TARTU ÜLIKOOL
ÕIGUSTEADUSKOND
Avaliku õiguse osakond

Jenny Jakobson

ANDMESUBJEKTI ENDA KOHTA KÄIVATE ISIKUANDMETE JA NENDE TÖÖTLEMISE KOHTA KÄIVA TEABELE TUTVUMISE ÕIGUSE PIIRAMINE POLITSEI ANDMETÖÖTLUSES

Magistritöö

Juhendaja
Dr. Paloma Krõõt Tupay

Tallinn
2024

SISUKORD

SISSEJUHATUS

Ühiskonnal on ootus turvalisele elukeskkonnale. Riik saab tagada turvalisust enda tegevusega. Eesti Vabariigi põhiseaduse[1] (PS) § 13 lg 1 esimese lause kohaselt peab riik kaitsma inimese põhiõigust teisest inimesest lähtuva riive eest. Riik on näiteks kohustatud kaitsma igaühe õigust elule (PS § 16). Euroopa Liidu (EL) tasandil on EL põhiõiguste harta[2] (ELPH) art-s 6 tunnustanud igaühe õigust vabadusele ja turvalisusele. Õigus riigi kaitsele on mõistetav laiemalt isiklike õiguste ja vabaduste kaitsest. Nimelt Euroopa Kohtu tõlgendusest võib järeldada, et ELPH art 6 sätestab EL-i üldist huvi pakkuva eesmärgina õiguse riigi julgeolekule ja avalikule korrale[3].

Politsei- ja Piirivalveamet (PPA, edaspidi ka *politsei* või *andmetöötleja*) kogub ja töötleb andmeid. Veelgi enam, loob ülesannete täitmise käigus võimalikult palju seoseid ja vastavusi[4] andmete vahel, sest selliselt tekivad teadmised, mis toetavad turvalisuse tagamist, sealhulgas õigusrikkumise ennetamist või tõe väljaselgitamist süüteomenetluses[5]. Igast infosüsteemist, kuhu kogutakse ja kust otsitakse konkreetse inimese või eseme kohta andmeid, võib saada turvalisuse tagamiseks kasutatav infosüsteem[6]. Tõenäoliselt töötleb politsei igapäevaselt suurel hulgal, erineval viisil ja digitaalselt või muus vormis andmeid, millest suurem osa on kellegi isikuandmed.

Praktiliselt iga andmetöötluse toiming toob kaasa isikuandmete kaitse riive inimesele, kelle isikuandmeid politsei töötleb (edaspidi *andmesubjekt*). Andmetöötlejal tuleb läbi viia riive kontroll iga andmetöötluse toimingu eel. Isikuandmete kaitse kui põhiõiguse tagamiseks on ka andmesubjektil õigus kontrollida põhiõiguse riive seaduspärasust seoses ennast puudutava andmetöötlusega. Vastav õigus tuleneb ELPH art 8 lg 2 teise lause esimesest lauseosast ning PS § 44 lg 3 esimesest lausest ja lg-st 4.

---

[1] Eesti Vabariigi põhiseadus. – RT I, 15.05.2015, 2.
[2] Euroopa Liidu põhiõiguste harta. – ELT C 202, 07.06.2016, lk 389–405.
[3] EKo C-293/12, *Digital Rights Ireland Ltd* versus *Minister for Communications, Marine and Natural Resources jt ja Kärntner Landesregierung jt,* ECLI:EU:C:2014:238, p 42.
[4] Analoogia korras vt Rosentau, M. Infoühiskond ja tema vajadused. – Akadeemia 2015/3, lk 459, 471, 473–474, 485–486, 491–492.
[5] Analoogia korras vt Rosentau, M. Tõendamine teadmise standardmudelis. – Juridica 2001/III, lk 202.
[6] De Hert, P., Sajfert, J. Chapter 15: Police, privacy and data protection from a comparative legal perspective. – Den Boer, M. (ed.). Comparative Policing from a Legal Perspective. 2018. – https://doi.org/10.4337/9781785369117 (05.03.2024), lk 322.

Andmesubjekti õiguse teostamine on reguleeritud EL-i teiseses õiguses, millest magistritöös on asjakohane õiguskaitseasutuste direktiiv[7] (ÕKAD). ÕKAD sätestab normid politsei poolt isikuandmete töötlemisele süüteo tõkestamisel, avastamisel ja menetlemisel ning karistuse täideviimisel (edaspidi koos ka *õiguskaitse eesmärk*). Eesti on üle võtnud ÕKAD-i isikuandmete kaitse seadusega[8] (IKS). Sellest tulenevalt peab IKS-iga võimaldama andmesubjektile juurdepääsu ja andmetöötluse kontrolli ehk tutvumise isikuandmetega ja nende töötlemist puudutava teabega vahetult ja kaudselt.

Andmesubjektil on õigus pöörduda taotlusega PPA poole IKS § 24 lg 1 alusel. Kui PPA töötleb andmesubjekti andmeid, siis on põhimõtteliselt õigus saada juurdepääs kõigile enda kohta käivatele isikuandmetele ja kogu nende töötlemise kohta käivale teabele. See puudutab tutvumist andmetega, mille andmesubjekt on ise politseile esitanud või muid andmeid, mille töötlemisest ta on teadlik ning andmetöötlust ja andmeid, mille pärimisest ja vahetamisest riigisiseselt või rahvusvahelise koostöö raames ei ole andmesubjekt teadlik. Samuti puudutab see kõiki korrastatud andmete kogumeid, mitte üksnes andmetöötlust teadaolevalt 26 PPA-s kasutusel olevas infosüsteemis.[9] Seda tutvumise viisi tähistatakse teaduskirjanduses ja magistritöös terminiga „vahetu juurdepääsuõigus“, kuna juurdepääsu taotleb andmesubjekt andmetöötlejalt ja tema otsustab juurdepääsu andmise üle.

Andmesubjekt ei pruugi saada tervikpilti ennast puudutavast andmetöötlusest, sest tutvumise õigus ei ole absoluutne. Põhiõigust isikuandmetega tutvumisele on politseil võimalik piirata IKS § 24 lg 2 kohaselt seaduses sätestatud juhtudel. Üldiselt võib selline vajadus olla näiteks siis, kui isikuandmete tutvustamine võib kahjustada teise inimese õigusi ja vabadusi, süüteo tõkestamist või kriminaalmenetlust. Andmesubjekt ei pruugi saada üldse teavet enda kohta, sest IKS § 24 lg 3 teine lause võimaldab isegi juhul, kui politsei töötleb andmeid, mitte kinnitada ega eitada andmetöötluse olemasolu.

Andmesubjekti tutvumise õiguse piiramise korral on tal õigus pöörduda Andmekaitse Inspektsiooni (AKI, edaspidi ka *järelevalveasutus*) ja vaidlustada vastav politsei otsus. AKI kontrollib andmesubjekti põhiõiguse riive seaduspärasust ja otsustab andmesubjekti

[7] Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/680, 27. aprill 2016, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK. – ELT L 119, 04.05.2016, lk 89–131.
[8] Isikuandmete kaitse seadus. – RT I, 11.03.2023, 11.
[9] Vt otsing Eesti riigi infosüsteemi haldussüsteemi (RIHA) infosüsteemide kataloogist märksõnaga „Politsei- ja Piirivalveamet“. – https://www.riha.ee/Infosüsteemid?searchText=politsei- ja piirivalveamet&sort=meta.update_timestamp&dir=DESC (05.03.2024).

juurdepääsuõiguse üle. Sellist tutvumise viisi tähistatakse teaduskirjanduses ja magistritöös terminiga „kaudne juurdepääsuõigus“.

Autorile on huvipakkuv analüüsida, kuidas kehtiv õigus näeb ette andmesubjekti tutvumise õiguse koostoimes politsei võimaliku vajadusega piirata andmetöötlusega tutvumist. Arusaam õigusnormidest võimaldab hinnata nende rakendatavust praktikas, et tagada isikuandmetega tutvumist taotleva kui ka muude andmetöötluses osalevate andmesubjektide õiguste tõhus kaitse. Kõneallolevalt on oluline luua selgus IKS-is sätestatust ja selle kooskõlast EL-i õigusega. IKS-i analüüs on ajakriitiline. Euroopa Komisjonile TIPIK-i poolt esitatud õigusliku analüüsi kohaselt ei ole Eesti üle võtnud kõiki vahetu juurdepääsuõiguse elemente.[10] Sama analüüsi kohaselt pole seadusandja sätestanud vastavuses ÕKAD-iga ka kaudset juurdepääsuõigust.[11] Selle võrra tähelepanuväärsemad on mitmed hiljutised ÕKAD-i tõlgendused. Muu hulgas 2024. a jaanuarikuus avaldatud ÕKAD-i kommenteeritud väljaandes.[12] Samuti, vähese ÕKAD-it puudutava kohtupraktika tõttu Euroopa Kohtu 2023. a novembrikuus avaldatud otsuses kaudse juurdepääsuõiguse teostamise kohta.[13] Kui andmesubjekti tutvumise õiguse regulatsioon IKS-is ei ole kooskõlas EL-i õiguse põhimõtetega, võib see kaasa tuua ebakorrektse andmesubjekti taotluse lahendamise nii PPA-s kui AKI-s.

Magistritöös analüüsib autor IKS §-is 24 sätestatud andmesubjekti õigust saada teavet ja tutvuda enda kohta käivate isikuandmetega. Keskne probleem on uurida, kas andmesubjekti juurdepääsuõiguse ja selle piiramise regulatsioon IKS-is on kooskõlas ÕKAD-i art 14, 15 ja 17. Magistritöö eesmärk on kujundada arusaam, kas politsei kaalutlusruum võib olla liiga lai, võimaldades piirata ülemääraselt andmesubjekti tutvumise õigust.

Magistritöö probleemist ja eesmärgist tulenevalt on esitatud järgmised uurimisküsimused:

- kuidas on reguleeritud andmesubjekti õigus teabele ja vahetu juurdepääsuõigus;
- kuidas on reguleeritud andmesubjekti vahetu juurdepääsuõiguse piiramine ning
- kuidas on reguleeritud andmesubjekti kaudne juurdepääsuõigus.

[10] TIPIK 2020: TIPIK Legal, "Report on the Transposition of Directive (EU) 2016/680", Report for the European Commisson, November 2020, p 15 (viidatud märkus 25. Dimitrova, D., LED Article 14/B.3). – Kosta, E. (ed. et al.). The EU Law Enforcement Directive (LED). A Commentary. Oxford University Press 2024 (edaspidi *Commentary*). – https://doi.org/10.1177/20322844231214484 (31.03.2024).
[11] Samas, p 18 (viidatud märkus 34. Franssen, V., Corhay, M., LED Article 17/B.3. Commentary).
[12] *Commentary*.
[13] EKo C-333/22, *Ligue des droits humains ASBL, BA* versus *Organe de contrôle de l'information policière*, ECLI:EU:C:2023:874.

Magistritöö koosneb neljast peatükist. Alustuseks analüüsitakse vahetu juurdepääsuõiguse teostamise tingimusi. Kvalitatiivse ja võrdleva meetodi abil uuritakse IKS-i kohaldumisala, sealhulgas kriminaalmenetluses ning andmesubjekti teavitamise ja tema taotlusele vastamise regulatsiooni. Seejärel analüüsitakse vahetu juurdepääsuõiguse teostamist. Kvalitatiivse ja võrdleva meetodi abil uuritakse isikuandmete ja nende töötlemise kohta käiva teabe, sealhulgas automatiseeritud otsuse tutvustamise regulatsioone. Siinkohal on liigutud vahetu juurdepääsuõiguse piiramise tingimuste analüüsini. Kvalitatiivse ja võrdleva meetodi abil uuritakse piiramise aluste ja nende kohaldamise regulatsiooni. Muu hulgas uuritakse andmesubjekti isiku tuvastamise nõuet tutvumise piiramise võimaliku uue alusena. Lõpetuseks analüüsitakse kaudse juurdepääsuõiguse teostamise tingimusi. Kvalitatiivse ja võrdleva meetodi abil uuritakse andmekaitse järelevalveasutuse võimalust kontrollida tutvumise õiguse piiramise seaduslikkust.

Magistritöös esitatud analüüs[14] põhineb õigusaktidel ja eelnõude juures olevatel seletuskirjadel või õigusaktide kommenteeritud väljaannetel ja kohaldamise aruannetel, teaduskirjandusel, EL-i andmekaitse nõuande- ja järelevalveasutuste juhenditel ning Eesti ja Euroopa kohtupraktikal. Samuti on uurimuses kasutatuid muid allikaid, mis toetavad uurimisküsimustele vastamist. Analüüsi aluseks on analoogia korras EL-i teisese andmekaitseõiguse tõlgendused, kuna IKS-i või tema rakendusseaduste kohta ei ole sageli asjakohast teaduskirjandust või kohtupraktikat.

Magistritöö märksõnad[15] on põhiõigused, andmekaitse, politsei, kuriteod.

[14] Autor väljendab magistritöös isiklikke hetketeadmisest ja -olukorrast lähtuvaid seisukohti, mis ei ole omistatavad asutusele, mille teenistuja autor käesoleval hetkel on ega ole talle siduvad tema edasises tegevuses.
[15] Eesti märksõnastik. – https://ems.elnet.ee/index.php (07.04.2024).

1. ANDMESUBJEKTI VAHETU JUURDEPÄÄSUÕIGUSE TEOSTAMINE

1.1. Isikuandmete kaitse seaduse kohaldamisala

Andmesubjekti tutvumise õiguse teostamisel kohaldab politsei IKS-i, kui töötleb isikuandmeid õiguskaitse eesmärgil. Politsei ülesandest sõltuvalt võib andmesubjekti tutvumise õiguse aluseks olla vahetult kohalduv isikuandmete kaitse üldmäärus[16] (IKÜM), valdkondlik vahetu õigusmõjuga EL-i või riigisisene õigusakt. Vaja on seega piiritleda andmetöötluse üleminek IKS-i kohaldamise etapist muusse etappi või vastupidi muust etapist IKS-i kohaldamise etappi. IKS-i määratlemisel õigusliku alusena kaasneb põhiõiguse intensiivsema riive võimalus. Põhjendamatult ei saa kasutada andmesubjekti juurdepääsuõiguse piiramise alusena IKS-i regulatsiooni. Eelkirjeldatu tõttu analüüsib autor vahetu juurdepääsuõiguse teostamise aluses selguse saamiseks IKS-i kohaldamisala.

IKS-is on andmesubjekti õiguste regulatsioon sätestatud 4. peatüki 3. jaos (edaspidi ka *4. peatükk*). Tegemist on erinormidega IKÜM-i 3. peatüki 1. jaos sätestatud andmesubjekti õiguste normide suhtes (ÕKAD art 1 lg 1 koosmõjus põhjendusega 10). Andmesubjekt saab tutvumise õigust teostada IKS §-i 24 alusel üksnes teatud politsei andmetöötluse suhtes. Selliseks andmetöötluseks on isikuandmete töötlemine ja „vaba liikumine“ eriomaselt „süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuse täitmisele pööramise eesmärgil, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmisel ja nende ennetamisel“ (ÕKAD art 1 lg 1).

ÕKAD-iga on art 1 lg 1 koosmõjus põhjendusega 12 ja 27 hõlmatud olukorrad, kus karistusseadustiku (KarS)[17] § 2 lg 2 tähenduses süüteo koosseisutunnuste esinemine pole veel teada, ohud turvalisusele võivad viia süüteo toimepanemiseni või on vaja analüüsida konkreetse süüteoga seoses toimunud tegevuste käigus saadud isikuandmeid laiemalt ja omavahel seostatuna. Eesti seadusandja on näinud ette IKS-i 4. peatüki kohaldamiseks kitsenduse, sest IKS § 12 lg 2 kohaselt pole kohaldamisalas andmetöötlus korrakaitseseaduse[18] (KorS) § 2 lg 4 tähenduses riikliku järelevalve teostamisel. Erinevalt ÕKAD-iga võimaldatust peab politsei isikuandmete töötlemisel riikliku järelevalve menetluses ja süüteoennetuses kohaldama KorS § 1 lg 1^1 alusel IKÜM-i.

[16] Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (EMPs kohaldatav tekst). – ELT L 119, 04.05.2016, lk 1–88.
[17] Karistusseadustik. – RT I, 06.08.2022, 27.
[18] Korrakaitseseadus. – RT I, 14.03.2023, 29.

Politseil on alus kohaldada andmesubjekti õiguste regulatsiooni IKS-i kohaselt kahe tingimuse kumulatiivsel täitmisel:

1) materiaalse kohaldamisala tõttu peab olema eesmärgiks isikuandmete töötlemine IKS § 12 lg 1 tähenduses süüteo tõkestamisel, avastamisel ja menetlemisel ning karistuse täideviimisel, arvestades, et süüteo uurimine ja selle eest vastutusele võtmine on hõlmatud menetlemise terminiga (õiguskaitse eesmärk) ja
2) isikulise kohaldamisala tõttu peab kehtima IKS § 13 lg 2 kohaselt kriminaalmenetluse seadustiku[19] (KrMS) tähenduses uurimisasutuse[20] või väärteomenetluse seadustiku[21] (VTMS) kohtuvälise menetleja[22] pädevus (edaspidi ka *õiguskaitseasutus*).[23]

IKS-is kasutatud terminil „süüteo tõkestamine“ puudub Eesti õiguses kõikehõlmav legaaldefinitsioon.[24] Samas on vaja piiritleda algusetapp, millest alates kohaldub IKS. Siinkohal on oluline eristada politsei ülesande eesmärk. Sarnaselt, nagu eristatakse karistusmenetluse repressiivset eesmärki riikliku järelevalve menetluse preventiivsest eesmärgist (ohu tõrjumine avalikule korrale) ning vastavaid eesmärgi saavutamiseks kasutatavaid meetmeid.[25] KorS-i selestuskirja kohaselt järeldab autor, et üldjuhul kohaldub IKÜM süüteo „planeerimise ja ettevalmistamise staadiumis“[26]. N. Parresti ja M. Juha selgituse järgi, kui avastatakse ohu ennetamise ja väljaselgitamise käigus rikkumine, siis seoses sellega alustatud süüteomenetlusest kohaldub andmetöötlusele IKS-i 4. peatükk[27]. Autori hinnangul võib üldise arusaama järgi pidada IKS 4. peatüki kohaldamise konkreetsemaks lävendiks süüteokahtluse olemasolu.[28] Kui uurimise käigus tuvastatakse KrMS § 194 kohaselt kuriteole viitav teave, olemas on vähemalt põhjendatud kahtlus kuriteo toimepanemises, tekib kriminaalmenetluse alustamise ajend, alustab politsei kriminaalmenetlust ning teabe kogumine loetakse uurimis- või menetlustoiminguks, nagu ka järgnevad tõendite kogumiseks vajalikud toimingud ja andmetöötlus. Selliselt on andmetöötlus hõlmatud IKS 4. peatüki regulatsiooniga.

---

[19] Kriminaalmenetluse seadustik. – RT I, 06.07.2023, 49.
[20] KrMS § 31 lg 1 tähenduses teiste seas PPA; vt ka KrMS § 15^2 lg 6 menetlejate kaasvastutuse kohta.
[21] Väärteomenetluse seadustik. – RT I, 22.03.2024, 10.
[22] VTMS § 9 tähenduses muu hulgas PPA.
[23] Täpsemalt kohaldamisala kohta vt Isikuandmete kaitse seaduse 679 SE seletuskiri. – https://www.riigikogu.ee/download/b7c9371a-7768-46b5-9d33-9eb4e3b98125 (13.04.2024), § 11 lk 19–21.
[24] Vrd terminite kasutust ÕKAD-i p 12, 27 ja 35 ning PPVS § 3 lg-s 1; Isikuandmete kaitse seaduse 679 SE seletuskiri, § 11 lk 19–21.
[25] Korrakaitseseaduse SE 49 seletuskiri. – https://www.riigikogu.ee/download/a67e1f77-6a73-26c5-5648-71b05c92d979 (13.04.2024), § 1 lk 11.
[26] Samas, § 1 lk 10–11.
[27] Parrest, N., Juha, M. Arutama hakatakse andmesubjekti kaebust kohustamaks maakohut väljastama teavet andmesubjekti isikuandmete töötlemise kohta. Kohtute aastaraamat 2020. – https://aastaraamat.riigikohus.ee/arutama-hakatakse-andmesubjekti-kaebust-kohustamaks-maakohut-valjastama-teavet-andmesubjekti-isikuandmete-tootlemise-kohta/ (13.01.2023), p 1.2.
[28] Väärteomenetluses kohaldatakse VTMS §-i 2 kohaselt kriminaalmenetluse sätteid, arvestades väärteomenetluse ja VTMS-i erisusi.

Politsei pädevust puudutavalt on õigusaktides eristatav ülesanne süütegusid ennetada[29] korrakaitseorganina KorS § 6 tähenduses ja tõkestada uurimisasutusena ning sellest tulenevalt IKS-i kohaldamine. Politsei ja piirivalve seaduse (PPVS)[30] § 3 lg 1 p 1 kohaselt on politsei ülesanne KarS-i teatud peatükkide „süütegusid ennetada“[31] ja kaitsta avalikku korda KorS-i tähenduses ning sama paragrahvi p 7 kohaselt „süütegusid menetleda“. Täpsemalt sätestab PPA põhimäärus[32] § 8 p-s 1 ülesandena muu hulgas „süütegude ennetamise ja riikliku järelevalve teostamise“ ning sama paragrahvi p-s 2 „süütegude menetlemise ja karistuste täideviimise“ ning § 16^2 p-des 1 ja 2 Keskkriminaalpolitsei ühe põhiülesandena teatud kuritegude „avastamise, tõkestamise ja menetlemise“.

Autor näeb siiski murekohana, et politsei ülesande täitmisel võib IKS-i 4. peatüki algus- või lõpuetapi ühene piiritlemine olla keeruline. Autori ettepanek on täiendavalt analüüsida IKS-i terminikasutust ning EL-i õigusega antud võimaluste eesmärgikohast rakendamist. IKS-i kohaldajale on vaja luua lõplik õigusselgus ohu- ja süü(teo)põhise sekkumise, sealhulgas teabe kogumise ning andmetöötluse õigusliku aluse piiritlemises ning IKS 4. peatüki tähenduses termini „süüteo ennetamine“ ja „süüteo tõkestamine“ määratluses.

EL-i vahetu õigusmõjuga valdkondliku, riigisisese EL-i teisest õigusakti ülevõtva või muu õigusakti osas märgib autor, et vastav õigusakt võib olla IKS-i 4. peatüki suhtes eriseaduseks. Küsimus on, kas selles on sätestatud andmesubjekti juurdepääsuõigus üksikasjalikumalt IKS-i 4. peatüki üldisest regulatsioonist. Euroopa Kohtu kohtujuristi arvamusest lähtudes, kui õigusaktis on lähtutud üldisest regulatsioonist, siis ei ole tegemist üldseadus/eriseadus suhtega.[33] Kohaldada saab viimasel juhul erisuste puudumisel IKS-i 4. peatükki osas, milles on võimalik seda vahetult kohaldada. Autori hinnangul võib eelnimetatust lähtuda ka olukorras, kus õigusaktis on sätestatud õiguskaitse eesmärgil toimuvat andmetöötlust puudutav teatud eripärane regulatsioon, kuid andmesubjekti õiguste tagamisel viidatakse Eesti õiguse mõistes IKS-i 4. peatüki sätete kohaldamisele.

Samas võib esineda olukord, kus valdkondlikus õigusaktis on täpsustatud andmesubjekti õiguste tagamise kontekstis IKÜM-i kohaldumine, aga ei ole sõnaselgelt välistatud samas

[29] KorS § 2 lg 1 ja lg 4, § 5 lg 7; ohu ennetamise kohta vt Laaring, M. KorSK § 2/2. – Laaring, M. jt. Korrakaitseseadus. Kommenteeritud vlj. Sisekaitseakadeemia 2017.
[30] Politsei ja piirivalve seadus. – RT I, 06.07.2023, 64.
[31] Isiku-, rahvatervise-, vara- ja avaliku rahu vastased, ameti- ja majandusalased ning üldohtlikud kuriteod vt vastavalt KarS-i 9., 12., 13., 16., 17., 21. ja 22. ptk.
[32] Politsei- ja piirivalveameti põhimäärus. SiMm 17.07.2014 nr 33. – RT I, 12.11.2022, 4.
[33] Analoogia korras IKÜM-i kohta vt EK C-129/21, *Proximus NV (üldkasutatavad elektroonilised kataloogid)* versus *Gegevensbeschermingsautoriteit*, ECLI:EU:C:2022:332, kohtujuristi M. Collins ettepanek, p 48, 54.

õigusaktis reguleeritud õiguskaitse eesmärgil toimuva andmetöötluse raames andmesubjekti õiguste tagamisel ÕKAD-i või muu õigusakti kohaldumine. Autori hinnangul saab sellisel juhul kohaldada IKS-i 4. peatükki, et võimaldada erisusi andmesubjekti juurdepääsuõiguse tagamisel või selle piiramisel. Seega kui on võimalik eristada õiguslikult ja praktiliselt andmetöötlusest õiguskaitse eesmärgil toimuv osa, saab eristada andmesubjekti õiguste tagamise alust.

1.2. Vahetu juurdepääsuõiguse teostamise eeldused

Andmesubjektil on õigus õiglasele andmetöötlusele (ELPH art 47 ja ÕKAD põhjendus 26). Samuti on tal õigus olla teavitatud enda õigustest ja nende teostamise korrast (IKS § 14 p 1 koosmõjus ÕKAD põhjendusega 26) ning saada vabalt üldiseks kasutamiseks mõeldud informatsiooni (PS § 44 lg 1) ja tutvuda enda kohta hoitavate andmetega (PS § 44 lg 3–4).

Artikli 29 töörühm leiab, et andmesubjekti teavitamine loob läbipaistvust ja usaldust õiglase andmetöötluse suhtes.[34] Samuti leiab ta, et teabe andmine aitab kujundada arusaama andmetöötluse „ulatusest ja tagajärgedest".[35] Andmesubjekti õigused ja nende teostamine on omavahel sõltuvuses ning politsei peaks enda tegevusega tagama teadlikkuse neist. Autor märgib siinkohal, et ÕKAD art 12 lg 2 kohaselt on andmetöötlejal kohustus toetada andesubjekti tema õiguste teostamisel, millele ei ole aga otsest vastet IKS-is.

Lähtudes ÕKAD-i 3. peatükis sätestatust, on IKS-i 4. peatüki 3. jaos sätestatud järgmised andmesubjekti õigused seoses isikuandmete töötlemisega politseis:

1) õigus teabe avalikult kättesaadavaks tegemisele (IKS § 22 lg 1);
2) vahetu juurdepääsuõigus (täielik, osaliselt piiratud või täielikult piiratud[36]), tähenduses
    a. õigus teavitamisele (IKS § 23 lg 1);
    b. õigus tutvustamisele (IKS § 24 lg 1);
    c. õigus parandamisele ja kustutamisele (IKS § 25 lg 1–3);
3) kaudne juurdepääsuõigus (õigus teavitamisele õigusest vaidlustada vahetu juurdepääsuõiguse piiramine, IKS § 24 lg 4 ja § 25 lg 7) ning
4) kaebeõigus (IKS § 28 lg 1).

[34] Suunised määruse 2016/679 kohase läbipaistvuse kohta. Artikli 29 alusel asutatud andmekaitse töörühm. WP 260REV1. Vastu võetud 29.11.2017. Viimati muudetud ja muudatused vastu võetud 11.04.2018. – https://ec.europa.eu/newsroom/article29/items/622227 (12.03.2024), vnr 1 lk 4, vnr 2 lk 4–5.
[35] Samas, vnr 10 lk 7.
[36] Autori IKS-i põhiste täpsustustega andmesubjekti õiguste teostamise kolmeastmelise lähenemise algallika kohta vt Sajfert, J., Quintel, T. 2017. Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities. – https://ssrn.com/abstract=3285873 (21.02.2024), lk 13.

Täpsemalt on andmesubjekti tutvumise eesmärgid kaardistanud D. Dimitrova ja P. De Hert, arvestades Euroopa Kohtu ja Euroopa Inimõiguste Kohtu praktikat ning teaduskirjandust, järgmiselt:

1) läbipaistvuse tagamine[37], mis võimaldab leida tasakaalu informatsioonilises enesemääramises, iseäranis andmetöötleja suhtes, kelle ülesannete iseloomu tõttu on osa andmetöötlusest varjatud;
2) seaduslikkuse ja muude isikuandmete töötlemise põhimõtete monitoorimine, sealhulgas andmesubjekti taotlusele eelneva andmetöötluse kohta[38], mille võimaldamine ja tulemus on eeldus muude andmesubjekti õiguste, näiteks parandamise õiguse[39] või kohtueelses menetluses kaitseõiguse teostamiseks[40];
3) taotletud meetmete võtmise monitoorimine, mis taaskord on oluline tagajärgede tõttu, mida ebaõiged või -täielikud andmed võivad andmesubjektile põhjustada[41] ning
4) teadlikkuse tõstmine andmetöötleja praktikatest ning poliitiliste ja õiguslike muudatuste algatamine ka teisi andmesubjekte puudutavalt.[42]

Siinkohal toob autor välja M.R. Leiseri ja B.H.M. Custersi seisukoha, et juurdepääsuõigus õiguskaitse eesmärgil andmetöötlusele loob eksitava läbipaistvuse, sest andmesubjekt ei saa „võimestatud“ ega „kontrolli“ andmetöötluse üle.[43] Seda enam tuleb autori hinnangul politseil vastavalt võimalusele esmajoones avalikustada üldine teave andmetöötluse kohta. Vastupidisel juhul on andmesubjektil samuti näiline ja võimalik, et ekslik arusaam andmetöötluse puudumisest või selle olemasolust.

Üksnes teabe saamisel andmetöötluse ja enda õiguste kohta on võimalik teadlikult taotleda vahetut juurdepääsuõigust PPA-lt ja saada juurdepääs või selle piiramise korral pöörduda AKI-sse. Eelkirjeldatu tõttu, olles eelnevalt määratlenud IKS-i kohaldamisala, analüüsib autor IKS-i 4. peatüki 3. jao sätteid, mis annavad andmesubjektile õiguse saada teavet tutvumise õiguse kohta ja esitada taotlus isikuandmetega tutvumiseks.

---

[37] EK C-553/07, *College van burgemeester en wethouders van Rotterdam* versus *M.E.E. Rijkeboer* (edaspidi *Rijkeboer)*, ECLI:EU:C:2008:773, kohtujurist D. Ruiz-Jarabo Colomer ettepanek, p 33–34.
[38] Samas, p 33–34 ja 54.
[39] EKo C-141/12, *YS* versus *Minister voor Immigratie, Integratie en Asiel*, ECLI:EU:C:2014:2081, p 44.
[40] Dimitrova, LED Article 14/A. Commentary.
[41] Kustutamist puudutavalt vt EKo C-118/22, *NG* versus *Direktor na Glavna direktsia „Natsionalna politsia“ pri Ministerstvo na vatreshnite raboti – Sofia*, ECLI:EU:C:2024:97, p 32, 72.
[42] Dimitrova, D., De Hert, P. The Right of Access Under the Police Directive: Small Steps Forward, lk 123. – Medina, M. (ed. et al.). Privacy Technologies and Policy. APF 2018. Lecture Notes in Computer Science, vol 11079. Springer, Cham. – https://doi.org/10.1007/978-3-030-02547-2_7 (18.03.2024), lk 114–115.
[43] Leiser, M.R., Custers, B.H.M. 2019. The Law Enforcement Directive: Conceptual Issues of EU Directive 2016/680, European Data Protection Law Review. Volume 5, Issue 3. – https://ssrn.com/abstract=4014545 (05.03.2024), lk 374, 378.

1.2.1. Andmesubjektile teabe avalikult kättesaadavaks tegemine

Politseil on kohustus teha andmesubjektile avalikult kättesaadavaks IKS § 22 lg 1 p-des 1–5 loetletud teave. ÕKAD-i art 13 lg-s 1 on sätestatud teave, mis tuleb avalikustada. IKS-i säte ei ole vastuolus ÕKAD-i sättega. Autori hinnangul on andmesubjekti teadlikkuse tõstmiseks vaja sättes samamoodi ÕKAD-i sõnastusega kasutada sõna „vähemalt", mis suunab andmetöötlejat mõtlema võimaluse korral ulatuslikumale teavitusele, kui kehtiv õigus ette näeb.

IKS § 22 lg 2 kohaselt tuleb teave avalikustada andmetöötleja veebilehel või muus andmesubjektile kergesti juurdepääsetavas kohas. IKS ei sätesta täpsemaid nõudeid avalikustamisele. Autor järeldab analoogia korras IKÜM-i kohta esitatud AKI juhendist, et IKS-i kohaselt võib teabe kättesaadavaks tegemine tähendada üldjuhul andmekaitsetingimuste avaldamist andmetöötleja välisveebis.[44] Andmekaitsetingimused on seega vorm, milles avalikustada kogu IKS § 22 lg 1 p-des 1–5 loetletud teave. Avalikustatavaks teabeks on ka teave selle kohta, et andmesubjektil on õigus tutvuda enda andmetega (IKS § 22 lg 1 p 2).

Autori hinnangul on kõneallolevalt PPA andmekaitsetingimused üldsõnalised ega anna ülevaadet kogu andmetöötlusest. Samas nähtub andmetöötluse tervikpilt selgemini Riigi infosüsteemi haldussüsteemi veebilehel olevast teabest politsei infosüsteemide kohta (vt viide 9).[45] Autori hinnangul on vaja andmesubjekti õiguste tõhusaks kaitseks täiendada PPA andmekaitsetingimusi, eeskätt isikuandmete töötlemise kavandatud eesmärgi ja andmesubjekti õiguste osas.

Lisaks on autori hinnangul otstarbekas PPA andmekaitsetingimustes teavitada andmesubjekti isikuandmete töötlemise õiguslikust alusest ja võimaluse korral algsest erinevast eesmärgist. IKS §-i 15 alusel võib töödelda isikuandmeid üksnes seaduse alusel. Andmetöötluse toimingu õiguslik alus ja eesmärk on seega sätestatud seaduses või andmekogu põhimääruses.[46] Andmesubjekt saab näiteks Riigi Teataja otsinguga välja selgitada, mis on politsei poolse andmetöötluse alused. Sageli aga ei ole M. Mikiveri Justiitsministeeriumile esitatud analüüsi kohaselt õigusaktid üldvolituse tõttu piisavalt selged ega täpsed, et andmesubjekt saaks aru

[44] Täpsemalt vt Isikuandmete töötlemise üldjuhend. Andmekaitse Inspektsioon. Kinnitatud 31.05.2018. Muudetud 28.09.2018. Muudetud 19.03.2019. – https://www.aki.ee/sites/default/files/dokumendid/isikuandmete_tootleja_uldjuhend.pdf (12.03.2024), lk 43, 48–49.

[45] PPA andmekaitsetingimuste kohta vt https://www.politsei.ee/et/juhend/isikuandmete-toeoetlemine ja https://www.politsei.ee/et/schengeni-piirikontroll (05.03.2024).

[46] Täpsemalt vt Mikiver, M. Analüüs. Andmekogud ja isikuandmed: EV Põhiseadusest ja IKÜM-st tulenevad nõuded regulatsioonile. Justiitsministeerium 2021. – https://www.just.ee/uuringud (17.03.2024), lk 36.

andmekogude omavahelisest koostoimest ja teda puudutavast andmetöötlusest.[47] Samuti on Mikiver leidnud, et eesmärk ei pruugi olla sätestatud iga andmetöötluse toimingu kohta.[48] Siinkohal on näiteks ka politsei infosüsteemi § 2, milles sätestatud eesmärk võimaldab töödelda infosüsteemis „korrakaitse ja süüteomenetlusega seotud andmeid, et tagada avalik kord ja siseturvalisus“.[49] Autori hinnangul tuleb võimaluse korral avalikustada politseil üheselt mõistetavalt teave andmetöötluse õigusliku aluse kohta seostatuna andmetöötluse eesmärgi või eesmärkidega.

ÕKAD art 12 lg 1 esimene lause näeb ette andmesubjekti teavitamise „kokkuvõtlikus, arusaadavas ja hõlpsasti kättesaadavas vormis, kasutades selget ja lihtsat sõnastust“. IKS § 27 lg 1 esimeses lauses on eelkirjeldatud kohustus seotud vastamisega andmesubjekti taotlusele, kuigi ÕKAD kohustab nii esitama teavet kui ka vastama taotlusele eelkirjeldatud vormis ja viisil. Autori hinnangul tuleb selguse huvides laiendada IKS § 27 lg 1 reguleerimisala.

1.2.2. Andmesubjekti teavitamisel antav teave

Politseil on kohustus esitada seaduses sätestatud konkreetsel juhul andmesubjektile teda puudutava andmetöötluse kohta IKS § 22 lg-s 1 nimetatud teabega koos IKS § 23 lg 1 p-des 2–3 nimetatud „lisateave“, arvestades, et loetelu ei ole lõplik. Mitmete ÕKAD-i täpsustuse kohta osalise selgituse andmine on nähtav IKS-i juurde kuuluvast seletuskirjast, võrreldes vastavaid ÕKAD art 13 lg 2 ja IKS § 23 lg 1.

Näiteks pole ÕKAD-i art 13 lg 2 p-s c vastuvõtjate kategooriad puudutav täpsustus sätestatud IKS-is. ÕKAD-i sätet on täpsustatud seletuskirjas selliselt, et isikuandmete vastuvõtjate kategooriateks võib olla välisriigi pädev asutus, kellele andmeid edastatakse vastastikuse õigusabi raames või julgeolekuasutused, kes teostavad isiku suhtes tausta- või julgeolekukontrolli[50]. Samas, IKS-i kõneallolevas sättes ega seletuskirjas ei ole selgitust autori hinnangul olulise ÕKAD-i art 13 lg 2 p-s d välja toodu kohta sellest, et lisateave on vaja anda eriti juhul, kui isikuandmed on kogutud andmesubjekti teadmata.

Autori hinnangul tuleb otstarbekusest lähtuvalt, kuid võimalikult palju täpsustusi välja tuua seaduse tasandil, sest sellega abistatakse andmetöötlejat määratlema proportsionaalsemalt

[47] Mikiver 2021, lk 37–38.
[48] Samas, lk 32.
[49] Politsei andmekogu põhimäärus. SiMm 22.12.2009 nr 92. – RT I, 25.08.2023, 5.
[50] Isikuandmete kaitse seaduse 679 SE seletuskiri, § 22 lk 28.

teavituse sisu ja ulatust. Iseäranis arvestades, et andmesubjekt ei pruugi olla teadlik andmetöötlusest, mistõttu on vaja talle esitada tema õiguste teostamiseks võimalikult palju lisateavet. Siiski ei ole tegemist vastavuse puudumisega ÕKAD-i ja IKS-i sätete vahel, arvestades eeskätt võimalusega, et IKS § 22 lg 1 teavitamise kohustus peab tulenema IKS-i suhtes eriseaduses sätestatud kohustusest, kus eelduslikult on välja toodud asjakohane teavituse sisu. Kui andmesubjektile ei anta üksikasjalikku lisateavet, ei teki tal arusaamist andmetöötlusest ega võimalikust vajadusest esitada taotlus, et tutvuda päriselt isikuandmetega.

1.2.3. Andmesubjekti taotlusel isikuandmete töötlemise kinnitamine

Andmesubjektil on IKS § 24 lg 1 esimese lause kohaselt õigus saada politseilt „kinnitus selle kohta, et tema isikuandmeid töödeldakse“ ning teise lause esimese lauseosa kohaselt saada juurdepääs isikuandmetele ja teabele nende töötlemise kohta. Tegemist on tutvumise õiguse teostamise alussättega, mis andmetöötluse korral politseis annab juurdepääsuõiguse isikuandmetele ja nende töötlemise kohta käivale teabele. Põhimõtteliselt on seadusandja üle võtnud IKS § 24 lg-ga 1 elemendid, mis on ette nähtud ÕKAD art-s 14. Autor märgib olulise aspektina, et kooskõlaliselt EL-i õigusega ei anna IKS valikuvõimalusi. See tähendab, politseil pole võimalik jätta andmesubjektile vastamata või suunata andmesubjekti AKI-sse enda tutvumise õigust teostama muul juhul, kui tutvumise õiguse piiramise korral.

Autori hinnangul võib aga olla ebaselge kõnealloleva IKS-i sätte ülesehitus. Andmetöötluse kohta kinnituse ja „soovi“ korral „teabele“ juurdepääsu saamise õigus on sätestatud eraldi lausetes. IKS § 24 lg 1 teisest lausest võib aru saada selliselt, et üksnes eraldi soovi avaldamise korral on võimalik saada juurdepääsuõigus isikuandmetele ja teabele nende töötlemise kohta. Ehk, taotluse saamisel ja andmetöötluse korral pole andmetöötlejal kohustust anda koos kinnitusega andmetöötluse kohta koheselt juurdepääsuõigust „teabele“, sest kui väljastataks lisaks kinnitusele isikuandmed ja teave, aga andmesubjektil ei ole soovi tutvuda nendega, on andmetöötlus olnud ülemäärane seoses andmesubjekti puudutavate isikuandmete otsimise jm töötlemisega. Andmetöötleja peaks seega täpsustama andmesubjektiga tema tegelikku tahet või arusaama tutvumise õiguse ulatusest. Eelkirjeldatud võimalik IKS § 24 lg 1 tõlgendus ei ole autori hinnangul eesmärgikohane ega kooskõlas üldkehtiva arusaamaga ning võib viia andmesubjekti tutvumise õiguse ebaproportsionaalse piiramiseni. Andmesubjektil pole kohustust täpsustada ega põhjendada tutvumise soovi ega esitada mitut pöördumist.

IKS-i keelelise või ebakorrektse tõlgenduse tõttu ei ole välistatud, et tutvumise õigus ja sellest tulenev muu õigus võib jääda täies ulatuses teostamata. IKS § 24 lg 1 teises lauses on seadusandja sõnadega „andmesubjekti soovil“ mõelnud eelduslikult rõhutada, et tutvumise õiguse teostamiseks on vaja andmesubjekti tegevust taotluse esitamise näol. Autori hinnangul tuleb kaaluda IKS § 24 lg 1 sõnastuse muutmist selliselt, et sõnaselgelt tuleb välja taotluse esitamise kohustus ja selle kehtivus tutvumise õiguse teostamisele tervikuna.

IKS § 24 lg 1 esimese lause sõna-sõnalt tõlgendus võib autori hinnangul viia järeldusele, et isikuandmete mittetöötlemise korral ei ole vaja seda andmesubjektile üle kinnitada. Seevastu ÕKAD art 14 sõnastus viitab andmesubjekti õigusele saada vastus „kas“-küsimusele ehk kinnitus nii andmetöötluse olemasolul kui ka selle puudumisel. Artikli 29 töörühm on rõhutanud, et üldjuhul on andmesubjektil õigus saada andmetöötlejalt negatiivne kinnitus ehk teave, et ta ei töötle tema isikuandmeid.[51] Samuti, rõhutanud, et andmetöötluse puudumisel negatiivse kinnituse andmata jätmine on võimalik üksnes juhul, kui on alus tutvumise õiguse piiramiseks.[52] Seega kui ei töödelda andmeid IKS § 24 lg 1 p 1 tähenduses ja andmesubjekti sellest ei teavitata, kuigi teavitamata jätmiseks puudub IKS § 24 lg 2 kohane õiguslik alus, on tegemist tutvumise õiguse ebaseadusliku piiramisega. Autori ettepanekul tuleb, arvestades ÕKAD-i art 14 sõnastust, kaaluda IKS § 24 lg 1 lause 1 täpsustamist selliselt, et andmetöötlejal on kohustus anda negatiivne kinnitus. Igal juhul tuleb andmetöötleja juhendis selgitada, et kinnituse andmine puudutab nii andmetöötluse olemasolu kui selle puudumist.

Autor juhib tähelepanu aspektile, et aktsepteeritav ei ole IKS § 24 lg-s 1 nimetatud teabe esitamise asemel juhtida andmesubjekti tutvuma andmekaitsetingimustega[53]. Artikli 29 töörühm on rõhutanud, et üldjuhul on andmesubjektil õigus saada vahetu juurdepääs kõigile isikuandmetele ja kogu teabele nende töötlemise kohta.[54] Samuti viitavad IKS seletuskirja koostajad, et kõnealloleva sätte eesmärk on tagada teadmine, kas isikuandmeid töödeldakse, tutvumine täieliku kokkuvõttega kogutud andmetest ning saada kõnealloleva sättes loetletud teavet töötlemise kohta.[55] Nii nagu tuleb esitada andmesubjektile tema enda kohta käivad isikuandmed, tuleb nõutud teave esitada seostatuna andmesubjekti isikuandmete töötlemisega.

[51] Vt Artikli 29 töörühm. WP 258, lk 16.
[52] Samas, lk 19.
[53] Analoogia korras praktika kohta vt Ausloos, J., Mahieu, R., Veale, M. Getting Data Subject Rights Right. A submission to the European Data Protection Board from international data rights academics, to inform regulatory guidance. 10 (2020) Journal of Intellectual Property, Information Technology and E-Commerce Law 283 para 1. – https://www.jipitec.eu/archive/issues/jipitec-10-3-2019/5031 (18.03.2024), p 58, 60–61.
[54] Vt Artikli 29 töörühm. WP 258, lk 16.
[55] Isikuandmete kaitse seaduse 679 SE seletuskiri, § 23 lk 28–29.

1.3. Kriminaalmenetluse seadustiku kohaldamisala

Politseil võib olla vaja andmesubjekti tutvumise õiguse teostamisel kohaldada KrMS-i või VTMS-i, sest Eesti seadusandja on kasutanud võimalust näha ette andmesubjekti õiguste tagamisele süüteomenetluse raames IKS-i 4. peatükist teistsugune kord. See tähendab andmekaitseõiguse kohaste sätete loomist süüteomenetlusõiguse kesksesse õigusakti. IKS sätestab § 2 p-s 1, et kohaldub süüteomenetlusele "menetlusseadustikes sätestatud erisustega". Seevastu Euroopa Komisjonile TIPIK-i poolt esitatud ÕKAD-i ülevõtmise analüüsis on leitud, et Eesti ei ole kehtestanud andmesubjekti õiguste teostamist riigisisese õiguse kohaselt, nagu võimaldab ÕKAD art 18[56]. Eelnimetatu tõttu analüüsib autor IKS-i kohaldamisala vaates ja tema suhtes eriseaduseks olevas KrMS-is sätestatud andmesubjekti juurdepääsuõiguse regulatsiooni, sealhulgas tuues magistritöö mahu piirangu tõttu VMTS-i osas välja üksnes erisusi.

KrMS § 15^2 lg 3 alusel saab sama seaduse kohaselt teostada „IKS-ist tulenevaid õigusi“ andmesubjekt, kelleks on „kahtlustatav, süüdistatav, kannatanu, tsiviilkostja, kolmas isik, tunnistaja või muu isik“.[57] Loetelu on laiem, kui KrMS § 16 lg 2 menetlusosaliste loetelu. Kuna nimetatud on „muu isik“, pole ebaproportsionaalselt piiratud ühegi andmesubjekti võimalust kriminaalmenetluse raames enda õigusi teostada. Lisaks on KrMS § 15^2 lg-s 4 sätestatud andmesubjekti „IKS-ist tulenevate õiguste“ piiramise alused ning sama paragrahvi lg-s 5 konkreetsed õigused, mida võib piirata.

ÕKAD art-st 18 tulenevalt on andmesubjektil õigus teabe kättesaadavusele ja teavitamisele, teabe ja isikuandmete tutvustamisele ning isikuandmete parandamise ja kustutamise nõudmisele. KrMS § 15^2 lg-st 3–4 ei selgu, millised andmesubjekti õiguseid on sättes silmas peetud ja milline on nende teostamise kord. KrMS § 15^2 lg-st 3 ei selgu muu hulgas, kuivõrd on andmesubjekti taotluse esitamise ning isikuandmete ja töötlemise kohta teabe saamise aluseks IKS § 24 lg 1, mis on andmesubjekti õiguste teostamise üldsäte (üksnes andmesubjekti õiguste piiramist puudutavad KrMS § 15^2 lg-d 4–5 on minimaalselt täpsema sõnastusega). Samuti pole IKS 4. peatüki 3. jaos sätestatud erisust seoses süüteomenetluse raames andmesubjekti õiguste ja nende piiramise aluste või teostamise korraga.

[56] TIPIK 2020, p 18 (viidatud märkus 37 Franssen, Corhay, LED Article 18/B.3. Commentary).
[57] VTMS §-i 18 tähenduses menetlusalune isik, kelle suhtes on alustatud väärteomenetlust.

IKS seletuskirja koostajad on selgitanud, et kriminaaltoimikus olevatele andmetele juurdepääsu regulatsioon KrMS §-is 224–224[1] koostoimes §-iga 214 on vastavuses ÕKAD art-ga 18.[58] Sellest tulenevalt saab politsei kriminaalmenetlusõiguse alusel ja KrMS § 214 lg 1 kohaselt üksnes prokuratuuri loal avaldada kohtueelse menetluse andmeid, arvestades sama paragrahvi lg-s 2 toodud piirangutega.[59] Samuti tähendab see, et andmesubjekti erinevate õiguste teostamine on seostatud vastavalt KrMS §-ile 224–224[1] kriminaaltoimiku tutvumiseks esitamisega või tutvustamisega lähtuvalt andmesubjekti staatusest menetluses.[60]

KrMS § 15[2] lg 3 puhul on autori hinnangul realiseerunud ÕKAD-i analüüsis välja toodud laiem etteheide. Nimelt leiavad P. Vogiatzoglou ja T. Marquenie, et ÕKAD art 18 koosmõjus põhjendusega 49 ja 107 võimaldab riigisisese kriminaalmenetlusõiguse alusel sätestada andmesubjekti õigustele teistsuguse regulatsiooni, kui EL-i õigus liikmesriikidele ühtselt ette näeb.[61] KrMS § 15[2] lg 3 sõnastuse kohaselt lähtutakse IKS-ist tulenevate õiguste teostamisel KrMS-ist. Sellise sõnakasutuse tõttu ei ole autori hinnangul selge, kas andmekaitseõigusest tulenevad õigused teostamise kord taandub kriminaalmenetlusõigusest tuleneva õiguste teostamise korra ees või jääb teatud osas paralleelselt kehtima. Lisaks ei ole autori hinnangul välistatud, et andmesubjektil ei teki võimalust enda IKS-ist tulenevaid õigusi teostada ka järgneval põhjusel. AKI järelevalvepraktikast nähtub, et kriminaalmenetlusega seotud andmesubjekti tutvumise õigust piirab andmetöötleja sageli instinktiivselt või igal ajahetkel lähtuvalt konkreetselt kriminaaltoimikule kehtivatest juurdepääsureeglitest KrMS-is, sealhulgas ei anta pärast menetlust uuesti juurdepääsu toimikule andmesubjekti õiguste üldise regulatsiooni raames[62].

V. Franssen ja M. Corhay rõhutavad vajadust ÕKAD-i art 18 korrektseks kohaldamiseks selgelt eristada vastavatest õigusharudest tulenevad andmesubjekti õigused.[63] Autor tõdeb Dimitrova välja toodu alusel, et kõneallolevas regulatsioonis ei saa eirata isikuandmete kaitse spetsiifilisi ja ÕKAD-i kohaselt sätestamist vajavaid põhimõtteid, nagu need on Eesti puhul toodud IKS-

[58] Isikuandmete kaitse seaduse 679 SE seletuskiri, § 23 lk 29.
[59] Vrd väärteo kohtuvälise menetlejana politseiametnik VTMS § 9 p 1 ja § 10 lg 1 kohaselt.
[60] Vt ka VTMS § 62.
[61] Vogiatzoglou, P., Marquenie, T. Assessment of the implementation of the Law Enforcement Directive. Policy Department for Citizens' Rights and Constitutional Affairs. Directorate-General for Internal Policies. PE PE 740.209. December 2022. – https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740209/IPOL_STU(2022)740209_EN.pdf (05.03.2024), lk 58.
[62] Vt vaideotsus ja ettekirjutus-hoiatus. AKI 07.05.2021 nr 2.1-3/21/1208. – https://www.aki.ee/sites/default/files/vaideotsus_ja_ettekirjutus-hoiatus_07.05.2021_avaliku_teabe_asjas_nr_2.1.-3_21_1208_politsei-_ja_piirivalveameti_ida_prefektuur_-_eraisik.pdf (28.01.2024).
[63] Franssen, Corhay, LED Article 18/B.3. Commentary.

is[64]. Lisaks tõdeb autor lähtudes Euroopa Kohtu otsusest, et IKS-i üldnormid jäävad paralleelselt kehtima[65]. Autori hinnangul tuleb KrMS-is senisest ammendavamalt sätestada, milliseid õiguseid andmesubjekt omab tulenevalt kriminaalmenetlus- ja andmekaitseõigusest, võimalik, et paralleelselt.

KrMS § 15^2 lg 3–5 puhul tekib küsimus selle kohaldamise ulatusest „kriminaalmenetluse raames".[66] Enne kehtiva IKS-i redaktsiooni on Riigikohus lähtunud põhjendusest, et „kriminaalmenetluse kestel mõjutab vahetult" selle toimumise kulgu „kriminaalmenetluses kogutud" isikuandmetele juurdepääsuõiguse andmine[67]. Seega on küsimus andmesubjektile juurdepääsu andmises KrMS-i raames ja KrMS § 160^1 tähenduses kriminaaltoimikule[68], mis on „kriminaalasjas kogutud dokumentide kogum" ja sisaldab ka andmetöötlust puudutavat teavet.[69] Eelnimetatud määratlus on autori hinnangul kooskõlas ÕKAD art-ga 18, mis piiritleb selle kohaldamise muu hulgas „kriminaaluurimise ja -menetluse käigus töödeldava toimikuga".

Tuleb täpsustada, et IKS-i 4. peatüki kehtivuse ajal on Eesti kohtupraktikas eristatud teavet selle alusel, kas ta on või ei ole saadud kriminaalmenetluse toiminguga, pööramata tähelepanu asjaolule, kas „teave või teabekandja on" osa kriminaaltoimikust.[70] Vastavalt on Tallinna Ringkonnakohus rõhutanud teabe kogumise eesmärgi tähtsust, leides, et kui teave on kogutud kriminaalasja kohtueelse uurimise käigus ja esitatakse tutvumiseks KrMS §-i 224 korras, on tegemist kriminaalmenetluse toimingutega ning konfidentsiaalsele teabele või seda sisaldavatele teabekandjatele juurdepääs tuleb otsustada või vaidlustada KrMS õigusnormide alusel kriminaalkohtumenetluse raames.[71]

Igal juhul kehtib kriminaaltoimiku osaks mitteolevale teabele juurdepääsuõigus KrMS § 15^2 lg 3–5 kohaselt. Asjakohane on AKI arvamus, et politseil erinevalt prokuratuurist on ebaproportsionaalne käimasoleva süüteoasja raames piirata andmesubjekti IKS-i või IKÜM-ist tulenevat õigust isikuandmete väljastamisele infosüsteemist.[72] Infosüsteemi võivad olla isikuandmed saadud muu kui õiguskaitse eesmärgil läbiviidud ülesande täitmise käigus, aga

[64] Dimitrova, LED Article 14/B.4. Commentary.
[65] Analoogia korras juurdepääsuõiguse kohta andmekaitseõiguse ja muu õiguse alusel vt EKo C-434/16, *Peter Nowak* versus *Data Protection Commissioner*, ECLI:EU:C:2017:994, p 56.
[66] Vrd sõnastust KrMS § 15^2 pealkirjas ja sama paragrahvi lg-s 2.
[67] RKKKm 3-1-1-116-04, p 19.
[68] VTMS § 81 lg 1 väärteotoimiku osas.
[69] Isikuandmete kaitse seaduse 679 SE seletuskiri, § 23 lk 29.
[70] TlnRnKHKm 3-19-2110/25, p 11.
[71] Samas, p 11.
[72] Vastus nõudekirjale. AKI 20.01.2021 nr 2.1.-5/21/219. – https://www.aki.ee/meist/teadlikkus/dokumendiregister (11.04.2024).

need isikuandmed võivad samas olla osaks kriminaaltoimikust ja tõendusväärtusega. Seega samad isikuandmed võivad olla andmetöötlejatel – politseil ja prokuratuuril – saadud erineval eesmärgil ja õiguslikul alusel ning võivad paikneda mitmes asukohas.

Andmetöötlejal on vaja kriminaaltoimiku osaks olevast teabest eristada teave, mis ei ole kogutud kriminaalmenetluse toiminguga. Põhimõtteliselt pole sel juhul välistatud, et politsei lahendab sellisele tõenduslikule teabele juurdepääsu taotluse kriminaalmenetluse ajal mitte IKS § 24 lg 1 või KrMS § 15^2 lg 3, vaid IKÜM art 15 lg 1 alusel. Eelkirjeldatust ja sellest, kellele on andmesubjekti taotlus suunatud, sõltub juurdepääsu andmise õiguslik alus.[73] Tuleb silmas pidada, et halduskohus ei oma pädevust teabele tõendi väärtuse ja tõendile juurdepääsu andmise küsimuses käimasoleva kriminaalmenetluse raames.[74] Kriminaaltoiminguga mitte saadud ja kriminaaltoimikus olevatele isikuandmetele IKÜM-i alusel juurdepääsu andmine ei saa aga viia võimatuseni vaidlustada andmetöötleja otsust kohtus.

Andmesubjekti õigused ei ole teostatavad KrMS § 15^2 lg 2–5 ega IKS §-i 24 alusel hetkest, kui kriminaalmenetlus on lõpetatud (KrMS § 206 lg 1 p 1 ja § 200–205^2, edasikaebetähtajad on möödunud ja kohtuotsus on jõustunud KrMS § 408 kohaselt) ja kriminaaltoimik arhiveeritud (KrMS § 209 lg 1). Nii nagu Riigikohus on selgitanud, ei ole sellest hetkest juurdepääsuõiguse lahendamine enam „suunatud toimepandud kuriteo avastamisele, tõendusteabe kogumisele ega kohtumenetluseks muude tingimuste loomisele“ ega moodusta „/…./ kriminaalmenetlusega ühtset tervikut, ei saa seda menetlust enam mõjutada ega ole seotud tehtud lahendi täitmisele pööramisega“.[75] Sisuliselt on sama olukord kriminaalmenetluse alustamata jätmisel (KrMS § 199 lg 1–2) ja pärast kriminaalmenetlusõigusest tulenevate õiguskaitsevahendite võimaluste ammendumist.[76]

Erijuhuks juurdepääsuõiguse teostamisele IKS § 24 lg 1 alusel kriminaalmenetluse lõpetamise järel või selle puudumisel võib pidada näiteks taotlust tutvuda ohu- või riskihinnangutega isiku ohtlikkuse, kuritegude toimepanemise tõenäosuse või korduvkuritegevuse kohta. Kui isikuandmed on kogutud õiguskaitse eesmärgil, on seaduslik alus nende isikuandmete võrdlemiseks ja kombineerimiseks, andmetöötluse tulemusel luuakse kriteeriumid selle kohta, kuidas süütegusid tõhusamalt tõkestada, avastada ja menetleda, siis võib autori hinnangul toimuda andmetöötlus õiguskaitse eesmärgil.

[73] Analoogia korras selle kohta, et kohtutoimikus oleva teabe väljastamisele kohaldub AvTS kui üldseadus, mitte halduskohtumenetlusnormid, kui teavet taotletakse teabevaldajalt, mitte kohtult vt RKHKo 3-20-1265, p 19–20.
[74] TlnHKm 3-19-2110/14, p 10–11.
[75] IKS v. r. ja ÕKAD-i vastuvõtmise järel vt RKKKm 3-1-1-116-04, p 20; RKHKo 3-3-1-84-15, p 20.
[76] Vrd VTMS § 29, § 30, § 119.

Märkimisväärne on Riigikohtu seisukoht, et kehtivas õiguses pole piisavalt ulatuslikult ja täpselt kindlaks määratud andmesubjekti õiguste teostamine kriminaalmenetluse käigus, sealhulgas pärast menetluse lõpetamist[77]. Autor nõustub tõdemusega, et vaja on korrastada Eesti õigust. IKS regulatsioon pole üldjuhul asjakohane õiguskaitse eesmärgi ärajäämisel. Vähemalt osaliselt on kriminaalmenetluse lõppemise tõttu ära langenud vajadus teabe andmist piirata või selle andmisest keelduda, sest teabele juurdepääsu andmine ei saa põhimõtteliselt mõjutada enam samaväärselt kriminaalmenetluse käiku võrreldes ajaga, kui andmesubjekt esitas taotluse ega olnud ise täielikult või osaliselt teadlik teda puudutavast andmetöötlusest.

Autor küsib analoogia korras kohtutoimiku kohta esitatud küsimusele, kas kriminaaltoimikus oleva teabe, sealhulgas isikuandmete ja nende töötlemise kohta käiva teabe töötlemise eesmärk võib pärast kriminaalmenetlust olla „eelkõige kas avalikes huvides arhiveerimine“ või kriminaalmenetluse „ülesande jätkuv täitmine“[78]. Autori hinnangul vähemalt teatud aja on tegemist mõtteliselt kriminaalmenetlusega seonduva andmetöötlusega.

Riigikohus on eelistanud, et KrMS-is sätestatakse ulatuslikumalt, täpsemalt ja ammendavalt andmesubjekti õiguste teostamise ka pärast menetluse lõpetamist ja toimiku arhiivimist.[79] Autor nõustub Riigkohtu seisukohaga otstarbekuse, selguse ja terviklikkuse huvides ning leiab, et andmesubjektile, tema esindajale, politseile ja prokuratuurile on lihtsamalt teadvustatavad andmekaitseõiguse spetsiifilised juurdepääsuõiguse normid juhul, kui need on sätestatud samas õigusaktis menetluse ajal ja pärast menetlust. Kehtivas KrMS § 206 lg-s 3 on sätestatud kannatanu õigus tutvuda kriminaaltoimikuga menetluse järgselt.[80] Sätestades KrMS-i aluse õiguste teostamisele pärast kriminaalmenetluse eesmärgi täitmist või kriminaalmenetluse eesmärgil kogutud andmete esialgsest erineval eesmärgil töötlemisele, tekib pooltel parem arusaam, samuti võrdlusmoment kriminaalmenetluse aegsest ja järgsest erisusest juurdepääsuõiguse teostamisel.

Tuleb rõhutada, et pärast kriminaalmenetlust ei ole menetlusosalisel suuremaid õigusi kolmandaid isikuid puudutavate isikuandmete või muu piiranguga teabe saamisele, millele juurdepääsu taotlemine allub avaliku teabe seaduse[81] (AvTS) § 14 lg 2 teabenõude

[77] RKHKo 3-3-1-84-15, p 17, 20, 26; RKKKo 1-19-8262, p 40, 47.
[78] Vt Vallimäe-Tuberg, K. II Isikuandmed kohtus IKÜM-i ajastul. Kohtutoimik kohtu arhiivis. Kohtute aastaraamat 2020. – https://aastaraamat.riigikohus.ee/kohtutoimik-kohtu-arhiivis/ (26.03.2024).
[79] RKHKo 3-3-1-84-15, p 17, 26; RKHKm 3-3-1-58-16, p 10; RKKKo 1-19-8262, p 40, 47.
[80] VTMS § 62 lg 3 sätestab väärteo tõttu kahju kannatanud isiku väärteotoimikuga tutvumise õiguse.
[81] Avaliku teabe seadus. – RT I, 07.03.2023, 11.

regulatsioonile, vaid üksnes teda ennast ja tema alaealist last puudutavate andmete saamisele IKÜM-i juurdepääsuõiguse alusel juhul, kui ei kohaldu piirangud.[82]

VTMS-is pole andmesubjekti õiguste tagamise regulatsiooni täpsustatud. Samuti ei leia selle kohta analüüsi IKS-i rakendusseaduse[83] (RS) seletuskirjast.[84] Autori hinnangul on vaja üle hinnata IKS-i kohaste õiguste teostamine väärteomenetluse raames ja proportsionaalsuse tagamiseks sätestada erisused KrMS-i regulatsioonist, eeskätt andmesubjekti juurdepääsuõiguse piiramisel.

[82] Nt Vaideotsus. AKI 14.01.2020 nr 2.1-3/19/4361. – https://www.aki.ee/sites/default/files/vaideotsused/2020/vaideotsus_14.01.2020_avaliku_teabe_asjas_nr_2.1.-3-19-4361_-_eraisik_-_politsei-_ja_piirivalveameti_laane_prefektuur.pdf (28.01.2024), lk 3.
[83] Isikuandmete kaitse seaduse rakendamise seadus. – RT I, 13.03.2019, 2.
[84] Seletuskiri isikuandmete kaitse seaduse rakendamise seaduse 778 SE, § 49 lk 60–63.

2. ANDMESUBJEKTILE VAHETU JUURDEPÄÄSUÕIGUSE ANDMINE

2.1. Andmesubjektile isikuandmete ja nende kohta käiva teabe tutvustamine

Artikli 29 alusel asutatud andmekaitse (edaspidi *Artikli 29*) töörühm on rõhutanud, et üldjuhul tuleb andmesubjekti taotlus või nõue täita ning üksnes erandjuhul võib taotluse või nõude täitmist piirata või nende täitmisest keelduda[85]. Samuti on kinnitanud Euroopa Kohtu praktika, et politseil on kohustus ise ja vahetult lahendada talle esitatud andmesubjekti taotlus[86]. Kui andmesubjekt on esitanud politseile taotluse ja tema andmeid töödeldakse õiguskaitse eesmärgil, tuleb politseil IKS § 24 lg 1 kohaselt talle teatavaks teha „tema kohta käivad isikuandmed" ja teave nende töötlemise kohta ning teave andmesubjekti nõudeõiguste, AKI-le kaebuse esitamise õiguse ja AKI kontaktide kohta. IKS-is on esitatud lõplik loetelu teabest, millega andmesubjektil on õigus tutvuda. Järgnevalt analüüsib autor IKS § 24 lg 1 p-i 1–6 kooskõla ÕKAD art 14 p-ga a–e ja g. Kaebeõigust ja AKI kontaktandmeid puudutav IKS § 24 lg 1 p 7 on autori hinnangul vastavuses ÕKAD art 14 p-ga f, mistõttu ei ole seda analüüsitud.

2.1.1. Isikuandmed ja nende esitamise vorm

IKS § 24 lg 1 p 1 alusel on politseil kohustus teha andmesubjektile teatavaks isikuandmed. ÕKAD-i art 14 pole isikuandmetega tutvumist eraldi punktina nimetatud, vaid see tuleneb selgitusest õiguse kohta tutvuda isikuandmetega nende töötlemise korral. IKS-is isikuandmetega tutvumise eraldi punktis rõhutamine annab autori hinnangul andmesubjektile selgemalt teada õigusest saada pärisandmeid iseenda kohta, mitte üksnes kirjeldust nende olemasolust ja tuletab politseile meelde kohustust isikuandmed väljastada.

Kõnealloleva kohustuse täitmise ulatus sõltub politsei hinnangust. Autori hinnangul võib kaalutlemine viia andmesubjekti tutvumise õiguse kitsendamiseni. Küsimus on selles, mis on andmetöötleja vaates isikuandmed ja isikuandmete töötlemine[87]. Vastav analüüs tuleb läbi viia andmesubjekti taotluse saamise hetkel olemasolevate kõigi isikuandmete ning kõigi töötlemise toimingute kohta.[88] Andmesubjektile tuleb esitada tema kohta andmetöötlejal olemasolevad

[85] Artikli 29 alusel asutatud andmekaitse töörühm. WP 258. Arvamus direktiivi (EL) 2016/680 mõne olulise aspekti kohta. Vastu võetud 29.11.2017 (edaspidi *Artikli 29 töörühm. WP 258*). – https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610178 (05.03.2024), lk 20.
[86] C-333/22, *Ligue des droits humains*, p 41; C-333/22 *Ligue des droits humains,* kohtujurist L. Medina ettepanek, p 39, 41.
[87] EKo C-487/21, *F.F.* versus *Österreichische Datenschutzbehörde*, ECLI:EU:C:2023:369, p 26 ja 28.
[88] EDPB Guidelines 01/2022, vnr 37.

isikuandmed kui ka nende töötlemisel saadud isikuandmetena mõistetav teave.[89] Täpsemalt, tutvumise õigus kohaldub nii andmetöötleja enda kogutud, salvestatud ja töödeldud andmetele kui kõigile täiendavatele andmetele ja uuele teabele, mida andmesubjekti kohta võidakse saada.[90]

Vastav analüüs puudutab ka isikuandmeid, mis on „ebaseaduslikud, ebaõiged" või mida andmetöötleja „enam ei vaja".[91] Andmesubjekti tuleb teavitada eelnimetatud tunnustele vastavate andmete olemasolust ja kavatsusest andmeid parandada või kustutada[92]. Andmesubjektile eelnimetatud isikuandmete mitteväljastamise soovi tõttu ja riigisisese kriminaalmenetluse kaitseks pole lubatud neid andmeid kustutada, ilma eelnevalt andmesubjektiga suhtlemata.[93] Vastupidiselt toimides on andmetöötlejal, mitte andmesubjektil kontroll andmetöötluse üle ja võimupositsioon, mida andmesubjekt ei saa tutvumise, parandamise ega kustutamise õiguse kaudu tasakaalustada.

IKS-is pole täpsustatud andmesubjektile isikuandmete väljastamise vormi. ÕKAD-is on põhjenduse 43 viiendas lauses selgitatud, et töödeldavad isikuandmed võib esitada koopiana. Lisaks peetakse samas põhjenduses piisavaks arusaadaval kujul andmete täieliku kokkuvõtte esitamist, mis võimaldab saada neist teadlikuks ja kontrollida nende õigsust.[94] Põhimõtteliselt seega piisab nimekirja esitamisest töödeldavate isikuandmete kohta.[95] Sellega võib andmetöötleja lugeda IKS § 24 lg 1 p-i 1 kohustuse täidetuks.

Autori hinnangul on siiski oluline analüüsida, millal on vaja esitada IKS § 24 lg 1 p-i 1 alusel tutvumise õigusega hõlmatud kõik isikuandmed koopiana. Andmetöötlejal tuleb lähtuvalt konkreetsest olukorrast kaaluda, kas koopia või kokkuvõte on proportsionaalne isikuandmete esitamise vorm. Euroopa Kohtu kohtujurist peab vajalikuks, et vastavas analüüsis arvestatakse andmesubjekti taotluse esemeks olevate andmete kategooria ja taotluse sisuga.[96]

---

[89] C-487/21, *F.F.*, p 26.
[90] EK C-487/21, *F.F.* versus *Österreichische Datenschutzbehörde*, ECLI:EU:C:2022:1000, kohtujurist G. Pitruzzella ettepanek, p 37–38.
[91] EDPS-i otsus. Vt Decision of the European Data Protection Supervisor in complaint case 2020-0908 against the European Agency for Law Enforcement Cooperation (Europol) (edaspidi *EDPS Case 2020-0908*). – https://edri.org/wp-content/uploads/2022/09/22-09-08_EDPS-Decision_2020-0908_redacted.pdf (09.04.2024), p 3.40.
[92] EDPB Guidelines 01/2022, vnr 39.
[93] Vt EDPS Case 2020-0908, p 3.22–3.23.
[94] ÕKAD p 43 neljas lause.
[95] Dimitrova, De Hert 2018, lk 119.
[96] C-487/21, *F.F.*, kohtujurist G. Pitruzzella ettepanek, p 57.

Läbipaistvuse põhimõtte järgimine nõuab andmesubjektile täieliku mõistmise tagamist talle antud teabe sisust.[97] Sellise mõistmise loomine võib olla võimalik üksnes koopia esitamisega. Asjakohane on Euroopa Kohtu seisukoht, et hädavajalik on koopia esitamine dokumendi või andmebaasi väljavõttena, et andmesubjekt saaks aru töödeldavate andmete kontekstist ja seekaudu talle esitatud teabest, sealhulgas isikuandmetest.[98]

Samas isikuandmete esitamise vorm pole iseenesest oluline. Euroopa Andmekaitsenõukogu seisukohalt tähistab isegi IKÜM-i kohane õigus saada koopia töödeldavatest isikuandmetest ainult võimalust saada juurdepääs isikuandmetele koopia vormis.[99] Euroopa Kohtu kohtujurist märkis otsesõnu, et IKÜM art 15 lg 3 esimene lause ei anna üldist õigust saada dokumentide koopiaid või andmebaaside väljavõtteid.[100] Samuti järeldab autor Euroopa Kohtu otsusest, et piisab andmete taasesitamisest täielikult ja täpselt[101]. Põhiline on, et andmetöötleja valitud muu vorm on andmesubjektile sama arusaadav kui koopia.[102]

Lisaks on küsimus, mida tähendab termin „koopia“. ÕKAD kasutab põhjenduses 43 terminit „andmed“, mille kohta võib esitada täieliku kokkuvõtte; terminit „teave“, mida tuleb eelnimetatud kokkuvõttes esitada ning terminit „isikuandmed“, mille kohta võib esitada kokkuvõtte töödeldavate isikuandmete koopiana. Euroopa Komisjon on kohtuasja raames esitanud seisukoha, et termin „koopia“ puudutab dokumendis sisalduvaid isikuandmeid ja andmesubjektile väljastatav koopia peab seega sisaldama kõiki töödeldavaid isikuandmeid, et ta saaks enda õigusi teostada.[103] Analoogia korras IKÜM-i terminikasutusega saab välja tuua Euroopa Kohtu otsusest, et koopia esitamine puudutab isikuandmeid, mitte muud teavet või muid elemente, nagu metaandmeid[104].

Autori järeldusel võib IKS § 24 lg 1 p-i 1 alusel väljastada ja on soovitatav väljastada töötlemise korral isikuandmete terminiga hõlmatu koopiana ning p-des 2–5 nimetatud andmed või teabe võib väljastada koopiana, kuid piisab andmete esitamisest kujul, mis annab täieliku kokkuvõtte esitamisele kuuluvatest andmetest või teabest. Põhimõtteliselt on nii koopia kui ka täieliku

[97] C-487/21, *F.F.*, p 36–38.
[98] Samas, p 41–42, 45.
[99] Guidelines 01/2022 on data subject rights – Right of Access. Version 2.0. European Data Protection Board. Adopted 28.03.2023. – https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf (05.03.2024), vnr 23 ja vt ka vnr 22, 24–31, 152.
[100] C-487/21, *F.F.*, kohtujurist G. Pitruzzella ettepanek, p 58, 62.
[101] C-487/21, *F.F.*, p 39, 45.
[102] C-141/12, *YS*, p 57–58.
[103] C-487/21, *F.F.*, p 32.
[104] Samas, p 46, 53.

kokkuvõtte andmise piiramine võimalik lähtuvalt üldisest tutvumise õiguse piiramise regulatsioonist IKS § 24 lg-s 2, sealhulgas p-is 2, mis sätestab õiguse piirata tutvumise õigust kui see võib kahjustada teise isiku õigusi ja vabadusi.

2.1.2. Isikuandmete töötlemise ajaperiood

IKS-is pole välja toodud, millise ajaperioodi kohta peab andmesubjekti taotlusel isikuandmete olemasolu kontrollima või neid väljastama. Analoogia korras järeldab autor Euroopa Kohtu tõlgendusest, et IKS-i tutvumise õigus on tagasiulatuv selleks, et andmesubjekt saaks enda tutvumise ja muid õigusi päriselt kasutada[105]. Hõlmatud on kogu andmetöötluse periood ehk põhiandmete säilitamise aeg[106].

Üldiselt, säilitamise tähtaja lühiduse või pikkuse määramisel ning konkreetselt, isikuandmete kohta taotluse saamisel lähtuvalt nende säilitamise tähtaja kehtivusest tuleb arvestada sellega, et andmesubjektil on päriselt võimalus enda juurdepääsuõigust teostada.[107] Autori hinnangul ei saa andmesubjekti puudutavate isikuandmete koosseis põhimõtteliselt muutuda taotluse saamisest kuni andmesubjektile vastamiseni ühe kuu jooksul tulenevalt IKS § 27 lg-st 2.

Eesti õiguse kohaselt tähendab tutvumise õiguse kohaldamine andmekogu näitel põhimõtteliselt selle kohaldumist kõigile andmetöötleja andmekogus töödeldavatele isikuandmetele[108]. Tutvumise õiguse teostamisel ei oma tähendust, kus asuvad isikuandmed või teave nende töötlemise kohta. Euroopa Kohtu otsusest lähtuvalt puudutab teabe saamise õigus ka isikuandmete töötlemise toimingute kohta tekkivaid logifaile.[109]

Samuti on Tallinna Ringkonnakohus lahendanud logide väljastamise seoses kaitseõigusega. Nimelt, andmesubjekt võib saada isikuandmeid mittesisaldavaid PPA dokumendihaldussüsteemi logisid andmetöötleja süülise käitumise tõendamiseks, kuid tuleb tähele panna, et selline taotlus lahendatakse teabenõude korras AvTS-i kohaselt, kuna dokumendi liikumise logi andmed pole kogutud kriminaalmenetluse toimingute raames (KrMS § 47 lg 1 p 1 kohane dokumentide nõudeõigus pole erinorm AvTS § 2 lg 2 p 4 tähenduses)[110].

---

[105] Vt EKo C-553/07, *College van burgemeester en wethouders van Rotterdam* versus *M.E.E. Rijkeboer* (edaspidi *Rijkeboer*), ECLI:EU:C:2009:293, p 54.
[106] Samas, p 58.
[107] EDPB Guidelines 01/2022, vnr 38.
[108] Termin „põhiandmed“ on määratletud AvTS § 43^6 lg-s 1; C-553/07, *Rijkeboer*, p 58.
[109] EKo C-579/21, *J.M.* versus *Apulaistietosuojavaltuutettu ja Pankki S* (edaspidi *Pankki S*), ECLI:EU:C:2023:501, p 62–63, 69, 83.
[110] TlnRnKHKo 3-19-743/33, p 15–16, 19–21.

2.1.3. Isikuandmete kategooriad

IKS § 24 lg 1 p-s 1 on sätestatud politseile kohustus teha andmesubjektile teatavaks „asjaomaste isikuandmete kategooriad“. IKS eelnõu koostajate vastavad näited on tervise-, kontakt- ja vanemaid puudutavad andmed.[111] Andmetöötlejal tuleb endal vastavalt andmetöötluse kontekstile määratleda andmesubjektile esitatava teabe sisu.

Isikuandmete kategooriat puudutavalt on Justiitsministeeriumi analüüsis rõhutatud, et seaduses peab olema sätestatud milliseid isikuandmete liike või üldisi gruppe andmekogus töödeldakse[112]. Autor soovib märkida, et üksnes õigusaktis sätestatule viitamisega ei lahenda andmetöötleja korrektselt andmesubjekti juurdepääsuõiguse taotlust. Andmesubjekti tutvumise õigus ei tähenda võimalust tutvuda PS § 3 lg 2 koostoimes §-iga 108 tähenduses avaldatud seadusetekstiga. Andmetöötleja esitatud vastus peab andma individuaalse kontekstipõhise ülevaate isikuandmetest ja kategooriatest, mille alla andmetöötleja neid paigutab.

Võttes arvesse EL-i teisest õigust puudutavaid suuniseid ja tõlgendusi, on autori hinnangul IKS-i kontekstis oluline meeles pidada §-is 18 sätestatud andmetöötleja võimalust „asjakohasel juhul“ määratleda andmesubjekti eri kategooriad. Kategooriat saab eristada „näiteks andmetöötlustoimikutes ja registrites“.[113] Andmesubjekti kategooria võib kattuda menetlusosalise rolliga süüteomenetluses (KrMS § 16 lg 2 või VTMS § 16).

Eelkirjeldatud lähenemine tagab tõhusamalt isikuandmete kaitse vastavalt isikuandmete töötlemise põhimõtetele. Näiteks suures hulgas andmetes võivad olla isikuandmed, mille puhul ei ole koheselt selge nende konkreetne kasutamise eesmärk ja vajadus.[114] Isikuandmete leidmine suurest hulgast andmetest on pika-aegne või nende analüüsi vajadus võib ilmneda pikema aja jooksul seoses kriminaalasjas ilmnenud uute asjaoludega vms, mistõttu võib säilitusperiood tunduda andmesubjektile pikk, kuigi on hinnatud vajalikuks ja proportsionaalseks andmetöötleja poolt[115]. Andmesubjekti vaates on eelkirjeldatu tõttu kahtluse

[111] Isikuandmete kaitse seaduse 679 SE seletuskiri, § 23 lk 29.
[112] Mikiver 2021, lk 34.
[113] Isikuandmete kaitse seaduse 679 SE seletuskiri, § 17 lk 26.
[114] De Hert, P., Sajfert, J. Regulating Big Data in and out of the Data Protection Policy Field: Two Scenarios of Post-GDPR Law-Making and the Actor Perspective. European Data Protection Law Review, Volume 5, Issue 3, 2019. – https://doi.org/10.21552/edpl/2019/3/8 (21.02.2024), lk 339, 342.
[115] Analoogia korras Europoli suhtes tehtud EDPS-i otsus. Vt Decision on the retention by Europol of datasets lacking Data Subject Categorisation (Cases 2019-0370 & 2021-0699). European Data Protection Supervisor. – https://edps.europa.eu/system/files/2022-01/22-01-10-edps-decision-europol_en.pdf (09.04.2024), p 2.13, 3.9, 3.15.

alla seatud juurdepääsu taotluse olemuslik tõhusus just „kriminaalmenetluse raames toimuvas automatiseeritud“ suurte andmehulkade kombineerimise ja „analüüsikeskses“ andmetöötluses[116].

Tutvumise taotlusele vastusena antud teave andmesubjekti kategooriast võimaldab seega täita selle olemuslikku eesmärki ja konkreetselt kontrollida isikuandmete töötlemise õigus- ja seaduspärasust. Ehk, kuidas andmetöötleja on seostanud andmesubjekti „objektiivselt riskiga“, mis võib temast lähtuda ja seega olla aluseks tema andmete töötlemiseks, sealhulgas säilitamiseks[117]. Pidades silmas isikuandmete vaba liikumise põhimõtet, saab rõhutada Euroopa Andmekaitseinspektori seisukohta, et ilma korrektse minimaalsuse põhimõtte rakendamiseta on tõenäoline andmesubjekti ebaõiglane seostamine kuritegeliku tegevusega EL-i tasandil, liikumisvabaduse piiramine EL-is ning era- ja perekonnaelu puutumatuse ülemäärane riive.[118] Kui isikuandmed ei ole seostatud teatud tähtaja jooksul õiguskaitse eesmärgil andmetöötluse ja asjakohase andmesubjekti kategooriaga, on andmesubjektil õigus nõuda isikuandmete parandamist või kustutamist.

2.1.4. Isikuandmete päritolu

IKS § 24 lg 1 p-st 2 tuleneb politseile kohustus esitada andmesubjektile olemasolev teave isikuandmete päritolu kohta. Isikuandmed võivad olla andmetöötleja kogutud või saadud füüsiliselt isikult või avaliku, era- või kolmanda sektori esindajalt. Artikli 29 töörühm on rõhutanud, et andmesubjektile tuleb esitada lisaks teave „kuidas ja mis tingimustel“ andmetöötleja isikuandmed sai ja võimalusel, „mis eesmärgil need edastati“.[119]

ÕKAD-i põhjenduse 43 kolmanda lause kohaselt võib teabe saamisel inimeselt jääda esitamata andmesubjektile teave selle inimese identiteedi kohta, iseäranis olukorras, kus teabe saamine on konfidentsiaalne, nagu tunnistaja puhul. Samaväärselt füüsilise isikuga võib olla vaja kaitsta isikuandmete või nende töötlemisel saadud teabe pärinemist teiselt õiguskaitseasutuselt.

---

[116] Galič, M., Lonneke Stevens, L., Koops, B.-J. Editorial: A trialogue on regulating data-driven criminal procedure. New Journal of European Criminal Law. Volume 14, Issue 4. December 2023. – https://doi.org/10.1177/20322844231213484 (04.02.2024), lk 425–426, 429.
[117] Vt EKo C-817/19, *Ligue des droits humains ASBL* versus *Conseil des ministres*, ECLI:EU:C:2022:491, p 262.
[118] Analoogia korras EDPS-i otsus Europoli suurte andmekogumite saamise ja hoidmise kohta. Vt Decision on the own initiative inquiry' on Europol's big data challenge. 18.09.2020. WW/xx/vm/ D(xxx) xxx C 2019-0370 (edaspidi *C 2019-0370*). European Data Protection Supervisor. – https://edps.europa.eu/data-protection/our-work/publications/investigations/edps-decision-own-initiative-inquiry-europols_en (05.03.2024), p 4.7, 4.9, 4.10.
[119] Artikli 29 töörühm. WP 258, lk 19.

Asjakohane Euroopa Kohtu otsus jäi tulemata seoses eelotsusetaotluse tagasivõtmisega. Selle küsimused puudutasid EL liikmesriigi kriminaalpolitsei keeldumist nimetada andmesubjektile, mis asutus tema kohta politseiregistris julgeolekukontrolli käigus sissekande tegi.[120] Eelnimetatud juhul ei saanud andmesubjekt teostada isegi tutvumise õigust, sest talle polnud teada, kes päriselt tema isikuandmeid töötles.[121] Autori hinnangul on oluline Saksamaa halduskohtu seisukoht, et andmesubjektile isikuandmete päritolu kohta teabe andmata jätmine ja põhjusena üksnes õiguskaitseasutuse üldise kahju tekkimise nimetamine, sealhulgas kohtule, on vastuolus ÕKAD-i andmesubjekti tutvumise õiguse piiramise ning kohtuliku kontrolli sätetega[122].

Eestis toimub eelduslikult vähemalt osa avaliku sektori andmevahetusest andmekogudes, mida puudutavast õigusloomest peaks selguma andmete päritolu ehk andmetöötlejale andmete andjad ja ka temalt andmete saajad. Sageli aga on andmekogude vaheline suhtlus reguleeritud üldistatult.[123] Siinkohal on seda olulisem saada andmesubjektil vastusena tutvumise taotlusele teavet isikuandmete päritolu kohta.

2.1.5. Isikuandmete vastuvõtjad

IKS § 24 lg 1 p-i 4 alusel on politseil kohustus esitada andmesubjektile teave isikuandmete vastuvõtjate või nende kategooriate kohta. Kui isikuandmete saamise (päritolu) puhul tuleb esitada teave isikuandmete saamise kohta avaliku sektori asutuselt, siis vastuvõtmise (vastuvõtja) puhul ei tule esitada teavet isikuandmete edastamisest avaliku sektori asutusele. Avaliku sektori asutusel on õigus võtta vastu isikuandmeid EL-i või riigisisese õiguse alusel ning tema pole „vastuvõtja“ (IKS § 13 lg 1 alusel IKÜM art 4 p 9). Lisaks ei lähe termini „vastuvõtja“ alla andmetöötleja töötaja, kes töötleb isikuandmed tema „alluvuses ja tema juhiste kohaselt“.[124]

Kõneallolevas IKS-i sättes ei ole seadusandja sätestanud teabe andmist vastuvõtjate kohta sama täpsusega, kui ÕKAD-i art 14 p c seda võimaldab. Samuti pole avatud seletuskirjas, mida vastuvõtjad või nende kategooriad tähendavad. [125] Vastavalt ÕKAD-ile saab IKS § 24 lg 1 p-s

[120] Määrus, EK president 09.08.2022, C-481/21, *TX* versus *Bundesrepublik Deutschland*, Verwaltungsgericht Wiesbadeni eelotsusetaotlus – Saksamaa registrist kustutamiseks. – ELT C 422, 18.10.2021.
[121] EK C-481/21, *TX* versus *Bundesrepublik Deutschland,* eelotsusetaotlus, p 26.
[122] Samas, p 27, 34.
[123] Nt Infosüsteem POLIS kohta § 7 lg 1 ja 4. – Politsei andmekogu põhimäärus.
[124] Vt C-579/21, *Pankki S*, p 73 koos p 63 ja 83.
[125] Vt isikuandmete kaitse seaduse 679 SE seletuskiri, § 24 lk 28–29.

4 täpsustada, et teabe esitamine ei puuduta tulevikus teabe saajaid, vaid üksnes teabe saajaid, kellele on isikuandmeid juba avalikustatud. Samamoodi saab täpsustada, et eelkõige võib teabe andmine puudutada kolmandates riikides olevaid vastuvõtjaid või rahvusvahelisi organisatsioone.

Võttes arvesse politsei töö iseloomust tulenevat võimalikku andmevahetust EL-i ja Euroopa Majandusühenduse väliste riikidega ning rahvusvaheliste koostööpartneritega[126], ei saa andmesubjektile vastavat teavet jätta ilma põhjenduseta esitamata. Analoogia korras saab IKÜM-i puudutava Euroopa Kohtu praktika alusel öelda, et kui andmetöötleja on isikuandmeid avalikustanud, on andmesubjektil õigus teada konkreetselt, kes on olnud tema isikuandmete vastuvõtjad.[127] Autori hinnangul on oluline juhtida eelnimetatule tähelepanu sarnaselt IKS § 22 lg1 p 4 juures esitatud seisukohale ning hea praktika loomiseks võimalusel täpsustada asjakohaselt IKS-i sätet.

Alternatiivina vastuvõtjate nimetamisele võimaldab IKS § 24 lg 1 p 4 andmesubjektile nimetada vastuvõtjate kategooriad. Politsei vaates on kategooriate nimetamine eelduslikult eelistatud, sest andmesubjektile ei pea nimetama kõiki vastuvõtjaid. Küsitav on, kas selle piirangu kasutamine sõltub siiski ainult ja näiteks andmetöötleja pingutusest või sarnaselt isikuandmete päritolu puudutavalt ja tulenevalt ÕKAD-i põhjendusest 43, teabe konfidentsiaalsena hoidmise kohustusest[128]. Kui lähtuda analoogia korras Euroopa Kohtu IKÜM-i tõlgendusest, võib üksnes juhul, kui andmesubjekt seda soovib või andmetöötlejal pole vastuvõtjaid võimalik teatavaks teha või need pole veel teada, esitada andmesubjektile teabe vastuvõtjate kategooriate kohta[129].

2.1.6. Isikuandmete töötlemise eesmärk

IKS § 24 lg 1 p-i 3 alusel on politseil kohustus esitada andmesubjektile teave isikuandmete töötlemise eesmärgi kohta. Eesmärgikohasuse põhimõttest sõltub muude, IKS §-is 14 sätestatud isikuandmete töötlemise põhimõtete sisustamine[130]. Eesmärgi kohta teabe saamisel kontrollib andmesubjekt selle seaduslikkust ja seda, kas andmetöötleja on eesmärgi saavutamisel järginud

[126] PPA rahvusvahelised koostööpartnerid. Vt https://www.politsei.ee/et/juhend/rahvusvaheline-koostoeoe. – https://www.politsei.ee/et/juhend/rahvusvaheline-koostoeoe (25.03.2024).
[127] EKo C-154/21, *RW* versus *Österreichische Post AG*, ECLI:EU:C:2023:3, p 43.
[128] Dimitrova, De Hert 2018, lk 119.
[129] C-154/21, *RW*, p 36, 48.
[130] Van der Sloot, B., LED Article 4/C.4. Commentary.

õigsuse, võimalikult väheste andmete kogumise ja säilitamise piirangu põhimõtteid[131]. Lisaks saab ta kontrollida, millise ülesande täitmiseks on politseil lubatud andmeid töödelda isikustatud kujul, sealhulgas kellega ja kuidas vahetada. IKS-is ei ole sätestatud, kuivõrd täpse teabe peab esitama andmesubjektile.

Isikuandmete kasutusõiguse või töötlemise eesmärk määratakse kindlaks üldiselt ja terviklikult, mitte andmesubjekti puudutavalt andmekogus iga töödeldava üksikjuhtumi kohta. Seda olulisem on avalikustada teave põhimõtteliselt isikustamata kujul suures mahus isikuandmete töötlemise ning ühtede ja samade isikuandmete töötlemise kõikide võimalike eesmärkide kohta[132]. Eelkirjeldatud juhul ei pruugi andmesubjektil olla võimalik teostada tutvumise õigust, kui tema isik jääb suurest hulgast andmetest tuvastamata, vaid ta saab teostada õigust saada teavet isikuandmete töötlemise kohta ja üldiselt veenduda andmetöötluse seaduslikkuses.

Andmesubjekti tutvumise õiguse kontekstis on märkimisväärne, et sama või muu andmetöötleja võib töödelda isikuandmeid IKS § 16 kohaselt algsest erineval eesmärgil. Samas ei kohusta andmesubjekti õiguste regulatsioon andma teavet algsest erineval eesmärgil toimuva andmetöötluse ning muutunud andmetöötleja ja õigusliku aluse kohta.[133] Autori hinnangul tuleb kaaluda IKS-i täpsustamist, et tagada andmesubjektile teabe saamine vastavalt võimalusele tegelikust eesmärgist ja andmetöötlejast. Igal juhul tuleb andmetöötlejal võimaluse korral anda teavet laiemalt, kui algse eesmärgi kohta[134].

Andmesubjekti saab esitada „mõistliku ajavahemiku“ järel taotlusi korduvalt ning erinevatele andmetöötlejatele. Tegemist on ÕKAD-ist tuleneva võimalusega teostada korrapärast kontrolli (põhjenduse 43 esimene lause). Siinkohal võib andmetöötleja pidada IKS § 28 lg 3 kohaselt samasisulist taotlust põhjendamatuks või ülemääraseks ning keelduda selle täitmisest (ÕKAD põhjenduse 40 kolmandas lause koosmõjus põhjenduse 43 esimese lausega). Kui aga andmesubjektil pole teavet isikuandmete päritolu või vastuvõtjate kohta, on tal võimalik taotlusi esitada vaid algsele andmetöötlejale. Seega andmesubjekti koormav lahendus ei pruugi olla ka otstarbekas.

Lisaks on autori hinnangul oluline märkida Justiitsministeeriumi avaliku sektori andmekogude regulatsioonide analüüsi tulemust. Selle kohaselt „näib olevat vastuolus andmekogude

[131] Dimitrova, De Hert 2018, lk 118.
[132] Bogdanov. D., Siil, T. Infotehnoloogilised võimalused põhiõiguste kaitsel. – Juridica 2020/6, lk 480.
[133] Dimitrova, De Hert 2018, lk 118.
[134] Vt EKo C-180/21, *VS* versus *Inspektor v Inspektorata kam Visshia sadeben savet*, ECLI:EU:C:2022:967, p 63.

ulatusliku ristkasutuse ja andmete ühekordse küsimise“ ja eesmärgikohasuse põhimõte.[135] Seega järeldab autor üldiselt, et andmesubjektile eesmärgi kohta selge vastuse andmise eeldus on laiem andmetöötluse proportsionaalsuse analüüs ja õigusloome võimalik korrastamine, et ära hoida sisuliselt[136] ja tehniliselt[137] võimalikku ulatuslikumat andmete kogumist ning edasist töötlemist. Andmesubjekt ei pruugi tutvumise õiguse alusel saada ammendavat teavet eesmärgi kohta ega ennast puudutava andmetöötluse näitel osata hinnata andmetöötluse seaduslikkust.

2.1.7. Isikuandmete töötlemise õiguslik alus

IKS § 24 lg 1 p-i 3 alusel on politseil kohustus esitada andmesubjektile teave isikuandmete töötlemise õigusliku aluse kohta. IKS ega ÕKAD pole sätestanud, kuivõrd täpne peab õigusliku aluse kohta esitatav teave olema. Artikli 29 töörühma seisukohalt peab antav teave olema „õige, selge ja piisav“, et andmesubjekt saaks kinnituse õigusliku aluse kohta.[138]

Põhiõiguse riive puhul on riigil kohustus läbi viia riive kontroll, mis Alexy kohaselt lõppeb üldjuhul põhiseadusjõuga õiguste kaalumisega.[139] Andmesubjekti vaates on just õiguslikus aluses sisustatud kaalumise tulemus. Küsimus on, millisel juhul on isikuandmete kaitse riive seadusandja ja PS-i vaates proportsionaalne.[140] Kuna isikuandmete kaitse õigus tuleneb EL-i õigusest, on asjakohane kontrollida õigusliku aluse vastavust ELPH-le.[141] Isikuandmete kaitse riive on õigustatud üksnes seaduslikul alusel ja proportsionaalsel juhul mõne muu ühiskondlikult kaitstava hüve kaitseks, kui koosmõjus on täidetud ELPH art 52 lg 1 ning PS §-i 11 ja §-i 26 teises lauses sätestatud tingimused. Eelnimetatu on andmesubjekti isikuandmetega tutvumise õiguse peamine eesmärk: kontrollida ennast puudutava andmetöötluse seaduspärasust (ÕKAD-i põhjenduse 43 esimene lause).

Kõneallolevalt võib andmesubjektil olla keeruline hinnata andmetöötluse proportsionaalsust, kui selles ei toeta teda õiguslik alus ise ega selle tõlgendused. Euroopa Kohtu otsuse kohaselt peab isikuandmete töötlemist sätestav õiguslik alus seaduses olema „tervikuna piisavalt selge

---

[135] Analoogia korras IKÜM-i põhiselt vt Mikiver 2021, lk 26.
[136] Nn *mission creep* ehk kättesaadavate isikuandmete kasutamine kogumise eesmärgist ulatuslikumalt vt Artikkel 29 töörühm. WP203, lk 4.
[137] Nn *function creep* ehk tehnoloogia võimaldatud andmete ulatuslikum töötlemine: Collins English Dictionary. HarperCollins Publishers. – https://www.collinsdictionary.com/dictionary/english/function-creep (26.11.2020)
[138] Artikli 29 töörühm. WP 258, lk 19.
[139] Alexy. R., Põhiõigused Eesti põhiseaduses. – Juridica 2001/ eriväljaanne , p 8.1.1.1.
[140] Kalmo, H., Kask. O., PSK § 11/33. – Eesti Vabariigi põhiseadus. Kommenteeritud vlj. 2020.
[141] Vt Euroopa Liidu põhiõiguste harta kohaldamine õigusaktides ja poliitikakujundamises riigi tasandil. Suunised. Euroopa Liidu Põhiõiguste Amet 2020. – https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-charter-guidance_et.pdf (05.03.2024), lk 67–79.

ja täpne“ ning ise määrama kindlaks põhiõiguste „harta artiklitega 7 ja 8 kaitstud põhiõiguste riive ulatuse“, mis ei välista piisavalt lahtist sõnastust, et „kohaneda erinevate juhtumite ja muutuvate asjaoludega“.[142] Samas pole Euroopa Kohus sageli ka ise õiguslikku alust tõlgendades esitanud andmesubjektile selget vaadet tema põhiõiguse riive lubatud ulatusest, sest analüüsitud pole nõudeid õiguslikule alusele samaaegselt proportsionaalsuse ja just seaduslikkuse põhimõtte koosmõjus.[143] Siiski on hiljutisest vastupidine näide, mis võib aidata laiemalt analoogia korras määratleda õiguskaitse eesmärgil toimuva isikuandmete töötlemise riive „asjaolusid“ ja „tingimusi“ sätestava õigusnormi piisavat selgust ja täpsust[144].

Autori juhib tähelepanu asjaolule, et isegi, kui andmesubjektile nimetatakse õiguslik alus, võib tal tõenäoliselt selle üldsõnalisuse või puudulikkuse[145] tõttu jääda saamata või arusaamatuks enda õiguste teostamiseks vajalik teave. Politseil on vaja vastuses andmesubjekti taotlusele selgitada võimalikult täpselt isikuandmete töötlemist osas, milles õigusaktis sätestatud õiguslik alus ei vasta ettenähtud sisulistele või vormilistele nõuetele.

2.1.8. Isikuandmete säilitamise tähtaeg

IKS § 24 lg 1 p-i 5 kohaselt on politseil kohustus esitada andmesubjektile teave kavandatava isikuandmete säilitamise tähtaja või säilitamise tähtaja määramise aluste kohta. Teabe saamisel on andmesubjekti kontrolli ese tähtaja „asjakohasus“ ehk hinnang, kas isikuandmete säilitamine on töötlemise eesmärgi saavutamiseks jätkuvalt vajalik[146]. Lisaks on võimalik kontrollida säilitatavatele isikuandmetele riigisiseses õiguses ettenähtud tehniliste ja korralduslike turvameetmete proportsionaalsust.[147] Teabe saamine säilitamise tähtaja kohta on eelduseks andmesubjekti isikuandmete kustutamise nõude esitamisele IKS § 25 lg-s 3 ettenähtud juhtudel.

Euroopa Kohus on rõhutanud, et riigisiseses õiguses ei pea sätestama isikuandmete säilitamisele rangeid ajalisi piire, „mille ületamise korral tuleks andmed automaatselt kustutada“.[148] Samuti on Euroopa Kohus leidnud seoses andmetöötlusega EL liikmesriigi

[142] C-817/19, *Ligue des droits humains*, p 114 koos seal viidatud kohtupraktikaga, 140.
[143] Vt EK C-118/22, *NG* versus *Direktor na Glavna direktsia „Natsionalna politsia“ pri Ministerstvo na vatreshnite raboti – Sofia*, ECLI:EU:C:2023:483, kohtujurist P. Pikamäe ettepanek, p 45 ja selles toodud viite nr 42 teine lause.
[144] C-817/19, *Ligue des droits humains*, p 117–118, 135, 139, 146, 180 teine lause, 183, 187 (selguse ja täpsuse nõuet ning proportsionaalsuse ja seaduslikkuse põhimõtet puudutavalt).
[145] Nt Infosüsteemi POLIS puudutavalt vt Mikiver 2021, lk 32.
[146] C-118/22, *NG*, p 45–46.
[147] Samas, p 57.
[148] Samas, p 52.

politseiregistris ilma säilitamise vajaduse korrapärase ülevaatamise nõudeta, et isegi süüdimõistetud isikuga kaasnevale ohule antud hinnang lähtuvalt tema toimepandud kuriteo laadist ja raskusest või korduvuse puudumisest ei pruugi tingimata õigustada tema isikuandmete säilitamist kuni tema surmani ning igal juhul peab riigisiseselt tagama andmesubjektile õiguse nõuda isikuandmete kustutamist.[149]

Sarnaselt on Euroopa Kohus otsustanud, et kui andmesubjektiga pole (tema isikuandmete kogumise ajahetkel) seostatud kuriteokahtlust, siis pole põhjendatud tema isikuandmete säilitamine sarnaselt andmesubjektiga, kellest lähtub või kellega seondub kuriteo toimepanemise objektiivne oht[150]. Samas, andmesubjekti kategooria muutumine võib tingida vajaduse muuta säilitamise tähtaega.[151] Seoses andmetöötluse eesmärgi muutumisega on vaja andmesubjektil teadvustada, et tal on lisaks esialgse eesmärgi kohasele säilitamise tähtajale õigus saada andmetöötlejalt teavet muul kui algsel eesmärgil töödeldavate isikuandmete säilitamise tähtaja kohta.[152] Andmesubjektil tuleb ka arvesse võtta, et andmetöötlejal on võimalik tähtaja lõppemisel säilitada andmeid edasi anonümiseeritult, mille osas andmesubjekti juurdepääsuõigus pole enam teostatav.

2.1.9. Isikuandmete parandamise ja kustutamise õiguse kohta teabe esitamine

IKS § 24 lg 1 p-i 6 kohaselt peab politsei andmesubjektile teada andma õigusest „taotleda“ ebaõigetel faktidel põhinevate isikuandmete parandamist ja mittetäielike isikuandmete täiendamist ja kogutud isikuandmete kustutamist või isikuandmete töötlemise piiramist, nagu näeb ette IKS § 25. Autor märgib siinkohal IKS-i erisuse, mille kohaselt pole andmesubjektil õigus nõuda, vaid andmetöötlejal on õigus piirata isikuandmete kustutamise asemel nende töötlemist IKS § 25 lg-s 4 sätestatud juhtudel. Andmesubjektil on teabe saamisel esitada vajaduse korral uus taotlus, milles ta nõuab konkreetsete toimingute tegemist enda isikuandmetega või saab andmetöötleja läbi viia toiminguid olemasoleva taotluse lahendamise raames, võttes arvesse kohustust toimingutele eelnevalt andmesubjektiga suhelda.

[149] Samas, p 32, 60, 67, 72.
[150] Vt nt C-817/19, *Ligue des droits humains*, p 248, 251, 255, 262.
[151] Vt ka Dimitrova, LED Article 14/A.3. Commentary.
[152] Dimitrova, De Hert 2018, lk 120.

2.2. Andmesubjektile teabe esitamine automatiseeritud otsuse tegemise kohta

IKS ei kohusta § 24 lg-ga 1 andma andmesubjektile teavet IKS § 21 lg 1 kohase automatiseeritud töötlusel põhineva otsuse, sealhulgas profiilianalüüsi (edaspidi koos ka *automatiseeritud otsus*) tegemise kohta. ÕKAD-i automatiseeritud otsuste regulatsiooni on peetud selguse ja ranguse tõttu andmesubjekti õigusi tugevalt tagavaks regulatsiooniks[153]. Samas andmesubjektile kõnealloleva teabe mitte esitamist on peetud ÕKAD-i andmesubjekti õiguste regulatsiooni probleemiks.[154] Eelkirjeldatu tõttu analüüsib autor vajadust esitada IKS-i tutvumise õiguse raames andmesubjektile teavet automatiseeritud otsuse tegemise kohta.

Nii ennetav kui ka kriminaalteabe põhine politseitöö meetod põhineb aina enam andmetel ja nende analüüsil[155]. Tehnika areng loob eeldused automatiseeritud andmetöötluseks. Euroopa Liidu Põhiõiguste Amet (FRA) peab vajalikuks tugevaid kaitsemeetmeid, et automatiseeritud andmetöötlus koostoimes inimkäelisega, sealhulgas andmete kogumisel, analüüsimisel ja andmesubjektile võimalikke tagajärgi toovate otsuste vastuvõtmisel ei tooks kaasa ebaseaduslikku andmetöötlust ja diskrimineerimist.[156] Eelnimetatud nõuded andmetöötlejale on sätestatud IKS § 21 lg-s 3–4. Andmesubjekt peaks saama kontrollida, kas teda puudutav otsus on seaduslik ja mittediskrimineeriv. Märkimisväärne on, et IKS § 21 kohaldub üksnes automatiseeritult tehtud otsusele. Kui andmetöötlus hõlmab inimkäelist tegevust, kohalduvad muud IKS-i sätted[157].

Küsimus on, mis osas on automatiseeritud töötlus isikuandmete töötlemine. Hiljuti tõdes Euroopa Kohtu kohtujurist, et automatiseeritud analüüsi käigus töödeldakse isikuandmeid.[158] Tehniliselt suhestatakse erinevaid andmesubjekte nende isikuandmete põhjal eelnevalt määratud hindamiskriteeriumite kaudu ning sellist automatiseeritud suhestamist peetakse teaduskirjanduses otsustusprotsessi loogikaks, millele kohaldada andmesubjekti juurdepääsuõigust.[159] Automatiseeritud otsus ise ei pruugi isikuandmeid sisaldada, kuna võib üksnes väljendada isikuandmete põhjal saadud positiivset või negatiivset vastavust eelnevalt

[153] ÕKAD art 11 ja IKÜM art 22 võrdluse kohta vt Sajfert, Quintel 2017, lk 9.
[154] Dimitrova, De Hert 2018, lk 127.
[155] Vt Seadusliku aluseta profiilide koostamise tõkestamine nüüd ja tulevikus: juhend. Euroopa Liidu Põhiõiguste Amet (edaspidi *FRA juhend*) 2022. – https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-preventing-unlawful-profiling-guide_et.pdf (05.03.2024).), lk 18–19.
[156] Samas, lk 22.
[157] ÕKAD-i art 11 kohta vt Sajfert, Quintel 2017, lk 8–12.
[158] EK C-817/19, *Ligue des droits humains ASBL* versus *Conseil des ministres*, ECLI:EU:C:2022:65, kohtujurist G. Pitruzzella ettepanek, p 230.
[159] Ausloos, Mahieu, Veale 2020, p 48.

määratud hindamiskriteeriumitele. Samuti ei ole hindamiskriteeriumid tagasiviidavad konkreetse inimeseni. Igal juhul jõutakse isikuandmeid töödeldes automatiseeritud otsustusprotsessi tulemusel otsuseni.

Euroopa Kohtu praktikas pole olnud selgust, kuivõrd puudutab tutvumise õigus andmesubjekti suhtes võetud otsust, seahulgas tema profiili (sisendandmed, üksikasjalik teave töötluse loogika kohta, põhjenduse kokkuvõte ja selle põhjal võetud lõppotsus) või üksnes õigust saada üldist teavet automatiseeritud otsustusprotsessi loogika ja algoritmi töö kohta.[160] Kuigi sellise analüüsi aluseks olevate eelnevalt kindlaks määratud kriteeriumite alusel loodud profiile ei pea Euroopa Kohtu kohtujurist vajalikuks avalikustada, peab läbipaistvuse tagamiseks olema nende rakendamise tulemus jälgitav.[161] Eelnimetatud arvamust täpsustas Euroopa Kohus, leides, et andmesubjektile tuleb teha arusaadavaks vastavate kriteeriumite ja neid rakendavate algoritmiliste programmide toimimine, mitte ei tule tingimata võimaldada tal tutvuda nende kriteeriumite ja programmidega.[162] Tutvumine puudutaks ka teaduskirjanduse põhjal isikuandmete töötlemise kohta käivat teavet, mille andmetöötlejad jätavad sageli tähelepanuta keskendudes juurdepääsu andmisel isikuandmetele.[163]

Küsimus on ka, millisel õiguslikul alusel saab andmesubjekt teavet. Ta peab olema võimeline esitama andmetöötlejale IKS § 21 lg-s 2 nimetatud vastuväite. Asjakohane ÕKAD-i art 11 lg 1 rõhutab „vähemalt“ otsese isikliku kontakti saamist ning koosmõjus põhjenduse 38 teise lausega peab sobivaks kaitsemeetmeks „konkreetse teabe“ ja selgituse andmist automatiseeritud otsuse kohta. Üldiselt loetakse andmesubjekti juurdepääsuõiguste regulatsiooni läbipaistvamaks ja andmesubjekti õigusi paremini tagavamaks kaitsemeetmetest, mis on sätestatud automatiseeritud otsuse regulatsioonis.[164] Seega on mõeldav, et tutvumise õiguse raames saab andmesubjekt teavet automatiseeritud otsuse kohta. Kõnealleolevas küsimuses on Euroopa Kohtu praktika vähene või ei käsitle andmesubjekti tutvumise õiguse kohaldumist. Teaduskirjanduses on sobivaks peetud andmesubjekti tutvumise õiguse regulatsiooni, mitte näiteks haldus- või kriminaalõiguse kohaselt teabe saamist.[165]

[160] Dimitrova 2020, lk 229.
[161] C-817/19, *Ligue des droits humains*, kohtujurist G. Pitruzzella ettepanek, p 228.
[162] C-817/19, *Ligue des droits humains*, p 210.
[163] Ausloos, Mahieu, Veale 2020, p 54.
[164] Dimitrova, D. The Right to Explanation under the Right of Access to Personal Data: Legal Foundations in and Beyond the GDPR. European Data Protection Law Review, Volume 6, Issue 2 (2020). – https://doi.org/10.21552/edpl/2020/2/8 (18.03.2024), lk 216.
[165] Dimitrova 2020, lk 216–217, 222.

Kohaldada võib IKS § 24 lg 1 p-i 1 ja 2 alusel koosmõjus §-iga 21 andmesubjekti õigusele saada teada tema kohta koostatud automatiseeritud otsuse aluseks olevatest kriteeriumidest ja otsuse põhjendusest, kuna tal õigus saada teavet käimasoleva andmetöötluse ja isikuandmete päritolu kohta.[166]

ÕKAD-i tõlgendamisel on siiski leitud, et tema vahetu õigusmõju puudumisest ja põhjenduse mittesiduvast olemusest tulenevalt ei peaks andmesubjekti tutvumise õiguse regulatsiooni pidama aluseks õigusele saada teavet automatiseeritud otsuse kohta.[167] Seda väljendab IKÜM-i art 15 p-le h sarnase sätte puudumine IKS § 24 lg-s 1. Andmesubjekt peaks enda õigusi tagama kohtulikus kontrollis. Nimelt Euroopa Kohus leidis, et kaebuse puhul peab kohtul ja puudutatud isikul olema võimalik tutvuda kõikide põhjenduste ja tõenditega, mille alusel automatiseeritud otsus tehti, sealhulgas eelnevalt kindlaksmääratud hindamiskriteeriumite ja neid kriteeriume kohaldavate programmide toimimisega.[168] Tutvumise õiguse raames ei pruugi andmetöötlejal olla võimalik esitada andmesubjektile teavet automatiseeritud otsuse kohta samaväärselt kui kohtule.

Kuigi pole välistatud tutvumise õiguse raames võimalusel teabe esitamine, peab kehtiva arusaama kohaselt andmesubjekt saama teavet muul viisil kui enda esitatud taotluse alusel. Küsimus on, millisel määral on võimalik pidada asjakohaseks avalikult teabe kättesaadavaks tegemist (IKS § 22) või andmesubjekti teavitamisel teabe esitamist (IKS § 23). Leitud on, et andmetöötleja on kohustatud esitama eelnimetatud alustel teavet automatiseeritud otsuse kohta.[169] Artikli 29 töörühm on rõhutanud võimalust anda vastavat teavet „eriti juhul, kui isikuandmed on kogutud andmesubjekti teadmata“, milleks automatiseeritud otsused sageli on.[170]

Eelnimetatust lähtuvalt saab andmesubjektile esitada teabe automatiseeritud otsuse kohta vähemalt konkreetsel juhul koos lisateabega õigusliku aluse, andmete säilitamise tähtaja ja vastuvõtjate kategooriate kohta IKS § 23 lg 1 p-i 5 alusel. Lisaks pole välistatud üldiselt tarkvara kontrolli eesmärgil automatiseeritud otsuse, mitte täpse algoritmi loogika kohta teabe kättesaadavaks tegemine.[171] Autori hinnangul saab selguse huvides täiendada IKS § 22 lg 1 loetelu kohustusega avalikustada üldine teave automatiseeritud töötlusel põhineva otsuse kohta.

[166] Vt ÕKAD art 14, art 14 p a ja art 14 p g ning art 11 näitel Dimitrova 2020, lk 211, 214, 218.
[167] Vt Sajfert, Quintel 2017, lk 10.
[168] Vt C-817/19, *Ligue des droits humains*, p 211.
[169] ÕKAD-i art 13 tõlgenduse kohta vt Sajfert, Quintel 2017, lk 10.
[170] ÕKAD art13 lg 2 p d osas vt Artikli 29 töörühm. WP 258, lk 15.
[171] Dimitrova, De Hert 2018, lk 120.

3. ANDMESUBJEKTI VAHETU JUURDEPÄÄSUÕIGUSE PIIRAMINE

3.1. Vahetu juurdepääsuõiguse piiramise tingimused

Kuigi näiliselt peab andmesubjekt saama teostada juurdepääsu õigust teabele ja enda kohta käivatele isikuandmetele „iseenesest" piiramatult, omab see õigus piirangut[172]. Iseäranis õiguskaitse eesmärgil toimuva andmetöötluse raames andmesubjekti õiguste tagamine nõuab P. De Herti ja V. Papakonstantinou arvates paindlikku lahendust, mis võimaldab eemalduda kohustusest tagada täielikult andmesubjekti õigused.[173] Politsei saab kohaldada piirangut enda otsusel, ent üksnes mitmete eelduste täitmisel.

Andmesubjekti tutvumise õiguse piirangu kohaldamine peab Dimitrova kohaselt vastama konkreetsetele tingimustele, võttes arvesse ÕKAD art 15 lg-s 1 sätestatut:

1) piirangu alus on riigisiseses õiguses sätestatud seadusandlik meede;
2) piirang kohaldub sellises „ulatuses ja seni, kuni" see on selliselt „vajalik ja proportsionaalne meede";
3) piirangu kohaldamisel arvestatakse konkreetse andmesubjekti „põhiõigusi ja õigustatud huve nõuetekohaselt", pidades silmas ELPH art 52 lg-s 1 sätestatut ning Euroopa Kohtu ja Euroopa Inimõiguste Kohtu praktikat;
4) piirang kaitseb vähemalt ühte eesmärki, mis on sätestatud riigisisese õiguse seadusandlikus meetmes.[174]

Eesti seadusandja on kasutanud ÕKAD-is ettenähtud võimalust sätestada tutvumise õiguse piirang. Järgnevalt analüüsib autor IKS § 24 lg 2–5 vastavust seadusandliku meetme tingimustele, mis tulenevad ÕKAD art 15 lg 1–2. Seoses muude IKS 4. peatüki 3. jaos sätestatud andmesubjekti õiguste piiramisega esitab autor magistritöö eesmärgi ja mahu piirangu tõttu üksnes tähelepanekud, arvestades, et IKS § 24 lg-ga 2 on samasõnaline isikuandmete töötlemisest teavitamist puudutavalt IKS § 23 lg 2 ning IKS § 24 lg-s 2 sätestatud asjaolu kohaldamisele viitab isikuandmete parandamist või kustutamist puudutavalt IKS § 25 lg 6. Andmetöötleja otsuse vaidlustamise regulatsioon on sama IKS § 24 lg-s 4 ja § 25 lg-s 7.

[172] Õiguse välisteooriast lähtuvalt õiguse piiri ehk piirangu kohta vt Ernits, M. Põhiõigused, demokraatia, õigusriik. Tartu: Tartu Ülikooli Kirjastus 2011, lk 156–157.
[173] De Hert, P., Papakonstantinou, V. The New Police and Criminal Justice Data Protection Directive: A First Analysis (2016). – https://ssrn.com/abstract=3447072 (05.03.2024), lk 9 ja 12.
[174] Dimitrova, LED Article 15/B.1. Commentary.

3.1.1. Piirangu seadusandlik meede

IKS § 24 lg 2–3 kohaselt on võimalik andmetöötlejal täielikult või osaliselt piirata andmesubjekti tutvumise õigust. Täpsemalt võimaldab IKS § 24 lg 2 esitada sama paragrahvi lg-s 1 „nimetatud teabe hiljem, piirata selle esitamist või keelduda selle väljastamisest" (edaspidi koos ka *piiramine*). Piiramine peab põhinema andmetöötleja arusaamal, et andmesubjekti tutvumise õiguse täielik tagamine IKS § 24 lg-s 1 ettenähtud kujul võib takistada, kahjustada või ohustada IKS § 24 lg 1 p-des 1–5 nimetatud asjaolu.

Lisaks on kõneallolevas IKS §-is 24 täpsustatud lg-ga 3 andmesubjekti teavitamise korda piirangu seadmisest ja selle põhjustest ning sama paragrahvi lg-ga 5 sätestatud eelnimetatu dokumenteerimise kohustus. Samuti näeb IKS § 24 lg-s 4 ette andmesubjekti teavitamise õigusest pöörduda andmetöötleja otsuse vaidlustamiseks AKI või kohtu poole.

IKS § 24 lg 2 kohaselt võib andmesubjekti tutvumise õigust piirata „seaduses sätestatud juhtudel". IKS § 24 lg 2 ei anna põhjendatult muud võimalust, kui ette näha tutvumise õiguse piirangu võimalikud juhud seadusandja poolt tulenevalt PS § 44 lg 3 teisest lausest koosmõjus § 65 p-ga 1. Lisaks võib piirangu alus tuleneda vahetult kohalduvast EL-i teisesest õigusaktist.

ÕKAD võimaldab täpsustada piirangut igal liikmesriigil endal. Selliselt sõltub piirangu sisustamine ja kohaldamine konkreetses ühiskonnas kehtivatest väärtushinnangutest[175]. IKS § 24 lg 2 ei sätesta sõna-sõnalt nagu ÕKAD art 15 lg 1, et piirangut võib kohaldada „põhiõigusi ja õigustatud huve nõuetekohaselt arvestades" ning „seni, kuni selline piiramine on demokraatlikkus ühiskonnas vajalik ja proportsionaalne meede". IKS seletuskirjas on kajastatud ÕKAD-i põhjenduse 44 teist lauset, mille kohaselt tutvumise õiguse piirangu rakendamine tähendab proportsionaalsuse hindamist üksikjuhtumi ja individuaalse juurdepääsu taotluse põhiselt[176]. Autori hinnangul peab IKS § 24 lg-tega 2–3 seaduse tasandil tagama, et andmesubjekti õiguse piiramise aluseks olev seadusandlik meede pole Dimitrova sõnade kohaselt „absoluutne" ega „suvaline"[177].

Artikli 29 töörühm ei pea võimalikuks, et riigisisese õigusega saaks kohaldada piiranguid üldiselt ja vahet tegemata kõikide andmesubjektide kõikidele taotlustele kogu tutvumise õiguse

[175] Täpsemalt väärtusjurisprudentsist vt Narits, R. Jurisprudentsi põhijoontest. – Juridica 1995/9, lk 378–380; R. Narits. Eesti õiguskord ja väärtusjurisprudents. – Juridica 1998/1, p 1 lk 2–6.
[176] Isikuandmete kaitse seaduse 679 SE seletuskiri, § 23 lk 29.
[177] Dimitrova, LED Article 15/A. Commentary.

ulatuses või konkreetse taotluse puhul kogu juurdepääsuõiguse suhtes, kui piirang on põhjendatud üksnes osale juurdepääsust[178]. De Hert ja Papakonstantinou täheldavad, et piirangu kohaldamine ei saa muuta andmesubjekti tutvumise õiguse regulatsiooni mõttetuks.[179]

Samuti rõhutas Euroopa Kohus hiljuti IKÜM-i teise isiku õiguste ja vabaduse kui piirangu asjaolu osas, et andmesubjekti tutvumise õiguse ja teise isiku õiguste ja vabaduse kaitse vahel kaalumine „ei tohiks" viia täieliku tutvumise õiguse piiramiseni, vaid leida tuleb põhiõigusi tasakaalustav lahendus.[180] Riigikohus on just andmesubjekti õiguste piiramise kontekstis ka leidnud, et iga piirangu alus peab sisaldama teatud kaalutlusõigust, sest vastupidisel tõlgendamisel „toob see kaasa põhiseadusvastase tulemuse".[181] Lisaks on Riigikohus selgitanud IKS-i varasema redaktsiooni puhul, et teise isiku õiguste ja vabanduste kontekstis tuleb proportsionaalsuse analüüsil tuvastada, kas juurdepääsuõiguse andmisega kaasneb riive teise isiku õigustele ning seejärel kaaluda, kas kaalukam on andmesubjekti juurdepääsuõiguse riive või juurdepääsuõiguse andmisel tekkiv teise isiku õiguse riive.[182]

Siinkohal märgib autor, et teaduskirjanduses on algatatud arutelu selle üle, millist meetodit kasutada proportsionaalsuse ja vajalikkuse hindamisel. ELPH art 52 lg-s 1 on ette nähtud meede, mille abil hinnata proportsionaalsuse põhimõtte kohaselt isikuandmete kaitse riive põhjendatust selle järgi, kas see on vajalik lähtuvalt EL-i „üldist huvi" pakkuvast eesmärgist või teiste isikute õiguste ja vabaduste kaitsest. Andmesubjekti juurdepääsuõiguse piirang ei tohi olla otseselt või kaudselt teda diskrimineeriv või tema muid põhiõigusi ja vabadusi ülemääraselt riivav. Euroopa Kohus on tunnustanud isikuandmete kaitsele piirangu seadmisel rangelt vajalikuga piirdumist.[183]

Eelnimetatust tulenevalt toob R. Gellert välja kehtiva arusaama, et proportsionaalsuse test sisaldab endas tasakaalustamist[184]. Samuti märgib L. Dalla Corte, et hinnangu läbiviimist lihtsustab asjaolu, et isikuandmete kaitset puudutavalt on proportsionaalsuse hindamine olemuslikult kinnistunud nii esmases kui ka teiseses EL-i õiguses.[185] Täpsemalt tähendab see

[178] Artikli 29 töörühm. WP 258, lk 20.
[179] De Hert, Papakonstantinou 2016, lk 13.
[180] C-487/21, *F.F.*, p 44.
[181] RKHKo 3-16-2348/21, p 18.
[182] Samas, p 18.
[183] Vt EKo C-362/14, *Maximillian Schrems* versus *Data Protection Commissioner*, ECLI:EU:C:2015:650, p 92.
[184] Gellert, R. Discussion On Risk, Balancing, and Data Protection: A Response to van der Sloot. – European Data Protection Law Reviev Volume 3, Issue 2 (2017). – https://doi.org/10.21552/edpl/2017/2/7(04.02.2024), lk 182.
[185] Täpsemalt Dalla Corte, L., On proportionality in the data protection jurisprudence of the CJEU. International Data Privacy Law, Volume 12, Issue 4, November 2022. – https://doi.org/10.1093/idpl/ipac014 (04.02.2024), lk 260.

üldise proportsionaalsuse põhimõtte ja põhiõiguste kohaldamise kui kaalumise näitel R. Alexy kohaselt piirangu aluses nimetatud asjaolule antavat väärtuse kaalumist muu põhiõiguse, printsiibi, normi või eesmärgiga.[186] Van Der Sloot aga leiab, et erinevaid huve ei peaks kaaluma ja tasakaalustama, vaid prioriseerima ja hierarhiasse seadma.[187] Muu hulgas toetub ta enda arusaamale EL-i teisesest andmekaitseõigusest, mis põhimõtteliselt ei tunne ega vaja kaalumise terminit[188].

Autor piirdub magistritöö eesmärgi ja mahu piirangu tõttu tõdemusega, et tasakaal isikuandmete kaitse ja andmetöötleja taotletava eesmärgi ehk piirangu asjaolu tagamise vahel tuleb leida lähtuvalt kehtivast arusaamast proportsionaalsuse testi osas. Autor toetab seisukohta, et üldine probleemkoht võib olla selles, et andmetöötlejal „puudub sageli" teadmine ja oskus sellise õigusliku hinnangu läbiviimiseks.[189] Analoogia korras IKÜM-i alusel andmesubjekti tutvumise õiguse piiramist puudutavalt on Riigikohus meelde tuletanud, et seadusandliku meetme olemasolu ei anna õigust „piirata andmesubjekti õigusi vahetult seaduse alusel", vaid vastav alus annab kaalutlusõiguse.[190] Kõnealloleva seaduse säte andis Rahapesu Andmebüroo juhile õiguse „kehtestada teabele juurdepääsu piirangu". Riigikohus tõlgendas vastavat alust selliselt, et see võimaldab asutuse juhil ka piirata andmesubjekti õigusi.[191] Küsimus on seega teadmistes ja arusaamades, kuidas kohaldub piirang individuaalsele juhtumile. Ebaseaduslik on piirangu kohaldamine üldiselt ja vahet tegemata, lähtudes üksnes seaduses antud võimalusest.

Euroopa Kohtu praktika toetab proportsionaalsuse hindamist praegu vähesel määral. Dalla Corte on leidnud, et ebaselgust loob ebaühtlane ja mittekonkreetne kohtupraktika.[192] Lisaks märgib autor, et kohtupraktika konkreetselt õiguskaitse eesmärgil andmetöötluse ja andmesubjekti õiguste tagamise osas on alles kujunemas.[193] Pole välistatud, et andmetöötlejad annavad riigisiseselt või riikide võrdluses sarnastes olukordades erineva hinnangu andmesubjekti tutvumise õiguse piiramise võimalikkusele.

---

[186] Täpsemalt Alexy, R. Kollisioon ja kaalumine kui põhiõiguste dogmaatika põhiprobleemid. – Juridica 2001/1, lk 5–8, 11–12.
[187] Van Der Sloot, B. Editorial. European Data Protection Law Review, Volume 3, Issue 1 (2017). – https://doi.org/10.21552/edpl/2017/1/3 (30.03.2024), lk 2.
[188] Täpsemalt samas, lk 3–4, 6 ja 10.
[189] Analoogia korras. Vt Kolza, D., Drechsler, L. Proportionality has come to the GDPR (9 December 2020). – https://europeanlawblog.eu/2020/12/09/proportionality-has-come-to-the-gdpr/ (30.03.2024), p 5.
[190] RKHKo 3-20-332/39, p 12.
[191] Samas, p 11.
[192] Dalla Corte 2022, lk 260.
[193] Vt EK eelotsusetaotluse etapis C-57/23, *JH* versus *Policejní prezidium* ja C-280/22 *Kinderrechtencoalitie Vlaanderen and Liga voor Mensenrechten* versus *Belgia* ning EKo C-118/22, *NG*; C-333/22 *Ligue des droits humains*; C-205/21, *V. S.*, menetluses osales *Ministerstvo na vatreshnite raboti, Glavna direktsia za borba s organiziranata prestapnost*, ECLI:EU:C:2023:49; C-180/21, *VS.* Vt otsing EK veebilehel DPcuria.eu märksõnaga „Law Enforcement Directive" (30.03.2024); vt ka C-481/21, *TX,* tagasi võetud eelotsusetaotlus.

Siinkohal tekib küsimus, kuivõrd on piirangut sätestava seadusandliku meetme rakendamise proportsionaalsuse hindamine võimalik, vähemalt esmajoones, PS § 149 kolmanda lause kohaselt põhiseadusliku järelevalve raames. Piirangu asjaolusid peab täpsustama riigisiselt ning IKS § 24 lg-s 2 nimetatud piirangu aluseks olevad asjaolude rakendamine pole EL-i õiguses täielikult reguleeritud. Võttes arvesse EL-i õiguse esimust, ühtsust ja tõhusust PS-i ees, Euroopa Kohtu tõlgendust ELPH-st ja Eesti kohustust tagada EL-i õiguse täielik toime, võib tõhusama õiguskaitse tõttu Riigikohtu kohaselt analüüsida riigisisese sätte põhiseaduspärasust ja kooskõla EL-i õigusega riigisisese põhiseaduslikkuse järelevalve raames.[194] Euroopa Kohtule eelotsusetaotluse esitamise asemel pole välistatud PS-ist lähtumine ja PS § 149 tähenduses Riigikohtus asja lahendamine, kui riigisisese sätte rakendamine ei ole täiel määral reguleeritud EL-i õigusega.

IKS § 24 ei saa näha ega ka näe ette võimalust piirata andmesubjekti õigust üldjuhul, vaid üksnes ja ainult erandjuhul, mille peab seadusandja olema sätestanud seaduses, arvestades, et piirangut saab kohaldada individuaalsel juhul vastavuses seaduslikus aluses sätestatud piirangu ulatuse ja selles nimetatud asjaoludega. Lisaks ei saa tutvumise õiguse piiramine olla igal võimalikul juhul lõplik. IKS § 24 lg-s 2 tähistab andmesubjektile teabe esitamise osalist piirangut võimalus esitada teave ajaliselt „hiljem“ või „piirata selle esitamist“ ning täielikku piirangut tähistab võimalus teabe esitamisest „keelduda“. Autori hinnangul tuleb tähele panna, et piirang ei pruugi kohalduda kogu IKS § 24 lg-s 1 loetletud teabele ühetaoliselt. See tähendab, et olenevalt teabe sisust võib kohalduda täielik või osaline piirang. IKS-is ei ole seevastu sõnaselgelt sätestatud, et teabele kohalduv piirang ei ole ajalises ega teabe sisu vaates lõplik.

Piirangu vajadus ja proportsionaalsus võivad järk-järgult või korraga ära langeda. Vastavale aspektile viitab otseselt ÕKAD art 15 lg 1 sõnastus „seni, kuni“. Kui piirangu asjaolu langeb ära, tuleb põhimõtteliselt andmesubjektile esitada piiranguga hõlmatud isikuandmed või teave nende töötlemise kohta. IKS ei sätesta, milline on eelnimetatud olukorras andmesubjekti õiguste tagamise korra erisus tavapärasest korrast. Küsimus on, kuidas tagada pidev või vähemalt teatud ajavahemiku järel toimuv piirangu aluse äralangemise kontroll ning mis on teavitamise tähtaeg alates põhjuse äralangemisest. Autori hinnangul võimaldab IKS § 24 lg 2 sõna-sõnalt tõlgendamine andmetöötlejal ebaproportsionaalselt piirata andmesubjekti tutvumise õigust, mistõttu tuleb kaaluda sätte täpsustamist piirangu võimaliku ulatuse ja kehtivusaja osas.

[194] RKÜKo 5-19-29/38, p 41, 43, 45–47.

3.1.2. Piirang tutvumisele isikuandmete ja nende töötlemise liikidega

Piirangu seadmine on võimalik teatud eesmärkide saavutamise vajaduse tõttu (ÕKAD art 15 lg 1) ja teatud eesmärkide kaitseks või huvides (PS § 44 lg 3 teine lause). Seadusandlikus meetmes peab seega sätestama eesmärgi, mis võimaldab tutvumise õigust piirata. Iga sellise eesmärgi kohaldumist tuleb politseil hinnata eraldi, lähtuvalt isikuandmetest ja teabest nende töötlemise kohta. Korraga saab kehtida üks või mitu eesmärki.

IKS-i kohaselt võib andmesubjekti tutvumise õiguse piirang olla vajalik

1) riigi tuumikfunktsiooni[195] tagamisel seoses
   a) süüteo tõkestamise, avastamise või menetlemise või karistuse täideviimise takistamise või kahjustamisega (IKS § 24 lg 2 p 1);
   b) riigi julgeoleku ohustamisega (IKS § 24 lg 2 p 3);
   c) avaliku korra kaitse ohustamisega (IKS § 24 lg 2 p 4);
   d) ametliku uurimise või menetluse takistamisega (IKS § 24 lg 2 p 5) või
2) teise isiku õiguste ja vabaduste kahjustamisega seoses (IKS § 24 lg 2 p 2).

IKS § 24 lg 1 p-des 1–5 nimetatud asjaolu kattub põhimõtteliselt ÕKAD art 15 lg 1 p-des a–e nimetatud eesmärgiga. See tähendab, et seadusandja on üle võtnud kõik viis võimalikku EL-i teisese õiguse loetelus ette nähtud andmesubjekti tutvumise õiguse piiramise põhjendust. Vastav loetelu asjaoludest on IKS-is põhjendatult kinnine. Loetelu ei võimalda võtta piirangu aluseks muid eesmärke, sealhulgas ELPH art 52 abiga üldist avalikku huvi pakkuvat olulist eesmärki[196]. IKS § 24 lg-s 2 ei ole seadusandja sätestanud uusi, ÕKAD-ist puuduvaid tutvumise õiguse piirangu aluseid.

IKS § 24 lg 2 sätestab, et tutvumise õigusele võib seada piirangu „seaduses sätestatud juhtudel“, mitte näiteks sõnastuses „käesolevas või muus seaduses sätestatud juhtudel“ või „käesolevas seaduses nimetatud tingimustel“. IKS-i kõneallolevas sättes pole hinnatud konkreetsete töödeldavate isikuandmete ja nende töötlemise toimingute ning nende töötlemise kohta käiva teabe kaupa, millised piirangu asjaolud on asjakohased ning proportsionaalsed. Seadusandja pole ühegi asjaolu kohaldumist seadnud sõltuvusse täiendavatest või täpsustatud eeldustest.

[195] Riigivõimu teostamise tähenduses PS § 3, § 10, § 13 ja § 14; Madise, PSK § 3/2.
[196] Vt Euroopa Liidu põhiõiguste harta. Selgitused põhiõiguste harta kohta. Euroopa Põhiõiguste Amet. – https://fra.europa.eu/et/search?search_api_fulltext_3=selgitused+p%C3%B5hi%C3%B5iguste+harta+kohta+ / (12.03.2024).

Samuti ei leia seletuskirjast IKS-i eelnõu koostajate selgitusi, mida täpsemalt üks või teine asjaolu tähendab või mis tingimustel seda on võimalik kohaldada.[197]

IKS § 24 lg 2 kohta kehtib üheselt Euroopa Komisjoni kriitika, et liikmesriigid järgivad ÕKAD art 15 üldist sõnastust[198]. Euroopa Komisjon ei pea selliselt sätestatud piirangu asjaolu enda tahet väljendavaks, sest ilma eriseaduses asjaolusid ja tingimusi täpsustamata on andmetöötlejal „piirangute kohaldamisel kaalutlusõigus".[199] Dimitrova ja De Hert on teatud liikmesriigi õiguse näitel rõhutanud, et „küllaltki lai" määratlus võimaldab ulatuslikku kaalutlusõigust.[200] Küsimus on seega IKS-iga andmetöötlejale jäetud liiga laias kaalutlusõiguses. Eelnimetatust tulenevalt pole IKS § 24 lg 2 sätestatud piisavalt selgelt ja täpselt, et seda kohaldada iseseisvalt piirangu alusena.

IKS eelnõu koostajad on ÕKAD-i ja IKS-i eelnõu kohaste sätete võrdlustabelis nimetanud üksnes seoses isikuandmetega tutvumise õiguse piiramisega isikuandmete töötlemise liikide põhiselt, et seadusandlik meede tuleb rakendada eriseadustes „[v]astavalt valdkonnaspetsiifilistest vajadustest"[201]. Seaduseelnõu juurde koostatud seletuskirjas eelnimetatut ei rõhutata, kuid eriseadustes üldise piirangu aluse sätestamise vajadus ilmneb IKS RS-i menetlusest IKÜM-i näitel.[202] IKS eelnõu koostajate eelnimetatud tahe ilmneb IKS-iga seoses laiemalt ja sõna-sõnalt eriseaduses piirangu asjaolude sätestamist puudutava muudatusettepaneku põhjendusest: „Uue IKS-i §-id 23–25 sätestavad üldisi aluseid andmesubjekti õiguste piiramiseks, kuid iga konkreetsel juhul peab piirangute rakendamise võimalikkus tulenema seadusest."[203]

Arutelukohta ei ole seega selles, et piirangu aluseks olev asjaolu tuleb sätestada täpsemalt eriseaduses tulenevalt täpsemast eesmärgist ja ülesandest, mille täitmise käigus politsei isikuandmeid töötleb. Samas ei saa autori hinnangul jätta magistritöös tähelepanuta IKS-i

[197] Vt isikuandmete kaitse seaduse 679 SE seletuskiri, § 23 lk 28–29.
[198] Vt Esimene aruanne õiguskaitse valdkonnas isikuandmete kaitset käsitleva direktiivi (EL) 2016/680 (õiguskaitsedirektiiv) kohaldamise ja toimimise kohta. Komisjoni teatis Euroopa Parlamendile ja nõukogule COM/2022/364 final. 25. juuli 2022. – https://ec.europa.eu/info/publications/communication-commission-european-parliament-and-council-first-report-application-and-functioning-data-protection-law-enforcement-directive-eu-2016-680-led_et (05.03.2024), lk 15.
[199] Samas, lk 15.
[200] Dimitrova, De Hert 2018, lk 122.
[201] Isikuandmete kaitse seaduse 679 SE seletuskirja lisa 1, lk 15–16. – https://www.riigikogu.ee/download/74b9da11-92a6-443e-8aaa-d455b2ba73cb (13.04.2024).
[202] Isikuandmete kaitse seaduse 679 SE seletuskiri, § 23 lk 28–29; analoogia korras, sest IKÜM art 23 ei ole otsekohalduv säte. Vt isikuandmete kaitse seaduse rakendamise seaduse 778 SE seletuskiri, § 44 lk 54–55.
[203] Pöördumine õiguskomisjoni poole seoses eelnõuga 680 SE. JuM 28.01.2019 kiri nr 10-4/720-1. – https://www.riigikogu.ee/download/1b65d0fe-cec0-4571-ab45-b8f6b0524c5e (13.04.2021), lisa lk 13.

analüüsi ja täpsustamise vajadust niivõrd, kuivõrd on vaja piirangu aluse mõistes üldseadust täpsustada. Lisaks, võttes arvesse aspekti, et kehtivast IKS-ist ei nähtu vajadust täpsustada eriseaduses piirangu aluseid. Eelnimetatu võimaldab autori hinnangul ka eriseaduses sätestada piirangu alused üldiselt ehk mittevastavuses EL-i õiguse mõttega.

Kui kehtivas õiguses on tegemist ebapiisava regulatsiooniga, on puuduste kõrvaldamiseni autori hinnangul siiski otstarbekas vajaduse korral ja individuaalsete juhtudel kohaldada andmesubjekti tutvumise õiguse piiramisele analoogia korras jätkuvalt IKS-ile ainuomaseid sätteid. Eriti juhul, kui IKS-i alusel on piiratud andmesubjekti tutvumise õigust täielikult ja vastava piirangu aluseks olev asjaolu ei ole ära langenud pärast andmetöötluse lõppemist kriminaalmenetluse või laiemalt õiguskaitse eesmärgil.

IKS-ist § 24 ei nähtu andmesubjekti tutvumise õiguse piiramise regulatsioonist sätet, millega on ÕKAD-i art 15 lg 2 tähenduses „määratud kindlaks isikuandmete töötlemise liigid, mille suhtes võib täielikult või osaliselt kehtida“ IKS § 24 lg-s 2 nimetatud üks või mitu asjaolu. Eelnimetatud ÕKAD-is sätestatud võimaluse puhul on tegemist väärarusaama tekitava sättega, mistõttu autor märgib järgmist. Dimitrova ja De Hert rõhutavad, et ilma konkreetse ja vastupidise Euroopa Kohtu tõlgenduseta võib säte jätta mulje võimalusest seadusandlikus meetmes üldvolitusega eelnevalt kindlaks määrata isikuandmete töötlemise liigid, mille suhtes kehtib edaspidi alaliselt tutvumise õiguse piirang.[204] Näiteks on liikmesriikide ÕKAD-iga mittevastav praktika, kui seadusandliku meetmega keelatakse vahetu ja võimaldatakse üksnes kaudne juurdepääsuõigus teatud isikuandmete liikidele või juurdepääs teatud infosüsteemide teatud tüüpi andmete kategooriatele.[205] Ehk taas on oluline meeles pidada põhimõtet, et ÕKAD ei võimalda sätestada riigisiseselt seadusandlikku meedet, mille alusel ilma igasuguse individuaalse üksikjuhtumi põhise hindamiseta on võimalik otsustada andmesubjekti tutvumise õiguse puudumise üle.

[204] Dimitrova, D., De Hert, P. The LED's right of Access to one's data: Loopholes on proper access, legality review and data protection authority. Accountability. New Journal of European Criminal Law 2023, Volume 0(0), pp 1–21, lk 11–12. – https://doi.org/10.1177/20322844231214484 (05.02.2024); individuaalsete piirangute võimalikkuse kohta vt Artikli 29 töörühm. WP 258, lk 18.
[205] Dimitrova, LED Article 15/C.2. Commentary.

3.2. Piirangu asjaolud

3.2.1. Õiguskaitse eesmärk, riigi julgeolek, avalik kord ja ametlik uurimine või menetlus

Õiguskaitse eesmärgil toimuval andmetöötlusel on „konkreetne laad“, millele on Euroopa Kohus hiljuti tähelepanu juhtinud muu hulgas seoses tutvumise õiguse piiramisega[206]. See on andmetöötlus süüteo tõkestamise, avastamise või menetlemise või karistuse täideviimise eesmärgil. Samal eelnimetatud eesmärgil võib politsei isikuandmetega tutvumist ka piirata IKS § 24 lg 2 p-i 1 alusel.

IKS-is sätestatud asjaolu ei erine sisuliselt ÕKAD art 15 lg 1 p-s b sätestatud eesmärgist, võttes arvesse, et ÕKAD-is sätestatud võimaluse on seadusandja üle võtnud Eesti õigusruumi sobival kujul. See tähendab, selle piirangu aluse kohaldamise analüüs kattub magistritöös esitatud analüüsiga IKS-i kohaldamisala osas, arvestades KrMS-i erisustega (vt 1.1).

Riigi julgeoleku ja põhiseadusliku korra tagamine vajab kaitset julgeolekuasutuste seaduse[207] (JAS) § 1 lg 1 alusel seoses julgeolekuasutuste[208] ülesannete täitmise või täitmise tagamisega. Andmesubjekti tutvumise õiguse piiramisega seoses riigi julgeoleku ohustamisega näeb ette IKS § 24 lg 2 p 3 kooskõlaliselt ÕKAD art 15 lg 1 p-ga d. Siinkohal on oluline tähelepanu pöörata üldisele piirangu kohaldamise aluseks oleva seadusandliku meetme ja selle kohaldamise, sealhulgas põhjendamise nõudele. Euroopa Kohtu menetlusest tagasivõetud eelotsusetaotluse raames oleks selgunud seisukoht küsimuses, kas ÕKAD-i art 15 on kooskõlas riigisisese õiguse säte, mis seab andmetega tutvumise õiguse andmise tingimuseks andmetöötlejale „andmekaitseõiguslikku vastutust kandva asutuse nõusoleku“.[209] See tähendab, kuivõrd on põhjendatud andmesubjekti juurdepääsuõiguse piiramise üle otsustada näiteks julgeolekuasutusel ise, politsei eest ja nimel.

Dimitrova sõnul ei tähenda piirangu alus julgeolekuasutuse õigust seda ühepoolselt seada. [210] Autor toetab eelnimetud seisukohta. Küsimus pole erinevate andmetöötlejate hinnangute võrdluses ja ühe ülimuslikkuses teise üle. Pädeva andmetöötleja hinnang on esmatähtis, sest temal on asjakohase asjaolu hindamise pädevus. Samas tuleb meeles pidada andmetöötleja

[206] C-333/22, *Ligue des droits humains,* p 42.
[207] Julgeolekuasutuste seadus. – RT I, 31.12.2022, 11.
[208] JAS § 5 tähenduses Kaitsepolitseiamet ja Välisluureamet.
[209] C-481/21, *TX,* eelotsusetaotlus, p 19 ja 26.
[210] Dimitrova, LED Article 15/C.1. Commentary.

õigusi ja kohustusi, sealhulgas põhimõtet tagada proportsionaalsus andmesubjekti taotluse lahendamisel. Isegi, kui tegemist on riigi julgeoleku kaitseks ettenähtud asjaoluga, on selle kohaldamist vaja hinnata igal üksikul juhul individuaalselt ning vastavalt võimalusele seotud andmetöötlejate koostöös.

IKS-i 4. peatüki kohaldamisalas ei ole isikuandmete töötlemine riigi julgeoleku tagamisel.[211] Magistritöö eesmärgi ja mahu tõttu piirdub autor üldiste tähelepanekutega. Edasist täpsemat analüüsi vajab küsimus, kuidas andmesubjekti tutvumise õiguse piiramise regulatsioon IKS § 24 lg-s 2–5 suhestub JAS § 21^1 lg-ga 3–4 koostoimes muude asjakohaste sätetega.

Avaliku korra kaitset puudutavalt on seadusandja võimaldanud piirata politseil andmesubjekti tutvumise õigust IKS § 24 lg 2 p-ga 4, mis on vastavuses ÕKAD art 15 lg 1 p-ga c, arvestades, et asjaolu sõnastamisel on sõna „julgeolek" asendatud Eesti õigusruumi sobiva sõnaga „kord". Politsei võib olla andmetöötlejana nii korrakaitseorgan kui õiguskaitseasutus. Andmesubjekti tutvumise õiguse taotluse lahendamisel on oluline eristada, vastavalt millisel asjaolul on vaja kohaldada politseil piirangut õiguskaitseasutuse pädevuses ja millal muus pädevuses.

Ametliku uurimise või menetluse takistamise tõttu andmesubjekti tutvumise õiguse piiramist võimaldav IKS § 24 lg 2 p 5 ei erine tervikvaates ÕKAD art 15 lg 1 p-s a sätestatud eesmärgist. Ainsa erisusena ei ole IKS-is võimaldatud piirangu seadmist „õiguslike päringute" takistamise vältimiseks. Murekoht on selles, et pole aru saada, millise ametliku uurimise või menetluse takistamist on seadusandja silmas pidanud (vt ka magistritöö 3.8). Andmetöötlejal on Dimitrova kohaselt sellise „üldise" ja „ebamäärase" sõnastuse tõttu liiga lai kaalutlusõigus.[212] Autor täheldab eelkirjeldatust tulenevalt, et vaja on täpsustada IKS § 24 lg 2 p-s 5 sätestatud piirangu asjaolu ning vastavalt muuta või täiendada sätte sõnastust, sealhulgas sätestada, kuivõrd ja kellele kohaldub kõneallolev piirangu alus osas, mis ei ole hõlmatud kitsa kohaldamisalaga IKS § 24 lg 2 p-ga 1.

3.2.2. Teise isiku õigused ja vabadused

Õiguskaitse eesmärgil toimuvas andmetöötluses ei ole puudutatud andmesubjektid ühetaoliselt kursis andmetöötlusega. Teise isiku õiguste ja vabaduste kahjustamise võimaluse tõttu tutvumise õiguse piiramist on politseile vaja tulenevalt andmetöötluse olemusest. Vastava

[211] Isikuandmete kaitse seaduse 679 SE seletuskiri, § 11 lk 20.
[212] Dimitrova, LED Article 15/C.1. Commentary.

piirangu aluse sätestab IKS § 24 lg 2 p-ga 2 kooskõlaliselt ÕKAD art 15 lg 1 p-ga e. Alus ei anna võimalust piirata andmesubjekti tutvumise õigust tema enda kaitseks.

Õiguskaitse eesmärgil andmetöötlus võib puudutada menetlusosalisi kriminaalmenetluses, nagu kahtlustatav, süüdistatav ning nende kaitsja, kannatanu, tsiviilkostja ja kolmas isik (KrMS § 16 lg 2) või väärteomenetluses, nagu menetlusalune isik ja tema kaitsja (VMTS § 16). Samas võib olla tegemist avaldajaga, kes on andnud teavet politseile seoses süüteoasjaga, ent ei ole ise menetlusosaline. Piirangu seadmise analüüsi lihtsustab andmesubjekti kategooriast lähtumine. Autor nõustub Dimitrova näitega, mille kohaselt juurdepääsu võib võimaldada tunnistajale, kes on teadlik andmetöötlusest, aga piirata kahtlusalusele, kes ei pruugi veel teadlik olla enda isikuandmete töötlemisest[213].

Piirangu aluses nimetatud teise isiku õigusi ja vabadusi tuleb tõlgendada laialt, lähtuvalt Riigikohtu otsusest. See tähendab, et piirangu alusega on hõlmatud nii isikuandmete kaitse kui ka „mistahes õigusnormile tuginev subjektiivne õigus".[214] Riigikohus on ajakohastanud PS § 44 lg 3 teisest lausest tulenevaid IKS-ist kitsamaid asjaolude sõnastusi, mis viitavad piirangu aluse kohaldamisele seoses „kuriteo tõkestamise, kurjategija tabamise või kriminaalmenetluses tõe väljaselgitamise huvidega". Piirangu kohaldamine pole seotud kitsalt KarS-is süüteokoosseisuna määratletud teoga.[215] Riigikohus on seoses korruptsiooni juhtumist teavitamisega leidnud, et juba isikuandmeid sisaldav teavitamise fakt saab kaitse isegi, kui teavituse sisu ei puuduta korruptsioonisüütegu[216].

IKS-i kõnealloleva sättes on asendatud ÕKAD-is kasutatud sõna „kaitse" sõnaga „kahjustamine". Tekib küsimus, kuivõrd peab ÕKAD silmas laiemat kaitset, kui üksnes kahju ehk negatiivne mõju isikule. Põhimõtteliselt saab kohaldada alust kahju saabumisest varasemas etapis. Riigikohus on kinnitanud, et juba isiku õiguste ja vabaduste kahjustamise võimalikkus on aluseks piirangu kohaldamisele.[217]

[213] Dimitrova, LED Article 6/C.1. Commentary.
[214] RKHKo 3-16-2348/21, p 18.
[215] Samas, p 19.
[216] Samas, p 18–19.
[217] Samas, p 18.

3.3. Andmesubjekti isiku tuvastamine tutvumise õiguse piirangu asjaoluna

IKS § 27 lg 4 sätestab politseile kohustuse tuvastada „andmesubjekti isik“. Autor peab võimalikuks kõnealloleva IKS-i sätte ning Dimitrova ja De Herti toodud riigisisese õiguse näitel analoogia korras küsida, kas andmesubjekti isiku tõsikindlalt tuvastamata jäämisel, kuna ta ei esita piisavalt lisateavet, on tegemist tema juurdepääsuõiguse piirangu alusega ning omakorda, kuivõrd on vastav lähenemine kooskõlas ÕKAD-iga[218]. Lisaks on küsimus, kas tuvastamata jäänud isiku teavitamine on olukord, millele kohaldub IKS § 24 lg 3, sest tema tutvumise õigust on piiratud.

Andmesubjekti isik on politseil vaja tuvastada enne, kui tema taotluse alusel isikuandmete töötlemist kontrollida. Anonüümse isiku kohta ei ole võimalik isikuandmete töötlemist kontrollida. Isikusamasust on võimalik tõestada kas reaalse identiteedi, nime ja isikut tõendava dokumendi või digitaalse identiteedi, määratud pseudotunnuse, IP-aadressi, küpsiste vms[219], samuti esindusõigust tõendava dokumendi abil. Isikusamasus on tuvastatud, kui see on „usaldusväärselt, piisavalt ja sarnaste olukordade vaates võrreldavalt“ tuvastatud.[220]

Tuvastamisega seoses ei ole välistatud erinevate ohtude realiseerumine, nagu

- keegi esitleb end andmesubjektina või andmetöötleja edastab taotlejale andmesubjekti mittepuudutavad andmed[221], mille tulemusel rikutakse turvanõudeid loata juurdepääsu andmise tõttu;
- andmetöötleja viib läbi ülemäärase isikusamasuse kontrolli, riivab ülemääraselt eraelu puutumatust ning rikub andmete töötlemise minimaalsuse ja säilitamise piirangu põhimõtet ebavajaliku või -kohase teabe küsimise[222] tõttu, samuti kui ta seab nõudeid, mis ei ole andmesubjektile ettenähtavad[223] või

[218] Vt Dimitrova, De Hert 2018, lk 122.
[219] Boniface, C. (et al.). Security Analysis of Subject Access Request Procedures How to authenticate data subjects safely when they request for their data. APF 2019 - Annual Privacy Forum, Jun 2019, Rome, Italy. – https://hal.inria.fr/hal-02072302 (18.03.2024), lk 12.
[220] Varik, H.. E-identiteet Eesti ja Euroopa Liidu õigusruumis: Euroopa Parlamendi ja Nõukogu eidentimise ja e-tehingute jaoks vajalike usaldusteenuste määruse kohaldamine Eestis – kujunemislugu, probleemid ja eelseisvad väljakutsed. Magistritöö. – Tallinn: Tartu Ülikool, 2015, lk 8–9.
[221] Vt Vogiatzoglou, P. (et al.). From Theory To Practice: Exercising The Right Of Access Under The Law Enforcement And PNR Directives. 11 (2020) Journal of Intellectual Property, Information Technology and E-Commerce Law 274 para 1. – https://www.jipitec.eu/archive/issues/jipitec-11-3-2020/5191 (18.03.2024), p 74 lk 295.
[222] Nt teise isiku kontaktandmed. Vt samas, p 74 lk 295.
[223] Nt tõend elamisõiguse kohta. Vt samas, p 80 lk 296, p 86 ja 89 lk 297.

- andmetöötleja keelab põhimõtteliselt ebaproportsionaalselt juurdepääsu, kui taotlus ei vasta nõuetele, sealhulgas autentimise nõuetele.[224]

Artikli 29 töörühm on leidnud, et andmesubjekti isikuandmetega tutvumise õigust tuleb rakendada olenemata riski tasemest, mis sellise andmetöötlusega kaasneb.[225] Eelnimetatust võib järeldada, et andmesubjekti juurdepääsuõigust tuleb pidada ülimuslikuks ja põhjendatud kahtluse olemasolu isikusamasuses pigem ebatõenäoliseks. IKS § 27 lg 4 sätestab seevastu üldise kohustuse, mis tähendab vahet tegemata igal juhul vastava toimingu läbiviimist. Seadusandja on sätet sõna-sõnalt tõlgendades jätnud andmetöötlejale laia kaalutlusruumi. Seda vaatamata ÕKAD art 12 lg-le 5, mis andmesubjekti õiguste teostamise üldises korras sätestab võimaluse „põhjendatud kahtlusel" isiku „isikusamasuse suhtes" nõuda andmesubjektilt lisateavet.[226]

Hinnanguliselt esineb andmesubjekti juurdepääsuõiguse ärakasutamist.[227] Euroopa Andmekaitsenõukogule esitatud ettepanekus on J. Ausloos, R. Mahieu ja M. Veale IKÜM-i näitel leidnud, et juurdepääsu taotlemisel on isikusamasuse tuvastamise tõendamiskoormus kõige kõrgem, võrreldes kustutamise, andmete töötlemisele vastuväite esitamise ja piiramise taotlemisega[228]. P. Vogiatzoglou jt järeldasid muu hulgas ÕKAD-i kohase tutvumise õiguse teostamise uuringu järel, et andmesubjekti, autori täiendusel ka andmetöötlejat, võib aidata andmekaitse järelevalveasutustega koostöös välja töötatud isikuandmetega tutvumise taotluse näidisvorm, kus andmetöötleja on õiguskonformselt palunud kõiki isikuandmeid ja teavet, mida on vaja isikutuvastuseks ja taotluse lahendamiseks ning nimetanud selle esitamise kanali[229].

Sageli võib olla isiku tuvastamise meetodiks allkirjastatud taotluse nõue. Analoogia korras märgib autor seisukoha Eesti kohtupraktikast seoses kriminaal- või kohtutoimikust andmete väljastamisega, võttes arvesse, et sellest andmetöötlusest on andmesubjekt teadlik. Nimelt teabenõude esitamisel AvTS § 14 lg 2 alusel on tunnustatud isikusamasuse tõendamist allkirjaga üksnes teise isiku asutusesiseseks kasutamises mõeldud andmete taotlemisel ja leitud,

[224] Autori kohandatud kolm ohuolukorda. Vt algallikas Boniface, C. (et al). 2019, lk 1 ja 3–4.
[225] Statement on the role of a risk-based approach in data protection legal frameworks. Article 29 Data Protection Working Party. 14 EN/WP218. Adopted 30.05.2014. – https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf (09.04.2024), p 2.
[226] Selgituste puudumise kohta vt isikuandmete kaitse seaduse 679 SE seletuskiri, § 26 lk 31.
[227] Nt Carson, A., Fake DSARs: They're a thing? – https://iapp.org/news/a/fake-dsars-theyre-a-thing/ (03.04.2024).
[228] Vt Ausloos, Mahieu, Veale 2020, p 127–128.
[229] Vogiatzoglou, P. (et al.) 2020, p 92 ja 94 lk 298.

et pole õiguspärane keelduda teabe väljastamisest, mis pole asutusesiseseks kasutamiseks mõeldud teave, kuni taotleja ei esita end tuvastada võimaldavaid andmeid[230].

Pöörates tähelepanu õiguskaitse eesmärgil toimuva andmetöötluse iseloomule, töödeldavatele isikuandmetele, andmesubjektide kategooriatele ning IKS § 24 lg-s 2 nimetatud piirangu asjaoludele, on autori hinnangul oluline võimaldada politseile juurdepääsuõiguse andmise eelselt andmesubjekti isiku tuvastamist. Isiku tuvastamise nõue on proportsionaalne üksnes juhul, kui lisateavet või allkirjastatud taotlust palutakse põhjendatud kahtluse korral andmetöötluse ja individuaalse taotluse, nagu taotletud isikuandmete, neid puudutava teabe, infosüsteemi, süüteo lahendamise etapi vms põhiselt ning võimaldatakse andmesubjektile proportsionaalsed isiku tuvastamise lahendused või vastavalt proportsionaalsuse analüüsi tulemusel saadud tingimustele. Autori hinnangul tuleb täpsustada IKS § 27 lg 4, et välistada isiku tuvastamise regulatsiooni ebakonkreetsusest tulenev mittevastavus ÕKAD-i regulatsioonile. Vaja on sätestada kaalutlusõiguse alusena põhjendatud kahtlus või muud tingimused, millal ja kuidas võib andmesubjekti isiku tuvastada, sealhulgas allkirjastatud taotluse alusel.

Eelkirjeldatu võimaldab autori hinnangul pidada andmesubjekti isiku tuvastamist IKS-i nõudena proportsionaalseks ja vastupidisel juhul võimalikuks tutvumise õiguse piiramise lisaaluseks. Üldjuhul ei ole andmesubjektilt lisateabe küsimisel tegemist autori hinnangul IKS § 24 lg 3 olukorraga, kuna andmetöötleja ei pruugi olla andmetöötlust veel või täies mahus kontrollinud, tulenevalt andmesubjekti isiku tõsikindlast tuvastamatusest. See tähendab, pole veel selgust andmetöötluse olemasolus ega selles, kuivõrd on vaja piirata tema tutvumisõigust isikuandmete ja neid puudutava töötlemise teabe osas.

3.4. Andmesubjekti teavitamine tutvumise õiguse osalisest piiramisest

IKS § 24 lg 3 esimeses lauses on sätestatud politsei kohustus teavitada andmesubjekti „viivitamata kirjalikult“ enda otsusest piirata või keelata tutvumise õiguse raames juurdepääs IKS § 24 lg-s 1 nimetatud isikuandmetele ja teabele nende töötlemise kohta ja „selle põhjustest“. Kõneallolev säte peaks looma eeldused teavituse läbipaistvusele, millest sõltuvalt saab andmesubjekt otsustada andmetöötleja otsuse vaidlustamise üle.[231]

[230] TlnHKo 3-19-1076/10, p 6, 11, 14 ja 16; TlnRnKo 3-19-1076/16, p 10–11.
[231] Dimitrova, LED Article 15/C.3. Commentary.

IKS § 24 lg 3 esimene lause tähistab andmesubjekti teavitamist tema tutvumise õiguse osalisest piiramisest. Seda eraldiseisvalt analüüsides on ebaselge, kas seadusandja peab piiramisest teavitamise all silmas täiendavat teavitamist või on tegemist sama teavitusega, mis puudutab IKS § 27 lg 2 kohast teavitamist andmetöötleja tehtud toimingutest andmesubjekti taotluse lahendamise raames. Põhimõtteliselt on tegemist ühe ja sama teavitusega. Selgust on vaja eeskätt selle tõttu, et IKS § 24 lg 3 esimene lause on üldsõnaline ega näe piisavalt selgelt ette andmesubjekti teavituse viisi ja vormi.

Teavitusega saab andmesubjekt teada tema tutvumise õiguse piiramisest ja selle asjaoludest, kuid üksnes niipalju, kui andmetöötleja hinnangu alusel on vaja. Sättes on esitatud täpsustus, et teavitamine on vaja läbi viia „viivitamatult" ja „kirjalikult". IKS § 24 lg 3 esimese lause sõnastus kattub selle ülevõtmise aluseks oleva ÕKAD art 15 lg 3 esimese lausega, millele Dimitrova on ette heitnud üldsõnalisust ja sellest tulenevalt sellega andmetöötlejale antud liiga laia kaalutlusruumi.[232] Autor nõustub märkusega ja märgib sama kõnealloleva IKS-i sätte kohta.

Artikli 29 töörühm on selgitanud, et ÕKAD-is kasutatud mõiste „põhjendamatu viivituseta" tähendab andmesubjekti taotlusele vastamist „niipea kui võimalik, kui teostatav, ühe kalendrikuu jooksul" andmesubjekti taotluse saamisest.[233] IKS § 24 lg 3 esimese lause sõnastuses ei ole sätestaud konkreetset andmesubjektile vastamise tähtaega. Selliselt on võimalik vastata andmesubjektile viivitamatult vastavalt võimalusele. Teavitamise tähtaega täpsustab andmesubjekti õiguste teostamise korda üldiselt sätestav IKS § 27 lg 2, mille kohaselt andmesubjekti teavitamine tuleb läbi viia „põhjendamatu viivituseta ühe kuu jooksul pärast taotluse saamist andmesubjekti taotluse alusel tehtud toimingutest".

Piisava selguse saamiseks andmesubjektile vastamise korra osas tuleb lisaks arvestada IKS § 27 lg-s 1 sätestatud nõudega vastata andmesubjektile „võimaluse korral" tema „soovitud viisil". Nimelt Artikli 29 töörühm näeb ette vastamise samas vormis, kui on esitatud taotlus.[234] Isegi, Artikli 29 töörühm soovitab osalise juurdepääsuõiguse andmisel, see tähendab, mitte keeldumisel, esitada andmesubjektile tema soovi korral ja võimalusel koopia isikuandmetest ja teabest nende töötlemise kohta.[235] Kehtivas õiguses on viide kirjalikult teavitamisele IKS § 24 lg 3 esimeses lauses. Kuna andmesubjekti teavitamine tehtud toimingutest peab olema ÕKAD

[232] Dimitrova, LED Article 15/C.2. Commentary.
[233] Vt ÕKAD art 15 lg 3 esimest lauset ja selle tõlgendust; Artikli 29 töörühm. WP 258, lk 19–20.
[234] Artikli 29 töörühm. WP 258, lk 20.
[235] Samas, lk 20.

art 12 lg 3 kohaselt kirjalik, on autori hinnangul otstarbekas vastavalt täpsustada IKS § 27 lg-s 1 ka üldist korda.

Praktikas võib olla põhjendatud taotlusele vastamise tähtaega pikendada. Tähtaja pikendamise võimalus ei nähtu IKS § 24 lg 3 esimesest lausest ega IKS § 27 lg-st 2. Küsimus on, mitmeid kordi on politseil proportsionaalne esmase ühe kuu järel vastamise tähtaega pikendada ning kuidas on see andmesubjektile ettenähtav. Lisaks ei ole IKS-is ette nähtud korda, kui on vaja piirangu asjaolu kohaldumise osas konsulteerida koostööpartneritega riigisiseselt või rahvusvaheliselt ning vastavalt pädevate asutuste hinnanguid arvestavalt otsus kujundada. Autorile pole arusaadav, miks ka ÕKAD-is pole eelnimetatud regulatsiooni, sealhulgas arvestades, et ÕKAD näeb ette korra isikuandmete töötlemiseks ja vabaks liikumiseks. Õiguskindluse ja selguse huvides saab autori ettepanekul reguleerida tähtaja pikendamist andmesubjekti õiguste teostamise korra üldnormiks olevas IKS § 27 lg-s 2 või eriseaduses, näiteks analoogia korras IKÜM art 12 lg-ga 3, mis võimaldab pikendamist kahe kuu võrra, sealhulgas sätestades erisused seoses piirangust osaliselt hilisema teavitamisega IKS § 24 lg 3 tähenduses. Lisaks on autori hinnangul vaja analüüsida kitsalt tutvumise õiguse raames juurdepääsuõiguse piiramise teavituse korra ühildamist laiemalt andmesubjekti õiguste teostamisele kehtiva korraga. Sageli üksnes IKS § 24 lg 3 esimese lause ja IKS § 27 lg 2 ühisel tõlgendamisel omandavad piirangust teavitamise korda puudutavad sätted minimaalse täpsuse, mis puudutab vastamise vormi, viisi ja tähtaega.

IKS § 24 lg 3 esimesest lausest ei selgu, kuivõrd täpselt on vaja andmesubjektile esitada teave piiramise põhjuste kohta. Euroopa Kohtu seisukohalt on andmesubjekti teavitamisel vaja talle esitada vähemalt teave juurdepääsuõiguse piiramisest või selle keelamisest ning põhjustest, kuid selle esitamine pole üldjuhul piisav.[236] Analoogia korras andmetöötlejale endale kehtiva dokumenteerimise kohustusega IKS § 24 lg-s 5 tuleks eeldada, et andmetöötleja esitab võimaluse korral ka andmesubjektile võimalikult täpselt piiramise faktilised ja õiguslikud alused. Põhimõtteliselt on üldjuhul ebapiisav ja ebaproportsionaalne üksnes IKS § 24 lg 2 p-s 1–5 nimetatud asjaolu väljatoomine, seda põhjuslikult seostamata vastava asjaolu kohaldumisega konkreetse andmesubjekti isikuandmetele ja teabele nende töötlemise kohta. Autori hinnangul tuleb analüüsida ja vastavalt täiendada IKS § 24 lg 3, et täpsustada andmetöötleja piirangust teavitamise kaalutlusruumi.

[236] Analoogia korras ÕKAD art 17 lg 3 kohta vt C-333/22, *Ligue des droits humains*, p 63.

Siinkohal tuleb rõhutada Riigikohtu meenutust andmetöötlejale vajaduse korral üle küsida andmesubjektilt tema juurdepääsu taotlemise põhjus, et tõhusamalt piirangu seadmist kaaluda[237]. Õiguskaitse eesmärgil isikuandmete töötlemisel võib olla suhtlus andmesubjektiga täpsustuste saamiseks keeruline või võimatu: sellega võib andmetöötleja avaldada tahtmatult teavet, mida andmesubjektile pole võimalik avaldada. Siiski ei saa sellist täpsustamist autori hinnangul välistada. Andmesubjekti enda antud selgitustest võib ilmneda, kuivõrd proportsionaalne on piirangu seadmine täielikult või osaliselt või kui üksikasjalikult saab selgitada teavituses piiramise põhjuseid.

3.5. Andmesubjekti teavitamine tutvumise õiguse täielikust piiramisest

IKS § 24 lg 3 teise lause alusel on politseil võimalik tutvumise õiguse piiramise korral „jätta põhjendused esitamata, kui sellise teabe andmine põhjustaks mõne“ sama paragrahvi „lõikes 2 nimetatud asjaolu esinemise“. Eelnimetatu on Artikli 29 töörühma kohaselt „mitte kinnitada ega eitada poliitika“, mis on tutvumise õiguse piiramise erandjuhus[238]. Kõneallolev vastus on Sajferti ja Quinteli sõnastuses „neutraalne“.[239] Kuna vastus on individuaalsele üksikjuhtumile kohandamata, on see sisutühi ja andmesubjektil pole võimalik aru saada, kas tema isikuandmeid töödeldakse või mitte. Analoogia korras on võimalik välja tuua, et Eesti kohtupraktikas on tõdetud neutraalse vastuse andmise võimalikkust. Riigikohus on Kaitseväe korralduse seaduse osas leidnud, et andmesubjekti eest on õigus „isikuandmete töötlemise fakti või ka isikuandmete töötlemise sisu varjata“.[240]

Sellist andmetöötleja äärmuslikku õigust on Dimitrova nimetanud eraldiseisvaks tutvumise õiguse piiramise aluseks.[241] Ehk IKS § 24 lg 2 p-s 1–5 nimetatud asjaolusid täiendavaks asjaoluks, mille sätestamine vastab põhimõtteliselt ÕKAD art 15 lg-s 3 teisest lausest tulenevale andmetöötleja õigusele. Andmetöötlejal on seega võimalus täielikult keelduda isikuandmete esitamisest ja teabe esitamisest nende töötlemise kohta IKS § 24 lg 1 p-de 1–6 tähenduses. Neutraalse vastuse andmisel on võimalik ja tuleb andmesubjekti teavitada õigusest vaidlustada andmetöötleja otsus AKI-s või kohtus, õigusest pöörduda AKI-sse kaebusega, samuti AKI kontaktandmetest. Üldjuhul on autori hinnangul ebatõenäoline, et eelnimetatu või muu IKS § 24 lg 1 ja lg 4 kohase üldise teabe andmine kahjustab andmetöötlust. Autori hinnangul on

[237] RKHKo 3-16-2348/21, p 18.
[238] Artikli 29 töörühm. WP 258, lk 19–20.
[239] Vt Sajfert, Quintel 2017, lk 13.
[240] RKPJKo 5-19-38, p 82.
[241] Vt Dimitrova, LED Article 15/C.3. Commentary.

oluline meeles pidada vajadust hinnata neutraalse teavituse põhjuse püsimist, et võimaluse tekkimisel anda viivituseta andmesubjektile osaliselt või täielikult sisulisem vastus ja vähendada tema tutvumise õiguse täielikust piiramisest tekkivat põhiõiguse intensiivset riivet.

IKS § 24 lg 3 esimene lause sätestab, et teavitama peab „teabega tutvumise piiramisest või sellise teabega tutvumise keeldumisest ja selle põhjustest". IKS § 24 lg 3 teine lause võimaldab „jätta põhjendused esitamata", kuid ei sätesta sõnaselgelt võimalust jätta esitamata teave, kas juurdepääsuõigust on piiratud või on selle andmisest keeldutud. ÕKAD võimaldab art 15 lg 3 esimese ja teise lause koosmõjus jätta esitamata „teabe" nii piiramise, keelamise kui ka nende põhjuste kohta. IKS seletuskirja kohaselt koosneb põhjendus „otsuse faktilistest ja õiguslikest alustest", mis on laiem, kui üksnes „põhjus".[242] Lisaks võib sõna „põhjendused" viidata laiemalt andmetöötleja õigusele põhjendada otsust enda äranägemisel vajalikul viisil. Andmetöötleja neutraalse vastuse sisu on ebaselge ainult esmapilgul.

Autor rõhutab analoogia korras IKÜM-iga, et keelata ei saa andmesubjekti juurdepääsuõiguse teostamist või jätta vastamata andmesubjekti taotlusele. Siinkohal on näiteks liikmesriik, kes 2020. a maikuus peatas valitsuse korraldusega seni esitatud andmesubjekti päringutele vastamise ja uute esitamise kuni koroonaviiruse levikust tingitud hädaolukorra lõpuni. Eelnimetatu osas leidis Euroopa Andmekaitseinspektor, et tegemist on põhiõiguse rikkumisega, kui tutvumise õigust ei ole olemuslikult võimalik ühelgi andmesubjektil ilma erisusteta teostada ning teostamise piirang on ajaliselt ja ulatuse mõistes piiritlemata.[243]

3.6. Andmesubjekti teavitamine otsuse vaidlustamise õigusest

Andmesubjektil on tutvumise õiguse piiramise korral õigus saada andmetöötlejalt teavet enda kaitseõiguse teostamise kohta. IKS § 24 lg 4 näeb politseile ette kohustuse teavitada õigusest „pöörduda otsuse vaidlustamiseks" AKI-sse või kohtusse. AKI-sse pöördumise võimalus on andmesubjekti õiguste piiramise korral kohalduv ÕKAD art 17 lg-s 1 loodud eriõigus. Sellega tagatakse andmesubjekti teadmine võimalusest teostada kaudset juurdepääsuõigust.

Teavitamise kohustuse täitmist on autori hinnangul võimalik seadusandjal sätestada selgemalt. ÕKAD art 17 lg 2 teavituse sisu – õigus „teostada oma õigusi järelevalveasutuse kaudu" –

[242] Isikuandmete kaitse seaduse 679 SE seletuskiri, § 23 lk 29.
[243] Vt Statement on restrictions on data subject rights in connection to the state of emergency in Member States. European Data Protection Board. Adopted 02.06.2020. – https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-restrictions-data-subject-rights-connection-state_en (09.04.2024), p 5 ja 13.

tähendab andmetöötleja otsuse vaidlustamist AKI-s, mille sätestab IKS § 24 lg 4. Samas näeb ÕKAD art 15 lg 3 kolmas lause ette vajaduse teavitada andmesubjekti õigusest esitada „kaebus järelevalveasutusele“, mille sätestab IKS § 24 lg 1 p 7 üldise teavitamise kohustuse all ning alternatiivina AKI-sse pöördumisele „kasutada õiguskaitsevahendit„ mille sätestab IKS § 24 lg 4.

Eeldatavasti täpsuse ja pragmaatilisuse tõttu on IKS § 24 lg-s 4 kasutusel sõnad „otsuse vaidlustamine“ seoses AKI-sse ja kohtusse pöördumisega. Samas ei saa autori hinnangul jääda tähelepanuta vajadus juurdepääsuõiguse taotluse raames teavitada andmesubjekti võimalusest esitada AKI-le ulatuslikum kaebus juhul, kui ta „leiab, et isikuandmete töötlemisel rikutakse tema õigusi“. Küsimus on IKS § 24 lg 4 ja § 28 lg 1 paralleelsest kohaldamisest. Lisaks tuleb esitada IKS § 24 lg 1 punkt 7 kohaselt AKI kontaktandmed, mille esitamise on Artikli 29 töörühm välja toonud ÕKAD art 15 kontekstis.[244] Kuna IKS-is on eraldi säte andmesubjekti õiguste teostamise kohta AKI-s, saab autori hinnangul täpsustada vastavat § 28 lg 1 andmesubjekti õigusega pöörduda AKI-sse ka tutvumise või muud õigust piirava otsuse vaidlustamiseks.

3.7. Piirangu otsuse dokumenteerimine

IKS § 24 lg 5 näeb kooskõlas ÕKAD art 15 lg-ga 4 ette politsei kohustuse dokumenteerida sama paragrahvi lg 2 alusel tehtud piiramise „otsuse faktilised ja õiguslikud alused“ ning „vajaduse korral“ teha „teave“ kättesaadavaks AKI-le. Sätte üldsõnalisus võimaldab andmetöötlejal dokumenteerida tegevusi ja argumentatsiooni vähesel määral. Dokumentatsiooni abiga saab kontrollida saab kontrollida ja tõendada piirangu seadmise seaduslikkust.

Autori hinnangul ei saa kohustus tähendada üksnes faktiliste ja õiguslike aluste, sealhulgas IKS § 24 lg 2 loetelus olevate asjaolude nimetamist. Analoogia korras Euroopa Andmekaitseinspektori antud suunistega peab andmetöötleja piirangu kohaldamise detailset hindamist puudutavas dokumendis enda otsust põhjendama täpsete faktiliste ja õiguslike argumentidega[245]. Lisaks leiab ta, et juurdepääsuõiguse andmisega kaasnevad „riskid“ andmetöötleja tegevusele peavad olema „konkreetsed“ ja „ettenähtavad“ ega saa olla üksnes

[244] Artikli 29 töörühm. WP 258, lk 21.
[245] EDPS Case 2020-0908, p 3.11–3.12.

„hüpoteetilised“.[246] Sellise dokumentatsiooni kohustus lähtub taaskord põhimõttest, et vaja on hinnata juurdepääsuõiguse piiramist ja tõendada enda mõttekäiku individuaalselt ja üksikjuhtumi põhiselt[247].

IKS § 24 lg 5 kohaselt vastavuses ÕKAD-i art 15 lg-ga 4, tuleb andmetöötlejal esitada AKI-le esmajärjekorras „teave“, mitte koheselt dokumentatsioon. Arusaadavalt on olulisem teabe vormistamisest piirangu otsuse aluseks olev teave ise. Dokumenteerimine võib praktilisel kaalutlusel olla autori hinnangul võimalik mitmes etapis. Igal juhul peab enne andmesubjekti taotlusele vastamist hinnangu olulisem osa olema vähemalt lühidalt dokumenteeritud. Lähtuvalt IKS § 24 lg-st 5 tuleb AKI-le teave teha kättesaadavaks „vajaduse korral“. Autori hinnangul on sõna-sõnalt tõlgendusega võimalik leida, et IKS-is on laiendatud ÕKAD art 15 lg 4 regulatsiooni. ÕKAD-ist nähtub sõna-sõnalt, et teave tehakse kättesaadavaks igal juhul, sarnaselt nagu on vaja dokumenteerida piiramise otsus igal juhul. Artikli 29 töörühm on siiski leidnud, et „taotluse alusel“ tuleb teave kättesaadavaks teha.[248] Selline lähenemine ühtib arusaamaga, et teave tehakse AKI-le kättesaadavaks kui andmesubjekt otsustab vaidlustada AKI-s andmetöötleja otsuse. Vastasel juhul jõuavad AKI-le ka need andmetöötleja piiramist puudutavad otsused, mida andmesubjekt pole vaidlustanud ega AKI järelevalve või muu raames taotlenud. Seega on IKS § 24 lg 5 täpsustus asjakohane. Lisaks tuleb arvestada IKS § 24 lg 4 puhul teabe esitamisega halduskohtule juhul, kui isik vaidlustab andmetöötleja otsuse kohtus.[249]

IKS-i 4. peatüki 3. jao regulatsioonis pole täpsustatud, kuidas tuleb andmetöötlejal koondada või säilitada teavet andmesubjekti tutvumise õiguse piiramise teostamise korra ja otsuse dokumenteerimise kohta. ÕKAD-i vastavas regulatsioonis puudub selline kord. Euroopa Nõukogu suuniste alusel ei tulekski juurdepääsuõiguse taotlust ega sellega seonduvat andmetöötlust registreerida.[250] Siinkohal on autori hinnangul otstarbekam lähtuda Euroopa Nõukogu alternatiivina välja pakutud lahendusest ning seadusandjal täpsustada kaalumise järel IKS §-i 27 üldiselt kohalduvana andmesubjekti õiguste teostamise korrale. Võimalik on kõneallolev teave ja dokumendid registreerida eraldi õiguskaitseasutuse õiguskaitse eesmärgil kasutatavatest infosüsteemidest, määrates suunistest lähtuvalt võimalikult „mõistlik“

[246] Samas, p 3.11.
[247] Dimitrova, LED Article 15/C.4. Commentary.
[248] Artikli 29 töörühm. WP 258, lk 21.
[249] IKS v.r. osas vt RKHKo 3-16-2348/21, p 21.
[250] Soovitus politsei andmetöötluse kohta. Vt Council of Europe Committe of Ministers Explanatory Memorandum to Recommendation No. R (87) 15 of the Committee of Ministers to member states regulating the use of personal data in the police sector (Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies). – https://rm.coe.int/168062dfd4 (01.04.2024), p 84 esimene lause.

säilitustähtaeg.[251]Autori hinnangul lähtub asjakohase tähtaja määramine näiteks võimaliku vaidemenetluse või muu kaitseõiguse teostamise tähtajast ning isikuandmete töötlemise põhimõtetest, sealhulgas eesmärgikohasuse ja säilitamise piirangu kohta.

3.8. Kriminaalmenetluse seadustiku kohaldamine

Politseil lähtub andmesubjekti õiguste piiramisel kriminaalmenetluses KrMS § 15^2 lg-s 4 sätestatud piirangu asjaoludest ja sama paragrahvi lg 5 p-des 1–6 loetletud õigustest, mida on võimalus piirata. KrMS § 15^2 lg-s 4 näeb seadusandja ette piirangud võimalusena ja seab nende kasutamise sõltuvusse vajadusest, nagu ÕKAD. Autor piirdub siinkohal samade hinnangute ja analüüsiga, mis on eelnevalt esitatud IKS § 24 lg-s 2 nimetatud asjaolude kohta (vt 3.1–3.2). Piirangu asjaolud on sätestatud sama täpselt kui ÕKAD-i art 15 lg-s 1, välja arvatud osas, et teise isiku õiguste ja vabaduse kahjustamisele lisaks näeb KrMS ette võimaluse piirata tutvumise õigust andmesubjekti isiku ja õiguste kahjustamise takistamiseks ning „ametliku menetluse takistamine“ on lahti kirjutatud, kuid avatud loeteluna („tsiviil-, haldus- või mistahes muu seadusliku menetluse läbiviimise“ takistamine). Siiski on KrMS § 15^2 lg 4 loetelu tervikuna sama üldine ja lai kui IKS § 24 lg-s 2. Põhimõtteliselt võimaldab KrMS-is sätestatu liiga laia kaalutlusruumi ega ole selle tõttu vastavuses ÕKAD-iga. Piirangu asjaolu (tähenduses piirangu aluse eesmärk) kohaldamine pole seotud mõne tingimuse ega asjaoluga, samuti pole täpsustatud selle kohaldumist lähtuvalt konkreetse andmesubjekti õigusest, isikuandmetest või teabest. Autor tõdeb, et kuigi teoreetiliselt võimalik, ei pruugi olla otstarbekas või ei olegi võimalik kõiki asjaolusid sätestada detailselt ja ammendavalt.[252] Selle võrra tähtsam on andmetöötleja igakülgne juhtumipõhine hinnang ja proportsionaalsuse analüüs.

Kriminaalmenetluse raames peaks kohaldama üksnes KrMS-i sätteid §-i 15^2 lg 3 alusel. Seadusandja on andmesubjekti õiguste regulatsiooni ülevõtmisel KrMS-i piirdunud ebaproportsionaalselt ÕKAD art 15 lg-s 1 sätestatud eesmärkide sätestamisega. Sätestatud ei ole andmesubjektile üheselt arusaadavalt ja ettenähtavalt tema teavitamine tema õiguse piiramisest, selle põhjustest ja õigusest teostada juurdepääsuõigust kaudselt pädevas järelevalveasutuses ning andmetöötleja kohustust eelnimetatu dokumenteerida vastavalt ÕKAD art 15 lg-tele 3 ja 4. KrMS-is ei ole näiteks erisätet IKS 4. peatüki 3. jao regulatsiooni

[251] Samas, p 84 teine ja kolmas lause.
[252] Selgituse kohta miks ei nähta vajadust detailse isikuandmete kaitse regulatsiooni kehtestamiseks KrMS-is vt isikuandmete kaitse seaduse rakendamise seaduse 778 SE seletuskiri. – https://www.riigikogu.ee/download/0629e042-d72a-4ae7-b885-58ec0fce0efc (13.04.2024), § 49 lk 60.

kohaldamiseks. Samas tuleb arvestada, et andmesubjekt saab enda õiguste teostamisel põhimõtteliselt lähtuda IKS-is kui KrMS-is suhtes üldseaduses sätestatud regulatsioonist.

KrMS § 15^2 lg-s 5 on ette nähtud võimalus piirata andmesubjekti erinevaid õigusi, sealhulgas mõne erisusega IKS-i vastavast § 24 lg-st 2. Täpsemalt on KrMS-is sätestatud võimalus piirata õigust saada teada „isikuandmete töötlemisest, sealhulgas sellest, milliseid isikuandmeid töödeldakse, samuti töötlemise viisi, meetodit, eesmärki, õiguslikku alust, ulatust või põhjust“ (§ 15^2 lg 5 p 1) ja õigust saada teada isikuandmete edastamisest välisriigile või rahvusvahelisele organisatsioonile (§ 15^2 lg 5 p 2). Samuti võimaldatakse piirata õigust saada teada isikuandmetega seotud rikkumisest, mida IKS ei sätesta tutvumise õiguse piiramise raames, vaid eraldiseisvalt § 45 lg-s 5 (KrMS § 15^2 lg 5 p 6). Selliste täpsustuste tõttu on andmesubjektile terviklikult selgem, milliseid tema õigusi on võimalik andmetöötlejal piirata. KrMS § 15^2 lg 5 ei sisalda punkti andmesubjekti isikuandmete parandamise ja kustutamise nõude õiguse piiramise kohta. Eelduslikult ei ole seadusandja välistanud andmetöötleja võimalust piirata parandamise ja kustutamise õigust.[253] Võimalik, et isikuandmete töötlemise piiramise õiguse piiramise all on silmas peetud parandamise ja kustutamise õiguse piiramist (KrMS § 15^2 lg 5 p 3). Autori hinnangul tuleb KrMS-i säte selles osas üle hinnata.

KrMS § 15^2 lg-st 4 ega 5 ei nähtu, et seadusandja on eristanud kriminaalmenetluse raames osalist ja täielikku andmesubjekti õiguste piiramist. Autor võib eeldada sõna-sõnalt tõlgendades, et liikmesriigile ÕKAD art 15 lg 3 teises lauses sätestatud osaline õiguste piiramise võimalus ei ole ettenähtavalt ja selgelt kriminaalmenetluse raames võimaldatud. Igal juhul tuleb andmetöötlejal hinnata üksikjuhtumi põhiselt ja individuaalselt isikuandmete ning teabe kaupa, kuivõrd on võimalik piirata andmesubjekti juurdepääsuõigust üksnes osaliselt, arvestades osalise piiramise võimalusega ka piirangu ajalise kehtivuse puhul. Osalise õiguste piiramise mittevõimaldamine viib ebaproportsionaalse andmesubjekti õiguste piiramiseni.

Tähelepanuväärne on, et KrMS § 15^2 lg 5 p 1 võimaldab andmetöötlejal põhimõtteliselt täielikult piirata õigust saada teada isikuandmete töötlemisest, isikuandmetest ja teabest nende töötlemise kohta ning piirangu põhjustest. Tinglikult võib tegemist olla täieliku andmesubjekti õiguste piiramise alusega ÕKAD art 15 lg 3 teise lause tähenduses. Samas pole autori hinnangul tegemist sõnaselge ja andmesubjektile ettenähtava võimalusega. Lisaks võimaldab kõneallolev säte ebaproportsionaalset õiguste piiramist sõna „sealhulgas“ kasutamise tõttu.

[253] Isikuandmete kaitse seaduse rakendamise seaduse 778 SE seletuskiri, § 49 lk 61.

Andmesubjektile ei ole näiteks selge, et andmetöötlejal on õigus piirata tema õigust saada teada isikuandmete säilitamise tähtaeg või teavet selle kohta, milliste isikuandmete kategooriatena teda puudutavaid isikuandmeid töödeldakse. Autori hinnangul ei näe ÕKAD ette juurdepääsuõiguse piiramist isikuandmete ja teabe avatud loetelu kaudu, mistõttu on ettepanek täpsustada sätet ja nimetada selles lõplikult piirangu ulatus. Autor märgib kattuvalt KrMS-i kohaldamisala puhul esitatud arvamusega, et andmesubjekti õiguste tõhusaks kaitseks tuleb üle hinnata KrMS § 15^2 lg 4–5 ja IKS § 24 kohaldamise juhud (vt 1.2).

4. ANDMESUBJEKTI KAUDSE JUURDEPÄÄSUÕIGUSE TEOSTAMINE

4.1. Kaudse juurdepääsuõiguse teostamise eeldused

Politseile on antud võimalus piirata andmesubjekti juurdepääsuõigust. Vastukaaluks on andmesubjektile antud täiendav võimalus juurdepääsuks enda kohta käivatele isikuandmetele. Lisaks andmetöötlejale on tal õigus esitada taotlus järelevalveasutusele. Seda põhjusel, et just õiguskaitse eesmärgil andmetöötluse ja õiguskaitseasutuse suhtes võib õiguste teostamine olla andmesubjektil endal „keeruline või isegi võimatu“[254]. Kõnealloleväks järelevalveasutuseks on Eestis AKI lähtuvalt IKS § 51 lg-st 1. Andmesubjektile ette nähtud ainulaadne õigus ei ole siiski teostatav samaväärselt vahetult teostatava juurdepääsuõigusega. Eelkirjeldatu tõttu analüüsib autor kaudse juurdepääsuõiguse regulatsiooni IKS-is.

Kaudse juurdepääsuõiguse taotlemise ÕKAD art 17 lg 1 kohane eeldus on, et politsei ei anna andmesubjektile juurdepääsu isikuandmetele või teavet isikuandmete töötlemise kohta. IKS-is on selgelt seostatud kaudne juurdepääsuõigus olukorraga, kus üksikjuhul on konkreetselt kohaldatud vahetu juurdepääsuõiguse piiramise alust. See tähendab, kaudse juurdepääsuõiguse taotlemise eeldus on, et andmesubjekt on andmetöötlejalt taotlenud juurdepääsu, ent andmetöötleja on enda otsusega IKS § 24 lg 2 alusel kohaldanud juurdepääsule piirangut. Sellest tulenevalt on politsei kohustatud IKS § 24 lg 4 kohaselt teavitama „andmesubjekti tema õigusest pöörduda otsuse vaidlustamiseks AKI-sse“.

Autor ei toeta lähenemist, mille kohaselt on andmesubjektil üksnes IKS § 24 lg-s 2 sätestatud piirangu asjaolude teoreetilise võimalikkuse tõttu õigus esitada tutvumise taotlus paralleelselt andmetöötlejale ja AKI-le.[255] Sellisel juhul tuleks AKI-l oodata andmetöötleja otsust juurdepääsuõiguse täieliku teostamise või selle osalise või täieliku piiramise kohta. Alternatiivselt peaks AKI omal algatusel tutvuma isikuandmetega ja teabega nende töötlemise kohta ning otsustama neile juurdepääsu andmise üle. Seejärel saaks AKI teostada kontrolliõigust vastavalt juhtumile. Paralleelse taotluse juhtudel on autori hinnangul tegemist segadust tekitava ja etteulatuvalt võimaliku kaudse juurdepääsuõiguse või kaebeõiguse teostamisega, milleks andmesubjekt ei pruugi soovi avaldada. Töökorralduslikult on AKI-l ja

[254] C-333/22, *Ligue des droits humains*, p 44.
[255] ÕKAD p 48 esimese lause ja igal juhul teostatava kaudse juurdepääsuõiguse tõlgendus ÕKAD art 17 lg 1 kohaselt. Vt Franssen, Corhay. LED Article 17/Section C.1. Commentary.

politseil vaja taotluse põhiselt hinnata, kas võib olla erijuhuna proportsionaalne selle paralleelne lahendamine.

Andmetöötlejal on kohustus avaldada andmesubjektile teavet isikuandmete töötlemise kohta üldiselt IKS § 22 lg 1 ja täpsemalt IKS § 23 lg 1 kohaselt. Autor nõustub Fransseni ja Corhay'i seisukohaga, et eelnimetatud kohustuse täitmata jätmine pole üheselt võetav põhjendus kaudse juurdepääsuõiguse paralleelsele teostamisele.[256] Autor leiab, et kui andmesubjektile ei ole teada andmetöötleja või tema kontaktid, on tal võimalik pöörduda AKI-sse üldise kaebeõiguse korras IKS § 28 lg 1 alusel.

IKS §-is 24 on viidatud kaudse juurdepääsuõiguse teostamise õigusele. ÕKAD art17 lg 1 ja põhjenduse 48 esimese lause sõna-sõnalt tõlgendus võimaldab mõista, et tegemist on riigisisese valikuga võimaldada või mitte juurdepääsu „ka pädeva järelevalveasutuse kaudu". Siiski on see Artikli 29 töörühma kohaselt liikmesriigile pandud kohustus sätestada kaudne juurdepääsuõigus.[257] Kuigi eelnimetatud IKS-i sätted ei ole autori hinnangul piisavalt selged ega täpsed, pole võimalik öelda, et seadusandja ei ole üldse sätestanud ÕKAD-i tähenduses kaudse juurdepääsuõiguse regulatsiooni. IKS on eemaldunud ÕKAD-i eelsest lähenemisest, kui oli võimalus riigisiseses õiguses valida, kas andmesubjekti õigus tagatakse vahetult või alternatiivselt järelevalveasutuse kaudu[258]. Samuti pole seadusandja sätestanud kaudset juurdepääsuõigust „ainuvõimaliku" ja vahetut juurdepääsuõigust „asendava" õigusena[259].

IKS § 24 lg-s 4 on sätestatud politsei teavitamise kohustus, nagu näeb ette ÕKAD art 17 lg 2. Autor peab ilmselgeks, et andmesubjekti õiguste teostamise võimaldamiseks peab andmetöötleja vastamisel omal algatusel ja igal juhul teavitama andmesubjekti sellest võimalusest. IKS-i 4. peatüki 3. jao sätetest ei nähtu aga lisasätteid kaudse juurdepääsuõiguse kohta. IKS-i eelnõu koostajad on lugenud ÕKAD art 17 üle võetuks IKS kehtivas redaktsioonis §-iga 28, sealhulgas läbi andmetöötleja teavitamiskohustuse.[260] Autori hinnangul ei täida pelgalt kaudsest juurdepääsuõiguse olemasolust teavitamise kohustuse ega AKI kohustuste üldises korras sätestamine ega teavitamine ise eesmärki teha andmesubjektile arusaadavaks, mis on selle õiguse olemus ja just selle teostamise kord AKI-s. Andmesubjekt peab aru saama, et AKI teostab andmetöötleja isikuandmete töötlemise seaduslikkuse ning piirangu seadmise

[256] Franssen, Corhay. LED Article 17/Section C.1. Commentary.
[257] Artikli 29 töörühm. WP 258, lk 23.
[258] Art 17 lg 1 p a ja art 18 lg 1 vt Nõukogu raamotsus 2008/977/JSK, 27. november 2008, kriminaalasjades tehtava politsei- ja õigusalase koostöö raames töödeldavate isikuandmete kaitse kohta. – EL T 350, 30.12.2008, lk 60–71.
[259] Vt C-333/22, *Ligue des droits humains,* kohtujurist L. Medina ettepanek, p 42, 44, 69.
[260] Isikuandmete kaitse seaduse 679 SE seletuskiri, lisa 1 lk 21–22.

nõuetele vastavuse kontrolli.[261] Eelnimetatust lähtuvalt leiab autor, et AKI pädevust puudutavalt tuleb IKS-i sätteid täpsustada ja muuta.

Kui politsei on piiranud andmesubjekti õiguse teostamist, siis Dimitrova ja De Herti kohaselt piisab AKI-sse pöördumiseks selgitusest, et andmesubjekt ei saanud juurdepääsu soovitud ulatuses ja ta soovib teostada enda õigusi järelevalveasutuse kaudu[262]. Seejärel, kui andmesubjekt otsustab seda õigust teostada, tuleb AKI-l kontrollida, sealhulgas milliseid isikuandmeid on töödeldud, kas töötlemine on seaduslik, kas esineb ebakõlasid ja kas isikuandmed on õiged[263].

Kui IKS § 24 sätestatud andmesubjekti õigusi on vaja tagada kriminaalmenetluse raames, siis ÕKAD art-i 18 kaudu kohaldub teabe andmise või tutvustamise piiramisele KrMS-i regulatsioon Kui ei ole tegemist kriminaalmenetluse raames teabe andmisega või on tegemist sellega, aga mitte kriminaalmenetluse toimingutega kogutud teabe andmisega, ei leia IKS-i eelnõu seletuskirja koostajate selgitusi selle kohta, miks ei ole võimaldatud õiguste teostamist AKI kaudu.[264] KrMS § 15^2 seevastu ei sätesta andmekaitseõiguse kohase andmesubjekti kaudse juurdepääsuõiguse teostamist kriminaalmenetluse ajal või selle teostamise erisusi koostoimes kriminaalmenetlusõigusega ja AKI pädevusega, nagu tõdes autor KrMS §-i 15^2 puudutavas analüüsis. Autor üksnes märgib magistritöö eesmärgi ja mahu piirangu tõttu, et kaudse juurdepääsuõiguse vaates tuleb üle hinnata ning vajaduse korral muuta KrMS-i regulatsiooni.

4.2. Piirangu seaduslikkuse kontroll ja andmesubjekti teavitamine

Andmesubjekti nimel järelevalveasutuse poolt juurdepääsuõiguse teostamise regulatsioon on tuletatav ÕKAD art 17 lg 3 esimesest lausest ja eeskätt art 46 lg 1 p-st g. Eelnimetatust ilmneb, et AKI kas „kontrollib isikuandmete töötlemise seaduslikkust“ või jätab kontrolli teostamata. Lisaks kohustavad ÕKAD art 17 lg 3 koosmõjus art 46 lg 1 p-ga g teavitama andmesubjekti „mõistliku aja jooksul kontrollimise tulemusest“ või selle „teostamata jätmise põhjustest“, mis on üksnes minimaalne kohustuslik teavituse sisu ning õiguskaitsevahendi kasutamise õigusest.

[261] Vt kaudse juurdepääsuõiguse puhul AKI pädevust puudutavalt ÕKAD art 46 lg 1 p g, mida ei ole IKS §-iga 56 täpselt üle võetud.
[262] Dimitrova, De Hert 2023, lk 9.
[263] Dimitrova, De Hert 2018, lk 123.
[264] Isikuandmete kaitse seaduse 679 SE seletuskiri, § 22 lk 28.

Seadusandja pole IKS-is, sealhulgas §-is 28 või §-is 56 vähemalt sõnaselgelt sätestanud kaudse juurdepääsu teostamise korda ja vastavalt AKI pädevust. Autori hinnangul on IKS-i üle võetud ÕKAD art 17 lg 3 mittevastavalt, sest pole sätestatud minimaalset teavitamise kohustust. Samuti ei nähtu IKS-i sätetest ÕKAD-i art 46 lg 1 p-s g sätestatud kontrolli pädevuse üle võtmine. Vastavast regulatsioonist peaks ilmnema AKI teostatava kontrolli miniaalne ulatus ja sisu ning sisend vastamiseks andmesubjektile.

EL-i õigusnorm sätestab minimaalsed nõuded teavitamisele ja nimetab üldiselt vajaduse teostada kontrolli, mis ei välista AKI põhjalikuma kontrolli teostamist. Seejärel, nagu Dimitrova ja De Hert selgitavad, üksikjuhtude kaupa lähtuvalt „proportsionaalsuse ja vajalikkuse" põhimõttest saab otsustada minimaalselt vajalikust või rohkemast teavitamise üle[265]. Euroopa Kohus isegi rõhutab, et teavituse sisu ei saa lõplikult ette määrata, sest kohustus teavitada minimaalsest ei pruugi kaalutlusõiguse alusel olla teatud juhtudel proportsionaalne[266]. Euroopa Kohtu otsuse kohaselt tuleb isegi ette näha andmesubjekti minimaalsest „ulatuslikum" teavitamine selleks, et ta saaks teadlikult otsustada kohtusse pöördumise üle.[267] Samuti leiab Euroopa Kohus, et järelevalveasutusele tuleks ette näha andmetöötleja juurdepääsuõiguse piiramisega sarnane regulatsioon. Ehk, ette näha õigus piirduda lühikese teavitusega kontrolli tulemustest ja võetud meetmetest selleks, et kaitsta „avaliku huvi eesmärki".[268] Eesti õiguse mõistes tähendab see andmetöötleja IKS § 24 lg 2 alusel nimetatud asjaolust teavitamist. Autori hinnangul on eelnimetatust tulenevalt vaja IKS-i täiendada AKI teavitamise ja muu pädevuse osas.

AKI kontroll saab tõenäoliselt alguse andmetöötleja piiramise otsuse puudutava dokumentatsioonist, mis tuleb IKS § 24 lg 5 kohaselt „vajaduse korral" kättesaadavaks teha. Eelnimetatust ilmnevad faktilised ja õiguslikud alused koos põhjendustega selle kohta, miks andmesubjektil pole osaliselt või täielikult õigus tutvuda isikuandmetega. Isegi ÕKAD-i kaudse juurdepääsuõiguse regulatsioon ei anna AKI-le vaikimisi õigust igal üksikul juhul saada samaväärselt andmetöötlejaga juurdepääsu kaudselt õigusi teostava andmesubjekti isikuandmetele, mille avaldamisest andmetöötleja keeldus.[269] Samas on AKI-l kaudse juurdepääsuõiguse regulatsiooni raames igakülgne uurimisvolitus ja ülesande täitmiseks vajalik

[265] Dimitrova, De Hert 2018, lk 123.
[266] C-333/22, *Ligue des droits humains*, p 60, 63; C-333/22 *Ligue des droits humains,* kohtujurist L. Medina ettepanek, p 70–71, 90, 92, 98.
[267] C-333/22, *Ligue des droits humains*, p 65.
[268] Samas, p 66.
[269] C-333/22, *Ligue des droits humains,* kohtujurist L. Medina ettepanek, p 73.

juurdepääs isikuandmetele ja neid puudutavale teabele.[270] Siiski peaks ebaseadusliku töötlemise avastamisel toimima konfidentsiaalne ehk usalduslik suhe AKI ja politsei vahel, sest AKI peaks andma „võimaluse olukorda parandada“ enne, kui vajadusel korral kasutab andmetöötleja suhtes enda eeskätt IKS § 56 lg-st 3 tulenevaid õigusi[271].

Andmesubjektil on õigus saada teavitus AKI-lt mõistliku tähtaja jooksul. Enne AKI poole pöördumist on andmesubjekt saanud andmetöötlejalt vastuse üldjuhul ühe kalendrikuu jooksul IKS § 27 lg 2 alusel. AKI taotluse lahendamisele peaks kehtima samuti tähtaeg või vähemalt olema see piiritletud. Kaudne õiguste teostamine ei allu kaebuse läbivaatamise regulatsioonile. Autor eeldab, et praktikas rakendub kaudse õiguse teostamise taotlusele vastamisel sama, üldjuhul 30 päevane tähtaeg IKS § 61 alusel.

Selguse huvides tuleks autori hinnangul terviklikult üle vaadata IKS § 28 koostoimes §-iga 61. Vastavalt vajadusele tuleks täpsustada näiteks täpsustada andmesubjekti õiguste teostamise jaos olevas IKS §-is 28, milline on mõistlik temale vastamise tähtaeg või muuta sätteid selliselt, et oleks arusaadav, kuivõrd kaudse juurdepääsuõiguse otsuse vaidlustamise taotlus ja isikuandmete töötlemise rikkumist puudutava kaebuse lahendamine alluvad regulatsioonile IKS §-is 61.AKI peab teavitama andmesubjekti õiguskaitsevahendi kasutamise õigusest. ÕKAD art 53 lg 1 koosmõjus põhjendusega 86 näeb ette üldiselt õiguse õiguskaitsevahendile järelevalveasutuse otsuse vastu, mis toob andmesubjektile siduvaid õiguslikke tagajärgi. Sellest tulenevalt näeb IKS § 28 lg 2 ette kohtuliku kontrolli, kohaldudes sõna-sõnalt üksnes kaebuse alusel tehtud otsuse vaidlustamisele. IKS-is ei ole seega kaudse juurdepääsuga seoses vastavat sõnaselget sätet AKI poolse teavitamise ega tema otsuse kohtuliku kontrolli kohta. Eelkirjeldatust tulenevalt leiab autor, et AKI-le tuleb luua alus ELPH art 52 lg 1 kohaseks kaalutlusõiguse teostamiseks kaudse juurdepääsuõiguse raames ülesanne täitmiseks ning sätestada täpsemalt kaudse juurdepääsuõiguse teostamise kord.

4.3. Andmekaitse Inspektsiooni otsuse vaidlustamine

Kõneallolevas olukorras kontrollib AKI andmesubjekti taotlusel andmetöötleja tegevust. Samas on äratanud kahtlusi järelevalveasutuse võimalus ja võimekus täielikku kontrolli läbi viia. Nimelt ei näi Dimitrovale ja De Hertile võimalik, et järelevalveasutus selgitab sõltumatult välja ebaõiged andmed ja nende tegeliku parandamise vajaduse, sest andmetöötleja ei pruugi

[270] Samas, p 74.
[271] Samas, p 89, 91.

anda juurdepääsu andmetele või teeb lõpliku otsuse andmesubjektile avalikustatava teabe osas, mille kohta ka järelevalveasutus ei saa andmesubjektile põhjendusi anda.[272] AKI ei saa aga olla Euroopa Kohtu kohtujuristi sõnade kohaselt üksnes politsei seisukoha „vahendaja" ja „kinnitaja".[273]

Euroopa Kohtu otsuse kohaselt on järelevalveasutusel andmesubjektist eraldiseisev EL-i esmasest õigusest tulenev roll.[274] Tal on Euroopa Kohtu kohtujuristi sõnul volitus olla enda otsuse vastuvõtmisel „juhtivas" ja „aktiivses" rollis.[275] Järelevalveasutust peavad Dimitrova ja De Hert sõnaselgelt „vabaks" iseseisvalt otsustama, millest andmesubjekti teavitada.[276] Sellise iseseisva otsustuse võimaluse AKI-le annab annab õigus saada juurdepääs isikuandmetele ja teabele vähemalt IKS § 24 lg 1 ulatuses. Nimelt järelevalveasutusel on Euroopa Kohtu kohtujuristi täpsustuse kohaselt „enda nimel" õigus saada vajadusel juurdepääs isikuandmetele, et aktiivselt ja õiguslikult hinnata andmetöötluse seaduslikkust ja omada parandamisvolitusi ning iseseisvalt ja sõltumatult otsustada, mis osas andmesubjektile vastata.[277]

Selline sõltumatu roll ELPH art 8 lg 3 tähenduses teeb tema kaudse juurdepääsuõiguse raames tehtud otsuse Euroopa Kohtu tõlgenduses õiguslikult siduvaks ja kohtus vaidlustatavaks ELPH art 47 (Eesti mõistes ka PS §-i 15) tähenduses[278]. Andmesubjekti õigus AKI kaudse juurdepääsu raames teostatud kontrolli omakorda kohtulikult kontrollida ei tulene IKS-ist sõna-sõnalt, vaid nähtub üksnes juhul, kui käsitleda kaudse juurepääsu õiguse teostamise taotlust kaebusena §-i 28 tähenduses. AKI-l tuleb enda vastuses teavitada andmesubjekti õigusest pöörduda tema otsuse vastu kohtusse. IKS-i vastavusse viimiseks ÕKAD-iga ja õigusselguse huvides peab autori hinnangul täiendama IKS-is näiteks §-i 28 selliselt, et selle sätted kajastaks selgelt andmesubjekti õigust vaidlustada AKI kaudse õiguse teostamise raames tehtud otsust.

Siinkohal eristuvad kaks alust, kui andmesubjekt saab pöörduda järelevalveasutuse poole. Esiteks saab vaidlustada andmetöötleja otsuse IKS § 24 lg 4 tähenduses. Teiseks saab esitada kaebuse tema poolt isikuandmete töötlemise õiguste rikkumise kohta IKS § 28 lg 1 alusel. Need

[272] Dimitrova, De Hert 2018, lk 123; Dimitrova, De Hert 2023, lk 13–14.
[273] C-333/22, *Ligue des droits humains,* kohtujurist L. Medina ettepanek, p 69.
[274] C-333/22, *Ligue des droits humains,* p 48.
[275] C-333/22, *Ligue des droits humains,* kohtujurist L. Medina ettepanek, p 56, 61.
[276] Rõhutatakse muu hulgas vajadust ÕKAD art 17 lg 3 ja art 46 lg 1 p g (IKS-i vasted puuduvad) sisustamisel pidada silmas ÕKAD art 42 lg 2 (sõltumatus), art 43 lg 2 (kvalifikatsioon, kogemus ja oskused) ja art 47 lg 1 (uurimisvolitused), sest art 17 lg 3 ei saa piirata art-st 46 tulenevaid järelevalveasutuse õigusi ülesannete täitmisel. Vt Dimitrova, De Hert 2023, lk 13–15.
[277] C-333/22, *Ligue des droits humains,* kohtujurist L. Medina ettepanek, p 63–65, 78–79.
[278] C-333/22, *Ligue des droits humains,* p 37, 50, 55, 73.1.

täiendavad võimalused ei tohi välistada teineteist, nagu Artikli 29 töörühm on rõhutanud.[279]Lisaks tuleb meelde tuletada, et andmesubjektil on eraldiseisvalt juurdepääsuõiguse teostamisest AKI kaudu ja AKI otsuse vaidlustamisest kohtus õigus kasutada õiguskaitsevahendit ELPH art-i 47 ja PS §-i 15 kohaselt ka PPA suhtes. Iseäranis arvestades Euroopa Kohtu seisukohta, et andmesubjekti juurdepääsuõiguse piiramine võib kitsendada ebaproportsionaalselt andmesubjekti õigust tõhusale kohtulikule kontrollile[280]. Samas on seadusandja andnud võimaluse vahetult ja kaudselt juurdepääsuõigust piirata. Eelnimetatust tulenevalt on võimalik tagada üksnes kohtulikult PPA juurdepääsuõiguse piiramise proportsionaalsuse täielik ja AKI kontrolli täiendav kontroll.

[279] Artikli 29 töörühm. WP 258, lk 23–24.
[280] Vt C-362/14, *Maximillian Schrems*, p 95.

KOKKUVÕTE

Eesti on ette näinud tulenevalt EL-i direktiivist õiguskaitse eesmärgil toimuva andmetöötlusega tutvumise korra politseis ja AKI-s. Magistritöö eesmärk oli kujundada arusaam, kas politsei kaalutlusruum on liiga lai, võimaldades piirata ülemääraselt andmesubjekti tutvumise õigust. Selleks analüüsiti andmesubjekti vahetu ja kaudse juurdepääsuõiguse regulatsiooni IKS §-is 24 ning selle vastavust ÕKAD-i art 14, 15 ja 17. Tutvumise õiguse teostamise aluses selguse saamiseks analüüsiti IKS-i kohaldamisala. Andmesubjekti tutvumise õiguse eeldus on teabe saamine andmetöötluse ja enda õiguste kohta. Selleks analüüsiti IKS §-i 22–23 vastavust ÕKAD-i art 13. Kriminaalmenetluses sätestab tutvumise õiguse mitte IKS, vaid KrMS. Selleks analüüsiti KrMS § 15^2 lg 3–5 vastavust ÕKAD-i art 18.

Andmesubjekti vahetu juurdepääsuõiguse alus IKS § 24 lg-s 1 on üldjoontes vastavuses ÕKAD-iga. Politseile on sätestatud kohustus anda kinnitus andmetöötluse kohta ja tagada täielik juurdepääs IKS § 24 lg 1 tähenduses isikuandmetele ja teabele. Andmesubjektil ei ole vaja esitada eraldi pöördumist andmetöötluse kohta kinnituse saamiseks ning isikuandmete ja teabega tutvumiseks. Samuti on tal õigus saada kinnitus juhul, kui tema andmeid politseis ei töödelda. Autori hinnangul vajab kaalumist eelnimetatud aspektides IKS-i täpsustamine.

Praktika kujundamise eesmärgil märgib autor tutvumise õiguse aluse kohta järgmist. Andmesubjekti juurdepääsuõigus puudutab andmetöötlusest põhiandmeid olenemata asukohast, kus isikuandmeid, töötlemise toiminguid või töötlemist puudutav teave on (näiteks logifailid). Taotlusele vastates tuleb esitada IKS § 24 lg 1 p-i 1 alusel kõik isikuandmed, sealhulgas osas, mis võivad olla töötlemisel ebaseaduslikult, vajada parandamist või peaksid olema kustutatud. Samuti tuleb esitada teave kõigi IKS § 24 lg 1 p-des 2–5 nimetatud töötlemise toimingute kohta taotlusele eelnevas osas tagasiulatuvalt ja etteulatuvalt tinglikult ühe kuu vaates, mis on IKS § 27 lg 2 kohane taotlusele vastamise tähtaeg. Kuigi IKS ei nõua isikuandmete esitamist koopia kujul, on see soovitatav praktika. Kui proportsionaalne, on võimalik koopia esitamise osas kohaldada IKS § 24 lg 2 alusel piiranguid. Teave töötlemise kohta on võimalik esitada kokkuvõtte vormis. Automatiseeritud otsuse kohta tuleb teave avalikustada üldiselt või anda teada konkreetsest otsusest andmesubjektile, sest selle kohta ei ole kohustuslik esitada teavet tutvumise õiguse raames.

IKS § 27 lg 4 suunab andmesubjektiga suhtlema olukorras, kus on vaja tuvastada tema isik ja juurdepääsuõigus. ÕKAD art 12 lg 5 võimaldab täiendavat teavet küsida seoses põhjendatud

kahtlusega andmesubjekti isikus. Kõneallolev säte IKS-is ei ole vastavuses isikuandmete töötlemise põhimõtetega, sest üldiselt kohalduvana võimaldab ülemäärast andmetöötlust seoses isikusamasuse tuvastamisega ja põhjendamata juhul on tõlgendatav uue tutvumise õiguse täieliku piirangu alusena. Autori hinnangul on vaja täpsustada IKS § 27 lg-s 4 politsei kaalutlusruumi tingimusena põhjendatud kahtlus või muud tingimused, millal ja kuidas võib andmesubjekti isiku tuvastada, sealhulgas nõuda allkirjastatud taotlust. Siinkohal märgib autor, et andmesubjekti tutvumise õiguse tõhusaks tagamiseks peab talle vastama tema konkreetsest taotlusest lähtuvalt ja teda abistavalt. Viimati nimetatud põhimõte ei ole IKS-i selgelt üle võetud, kuid on oluline meeles pidada andmesubjekti isiku tuvastamisel.

Andmesubjekti tutvumise õiguse piiramine on võimalus, mida politsei saab kasutada seaduses sätestatud juhul. Piirangut saab ÕKAD-i sõnastuses kohaldada üksnes seni, kuni vaja ja proportsionaalne. Kooskõlas EL-i õigusega võimaldab IKS § 24 lg 2 piirata andmesubjekti tutvumise õigust üksnes erandina, samuti eristab IKS § 24 lg-s 3 andmesubjekti tutvumise õiguse piiramist osaliselt (IKS § 24 lg 2 alusel koosmõjus lg 3 esimese lausega) või täielikult (IKS § 24 lg 2 alusel koosmõjus lg 3 teise lausega). EL-i õigusega ei ole kooskõlas piirangu ajalise ja sisulise kohaldamise lai määratlus. IKS-is on vaja autori hinnangul sõnaselgelt ja ÕKAD art 15 lg 1 kohaselt sätestada, et teatud ajavahemiku järel tuleb üle hinnata, kas piirangu aluseks oleva õigushüve (asjaolu) kaitse on jätkuvalt põhjendatud. Piirangu kohaldamine selle põhjuse äralangemisel on ülemäärane.

Andmesubjekti tutvumise õiguse piiramise asjaolud on nimetatud IKS § 24 lg 2 p-des 1–5. Andmetöötlejal on võimalik seada andmesubjekti juurdepääsuõigusest ülimuslikumaks vajadus piirata tema tutvumise õigust süüteo tõkestamise, avastamise, menetlemise või karistuse täideviimise; riigi julgeoleku; avaliku korra; ametliku uurimise, ametliku menetluse või teise isiku õiguste ja vabaduste kaitseks. Piirangu aluse kohaldamiseks peab esinema vähemalt üks asjaolu, mis võib saada kahjustatud, ohustatud või mille tõttu on takistatud sellega ettenähtud eesmärgi saavutamine. Asjaolud on sõnastatud sama üldiselt, kui sätte loomise aluseks oleva ÕKAD art 15 lg 1 p-des a–e nimetatud kaitset vajavad eesmärgid. IKS-i regulatsiooni väliselt tekib küsimus piiramise aluse vastavusest EL-i õigusele, politsei liiga laiast kaalutlusruumist ja ülemäärasest tutvumise õiguse piiramisest siis, kui IKS-is ettenähtud asjaolusid ei ole IKS-i suhtes eriseaduses viidud õiguskaitse eesmärgil täidetava ülesande raames läbiviidava andmetöötluse konteksti. Küsimus juurdepääsuõiguse piiramise seaduslikkusest tekib ka siis, kui politsei ei ole üksikjuhtumi põhiselt ja iga asjaolu kohaldumise suhtes läbi viinud ELPH art 52 lg 1 ja PS §-i 11 ja §-i 26 teise lause kohast piirangu seadmise vajalikkuse ja

proportsionaalsuse analüüsi. Seega on vaja valdkondlikus seaduses täpsustada politsei kaalutlusruumi, et tagada õigusselgus ja piirangu kohaldamise aluse vastavus ÕKAD art 15 lg-le 1.

IKS §-i 24 kohaldamiseks on vaja aru saada, kas politsei töötleb isikuandmeid õiguskaitseasutusena õiguskaitse eesmärgil. Tinglikult, kas andmetöötlus puudutab andmesubjektiga seostatavat konkreetset kahtlust seoses KarS-i tähenduses süüteo tõkestamise, avastamise, menetlemise või karistuse täideviimisega. Kehtivas Eesti õiguses puudub termini „süüteo tõkestamine“ legaaldefinitsioon. Andmetöötluse eesmärgi piiritlemise praktiline keerukus või võimatus andmete kogumise, analüüsi või muu töötlusega seoses võib kaasa tuua olukorra, kus andmesubjekti taotlus lahendatakse IKS §-i 24 kohaselt, mis võimaldab intensiivsemat põhiõiguse riivet. Autori hinnangul on vaja senisest selgemalt määratleda IKS-i 4. peatüki kohaldamisala tutvumise õiguse tagamise kontekstis.

Andmesubjekti kaudse juurdepääsuõiguse teostamisele viitab IKS-is § 24 lg 4, mille kohaselt peab politsei teavitama andmesubjekti tema õigusest pöörduda tutvumise õigust piirava otsuse vaidlustamiseks AKI-sse või kohtusse. Autori hinnangul on kaudne juurdepääsuõigus võimalik mitte tutvumise õiguse teoreetilise võimaluse, vaid reaalse tutvumise piiramise olukorras. Seega kui andmesubjekt leiab, et juurdepääsuõiguse piirang on teda diskrimineeriv või tema muid põhiõigusi ja vabadusi ülemääraselt riivav või tal puudub igasugune teave andmetöötluse kohta täieliku juurdepääsuõiguse piirangu tõttu, on tal võimalik teostada enda õigusi AKI kaudu. Kooskõlas ÕKAD art 17 lg-ga 1 on seadusandja käsitlenud IKS-is kaudse juurdepääsuõiguse teostamist täiendava õigusena vahetu juurdepääsuõiguse teostamisele, mitte ainuvõimaliku või vahetut juurdepääsuõigust asendava õigusena. Autori hinnangul on ÕKAD art 17 lg 3 esimese lause ja eeskätt art 46 lg 1 p-i g täielikuks üle võtmiseks vaja IKS-i regulatsiooni täpsustada, eeskätt §-is 28. Andmesubjektile peab selguma täpsemalt kaudse juurdepääsuõiguse olemus ning AKI ülesanne sisuliselt ja iseseisvalt kontrollida isikuandmete töötlemise ja piirangu seadmise seaduslikkust; õigus jätta kontroll PPA osas teostamata või piirata andmesubjekti õigust saada teavet eelnimetatu kohta. Kaebeõiguse kord näeb ette andmesubjekti õiguse vaidlustada kaebuse alusel tehtud otsus kohtus, kuid on vaja välja tuua õigus vaidlustada ka kaudse juurdepääsuõiguse raames tehtud otsus. Andmesubjekti kaudse juurdepääsuõiguse teostamine ei välista pöördumist AKI poole IKS § 28 lg 1 alusel, kui andmesubjekti arvates politsei rikub isikuandmete töötlemisel tema õigusi.

KrMS-i kohaldab politsei tutvumise õiguse alusena kriminaalmenetluse raames. Põhimõtteliselt ei ole KrMS-i § 15^2 lg 3 regulatsioon vastavuses ÕKAD art-ga 18, sest sellest ei nähtu üheselt kuidas andmesubjekt saab kriminaalmenetluse raames teostada talle andmekaitseõigusega tagatud spetsiifilisi õigusi osas, mis ei tulene kriminaalmenetlusõigusest, sealhulgas kriminaalmenetluse toiminguga mitte kogutud isikuandmete osas. Samuti ei nähtu sellest, milliseid IKS-ist tulenevaid õigusi ja kuidas saab andmesubjekt teostada, arvestades, et IKS-i ega KrMS-is regulatsioonide kohaldamise kattuvusi või erisusi pole sätestatud. Autori hinnangul on vaja KrMS § 15^2 lg-s 3 täpsustada, et selles sätestatu võib kehtida teatud osas paralleelselt muu regulatsiooniga KrMS-is ning mis osas kehtib paralleelselt IKS kui üldseadus tutvumise õigust puudutavalt olukordades, milles pole KrMS-is eriregulatsiooni.

KrMS § 15^2 lg-s 4–5 on sätestatud juurdepääsuõiguse piirangu alused ja piiranguga hõlmatud teave. Sättes on täpsem üksnes seaduslikku menetlust puudutav alus ja täiendavalt on sätestatud õigus piirata juurdepääsuõigust andmesubjekti enda kaitseks (KrMS § 15^2 lg 4 teine lauseosa). Selline lai kaalutlusõigus põhiõiguse piiramiseks pole vastavuses EL-i õiguse ja selle tõlgendusega, nagu autor IKS-i puhul välja tõi. Lisaks on KrMS-is ebaselge täieliku juurdepääsuõiguse piirangu kohaldamine andmekaitseõiguse alusel kriminaalmenetluse raames. Kui seadusandja soovib võimaldada sarnaselt IKS § 24 lg 3 teise lausega neutraalse vastuse andmist andmesubjektile, tuleb vastavalt KrMS-i muuta.

Õigusliku aluse mõistes puudub õigusselgus andmesubjekti õiguste tõhusaks tagamiseks pärast kriminaalmenetlust, sealhulgas kriminaaltoimiku tutvustamise osas. Juurdepääsuõiguse üle otsustamisel ei ole tegemist enam otsusega, mis mõjutab kriminaalmenetlust ega laiemalt õiguskaitse eesmärgil andmetöötlusega. Muu hulgas peaks olema üldjuhul kriminaalmenetluse lõppemisega ära langenud vajadus täieliku juurdepääsuõiguse piiramiseks. Vastavalt pole kehtiva IKS §-i 24 ega KrMS § 15^2 lg 3–5 võimalik kohaldada. Analüüsist ilmnes, et regulatsiooni ei ole puudulikus osas KrMS-is ega muus õigusaktis muudetud. Selle tõttu on vaja andmekaitseõigusest lähtuvalt luua täpne ja selge õiguslik alus kõnealloleval juhul juurdepääsuõiguse teostamiseks. Seda eelistatult KrMS-i, et õigusselgemalt välja tuua andmekaitse- ja kriminaalmenetlusõiguse seosed või erisused juurdepääsuõiguse teostamisel kriminaalmenetluse ajal ja järel.

Vahetu juurdepääsuõiguse ja selle piiramise korra kaudse juurdepääsuõiguse ega kaebeõiguse teostamine ei välista PPA või AKI suhtes kohtuliku kontrolli teostamist ELPH art-i 47 ja PS §-i 15 alusel. Kuigi isikuandmete kaitse ja kitsamalt andmesubjekti juurdepääsuõigus on EL-i

esmase õigusega tagatud põhiõigus, omab PS täiendavat rolli isikuandmete kaitse tagamisel põhiseaduslikkuse järelevalve korras juhul, kui riigisisese sätte kohaldamine ei ole EL-i õigusega täielikult reguleeritud. Võimalik on juurdepääsuõiguse piiramise seaduslikkust ja EL-i õigusele vastavust kontrollida Riigikohtus PS-i alusel, mitte koheselt Euroopa Kohtus.

Politseil on kohustus teha andmesubjektile avalikult kättesaadavaks IKS § 22 lg 1 nimetatud teave, sealhulgas andmesubjekti tutvumise õiguse kohta. Vastavalt on PPA avaldanud enda veebilehel andmekaitsetingimused. Kõneallolevalt on PPA andmekaitsetingimused autori hinnangul liiga üldised ning vajavad täpsustamist selleks, et anda andmesubjektile selge ja võimalikult täpne ülevaade andmetöötlusest politseis, sealhulgas selle eesmärkidest.

Andmesubjekti juurdepääsuõiguse regulatsioonist nähtub, kuidas igaühe õigus isiklikule ja laiemale, riigi julgeoleku ja avaliku korra tähenduses turvalisusele võimaldab riivata igaühe õigust isikuandmete kaitsele. Andmesubjekti põhiõigus tutvuda isikuandmetega vastandub esmapilgul politsei võimalusega piirata andmesubjekti tutvumise õigust. Teaduskirjanduses ja kohtupraktikas on algatatud arutelu selle üle, kuidas hinnata andmesubjekti tutvumise õiguse piiramise kaalutlusruumi proportsionaalsust. Küsimus on, kas põhiõigusi tuleb tasakaalustada või seada hierarhiasse.

Olenemata proportsionaalsuse hindamise meetodist, on oluline politsei igakülgne ja juhtumipõhine tutvumise õiguse piiramise hindamine, iseäranis olukorras, kus seaduses sätestatud tutvumise piiramise alused on või võivad olla üldsõnalised. Andmesubjekti tutvumise õiguse piiramise alused IKS-is võimaldavad liiga laia kaalutlusruumi. Samas, tulenevalt IKS-ist on tutvumise õiguse piiramine võimalik seaduses sätestatud juhul. Seega ettenähtud kaalutlusruumi proportsionaalsuse lõplikuks hindamiseks on vaja analüüsida eriseadusi, milles peaks olema sätestatud tutvumise õiguse piiramise täpsemad asjaolud. Eriseadusena on näiteks mõistetav KrMS, milles piiramise asjaolud on sätestatud põhimõtteliselt sama üldsõnaliselt kui IKS-is, võimaldades liiga laia kaalutlusruumi. Vaja on täpsustada või muuta KrMS-i ja muid asjakohaseid seadusi. Õigusnorm peab võimaldama proportsionaalselt tutvumise õiguse piiramist, austades andmesubjekti isikuandmete ja teabega tutvumise õigust olenemata tema staatusest süüteomenetluses.

LIMITATIONS TO THE RIGHT OF ACCESS TO ONE'S OWN PERSONAL DATA AND INFORMATION ON PROCESSING OF IT BY THE DATA SUBJECT IN DATA PROCESSING BY THE POLICE. Summary

According to the Constitution of the Republic of Estonia (Constitution), the state has to protect a person from interference in their fundamental rights by another person (§ 13(1) first sentence). At everyone's right to liberty and security. In the interpretation of the European Court of Justice, the Art 6 of the Charter of Fundamental Rights (CFR) of the European Union (EU) ensures in addition to personal right to protection, the right to national and public security.

Estonian Police and Border Guard Board (PBGB, hereinafter also *police* or *data processor*) collects data and processes it by other ways. Data and analysis of it creates knowledge, which enables to ensure public security, prevent offences, and seek out truth in proceedings of offences. Likely, data is processed in large amounts, different ways, both digitally in PBGB's 26 information systems and by other means. In many cases, processing involves processing of someone's personal data. Therefore, almost any data processing activity by the police is interference to right to protection of personal data of the person, whose data is processed (hereinafter *data subject*). To verify lawfulness of processing, Art 8 (2) of the CFR and, § 44 (3) of the Constitution recognises right to apply access to one's own personal data and information on processing of this data.

This right of access by data subject is stipulated in the secondary law of the EU. In this Thesis, the Law Enforcement Directive 2016/680 (LED) of the EU is relevant, as it specifies rules on processing of personal data in the prevention, detection and proceedings of offences and execution of punishments (law enforcement purpose). Thereby, as the LED must be transposed to national law, author analyses in this thesis the data subject's right to have information and access to one's own personal data according to the Estonian Personal Data Protection Act (PDPA) § 24. According to the LED, national law must provide for the access right in two ways. For the first, data subject shall request confirmation concerning data processing on them from police. If data is processed, police is obliged to provide any personal data and information on processing of it to the data subject according to the PDPA § 24(1). As access is provided by the data processor, the term "direct access" will be used when referring to this form of the right of access.

However, the right of access is not absolute. The police have possibility to restrict the right of access. According to the PDPA § 24(2), this restriction shall be applied individually, be

necessary and proportionate measure and based on the circumstances provided by law. In some extreme cases, the data subject may not have any information from police. The second sentence of § 24(3) of the PDPA provides possibility to implement the "neither confirm nor deny" policy (neutral response), as called by the Article 29 Data Protection Working Party. If police have limited right of access, data subject may exercise right of access through the national supervisory authority. Consequently, the term "indirect access" is used here. In Estonia, the Data Protection Inspectorate (DPI) is the authority having right to verify the lawfulness of data processing by police.

Author is interested to analyse how the legislation foresees right of access of the data subject in conjunction with the possible need of the police to restrict access to data processing. Understanding of the regulations makes it possible to assess its applicability in practice to ensure effective protection of the rights of data subjects requesting access to personal data as well as rights of other data subjects involved in the processing. As regards national law-making, the report for the European Commission by TIPIK states that Estonia has not implemented all the elements of the direct access nor transposed in compliance the provisions of the indirect access nor right of access of the data subject during criminal proceedings. These findings indicate, that implementing of PDPA to solving application of right of access may lead to incorrect practice by PBGB and DPI. The main problem to examined is the compliance of the regulation of data subject's right to access and limitation of this right in the PDPA with Art 14, 15 and 17 of the LED. The purpose of the Thesis is to create understanding, if margin of the appreciation by the police is too broad, enabling excessive limitation of data subject's access right. Deriving from problem and purpose of the Thesis, author posed the following research questions:

- how is data subject's right to information and right to direct access regulated,
- how is restriction of data subject's right to direct access regulated and
- how is data subject's right to indirect access regulated.

The Thesis consist of four chapters. As a starting point, to clarify the basis for exercising the right of access, the scope of application of the PDPI and, the conditions for exercise of the direct access are analysed. To this end, scope of application of the CCP was analysed. As the pre-condition for data subject's right of access is to obtain information on the processing of data and on their rights, the right to information was analysed. In the following, the exercise of direct access is analysed. Namely, providing access to personal data and information related to processing of this data, including information on automated decisions. Having analysed the

direct access, the thesis moved on to analyse conditions of the limitations to the right of direct access. This means examining the legal base of the circumstances for restrictions and for their implementation, inter alia requirement to identify the data subject as a new possible limitation to providing access. To conclude, the conditions for indirect access are analysed in the meaning of possibilities of the national supervisory authority to verify the lawfulness of the limitation of right of access. Throughout the Thesis, the qualitative and comparative method is used.

Author concluded the following. The basis for the data subject's direct right of access in § 24(1) of the PDPA is broadly in accordance with the LED. The police is required to give confirmation of data processing and to ensure full access to personal data and information within the meaning of § 24(1) of the PDPA. The data subject does not need to submit a separate request for confirmation of data processing and access to personal data and information. They also have the right to obtain confirmation if their data is not processed by the police. In the opinion of the author, the clarification of the PDPA in the above-mentioned aspects needs to be considered.

As regards the basis for the right of access, the author states the following to develop the practice. The data subject's right of access concerns basic data relating to data processing, regardless of the location where the information concerning personal data, processing operations or processing is (e.g. log files). When responding to an application, all personal data, including the part that may be unlawfully processed, need to be rectified or should be deleted, must be submitted based on § 24(1) of the PDPA. Information on all processing operations referred to in § 24(1)(2)-(5) of the PDPA must also be submitted retroactively and pre-emptively in respect of one month's view in the part preceding the application, which is the time limit for replying to an application pursuant to § 27(2) of the PDPA. Although the PDPA does not require the submission of personal data in the form of a copy, this is a recommended practice. If proportionate, it is possible to apply restrictions on the submission of a copy based on § 24(2) of the PDPA. Information on processing can be provided in the form of a summary. In relation to an automated decision, information must be made public in general, or a specific decision must be communicated to the data subject, as it is not mandatory to provide information within the framework of the right of access.

The PDPA § 27(4) directs to communicate with the data subject in a situation where it is necessary to identify the person and the right of access. Art 12(5) of the LED allows requesting further information in relation to a reasonable doubt of the identity of the data subject. The provision in question does not comply with the principles governing the processing of personal

data. If generally applicable, excessive data processing in connection with identification can be interpreted as a ground for a full restriction and new basis for limitation of the right of access. In the author's opinion, it is necessary to specify in § 27(4) of the PDPA, as a condition of the police's discretion, reasonable doubt, or other conditions as to when and how the person of a data subject may be identified, including by requesting a signed application. In that regard, the author states that, to ensure that the data subject's right of access is effectively guaranteed, they must be answered based on his or her specific request and in a manner which assists him or her. The latter principle has not been clearly transposed into the PDPA, but it is important to remember when establishing the identity of the data subject.

Restriction of the data subject's right of access is an option that the police can use in the case provided by law. In the wording of the LED, the restriction can only be applied for as long as necessary and proportionate. In accordance with EU law, § 24(2) of the PDPA allows to restrict the right of access of a data subject only by way of exception, and also in § 24(3) the PDPA makes a distinction between the restriction of the right of access of the data subject in part (under § 24(2) in conjunction with the first sentence of subsection (3)) or in full (under § 24(2) in conjunction with the second sentence of subsection (3)). The broad definition of the temporal and substantive application of the restriction is not compatible with EU law. In the opinion of the author, it is necessary to stipulate expressly and in accordance with Art 15(1) of the LED that, after a certain period, it is necessary to over-assess whether the protection of the circumstances on which the restriction is based continues to be justified. It is excessive to apply a restriction where cause ceases to exist.

The circumstances of the restriction of the right of access of the data subject are set out in § 24(2)(1)-(5) of the PDPA. The data controller can override the data subject's right of access to the need to restrict his or her right of access in order to protect the prevention, detection, prosecution, or execution of a penalty; national security; public policy; a formal procedure, a formal investigation or the rights and freedoms of another person. For the ground for restriction to be applied, there must be at least one of the circumstances which may be damaged, endangered or hindered when right of access is granted (in full). The circumstances are formulated in the same general way as the objectives of protection referred to in points (a) to (e) of Art 15(1) of the LED, which are the basis for this provision. Outside the PDPA regulation, the question of to the compatibility with EU law arises related to the ground for restriction. The too wide discretion of the police and the excessive restriction of the right of access may occur if the circumstances prescribed in the PDPA have not been brought into the context of the

processing of data in the *lex specialis*. The question of the lawfulness of the restriction of the right of access also arises if the police have not carried out, on a case-by-case basis and regarding the application of each circumstance, an analysis of the necessity and proportionality of imposing a restriction pursuant to Art 52(1) of the CFR and § 11 and the second sentence of § 26 of the Constitution. It is therefore necessary to specify the discretion of the police in the sectoral law to ensure legal clarity and compliance of the basis for the application of the restriction with Art 15(1) of the LED.

For the purposes of applying § 24 of the PDPA, it is necessary to understand whether the police are processing personal data as a law enforcement authority for law enforcement purposes. Conditionally, whether the data processing concerns a specific suspicion attributable to the data subject in relation to the prevention, detection, or prosecution of an offence within the meaning of the Estonian Penal Code or the execution of punishments. In Estonian law, there is no legal definition of the term "prevention of an offence". The practical complexity or impossibility of defining the purpose of data processing in relation to the collection, analysis or other processing of data may lead to a situation where the request of a data subject is resolved pursuant to § 24 of the PDPA, which allows for a more intense interference with a fundamental right. According to the author, it is necessary to define more clearly the scope of the PDPA in the context of guaranteeing the right of access.

The § 24(4) of the PDPA refers to the exercise of the data subject's indirect right of access, according to which the police must inform the data subject of his or her right of access to appeal the decision restricting the right of access to the DPI or to a court. According to the author, an indirect right of access is possible not in a situation where the right of access is theoretical, but in a situation where actual access is restricted. Thus, if the data subject considers that a restriction on the right of access is discriminatory or excessively prejudicial to their other fundamental rights and freedoms or does not have any information concerning the processing of data due to the restriction of the full right of access, he or she is able to exercise his or her rights through the DPI. In accordance with Art 17(1) of the LED, the legislator has considered the exercise of the indirect right of access in the PDPA as an additional right to exercise the right of direct access and not as the exclusive or substituting right of direct access. In the opinion of the author, to transpose the first sentence of Art 17(3) and Art 46(1)(g) of the LED in full, it is necessary to specify the procedure of the DPI, in § 28. The data subject must be made aware of the nature of the indirect right of access and the task of the DPI to verify, in substance and independently, the lawfulness of the processing and restriction of personal data; the right not to

carry out checks on the PBGB or to restrict the data subject's right to be informed about the above. The PDPA lays down the right of the data subject to challenge a decision taken by DPI based on a complaint before a court, but it is necessary to indicate the right to challenge a decision taken in the context of an indirect right of access. The exercise of the data subject's indirect right of access does not preclude recourse to the DPI based on § 28(1) of the PDPA if, in the opinion of the data subject, the police interferes his or her rights when processing personal data.

The Code of Criminal Procedure (CCP) is applied by the police as a basis for the right of access in the context of criminal proceedings. In principle, the regulation of § 15^2 (3) of the CCP is not in conformity with Art 18 of the LED, because it does not clearly show how specific rights guaranteed by data protection law can be exercised by a data subject in the framework of criminal proceedings in so far as they do not derive from criminal procedural law, including personal data not collected by an act of criminal procedure. Nor can it be seen from what rights arising from the PDPA and how the data subject can exercise, considering that no overlaps or differences in the application of the regulations have been laid down in the PDPA or the CCP. In the opinion of the author, it is necessary to specify in § 15^2(3) of the CCP that the provisions thereof may apply to a certain extent in parallel to other regulations in the CCP, as well as which are applicable in parallel to the PDPA as regards the right of access in situations where there is no special regulation in the CCP.

The CCP § $15(^2)$(4)-(5) sets out the grounds for the restriction of the right of access and the information covered by the restriction. The provision contains more precise grounds concerning only legal proceedings and additionally provides for the right to restrict the right of access for the protection of the data subject himself or herself (second part of the sentence of § 15^2 (4) of the CCP). Such a wide discretion to restrict a fundamental right is incompatible with EU law and its interpretation, as the author pointed out in the case of PDPA. Furthermore, the application of the restriction of the full right of access under data protection law in the context of criminal proceedings is unclear in the CCP. If, like the second sentence of § 24(3) of the PDPA, the legislator wishes to allow a neutral response to the data subject, the CCP must be amended accordingly.

In terms of legal basis, there is no legal clarity for the effective enforcement of the rights of the data subject after criminal proceedings, including the presentation of the criminal file. The decision on the right of access is no longer a decision affecting criminal proceedings or, more

broadly, data processing for law enforcement purposes. Among other things, the need to limit the right of full access should, as a rule, be no longer necessary at the end of the criminal proceedings. Accordingly, it is not possible to apply § 24 of the PDPA or §15(^{2})(3)-(5) of the CCP. It is therefore necessary to establish a precise and clear legal basis for the exercise of the right of access in this case, in accordance with data protection law. Preferably in the CCP to highlight more clearly the links or differences between data protection law and criminal procedural law in the exercise of the right of access during and after criminal proceedings.

The exercise of the indirect right of access or the right of appeal in the procedure for direct access and restriction thereof does not preclude the exercise of judicial review regarding the PBGB or the DPI based on Art 47 of the CFR and § 15 of the Constitution. Although the protection of personal data and, more specifically, the right of access of the data subject is a fundamental right guaranteed by EU primary law, the Constitution plays an additional role in ensuring the protection of personal data in the constitutional review procedure if the application of a national provision is not fully regulated by EU law. It is possible to verify the lawfulness of the restriction of the right of access and the compliance with EU law in the Supreme Court on the basis of the Constitution, not immediately in the European Court of Justice.

The police have the obligation to make publicly available to the data subject the information specified in § 22(1) of the PDPA, including on the right of access of the data subject. Accordingly, the PPA has published data protection terms on its website. In the opinion of the author, the PPA's data protection conditions are too general and need to be clarified in order to give the data subject a clear and as accurate overview of the data processing by the police, including its purposes.

The regulation of the data subject's right of access shows how everyone's right to personal security, national security and public order enables to interfere to everyone's right to the protection of personal data. The data subject's fundamental right of access to personal data is at first sight opposed to the possibility for the police to restrict the right of access of the data subject. A discussion has been launched in scientific literature and case-law on how to assess the proportionality of the discretion to restrict the right of access of a data subject. The question is whether fundamental rights must be balanced or placed in a hierarchy. Irrespective of the method of assessing proportionality, it is important to carry out a comprehensive and case-by-case assessment of the police's restriction of the right of access, where the grounds for restriction of access laid down by law are or may be generalised. The grounds for restricting

the right of access of the data subject in the PDPA allow for an excessive margin of discretion. However, as a result of the PDPA, it is possible to restrict the right of access in the case provided by law. Thus, in order to make a definitive assessment of the proportionality of the discretion provided for, it is necessary to examine specific laws which should set out more specific circumstances in which the right of access is restricted. For example, the CCP can be understood as a special law, in which the circumstances of the restriction are laid down in principle in the same general terms as the PDPA, allowing for too wide discretion. It is necessary to clarify or amend the CCP and other relevant laws. The provision must allow for a proportionate limitation of the right of access, respecting the data subject's right of access to personal data and information, irrespective of his or her status in criminal proceedings.

KASUTATUD KIRJANDUS

1. Alexy, R. Kollisioon ja kaalumine kui põhiõiguste dogmaatika põhiprobleemid, lk 5–13. – Juridica 2001/1.
2. Alexy. R., Põhiõigused Eesti põhiseaduses, lk 5–96. – Juridica 2001/ eriväljaanne.
3. Ausloos, J., Mahieu, R., Veale, M. Getting Data Subject Rights Right. A submission to the European Data Protection Board from international data rights academics, to inform regulatory guidance. 10 (2020) Journal of Intellectual Property, Information Technology and E-Commerce Law 283 para 1. – https://www.jipitec.eu/archive/issues/jipitec-10-3-2019/5031 (18.03.2024).
4. Bogdanov. D., Siil, T. Infotehnoloogilised võimalused põhiõiguste kaitsel, lk 474–481. – Juridica 2020/6.
5. Dalla Corte, L., On proportionality in the data protection jurisprudence of the CJEU. International Data Privacy Law, Volume 12, Issue 4, November 2022, lk 259–275. – https://doi.org/10.1093/idpl/ipac014 (04.02.2024).
6. De Hert, P., Papakonstantinou, V. The New Police and Criminal Justice Data Protection Directive: A First Analysis (2016), lk 7–19. – https://ssrn.com/abstract=3447072 (05.03.2024).
7. De Hert, P., Sajfert, J. Regulating Big Data in and out of the Data Protection Policy Field: Two Scenarios of Post-GDPR Law-Making and the Actor Perspective. European Data Protection Law Review, Volume 5, Issue 3, 2019, lk 338–351. – https://doi.org/10.21552/edpl/2019/3/8 (21.02.2024).
8. Den Boer, M. (ed.). Comparative Policing from a Legal Perspective. 2018, lk 306–327. – https://doi.org/10.4337/9781785369117 (05.03.2024).
9. Dimitrova, D., De Hert, P. The LED's right of Access to one's data: Loopholes on proper access, legality review and data protection authority. Accountability. New Journal of European Criminal Law 2023, Volume 0(0), lk 1–21. – https://doi.org/10.1177/20322844231214484 (05.02.2024).
10. Dimitrova, D. The Right to Explanation under the Right of Access to Personal Data: Legal Foundations in and Beyond the GDPR. European Data Protection Law Review, Volume 6, Issue 2 (2020), lk 211– 230. – https://doi.org/10.21552/edpl/2020/2/8 (18.03.2024).
11. Eesti Vabariigi põhiseadus. Kommenteeritud vlj. 2020.
12. Euroopa Liidu põhiõiguste harta. Selgitused põhiõiguste harta kohta. Euroopa Põhiõiguste Amet. – https://fra.europa.eu/et/search?search_api_fulltext_3=selgitused+p%C3%B5hi%C3%B5iguste+harta+kohta+ / (12.03.2024).

13. Ernits, M. Põhiõigused, demokraatia, õigusriik. Tartu: Tartu Ülikooli Kirjastus 2011.
14. Gellert, R. Discussion On Risk, Balancing, and Data Protection: A Response to van der Sloot. – European Data Protection Law Reviev Volume 3, Issue 2 (2017), lk 180–186. – https://doi.org/10.21552/edpl/2017/2/7 (04.02.2024).
15. Kosta, E. (ed. et al.). The EU Law Enforcement Directive (LED). A Commentary. Oxford University Press 2024.
16. Laaring, M. jt. Korrakaitseseadus. Kommenteeritud vlj. Sisekaitseakadeemia 2017.
17. Leiser, M.R., Custers, B.H.M. 2019. The Law Enforcement Directive: Conceptual Issues of EU Directive 2016/680, European Data Protection Law Review. Volume 5, Issue 3, lk 367–378. – https://ssrn.com/abstract=4014545 (05.03.2024).
18. Narits, R. Eesti õiguskord ja väärtusjurisprudents, lk 2–6. – Juridica 1998/1.
19. Narits, R. Jurisprudentsi põhijoontest, lk 378–380. – Juridica 1995/9.
20. Rosentau, M. Infoühiskond ja tema vajadused, lk 453–496. – Akadeemia 2015/3.
21. Rosentau, M. Tõendamine teadmise standardmudelis, lk 188–205. – Juridica 2001/III, lk 202.
22. Sajfert, J., Quintel, T. 2017. Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities, lk 1–22. – https://ssrn.com/abstract=3285873 (21.02.2024).
23. Van Der Sloot, B. Editorial. European Data Protection Law Review, Volume 3, Issue 1 (2017), lk 1–12. – https://doi.org/10.21552/edpl/2017/1/3 (30.03.2024).
24. Vogiatzoglou, P. (et al.). From Theory To Practice: Exercising The Right Of Access Under The Law Enforcement And PNR Directives. 11 (2020) Journal of Intellectual Property, Information Technology and E-Commerce Law 274 para 1. – https://www.jipitec.eu/archive/issues/jipitec-11-3-2020/5191 (18.03.2024).

KASUTATUD ÕIGUSAKTID

25. Avaliku teabe seadus. – RT I, 07.03.2023, 11.
26. Euroopa Liidu põhiõiguste harta. – ELT C 202, 07.06.2016, lk 389–405.
27. Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/680, 27. aprill 2016, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK. – ELT L 119, 04.05.2016, lk 89–131.
28. Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi

95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (EMPs kohaldatav tekst). – ELT L 119, 04.05.2016, lk 1–88.
29. Eesti Vabariigi põhiseadus. – RT I, 15.05.2015, 2.
30. Isikuandmete kaitse seadus. – KRT I, 11.03.2023, 11.
31. Isikuandmete kaitse seaduse rakendamise seadus. – RT I, 13.03.2019, 2.
32. Julgeolekuasutuste seadus. – RT I, 31.12.2022, 11.
33. Kaitseväe korralduse seadus. – RT I, 26.05.2020, 9.
34. Karistusseadustik. – RT I, 06.08.2022, 27.
35. Korrakaitseseadus. – RT I, 14.03.2023, 29.
36. Kriminaalmenetluse seadustik. – RT I, 06.07.2023, 49.
37. Nõukogu raamotsus 2008/977/JSK, 27. november 2008, kriminaalasjades tehtava politsei- ja õigusalase koostöö raames töödeldavate isikuandmete kaitse kohta. – EL T 350, 30.12.2008, lk 60–71.
38. Politsei andmekogu põhimäärus. SiMm 22.12.2009 nr 92. – RT I, 25.08.2023, 5.
39. Politsei- ja piirivalveameti põhimäärus. SiMm 17.07.2014 nr 33. – RT I, 12.11.2022, 4.
40. Politsei ja piirivalve seadus. – RT I, 06.07.2023, 64.
41. Väärteomenetluse seadustik. – RT I, 22.03.2024, 10.

KASUTATUD EELNÕUD JA SELETUSKIRJAD

42. Council of Europe Committe of Ministers Explanatory Memorandum to Recommendation No. R (87) 15 of the Committee of Ministers to member states regulating the use of personal data in the police sector (Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies). – https://rm.coe.int/168062dfd4 (01.04.2024).
43. Isikuandmete kaitse seaduse 679 SE seletuskiri. – https://www.riigikogu.ee/download/b7c9371a-7768-46b5-9d33-9eb4e3b98125 (13.04.2024).
44. Isikuandmete kaitse seaduse 679 SE seletuskirja lisa. – https://www.riigikogu.ee/download/74b9da11-92a6-443e-8aaa-d455b2ba73cb (13.04.2024).
45. Isikuandmete kaitse seaduse rakendamise seaduse 778 SE seletuskiri. – https://www.riigikogu.ee/download/0629e042-d72a-4ae7-b885-58ec0fce0efc (13.04.2024).

46. Korrakaitseseaduse SE 49 seletuskiri. – https://www.riigikogu.ee/download/a67e1f77-6a73-26c5-5648-71b05c92d979 (13.04.2024).

KASUTATUD KOHTUPRAKTIKA

47. EKo C-553/07, *College van burgemeester en wethouders van Rotterdam* versus *M.E.E. Rijkeboer*, ECLI:EU:C:2009:293.
48. EKo C-141/12, *YS* versus *Minister voor Immigratie, Integratie en Asiel*, ECLI:EU:C:2014:2081.
49. EKo C-293/12, *Digital Rights Ireland Ltd* versus *Minister for Communications, Marine and Natural Resources jt ja Kärntner Landesregierung jt*, ECLI:EU:C:2014:238.
50. EKo C-362/14, *Maximillian Schrems* versus *Data Protection Commissioner*, ECLI:EU:C:2015:650.
51. EKo C-434/16, *Peter Nowak* versus *Data Protection Commissioner*, ECLI:EU:C:2017:994.
52. EKo C-817/19, *Ligue des droits humains ASBL* versus *Conseil des ministres*, ECLI:EU:C:2022:491.
53. EKo C-154/21, *RW* versus *Österreichische Post AG*, ECLI:EU:C:2023:3.
54. EKo C-180/21, *VS* versus *Inspektor v Inspektorata kam Visshia sadeben savet*, ECLI:EU:C:2022:967.
55. EKo C-487/21, *F.F.* versus *Österreichische Datenschutzbehörde*, ECLI:EU:C:2023:369.
56. EKo C-579/21, *J.M.* versus *Apulaistietosuojavaltuutettu ja Pankki S*, ECLI:EU:C:2023:501.
57. EKo C-118/22, *NG* versus *Direktor na Glavna direktsia „Natsionalna politsia“ pri Ministerstvo na vatreshnite raboti – Sofia*, ECLI:EU:C:2024:97.
58. EKo C-205/21, *V.S.*, *menetluses osales Ministerstvo na vatreshnite raboti, Glavna direktsia za borba s organiziranata prestapnost*, ECLI:EU:C:2023:49.
59. EKo C-333/22, *Ligue des droits humains ASBL, BA versus Organe de contrôle de l'information policière*, ECLI:EU:C:2023:874.
60. RKHKm 3-3-1-58-16.
61. RKHKo 3-16-2348/21.
62. RKHKo 3-3-1-84-15.
63. RKHKo 3-20-332/39.
64. RKHKo 3-20-1265.
65. RKKKm 3-1-1-116-04.

66. RKKKo 1-19-8262.
67. RKÜKo 5-19-29.
68. RKPJKo 5-19-38.
69. TlnHKm 3-19-2110/14.
70. TlnHKo 3-19-1076/10.
71. TlnRnKHKm 3-19-2110/25.
72. TlnRnKHKo 3-19-743/33.
73. TlnRnKo 3-19-1076/16.

KASUTATUD JUHENDID JA ARUANDED

74. Arvamus direktiivi (EL) 2016/680 mõne olulise aspekti kohta. Artikli 29 alusel asutatud andmekaitse töörühm. WP 258. Vastu võetud 29.11.2017. – https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610178 (05.03.2024).
75. Guidelines 01/2022 on data subject rights – Right of Access. Version 2.0. European Data Protection Board. Adopted 28.03.2023. – https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf (05.03.2024).
76. Isikuandmete töötlemise üldjuhend. Andmekaitse Inspektsioon. Kinnitatud 31.05.2018. Muudetud 28.09.2018. Muudetud 19.03.2019. – https://www.aki.ee/sites/default/files/dokumendid/isikuandmete_tootleja_uldjuhend.pdf (12.03.2024).
77. Esimene aruanne õiguskaitse valdkonnas isikuandmete kaitset käsitleva direktiivi (EL) 2016/680 (õiguskaitsedirektiiv) kohaldamise ja toimimise kohta. Komisjoni teatis Euroopa Parlamendile ja nõukogule COM/2022/364 final. 25. juuli 2022. – https://ec.europa.eu/info/publications/communication-commission-european-parliament-and-council-first-report-application-and-functioning-data-protection-law-enforcement-directive-eu-2016-680-led_et (05.03.2024).
78. Euroopa Liidu põhiõiguste harta kohaldamine õigusaktides ja poliitikakujundamises riigi tasandil. Suunised. Euroopa Liidu Põhiõiguste Amet 2020. – https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-charter-guidance_et.pdf (05.03.2024).
79. Mikiver, M. Analüüs. Andmekogud ja isikuandmed: EV Põhiseadusest ja IKÜM-st tulenevad nõuded regulatsioonile. Justiitsministeerium 2021. – https://www.just.ee/uuringud (17.03.2024).

80. Seadusliku aluseta profiilide koostamise tõkestamine nüüd ja tulevikus: juhend. Euroopa Liidu Põhiõiguste Amet 2022. – https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-preventing-unlawful-profiling-guide_et.pdf (05.03.2024).
81. Statement on the role of a risk-based approach in data protection legal frameworks. Article 29 Data Protection Working Party. 14 EN/WP218. Adopted 30.05.2014. – https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf (09.04.2024).
82. Statement on restrictions on data subject rights in connection to the state of emergency in Member States. European Data Protection Board. Adopted 02.06.2020. – https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-restrictions-data-subject-rights-connection-state_en (09.04.2024).
83. TIPIK 2020: TIPIK Legal, "Report on the Transposition of Directive (EU) 2016/680", Report for the European Commisson, November 2020 (viidatud The EU Law Enforcement Directive (LED). A Commentary. Kosta, E. (ed. et al.). Oxford University Press 2024. – https://doi.org/10.1177/20322844231214484 (31.03.2024).
84. Vogiatzoglou, P., Marquenie, T. Assessment of the implementation of the Law Enforcement Directive. Policy Department for Citizens' Rights and Constitutional Affairs. Directorate-General for Internal Policies. PE PE 740.209. December 2022. – https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740209/IPOL_STU(2022)740209_EN.pdf (05.03.2024).

MUUD KASUTATUD ALLIKAD

85. Boniface, C. (et al.). Security Analysis of Subject Access Request Procedures How to authenticate data subjects safely when they request for their data. APF 2019 – Annual Privacy Forum, Jun 2019, Rome, Italy, lk 1–20. – https://hal.inria.fr/hal-02072302 (18.03.2024).
86. Carson, A., Fake DSARs: They're a thing? – https://iapp.org/news/a/fake-dsars-theyre-a-thing/ (03.04.2024).
87. Collins English Dictionary. HarperCollins Publishers. – https://www.collinsdictionary.com/dictionary/english/function-creep (26.11.2020).
88. Decision of the European Data Protection Supervisor in complaint case 2020-0908 against the European Agency for Law Enforcement Cooperation (Europol). – https://edri.org/wp-content/uploads/2022/09/22-09-08_EDPS-Decision_2020-0908_redacted.pdf (09.04.2024).

89. Decision on the retention by Europol of datasets lacking Data Subject Categorisation (Cases 2019-0370 & 2021-0699). European Data Protection Supervisor. – https://edps.europa.eu/system/files/2022-01/22-01-10-edps-decision-europol_en.pdf (09.04.2024).
90. Decision on the own initiative inquiry' on Europol's big data challenge. 18.09.2020. WW/xx/vm/ D(xxx) xxx C 2019-0370. European Data Protection Supervisor. – https://edps.europa.eu/data-protection/our-work/publications/investigations/edps-decision-own-initiative-inquiry-europols_en (05.03.2024).
91. Eesti märksõnastik. – https://ems.elnet.ee/index.php (07.04.2024).
92. EK C-553/07, *College van burgemeester en wethouders van Rotterdam* versus *M.E.E. Rijkeboer*, ECLI:EU:C:2008:773, kohtujurist D. Ruiz-Jarabo Colomer ettepanek.
93. EK C-817/19, *Ligue des droits humains ASBL* versus *Conseil des ministres*, ECLI:EU:C:2022:65, kohtujurist G. Pitruzzella ettepanek.
94. EK C-129/21, *Proximus NV (üldkasutatavad elektroonilised kataloogid)* versus *Gegevensbeschermingsautoriteit*, ECLI:EU:C:2022:332, kohtujuristi M. Collins ettepanek.
95. EK C-487/21, *F.F.* versus *Österreichische Datenschutzbehörde*, ECLI:EU:C:2022:1000, kohtujurist G. Pitruzzella ettepanek.
96. EK C-481/21, *TX* versus *Bundesrepublik Deutschland*, eelotsusetaotlus.
97. EK C-118/22, *NG* versus *Direktor na Glavna direktsia „Natsionalna politsia" pri Ministerstvo na vatreshnite raboti – Sofia*, ECLI:EU:C:2023:483, kohtujurist P. Pikamäe ettepanek.
98. Galič, M., Lonneke Stevens, L., Koops, B.-J. Editorial: A trialogue on regulating data-driven criminal procedure. New Journal of European Criminal Law. Volume 14, Issue 4. December 2023. – https://doi.org/10.1177/20322844231213484 (04.02.2024).
99. Kolza, D., Drechsler, L. Proportionality has come to the GDPR (9 December 2020). – https://europeanlawblog.eu/2020/12/09/proportionality-has-come-to-the-gdpr/ (30.03.2024).
100. Medina, M. (ed. et al.). Privacy Technologies and Policy. APF 2018. Lecture Notes in Computer Science, vol 11079. Springer, Cham, pp 111–130. – https://doi.org/10.1007/978-3-030-02547-2_7 (05.03.2024).
101. Määrus, EK president 09.08.2022, C-481/21, *TX* versus *Bundesrepublik Deutschland*, Verwaltungsgericht Wiesbadeni eelotsusetaotlus – Saksamaa registrist kustutamiseks. – ELT C 422, 18.10.2021.

102. Parrest, N., Juha, M. Arutama hakatakse andmesubjekti kaebust kohustamaks maakohut väljastama teavet andmesubjekti isikuandmete töötlemise kohta. Kohtute aastaraamat 2020. – https://aastaraamat.riigikohus.ee/arutama-hakatakse-andmesubjekti-kaebust-kohustamaks-maakohut-valjastama-teavet-andmesubjekti-isikuandmete-tootlemise-kohta/ (13.01.2023).
103. PPA andmekaitsetingimused. – https://www.politsei.ee/et/juhend/isikuandmete-toeoetlemine ja https://www.politsei.ee/et/schengeni-piirikontroll (05.03.2024).
104. PPA rahvusvahelised koostööpartnerid. – https://www.politsei.ee/et/juhend/rahvusvaheline-koostoeoe (25.03.2024).
105. Riigi infosüsteemi haldussüsteemi infosüsteemide kataloog. – https://www.riha.ee/Infos%C3%BCsteemid?searchText=politsei-%20ja%20piirivalveamet&sort=meta.update_timestamp&dir=DESC (05.03.2024).
106. Pöördumine õiguskomisjoni poole seoses eelnõuga 680 SE. JuM 28.01.2019 kiri nr 10-4/720-1. – https://www.riigikogu.ee/download/1b65d0fe-cec0-4571-ab45-b8f6b0524c5e (13.04.2021), lisa lk 13.
107. Vaideotsus ja ettekirjutus-hoiatus. AKI 07.05.2021 nr 2.1-3/21/1208. – https://www.aki.ee/sites/default/files/vaideotsus_ja_ettekirjutus-hoiatus_07.05.2021_avaliku_teabe_asjas_nr_2.1.-3_21_1208_politsei-_ja_piirivalveameti_ida_prefektuur_-_eraisik.pdf (28.01.2024).
108. Vaideotsus. AKI 14.01.2020 nr 2.1-3/19/4361. – https://www.aki.ee/sites/default/files/vaideotsused/2020/vaideotsus_14.01.2020_avaliku_teabe_asjas_nr_2.1.-3-19-4361_-_eraisik_-_politsei-_ja_piirivalveameti_laane_prefektuur.pdf (28.01.2024).
109. Vallimäe-Tuberg, K. II Isikuandmed kohtus IKÜM-i ajastul. Kohtutoimik kohtu arhiivis. Kohtute aastaraamat 2020. – https://aastaraamat.riigikohus.ee/kohtutoimik-kohtu-arhiivis/ (26.03.2024).
110. Varik, H.. E-identiteet Eesti ja Euroopa Liidu õigusruumis: Euroopa Parlamendi ja Nõukogu eidentimise ja e-tehingute jaoks vajalike usaldusteenuste määruse kohaldamine Eestis – kujunemislugu, probleemid ja eelseisvad väljakutsed. Magistritöö. – Tallinn: Tartu Ülikool, 2015.
111. Vastus nõudekirjale. AKI 20.01.2021 nr 2.1.-5/21/219. – https://www.aki.ee/meist/teadlikkus/dokumendiregister (11.04.2024).

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, Jenny Jakobson,

(autori nimi)

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

Andmesubjekti enda kohta käivate isikuandmete ja nende töötlemise kohta käiva teabega tutvumise õiguse piiramine politsei andmetöötluses,

(lõputöö pealkiri)

mille juhendaja on Dr. Paloma Krõõt Tupay,

(juhendaja nimi)

reprodutseerimiseks eesmärgiga seda säilitada, sealhulgas lisada digitaalarhiivi DSpace kuni autoriõiguse kehtivuse lõppemiseni.

2. Annan Tartu Ülikoolile loa teha punktis 1 nimetatud teos üldsusele kättesaadavaks Tartu Ülikooli veebikeskkonna, sealhulgas digitaalarhiivi DSpace kaudu Creative Commonsi litsentsiga CC BY NC ND 4.0, mis lubab autorile viidates teost reprodutseerida, levitada ja üldsusele suunata ning keelab luua tuletatud teost ja kasutada teost ärieesmärgil, kuni autoriõiguse kehtivuse lõppemiseni.

3. Olen teadlik, et punktides 1 ja 2 nimetatud õigused jäävad alles ka autorile.

4. Kinnitan, et lihtlitsentsi andmisega ei riku ma teiste isikute intellektuaalomandi ega isikuandmete kaitse õigusaktidest tulenevaid õigusi.

Jenny Jakobson

29.04.2024