1&DocId=694350&Usage=2 (04.05.2015).
[72] Data Protection. Complilation of texts, 2010, lk 10.

siduv,[73] on see siiski üks põhilisi dokumente andmekaitse kohta politseitöö valdkonnas ning arvukad EL õigusaktid viitavad sellele.[74]

Soovituse kohaldamisalasse kuuluvad eelkõige politseiasutused. Siiski tuleks meeles pidada, et arvestades õigussüsteemide erinevusi võib pädeva asutuse mõiste olla varieeruv.[75] Eesti kontekstis näiteks hõlmaks soovituse kohaldamisala lisaks politseile ka teisi uurimisasutusi, kellel on süütegude ennetamise ja menetlemise pädevus. Siinkohal ongi asutuse definitsioonist olulisem tähelepanu pöörata ülesannetele, mida asjaomane asutus täidab, ning seatud eesmärkidele. Soovituse seletuskirja kohaselt on reguleerimisala seotud "politsei rolli lõplikkusega" (*finality of police purposes*), mille sisustamisel tuleb arvesse võtta kaitstavaid ühiskonnahuve. Siiski eristatakse soovituses kahte liiki ülesandeid, mida pädevad asutused täidavad - kuritegude vastu võitlemine ning ennetamine ja avaliku korra säilitamine.[76]

Soovituses on kaheksa põhimõtet selle kohta, kuidas tuleks politseitöös isikuandmeid töödelda. Põhimõtted on oma sisult sarnased üldistele andmekaitsepõhimõtetele, sh konventsioonis 108 sätestatule, kuid on sõnastatud märkimisväärselt paindlikumalt, võimaldades seeläbi pädevatel asutustel põhimõtete laiemat tõlgendamist.

Andmete kogumine peaks olema politseitöös lubatud üksnes juhul, kui see on vajalik tegeliku ohu vältimiseks või kuriteo takistamiseks. Siinjuures on asjakohane märkida, et nii ohu vältimine kui ka kuriteo takistamine kuuluvad Eesti õiguse kontekstis eelkõige korrakaitseõiguse valdkonda. Kõik erandid kõnealusest reeglist peaksid põhinema ainult siseriiklikul õigusel. Soovitus 2.4 käsitleb delikaatseid isikuandmeid ning üldiselt keelab selliste andmete kogumise, välja arvatud juhul, kui see on äärmiselt vajalik konkreetse taotluse lahendamiseks. Neljas põhimõte rõhutab, et politsei poolt kogutud andmeid tuleks kasutada ainult nende kogumise eesmärkidel. Samuti reguleeritakse soovituses isiku õigused tema kohta käivate andmete osas (õigus tutvuda, vaidlustada, parandada ning samuti ka info avalikustamine), andmevahetust nii politseiasutuste siseselt kui väljaspool, turvameetmeid ning säilitamise perioode.[77]

Euroopa Liidus reguleerib andmekaitset üldõigusaktina 1995. a vastu võetud direktiiv nr 95/46/EÜ. Direktiivi sätted kohalduvad artikli 3 lg 1 kohaselt isikuandmete täielikult või

[73] Teave Euroopa Nõukogu kodulehelt. Arvutivõrgus: http://www.coe.int/t/cm/aboutCM_en.asp (04.05.2015).
[74] F. Boehm, 2012, lk 96.
[75] Soovituse (87) 15 seletuskiri. Arvutivõrgus: https://wcd.coe.int/ViewDoc.jsp?id=704861&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383 (04.05.2015).
[76] *ibid*
[77] *ibid*

osaliselt automatiseeritud töötlemisele ning isikuandmete automatiseerimata töötlemisele, kui sellised andmed kuuluvad kataloogi või neid soovitakse hiljem kataloogi kanda. Direktiivi üks eesmärke on kaitsta EIÕK art 8 ning EL õiguse üldpõhimõtetes tunnustatud põhiõigusi ja -vabadusi, eelkõige õigust eraelu puutumatusele. Seejuures on aga oluline, et EL-is peab tagatav kaitse tase olema teistes rahvusvahelistes õigusaktides sätestatust kõrgem (põhjenduspunkt 10). Direktiivi artikkel 3 lg 2 näeb ette kaks erandit, millistel juhtudel direktiivi sätted kohaldamisele ei kuulu. Direktiivi kohaldamisalast on muuhulgas välistatud töötlemine, mis leiab aset valdkodades, mis jäävad väljapoole Euroopa Liidu pädevust (selle alla paigutub näiteks riigikaitse). Samuti ei kehti direktiiv sellise töötlemise suhtes, mis on seotud avaliku korra, riigikaitse, riigi julgeoleku ja riigi toimingutega kriminaalõiguse valdkonnas.

Arvestades kuni EL lepingu ja EL toimimise lepingu muudatuste jõustumist kehtinud nn kolme samba süsteemi[78] erinevad andmekaitsereeglid kriminaalõiguse valdkonnas oluliselt nendest, mis on kehtestatud siseturuvaldkonnas. Liidu pädevus nn kolmanda samba valdkonnas ehk politsei- ja õigusalases koostöös kriminaalasjades[79] oli oluliselt piiratud ning õigusaktide vastuvõtmine ühehäälsuse nõude tõttu äärmiselt keeruline. Just varem kehtinud sambasüsteem on põhjuseks, miks direktiiv 95/46/EÜ sisaldab erandit politsei- ja kriminaalõigusalase koostöö kohta.[80] Direktiivi 95/46/EÜ kohaldamisala on Euroopa Kohtu poolt erinevatel ajahetkedel täpsustatud ning muutunud.[81] Näiteks leidis Euroopa Kohus 2003.a kohtuasjas *Österreichischer Rundfunk*, et direktiivi 95/46/EÜ tuleb tõlgendada EIÕK art 8 valguses, mis omakorda kuulub EL õiguse aluspõhimõtete hulka. Samuti märkis kohus, et direktiiv 95/46/EÜ hõlmab oma põhiõiguste kaitsele suunatud iseloomu tõttu mitmeid muid valdkondi ilma, et tuleks igakordselt tõendada seotuse siseturu arendamisega.[82] 2006.a kinnitas Euroopa Kohus vaidluses lennureisijate broneeringuinfo Ameerika Ühendriikidesse edastamise üle lõplikult, et andmekaitsedirektiiv ei kohaldu õiguskaitsevaldkonnale. Kohus leidis, et kuigi lennureisijate broneeringuinfo algne kogumine leiab aset lennuettevõtjate majandustegevuses, tuleb arvesse võtta andmete õiguskaitseasutustele edastamise eesmärki, milleks on süütegude ennetamine ja uurimine ning seega ei kuulu direktiivi 95/46/EÜ kohaldamisalasse.[83]

[78] EL nn sammaste süsteemi selgitus EL õigusloome kodulehel. Arvutivõrgus: http://europa.eu/legislation_summaries/glossary/eu_pillars_en.htm.
[79] *Ibid.*
[80] F. Boehm. 2012, lk 107.
[81] *Ibid*, lk 109
[82] *Ibid*, lk 110.; EKo 20.05.2003, C-465/00, *Rechnungshof vs ÖsterreichischerRundfunk*, p 68.
[83] EKo 30.06.2006, C-317/04 ja C-318/04, *Euroopa Parlament vs nõukogu ja komisjon*, p 54-60.

Siiski tuleb tõdeda, et Euroopa Kohtu lähenemine ei ole alati järjepidev. Ühe vaieldava õigusliku aluse ja kohaldamisalaga on ka direktiiv 2006/24/EÜ, mis käsitleb üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist (*edaspidi direktiiv 2006/24/EÜ* või *andmete säilitamise direktiiv*).[84] Direktiiviga luuakse sideettevõtjate kohustus säilitada teatud informatsiooni, eesmärgiga võimaldada sellise info kättesaadavust tõsiste süütegude uurimise, avastamise ja kohtus menetlemiseks[85] (art 1 lg 2). Sellele vaatamata leidis kohus oma otsuses C-301/06 Iirimaa *vs* Parlament ja nõukogu, et tegemist on korrektsel õiguslikul alusel EL nn esimese samba raames vastu võetud direktiiviga, kuivõrd reguleeritakse üksnes sideettevõtjate kohustusi ning mitte edasist andmete edastamist õiguskaitseasutustele.[86]

Vaatamata sellele, et andmekaitsedirektiiv *de iure* kriminaalmenetluse valdkonnale ei kohaldu, on sellel siiski oluline roll EL andmekaitseõiguse tõlgendamisel. Seejuures on asjakohane märkida, et kuigi EL ei ole ette näinud direktiivi sätete kohaldamist õiguskaitsevaldkonnale, on selles sätestatud põhimõtted siiski jõudnud Eesti õigusesse, kuivõrd isikuandmete kaitse seadus, millega direktiiv üle võeti, ei välista kriminaalmenetlust täielikult kohaldamisalast. Seega on direktiiv sätetel oma roll Eesti kriminaalmenetluses, sest just direktiivi valguses tuleb tõlgendada IKS-i sätteid, samuti kohalduvad mitmed IKS-i sätted kriminaalmenetluses.

Andmekaitsedirektiiv ei ole siiski kaugeltki ainus õigusakt, mis reguleerib isikuandmete kaitse valdkonda EL-is ja selle liikmesriikides. Andmekaitsevaldkonda reguleerivad mitmed teisedki õigusaktid, millest mõnel on tähendus ka kriminaalmenetluses. Rääkides aga sektoriülestest õigusnormidest, väärib kriminaalmenetluse kontekstis kindlasti ära märkimist nõukogu 2008.a raamotsus 2008/977/JSK kriminaalasjades tehtava politsei- ja õigusalase koostöö raames töödeldavate isikuandmete kaitse kohta.[87]

Raamotsuse eelnõu koostamisel 2005.a oli selle eesmärgiks reguleerida andmekaitset endise nn kolmanda samba valdkonnas ehk politsei- ja õigusalase koostöö raames. Algselt esitatud

[84] Euroopa Parlamendi ja nõukogu direktiiv 2006/24/EÜ, mis käsitleb üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist ja millega muudetakse direktiivi 2002/58/EÜ. ELT L 105, 13.04.2006, lk 54 - 63. Arvutivõrgus: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:ET:PDF (04.05.2015).
[85] Inglise keeles kasutatakse termineid *investigation, detection and prosecution.* Eesti keeles ei ole täpset vastet terminile *prosecution* ning direktiivi ametlikus tõlkes on kasutatud ühendit "kohtus menetlemine". Siiski tuleb märkida, et inglisekeelne sõna *prosecution* on laiem ning hõlmab nii kohtumenetlust kui ka kohtueelset menetlust prokuratuuris.
[86] EKo 10.02.2009, C-301/06 *Iirimaa vs Parlament ja Nõukogu*, 74 - 85.
[87] Nõukogu raamotsus 2008/977/JSK, 27.11.2008, kriminaalasjades tehtava politsei- ja õigusalase koostöö raames töödeldavate isikuandmete kaitse kohta. ELT L 350, 30.12.2008, lk 60 – 71.

ettepanek oli piisavalt ambitsioonikas ning lähtus suuresti andmekaitsedirektiivi põhimõtetest ja sätetest. Raamotsus oli kavandatud kohalduma nii siseriiklikult toimuvale andmetöötlusele kui ka piiriülesele andmevahetusele.[88] Arvestades, et politsei- ja õigusalase koostöö valdkond oli eristaatuses ning valdkonna õigusaktide vastuvõtmiseks oli vaja saavutada ühehäälsust, liikusid eelnõu arutelud vaevaliselt. Pärast mitmeid muudatusi, ümberkirjutamisi ning pikki vaidlusi jõudis nõukogu raamotsuse vastuvõtmiseni 2008.a lõpus.[89] Selleks ajaks oli ettepanek muutunud oluliselt lahjemaks ning muuhulgas jäi raamotsuse kohaldamisalast välja kogu siseriiklik andmetöötlus õiguskaitseasutuste poolt. Seega kohaldub raamotsus üksnes piiriülesele andmetöötlusele liikmesriikide vahel ning andmevahetusele EL-i mittekuuluvate riikidega (art 1 lg 2).

Tuleb tõdeda, et raamotsus ei ole kindlasti võrdväärne direktiiviga 95/46/EÜ. Raamotsuse suurimaid puudujääke on selle kohaldamisala. Nagu eespool mainitud, kohaldub raamotsus üksnes piiriülesele andmevahetusele ega ei kohaldu andmetöötlusele liikmesriikide siseselt. Seega on raamotsuse kohaldamisalast väljas näiteks kogu andmetöötlus, mis leiab aset Eesti politsei ja prokuratuuri poolt. Märkimisväärne on ka see, et raamotsus ei kohaldu ka õiguskaitsevaldkonnas asutatud EL agentuuridele nagu Europol või Eurojust. Arvestades raamotsuse piiratud kohaldamisala on väga küsitav, milline on raamotsuse praktiline väärtus. Nimelt andmete kogumise hetkel liikmesriigis ei ole üldjuhul võimalik ette näha, kas andmed tuleb mingil ajahetkel edastada teise liikmesriiki, mis omakorda on eeldus raamotsuse reeglite kohaldumisele.[90]

Raamotsuse teiseks nõrkuseks peetakse selle tagatavat andmekaitsetaset.[91] On ilmne, et arvestades politseitöö ja kriminaalmenetluse valdkonna eripärasid ei ole siinkohal võimalik täies ulatuses lähtuda direktiivis 95/46/EÜ kehtestatud reeglitest, kuivõrd kaitstavate huvide ja väärtuste tasakaal on teine. Siiski leiab ka raamotsusest viiteid vajadusele tagada kõrgetasemeline andmekaitse EL-is (põhjenduspunktid 10 ja 16, art 1 lg 1). Paratamatult hinnatakse aga raamotsust alati võrdluses direktiiviga ning siinkohal pole raamotsusel midagi vastu panna. Samuti tuleb aga arvestada, et direktiivi eesmärk on tagada võimalikult kõrge andmekaitsetase eelkõige olukorras, kus ettevõtted püüavad isikuandmeid kasutades oma

[88] P. De Hert, V. Papakonstantinou. The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for. - Computer Law and Security Review. 2009/25, lk 406-407.
[89] *Ibid*, lk 407-408.
[90] H. Hijmans, A. Scirocco. Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty be Expected to Help? Common Law Market Review, 2009/46, lk 1494.
[91] *Ibid*, lk 1494.

kasumit suurendada, samas kui politsei eesmärgid on suunatud isikute põhiõiguste, turvalisuse ja avaliku korra kaitsele.[92] Kuigi raamotsuses ettenähtud erandite loetelu on küllaltki lai, puuduvad sellest näiteks soovituses (87) 15 ettenähtud lisatagatised andmesubjektidele. Hijmans ja Scirocco toovad siinkohal näite raamotsuse artiklist 11, mille kohaselt on andmete kasutamine lubatud mistahes muul eesmärgil võrreldes andmete edastamise algse eesmärgiga, kui andmeid edastav liikmesriik sellega nõustub.[93] Raamotsuse

Lisaks eelpool käsitletud raamotsusele on ELis teisigi andmekaitsealaseid regulatsioone, mis kohalduvad õiguskaitsevaldkonnas. Siiski on tegemist sektoraalsete õigusaktidega, mis reguleerivad väga konkreetseid olukordi. Näiteks on oma andmekaitsereeglistik nii erinevatel EL-i agentuuridel, näiteks Europolil[94] ja Eurojustil[95], samuti Schengeni konventsioonis[96], erinevate õiguskaitsevaldkonna andmebaase reguleerivates õigusaktides,[97] biomeetriliste andmete edastamist käsitlevates nn Prüm otsustes.[98] Järgmises peatükis käsitleb autor lähemalt andmekaitse erireeglite kohaldamist, kuivõrd nendes välja toodud aspektid on rangelt sektoraalsed ega oma laiemat kohaldatavust.

Võib öelda, et õiguskaitsevaldkonna andmekaitsealane regulatsioon sisaldab küll üldist reeglistikku, mis aga sisaldab väga suurt hulka erandeid ja erireegleid. Sageli ei ole selge, millised õigusnormid teatud olukordades kohalduvad ning kuidas tuleks lahendada tekkivad normikollisioonid. EL-is puudub õiguskaitsevaldkonnas kindel ja stabiilne õigus ning olemasolevat olukorda võib defineerida lapitekiks.[99]

Euroopa Liit on teadlik kirjeldatud õigusliku regulatsiooni puudustest, mistõttu esitas Euroopa Komisjon 2012.a jaanuaris uue andmekaitse reformipaketi, kuhu kuulub andmekaitse üldmääruse eelnõu,[100] mis peaks reguleerima andmekaitset era- ja avalikus sektoris, ning

[92] P. De Hert, V. Papakonstantinou, 2009, lk 411.
[93] H. Hijmans, A. Scirocco,. 2009, lk 1494.
[94] Nõukogu otsus, 6.04.2009, millega asutatakse Euroopa Politseiamet (Europol) (2009/371/JSK). ELT L 121, 15.05.2009, lk 37 – 66.
[95] Nõukogu otsus, 28.02.2002, millega moodustatakse Eurojust, et tugevdada võitlust raskete kuritegude vastu (2002/187/JSK). ELT L 63, 06.03.2002, lk 1 – 13.
[96] Konventsioon, 14.05.1985, millega rakendatakse 14.06.1985.a Schengeni lepingut Beneluxi Majandusliiku riikide, Saksamaa Liitvabariigi ja Prantsuse Vabariigi valitsuste vahel nende ühispiiridel kontrolli järkjärgulise kaotamise kohta. ELT L 239, 22.09.2000, lk 19 – 62.
[97] Näiteks nõukogu otsus, 2007/12.06.2007, mis käsitleb teise põlvkonna Schengeni infosüsteemi (SIS II) loomist, toimimist ja kasutamist. - ELT L 205 / 07.08.2007, lk 63 – 84.
[98] Nõukogu otsus, 2008/615/JSK, 23.06.2008, piiriülese koostöö tõhustamise kohta, eelkõige seoses terrorismi- ja piiriülese kuritegevuse vastase võitlusega. - ELT L 210, 06.08.2008, lk 1 - 11. Nõukogu otsus, 2008/616/JSK, 23.06.2008, millega rakendatakse otsust 2008/615/JSK piiriülese koostöö tõhustamise kohta, eelkõige seoses terrorismi- ja piiriülese kuritegevuse vastase võitlusega. - ELT L 210, 06.08.2008,, lk 12 – 17.
[99] H. Hijmans, A. Scirocco, 2009, p 1496.
[100] Euroopa Komisjon. Ettepanek: Euroopa Parlamendi ja Nõukogu määrus üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (isikuandmete kaitse üldmäärus). COM (2012) 11 final,

õiguskaitsevaldkonna andmekaitsedirektiivi eelnõu, mis kohalduks andmete töötlemisele politseitöös ja kriminaalmenetluses. Seejuures on oluline mainida, et komisjoni eelnõu kohaselt soovitakse kehtestada uue direktiivi reeglid ka siseriiklikule andmetöötlusele (eelnõu art 2).

Eestis reguleerib andmekaitsevaldkonda üldõigusaktina isikuandmete kaitse seadus (*edaspidi IKS*). IKS-is reguleeritakse isikuandmete töötlemise tingimused ja kord, isikuandmete töötlemise riikliku järelevalve kord ning vastutus isikuandmete töötlemise nõuete rikkumise eest. Nagu varasemalt märgitud, on IKS-iga üle võetud nii direktiiv 95/46/EÜ kui ka konventsioon 108. Ühtlasi nähtub Eesti poolt Euroopa Komisjonile edastatud infost, et IKS võtab üle ka raamotsuse 2008/977/JSK.[101]

IKS-i eesmärk on sõnastatud § 1 lg-s 1 ning selleks on füüsilise isiku põhiõiguste ja -vabaduste, eelkõige eraelupuutumatuse kaitse isikuandmete töötlemisel. IKS § 2 sätestab seaduse kohaldamisala. Tegemist on õigusaktiga, mille kohaldatavus on üsna lai ning selle kohaldamisalast ei ole välistatud ka isikuandmete töötlemine kriminaalmenetluses. Siiski on IKS-is ka käesoleva töö vaatevinklist olulised sätted, mis sätestavad IKS-i kohaldumise eriolukorrad. Esiteks on märkimisväärne, et IKS kohaldub ka kriminaalmenetlusele ja kohtumenetlusele, kuid vastavates menetlusseadustikes ette nähtud eranditega (IKS § 2 lg 2). Kriminaalmenetluse seadustikus puudub sõnaselge regulatsioon isikuandmete kaitse kohta, mistõttu on IKS § 2 lg 2 sätestatu praktiline kohaldamine küsitav. Samuti ei kohaldata IKS-i üldjuhul riigisaladuse töötlemisele ning sellele viitab IKS § 2 lg 3, mis näeb ette piiratud juhud, millal on siiski vajalik riigisaladuse töötlemisel IKS-is lähtuda. Kriminaalmenetluse vaatevinklist on oluline aga see, et riigisaladuseks on ka jälitusteave (riigisaladuse ja salastatud välisteabe seaduse[102] §-d 8 ja 9).

25.01.2012. Arvutivõrgus: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_et.pdf (04.05.2015).

[101] Euroopa Komisjon. Komisjoni aruanne Euroopa Parlamendile, Nõukogule, Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele nõukogu 27. novembri 2008. aasta raamotsuse (kriminaalasjades tehtava politsei- ja õigusalase koostöö raames töödeldavate isikuandmete kaitse kohta) artikli 29 lõike 2 alusel. COM (2012) 12 final, 25.01.2012. Arvutivõrgus: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0012:FIN:ET:PDF (04.05.2015).
European Commission. Commission Staff Working Document. Annex Accompanying the document: Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions based on Article 29 (2) of the Council Framework Decision of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. SEC (2012) 75 final, 25.01.2012. Arvutivõrgus: http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_75_en.pdf (04.05.2015).

[102] Riigisaladuse ja salastatud välisteabe seadus. - RT I 2007, 16, 77 ... RT I, 22.12.2011, 24.

1.4 Isikuandmete töötlemine kriminaalmenetluses

KrMS § 211 lg 1 kohaselt on kohtueelse menetluse eesmärgiks tõendusteabe kogumine ja kohtumenetluseks vajalike tingimuste loomine. Tõendamisel tuleb tuvastada kuriteo toimepanemise aeg, koht, viis ja muud tehiolud, kuriteokoosseis, kuriteo toimepannud isiku süü ning isiku vastutust mõjutavad asjaolud (KrMS § 62). Kriminaalmenetluse käigus kogub menetleja tõendeid ja seega ka tõenditel kajastuvaid isikuandmeid (sh delikaatseid isikuandmeid) menetlustoimingute raames.[103] Seejuures on oluline eristada tõendi ja tõendis sisalduda võivate isikuandmete erinevat tähendust menetluses. KrMS § 63 annab tõendi definitsiooni, sätestades tõendi mõiste läbi kriminaalmenetluses lubatavate tõendite loetelu. Võib väita, et peaaegu kõik tõendid sisaldavad suuremal või vähemal hulgal isikuandmeid, näiteks teavet tunnistajate kohta, süüdistatava isikukood, ekspertiisiakti kantud DNA-profiil jt. Siiski ei ole isikuandmete kogumine tõendamise eesmärk omaette ning tõendi kogumise tähendus kriminaalmenetluses on selgelt erinev. Võib eeldada, et isikuandmete töötlemine leiab aset alates esimese menetlustoimingu tegemisest, millega kriminaalmenetlus alustatakse ning kuni kohtuotsuse või -määruse täitmisele pööramiseni. Seejuures ei lõpe andmete töötlemine lahendi jõustumisega, vaid võib jätkuda määramata aja jooksul, kuivõrd üldjuhul jõustunud kohtuotsus või -määrus avalikustatakse (KrMS § 408[1]).[104]

Nagu esimeses peatükis käsitletud, hõlmab IKS-i kohaldamisala teatud eranditega ka andmetöötlust kriminaalmenetluses. Vastavalt IKS § 2 lg-le 2 kohaldatakse seaduse sätteid mh ka kriminaalmenetlusele, kuid menetlusseadustikes sätestatud eranditega. Antud juhul peaksid asjakohased erandid olema sätestatud KrMS-s. Siinkohal tasub märkida, et KrMS kui kohtumenetluse valdkonda reguleeriv seadus on PS § 104 tähenduses konstitutsiooniline seadus, mille vastuvõtmine ja muutmin eeldab Riigikogu koosseisu häälteenamust (PS § 104 p 14). IKS on omakorda lihtseadus ning sellele kohalduvad üldised seaduse vastuvõtmise reeglid ning vastuvõtmiseks piisab kohal viibivate Riigikogu liikmete poolthäälte enamusest (PS § 73).[105] Arvestades põhimõtet *lex superior derogat legi inferiori* ei teki kahtlust, et KrMS võib sätestada IKS-ist erandeid. Küll aga võib küsida, kas IKS võib olla KrMS osas üldseadus,

[103] M. Männiko. Õigus privaatsusele ja andmekaitse. Tallinn: Juura, 2011, lk 201.
[104] Kohtulahendite avalikustamise temaatikat ning sellega kaasnevat põhiõiguste riivet on põhjalikult käsitlenud T. Hansen oma 2012.a magistritöös "Õigus eraelu puutumatusele *vs* kohtulahendi avalikustamine", Tartu: Tartu Ülikool, 2012.
[105] L. Madise, A. Mõttus jt. PS § 73 / 1.2.

kuivõrd sel moel IKS reguleerib osaliselt ka kriminaalmenetluse, sh kriminaalkohtumenetluse läbiviimise tingimusi.

Üldaktsepteerituks peetakse seisukohta, et lihtseadusega ei tohi minna konstitutsioonilise seaduse põhisisu kallale.[106] Riigikohus on kõnealust küsimust käsitledes leidnud, et konstitutsiooniliste seaduste reguleerimisvaldkonda kuuluvate suhete reguleerimine lihtseadustega on põhiseadusvastane, samuti ei ole konstitutsioonilistes seadustes lubatud viited lihtseadustele ega delegatsioonid täitevvõimu üldakti andmiseks küsimustes, mis oma olemuselt kuuluvad konstitutsiooniliste seaduste reguleerimisesemesse.[107] Tõlgendades Riigikohtu seisukohta võib jõuda kahele erinevale järeldusele: lihtseaduses viitamine konstitutsioonilises seaduses ei ole üldse lubatud või on viitenormid siiski lubatud juhul, kui nendega ei reguleerita olemuslikult konstitutsioonilise seaduse reguleerimiseset.[108] Viimast seisukohta on toetanud ka Riigikohtu hilisem praktika.[109] Seega tuleks käesoleval ajal kehtivale Riigikohtu praktikale tuginedes tuvastada, kas IKS-i sätted, mis kriminaalmenetluse valdkonnale kohalduvad, reguleerivad olemuslikult KrMS-i sisu.

Esiteks tuleb siinkohal märkida, et PS § 104 lg 2 nõuab Riigikogu koosseisu häälteenamust üksnes kohtumenetluse valdkonna reguleerimiseks, kuid KrMS sisaldab nii kohtumenetlust kui ka kohtueelset menetlust, karistuse täitmisele pööramist jt erivaldkondi reguleerivaid sätteid. Riigikohus jõudis seejuures seisukohale, et PS § 104 lg-s 2 sätestatud nõude kehtimiseks ei pea tegemist olema tingimata menetlusseadustikuga, vaid säte kohaldub ka valdkonnaseaduste puhul, millega muuhulgas reguleeritakse üksikuid kohtumenetlust puudutavaid küsimusi.[110] Seega põhimõtteliselt saaks IKS-is igal juhul reguleerida neid küsimusi, mis ei puuduta kriminaalkohtumenetluse osa. Küll aga on keerulisem tuvastada, kas isikuandmete kaitse valdkond kuulub kohtumenetluse sisu juurde. Üldiselt võib arvata, et andmekaitse ei kuulu nende küsimuste hulka, mida PS § 104 lg 2 tähenduses tuleks käsitleda kohtumenetluse olemust reguleerivana. Siiski võib olukord osutuda keerulisemaks, kui IKS-ist tulenevate nõuete tõttu takerdub kohtumenetluse läbiviimine. Siinkohal saab näiteks tuua andmete piiriülest edastamist, mida autor käsitleb lähemalt käesoleva töö kolmandas peatükis. Etteruttavalt võib aga märkida, et kuivõrd teatud andmevahetuse olukorrad ei ole KrMS-is reguleeritud, tuleb lähtuda IKS-is sätestatust ning seega võib IKS-ist tuleneva andmete edastamisele kehtestatud

[106] V. Saarmets. Konstitutsioonilistest seadustest. – Õiguskeel 2009 / 4, lk 10.
[107] RKPJKo 3-4-1-1-98, p 4.
[108] A. Mõttus jt. PS § 104 / 8.
[109] RKHKo 3-3-1-42-08, p 14.
[110] RKPJKo 3-4-1-54-15, p 47-52.

tingimuse mittetäitmine luua olukorra, kus kohtumenetluses ei ole võimalik edastada andmed välismaale, kuigi see on menetluse huvidest lähtuvalt vajalik. Selliselt võib aga tekkida olukord, kus lihtseadus mõjutab oluliselt konstitutsioonilise seaduse peamist reguleerimiseset ning „takistab“ konstitutsioonilise seaduse toimimist. Autori hinnangul ei ole IKS-i ja KrMS-i kui üld- ja eriseaduse suhe piisavalt selge ning vajab põhjalikumat piiritlemist. Lahenduseks oleks autori arvates kõigi olulisemate andmekaitsealaste erandite ja nõuete reguleerimine KrMS-is, välistades sellega olukorrad, kus IKS-i normid raskendavad oluliselt KrMS-i rakendamist.

Konventsioon 108 on käesoleval ajal omakorda ainus siduv rahvusvaheline instrument Euroopas, mis sätestab üldised andmekaitsestandardid, kohaldub laiemalt tervele kriminaalmenetlusele.[111] Vaatamata konventsiooni kohaldamisala ulatusele lubab see siiski teha teatud erandeid mh ka kuritegevusevastase võitluse eesmärgil, kui erandi võimalikkus on sätestatud osalisriigi õiguses. Sellest lähtuvalt võib eeldada, et IKS § 2 lg 2 ettenähtud erand on konventsiooni reeglitega kooskõlas. Siiski tuleb enne lõppjärelduse tegemist pöörata tähelepanu sellele, kuidas on konventsioonis sätestatud erandite tegemine lubatud.

Konventsiooni art 9 lg 2 lubab kriminaalmenetluse huvides teha erandeid juhul, kui sellised kitsendused "on lubatud osalisriigi õigusega ning osutuvad demokraatlikus ühiskonnas vajalikuks."[112] Arvestades, et konventsioon põhineb EIÕK art-l 8, on ka selles sätestatud erandite tegemise võimalikkuse piirid määratletud EIÕK art 8 lg-ga 2, mis kasutab sarnast sõnastust.[113] Selgitamaks välja, kui kaugele ulatub erandite tegemise lubatavus, tuleks seega hinnata, milline on nii EIÕK art 8 lg 2 kui ka konventsiooni 108 art 9 lg 2 tähenduse piirid. EIK on oma tõlgendustes olnud pigem seisukohal, et EIÕK art 8 lg 1 tuleb tõlgendada laialt, art 8 lg 2 aga kitsalt.[114] [115] EIK on asunud seisukohale, et piirangu kasutamine on õiguspärane, kui mõistet "lubatud õiguses" (*in accordance with the law*) tõlgendada kolme kriteeriumi valguses. Esiteks peab kasutatav sekkumismeede olema siseriiklikus õiguses reguleeritud. Seejärel tuleb aga hinnata siseriikliku õiguse kvaliteeti. Vastavad õigusnormid peavad olema isikule

[111] D. Alonso Blas, 2010, lk 226-227.
[112] Inglisekeelne sõnastus on "[...] derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interest of [...]". Prantsuse keeles on sõnastus järgmine: "[...] dérogation prévue par la loi de la Partie, constitue une mesure nécessaire dans une société démocratique [...]".
[113] EIÕK art 8 lg 2 sõnastuses on piirang lubatud kui see on "kooskõlas seadusega" (inglise keeles *in accordance with the law,* prantsuse keeles *est prévue par la loi*). Autor on seisukohal, et vaatamata konventsiooni 108 art 9 lg 2 ning EIÕK art 8 lg 2 eesti- ja inglisekeelsete sõnastuste mõningale erinevusele on sätte tähendus ning piirangu ulatus sama.
[114] National security and European Case Law. Strasbourg: Council of Europe / European Court of Human Rights 2013, lk 2. Arvutivõrgus: http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/Jurisprudence%20CEDH_En%20%28final%29.pdf (04.05.2015).
[115] EIKo 06.09.1978, 5029/71, *Klass vs Saksamaa,* p 40 - 60.

kättesaadavad ning nende normide tagajärjed peavad olema ettenähtavad.[116] Kuigi kohus on hinnanud õigusnormide ettenähtavust eelkõige salajase pealtkuulamise valguses, võib siiski kohtupraktikast teha laiema järelduse, et "ettenähtav" õigusnorm peab andma isikule adekvaatse teabe nende tingimuste ja asjaolude kohta, mille korral on pädevatel asutustel lubatud kasutama isiku eraellu sekkuvaid meetmeid. Seadusest peab selgelt tulenema pädevale asutusele antud diskretsiooni piirid ning selle kasutamise kord.[117] Nii EIÕK art 8 lg 2 kui konventsiooni 108 art 9 lg 2 sätestatud piirangute lubatavuse hindamisel tuleb teise kriteeriumina hinnata vajalikkust demokraatlikus ühiskonnas. Nagu varasemalt märgitud, on EIK tõlgendanud seda sätet proportsionaalsuse valguses ning eelkõige hinnanud meetme sobivust, vajalikkust ning mõõdukust taotletava eesmärgi suhtes.

Eeltoodule tuginedes asub autor seisukohale, et IKS § 2 lg 2 sätestatud kohaldamisala piiramine kriminaalmenetluse suhtes on laiemas plaanis kooskõlas EIÕK ning konventsiooni 108 nõuetega, kuid seda üksnes juhul, kui vastavad erireeglid on KrMS-s selgelt sätestatud ning taotletava eesmärgi suhtes proportsionaalsed.

Proportsionaalsuse hindamisel tuleb lähtuda nii konkreetse meetme või piirangu kui ka kriminaalmenetluse kui terviku eesmärkidest. Arvestades, et kriminaalmenetlus on suunatud riigi õiguskorra kaitsmisele ning seeläbi isikute põhiõiguste tagamisele, ei teki kahtlust, et kõnealuse ülesande täitmiseks on pädevatel asutustel õigus kasutada erinevaid meetodeid ja tehnoloogiaid vajaliku info kogumiseks. Samas tuleb meeles pidada, et karistusõiguse ja kriminaalmenetluse kaudu kaitstavad väärtused peavad olema tasakaalustatud teiste põhiõigustega ning igal juhul tuleb lähtuda tunnustatud põhiõigustesse sekkumise teooriast. Riigi kohustus on luua õiguslik regulatsioon, mis tagaks vajaliku tasakaalu õiguskaitseorganite ülesannete täitmise ja põhiõiguste kaitse vahel.

Erinevalt andmekaitsedirektiivist, mille eesmärgiks on EL siseturu edendamine ning mis sellest tulenevalt näeb ette liikmesriikide õiguse harmoneerimise,[118] kehtestab konventsioon 108 üksnes miinimumreeglid.[119] Seega konventsiooni rakendamisel on osalisriikidel võimalik sätestada siseriiklikus õiguses sellised reeglid, mis tagavad kõrgema isikuandmete kaitse

[116] EIKo 18.05.2010, 26839/05, *Kennedy vs Ühendkuningriik*; EIKo 04.05.2000, 28341/95, *Rotaru vs Rumeenia* jt EIK otsused.
[117] EIKo 08.08.1984, 8691/79, *Malone vs Ühendkuningriik*; EIKo 18.05.2010, 26839/05, *Kennedy vs Ühendkuningriik* jt EIK otsused.
[118] P. Hustinx. EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation. Avaldatud kõne, 2014, lk 9. Arvutivõrgus: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2014/14-09-15_Article_EUI_EN.pdf (04.05.2015).
[119] L. A. Bygrave. 2014, p 36.

taseme kui konventsioon. Siiski on sellise võimaluse kasutamine kriminaalmenetluse valdkonnas küsitav, kuivõrd pigem eeldab kriminaalmenetlus ulatuslikumat sekkumist isiku õigustesse ning seega konventsioonist tulenevate reeglite kitsendamist. Näiteks kehtib Saksamaal andmekaitse osas üldõigusaktina[120] föderaalne andmekaitseseadus (*Bundesdatenschutzgesetz, edaspidi BDSG*)[121], mis kohaldub andmetöötlusele nii avaliku kui erasektori poolt. Siiski sätestab BDSG, et valdkondlike aktide olemasolul tuleb andmetöötlusel lähtuda eelkõige nendest (§ 1 lg 3). Näiteks on selliseks eriseaduseks föderaalne politseiseadus (*Bundespolizeigesetz, BPolG*), mis sätestab isikuandmete töötlemise erireeglid föderaalpolitsei tegevuses (nt BPolG § 21 jt).[122] Lätis kehtib isikuandmete kaitse seadus[123] üldiselt kõigi avaliku või erasektori aset leidvate töötlemistoimingute suhtes samas seaduses sätestatud eranditega (Läti isikuandmete kaitse seaduse § 3 lg 1). Erandeid teeb seadus näiteks teatud andmekaitsepõhimõtete kohaldamisest (§ 10 lg 4) või andmesubjekti õiguste rakendamisest (§ 15 lg 5).

Pädevatele asutustele volituste andmine kodanike privaatsusõigustesse sekkumiseks ei saa põhineda eeldusel, et uurimisasutused või menetlejad ei kuritarvita neile antud õigusi. Tasakaalu saavutamiseks on vaja ette näha selget õiguslikku regulatsiooni ja tõhusat kontrolli õiguskaitseorganite tegevuse üle. Esmane regulatsioon tuleneb juba PS §-st 26 enesest, mille teine lause annab riigile võimalused piirata isiku õigust era- ja perekonnaelu puutumatusele. Samas peavad valdkonnaseadused, antud juhul eelkõige KrMS, omakorda kehtestama selged ning detailsed reeglid, mis tagaksid EIK tõlgendustes välja toodud õigusnormi kvaliteedi ning ettenähtavuse kriteeriumide täitmise. Edaspidi analüüsib autor üldiste andmekaitse aluspõhimõtete kohaldatavust kriminaalmenetluses ning asjakohaste õigusnormide vastavust eelmainitud kriteeriumidele.

[120] Saksamaal kehtivad nii föderaalseadused kui ka liidumaade seadused ning ka andmekaitse valdkonnas kohalduvad sõltuvalt olukorrast kas BDSG, liidumaade andmekaitseseadused, samuti föderaalsed või liidumaade eriseadused. – A. F. V.d. Bussche, M.Stamm. Data Protection in Germany. München: Verlag C.H.Beck, 2013, lk 5-6.

[121] Federal Data Protection Law. – Federal Law Gazette I p 66, 14.01.2003 … Federal Law Gazette I, p 2814, 01.08.2009. Arvutivõrgus: http://www.gesetze-im-internet.de/englisch_bdsg/ (04.05.2015).

[122] Gezetz über die Bundespolizei. – BGBI 19.10.1994 … 20.06.2013.

[123] Personal Data Protection Law. Latvijas Vēstensis 23.03.2000 … Latvijas Vēstensis 06.02.2014. Arvutivõrgus: http://www.dvi.gov.lv/en/legal-acts (04.05.2015).

2 ISIKUANDMETE KAITSE KRIMINAALMENETLUSES

Käesolevas peatükis analüüsib autor isikuandmete kaitse aluspõhimõtete ning nõuete kohaldatavust kriminaalmenetluses. Samuti hindab autor, kas isiku andmekaitsealased õigused kriminaalmenetluses on tagatud ning eraellu sekkumine proportsionaalne. Autor analüüsib siinkohal uuemaid KrMS muudatusi menetlustoimingute puhul, mille põhisisuks on isikuandmete töötlemine. Autor analüüsib, kas vastavad reeglid on kooskõlas isiku põhiõigustesse sekkumise tingimustega ning arvestavad piisavalt andmekaitseõigusest tulenevaid nõudeid.

2.1 Andmekaitse aluspõhimõtete ja - nõuete kohaldatavus kriminaalmenetluses

IKS § 5 annab isikuandmete töötlemise definitsiooni. Isikuandmete töötlemiseks loetakse isikuandmetega mistahes tehtavat toimingut, sh näiteks kogumine, säilitamine, muutmine, avalikustamine, andmetele juurdepääsu võimaldamine, päringute teostamine, kasutamine, edastamine, kustutamine või hävitamine sõltumata toimingu teostamise viisist ja kasutatavatest vahenditest. IKS-is antud isikuandmete töötlemise definitsioon vastab nii andmekaitsedirektiivi art 2 punktis b antud definitsioonile kui ka konventsiooni 108 art 2 punktis c sätestatule. Kriminaalmenetluses toimub isikuandmete töötlemine sisuliselt iga toimingu juures, olgu see andmete kandmine registrisse, tunnistaja ülekuulamine, jälitustoiming, isiku daktüloskopeerimine või süüdistusakti koostamine.

IKS § 6 kohaselt on isikuandmete kaitse aluspõhimõtted töötlemise seaduslikkus, eesmärgipärasus, minimaalsus, kasutuse piiratus, individuaalne osalus ning andmete kvaliteet ning turvalisus. Põhimõtted pärinevad eelkõige konventsiooni 108 art-st 5 ning andmekaitsedirektiivi art-st 6. Arvestades eespool käsitletud IKS-i kohaldumist ka kriminaalmenetluse valdkonnale, tuleb üldjuhul lähtuda nendest põhimõtetest ka menetluse raames andmete töötlemisel. Siiski ei ole IKS-i kohaldamine absoluutne ning seega on eelduslikult võimalik nendest põhimõtetest kõrvalekaldumine, kui vastav erand on KrMS-s ette nähtud. Kindlasti aga peab olema tagatud kooskõla isikuandmete kaitse piiramise ning taotletava eesmärgi vahel. Arvestades, et õigus isikuandmete kaitsele on põhiõigus, tuleb lähtuda põhiõiguste piiramisele sätestatud tingimustest. Põhiseaduse § 11 kohaselt on põhiõiguste piiramise tingimuseks asjaolu, et taoline piirang on demokraatlikus ühiskonnas vajalik ega moonuta piiratava põhiõiguse olemust. Seega KrMS-s sätestatud IKS-i kohaldumise

eritingimuste hindamisel tuleb igakordselt hinnata, kas seadusandja kehtestatud regulatsioon on piisavalt põhjendatud ning kooskõlas PS-ga.

Kõigi IKS §-s 6 sätestatud aluspõhimõtete tagamine kriminaalmenetluses ei pruugi olla alati võimalik. Seaduslikkuse põhimõtte (IKS § 6 p 1) kohaselt on andmete kogumine lubatud üksnes ausal ning seaduslikul teel. Siinkohal tulen märkida, et kuigi IKS § 6 p 1 kehtestab seaduslikkuse põhimõte justkui üksnes andmete kogumisele, tuleks selle kohaldamist siiski laiendada kõigile töötlemistoimingule. Põhimõtte laiemale kehtivusele viitab nii IKS § 6 sissejuhatav lause ("Isikuandmete töötleja on kohustatud isikuandmete töötlemisel järgima järgmisi põhimõtteid [...]") kui ka IKS-i aluseks olevate rahvusvaheliste õigusaktide sätted.[124] Tegemist on andmekaitse ühe olulisima aluspõhimõttega, mis hõlmab ning on aluseks mitmele teisele printsiibile. Andmete seaduslikul teel töötlemise nõue ei ole raskesti sisustatav ning on enesestmõistetav.[125] Arvestades andmekaitsedirektiivi põhjenduspunktis 30 sätestatut võib järeldada, et seadusliku töötlemise tingimused on täidetud, kui isikuandmete töötlemine toimub andmesubjekti nõusolekul või on vajalik seoses andmesubjekti jaoks siduva kokkuleppe sõlmimise või täitmisega, seadusest tuleneva kohustuse, üldiste huvidega seotud ülesande täitmise, avaliku võimu teostamise või mõne füüsilise või juriidilise isiku õigustatud huvidega. Kriminaalmenetluse puhul võib öelda, et üldjuhul põhineb andmete töötlemine seadusel, mistõttu võib eeldada, et seaduslikkuse nõue on täidetud. Oluliselt keerulisem olukord on andmete töötlemise ususe hindamisel. Kuigi ausa töötlemise kontseptsioon võib ajas muutuda, hõlmab see vaieldamatult töötleja kohustuse võtta arvesse andmesubjekti huvid ning põhjendatud ootused. Andmetöötlus peaks toimuma viisil, mis ei sekku põhjendamatult andmesubjekti eraellu ning privaatsusega seotud huvidesse. Ausa töötlemise põhimõtet võib kokku võtta kui töötleja kohustust hoiduda oma seisundi kuritarvitamisest.[126] Käimasoleva andmekaitsereformi järgides võib täheldada, et õiguskaitsevaldkonna andmekaitsedirektiivi läbirääkimistel on EL liikmesriikidele suureks probleemiks olnud muuhulgas ausa töötlemise nõude kehtestamine õiguskaitsevaldkonnas.[127]

[124] Nii konventsiooni 108 art 5 p a kui ka direktiivi 95/46/EÜ art 6 lg 1 p 1 sätestavad töötlemise seaduslikkuse ning ususe nõude.
[125] L.A. Bygrave. Data Privacy Law: An International Perspective. Oxford: Oxford Scholarship Online, 2014, lk 146.
[126] *Ibid*, lk 146.
[127] Proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data - Chapters I, II and V. Nõukogu dokument nr ST15659/15 REV 1, 19.11.2014. Art 4 lg 1 p a, lk 41. Arvutivõrgus: http://data.consilium.europa.eu/doc/document/ST-15659-2014-REV-1/en/pdf (04.05.2015).

Olukorras, kus isikuandmeid töödeldakse tõendite kogumise kontekstis, võib andmete töötlemise seaduslikkuse ja ususe hindamine toimuda kohtumenetluses üldise tõendite lubatavuse hindamise raames. Ehkki KrMS-is eneses ei ole üheselt reguleeritud õigusvastaselt kogutud tõendite kasutamist kohtumenetluses, on Riigikohus antud küsimust mitmel korral analüüsinud.[128] Nii on Riigikohus näiteks sedastanud, et tõendi lubatavuse hindamisel tuleb arvestada sellega, et mitte igasugune tõendite kogumise korra rikkumine ei too kaasa tõendi kuulutamist lubamatuks. Tõend on lubamatu üksnes siis, kui tõendi kogumise korda on oluliselt rikutud. Seejuures tuleb hinnata rikutud normi eesmärki ning seda, kas selliseid tõendeid poleks saadud, kui normi rikutud ei oleks. Erinevate tõendite puhul võib samasuguse rikkumise mõju olla erinev.[129] Tõendi kogumist reguleerivate menetlusõiguslike sätete rikkumise tuvastamine ei tingi alati ja automaatselt selle tõendi lubamatust. Üldjuhul hinnatakse menetlusõigust rikkuvalt saadud tõendi lubatavust kaalumise tulemina, arvestades ühelt poolt rikkumise olulisust (seega KrMS §-s 339 sätestatut) ja teiselt poolt menetletava kuriteo raskust ning sellest tulenevat avalikku menetlushuvi.[130]

Vaatamata Riigikohtu praktikale on siiski selgusetu, kas kohus peaks tõendi lubatavust kaaluma ka põhiõiguste rikkumisega saadud tõendi puhul või üksnes tehnilist laadi menetlusreeglite rikkumise korral.[131] Arvestades Riigikohtu praktikat võib eeldada, et üldjuhul ei tingiks pelgalt isikuandmete töötlemise nõuete rikkumine tõendi õiguspärasust, sest selline rikkumine pigem ei kvalifitseeruks oluliseks kriminaalmenetlusõiguse rikkumiseks ega tooks seega kaasa tõendi lubamatust.

Töötlemise seaduslikkuse nõudega haakub ka IKS § 10 lg-s 1 sätestatud töötlemise lubatavus. Üldjuhul on isikuandmete töötlemine lubatud üksnes isiku nõusolekul, kui seadus ei sätesta teisiti. Taaskord on tegemist rahvusvahelisest õigusest üle tulnud kontseptsiooniga,[132] mille aluseks on põhimõte, et iga isik on oma andmete omanik. Seega eeldab isikuandmete töötlemine andmete omaniku ehk andmesubjekti nõusolekut. Arusaadavatel põhjustel ei toimu andmete töötlemine kriminaalmenetluses üldjuhul isiku nõusoleku alusel - nõusoleku põhimõte on iseloomulik eelkõige eraõiguslikele suhetele. Olukorras, kus isikuandmete töötlemine on aga vajalik avaliku ülesande täitmiseks, oleks nõusoleku küsimine ebaotstarbekas. Just selliste avaliku ülesande täitmisega seotud olukordadele kohaldub IKS § 10 lg 1 teine osa, mis viitab

[128] U. Lõhmus. Tõendi lubatavus ja välistamine kriminaalmenetluses. - Juridica. 2014/9, lk 698.
[129] RKKKo 3-1-1-19-05, p 7.4.
[130] RKKKo 3-1-1-31-11, p 15.
[131] U. Lõhmus. Tõendi lubatavus, 2014, lk 699.
[132] Direktiivi 95/46/EÜ art 7 p a.

isikuandmete töötlemise võimalikkusele ka juhul, kui seadus sätestab nõusoleku nõudest erandi. Arvestades IKS § 10 lg 1 sõnastust võib eeldada, et asjakohasest seadusest peaks alati selgelt tulenema võimalus teostada andmetöötlust ilma isiku nõusolekuta. Samale järeldusele viib ka IKS § 14 lg 1 sõnastus. Tuleb märkida, et KrMS-st ei tulene sõnaselget võimalust isikuandmete töötlemiseks ilma isiku nõusolekuta. Kuigi on ilmne, et kriminaalmenetluse läbiviimiseks on vajalik isikuandmete töötlemine, võib olla kohane märkida KrMS-s *expressis verbis* pädevate asutuste õigust töödelda menetluse huvidest lähtuvalt isikuandmeid ilma isiku nõusolekuta, luues seega konkreetse seadusliku aluse andmete nõusolekuta töötlemiseks. Sellega oleks võimalik vältida potentsiaalset väärtõlgendamist ning tagaks selgema andmetöötluse regulatsiooni.

Eesmärgipärasusest võib samuti rääkida kui üldisest andmekaitsepõhimõttest,[133] mille täitmist kriminaalmenetluses võib olla raske kindlustada. IKS § 6 p 2 määratleb eesmärgipärasuse põhimõtet kui luba isikuandmeid koguda üksnes määratletud ja õiguspäraste eesmärkide saavutamiseks ning neid ei või töödelda viisil, mis ei ole andmetöötluse eesmärkidega kooskõlas. L.A. Bygrave´i hinnangul on eesmärgipärasus seotud eelkõige vajadusega tagada andmetöötluse tulemuste ettenähtavus. Pidades kinni eesmärgipärasuse põhimõttest peaks töötlejal olema võimalik tagada, et nii andmetöötlus ise kui selle tulemus vastavad andmesubjekti põhjendatud ootustele.[134] Eesmärgipärasuse põhimõttega on tihedalt seotud nn kasutuse piiramise põhimõte (IKS § 6 p 4), mille kohaselt tohib andmeid algsest kogumise eesmärgist erineval eesmärgil kasutada üksnes andmesubjekti nõusolekul või pädeva organi loal. Kriminaalmenetluse eripära arvestades on üsna tavapärane, et andmete kasutuse eesmärk muutub ning tekib vajadus varem kogutud andmeid kasutada muudel eesmärkidel. Näiteks on andmekaitse raamotsuses oluliselt kitsendatud eesmärgipärasuse nõude kehtivust ning sätestatud rida erandeid. Raamotsuse art 3 lg 2 loetleb rea olukordi, millal nn "edasine andmetöötlus" (*further processing*) on lubatud:

- see ei ole vastuolus andmete kogumise eesmärgiga;

- vastavatel asutustel on seadusest tulenev õigus töödelda isikuandmeid ka uuel eesmärgil;

- töötlemine on uue eesmärgi suhtes proportsionaalne ning vajalik.

KrMS algsest eesmärgist erineva töötlemise tingimusi ei sätesta. Taolist sätet ei leia ka IKS-ist. IKS § 24 p 1 kehtestab andmete töötleja kohustuse viivitamatult kustutama või sulgema

[133] Näiteks on eesmärgipärasuse põhimõte sätestatud IKS § 6 p-s 2, andmekaitsedirektiivi art 6 lg 1 p b, konventsioon 108 p b.
[134] L.A. Bygrave. 2014, p 153.

andmed, mis ei ole eesmärkide saavutamiseks vajalikud, kui seadus ei sätesta teisiti. Võib vaielda, kas IKS § 24 p 1 annab võimaluse kalduda eesmärgipärasuse põhimõttest kõrvale ning lubab kasutada andmeid ka muudel eesmärkidel. Pigem siiski on IKS § 24 p 1 eesmärk võimaldada vajadusel andmete edasine säilitamine ka pärast kogumise eesmärgi äralangemist, mis aga ei hõlma edasise töötlemise võimaldamist muudel eesmärkidel. Tõlgendades eesmärgipärasuse põhimõtet väga kitsalt võiks eeldada, et igas kriminaalmenetluses on võimalik üksnes selle kriminaalmenetluse raames kogutud isikuandmete töötlemine. Siiski sageli kasutatakse kriminaalmenetluses kas varem kriminaalmenetluslikul eesmärgil teise kriminaalmenetluse raames kogutud andmeid uurimiseks (nt registritesse kantavate biomeetriliste andmete puhul) või kasutatakse mõnel teisel eesmärgil kogutud andmeid, mis võivad sisaldada vajalikku tõendusteavet (nt isiku pangakonto väljavõte, sideandmed jt). KrMS ning teised asjakohased õigusaktid sisaldavad mitmeid sätteid, millest tuleneb uurimisasutuse, prokuratuuri ja kohtu võimalus koguda erinevat teavet ning seda kriminaalmenetluslikel eesmärkidel töödelda. Selline teave hõlmab sageli ka isikuandmeid (näiteks KrMS §-id 90^1, 99^1, 215 lg 1, krediidiasutuste seaduse[135] § 88 lg 5 p 1, psühhiaatrilise abi seaduse[136] § 5 lg 2, kohtutäituri seaduse[137] § 11 lg 3 p 3 jt) ning vastavad sätted tuleks lugeda IKS § 6 p-st 2 erinormideks. Riigikohus on asunud seisukohale, et iseenesest ei ole mõnes muus menetluses kogutud tõendite kasutamine kriminaalmenetluses lubamatu, kui nende tõendite kogumisel on järgitud KrMS §-s 64 sätestatud tingimusi või teatud kriminaalmenetluslikke garantiisid.[138] Samas, vaatamata eriseadustes sisalduvale regulatsioonile ning ka Riigikohtu seisukohale ei näe IKS § 6 p 2 ise võimalust teha sättest erandeid ning on sõnastatud absoluutse nõudena. Näiteks Läti isikuandmete kaitse seaduse § 10 lg 4 loetleb selgelt olukordi, millal eesmärgipärasuse põhimõttest on võimalik kõrvale kalduda ning muul eesmärgil kogutud andmeid kriminaalmenetluses kasutada. Sarnase võimaluse näeb ette ka BPolG § 29 lg 1, samuti BDSG § 14 lg 2 p 7. Soome politsei poolt isikuandmete töötlemise seadus[139] näeb samuti ette võimalused andmete kasutamiseks algsest kogumise eesmärgist erineval eesmärgil (nt § 15). Seega leiab autor, et IKS-is tuleks näha ette võimalus teha kriminaalmenetluses erand eesmärgipärasuse põhimõttest.

[135] Krediidiasutuste seadus. - RT I 1999, 23, 349 ... RT I, 19.03.2015, 41.
[136] Psühhiaatrilise abi seadus. - RT I, 1997, 16, 260 ... RT I, 15.06.2012, 6.
[137] Kohtutäituri seadus. - RT I 2009, 68, 463 ... RT I, 05.03.2015, 3.
[138] RKKKo 3-1-1-116-10, p 8.
[139] Act on the Processing of Personal Data by the Police (761/2003; 523/2004). Finlex. Arvutivõrgus: /fi/laki/kaannokset/2003/en20030761.pdf (04.05.2015).

IKS § 6 p-s 3 sisalduv minimaalsuse põhimõte kohustab töötlejat koguma andmeid üksnes sellises ulatuses, mis on vajalik määratletud eesmärkide saavutamiseks. Eraõigusliku suhte puhul peaks minimaalsuse põhimõtte rakendamine olema igati teostatav, kuid kriminaalmenetluses võib kohustuse täitmisega tekkida keeruline olukord. Nimelt ei pruugi kriminaalmenetluse erinevatel etappidel olla teada, millised andmed on taotletava eesmärgi suhtes asjakohased. Arusaadavalt ei ole näiteks internetiteenuse pakkujal vaja teada isiku perekonnaseisu, kuivõrd vastav teabe ei ole internetiteenuse osutamise kontekstis oluline. Samas aga ilmselt kogub menetleja kriminaalmenetluses andmeid isiku perekonna kohta, kuivõrd perekonnaliikmed võivad omada menetluse seisukohalt olulist infot. Seega kuigi eesmärk on konkreetse kuriteo uurimine, võib menetlejal olla vajadus koguda andmeid märkimisväärselt ulatuslikumalt kui tegelikult kokkuvõttes kasutatakse. Kriminaalmenetluse andmete kogumise puhul on ühtlasi väga suur võimalus koguda teavet teiste isikute kohta kui kahtlustatav või süüdistatav. Sellise tegevusega aga riivatakse kriminaalmenetlusega mitteseotud isikute põhiõigusi, mistõttu tuleks selliste andmete puhul näha ette täpsemad töötlemise reeglid. Minimaalsuse põhimõtte täpsem reguleerimine kriminaalmenetluse valdkonnas võimaldaks muuhulgas vähendada olukordi, kus ametiisikute seadusevastase tegevuse tulemusena on õigustamata isikud saanud kolmandate isikute eraelu puudutavat teavet.

Minimaalsuse põhimõttega seoses on asjakohane märkida, et IKS-ist ei leia konkreetset sätet säilitamistähtaegade piiramise kohta, kuigi vastav põhimõte on olemas konventsioonis 108 (art 5 p e) ning andmekaitsedirektiivis (art 6 lg 1 p e). Säilitamistähtaja piiramise põhimõte (*principle of limited retention of data*) tähendab, et andmeid tohib säilitada andmesubjekti tuvastamist võimaldaval viisil üksnes nii kaua, kui see on vajalik sätestatud eesmärgi saavutamiseks. Seejärel tuleb andmed kustutada.[140] Põhimõte on selgelt välja toodud ka soovituses (87) 15, mille seitsmes põhimõte käsitleb andmete säilitamistähtaja kehtestamist ja andmete kustutamist, kui need ei ole enam eesmärgi saavutamise jaoks vajalikud. Seejuures tuleks eriti arvestada järgmisi asjaolusid: vajadus säilitada andmeid seoses teabepäringuga asjakohase juhtumi kohta; lõplik kohtuotsus, eriti õigeksmõistmine; rehabiliteerimine; kantud karistused; amnestiad; andmesubjekti vanus, andmete eriliigid (põhimõte 7.1). Kohtuotsuses *S ja Marper vs Ühendkuningriik*[141] märgib EIK, et andmekaitse aluspõhimõtete kohaselt peavad

[140] Handbook on European Data Protection Law. Luxembourg: Publications Office of the European Union. 2014. Arvutivõrgus: http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf (04.05.2015).
[141] EIKo 4.12.2008, 30562/04 ja 30566/04, *S ja Marper vs Ühendkuningriik*, p 107.

andmed olema proportsionaalselt kogumise eesmärgi suhtes ning säilitatud piiratud aja jooksul. KrMS alusel kriminaaltoimikusse kantud teabe säilitamise tähtajad on reguleerituid vastavas Vabariigi Valitsuse määruses[142] ning teatud juhtudel on määratletud ka teiste KrMS alusel kogutud andmete säilitamise tähtajad.

Andmete kvaliteedi põhimõtte (IKS § 6 p 5) tagamine kriminaalmenetluses võib samuti tuua teatud raskusi. Nii peavad töödeldavad andmed olema asjakohased ning täielikud. Paraku ei pruugi kriminaalmenetluses olla kindlat teavet selle kohta, kas andmed on asjakohased ning täielikud, ühtlasi on teatud olukorras vaja säilitada ka selliseid andmeid, mis ei ole asjakohased. 2012.a esitatud õiguskaitsevaldkonna andmekaitsedirektiivi eelnõu art 6 nägi ette liikmesriikide kohustuse võimalusel tagada andmete kvalifitseerimine nende täpsuse ja usaldusväärsuse järgi. Samuti sooviti luua kohustus eristada faktilistel ning hinnangutel põhinevad isikuandmed. Autori hinnangul oleks selline eristamine kriminaalmenetluse kontekstis problemaatiline. Sisuliselt loodaks sellise regulatsiooniga kriminaalmenetluses süsteem erinevate tõendite ja asjaolude usaldusväärsuse hindamiseks, kuivõrd tunnistaja ütluste salvestamisel kriminaaltoimikus tuleks kohe algselt määratleda nende täpsus, usaldusväärsus ning hinnangulisus. Kriminaalmenetluse kontekstis ei saa selline jaotamine olla kohane. Direktiivi eelnõu sätteid analüüsinud Justiitsministeerium leidis samuti, et andmete eristamise kohustuse sätestamine oleks vastuolus kriminaalmenetluse põhimõtetega, kuivõrd kriminaalmenetluses loetakse asjaolud lõplikult tõendatuks üksnes kohtuotsuse jõustumisel ja kuni kohtuotsuseni tuleb kõiki kogutud andmeid käsitleda võrdselt.[143]

Andmete turvalisuse põhimõtte (IKS § 6 p 6) järgimine kriminaalmenetluses on enesestmõistetav ning üldiselt pikemat selgitamist ei vajaks. Kriminaalmenetluse andmed kuuluvad avalikustamisele üksnes seaduses sätestatud korras (vt p 4.1.4) ning õigustavata juurdepääs andmetele või avalikustamine võib oluliselt kahjustada kriminaalmenetluse läbiviimist ning tõe väljaselgitamist. Seega tuleb andmete töötlemisel luua tingimused, mis takistaksid andmete volitamata töötlemist, õigustamata isikute juurdepääsu andmetele, andmete avalikustamist või hävimist.

[142] Vabariigi Valitsuse 30.07.2004.a määrus nr 261 "Kriminaaltoimiku arhiivimise kord ja säilitamise tähtajad".- RT I 2004, 60, 261 ... RTI , 02.09.2011, 5.

[143] Seletuskiri Vabariigi Valitsuse istungi päevakorrapunkti „Eesti seisukohad Euroopa Parlamendi ja nõukogu määruse üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (isikuandmete kaitse üldmäärus)“ ja Euroopa Parlamendi ja nõukogu direktiivi üksikisikute kaitse kohta seoses pädevates asutustes isikuandmete töötlemisega kuritegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumise kohta, juurde, lk 15. Arvutivõrgus: http://eelnoud.valitsus.ee/main#2HOqo0Qb (04.05.2015)

Viimase põhimõttena sätestab IKS § 6 p 7 individuaalse osaluse põhimõtet, millest tuleb juttu pikemalt edaspidi.

Käsitledes üldiste andmekaitsenõuete kohaldumist kriminaalmenetluses on vajalik hinnata ka andmekaitse sõltumatu järelevalvega seonduvat. Järelevalveasutused on andmekaitsealaste põhiõiguste ja vabaduste valvajad ning selliste sõltumatute asutuste olemasolu on andmekaitse seisukohalt esmatähtis.[144] Riigi kohustus asutada või nimetada sõltumatu andmekaitse järelevalveasutus on sätestatud nii andmekaitsedirektiivi artiklis 28, andmekaitse konventsiooni 1. lisaprotokollis[145] ning ka andmekaitse raamotsuse artiklis 25. Järelevalveasutus peab olema täiesti sõltumatu ning Euroopa Kohus on sedastanud, et täielik sõltumatus on tagatud olukorras, kus järelevalveasutus teeb otsuseid ilma mistahes otseste või kaudsete väliste mõjudeta.[146]

IKS § 32 lg 2 näeb ette, et nii IKS-i enda kui teiste selle alusel kehtestatud õigusaktide nõuete täitmise üle teostab nii riiklikku kui haldusjärelevalvet Andmekaitse Inspektsioon (*edaspidi AKI*). KrMS §126[15] lg 1 näeb ette erikorra, mille kohaselt teostab jälitustoimingute üle järelevalvet prokuratuur. Seega võib järeldada, et kõigi muude isikuandmete töötlemistoimingute õiguspärasuse üle järelevalve teostamiseks on pädev AKI. Siiski praktikas kontrollib kriminaalmenetluses isikuandmete töötlemise õiguspärasust eelkõige pädev asutus ise või prokuratuur.[147] Nagu eespool märgitud on järelevalvesüsteemi esmatähtis tunnus selle sõltumatus kontrollile allutatud töötlejast. Autori hinnangul on kaheldav, kas uurimisasutus või prokuratuur on kriminaalmenetluse puhul piisavalt sõltumatud, täitmaks andmekaitse järelevalveasutuse funktsioone, ühtlasi peab andmekaitsenõuetest tulenevalt asutuse järelevalvepädevus olema seaduses selgelt sätestatud. Nagu eespool käsitletud, ei pruugi isikuandmete töötlemise seaduslikkuse üle kontrolli toimuda ka kohtumenetluses, kuivõrd tõendi lubatavuse kontrollimisel ning tõendite hindamisel ei pruugi kohus pöörata isikuandmete kaitsega seotud küsimustele tähelepanu. Liiatigi võib paljudel juhtudel andmetöötlus olla seotud ka selliste andmetega, mida ei lisata kohtule esitatavasse toimikusse.

Kriminaalmenetluse iseloomust tulenevalt toimub selles pidevalt erinevate isikuandmete, sh delikaatsete isikuandmete töötlemine. Arvestades isikuandmete töötlemise mõiste ulatust on selge, et töötlemistoiminguid viivad läbi kõik menetlusosalised - nii menetlejad kui ka kahtlustatavad, süüdistatavad, kaitsja jt. Töötlemine ei toimu siiski üldjuhul isiku nõusolekul,

[144] EKo 09.03.2010, C-581/07 *European Commission vs Saksamaa Liitvabariik*, p 23.
[145] Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni järelevalveasutusi ja andmete liikumist üle piiri käsitlev lisaprotokoll. - RT II 2009, 17, 44. Eesti on lisaprotokolli ratifitseerinud 2009.a Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni lisaprotokolli ratifitseerimise seadus. - RT II 2009, 17, 44
[146] EKo 09.03.2010, C-581/07, p 19.
[147] Teave Andmekaitse Inspektsioonilt.

vaid IKS § 10 lg 2 kohaselt seaduslikul alusel. Samas, KrMS ei näe hetkel ette isikuandmete kaitse üldregulatsiooni ega kehtesta pädevate asutuste õigust töödelda KrMS-i eesmärkide saavutamiseks isikuandmeid. Näiteks korrakaitseseaduse § 13 sätestab sõnaselgelt, et korrakaitseorgan võib riikliku järelevalve menetluses töödelda isikuandmeid.[148] Advokatuuriseaduse § 41 lg 1 p 4^1 kohaselt võib vandeadvokaat töödelda töölepingu või seaduse alusel saadud muu isiku kui kliendi isikuandmeid ilma nende isikute nõusolekuta, kui see on vajalik õigusteenuse osutamiseks.[149] Samas näiteks prokuratuuriseadusest[150] taolist sätet ei leia. Loomulikult on ilmne, et kõik pädevad asutused peaksid saama ja saavad isikuandmeid töödelda ning autori hinnangul on õigusselguse tagamiseks ning õiguskorras välja kujunenud praktika arvestamiseks oleks asjakohane sätestada IKS-is või KrMS-s selgelt nii isikuandmete töötlemise lubatavus kui ka menetluse tagamiseks vajalike erandite tegemise võimalust IKS §-s 6 sätestatud andmekaitsepõhimõtetest, eelkõige seoses andmete eesmärgipärase töötlemise ning andmete kvaliteediga.

2.2 Andmesubjekti õigused kriminaalmenetluses

Isikuandmete kaitse reeglite otstarve on vaieldamatult andmete töötlemise ulatuse piiritlemine ning töötlemistoimingute reguleerimine eesmärgiga tagada võimalikult vähene sekkumine isiku privaatsusesse. Teiselt poolt on andmekaitseõiguses väga olulisel kohal andmesubjekti õiguste tagamine. Kuigi isik võib olla andnud nõusoleku enda andmete töötlemiseks või tuleneb töötleja vastav õigus seadusest, ei anna see töötlejale absoluutset võimu andmete üle. Isik peab saama oma andmete töötlemist üldjuhul mõjutada ning selles osaleda, omades seejuures jätkuvalt kontrolli andmete töötlemise üle.[151] Seega võib kriminaalmenetluses lisaks menetlusosalise õigustele rääkida ka andmesubjekti õigustest.

Individuaalse osaluse põhimõte (IKS § 6 p 7) on andmekaitseõiguse üks nurgakive, andes andmesubjektile kontrolli tema kohta töödeldavate andmete üle. Vastavalt direktiivi 95/46/EÜ põhjenduspunktile 25, mida on oma praktikas rõhutanud ka Euroopa Kohus, peavad andmekaitsepõhimõtted kajastuma ühelt poolt töötlemise eest vastutavatele isikutele

[148] Korrakaitseseadus. - RT I , 22.03.2011, 4 ... RT I, 31.12.2014, 28.
[149] Advokatuuriseadus. - RT I 2001, 36, 201 ... RT I, 21.06.2014, 50.
[150] Prokuratuuriseadus. - RT I 1998, 41, 625 ... RT I, 10.03.2015, 17.
[151] T. Ilus. Andmesubjekti osaluse põhimõte Euroopa Nõukogu konventsioonide ning Euroopa Inimõiguste Kohtu lahendite valguses. - Juridica 2005 / 8, lk 525.

kehtestatud kohustustes ja teisest küljest õigustes, mis on antud üksikisikule, kelle andmeid töödeldakse. Isiku õiguste tagamiseks tuleb talle töötlemisest teatada, võimaldada tal andmetega tutvuda ning ta võib nõuda andmete korrigeerimist ja teatavatel asjaoludel isegi esitada vastuväiteid andmete töötlemise suhtes.[152]

Andmesubjekti õigused on sätestatud IKS-i 3. peatükis:

- andmesubjekti õigus saada teavet ja tema kohta käivaid isikuandmeid (IKS § 19);

- andmesubjekti õigus nõuda isikuandmete töötlemise lõpetamist ning isikuandmete parandamist, sulgemist ja kustutamist (IKS § 20);

- andmesubjekti õigus pöörduda Andmekaitse Inspektsiooni ja kohtu poole (IKS § 21);

- andmesubjekti õigus nõuda kahju hüvitamist (IKS § 22).

Nagu eespool käsitletud, kohaldub IKS kriminaalmenetlusele KrMS-s sätestatud erisustega, kuid KrMS ise vastavaid erisusi üldjuhul ei täpsusta. Autori hinnangul tekib siinkohal vastuolu IKS-i ja KrMS-i vahel, kuivõrd kriminaalmenetluse eesmärke arvestades on raske ette kujutada näiteks olukorda, kus kahtlustatav nõuaks tema kohta käivate andmete parandamist kriminaaltoimikus. Ometi on IKS § 21 lg 1 kohaselt temal selline õigus olemas ning KrMS ei näe ette siinkohal mingeid reegleid, et isik ei saaks seda taotleda. Probleemi ei ole, kui kahtlustatav taotleks perekonnanimes trükivea parandamist, küll aga võib olukord olla märkimisväärselt keerulisem. Arvestades isikuandmete mõiste avarat definitsiooni, mis hõlmab ka hinnanguid ja subjektiivseid arvamusi, tekib kahtlustataval õigus nõuda näiteks tema kohta käivate andmete parandamist tunnistaja ütlustes. Kuivõrd IKS § 21 ei näe ette piiranguid andmete parandamise õiguse kasutamiseks ning vastavaid sätteid ei ole ka KrMS-is, tekib õiguslikult ebaselge olukord. Ühelt poolt on isikul õigus nõuda toimingu tegemist, teiselt poolt on ilmne, et sellist toimingut ei ole võimalik sooritada, kuivõrd toiming oleks vastuolus kriminaalmenetluse olemuse ja eesmärgiga. Ilmselgelt peab iga andmesubjekti taotluse lahendamise puhul hinnata käimasoleva menetluse hetkeseisu ning taotluse asjaolusid. Arvestades kriminaalmenetluse eesmärkide ning andmesubjekti huvide vastastikku kollisiooni lasub andmete töötlejal kohustus igakordselt otsida tasakaal, mis võimaldaks tagada andmesubjekti õigusi seadmata ohtu kriminaalmenetluse tulemuslikkus.[153]

[152] EKo 07.05.2009, C-553/07 College *van burgemeester en wethouders van Rotterdam vs M. E. E. Rijkeboer*, p 48.
[153] D. Alonso Blas, 2010, lk 232-233.

Andmetöötluse ja isikuandmete kaitse seisukohalt on väga oluline IKS §-s 19 sätestatud andmesubjekti õigus saada teavet tema andmete töötlemise kohta ning ühtlasi ka juurdepääsu töödeldavatele isikuandmetele. Kõnealune põhimõte on leitav ka andmekaitsedirektiivi artiklist 12 ning on direktiivi üks olulisemaid sätteid, kuivõrd teadlikkus andmete töötlemise faktist annab isikule võimaluse rakendada praktikas teisi tema kui andmesubjekti õigusi ning seeläbi teostada kontroll enda andmete töötlemise üle.[154] Andmetöötluse läbipaistvus on määrava tähtsusega andmekaitseõiguse tõhususe seisukohalt.[155] EIK hinnangul on andmesubjekti õigust saada teavet iseenda kohta olulise tähtsusega isiku identiteedi ning isiksuse seisukohalt.[156]

IKS §-i 20 kohaselt on võimalik andmesubjekti õigust saada enda kohta käivat teavet piirata kui see võib mh kahjustada kuriteo tõkestamist või kurjategija tabamist (§ 20 p 3) või raskendada kriminaalmenetluses tõe väljaselgitamist (§ 20 p 4). Samas ei ole ei IKS-is ega KrMS-is regulatsiooni selle kohta, kuidas peaks andmesubjektile juurdepääsu võimaldamisest keeldumine toimuma ning kas ja millistel juhtudel tuleks see põhjendada. Siinjuures võib näitena tuua andmekaitse raamotsuse art 17 lg 3, mille kohaselt peab üldjuhul iga juurdepääsu piiramise või keeldumise otsus olema kirjalik ning põhjendatud. Siinkohal võimaldab raamotsus põhjendamisest loobumist juhul, kui see ohustaks erinevate menetluste, sh kriminaalmenetluse läbiviimist, avalikku korda, riigi julgeolekut või andmesubjekti enda või teiste isikute põhiõigusi. Küll aga tuleb isikut igal juhul informeerida võimalusest esitada keeldumise peale kaebus järelevalveasutusele. Positiivse näitena KrMS-ist saab tuua §-i 126^{14}, mille kohaselt võimaldatakse isikul, keda teavitati tema suhtes jälitustoimingu tegemisest, tutvuda soovi korral tema kohta kogutud andmetega ja jälitustoimingu käigus tehtud foto, filmi, heli- või videosalvestiste või muu teabetalletusega.

Juurdepääs andmetele kriminaalmenetluses on reguleeritud KrMS-is sätetega, mis reguleerivad juurdepääs kriminaaltoimikule. Kriminaaltoimik on KrMS § 160^{1} kohaselt kriminaalmenetluses kogutud dokumentide kogum, seega sisaldab kriminaaltoimik nii kriminaalmenetluses töödeldud andmeid kui ka andmetöötlust puudutavat teavet. KrMS §-ide 224 ja 224^{1} kohaselt on kahtlustataval, süüdistataval, kaitsjal, kannatanul ning tsiviilkostjal õigus tutvuda kriminaaltoimikuga. Toimikuga tutvumise õigus on suunatud kaitseõiguse

[154] EKo 07.05.2009. C-553/07 *College van burgemeester en wethouders van Rotterdam vs M. E. E. Rijkeboer,* p 51.

[155] F. Coudert, J. Dumortier, E. Kosta. Data Protection in the Third Pillar: In the Aftermath of the ECJ Decision on PNR Data and the Data Retention Directive. - International Review of Law, Computers & Technology, nr 3, 2007, lk 354.

[156] T. Ilus. 2005, lk 519 - 531; EIKo 07.07.1989, 10454, *Gaskin vs Ühendkuningriik*.

tagamisele ning kohtumenetluse pooltele võrdsete võimaluste loomisele.[157] Kriminaaltoimikuga tutvumise regulatsiooni muutmisel on 2011.a jõustunud KrMS muutmise seaduse seletuskirjas märgitud, et toimikuga tutvumisel tuleb arvestada isikuandmete kaitse põhimõtetega ning seetõttu on teatud juhtudel põhjendatud toimikuga tutvumise õigusele täiendavate piirangute kehtestamine.[158] KrMS kohaselt on selgelt piiritletud isikute ring, kellel on õigus toimikuga tutvuda. Samas võib toimikus sisalduda märkimisväärsel hulgal ka infot teiste isikute kohta, kellele aga ei ole võimaldatud toimikule ja sellest tulenevalt ka nende kohta kogutud isikuandmetele. Näiteks võib toimikus olla ulatuslikult teavet tunnistajate ja menetlusosaliste pereliikmete või tuttavate kohta, nende eraelu puudutavaid andmeid ja muu privaatsusõiguse kaitsealasse jääv teave. Siiski ei teki nendel isikutel toimikuga tutvumise õigust, kuivõrd see võib kahjustada kriminaalmenetlust. EIK tõlgenduse kohaselt tuleb andmetele juurdepääsupiirangu kehtestamisel kaaluda andmesubjekti huve ning andmete kaitse eesmärki. Kohtuasjas *Leander vs Rootsi* sedastas kohus, et riigil on õigus piirada isiku juurdepääsuõigust oma andmetele, kui see on vajalik riigikaitselistel eesmärkidel.[159] Samas näiteks kohtuasjas *Gaskin vs Ühendkuningriik*[160] pidas kohus isiku õigust tema päritolu ja lapsepõlve puudutavale infole olulisemaks kui riigi poolt kehtestatud konfidentsiaalsusnõue. Kuivõrd kriminaalmenetlus on eelkõige suunatud üldiste huvide kaitseks, või pidada IKS § 20 p 3 ja 4 ning KrMS §-des 224 ja 224[1] sätestatud kitsendusi asjakohaseks.

Lisaks õigusele saada teavet on andmesubjektil ka õigus nõuda andmete parandamist, sulgemist või kustutamist. Isiku õigus andmete kustutamisele on leidnud laia kõlapinda seoses Euroopa Kohtu 2014.a otsusega kohtuasjas *Google vs Hispaania*[161], mille kohaselt tekib üksikisikul sisuliselt "õigus olla unustatud" (*right to be forgotten*)[162]. Andmekaitsedirektiivi art 12 p b kohaselt on isikul õigus nõuda tema kohta käivate andmete parandamist, sulgemist või kustutamist, eriti ebatäpsete ning ebaõigete andmete puhul. Euroopa Kohtu tõlgenduse kohaselt aga hõlmab ebatäpsete ja ebaõigete andmete sisu muuhulgas ka olukordi, kus andmed ole piisavad või asjakohased või ületavad selle otstarbe piire, mille tarvis neid töödeldakse, et neid ei ajakohastata või säilitatakse pikema aja jooksul kui vajalik (kohtuotsuse p 92). Kuigi

[157] E. Kergandberg, M. Sillaots. Kriminaalmenetlus. Tallinn: Juura 2006, lk 320.
[158] Kriminaalmenetluse seadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu 599 SE seletuskiri, lk 60 - 64. Arvutivõrgus: http://www.riigikogu.ee/tegevus/eelnoud/eelnou/ab9521d9-5558-45b8-c93a-b5122208c53b/Kriminaalmenetluse-seadustiku-muutmise-ja-sellega-seonduvalt-teiste-seaduste-muutmise-seadus/ (04.05.2015).
[159] EIKo 26.03.1987, 9248/81, *Leander vs Rootsi*, p 59.
[160] EIKo 07.07.1989, 10454, *Gaskin vs Ühendkuningriik*, p 49.
[161] EKo 13.05.2014, kohtuasi C-131/12, *Google Spain SL, Google Inc. vs Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, p 92 – 99.
[162] Bygrave, L.A. A Right to be Forgotten? - Communications of the ACM. 2015, vol 58, nr 1, lk 35.

konkreetne Euroopa Kohtu otsus on tehtud andmekaitsedirektiivi alusel, võib sellel olla ka teatud mõju kriminaalmenetluse valdkonnale. Esiteks on siinkohal vajalik taas märkida, et direktiivi Eesti õigusesse üle võtva õigusakti (IKS) kohaldamisala on laiem kui direktiivis sätestatud, mistõttu võib direktiivi sätete tõlgendus muutuda asjakohaseks ka kriminaalmenetluse raames töödeldavate andmete puhul. Kuigi Google *vs* Hispaania kohtuotsus on tehtud kommertseesmärkidel andmete töötlemise kontekstis, võib see jõuda ka teistel alustel andmete töötlemise valdkondadesse, kuivõrd kohus annab oma otsuses laiema tõlgenduse ühele üldtunnustatud andmesubjekti õigusele. Teatud kohendustega on "õigust olla unustatud" võimalik teoreetiliselt rakendada ka kriminaalmenetluse kontekstis, arvestades valdkonna eripärast tulenevaid tingimusi.

Andmekaitse raamotsus näeb samuti töötleja kohustuse tagada andmete õigsuse, samuti sulgeda või kustutada andmed kui need ei ole enam vajalikud lähtuvalt kogumise eesmärgist (raamotsuse art 4). Raamotsuse art 18 kohaselt on andmesubjektil õigus nõuda andmete parandamist, sulgemist või kustutamist ning nende kohustuste täitmisest keeldumine peab olema edastatud andmesubjektile kirjalikult. Andmesubjekti õigust andmete kustutamisele ning parandamisele on sätestab ka konventsioon 108 art 8 p c.

Ka IKS § 21 lg 1 kohaselt saab isik nõuda ebaõigete andmete parandamist. Seejuures ei ole käesolevas sättes toodud täiendavaid piiranguid selle kohta, millistel juhtudel ei ole andmete parandamise lubatud või võimalik. IKS § 21 lg 2 sätestab, et isikul on õigus nõuda andmete töötlemise lõpetamist, andmete avalikustamise või andmetele juurdepääsu võimaldamise lõpetamist või andmete sulgemist ja kustutamist juhul, kui andmete töötlemine ei ole seaduse alusel lubatud. Kuigi esmapilgul võib tunduda, et IKS § 21 lg 2 on väga kitsa kohaldamisalaga, on autori hinnangul mõiste "ei ole seaduse alusel lubatud" laiema tähendusega. Nimelt ilmselgelt hõlmab § 21 lg 2 selliseid olukordi, kus andmetöötlusel puudub seaduslik alus või andmete töötlemine on seadusega *expressis verbis* keelatud. Siiski tuleb IKS § 21 lg 2 tõlgendamisel võtta aluseks muuhulgas ka teisi kriteeriume ning põhimõtteid, mille alusel ei ole andmetöötlus lubatud. Näiteks tuleks arvestada, et IKS §-s 5 sätestatud andmetöötluse põhimõtted on töötlejale kohustuslikud, seega andmetöötluspõhimõtete järgimata jätmisel ei ole töötlemine lubatud ning isikul on õigus nõuda andmete kustutamist IKS § 21 lg 2 alusel. Teise näitena võib tuua töötleja kohustuse pidada kinni säilitamistähtaegadest. Politsei ja piirivalve seaduse § 45^1 lg 4 kohaselt tuleb politseiametniku daktüloskopeerimisel ja DNA-proovi analüüsil saadud andmed kustutada riiklikest registritest kolme aasta möödumisel politseiametniku politseiteenistusest vabastamisest arvates. Juhul, kui andmete töötleja ei täida

temale seaduse alusel pandud kohustust ega kustuta politseiametniku andmed sätestatud tähtaja jooksul, on isikul õigus nõuda andmete kustutamist.

KrMS-s võib andmesubjekti andmetele juurdepääsuõigust reguleerivaks sätteks pidada KrMS § 214. Kuigi säte käsitleb kohtueelse menetluse andmete avaldamist, hõlmab avaldamine nii andmete avalikustamist näiteks ajakirjanduses kui ka andmete edastamist teistele mitteõigustatud isikutele.[163] Küsitav on seejuures, keda hõlmab õigustamata isikute ring. Eelduslikult mõeldakse sättes isikuid, kellel puudub kriminaalmenetluses õigus saada kohtueelse menetluse andmeid. KrMS § 214 lg 2 sätestab rea tingimusi, millal on menetluse andmete avaldamine võimalik. Sellest tulenevalt võib eeldada, et andmesubjektil on võimalik taotleda prokurörilt tema kohta kohtueelses menetluses kogutud andmetega tutvumist ning prokurör saaks anda andmete avaldamiseks loa kui on täidetud KrMS § 214 lg 2 tingimused. Andmesubjekti taotluse lahendamisel tuleb seega ühelt poolt võtta arvesse isiku õigus tutvuda tema kohta kogutud andmetega ning seeläbi teostada oma andmekaitsealast õigust ja teiselt poolt kaaluda kriminaalmenetlusest tulenevaid kitsendusi ja menetluse huve. Autor leiab, et nende kahe vastandliku huvi konflikti oleks võimalik lahendada olukorras, kus isikule avaldatakse üksnes temaga seonduvad andmed väga piiratud ulatuses, mis ei kahjustaks kriminaalmenetlust.

Kokkuvõttes võib öelda, et KrMS ei näe ette erireegleid menetlusosaliste ega teiste isikute andmekaitse alaste õiguste teostamiseks. Seega tuleks asuda seisukohale, et IKS kehtib üldregulatsioonina ka KrMS-is sätestatule. Paraku nagu eespool näidatud, ei ole tegelikkuses ning kriminaalmenetluse eripära arvestades nende õiguste piiramata teostamine võimalik. Arvestades menetluses töödeldavate andmete hulka ning sellega kaasnevat põhiõiguste riivet oleks IKS-is ja KrMS-s otstarbekas näha ette regulatsioon, mis tagaks andmesubjektile suuremad võimalused oma andmekaitsealaste õiguste teostamiseks ning annaks menetlejale selgemad juhised kaalutlusõiguse teostamiseks.

2.3 Andmete avalikustamine

[163] N. Aas. KrMS § 214 / 5. - Kergandberg, E., Pikamäe, P. jt (toim). Kriminaalmenetluse seadustik. Komm vlj. Tallinn: Juura, 2012.

Kriminaalmenetluse raames võib osutuda vajalikuks jagada teavet süüteomenetluse kohta - näiteks avaldada infot võimaliku kurjategija kohta massiteabevahendites tema leidmiseks või otsida sel teel võimalikke kannatanuid. Samuti võib olla mõningate menetluse faktide osas äärmiselt kõrge avalik huvi. Sageli käsitletakse kohtueelse menetluse andmete avalikustamist süütuse presumptsiooni põhimõtte valguses.[164] Nagu varem käsitletud, on andmete avalikustamine üks töötlemistoiming ning sellele kohalduvad täies ulatuses andmekaitsereeglid. Kuigi kohtueelse menetluse andmete avalikustamise puhul on põhirõhk kahtlustatava õigusel süütuse presumptsioonile, väärib andmete avalikustamise temaatika käsitlust ka isikuandmete kaitse kontekstis. Käesolevas analüüsis keskendub autor kohtueelses menetluses kogutud isikuandmete avalikustamisele.

Kohtueelse menetluse andmeteks on kohtueelse kriminaalmenetluse käigus menetleja poolt kogutud info, samuti teave menetlustoimingute (sh nende läbiviimise fakti) kohta. Kohtueelse menetluse andmete mõiste on väga lai, hõlmates näiteks nii kuriteoteadet ja selles sisalduvat infot kui ka menetlejale antud ütlused ja kogutud tõendid. Siiski ei ole kohtueelse menetluse andmeteks näiteks avalikud andmed, isegi kui sellised andmed omavad olulist tähtsust kriminaalmenetluses. Näiteks avalikesse registritesse (äriregister, kinnistusraamat jt) kantud andmed on avalikult kättesaadavad ning kuigi nendel andmetel võib kriminaalmenetluses olla oluline tõenduslik väärtus, ei saa neid käsitada kohtueelse menetluse andmetena.[165]

Arvestades kohtueelse menetluse andmete määratlust on ilmne, et selliste andmete hulka kuulub palju isikuandmeid. Kohtueelse menetluse raames kogutud materjalid puudutavad üldjuhul väga mitmeid isikuid, sh kahtlustatavaid, tunnistajaid, kuriteoohvreid, kolmandaid isikuid jt. Seega kohtueelse menetluse andmete avaldamisel tuleb lähtuda mitte üksnes menetluslikest huvidest ja eesmärkidest, vaid arvestada ka vajadusega tagada piisav isikuandmete kaitse.

Eelmises alapeatükis on juba mainitud, et kohtueelse menetluse andmete avaldamist kriminaalmenetluses reguleerib KrMS § 214, mis hõlmab nii andmete avaldamist mistahes piiratud isikute ringile kui ka andmete avalikustamist. Isikuandmete avalikustamise üldregulatsioon tuleneb IKS §-st 11. Lisaks on asjakohane ka avaliku teabe seaduse[166] (*edaspidi AvTS*) § 35 lg-s 1 sätestatu, mis kehtestab alused teabe asutusesiseseks kasutamiseks

[164] M. Männiko, 2011, lk 210.
[165] N. Aas. KrMS § 214/3.1 - 3.2.
[166] Avaliku teabe seadus. – RT I 2000, 92, 597… RT I, 12.07.2014.

tunnistamiseks.[167] KrMS § 214 eesmärk on sätestada tingimused kuritegude efektiivseks menetlemiseks ja tagada süütuse presumptsioonist kinnipidamine. Ühtlasi aga teenib säte avalikke huve, võimaldades informeerida avalikkust kriminaalmenetlustest ja kuritegudest, samuti levitada preventiivseid sõnumeid eesmärgiga vältida inimeste langemist kuriteo ohvriteks või inimeste poolt süütegude toimepanemist.[168] Tegemist on erinormiga IKS §-st 11 ning täpsustava sättega AvTS § 35 lg 1 suhtes.

KrMS § 214 kohaselt võib kohtueelse menetluse andmeid avaldada ainult prokuratuuri loal ning tema määratud ulatuses (lg 1) lähtuvalt kriminaalmenetluse, avalikkuse või andmesubjekti huvidest ja üksnes järgmistel tingimustel, kui see ülemäära (lg 2):

- ei soodusta kuritegevust ega raskenda kuriteo avastamist (p 1);

- ei kahjusta Eesti Vabariigi või kriminaalmenetluse huve (p 2);

- ei sea ohtu ärisaladust ega kahjusta juriidilise isiku tegevust (p 3);

- ei kahjusta andmesubjekti ega kolmandate isikute õigusi, eriti delikaatsete isikuandmete avaldamise puhul (p 4).

Andmete avaldamise otsustamisel tuleb hinnata erinevate õiguste ja väärtuste omavahelist tasakaalu.[169] Isikuandmete avalikustamisel kriminaalmenetluses tuleb võtta eelduseks lähtekoha, et igasugune teave, mis viitab isiku seotusele kriminaalmenetlusega, riivab oluliselt isiku õigust eraelu puutumatusele ning riive on oma olemuselt intensiivne sõltumata isiku menetlusõiguslikust staatusest. Seejuures võib vaielda selle üle, kas kahtlustatava andmete avaldamine riivab isiku õigusi tugevamini kui näiteks tunnistaja andmete avaldamine. Käesoleva töö autori hinnangul ei ole andmesubjekti menetlusõiguslik staatus tingimata määrava tähtsusega riive tugevuse hindamisel. Andmete avaldamise otsuse tegemisel tuleb igakordselt hinnata, kas andmete avaldamise eesmärgid kaaluvad üles isiku põhiõiguste riive.

N. Aas märgib, et kuriteo ja kriminaalmenetluse kohta andmete avaldamisel mängivad rolli kolm põhilist huvi:

[167] Muuhulgas peab asutusesiseseks teabeks tunnistama kriminaalmenetluses kogutud andmed, v.a. neis seadustes sätestatud tingimustel avaldatav teave (AvTS § 35 lg 1 p 1), delikaatseid isikuandmeid sisaldav teave (AvTS § 35 lg 1 p 11), andmesubjekti eraelu käsitlev teave, kui selle avalikustamine kahjustaks oluliselt andmesubjekti eraelu puutumatust (AvTS § 35 lg 1 p 12).
[168] N. Aas. KrMS § 214/1.
[169] N. Aas. KrMS § 214/7.2.

1) avalikkuse huvid - demokraatia toimimise eelduseks on avalikkuse võimalikult hea informeeritus kõikidest ühiskonna jaoks olulistest seikadest, sh kuritegudest ja kriminaalmenetlusest;

2) kriminaalmenetluse huvid - siinkohal on oluliseks kuritegude väljaselgitamine ja õiglane kohtupidamine;

3) kuriteoga seotud isikute huvid - isikute huvides on ise määrata, palju nendega seotud andmeid avaldatakse.[170]

Kolmest huvist, mida andmete avaldamine teenib, on autori hinnangul üks subjektiivsemaid avalikkuse huvi olemasolu. Üldiselt leitakse, et mida olulisem on probleem ühiskonnale ja mida suuremat hulka inimesi sündmus puudutab, seda suurem on avalikkuse huvi info avalikustamise vastu. Kui tegemist on aga pelgalt uudishimu rahuldamisega üksikisiku eraelu puudutavate detailide arvelt ning kõnealune info ei ole seotud avalike ülesannete täitmisega, ei ole tegemist avaliku huviga ning põhjus info avalikustamiseks puudub. Muuhulgas võib info avaldamise huvide taga olla ka ajakirjanduse ärihuvid, mis aga pole kindlasti piisav põhjus isiku eraelu puutumatuse riiveks. EIK on sellisele seisukohale asunud 2004.a.[171] Oma 2001.a Eesti suhtes tehtud otsuses rõhutas EIK, et isiku eraelu käsitleva info avaldamiseks peaks selline info olema ühiskonna jaoks asjakohane, avalikkuse jaoks olulise iseloomuga või mõjutaks ühiskonna elu.[172] Kuivõrd kuriteod ohustavad avalikku korda ning ühiskonna turvalisust, on kohane eeldada, et selle vastu eksisteerib ka põhjendatud avalikkuse huvi. Samas tuleb esiteks arvesse võtta sündmuse iseloomu ning seejärel leida vajalik tasakaal avaliku ja üksikisiku huvi vahel. Riigikohus on asunud seisukohale, et korruptsioonikuritegude puhul on avalikkuse huvi olemas ning ühiskonnal on õigus teada kuriteo asjaolusid.[173]

Käesoleva töö autori hinnangul on aga KrMS § 214 puhul jäänud piisavalt täpsustamata, et ainuüksi § 214 lg 2 punktides 1 - 4 sätestatud eelduste olemasolust ei piisa selleks, et avaldada kriminaalmenetluse info, kui selle raames avaldatakse ka isikuandmed. Avalikust huvist lähtuv andmete avaldamist tuleks autori hinnangul sageli piirata üksnes sündmuse asjaolude kirjeldamisega ning konkreetse isiku seostamine sündmusega ei ole avalikust huvist lähtuvalt vajalik ega kohane. Isikuandmete avalikustamisel tuleks lisaks avaliku huvi kriteeriumile hinnata isiku eraelu riivet ning langetada põhjendatud otsus selle kohta, et avalikust huvist

[170] N. Aas. KrMS § 214/7.1.
[171] EIKo 24.06.2004, 59320/00, *von Hannover vs Saksamaa*.
[172] EIKo 04.04.2001, 41205/98, *Tammer vs Eesti.*
[173] RKTKo 3-2-1-83-10, p 13.

lähtuvalt on oluline lisaks muule menetlusinfole ka konkreetset isikut käsitlevate andmete avalikustamine. Õiguskantsler on käsitlenud isikuandmete avaldamist kriminaalmenetlusteabe avalikustamise kontekstis oma menetluses seoses kahtlustatava isiku andmete avaldamisega Kaitsepolitseiameti aastaraamatus.[174]

2.4 Andmete nõudmine sideettevõtjalt

Tehnoloogia arenedes laienevad oluliselt menetlejate võimalused kriminaalmenetluses vajaliku teabe hankimiseks. Arvestades tänapäeva ühiskonnas telekommunikatsiooni sidevahendite laia levikut, on ootuspärane, et sidevahendite kasutamisega seotud info võib olla olulise tähtsusega ka kriminaalmenetluses. Sellest lähtuvalt sätestab KrMS § 90^1 menetleja võimaluse teha päringu elektroonilise side ettevõtjale eesmärgiga saada kriminaalmenetluses vajalikku teavet. Kõnealune õigusnorm on tihedalt seotud elektroonilise side seaduse (*edaspidi ESS*) §-ga 111^1, mille kohaselt on sideettevõtjatel kohustus säilitada teatud andmeid. Nii KrMS § 90^1 kui ESS § 111^1 võtavad Eesti õigusesse üle andmete säilitamise direktiiv, mis käsitleb sideettevõtjate kohustust säilitada teatud sideandmeid eesmärgiga võimaldada õiguskaitseasutuste juurdepääs nendele andmetele raskete kuritegude uurimiseks, avastamiseks ja kohtus menetlemiseks (direktiivi art1 lg 1). Enne sisulise analüüsi teostamist on oluline märkida, et andmete säilitamise direktiivi sätted, ESS § 111^1 ega KrMS § 90^1 ei hõlma sidekanali kaudu edastatava sõnumi sisu, vaid ainult sõnumi edastamise faktiga kaasnevat teavet. Arvestades isikuandmete mõiste laia definitsiooni ning ka Euroopa Kohtu antud tõlgendust[175] on ilmne, et andmete säilitamise direktiivi alusel kogutavate andmete puhul on tegemist isikuandmetega. Niinimetatud "sõnumi liikumise andmed" hõlmavad näiteks teavet sõnumi saatja ja saaja aadressi või telefoninumbri kohta, sõnumi edastamise aja ja kestuse, saaja ja saatja asukoha ning muude asjaolude kohta. Kuivõrd sellised andmed võivad olla kriminaalmenetluses väga suure tähtsusega, on mõistetav nende andmete menetlejatele kättesaadavuse vajalikkus.[176]

[174] Õiguskantsleri 18.02.2011.a kiri nr 7-4/101805/1100879 Riigikogu julgeoleku asutuste järelevalve komisjonile. Arvutivõrgus: http://oiguskantsler.ee/sites/default/files/old/File/OMBUDSMANI_MENETLUSED/Soovitused_oigusparasuse_ja_hea_halduse_tava_jargimiseks/2011/RK_julgeolekuasutuste_j_relevalve_erikomisjon_seisukoha_edastamine_Toomse.pdf (04.05.2015).

[175] EKo 24.11.2011, kohtuasi C-70/10, Scarlet Extended SA *vs* **S**ociété belge de sauteurs, compositeurs et éditeurs SCRL (SABAM).

[176] U. Lõhmus. Põhiõigused kriminaalmenetluses, 2014, lk 330.

Siiski tuleb õiguskaitseasutustele andmetele juurdepääsu võimaldamisel tagada kooskõla vajadusega kaitsta isiku eraelu.

Põhiseaduse kommentaaride ning KrMS § 90^1 kohta seletuskirjas[177] märgitu kohaselt ei kuulu sõnumi edastamise faktiga seotud teave PS § 43 (õigus sõnumi saladusele) kaitsealasse, vaid on hõlmatud PS §-ga 26, mis käsitleb õigust eraelu puutumatusele.[178] EIK on aga otsustes[179] omakorda asunud seisukohale, et sõnumi edastamise faktiga seotud teave kuulub EIÕK art 8 kaitsealasse. Seejuures ei ole EIÕK seisukohalt oluline, kas tegemist on eraelu puutumatu või korrespondentsi kaitsega, kuivõrd EIÕK art 8 hõlmab mõlemat õigust ning seega ei pidanud vastavat täpsustust vajalikuks ka EIK. Küll aga näeb PS eraelu puutumatuse (§ 26) ja sõnumi saladuse (§ 43) kaitseks erinevaid tagatisi, mistõttu Eesti õiguse kontekstis on oluline tuvastada, millise PS sätte kaitsealasse sõnumi edastamise faktiga seotud teave jääb. Kui PS §26 sätestatud era- ja perekonnaelu puutumatuse riive võimalik muuhulgas kuriteo tõkestamiseks või kurjategija tabamiseks ilma täiendava loamenetluseta, siis PS § 43 lubab sekkumist sõnumisaladusse kuriteo tõkestamiseks või kriminaalmenetluses tõe väljaselgitamiseks üksnes kohtu loal. Kehtivast õigusest nähtub, et seadusandja on otsustanud paigutada sideettevõtjale päringu tegemist PS § 26 kaitsealasse.

Kuni 01.01.2013.a kehtinud KrMS redaktsioonis[180] oli vastav regulatsioon sätestatud §-s 117 ning andmete kogumine oli käsitletav jälitustoiminguna, mille läbiviimine eeldas menetlust juhtiva prokuröri luba (KrMS § 112 lg 3). Ühtlasi eeldas päringu esitamine sideettevõtjale toimingu vastavust üldistele jälitustoimingute teostamise eeldustele, mis olid sätestatud KrMS §-des 110 - 112. KrMS § 110 lg 1^1 piiras oluliselt ka kuritegude ringi, millal päring sideettevõtjale oli lubatud. KrMS muutmisel leidis jälitustegevust analüüsinud töörühm, et ESS §-s 111^1 loetletud andmed võib arvata jälitustoimingute ringist välja.[181] Seletuskirja kohaselt võivad menetlejad kriminaalmenetluse raames teha mitmeid erinevaid päringuid erinevate andmete saamiseks (näiteks elukohapäring, telefoninumbri otsimine telefoniraamatust, info küsimine infoliinilt, isikule kuuluva kinnisvara päring, isiku sõiduautode päring jt), mis sisaldavad samuti andmeid isiku eraelu kohta, võimaldades luua ettekujutus isiku igapäevase

[177] Kriminaalmenetluse seadustiku muutmise ja sellega seonduvate teiste seaduste muutmise seaduse (175 SE) seletuskiri, lk 4. Arvutivõrgus: http://www.riigikogu.ee/tegevus/eelnoud/eelnou/86dde8ff-c50e-48ba-a39e-a325fe15a3f0/Kriminaalmenetluse-seadustiku-muutmise-ja-sellega-seonduvalt-teiste-seaduste-muutmise-seadus/ (04.05.2015).
[178] S. Laos, U. Lõhmus. PS-i § 43/6.
[179] EIKo 08.08.1984, 8691/79, *Malone vs The United Kingdom*, p 80. EIKo 93.04.2007, 6261/00, *Copland vs The United Kingdom*, p 44.

[180] Kriminaalmenetluse seadustik. – RT I 2003, 27, 166 … RT I, 16.11.2012, 17.
[181] 175 SE seletuskiri, lk 3.

elu kohta. Samas ei ole sellised päringud käsitletavad jälitustoimingutena, mistõttu puudub põhjendus pidada jälitustoiminguks ka ESS § 111^1 sätestatud andmete pärimist sideettevõtjalt. Seletuskirjas leitakse, et selliste andmete teadasaamisel ei pruugi menetleja saada sellist infot, mis riivaks isiku põhiõigusi määral, et eeldaks teabe käsitlemist jälitustoiminguna.[182]

Käesoleva töö autor nõustub seletuskirjas väljendatud seisukohaga üksnes osaliselt. Asjaolu, kas sideettevõtjale päringu esitamist tuleks lugeda jälitustoiminguks või mitte ei ole siinkohal määrava tähtsusega. Arvestades KrMS § 126^1 lg 1 toodud jälitustoimingu definitsiooni ei pruugi päringu tegemine sideettevõtjale konkreetse definitsiooni alla paigutuda, kuivõrd andmete töötlemise fakt ega sisu ei ole andmesubjekti jaoks täielikult varjatud - nii säilitatavate andmete loetelu kui ka õiguskaitseasutuste andmetele ligipääsu võimalus on reguleeritud seaduses. Küll aga tuleb hinnata päringuga kaasneva isiku õiguste riive ulatust ning hinnata, kas seaduses on sätestatud piisavad tagatised riive õiguspärasuse tagamiseks.

KrMS § 90^1 jaotab sideettevõtjalt saadavad andmed kaheks:

- andmed, mille puhul ei ole päringu tegemiseks vaja eraldi lubasid ning päringu tegemise otsustab menetleja (KrMS §90^1 lg 1);

- andmed, mille pärimine eeldab kohtueelses menetluses prokuratuuri ja kohtumenetluses kohtu luba (KrMS §90^1 lg 2).

Ilma eraldi loata saab KrMS § 90^1 lg 1 kohaselt teha päringu selliste andmete kohta, mis on vajalikud üldkasutatava elektroonilise side võrgus kasutatavate identifitseerimistunnustega seotud lõppkasutaja tuvastamiseks, välja arvatud sõnumi edastamise fakti käsitlevad andmed. Paraku KrMS § 90^1 lg 1 ei viita ESS-ile ega täpsusta, milliseid andmeid täpsemalt silmas peetakse. Sätte seletuskirja kohaselt käsitleb KrMS § 90^1 lg 1 nn omanikupäringuid. Sellised päringud võivad hõlmata näiteks telefoni IMEI-numbrit, SIM-kaardi numbrit, kasutajakonto andmeid, IP-aadressi jt.

Käesoleva töö autor nõustub seletuskirjas märgituga selles osas, et KrMS § 90^1 lg 1 sätestatudandmete teadasaamisel ei pruugi menetleja kohe identifitseerida isikut, kes konkreetsel huvipakkuval hetkel seadet kasutas, sest sama IP-aadressi või telefoninumbrit võib kasutada mitu erinevat inimest. Siiski leiab autor, et näiteks internetiportaali kasutajatunnus, aga ka telefoninumber koosmõjus muu menetlejale teadaoleva või kättesaadava teabega võib tugevalt riivata isiku õigust eraelu puutumatusele. Euroopa Kohus asus seisukohale, et andmete säilitamise direktiivis sätestatud säilitatavate andmete loetelu võimaldab tuvastada, millise

[182] *Ibid*, lk 3-4.

isikuga ja millise sidevahendi kaudu abonent või registreeritud kasutaja suhtles, ning teha kindlaks side toimumise aja ja koha. Need andmed võimaldavad tuvastada, kui sageli abonent või registreeritud kasutaja teatud isikutega mingil ajavahemikul suhtles ning teha väga täpseid järeldusi selliste isikute eraelu kohta, kelle andmeid säilitatakse, näiteks nende igapäevaelu harjumuste, alalise või ajutise elukoha, igapäevaste või muude liikumiste, tegevuste, sotsiaalsete suhete ja ühiskonnagruppide kohta, kellega nad läbi käivad. [183]

KrMS § 90^1 lg 2 näeb ette kriminaalmenetluse raames päringu tegemist sideettevõtjale ESS §111^1 lg 2 ja 3 nimetatud andmete saamiseks, mida ei ole nimetatud KrMS § 90^1 lg-s 1. Seega saab selle sätte alusel teha sideettevõtjale päringu selliste andmete saamiseks, mis käsitlevad sõnumi edastamise fakti. Nagu eespool märgitud on päringu tegemise eelduseks kohtueelses menetluses prokuratuuri ja kohtumenetluses kohtu loa olemasolu. Seletuskirja kohaselt hõlmab KrMS § 90^1 lg 2 päringute tegemist nn kõneeristuste kohta. Siinkohal soovib käesoleva töö autor märkida, et õigusselguse seisukohalt oleks otstarbekas selgelt piiritleda KrMS § 90^1 lg 1 ja lg 2 kohaldamisalad, kuivõrd praeguses sõnastuses ei pruugi eraisikule olla lõplikult selge, millal on päringu tegemiseks vajalik luba ja millal mitte. Selline olukord võib mõjutada negatiivselt õigusselgust ning seega ka isiku teadlikkust.

KrMS § 90^1 lg 3 sätestab, et sideettevõtjale päringu tegemine on lubatud üksnes juhul, kui see vältimatult vajalik kriminaalmenetluse saavutamise eesmärgil. Seletuskirja kohaselt on sätte eesmärk rõhutada KrMS § 90^1 olulisust ning korrata üle kriminaalmenetluses kehtivat *ultima ratio* põhimõtet.[184] Erinevalt kuni 01.01.2013.a kehtinud regulatsioonist (KrMS § 110 lg 1 ja lg 1^1 ning § 117) ei sisalda kehtiv õigus enam muid kitsendusi sideettevõtjale päringu tegemiseks. Varasemalt laienesid päringu tegemisele jälitustoimingu lubatavuse üldised eeldused. Jälitustoimingut (sh §-s 117 sätestatud) tohtis teostada üksnes olukorras, kui tõendite kogumine muude menetlustoimingutega oli kas välistatud või oluliselt raskendatud, kriminaalmenetluse esemeks oli esimese astme kuritegu või tahtlikult toimepandud teise astme kuritegu, mille eest oli ette nähtud karistusena vähemalt kuni kolm aastat vangistust (kuni 01.01.2013.a kehtinud KrMS § 110 lg 1). KrMS § 110 lg 1^1 täiendas, et tõendite kogumine KrMS §-s 117 nimetatud toiminguga on lubatud ainult kirjaliku üksikpäringuga konkreetse telefonikõne, konkreetse elektronkirja, konkreetse elektroonilise kommentaari või muu üksiksõnumi edastamisega seotud sideseansi kohta. Arvestades, et sideandmete päring võib olla oluline ka selliste

[183] EKo 8.04.2014, liidetud kohtuasjad C-293/12 *Digital Rights Ireland Ltd vs Minister for Communications, Marine and Natural Resources ja teised* ja C-594/12 *Kärntner Landesregierung ja teised*, p 26-27.
[184] 175 SE seletuskiri, lk 5.

kuritegude puhul, mis ei olnud kaetud KrMS § 110 lg-s 1 sätestatud kriteeriumidega, nägi § 110 lg 1^1 täiendava nimekirja kuritegudest.[185] KrMS §110 lg 1^1 hõlmas selliseid kuritegusid, mille uurimisel võiksid sideandmed olla määrava tähtsusega. Näiteks arvutiviiruste levitamist (KarS § 208) oleks ilmselgelt raske uurida olukorras, kus menetlejal puudub ligipääs sideettevõtja poolt säilitatavatele andmetele.

Kuigi andmete säilitamise direktiivi art 1 lg 1 piiritleb direktiivi kohaldamisala ainult raskete kuritegudega (*serious crime*), ei ole Eesti kehtivasse õigusesse vastavat kriteeriumi üle võetud. Arvestades direktiivi õiguslikku tähendust, EL karistusõiguses levinud arusaamu ning EL liikmesriikide õigussüsteemide erinevust ning asjaolu, et direktiivi vastuvõtmine toimus 2006.a, st enne Lissaboni lepingu jõustumist ja kriminaal- ning karistusõiguse valdkonnas ELi pädevuse suurenemist, ei ole direktiivis raske kuriteo mõiste defineeritud. Direktiivi põhjenduspunkt 9 toob mõiste "raske juhtum" *(serious matter)* sisustamiseks organiseeritud kuritegevuse ja terrorismi näite. Samas kooskõlas EL pädevusega karistusõiguse valdkonnas on raske kuriteo defineerimine jäetud liikmesriikidele. Sideandmete päringu osas 01.01.2013.a jõustunud KrMS muudatused enam kohaldamisala piiramist ette ei näe ning KrMS § 90^1 sätestatud menetlustoiming on lubatud kõikide kuritegude puhul.

Euroopa Kohus tegi 8.aprillil 2014.a märgilise tähtsusega otsuse, millega tunnistas andmete säilitamise direktiiv kehtetuks. Kohus leidis, et direktiivi vastuvõtmisel ei ole järgitud proportsionaalsuse põhimõtet ning direktiiv ei ole kooskõlas EL põhiõiguste harta artiklitega 7 (õigus era- ja perekonnaelu austamine) ja 8 (isikuandmete kaitse) ning artikli 52 lõikega 1 (proportsionaalsuse põhimõte). Kohtu hinnangul ei sisalda direktiiv piisavaid tagatisi üksikisikute õiguste kaitseks ning jätab liikmesriikidele võimaluse rakendada direktiiv viisil, mis ebaproportsionaalselt riivab isikute põhiõigusi. Samas leiab kohus, et üldiselt on õiguskaitseasutuste juurdepääs sideettevõtjate andmetele raske kuritegevuse vastase võitluse kontekstis vajalik meede ning on kooskõlas üldise huvi eesmärgiga (kohtuotsuse punktid 41 - 44). Direktiivi kehtetuks tunnistamise põhjuseks on seega ebapiisavad proportsionaalsuse

[185] Nimekirjas olid järgnevad kuriteod: KarSi §-des 120 (ähvardamine), 156 (sõnumisaladuse rikkumine), 157 (kutse- ja ametitegevuses teatavaks saanud saladuse hoidmise kohustuse rikkumine), 179 (lapseealise seksuaalne ahvatlemine), 180 (alaealisele vägivalla eksponeerimine), 206 lg 1 (arvutiseadmetesse sekkumine), 207 (arvutisüsteemi toimimise takistamine), 208 lg 1 (nuhkvara, pahavara ja arvutiviiruse levitamine), 217 lg 1 (arvutisüsteemi ebaseaduslik kasutamine), 245 (Eesti Vabariigi ametliku sümboli teotamine), 247 (rahvusvaheliselt kaitstud isiku laimamine), 249 (välisriigi ja rahvusvahelise organisatsiooni ametliku sümboli teotamine), 275 (võimuesindaja ja avalikku võimu kaitsva muu isiku laimamine ja solvamine), 305 (kohtu ja kohtuniku laimamine), 323^1 (saladuse hoidmise kohustuse rikkumine), 331^1 (kohtulahendi täitmata jätmine), 377 lg 1 (ärisaladuse õigustamatu avaldamine ja kasutamine) ja 398 (siseteabe väärkasutamine).

tagatised, mitte aga andmete säilitamise ja õiguskaitseasutustele väljastamise regulatsiooni ebaseaduslikkus kui selline.

Üldjuhul ei too direktiivi kehtetuks tunnistamine automaatselt kaasa liikmesriikide siseriiklike seaduste kehtetust ning samale seisukohale asus ka õiguskantsler[186]. Siiski võib liikmesriigi kohus tunnistada siseriiklikud sätted kehtetuks tuginedes riigi põhiseadusele, aga ka EL õiguse üldpõhimõtetele, samuti saab riigi kohus arvestada oma hinnangu andmisel EL Kohtu argumentatsiooni. EL Põhiõiguste harta on liikmesriikidele siduv küll üksnes niivõrd, kuivõrd liikmesriik rakendab EL õigust, kuid andmete säilitamise direktiivi tühistamise järgselt on mitmed riigid asunud analüüsima oma andmete säilitamise reegleid. Saksamaa Konstitutsioonikohus oli andmete säilitamist reguleerivad siseriiklikud sätted kehtetuks tunnistanud juba 2010.a.[187] Austria Konstitutsioonikohus tunnistas vastava siseriikliku seaduse ebaproportsionaalseks ja seega kehtetuks juunis 2014.[188] Samale järeldusele jõudis ka näiteks Rumeenia konstitutsioonikohus ning Hollandi kohus.[189]

Kohtuotsuse valguses tõusetub paratamatult küsimus, kas Eesti õigus on proportsionaalne ning tagab piisava põhiõiguste kaitse. Andmete säilitamise regulatsiooni põhiseaduspärasust ning selle regulatsiooni alusel kogutud tõendite lubatavust hindas ka Riigikohus.[190] Riigikohtu hinnangul olid kuni 01.01.2013.a kehtinud kriminaalmenetlusseadustiku sätted proportsionaalsed ning põhiseadusega kooskõlas. Paraku käsitles viidatud kohtuasi varasemat olukorda ning hinnangu andmisel lähtus Riigikohus KrMS vanast redaktsioonist, mille kohaselt oli sideettevõtjale päringu tegemine käsitletud jälitustoiminguna ning seadus sätestas andmete kasutamiseks rangemaid tingimusi.

---

[186] Õiguskantsleri kiri 15.07.2014.a kiri nr 6-1/140621/1403065. Arvutivõrgus: http://adr.rik.ee/jm/dokument/4042786 (04.05.2015).

[187] Saksa Konstitutsioonikohtu 02.03.2010.a otsus kohtuasjades 1 BvR 256/08, 1 BvR 263/08 ning 1 BvR 263/08 Arvutivõrgus: http://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2010/bvg10-011.html;jsessionid=3ED96B75BBF41C49EB668A862157530D.2_cid361 (kohtuotsuse inglisekeelne kokkuvõte; 04.05.2015) http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2010/03/rs20100302_1bvr025608.html;jsessionid=C06B254E3D18C0837807FEF6319183CA.2_cid393 (kohtuotsus saksa keeles; 04.05.2015)

[188] Austria Konstitutsioonikohtu 27.06.2014.a otsus kohtuasjades G 47/2012-49, G 59/2012-38, G 62/2012-46, G 70/2012-40, G 71/2012-36. Arvutivõrgus: https://www.vfgh.gv.at/cms/vfgh-site/attachments/1/5/8/CH0006/CMS1409900579500/erwaegungeneng28082014.pdf (kohtuotsuse inglisekeelne kokkuvõte; 04.05.2015). http://www.ris.bka.gv.at/Dokumente/Vfgh/JFT_20140627_12G00047_00/JFT_20140627_12G00047_00.pdf (terve kohtuotsus saksa keeles; 04.05.2015)

[189] Rumeenia konstitutsioonikohtu 08.07.2014.a otsus nr 440. Arvutivõrgus: http://privacy.apti.ro/decizia-curtii-constitutionale-date-trafic/ (rumeenia keeles; 04.05.2015). Haagi kohtu 11.03.2015.a otsus nr C/09/480009/KGZA14/1575. Arvutivõrgus: http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2015:2498 (hollandi keeles; 04.05.2015).

[190] RKKKo 3-1-1-51-14, p 18 – 22.4.

KrMS § 90[1] proportsionaalsuse hindamisel tuleb hinnata kasutatava meetme õigustatust taotletava eesmärgi suhtes. Nagu eespool käsitletud, on üldiselt aktsepteeritud seisukoht, et kriminaalmenetluse eesmärkide saavutamine annab piisava aluse isiku põhiõiguste piiramiseks. Seega võib autori hinnangul väita, et sideandmete kasutamine kriminaalmenetluses on üldiselt asjakohane viis tõendusteabe hankimiseks, eriti arvestades sidevahendite suurt rolli tänapäeva ühiskonnas. Nüüdisaja tehnoloogiate kasutamine kuritegevusvastases võitluses on vajalik, kuivõrd võimaldab kuritegusid tõhusamalt uurida.[191] Siiski tõusetub küsimus selles osas, kas kuivõrd proportsionaalne on kõigi andmete säilitamine kõigi isikute kohta, samuti päringu tegemise võimalus iga kuriteo puhul ning kas iga kuriteo jaoks peaks olema võimalik esitada päringu mistahes andmete saamiseks. KrMS §90[1] ei sea menetlejate võimalust nõuda sideettevõtjalt andmete esitamist sõltuvusse kuriteo raskusastmest või kuriteotunnustest. Arvestades, kuivõrd lai on ESS § 111[1] andmete loetelu, võib väiksemate kuritegude puhul kõigi andmete küsimise võimalus olla autori hinnangul ebaproportsionaalne. KrMS § 90[1] lg 3 sätestatut ei saa käsitleda piisava piiranguna, kuivõrd tegemist on üldise kriminaalmenetluse põhimõtte ülekordamisega ning põhimõtte sisustamine jääb täielikult menetlejate otsustada.

Oluline on selgelt defineerida, millistel juhtudel, milliste kriteeriumide alusel on pädevatel asutustel võimalik esitada sideettevõtjale päringu. Vähem olulised ei ole ka päringu esitamise vormilised nõuded, kuivõrd arvestades isiku privaatsusõiguse riivamise ulatust peab päringu esitamise õiguspärasus olema kontrollitav. Siinkohal on aga Eesti õiguses kehtestatud nõuded küllaltki pealiskaudsed - järelepärimine peab olema kirjalikus või elektroonilises vormis, kusjuures teatud andmete puhul on lubatud ka päringu tegemine suuliselt (ESS § 112 lg 2). Autori hinnangul on tervitatav, et seadusandja on päringu vormi kehtestamisel eristanud rohkem- ja vähemsekkuvat teavet ning sellest lähtuvalt ka diferentseerinud järelepärimise vormi. Kuigi järelepärimises eneses ei oleks eelduslikult asjakohane välja tuua põhjused, millest tulenevalt päring tehakse, kuivõrd see võib kahjustada kriminaalmenetlust, tuleks vastavad põhjused selgitada vähemalt isikuõigustesse rohkem sekkuva teabe pärimisel näiteks kriminaaltoimikusse lisatavas dokumendis. Samuti on autori hinnangul küsitav võimalus esitada päring suuliselt, olgugi et parooli esitamisel. Kuigi suulise päringu alusel väljastatavad andmed ei ole isiku eraelu tugevalt riivavad,[192] kujutab päring endast siiski sekkumise privaatsfääri ning sellisel juhul peaks õiguskaitseasutuse tegevus olema kontrollitav, mida aga

[191] EKo liidetud kohtuasjades C-293/12 ja C-594/12, p 49.

[192] ESS § 112 lg 2 alusel on suulise päringu alusel võimalik saada teavet telefoniteenuse puhul helistaja numbri ning kliendi nime ja aadressi, vastuvõtja numbri ning kliendi nime ja aadressi ning internetiteenuse puhul kliendi nime ja aadressi, kelle nimele Interneti-protokolli aadress, kasutajatunnus või number olid side toimumise ajal eraldatud.

ei ole võimalik tagada suulise päringu puhul. Euroopa Kohtu hinnangul mõjutab sideandmetele juurdepääsu võimaldamise seaduslikkust ka asjaolu, kas päringu tegemine eeldab sõltumatu asutuse luba päringu tegemiseks. Siinkohal on Eesti õiguses siiski tehtud erisus ning teatud andmete puhul on vajalik prokuratuuri luba. Kuigi prokuratuur ei pruugi vastata kohtu nimetatud sõltumatu haldusasutuse kriteeriumitele,[193] on see autori hinnangul arvestades kriminaalmenetluse muid sätteid siiski piisavalt asjakohane eelkontrolli asutus. Küll aga on autor seisukohal, nagu eespool käsitletud, et seaduses tuleks selgemalt piiritleda, milliste andmete puhul on eelneva loa saamine kohustuslik. Kohus toob olulisena välja ka andmete säilitamise tähtaja, kuivõrd tähtaja piiramine kuulub andmekaitse aluspõhimõtete hulka. Kuivõrd Eestis on säilitamise tähtajaks märgitud 1 aasta (ESS § 111^1 lg 4), on see autori hinnangul sobilik.

Tagamaks sideettevõtjale päringu tegemise põhiseaduspärasuse, on autori hinnangul vajalik selgete kriteeriumide sätestamine seaduses, millistel juhtudel on menetlejal võimalik teostada päring sideettevõtjale. Autor leiab, et kuigi sideandmete saamiseks päringu esitamise võimalus on kriminaalmenetluses taotletava eesmärgi suhtes vajalik meede, tuleb isiku eraellu sekkumise õiguspärasuse tagamiseks kehtestada kindlad reeglid ja piirangud selle kohta, kuidas ning millistel juhtudel on päringu esitamine lubatud. Arvestades eraelu puutumatuse riive intensiivsust tuleb PS-ga kooskõla tagamiseks täpselt piiritleda, milliste kuritegude puhul on õiguskaitseasutustel võimalus saada milliseid andmeid. Ühtlasi tuleks kehtestada päringu tegemisel põhjendamise nõue, mis säilitatakse koos kriminaalmenetluse materjalidega.

2.5 Biomeetriliste andmete töötlemine

Tänapäeval on ilmselt raske alahinnata biomeetriliste andmete rolli isikute identifitseerimisel ning nende andmete suurt tähtsust kriminaalmenetluses. Biomeetrilised andmed on oma olemuselt isikuandmed ning IKS § 4 lg 2 p 5 liigitab need delikaatseteks isikuandmeteks. IKS ei kehtesta delikaatsete isikuandmete töötlemisele rangemaid reegleid,[194] kuigi selline eeldus

[193] Kohus käsitleb asjakohaseks eelkõige kohtu või sellise sõltumatu haldusasutuse otsust, kelle eesmärk on piirata andmetele juurdepääsu üksnes selliste päringutega, mis on rangelt vajalikud. EKo liidetud kohtuasjades C-293/12 ja C-594/12, p 62.

[194] IKS § 27 näeb ette delikaatsete isikuandmete töötleja registreerimist. Siiski ei ole autori hinnangul registreerimiskohustusel mõju andmete kaitse tagamisele, kuivõrd tegemist on töötlemisele eelneva kontrolliga ning loa andmisega. Samuti ei ole selge registreerimiskohustuse kohaldumine riigiasutustele, kuivõrd IKS § 27 lg 2 viitab töötleja majandustegevusele, tegevusloale ning litsentsile, mis aga ei ole kohaldatavad haldusasutuste puhul. Registreerimiskohustuse alternatiiviks on andmekaitse eest vastutava isiku määramine, kelle kohustuseks

on tuletatav nii konventsioon 108 art-st 6 kui ka andmekaitsedirektiivi art-st 8. KrMS § 99[1] sätestab teatud juhtudel kahtlustatavate, süüdistatavate ning süüdimõistetud isikute daktüloskopeerimist ning nendelt DNA-proovi[195] võtmist. Toimingute eesmärk on süütegude menetlemine, avastamine ning ärahoidmine. Saadud andmed kantakse vastavalt riiklikusse sõrmejälgede registrisse (*edaspidi RSR*) või riiklikusse DNA-registrisse (*edaspidi RDNAR*) (KrMS § 99[1] lg 4). Tegemist on juba 2006.a loodud riiklike registritega, mille ülesandeks on kohtuekspertiisiseaduse (*edaspidi KES*) §-ide 9[4] ja 9[5] kohaselt isikutelt ning sündmuskohalt seaduse alusel kogutud naha papillaarkurrustiku jälgede ja DNA-proovide analüüsil saadud andmete töötlemine ja säilitamine. Eesti riiklikusse sõrmejälgede registrisse on kantud ligikaudu 150 000 isiku sõrmejäljed.[196]

KrMS § 99[1] sätestatu alusel kantakse ja säilitatakse riiklikes registrites kahtlustatavate, süüdistatavate ning süüdimõistetud isikute sõrmejäljed ning DNA andmed (*edaspidi koos biomeetrilised andmed*). KrMS § 99[1] lg 1 kohaselt on biomeetriliste andmete kogumine ja säilitamine kohustuslik teatud liiki kuritegude puhul. Kuritegude nimekiri hõlmab KarS 9. peatüki 1., 2., 6. või 7. jaos, 11. peatüki 2. jaos, 22. peatüki 1. või 4. jaos sätestatud tahtlikke kuritegusid või muus peatükis sätestatud tahtlikke kuritegusid, mille koosseisutunnus on vägivalla kasutamine ja mille eest on ette nähtud vähemalt kaheaastane vangistus. Seletuskirja kohaselt on tegemist kuritegudega, mille toimepanemisel on tugevalt rikutud kannatanu füüsilist, psüühilist või seksuaalset puutumatust, või tegemist üldohtlike tegudega, mistõttu esineb eriti suur huvi nende tegude kordumist ära hoida. Lahtist loetelu on põhjendatud sellega, et mitmed koosseisud karistusseadustiku[197] teistes peatükkides näevad kas põhikoosseisus või raskendava asjaoluna ette vägivalla kasutamise (näiteks KarS-i §-d 151, 200, 209, 240, 257, 263). [198]

Lisaks KrMS § 99[1] lg 1 sätestatud kohustuslikule andmete kogumisele näeb KrMS § 99[1] lg 2 ette võimaluse koguda ning kanda registritesse sõrmejälgi ning DNA andmeid tõendamisvajadusest lähtuvalt ka mistahes muude vähemalt 1-aastase vangistusega

---

on sõltumatu kontrolli teostamine delikaatsete andmete töötlemise üle. Samas, kuivõrd töötlemisele erikorda kehtestatud ei ole, kontrollib andmekaitse eest vastutav isik sisuliselt üldiste andmekaitsereeglite täitmist.

[195] DNA (desoksüribonukleiinhape) on kõigis elusorganismides sisalduv nn pärilikkusaine. DNA makromolekul on polümeer, milles sisaldub kümneid tuhandeid geene. Iga elusolendi geenide koosseis ehk genoom on unikaalne (erandiks on siinkohal ühemunarakukaksikud). Organismi kõigis rakkudes sisalduv DNA on ühesugune, see ei muutu inimese elu jooksul. (Lindmäe, H. 1997. Menetlustaktika II. Tallinn: Juura, lk. 158).

[196] Teave Eesti Kohtuekspertiisi Instituudilt 13.04.2015.a seisuga.

[197] Karistusseadustik. – RT I 2001, 61, 364 … RT I, 23.12.2014, 16.

[198] Kohtuekspertiisiseaduse ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu seletuskiri, lk 13. Kättesaadav: http://www.riigikogu.ee/?op=ems&page=eelnou&eid=a1404746-e1ec-4720-87a8-0f1550237bea&

karistatavate kuritegude puhul. Seega sellistel juhtudel saab menetleja kaalutlusõiguse alusel otsustada andmete kogumise vajaduse.

Inimese rakkudes sisalduv kodeeritud informatsioon on ideaalne vahend isiku identifitseerimiseks. Geneetilised koodid sisaldavad tohutu hulka erinevat informatsiooni – alates inimese kasvust ja kehaehitusest kuni tema juuste ja silmade värvini. Kriminaalmenetluses ei uurita inimese täielikku geneetilist koodi – isiku identifitseerimiseks piisab teatud DNA lõikude analüüsimisest.[199]

Seoses riiklike DNA ja sõrmejälgede andmebaasidega on aktuaalne küsimus biomeetriliste andmete säilitamise proportsionaalsusest. EIK märgib oma 4.12.2008.a otsuses *S ja Marper vs Ühendkuningriik*, et nii sõrmejälgede kui DNA-proovide ja -profiilide puhul on tegemist isikuandmetega. Kuigi DNA-profiilid sisaldavad oluliselt piiratumal hulgal geneetilist informatsiooni kui DNA-proovid, võimaldab profiilide automatiseeritud töötlemine sekkuda ulatuslikult isiku eraellu. DNA-profiili alusel on pädeval asutusel võimalik määratleda isiku geneetilised seosed teiste isikutega, isiku etnilist päritolu jt eraelupuutumatust riivavat teavet. Seejuures pole oluline, et profiilid sisaldavad üksnes kodeeritud infot, millest arusaamine eeldab vastava tarkvara ja väljaõppe olemasolu. Sõrmejälgede osas märgib kohus, et kuigi neis sisalduv info ei ole niivõrd tundlik, kui DNA-proovide ja - profiilide puhul, on sellise info säilitamine struktureeritud kujul ning võimalus võrrelda andmeid andmebaasis sisalduvate isikustatud ning isikustamata jälgedega riivad isiku eraelu puutumatust EIÕK art 8 tähenduses.[200]

Nagu varasemalt käsitletud, võib vajadus kriminaalmenetluse läbiviimiseks õigustada sekkumist isiku põhiõigustesse. Seega tuleb leida sobilik tasakaal isiku DNA-profiili ning sõrmejälgede säilitamise ning isikuandmete kaitse vajaduse vahel. Autori hinnangul ei ole kaheldav, et kriminaalmenetluse raames on andmete kogumine kurjategija väljaselgitamise ja karistamise eesmärgil vajalik ning proportsionaalne meede. EIK on muuhulgas leidnud, et võitlus organiseeritud kuritegevuse ja terrorismi vastu, mis on kaasaegse ühiskonna suuremaid väljakutseid, sõltub suuresti uudsete tehnoloogiate kasutamisest.[201] Autor leiab, et KrMS § 99^1 lg 1 sätestab üldiselt piisava ettenähtavusega asjaolud ning tingimused, mille puhul on biomeetriliste andmete kogumine ning säilitamine kriminaalmenetluses lubatud. Samas on

[199] D. Owen. Politseilabor. Kuidas teaduslik kohtuekspertiis aitab leida kurjategijaid. Tallinn: Koolibri, 2005, lk 108.

[200] *S. ja Marper vs Ühendkuningriik*, p 68 – 75.
[201] *S. ja Marper vs Ühendkuningriik*, p 105.

küsitav, kas KrMS § 99^1 lg 2 sätestab piisava täpsusega menetleja kaalutlusõiguse piirid biomeetriliste andmete kogumise otsustamisel. Diskretsiooniõiguse kasutamise otsustamisel on hetkel pandud menetlejale ainult kohustus kontrollida, kas isik on kahtlustatav või süüdistatav kuriteos, mille eest on ette nähtud vähemalt 1-aastane vangistus. Autori arvates on küsitav, kas seaduses sätestatud kaalutlusõiguse piirid on piisavad ning tagavad vajaliku ettenähtavuse ja proportsionaalsuse. Esiteks ei nõua seadus menetleja diskretsiooniotsuse kirjalikku fikseerimist ega põhjendamist ning teiseks ei ole defineeritud muid otsuse tegemise kriteeriume kui seaduses sätestatud karistus. Autori arvates on vajalik KrMS § 99^1 lg 2 sätestatud tingimuste täpsem määratlemine, näiteks lähtuvalt konkreetse isikule süüks arvatava kuriteo asjaoludest.

Lisaks KrMS § 99^1 sätestatule on kriminaalmenetluses võimalik kasutada ka muul eesmärgil kogutud daktüloskopeerimisel ja DNA-proovi analüüsil saadud andmeid. KrMS-is sätestatust erinevatel eesmärkidel kogutakse isikute biomeetrilisi andmeid näiteks korrakaitseseaduses[202] (§ 33), isikut tõendavate dokumentide seaduses[203] (§ 9^2), välismaalaste seaduses[204] (mh § 275, 276), välismaalasele rahvusvahelise kaitse andmise seaduses[205] (§ 15, § 47, § 60) ja teistes seadustes. Üldistatult võib öelda, et kõigi nende sätete alusel on andmete kogumise eesmärgiks isikusamasuse tuvastamine, st kinnituse leidmine, et konkreetne isik on just see, kellena ta end esitleb. Inimgeeniuuringute seaduse[206] alusel säilitatakse geenivaramus ka isikute DNA andmeid, kuid seaduse § 16 lg 1, mis on erinorm KrMS § 99^2 suhtes, keelab sõnaselgelt geenivaramu kasutamist tsiviil- ja kriminaalmenetluses tõendite kogumiseks või jälitustegevuseks.

Tagamaks KrMS § 99^2 lg 1 proportsionaalsuse, näeb seadus ette tingimused, millal on muul eesmärgil kogutud andmete kasutamine kriminaalmenetluses lubatud. KrMS § 99^2 lg 1 sätestab, et sätte kasutamine on lubatud üksnes juhul, kui tõendite kogumine muu menetlustoiminguga ei ole võimalik või on oluliselt raskendatud või kui see võib kahjustada kriminaalmenetluse huve. KrMS § 99^2 lg 2 täpsustab, et andmete kasutamine on võimalik üksnes juhul, kui kriminaalmenetluses kogutakse teavet sellise esimese astme kuriteo kohta, mille eest nähakse karistusena ette vähemalt kolmeaastane vangistus. Lisaks peab muudel eesmärkidel kogutud andmete kasutamise taotlemiseks olema kirjalik prokuratuuri luba, mis peab sisaldama ka selle kohta, miks andmete kasutamine on vajalik (KrMS § 99^2 lg 3). KrMS § 99^2 lg-tes 1 ja 2

[203] Isikut tõendavate dokumentide seadus. - RT I 1999, 25, 365 ... RT I, 23.03.2015, 16.
[204] Välismaalaste seadus. - RT I 2010, 3, 4 ... RT I, 23.03.2015, 7.
[205] Välismaalasele rahvusvahelise kaitse andmise seadus. - RT I 2006, 2, 3 ... RT I, 23.03.2015, 25.
[206] Inimgeeniuuringute seadus. - RT I 2000, 104, 685 ... RT I, 14.03.2014, 30.

sätestatud piirangud on samad, mis sisaldusid kuni 01.01.2013.a kehtinud KrMS § 110 lg-s 1, mis käsitles jälitustoiminguga andmete kogumise tingimusi. Kehtivas jälitustoimingute regulatsioonis on süütegude ring, mille puhul on jälitustoimingu tegemine lubatud, oluliselt kitsendatud. Autor on seisukohal, et muudel eesmärkidel kogutud andmete kasutamine kriminaalmenetluses võib olla õiguspärane ega riivaks isiku õigusi ebaproportsionaalselt, kui selline võimalus on seaduses selgelt reguleeritud. Hinnates KrMS §-s 99^2 kehtestatud andmete kasutamise tingimusi on autor seisukohal, et seadusandja on piisavalt piiritlenud juhtumid, mille puhul võib kasutada muul eesmärgil kogutud andmeid. Samuti leiab autor, et kuigi konkreetsetes seadustes, mille alusel andmeid algselt kogutakse, ei ole sätestatud andmete kasutamise võimalikkust kriminaalmenetluses, on õiguskord siiski piisavalt ettenähtav, sest esiteks andmete kasutamise võimalus on üheselt sõnastatud seaduses ning teiseks on seaduses ka nimetatud need süüteod, mille puhul andmete kasutamine on potentsiaalselt võimalik.

Proportsionaalsuse seisukohalt on väga oluline piiritleda, milliste isikute andmed säilitatakse ning mis perioodi jooksul on õiguskaitseasutustel võimalik saada andmetele juurdepääs. Iga andmetöötlus peab vastama minimaalsuse põhimõttele (IKS § 6 p 3), mille kohaselt võib isikuandmeid koguda üksnes ulatuses, mis on vajalik kindlaksmääratud eesmärgi saavutamiseks. KrMS §-d 99^1 ega 99^2 säilitamistähtaegu ei määratle, kuid vastav regulatsioon on olemas KES §-s 9^9. Üldreeglina näeb seadus RSR-i ja RDNAR-i kantud andmete säilitamist 40 aasta jooksul alates registrisse kandmisest (KES § 9^9 lg 1). KES § 9^9 lg 2 kohaselt kustutatakse isiku kohta registritesse kantud andmed juhul, kui isik mõistetakse õigeks või kriminaalmenetlus lõpetatakse KrMS § 200 alusel. Kohtuasjas S ja Marper *vs* UK leidis EIK, et ebaproportsionaalne on selliste isikute andmete säilitamine, kelle suhtes ei ole tehtud süüdimõistvat otsust.[207] Selles osas on Eesti õigus kooskõlas EIK praktikaga ega riiva põhjendamatult isiku privaatsust.

Olles väga tõhus isiku identifitseerimise viis, pakuvad biomeetrilised andmed ulatuslikult teavet kriminaalmenetluses ning on tänapäeval aktiivselt kasutuses. Samas riivab biomeetriliste andmete kasutamine isiku õigust eraelu puutumatusele ning seega peab selliste andmete kasutamine kriminaalmenetluses olema täpselt reguleeritud. Autori hinnangul tagab Eestis kehtiv regulatsioon üldiselt isiku õiguste kaitse ning piirab menetleja võimalust isiku eraellu sekkumiseks. Siiski tuleks seaduses täpsustada KrMS § 99^1 lg 2 ettenähtud menetleja kaalutlusõiguse piirid.

[207] *S. ja Marper vs Ühendkuningriik*, p 123.

2.6 Isikuandmete piiriülene edastamine

Andmete edastamine välisriikidesse kasvab järjepidevalt seoses majanduse globaliseerumise. Inimeste suurenev mobiilsus, tehnoloogia areng ning interneti laienev kättesaadavus mõjutavad paratamatult ka kuritegevuse struktuuri. Uutes oludes on vaja leida sobilikke lahendusi, mis võimaldaksid tõhusa teabevahetuse riikide pädevate asutuste vahel, unustamata seejuures isiku põhiõiguste kaitset. 1999.a otsustasid EL valitsusjuhid luua vabadusel, turvalisusel ja õigusel põhinev ala eesmärgiga tõhustada liikmesriikide vaheline koostöö võitluses piiriülese kuritegevuse ja ebaseadusliku rändega,[208] mis andis tõuke senisest oluliselt ulatuslikumale kriminaalõiguse harmoneerimisele. Arvestades rahvusvahelise koostöö mahtu kriminaalmenetluses[209] on ilmselgelt vajalik ka tõhusa andmekaitseraamistiku kehtestamine, mis võimaldaks tõrgeteta andmeid vahetada ning saadud andmeid kriminaalmenetluses kasutada. Uute tehnoloogiate kasutuselevõtt võimaldab kiiremat ja suuremahulisemat andmevahetust, mis paratamatult suurendab riske privaatsusele.[210] Arvestades EL-i ala ühtsust ja selle toimimise põhimõtteid ei ole EL seadusandluse kohaselt lubatud liikmesriikide vahelise andmevahetuse takistamine või piiramine, seega rääkides isikuandmete piiriülesest edastamisest peetakse silmas eelkõige andmevahetust väljaspool EL õigusruumi asuvate riikidega. Üldiselt peetakse nn kolmandate riikidega[211] toimuva andmevahetuse piiramist ja selget reglementeerimist vajalikuks vältimaks möödahiilimise võimalust EL-is kehtestatud rangetest isikuandmete kaitse normidest. Vastasel juhul võib siseriiklikel asutustel tekkida võimalus vältida EL-siseste reeglite täitmist edastades andmed nende riikide kaudu, kuhu EL reeglid ei ulatu. Liiatigi võivad kolmandate riikidega kehtestatud madalamad andmekaitsestandardid olla vastuolus tõhusa kaitse tagamise põhimõttega, sest väljaspool EL-i asuvad riigid ei pruugi pakkuda üksikisikule samasugust kaitse taset nagu EL-is.[212]

---

[208] Euroopa Ülemkogu 15. ja 16.10.1999.a Tamperes toimunud kohtumise järeldused. Arvutivõrgus: http://www.europarl.europa.eu/summits/tam_en.htm (04.05.2015).

[209] Rahvusvahelise koostööga tegeleva riigiprokuröri Eve Oleski poolt 24.04.2015.a seisuga edastatud statistika kohaselt laekus Eestile 2013.a 719 ning 2014.a 738 taotlust. Eesti omakorda esitas välisriikidele vastavalt 275 ning 221 taotlust.

[210] OECD. Report on the enforcement of cross-border privacy laws. 2006, lk 3. Arvutivõrgus: http://www.oecd.org/internet/ieconomy/37558845.pdf (04.05.2015).

[211] Kolmandate riikidena käsitletakse siinkohal riike, mis ei kuulu EL andmekaitseõiguse territoriaalsesse kohaldamisalasse.

[212] H. Hijmans, A. Scirocco. 2009, lk 1499.

01.01.2015.a jõustunud KrMS rahvusvahelist koostööd puudutavate muudatuste raames on KrMS 19. peatükki täiendatud ka isikuandmete kaitset puudutava regulatsiooniga (KrMS §-id 489^3 - 489^5), mis kohaldub riikide vahel kriminaalmenetlusalase koostöö raames vahetatavate andmete töötlemisele.[213] Andmekaitse raamotsuse ülevõtmisel lähtus Eesti IKS § 2 lg-s 2 sätestatust, mille kohaselt kohaldub IKS üldjuhul ka kriminaalmenetlusele. KrMS muudatustega võeti üle need sätted, mis ei olnud seni IKS-is piisavalt selgelt reguleeritud. Muuhulgas märgitakse KrMS § 489^3 lg-s 1, et isikuandmete edastamisel teisele liikmesriigile tuleb järgida IKS §-s 6 sätestatud põhimõtteid. Seejuures on aga märkimisväärne, et sätte sõnastuse kohaselt tuleb IKS § 6 põhimõtetest lähtuda üksnes andmete edastamisel teisele EL liikmesriigile, kuigi teoreetiliselt peaks sama reegel kehtima ka andmete edastamisel kolmandatele riikidele ning rahvusvahelistele organsatsioonidele. KrMS § 489^3 lg 2 kehtestab omakorda üldreegli, mille kohaselt on teiselt liikmesriigilt saadud andmete töötlemine lubatud üksnes nendel eesmärkidel, milleks andmeid edastati.[214]

Arvestades vajadust kaitsta EL elanike isikuandmeid tõhusalt sõltumata sellest, kas andmed töödeldakse ainult EL-i siseselt või edastatakse ka väljapoole EL-i, näeb andmekaitsedirektiivi art 25 üldreeglina ette, et andmete edastamine kolmandasse riiki on lubatud üksnes juhul, kui vastavas riigis on tagatud piisav (*adequate*) andmekaitsetase. Andmekaitsetaset hindab Euroopa Komisjon. EL-is kehtiv kõrge andmekaitsetaseme kontseptsioon pärineb andmekaitsedirektiivi põhjenduspunktist 10, mis kehtestab nõude, et EL-is tagatav põhiõiguste ja - vabaduste kaitse, sh isikuandmete töötlemisel, ei tohi väheneda võrreldes EIÕK ja EL õiguse üldpõhimõtetes sätestatuga, vaid peab olema kõrgem. Seega on andmekaitsetaseme hindamise mõõdupuuks eelkõige EIÕK art-s 8 (ja selle alusel antud konventsioonis 108) sätestatu ning EL-is kehtiv andmekaitsereeglistik tagab isikule sellest kõrgemat kaitstuse taset. Konventsioon 108 näeb samuti ette piiriülese andmevahetuse reeglid, mis on paraku küllaltki üldised.

Kriminaalmenetluse kontekstis on selge ja tõhus andmekaitsereeglistik oluline liikmesriikide vahelise usalduse suurendamiseks ning üksikisiku õiguste kaitseks.[215] Paraku ei näe andmekaitse raamotsus direktiiviga sarnaseid piiriülese andmevahetuse detailseid reegleid. Eesti õiguses on isikuandmete välisriiki edastamise aluseks eelkõige IKS § 18. Üldreegli

[213] Kriminaalmenetluse seadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse SE 578 seletuskiri, lk 1. Arvutivõrgus: http://www.riigikogu.ee/tegevus/eelnoud/eelnou/5ebd76d0-c075-4845-89b0-c6b23cca607f/Kriminaalmenetluse-seadustiku-ja-sellega-seonduvalt-teiste-seaduste-muutmise-seadus/ (04.05.2015).
[214] Sätte aluseks on andmekaitse raamotsuse art 11.
[215] Andmekaitse raamotsus, põhjenduspunkt 5.

kohaselt tohib isikuandmeid edastada välisriiki üksnes siis, kui vastuvõtvas riigis on tagatud piisav andmekaitse tase (IKS § 18 lg 1). Piisava andmekaitsetasemega riigiks loetakse alati EL-i liikmesriiki ning Euroopa Majanduspiirkonnaga ühinenud riiki[216]. Samuti võib Euroopa Komisjon tunnistada riiki piisava andmekaitsetasemega riigiks (IKS § 18 lg 2, andmekaitsedirektiivi art 25 lg 6). Andmekaitse taseme piisavuse definitsiooni IKS-ist ei leia, seega tuleks põhimõtte sisustamisel lähtuda andmekaitsedirektiivi art 25 lg-st 2, mille kohaselt tuleb andmekaitsetaseme hindamisel arvesse võtta kõiki andmete edastamise toimingute asjaolusid ning eelkõige tuleb tähelepanu pöörata andmete laadile, kavandatud töötlemistoimingu eesmärgile ja kestusele, päritoluriigile ja lõppsihtriigile, kõnealuses riigis kehtivatele üldistele ja sektoraalsetele õigusnormidele ning riigis järgitavatele eeskirjadele ja turvameetmetele. Kuivõrd andmekaitsetaseme hindamisel võetakse lähtealuseks eelkõige EL-is kehtivat õigusraamistikku, on kolmandatel riikidel üsna keeruline saavutada taset, mida hinnataks piisavaks.[217] Seejuures tuleb aga arvestada, et andmekaitsedirektiiv ei kohaldu kriminaalmenetlusele ning selles tulenevalt ei laiene Euroopa Komisjoni otsused kriminaalõigusalasele koostööle.

Andmekaitse raamotsuse art 13 lg 1 loetleb rea kumulatiivseid tingimusi, mis peaksid olema täidetud andmete edastamiseks kolmandatesse riikidesse või rahvusvahelistele organisatsioonidele. Raamotsuses sätestatud tingimusi on Eesti õigusesse üle võetud KrMS §-ga 489[4], mille lg 1 loetleb olukorrad, millal andmete edastamine väljapoole EL-i on lubatud:

- see on vajalik kuritegude avastamiseks ja tõkestamiseks, kriminaalmenetluse läbiviimiseks või kriminaalkaristuse täideviimiseks;

- andmeid vastu võttev asutus või organisatsioon vastutab kuritegude avastamise ja tõkestamise, kriminaalmenetluse läbiviimise või karistuse täideviimise eest;

- isikuandmeid Eestile edastanud EL liikmesriik on andnud nõusoleku nende andmete edastamiseks kolmandale riigile või rahvusvahelisele organisatsioonile ja

- isikuandmeid vastu võttev riik või organisatsioon tagab andmete piisava kaitse.

[216] Euroopa Majanduspiirkond hõlmab EL liikmesriike ning täiendavalt kolme riiki: Islandit, Norrat ning Liechtensteini. Arvutivõrgus: http://www.efta.int/eea/eea-agreement (04.05.2015).

[217] Käesoleval hetkel on Euroopa Komisjon hinnanud piisavaks kõigest 7 riigi andmekaitsetaset (Iisrael, Argentiina, Uruguai, Andorra, Kanada, Šveits, Uus-Meremaa) ning 4 eriterritooriumi (Fääri saared, Jersey, Man saar, Guernsay). Samuti on Ameerika Ühendriikidega sõlmitud nn *Safe Harbour* leping, millega ühinemisel loetakse konkreetset ettevõtted EL andmekaitasemele vastavaks. Arvutivõrgus: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm (04.05.2015).

Vaadates loetletud tingimusi on üsna ilmne, et andmete edastamise alused on küllaltki laiad. Lisaks tuleb märkida, et KrMS-s piiriülest andmevahetust käsitlevad sätted kehtivad üksnes selliste andmete edastamisele, mis on omakorda Eestile edastatud teiselt liikmesriigilt. Seega ei laiene tingimused ega reeglid sellistele andmetele, mis koguti Eestis. Autori hinnangul teeb KrMS regulatsioon andmete puhul esiteks põhjendamatu sõltuvalt sellest, kus andmed on kogutud. Õiguslikult puudub põhjus, miks peaks tõhusamalt kaitsma need isikuandmed, mille algne päritolu ei ole Eestis. Arvestades, et andmekaitsereeglite eesmärk on isiku põhiõiguste tagamine kujuneb KrMS sätete alusel seega olukord, kus välismaised andmesubjektid või need Eesti andmesubjektid, kelle kohta koguti andmeid teises EL liikmesriigis, saavad eelisseisundi ning neile kohaldatakse tõhusamad põhiõiguste kaitsemeetmed võrreldes teiste isikutega. Teiseks on sätete kohaldamise praktikas küllaltki keeruliseks, sest normi rakendajad peaksid järjepidevalt kontrollima, milline on andmete päritolu ning sellest lähtuvalt ka otsustama sätete kohaldatavuse. Liiatigi ei pruugi andmete päritolu olla kuigi lihtne kindlaks teha. Asjakohasem oleks sätestada ühtsed andmevahetuse reeglid sõltumata sellest, milline on andmete päritoluriik ning vältida sellega potentsiaalselt võimalik olukord, kus sisuliselt sarnases olukorras olevate isikute põhiõigusi kaitstakse erinevalt.

Kuigi sarnaselt IKS §-ga 18 ei selgita ka KrMS, millistel tingimustel loetakse riigi või organisatsiooni andmekaitse taset piisavaks, sätestab vastavad tingimused raamotsuse art 13 lg 4. Oma sisult kattuvad raamotsuses toodud kriteeriumid andmekaitsedirektiivi art 25 lg-s 2 märgituga ning seega ka KrMS § 489^4 lg 1 tõlgendamisel ning esitatud tingimuste sisustamisel tuleks aluseks võtta raamotsuse ning direktiivi sätete tõlgendust. Samuti võib praktikas kujuneda küsitavaks KrMS § 489^4 lg 2 p-s 3 sätestatud andmete päritoluriigi nõusoleku küsimine. Küll aga ei ole selge, kes peaks andmekaitse taset hindama ning kuidas peaks toimuma nõusoleku küsimine. Lisaks tuleb arvestada, et KrMS § 489^4 lg-d 3 ja 4 sätestavad andmete edastamise üldreeglist erandid nii ilma nõusolekuta andmete edastamiseks kui ka piisava andmekaitse tasemeta riiki. Vaadates tingimusi, mille kohaselt ei pea pädevad asutused piisava andmekaitse taseme nõudest lähtuma võib asuda seisukohale, et see võib hõlmata enamuse andmete edastamise olukordi, sest erandi kohaldamiseks piisab asjaolust, et andmete edastamine on vajalik kaalukate avalike huvide kaitseks. Kuivõrd kriminaalmenetlus ongi üldjuhul suunatud (kaalukate) avalike huvide kaitsele, on KrMS §-s 489^4 sätestatud üldnormide kohaldamine küsitav. Lisaks on võimalik ka andmete edastamine riikidele ja organsatsioonidele, kes küll ei taga piisavat andmekaitse taset, kuid pakuvad isikuandmete kaitseks piisavaid tagatisi, mis on kooskõlas Eesti õigusega (KrMS § 489^4 lg 4 p 2). Seejuures on lahtine, kes, kuidas ning millise korra järgi peaks hindama rahvusvahelise organisatsiooni

või kolmanda riigi pakutavate andmekaitse tagatiste piisavust, eriti arvestades asjaolu, et kriminaalmenetluses võib andmete edastamise vajaduse tõusetuda ootamatult ning menetluse huvides võib olla andmete kiire edastamine.

Võib öelda, et hetkel kehtib kriminaalmenetluses kahesugune õigusrežiim, kus kriminaalmenetlusalase koostöö raames teiselt EL liikmesriigilt saadud andmete edastamisel kolmandasse riiki tuleb lähtuda KrMS sätetest, muudel juhtudel aga IKS §-st 18. Seejuures tuleb aga märkida, et IKS § 18 kohaldamine kriminaalmenetlusele võib olla problemaatiline, sest andmete edastamise tingimuseks on kas piisav andmekaitse tase vastuvõtvas riigis, AKI luba andmeid edastada, andmesubjekti nõusolek või erandjuhtudel (IKS § 18 lg 5 p 2) andmesubjekti või muu isiku elu, tervise või vabaduse kaitseks, kui andmesubjektilt ei ole võimalik nõusolekut saada või kui kolmas isik taotleb teavet, mis on saadud või loodud avalikke ülesandeid täites ja taotletav teave ei sisalda delikaatseid isikuandmeid ning sellele ei ole muul põhjusel kehtestatud juurdepääsupiirangut. Kriminaalmenetluse spetsiifikat arvestades võib nende tingimuste täitmine osutuda keeruliseks, kuid teiselt poolt ei tohiks see takistada kriminaalmenetluse läbiviimist.

KrMS § 489^5 toob Eesti õigusesse regulatsiooni kriminaalmenetluse andmete edastamisest eraisikule. Sättega võeti üle raamotsuse art 14. Siiski on tegemist Eesti õiguse jaoks uudse lähenemisega, kuivõrd seni ei ole Eestis §-s 489^5 toodud tingimustel olnud andmete avaldamist eraisikutele reguleeritud ning tegemist on seega sisuliselt KrMS § 214 suhtes eriregulatsiooniga. Kui KrMS § 214 sätestab andmete avaldamise tingimustena nii andmete edastamise vajaduse kui ka piirangud, siis KrMS § 489^5 piiranguid selgelt ei määratle, kuid loetleb üsna detailselt olukorrad, millal andmete avaldamise vajadus on põhjendatud. Seega tekib taaskord esiteks praktilise rakendamise probleem (menetleja peab kohaldama andmetele erinevaid reegleid sõltuvalt sellest, milline on andmete päritolu) kui ka isikutele erineva kaitse taseme võimaldamise õiguspärasus.

Kuigi andmevahetus on kriminaalmenetlusalase koostöö üks võtmetegevusi, ei leia siiski Eesti kahepoolsetest koostöölepingutest kuigi palju andmekaitset puudutavaid sätteid. EL poolt sõlmitavad lepinguid reeglina sisaldavad andmekaitsesätteid, kuid siinkohal säilib liikmesriikidel reeglina võimalus rakendada oma varasemaid kokkuleppeid. Kuivõrd kahepoolsetes lepingutes andmekaitsereegleid ei sisaldu, tuleb lähtuda IKS §-st 18 ning selle rakendamisega seotud probleeme on käsitletud eespool. Siinkohal tuleb ära märkida hiljutist KrMS täiendamist § 436 lg-ga 3, mis annab Pädevale asutusele võimaluse keelduda rahvusvahelisest koostööst kolmanda riigiga, kui on ilmne, et vastav riik ei taga piisavat

andmekaitse taset. Keeldumisotsuse peab tegema Justiitsministeerium kooskõlastatult Välisministeeriumi, AKI ning Riigiprokuratuuriga. Võib öelda, et konkreetse sätte puhul tegemist esimese sammuga selles suunas, et andmekaitsereegleid tunnustataks asjakohastena ka kriminaalmenetlusalase koostöö raames. Paraku võib säte jääda üsna deklaratiivseks, kuivõrd eelduslikult üldjuhul on rahvusvahelise koostöö puhul tegemist raskemate kuritegudega ning sellises olukorras oleks koostööst keeldumine õigustamatu. Siiski annab säte pädevatele asutustele teatud diskretsiooniõiguse ning võimaluse nõuda kolmandalt riigilt vähemalt minimaalsete andmekaitsereeglite täitmist.

EL-is on kriminaalmenetlusalane koostöö üsna laialdaselt reguleeritud ning mitmed õigusaktid viitavad andmekaitse raamotsusele kui vajalikku andmekaitse miinimumtaset kehtestavale õigusaktile. Seega on KrMS § 489^3 - 489^5 oluline roll ka muude EL õigusaktide täitmisel.[218] Siiski ei tohiks EL õiguse rakendamisel lähtuda sätestatud kohustustest liiga kitsalt, kuivõrd vastasel juhul võib tulemuseks olla praktikas raskesti rakendatav ning õigusselgusetu olukord. Võib öelda, et kuigi KrMS võtab korrektselt üle andmekaitse raamotsuse, ei pruugi seaduses sätestatud tingimuste täitmine olla praktikas võimalik ega paranda isikute õiguste kaitset olukorras, kus andmeid edastatakse piiriüleselt. Autori hinnangul oleks asjakohane lähtuda andmekaitse reeglite kehtestamise põhjustest ning võtta õigusnormide väljatöötamisel lähtekohaks vajaduse tõhusalt kaitsta andmesubjekti õigused. Seega oleks otstarbekas laiendada KrMS §-des 489^3 - 489^5 kohaldamisala selliselt, et sätetes kehtestatud reeglid kehtiksid kogu piiriülesele andmevahetusele. Vastav muudatus ei oleks vastuolus raamotsuse sätetega, sest raamotsus kehtestab üksnes miinimumnõuded ning liikmesriigil on võimalik raamotsuse sätted rakendada laiemalt.

[218] Näiteks Nõukogu raamotsus 2006/960/JSK, 18.12.2006, Euroopa Liidu liikmesriikide õiguskaitseasutuste vahelise teabe ja jälitusteabe vahetamise lihtsustamise kohta. - ELT L 29.12.2006/368, lk 89 - 100. Samuti Nõukogu otsus, 2008/615/JSK, 23.06.2008, piiriülese koostöö tõhustamise kohta, eelkõige seoses terrorismi- ja piiriülese kuritegevuse vastase võitlusega. - ELT L 06.08.2008/210, lk 1 - 11. Nõukogu otsus, 2008/616/JSK, 23.06.2008, millega rakendatakse otsust 2008/615/JSK piiriülese koostöö tõhustamise kohta, eelkõige seoses terrorismi- ja piiriülese kuritegevuse vastase võitlusega. - ELT L 06.08.2008/210, lk 12 - 17 (nn Prüm otsused).

KOKKUVÕTE

Isikuandmete kaitse on lahutamatu osa isiku õigusest eraelu puutumatusele. Isik on teda puudutavate andmete omanik ning tal on õigus omada teda puudutavate andmete üle kontrolli. Nüüdisaja tehnoloogia arengu ning globaliseerumise tulemusena on isikuandmed muutunud mõõdetava väärtusega omaette väärtuseks ning muutnud andmete töötlemist igaühe igapäevaseks tegevuseks. Üldjuhul on riigivõimul, sealhulgas õiguskaitseasutustel lubatud sekkuda isiku privaatsusesse üksnes piiratud juhtudel, kui see on proportsionaalne sekkumise põhjuseks oleva eesmärgi suhtes. Paratamatult on aga teenuste ulatuslik digitaliseerimine teinud ka õiguskaitseasutuste juurdepääsu andmetele märkimisväärselt lihtsamaks ning kiiremaks.

Käesoleva töö raames analüüsis autor isikuandmete kaitset puudutava regulatsiooni Eesti kriminaalmenetluses. Autori teema käsitlus oli piiratud andmete töötlemisega kohtueelses menetluses ning sellest väljapoole jäävaid aspekte ei uuritud.

Analüüsi käigus uuris autor isikuandmete kaitse olemust ning selle paigutust õigusruumis. Isikuandmeteks loetakse mistahes teavet tuvastatud või tuvastatava isiku kohta ning isikuandmete töötlemine on iga isikuandmetega tehtav toiming, sealhulgas kogumine, säilitamine, muutmine, avalikustamine, päringute teostamine, kasutamine, edastamine, kustutamine jt. Kuigi ei EIÕK ega PS ei sisalda selget viidet isikuandmete kaitsele kui põhiõigusele, on selline tõlgendus juurdunud kohtupraktikas. EIK on mitmel korral asunud seisukohale, et õigus isikuandmete kaitsele kuulub EIÕK art-s 8 tagatud eraelupuutumatuse kaitsealasse, mistõttu tuleb andmete töötlemisel alati arvestada EIÕK-s sätestatud põhimõtetega. Samale seisukohale on asunud ka Riigikohus, paigutades õiguse isikuandmete kaitsele PS § 26 kohaldamisalasse. Arvestades isikuandmete kaitse õiguse kuulumist põhiseadusega kaitstud väärtuste hulka tuleb isikuandmete töötlemisel lähtuda põhiseaduses sätestatud põhimõtetest ning piirangutest. PS § 11 kohaselt tohib põhiõigusi piirata üksnes kooskõlas põhiseaduse ning seadusega juhtudel, kui see on vajalik demokraatlikus ühiskonnas. Kõnealust tingimust tuleb kohtupraktika valguses tõlgendada proportsionaalsuse põhimõttena ning seega on põhiõigustesse sekkumine lubatud üksnes juhul, kui konkreetne meede on taotletava eesmärgi suhtes vajalik, mõõdukas ning asjakohane. PS lubab riigi- ja kohalikel omavalitsustel sekkuda isiku eraellu üksnes piiratud juhtudel, sealhulgas kui see on vajalik teiste inimeste õiguste ja vabaduste kaitseks, kuriteo tõkestamiseks või kurjategija tabamiseks. Kriminaalmenetlus on üks riigi põhifunktsioone, mis on suunatud üksikisikute õiguste ja vabaduste kaitsele ning turvalisuse tagamisele. Kriminaalmenetluse läbiviimine eeldab erineva tõendusteabe kogumist ning selle raames leiab aset ulatuslik isikuandmete töötlemine. Kuivõrd

kriminaalmenetluse eesmärgid on kollisioonis isikuandmete kaitse eesmärkidega, tuleb leida sobiv tasakaal kriminaalmenetluse kaudu kaitstavate huvide ning üksikisiku õiguste vahel.

Oluline on märkida, et kuigi IKS kohaldub kriminaalmenetlusele KrMS-s sätestatud erisustega, ei sisalda KrMS-s kuigi palju andmekaitsereegleid. Andmekaitseõiguses on mitmeid aluspõhimõtteid, mille täitmine tagab andmetöötluse õiguspärasuse. Autor uuris, kas ning millises ulatuses on isikuandmete kaitse üldpõhimõtted ning reeglid kohaldatavad kriminaalmenetluse kontekstis. Kuivõrd KrMS-s ei piira IKS-is sätestatud andmekaitse põhimõtete kehtivust kriminaalmenetlusele, tuleks teoreetiliselt kohaldada kriminaalmenetluses kõik põhimõtteid ilma erandeid tegemata. Siiski leidis autor analüüsi tulemusena, et kuigi kõik andmekaitsepõhimõtted peaksid kehtima ka kriminaalmenetluses, võib tekkida vajadus teatud põhimõtete kohaldamist piirata. Selleks oleks asjakohane luua KrMS-is selge isikuandmete kaitse üldregulatsioon, mis sätestaks isikuandmete töötlemise põhimõtted ja alused kriminaalmenetluses.

Kui kriminaalmenetluse puhul saab rääkida isiku menetlusõigustest, siis täiendavalt saab rääkida ka andmesubjekti õigustest. Andmesubjekti õigus omada kontrolli oma andmete üle on üks andmekaitseõiguse alustalasid. Siiski jõudis autor seisukohale, et kriminaalmenetluses ei ole andmesubjekti õiguste tagamine täies ulatuses ei ole kriminaalmenetluses võimalik. Näiteks ei saa üldjuhul eeldada, et isikul oleks õigus nõuda tema kohta menetluse raames kogutud andmete parandamist või kustutamist. Arvestades kriminaalmenetluses töödeldavate andmete hulka, andmete tundlikkust ning kaasnevat põhiõiguste riivet tuleks autori hinnangul sätestada KrMS-is selge regulatsioon, mis võimaldaks andmesubjektil teostada oma õigused, arvestades kriminaalmenetluse huvidega. Samuti asus autor seisukohale, et KrMS-s tuleks selgelt välja tuua andmesubjekti võimalus pöörduda andmekaitsealase rikkumise korral Andmekaitse Inspektsiooni poole, kellel on andmekaitse valdkonnas järelevalve teostamise pädevus.

Autor käsitles töös ka kohtueelse kriminaalmenetluse andmete avalikustamise küsimust. Autori hinnangul sätestab KrMS § 214 küll piisavalt selged tingimused, mida menetleja peaks otsuse tegemisel arvesse võtma, kuid ei reguleeri piisavalt andmekaitse aspekti. Autor leiab, et kuivõrd kriminaalmenetluse andmed on nii Eesti kui rahvusvahelise õiguse kohaselt tundlikud, tuleks andmete avaldamisel alati kaaluda, kas piisab umbisikulise teabe avalikustamisest või on vajalik ka konkreetse isiku andmete avaldamine. KrMS-i tuleks lisada vastavad täpsustused.

Lisaks üldiste andmekaitsereeglite käsitlusele analüüsis autor ka isikuandmete töötlemist kolmes olukorras – õiguskaitseasutuste juurdepääs sideandmetele, biomeetriliste andmete kasutamine ning piiriülene andmevahetus. Analüüsides 2014.a kevadel tehtud Euroopa Kohtu

lahendi valguses sideandemete säilitamise ja selliste andmete kriminaalmenetluses kasutamise regulatsiooni leidis autor, et Eestis kehtiv õigusraamistik ei ole kooskõlas proportsionaalsuse põhimõttega. Autori hinnangul tuleb regulatsioon muuta, kehtestades selged sideettevõtjale päringu esitamise tingimused ning piirangud. Sealhulgas oleks kohane eristada, milliseid andmeid on võimalik menetlejal pärida sõltuvalt süüteo raskusest.

Biomeetriliste andmete regulatsiooni osas asus autor seisukohale, et üldiselt reguleerib Eesti õigus selliste andmete säilitamist kriminaalmenetluses kooskõlas põhiseadusega. Üheks aspektiks, kus autor näeb hetkel puudusi, on seotud menetlejale jäetud diskretsiooniõiguse laiusega olukordades, kus biomeetriliste andmete kogumine ei ole kohustuslik, kuid menetlejal on võimalik andmeid menetluse huvidest lähtuvalt koguda. Autori hinnangul tuleb seaduses sätestada selgemad kriteeriumid, mida menetleja peaks oma kaalutlusõiguse kasutamisel arvestama. Kehtivas olukorras võib andmete kogumine menetleja kaalutlusõiguse alusel kujuneda ebaproportsionaalseks.

Viimaks uuris autor piiriülesele isikuandmetele edastamisele kehtivaid õigusnorme. Kuigi Eesti on võtnud nõuetekohaselt EL andmekaitse raamotsuse, on õigusraamistik autori hinnangul väga ebaselge ning lünklik. Kehtivas õiguskorras on tekkinud olukord, kus andmekaitsereeglid on erinevad sõltuvalt sellest, kas andmed, mida soovitakse välisriiki edastada, on kogutud Eestis või pärinevad need teisest liikmesriigist. Ühtlasi on problemaatiline IKS sätete kohaldumine andmete edastamisel välisriiki kriminaalmenetluse kontekstis. Autor leiab, et KrMS-s tuleks ühtlustada andmete piiriülese edastamise sätted ning kehtestada kindlad reeglid, mille järgi andmevahetus peaks käima.

Autor püstitas hüpoteesi, et üksikisiku õigus isikuandmete kaitsele ei ole kohtueelses kriminaalmenetluses piisavalt tagatud ning eraelu puutumatuse riive proportsionaalsus on küsitav. Autori hinnangul leidis hüpotees kinnituse. Kehtiva õiguse järgi kohaldub kriminaalmenetlusele isikuandmete kaitse seadus. IKS viitab omakorda erireeglite osas KrMS-ile, kuigi KrMS-is puudub kohane andmekaitseregulatsioon. IKS-i kohaldumine kriminaalmenetluses on problemaatiline suuresti põhjusel, et IKS-iga võeti Eesti õigusesse üle EL andmekaitsedirektiiv, mis on aga mõeldud reguleerima andmetöötlust EL siseturuvaldkonnas. Sellest lähtuvalt tuleks seaduses ette näha selged reeglid ning erandid, mis tagaks kriminaalmenetluses vajaliku andmekaitsetaseme, kuid samas arvestaks ka kriminaalmenetluse eripäradega.

PERSONAL DATA PROTECTION IN PRE-TRIAL CRIMINAL PROCEDURE IN ESTONIA

SUMMARY

Protection of personal data is inextricable part of the person´s fundamental right to privacy. A person is the owner of data concerning him or her and has the right of control over such data. Due to globalisation and development of new technologies personal data has acquired measurable value and changed data processing into everyone´s daily activity. Public and law enforcement authorities are generally allowed to interfere with one´s private life only when such interference is proportionate towards the aim of activities. However, continuous digitalisation of services has changed the possibilities of law enforcement authorities and gathering personal data became quicker and easier than ever before.

In this thesis the author analyzed data protection rules applicable in pre-trial criminal procedure in Estonia.

The author studied the concept of data protection within the context of relevant legislation. Though not the European Convention on Human Rights and Fundamental Freedoms nor Estonian Constitution refers to the right to data protection, though European Court of Human Rights and Supreme Court of Estonia has ascertained that the right to data protection constitutes a part of the right to privacy as set in Article 8 of the Convention and Article 26 of the Constitution accordingly. Hence, processing of personal data has to be carried out in accordance with principles and restrictions provided for in the Constitution. Article 11 of the Constitution allows circumscription of the right and freedoms only in accordance with the Constitution and the law and if such interference is necessary in the democratic society. In accordance with relevant case-law the latter condition should be interpreted as a principle of proportionality and therefore circumscription is permitted only when particular measure is necessary, moderate and relevant in regard to the aim pursued.

Criminal procedure is one of the main functions of the state targeting protection of rights and freedoms of individuals and ensuring security. Gathering of evidence is by far one of the main activities within criminal investigation and extensive processing of personal data is generally performed. Aims of criminal investigation are in legal collision with aims of data protection rules, therefore it is essential to strike a right balance between the right to data protection and fundamental interest that are protected through criminal investigation.

In Estonia, the basic principles of data processing in the context of criminal procedure are derived from the Convention and Constitution. It is worth noticing that although Personal Data Protection Act applies to criminal proceedings only under specifications provided by procedural law, the Code of Criminal Procedure does not include much in regard to the data protection.

Several basic principles of data protection are in place to ensure lawfulness of data processing. The author studied if and to what extend the principles and provisions of data privacy law apply in criminal procedure. In theory, since the Criminal Procedure Code does not limit the applicability of data processing principles laid down in the Personal Data Protection Act, those principles should be applied also to the data processed in context of criminal investigation. However, the author is of the opinion that due to the nature of criminal procedure, the need might arise to limit the applicability of basic principles. Author believes it would be beneficial to lay down general rules, principles and applicable limitations in the field of data protection in the Criminal Procedure Code.

Taking into account the amount of data processed in criminal procedure as well as interference with fundamental rights, specific provisions should be introduced to Criminal Procedure Code to allow individuals to exercise their rights while maintaining the interest of criminal procedure. It should also be clearly stated in the Criminal Procedure Code that an individual has the right to lodge a complaint with Data Protection Inspectorate also in regard to the data processed in the context of criminal procedure.

In addition to study on general data protection rules the author also analysed the issue of data protection in three specific situations – access of law enforcement authorities to telecommunication data, use of biometric data and international transfers of data. The author concluded that Estonian law is not clear nor ensure necessary protection of privacy in regard to telecommunication data retention. The applicable legislation should be changed and brought in line with the principle of proportionality, providing for clear conditions for access to such data by the law enforcement authorities and necessary limitations. In regard to biometric data, the author finds Estonian legislation to be satisfactory. On the international transfers, the authord finds that despite the fact that Estonia has implemented the EU Data Protection framework decision, the legislation in place is rather unclear and has several gaps. The author´s view is that the rules on international transfers should be aligned in the Criminal Procedure Code and the scope of such rules should be applicable to all international transfers and also provide clear guidance to the investigators in this regard.

In the beginning of this study the author established hypothesis that individuals´ data protection rights are not sufficiently guaranteed under Estonian law and interference with the right to privacy might not be proportionate. Author is of the opinion that hypothesis is confirmed. Under current legislation the Personal Data Protection Act applies also to criminal proceedings. The Personal Data Protection Act in turn refers to Criminal Procedure Code, though there are not many clear data protection rules. The application of Personal Data Protection Act is problematic mainly because it implemented into Estonian law the 1995 EU Data Protection directive, which is designed for the situations under EU single market concept. Author suggests to implement proper and clear rules and lawful limitations within the legislation, ensuring and balancing both data protection and criminal procedure.

KASUTATUD KIRJANDUS

1. Alexy, R. Põhiõigused Eesti põhiseaduses. – Juridica, 2001, eriväljaanne, lk 5-96
2. Alonso Blas, D. First and Third Pillar: Need for a Common Approach on Data Protection? - Gutwirth, S. jt (toim). Reinventing Data Protection? Springer Science+Business Media B.V., 2009, lk 225 - 237
3. Alonso Blas, D. Ensuring effective data protection in the field of police and judicial activities: some considerations to achieve security, justice and freedom. ERA Forum (2010) 11, lk 233–250
4. Boehm, F. Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Berlin: Springer - Verlag Berlin Heidelberg, 2012
5. A. F. V.d. Bussche, M.Stamm. Data Protection in Germany. München: Verlag C.H.Beck, 2013
6. Bygrave, L.A. Data Privacy Law: An International Perspective. Oxford Scholarship Online 2014
7. Bygrave, L.A. A Right to be Forgotten? - Communications of the ACM. 2015, vol 58, nr 1
8. Coudert, F., Dumortier, J., Kosta, E. Data Protection in the Third Pillar: In the Aftermath of the ECJ Decision on PNR Data and the Data Retention Directive. - International Review of Law, Computers & Technology, nr 3, 2007, lk 347-362
9. De Hert, P., Gutwirth, S. Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action. - Gutwirth, S. jt (toim). Reinventing Data Protection? Springer Science+Business Media B.V., 2009
10. De Hert, P., Papakonstantinou V. The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal mattes – A modest achievement however not the improvement some have hoped for. Computer Law and Security Review. 2009, 25, lk 403-414
11. Diggelmann, O., Wildhaber, L. Euroopa Inimõiguste konventsioon ja eraelu kaitse. Uuemad arengusuunad. – Juridica 2007 / 1, lk 3-15
12. Gomez-Barrosom J.-L., Feijóo-Gonzalez. Información personal: la nueva moneda de la economia digital. - El profesional de la información 2013 / 4, lk 290 - 297

13. Gonzalez Fuster, G., Gellert, R. The fundamental right of data protection in the European Union: in search of an uncharted right. International Review of Law, Computers and Technology, 2012/1, lk 73-82
14. Gutwirth, S. jt (toim). Reinventing Data Protection? Springer Science+Business Media B.V., 2009
15. Hijmans, H., Scirocco, A. Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty be Expected to Help? Common Law Market Review, 2009/46, lk 1485-1525
16. Ilus, T. Andmesubjekti osaluse põhimõte Euroopa Nõukogu konventsioonide ning Euroopa Inimõiguste Kohtu lahendite valguses. – Juridica 2005 / 8, lk 519 - 531
17. Johlen, H. Artikel 8 Grundrechtecharta. Kölner Gemeinschaftskommentar zur Europäichen Grundrechte-Charta. BeckVerlag, München, 2006, art 8/1 *ja* Simitis, "S. Bundesdatencshutzgezetz" commentary. NomosVerlag, Baden-Baden, 2006, lk 64 *nagu viidatud* Boehm, F. Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Springer Verlag, Berlin Heidelberg, 2012, lk 19-20
18. Kergandberg, E., Pikamäe, P. jt (toim). Kriminaalmenetluse seadustik. Komm vlj. Tallinn: Juura, 2012
19. Kergandberg, E., Sillaots, M. Kriminaalmenetlus. Tallinn: Juura 2006
20. Lindmäe, H. Menetlustaktika II. Tallinn: Juura, 1997.
21. Lõhmus, U. Põhiõigustest kriminaalmenetluses. 2. tr. Tallinn: Juura, 2014
22. Madise, Ü. jt (toim). Põhiseadus. Komm vlj. Tallinn: Juura, 2012
23. Mikli, S. Kui kauge Euroopa Liidu õigus saab järsku igapäevatöö osaks: probleeme Euroopa Liidu õiguse ülevõtmisel ja rakendamisel õiguskindluse põhimõtte kontekstis. - Juridica 2015 / 2, lk 103 - 112
24. Moreham, N.A. The right to respect for private life in the European Convention on Human Rights: a re-examination. European Human Rights Law Review, 2008/1, lk 44-79
25. Murphy, E. Databases, Doctrine and Criminal Procedure. Fordham Urban Law Journal, nr 37, 2010, lk 803-836
26. Owen, D. Politseilabor. Kuidas teaduslik kohtuekspertiis aitab leida kurjategijaid. Tallinn: Koolibri, 2005

27. Rodota, S. Data Protection as a Fundamental Right. - Gutwirth, S. jt (toim). Reinventing Data Protection? Springer Science+Business Media B.V., 2009, lk 79
28. V. Saarmets. Konstitutsioonilistest seadustest. – Õiguskeel 2009 / 4, lk 1 – 23. Arvutivõrgus: http://www.just.ee/sites/www.just.ee/files/virgo_saarmets._konstitutsioonilistest_seadustest.pdf (04.05.2015)

29. Solove D.J. The Digital Person: Technology and Privacy in the Information Age. New York University Press 2004, New York. Lk 14 *nagu viidatud* Murpy, E. Databases, Doctrine and Criminal Procedure. Fordham Urban Law Journal, nr 37, 2010, lk 803-836
30. Talvik, E. Legaalsuse põhimõte Eesti Vabariigi põhiseaduse tekkimises, muutmises ja muutmiskavades. Tartu 1991, lk 12 jj *nagu viidatud* Merusk, K., Annus, T., Ernits, M. jt. PS-i § 3 /2

Eesti õigusaktid

1. Advokatuuriseadus. – RT I 2001, 36, 201 … RT I, 21.06.2014, 50
2. Avaliku teabe seadus. – RT I 2000, 92, 597… RT I, 12.07.2014
3. Eesti Vabariigi Põhiseadus. - RT 1992, 26, 349 … RT I, 27.04.2011, 2
4. Inimgeeniuuringute seadus. - RT I 2000, 104, 685 ... RT I, 14.03.2014, 30
5. Isikuandmete kaitse seadus. - RT I 2007, 24, 127 ... RT I, 12.07.2014, 51
6. Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni ratifitseerimise seadus. - RT II 2001, 1, 3
7. Isikut tõendavate dokumentide seadus. - RT I 1999, 25, 365 ... RT I, 23.03.2015, 16
1. Karistusregistri seadus. – RT I, 21.03.2011 … RT I, 05.12.2014, 15
2. Karistusseadustik. – RT I 2001, 61, 364 … RT I, 23.12.2014, 16
3. Kohtutäituri seadus. – RT I 2009, 68, 463 … RT I, 05.03.2015, 3
4. Korrakaitseseadus. – RT I, 22.03.2011, 4 … RT I, 31.12.2014, 28
5. Krediidiasutuste seadus. – RT I, 1999, 23, 349 … RT I, 19.03.2015, 41
6. Kriminaalmenetluse seadustik. - RT I 2003, 27, 166 ... RT I, 19.03.2015, 21
7. Kriminaalmenetluse seadustik. – RT I 2003, 27, 166 … RT I, 16.11.2012, 17.
8. Politsei ja piirivalve seadus. - RT I 2009, 26, 159 … RT I, 26.03.2013, 12
9. Prokuratuuriseadus. – RT I 1998, 41, 625 … RT I, 10.03.2015, 17

10. Psühhiaatrilise abi seadus. – RT I 1997, 16, 260 … RT I, 15.06.2012, 6
11. Riigisaladuse ja salastatud välisteabe seadus. - RT I 2007, 16, 77 … RT I, 22.12.24
12. Vabariigi Valitsuse 30.07.2004.a määrus nr 261 "Kriminaaltoimiku arhiivimise kord ja säilitamise tähtajad". - RT I 2004, 60, 261 ... RTI , 02.09.2011, 5
13. Välismaalasele rahvusvahelise kaitse andmise seadus. - RT I 2006, 2, 3 ... RT I, 23.03.2015, 25
14. Välismaalaste seadus. - RT I 2010, 3, 4 ... RT I, 23.03.2015, 7

Euroopa Liidu, rahvusvahelised ja välisriikide õigusaktid

15. Convention for the Protection of Individuals with regard to Automated Processing of Personal Data, Strasbourg 28.01.1981. Arvutivõrgus: http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm
16. Euroopa Liidu leping. – ELT C 115 / 09.05.2008, lk 13-45
17. Euroopa Liidu Põhiõiguste Harta, ELT C 83/ 30.03.2010, lk 389-403
18. Euroopa Parlamendi ja nõukogu direktiiv 95/46/EÜ, 24.10 1995, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. ELT L 281 / 23.11.1995, lk 31 – 50
19. Euroopa Parlamendi ja Nõukogu direktiiv, 2006/24/EÜ, 15. märts 2006, mis käsitleb üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist ja millega muudetakse direktiivi 2002/58/EÜ. ELTL 105 / 13.04.2006, lk 54-63
20. Euroopa Nõukogu Parlamentaarse Assamblee resolutsioon 428 (1970) "Declaration on mass communication media and Human Rights". Arvutivõrgus: http://assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewPDF.asp?FileID=15842&lang=en (25.04.2015)
21. Inimõiguste ja põhivabaduste kaitse konventsioon. - RT II 2000, 11, 57
22. Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon. - RT II 2001, 1, 3
23. Konventsioon, 14.05.1985, millega rakendatakse 14.06.1985.a Schengeni lepingut Beneluxi Majandusliiku riikide, Saksamaa Liitvabariigi ja Prantsuse Vabariigi

valitsuste vahel nende ühispiiridel kontrolli järkjärgulise kaotamise kohta. ELT L 239, 22.09.2000, lk 19 - 62.
24. Nõukogu otsus, 28.02.2002, millega moodustatakse Eurojust, et tugevdada võitlust raskete kuritegude vastu (2002/187/JSK). ELT L 63/06.03.2002, lk 1 – 13
25. Nõukogu otsus, 2007/533/JSK, 12.06.2007, mis käsitleb teise põlvkonna Schengeni Infosüsteemi (SIS II) loomist, toimimist ja kasutamist. – ELT L 205/ 07.08.2007, lk 63 – 84
26. Nõukogu otsus, 2008/615/JSK, 23.06.2008, piiriülese koostöö tõhustamise kohta, eelkõige seoses terrorismi- ja piiriülese kuritegevuse vastase võitlusega. - ELT L 06.08.2008/210, lk 1 - 11.
27. Nõukogu otsus, 2008/616/JSK, 23.06.2008, millega rakendatakse otsust 2008/615/JSK piiriülese koostöö tõhustamise kohta, eelkõige seoses terrorismi- ja piiriülese kuritegevuse vastase võitlusega. - ELT L 06.08.2008/210, lk 12 - 17
28. Nõukogu otsus, 06.04.2009, millega asutatakse Euroopa Politseiamet (Europol) (2009/371/JSK). ELT L 121/15.05.2009, lk 37-66
29. Nõukogu raamotsus 2006/960/JSK, 18.12.2006, Euroopa Liidu liikmesriikide õiguskaitseasutuste vahelise teabe ja jälitusteabe vahetamise lihtsustamise kohta. - ELT L 29.12.2006/368, lk 89 - 100
30. Nõukogu raamotsus 2008/977/JSK, 27.11.2008, kriminaalasjades tehtava politsei- ja õigusalase koostöö raames töödeldavate isikuandmete kaitse kohta. ELT L 350 / 30.12.2008, lk 60 – 71
31. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Arvutivõrgus: http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (04.05.2015)
32. Recommendation No R (87) 15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector. Arvutivõrgus: https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2196553&SecMode=1&DocId=694350&Usage=2 (05.04.2015)

Kohtuotsused

33. Austria Konstitutsioonikohtu 27.06.2014.a otsus kohtuasjades G 47/2012-49, G 59/2012-38, G 62/2012-46, G 70/2012-40, G 71/2012-36. Arvutivõrgus: https://www.vfgh.gv.at/cms/vfgh-site/attachments/1/5/8/CH0006/CMS1409900579500/erwaegungeneng28082014.pdf (kohtuotsuse inglisekeelne kokkuvõte; 05.04.2015). http://www.ris.bka.gv.at/Dokumente/Vfgh/JFT_20140627_12G00047_00/JFT_20140627_12G00047_00.pdf (terve kohtuotsus saksa keeles; 05.04.2015)
34. EIKo 06.09.1978, 5029, *Klass vs* Saksamaa
35. EIKo 08.08.1984, 8691/79, *Malone vs* Ühendkuningriik
36. EIKo 26.03.1987, 9248/81, *Leander vs* Sweden
37. EIKo 07.07.1989, 10454, *Gaskin vs* Ühendkuningriik
38. EIKo 25.02.1997, 22009/93, *Z vs* Soome
39. EIKo 27.08.1997, 20837/92, *M.S. vs* Rootsi
40. EIKo 16.02.2000, 27798/95, *Amann vs* Šveits
41. EIKo 04.05.2000, 2834/92, *Rotaru vs* Rumeenia
42. EIKo 03.04.2007, 6261/00, *Copland vs* Ühendkuningriik
43. EIKo 12.02.2009, 2512/04, *Nolan* ja *K vs* Russia
44. EIKo 04.12.2008, 30562/04 ja 30566/04, *S* ja *Marper vs* Ühendkuningriik
45. EIKo 18.05.2010, 26839/05, *Kennedy vs* Ühendkuningriik
46. EIK 13.11.2012, 24029/07, *M.M. vs* Ühendkuningriik
47. EKo 30.06.2006, liidetud kohtuasi C-317/04 ja C-318/04, Euroopa Parlament vs nõukogu ja komisjon
48. EKo 20.05.2003, kohtuasi C-465/00, *Rechnungshof vs Österreichischer Rundfunk* ja teised
49. EKo 06.11.2003.a, C-101/01, Rootsi *vs* Lindqvist
50. EKo 10.02.2009, C-301/06 Iirimaa *vs* Parlament ja Nõukogu
51. EKo 07.05.2009, kohtuasi C-553/07 College van burgemeester en wethouders van Rotterdam vs M. E. E. Rijkeboer
52. EKo 09.03.2010, kohtuasi C-518/07 Euroopa Komisjon *vs* Saksamaa Liitvabariik.
53. EKo 24.11.2011.a, C-70/10, Scarlet Extended SA *vs* **S**ociété belge de sauteurs, compositeurs et éditeurs SCRL (SABAM)
54. EKo 8.04.2014, liidetud kohtuasjad C-293/12 Digital Rights Ireland Ltd vs Minister for Communications, Marine and Natural Resources ja teised ja C-594/12 Kärntner Landesregierung ja teised

55. EKo 13.05.2014, kohtuasi C-131/12, Google Spain SL, Google Inc. vs Agencia Española de Protección de Datos (AEPD), Mario Costeja González
56. Haagi kohtu 11.03.2015.a otsus nr C/09/480009/KGZA14/1575. Arvutivõrgus: http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2015:2498 (25.04.2015)
57. RKHKo 3-3-1-3-12, 12.06.2012
58. RKHKo 3-3-1-42-08, 20.10.2008
59. RKKKo 3-1-1-19-05, 18.04.2005
60. RKKKo 3-1-1-116-10, 10.03.2011
61. RKKKo 3-1-1-31-11, 28.04.2011
62. RKKKo 23.02.2015, 3-1-1-51-14
63. RKPJKo 3-4-1-3-97, 06.10.1997
64. RKPJKo 3-4-1-1-98, 05.02.1998
65. RKPJKo 3-4-1-5-05, 13.06.2005
66. RKPJKo 3-4-1-16-08, 26.03.2009
67. RKPJKo 3-4-1-54-15, 27.02.2015
68. RKTKo 3-2-1-83-10, 26.11.2010
69. RKÜKo 3-1-1-86-07, 16.05.2008
70. Rumeenia konstitutsioonikohtu 08.07.2014.a otsus nr 440. Arvutivõrgus: http://privacy.apti.ro/decizia-curtii-constitutionale-date-trafic/ (25.04.2015). Saksa Konstitutsioonikohtu 02.03.2010.a otsus kohtuasjades 1 BvR 256/08, 1 BvR 263/08 ning 1 BvR 263/08 Arvutivõrgus: http://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2010/bvg10-011.html;jsessionid=3ED96B75BBF41C49EB668A862157530D.2_cid361 (kohtuotsuse inglisekeelne kokkuvõte; 25.04.2015) http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2010/03/rs20100302_1bvr025608.html;jsessionid=C06B254E3D18C0837807FEF6319183CA.2_cid393 (kohtuotsus saksa keeles; 25.04.2015)

Muud materjalid

71. Act on the Processing of Personal Data by the Police (761/2003; 523/2004). Finlex. Arvutivõrgus: /fi/laki/kaannokset/2003/en20030761.pdf (04.05.2015)

72. J. Antonova. Lennureisijate broneeringuinfo kasutamine õiguskaitse eesmärkidel Eestis. Bakalaureusetöö. Tallinn: Tartu Ülikool, 2013.

73. Article 29 Data Protection Working Party. Opinion 01/2013 providing further input into the discussions on the draft Police and Criminal Justice Data Protection Directive. Arvutivõrgus: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp201_en.pdf (04.05.2015).

74. Article 29 Working Party. 20.04.2011. Advice paper on special categories of data ("sensitive data"). Arvutivõrgus: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf (04.05.2015).

75. Article 29 Data Protection Working Party, 20.06.2007, Opinion 4/2007 on the concept of personal data, lk 6-7. Arvutivõrgus: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf (04.05.2015).

76. Data Protection. Compilation of Council of Europe texts. Directorate General of Human Rights and Legal Affairs. Strasbourg. Council of Europe, 2010

77. Euroopa Nõukogu Ministrite Komitee soovituse (87) 15 seletuskiri. Arvutivõrgus: https://wcd.coe.int/ViewDoc.jsp?id=704861&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383 (04.05.2015)

78. European Commission, 25.01.2012. Commission Staff Working Document. Annex accompanying the document. Report from the Commission to the European Parliament, the Council, the European and Economic and Social Committee and the Committee of the Regions based on Article 29 (2) of the Council Framework Decision of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal mattes, SEC(2012)75. Arvutivõrgus: http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_75_en.pdf (04.05.2015)

79. Euroopa Komisjon, 25.01.2012, COM (2012) 10 lõplik. Ettepanek: Euroopa Parlamendi ja Nõukogu direktiiv üksikisikute kaitse kohta seoses pädevates asutustes isikuandmete töötlemisega kuritegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumise kohta. Arvutivõrgus: http://eur-

lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:ET:PDF (04.05.2015)
80. Euroopa Komisjon, 25.01.2012. Ettepanek: Euroopa Parlamendi ja nõukogu määrus üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (isikuandmete kaitse üldmäärus), KOM (2012) 11 lõplik. Arvutivõrgus: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_et.pdf (04.05.2015)
81. Euroopa Komisjon, 25.01.2015, COM (2012) 12 final. Komisjoni aruanne Euroopa Parlamendile, Nõukogule, Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele nõukogu 27. novembri 2008. aasta raamotsuse (kriminaalasjades tehtava politsei- ja õigusalase koostöö raames töödeldavate isikuandmete kaitse kohta) artikli 29 lõike 2 alusel. Arvutivõrgus: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0012:FIN:ET:PDF (04.05.2015)
82. Euroopa Komisjoni veebileht: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm (04.05.2015)
83. Euroopa Vabakaubandusorganisatsiooni veebileht: http://www.efta.int/eea/eea-agreement (04.05.2015)
84. Euroopa Ülemkogu 15. ja 16.10.1999.a Tamperes toimunud kohtumise järeldused. Arvutivõrgus: http://www.europarl.europa.eu/summits/tam_en.htm (04.05.2015)
85. Federal Data Protection Law. – Federal Law Gazette I p 66, 14.01.2003 … Federal Law Gazette I, p 2814, 01.08.2009. Arvutivõrgus: http://www.gesetze-im-internet.de/englisch_bdsg/ (04.05.2015)
86. Gezetz über die Bundespolizei. – BGBI 19.10.1994 … 20.06.2013. Arvutivõrgus: https://www.google.ee/webhp?sourceid=chrome-instant&rlz=1C1CHWA_enBE617BE617&ion=1&espv=2&ie=UTF-8#q=BGBI (04.05.2015)
87. Handbook on European Data Protection Law. European Union Agency for Fundamental. Council of Europe. Luxembourg: Publications Office of the European Union. 2014. Arvutivõrgus: http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf (04.05.2015)
88. Hansen, T. Õigus eraelu puutumatusele *vs* kohtulahendi avalikustamine. Magistritöö. Tartu: 2012
89. P. Hustinx. EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation. Avaldatud kõne, 2014, lk 9.

Arvutivõrgus: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2014/14-09-15_Article_EUI_EN.pdf (04.05.2015).

90. Isikuandmete kaitse seaduse seletuskiri. Arvutivõrgus: http://www.aki.ee/et/eraelu-kaitse/oigusaktid (04.05.2015)
91. Kohtuekspertiisiseaduse ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu seletuskiri. Kättesaadav: http://www.riigikogu.ee/?op=ems&page=eelnou&eid=a1404746-e1ec-4720-87a8-0f1550237bea& (04.05.2015)
92. Kriminaalmenetluse seadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu 599 SE seletuskiri. Arvutivõrgus: http://www.riigikogu.ee/tegevus/eelnoud/eelnou/ab9521d9-5558-45b8-c93a-b5122208c53b/Kriminaalmenetluse-seadustiku-muutmise-ja-sellega-seonduvalt-teiste-seaduste-muutmise-seadus/ (04.05.2015)
93. Kriminaalmenetluse seadustiku muutmise ja sellega seonduvate teiste seaduste muutmise seaduse (175 SE) seletuskiri. Arvutivõrgus: http://www.riigikogu.ee/tegevus/eelnoud/eelnou/86dde8ff-c50e-48ba-a39e-a325fe15a3f0/Kriminaalmenetluse-seadustiku-muutmise-ja-sellega-seonduvalt-teiste-seaduste-muutmise-seadus/ (04.05.2015)
94. Kriminaalmenetluse seadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse SE 578 seletuskiri. Arvutivõrgus: http://www.riigikogu.ee/tegevus/eelnoud/eelnou/5ebd76d0-c075-4845-89b0-c6b23cca607f/Kriminaalmenetluse-seadustiku-ja-sellega-seonduvalt-teiste-seaduste-muutmise-seadus/ (04.05.2015)
95. National security and European Case Law. European Court of Human Rights. Research Division. Council of Europe / European Court of Human Rights, 2013. Arvutivõrgus: http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/Jurisprudence%20CEDH_En%20%28final%29.pdf (04.05.2015)
96. NSA slides explain the PRISM data-collection program. - Washington Post, 10.07.2013.a Arvutivõrgus: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ (04.05.2015)
97. OECD. Report on the enforcement of cross-border privacy laws. 2006, lk 3. Kättesaadav: http://www.oecd.org/internet/ieconomy/37558845.pdf (04.05.2015)

98. Personal Data Protection Law. - Latvijas Vēstensis 23.03.2000 … 06.02.2014. Arvutivõrgus: http://www.dvi.gov.lv/en/legal-acts (04.05.2015)

99. Proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data - Chapters I, II and V. Nõukogu dokument nr ST15659/15 REV 1, 19.11.2014.. Arvutivõrgus: http://data.consilium.europa.eu/doc/document/ST-15659-2014-REV-1/en/pdf (04.05.2015)

100. Seletuskiri Vabariigi Valitsuse istungi päevakorrapunkti „Eesti seisukohad Euroopa Parlamendi ja nõukogu määruse üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (isikuandmete kaitse üldmäärus)“ ja Euroopa Parlamendi ja nõukogu direktiivi üksikisikute kaitse kohta seoses pädevates asutustes isikuandmete töötlemisega kuritegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumise kohta, juurde. Arvutivõrgus: http://eelnoud.valitsus.ee/main#2HOqo0Qb (04.05.2015)

101. Soovituse (87) 15 seletuskiri. Arvutivõrgus: https://wcd.coe.int/ViewDoc.jsp?id=704861&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383 (04.05.2015)

102. Vabariigi Valitsuse määruse “Riikliku DNA-registri asutamine ja registri pidamise põhimäärus” eelnõu seletuskiri. Arvutivõrgus: http://eelnoud.valitsus.ee/main/mount/docList/fd85eddd-af0d-4a85-bdd3-7cf0937474ca?activity=2#fKlQws54 (04.05.2015)

103. Õiguskantsleri 18.02.2011.a kiri nr 7-4/101805/1100879 Riigikogu julgeoleku asutuste järelevalve komisjonile. Arvutivõrgus: http://oiguskantsler.ee/sites/default/files/old/File/OMBUDSMANI_MENETLUSED/Soovitused_oigusparasuse_ja_hea_halduse_tava_jargimiseks/2011/RK_julgeolekuasutuste_j_relevalve_erikomisjon_seisukoha_edastamine_Toomse.pdf (04.05.2015)

104. Õiguskantsleri kiri 15.07.2014.a kiri nr 6-1/140621/1403065. Arvutivõrgus: http://adr.rik.ee/jm/dokument/4042786 (04.05.2015)

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, Julia Antonova,

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

ISIKUANDMETE KAITSE KOHTUEELSES KRIMINAALMENETLUSES EESTIS,

mille juhendajad on Sandra Mikli ja Jaan Sootak,

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, **04.05.2015**