TARTU ÜLIKOOL
ÕIGUSTEADUSKOND
Karistusõiguse osakond

Piret Muinast

ISIKUANDMETE KAITSE NÕUETE RIKKUMISE SANKTSIONEERIMINE ENNE JA PÄRAST EUROOPA LIIDU ANDMEKAITSEREFORMI VALGUSES

Magistritöö

Juhendaja: *prof* Jaan Sootak
Kaasjuhendaja: Julia Antonova, *MA*

Tartu
2018

SISUKORD

SISSEJUHATUS

Tänapäeval on tehnoloogia muutunud lahutamatuks osaks igapäevaelust – inimestel on võimalik suhelda tehnoloogiliste rakenduste abil, osta veebipoest toitu, autod saavad õnnetuse korral kutsuda ise välja päästeteenistuse jt. Selleks, et tehnoloogia saaks toimida, vajab see teavet. Erinevad tehnoloogilised lahendused koguvad suurel hulgal andmeid, sealhulgas võivad andmed sisaldada ka teavet isiku eraelu, harjumuste, töö, toidueelistuste ja muude asjaolude kohta. Kuigi tehnoloogia võib kujutada endast ohtu, võib tehnoloogia ka pakkuda lahendust privaatsuse kaitsmisel.[1] Tehnoloogia võib tõhustada andmete kaitsmist ning anda uusi teadmisi automatiseeritud andmetöötluses. Tänu uuenenud tehnoloogiale on võimalik tagada parem andmekaitse, kuna andmete töötlemine on muutunud turvalisemaks ning võimaldab kontrollida andmetöötlejate tegevust. Eelkõige peaks see vähendama töötlejate poolset andmete kuritarvitamist ning andma isikule võimaluse kontrollida oma andmete töötlemist, st teada kes, milliseid andmeid, mille jaoks kogub ja vajadusel nõuda töötlemise lõpetamist või andmete kustutamist. Tehnoloogia abil võib kombineerida erinevaid andmeid nii, et iseenesest vähetähtsad andmed moodustavad kogumi ning koguda ja levitada andmeid üle kogu maailma. Igal juhul peab andmekaitse aspekt olema infosüsteemide hindamisel osa nii selle kaudu, kuidas süsteem aitab tagada paremat andmekaitset, kui ka selle kaudu, missuguseid võimalikke ohte see esile toob ja kuidas nende vastu võidelda tõhusalt ja samas proportsionaalselt.[2] Kiirelt areneva tehnoloogiaga peab sammu pidama privaatsusõigus ja andmekaitse, esitades samas väljakutseid ka õigussüsteemile, et rakendada tõhusalt õigusnorme.

P. K. Tupay on öelnud: ”E-riigiga kaasnevate võimaluste, ohtude ja probleemide analüüs ning avatud mõttevahetus võib anda aluse nüüdisaegsele isikuandmete kaitse käsitlusele tingimusel, et õpime isikuandmete kaitses nägema enamat kui digitaalse arengu pidurit”[3]. Eesti riik on maailmas tuntud uudsete infotehnoloogiliste lahenduste poolest, kuid kiire tehnoloogia areng vajab ka vastavat õigusraamistikku isikuandmete kaitsel. Infoajastuga kaasneb paratamatult ka andmete töötlemise kuritarvitamist ning andmekaitseõiguse rikkumist. Seega on isikuandmete kaitse normidel väga oluline eesmärk - kaitsta üksikisiku privaatsust. Andmekaitse keskmes on

[1] S. Gutwirth, Y. Poullet, P. D. Hert, C. Terwangne, S. Nouwt Editors „.Reinventing Data Protection?“,?, Springer Science+Business Media B.V.2009.
[2] K. Nyman Metcalf. Privaatsusõigus inimõigusena ja igapäevatehnoloogiad. Privaatõiguse ja andmekaitse õiguslikud aspektid. Inimõiguste Instituut. Uuring 2014, V osa lk 82. Arvutivõrgus: https://humanrightsestonia.ee/wp/wp-content/uploads/2014/11/EST-Uuringu-V-osa-Privaat%c3%b5iguse-ja-andmekaitse-%c3%b5iguslikud-aspektid.pdf (31.01.2018).
[3] P. K. Tupay. Õigusest eraelule kuni andmekaitse üldmääruseni ehk tundmatu õigus isikuandmete kaitsele. - Juridica 2016 / 4, lk 240.

andmesubjekt ehk isik, kelle andmeid töödeldakse. Isikuandmete töötlemise all käsitletakse mis tahes toiminguid inimese kohta käivate andmetega, nt isikuandmete kogumine, salvestamine, säilitamine, edastamine ja avalikustamine. Isikuandmete töötlemisel tuleb järgida kindlaid põhimõtteid, mis aitavad saavutada andmekaitse eesmärke. Need on seaduslikkuse, eesmärgikohasuse, minimaalsuse, kasutuse piiramise, andmete kvaliteedi, turvalisuse ja andmesubjekti osaluse põhimõte.[4]

Isikuandmete käibe õiguslik reguleerimine on võrdlemisi uus trend. Esimesed otseselt isikuandmete käibe piiramisele suunatud õigusaktid pärinevad 1970. aastatest.[5] Samas elame maailmas, kus info- ja kommunikatsioonitehnoloogia areneb suure kiirusega ning oluline roll on isikutel ja nendega seonduvatel andmetel. Sellise infoühiskonnaga tuleb juurde erinevaid e-teenuseid ning inimestel on oluline teada milliseid andmeid, kes kogub ja mis eesmärgil. Andmete kogumisel peab selgelt teadma, mis eesmärki andmete kogumine teenib ning millised andmed on selle eesmärgi jaoks vajalikud.

Isikuandmete kaitse reguleerimisel on liikmesriigid seotud Euroopa Liidu (*edaspidi EL*) õigusega. Isikuandmete kaitse aluseks on põhiõiguste harta[6] artikkel 8, mis sätestab õiguse isikuandmete kaitsele iseseisva põhiõigusena. Artiklis on öeldud, et igaühel on õigus oma isikuandmete kaitsele. Selliseid andmeid tuleb töödelda asjakohaselt ning kindlaksmääratud eesmärkidel ja asjaomase isiku nõusolekul või muul seaduses ettenähtud õiguslikul alusel. Igaühel on õigus tutvuda tema kohta kogutud andmetega ja nõuda nende parandamist. Nende sätete täitmist kontrollib sõltumatu asutus. Kehtiva EL andmekaitse direktiivi 95/46/EÜ[7] (*edaspidi direktiiv 95/46/EÜ*) artiklit 4 järgi kohaldatakse isikuandmete töötlemisel selle liikmesriigi siseriiklikke õigusnorme, kelle territooriumil on registreeritud andmete vastutav töötleja. Alates 25. maist 2018 kehtima hakkava andmekaitse üldmääruse[8] (*edaspidi* üldmäärus) eesmärk on ühtlustada andmekaitse õiguslikku regulatsiooni kõigis liikmesriikides.

[4] M. Männiko. Õigus privaatsusele ja andmekaitse. Tallinn: Juura 2011, lk 44-47.
[5] A. Nõmper, E. Tikk. Informatsioon ja õigus. Tallinn: Juura 2007, lk 66.
[6] Euroopa Parlament. Nõukogu. Komisjon. Euroopa Liidu põhiõiguste harta. (2010/C 83/02). ELT C 83/389, 30.03.2010.
[7] Euroopa Parlamendi ja nõukogu direktiiv 95/46/EÜ, 24.10.1995, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. – EL TELT L 281, 23.11.1995. Arvutivõrgus: http://eur-lex.europa.eu/legal content/ET/TXT/HTML/?uri=CELEX:31995L0046&from=ET
[8] 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 kaitseüldmäärus). – ELT L 119, 04.05.2016

Eesti õiguses on igaühel Eesti Vabariigi põhiseaduse[9] (*edaspidi PS*) §-st 26 tulenev õigus perekonna- ja eraelu puutumatusele. Isikuandmete kaitse seaduse[10] (*edaspidi IKS*) § 1 lg 1 rõhutab omakorda veelgi, et eesmärgiks on kaitsta isikuandmete töötlemisel füüsilise isiku põhiõigusi ja –vabadusi, eelkõige õigust eraelu puutumatusele.

Privaatsuse kaitse nõue tähendab vajadust tõhusalt reguleerida isikuandmete töötlemist, arvestades samas ka vajadusega tasakaalustada õigust privaatsusele teiste põhiõiguste ja ühiskonna toimimisega laiemalt. Nagu eespool viidatud, on laiaulatuslik andmete töötlemine kaasaegse elu lahutamatu osa, mistõttu lasub seadusandjal kohustus kehtestada normid, mis ühelt poolt võimaldavad ühiskonna tõhusat toimimist ning tehnoloogia arengut ja teiselt poolt kindlustavad igaühe õigust eraelu puutumatusele ja isikuandmete kaitsele. Olukorras, kus ettevõtete huvi[11] andmete vastu järjest kasvab, muutub väga aktuaalseks isikuõiguste jõustamiseks ettenähtud meetmed. Autori hinnangul on ilmne, et ülemaailmse haardega tehnoloogiaettevõttetel on ulatuslikud võimalused koguda teavet isiku teadmata, tuues turule järjest uuemaid ja nutikamaid lahendusi, mis ühelt poolt pakuvad kasutajale mugavust, kuid teiselt poolt talletavad kasutaja kohta hulgaliselt andmeid, mis omakorda toodab ettevõtetele kasumit, võimaldades luua järjest täpsemaid meetmeid tarbija harjumuste väljaselgitamiseks ja sihistatud turunduse kasutamiseks. Sellele vastukaaluks peavad isikul ehk andmesubjektil olema kasutada meetmed oma andmekaitsealaste õiguste jõustamiseks.

Eesti ajakirjandus on seoses uue EL andmekaitsereeglistikuga kajastanud nn hiigeltrahvide tekkimise võimalust. Advokaat Mari Männiko on kommenteerinud, et uus EL andmekaitse üldmäärus võimaldab määrata trahvid kuni 20 000 000 eurot või 4% ettevõtte ülemaailmsest aastakäibest.[12] Viidatud numbrid ei ole autori hinnangul vastavuses hetkel kehtiva Eesti õigusega ning seetõttu tekib küsimus, kas Eesti peab vastavaid trahvimäärasid oma õigusesse üle võtma ning kas ja kuidas on seda võimalik teha, arvestades meie kehtivat õigussüsteemi.

[9] Eesti Vabariigi Põhiseadus. – RT 1992, 26, 349 … RT I, 15.05.2015, 2.
[10] Isikuandmete kaitse seadus. RT I 2007, 24, 127 ... RT I, 06.01.2016, 10.
[11] Andmekaitse inspektsiooni avastus: SEB küsib ainsana mobiilipanga kasutajalt ligipääsu telefoniraamatule. – Delfi. 20.02.2017. Arvutivõrgus: http://kasulik.delfi.ee/news/uudised/andmekaitse-inspektsiooni-avastus-seb-kusib-ainsana-mobiilipanga-kasutajalt-ligipaasu-telefoniraamatule?id=77286196 (18.01.2018).
[12] M. Männiko. Andmekaitsereform toob hiigeltrahvid. – Äripäev. 09.05.2016. Arvutivõrgus: https://www.aripaev.ee/uudised/2016/05/04/andmekaitsereform-toob-hiigeltrahvid (18.01.2018)).

Autor soovib uurida oma töös, millised jõustamismeetmed on Eestis kasutusel, kuidas neid praktikas kohaldatakse, hinnata nende efektiivsust ning vaadelda, kas kehtiv süsteem sobib kokku arengutega EL-is ning millisel viisil on Eestil võimalik täita EL andmekaitse üldmäärusest tulenevaid kohustusi ja kindlustada andmesubjekti õiguste tõhus jõustamine.

Käesoleva töö autor püstitab hüpoteesi, et Eesti õiguses ei ole piisavalt tõhusaid meetmeid andmekaitseõiguse jõustamiseks ning olemasolev sanktsioneerimise süsteem ei vasta täida EL õigusest tulenevaid nõudeid. Magistritöö on lähtuvalt püstitatud eesmärgist ja hüpoteesist jagatud kolmeks peatükiks.

Töö esimeses peatükkis selgitatakse isikuandmete kaitse reguleerimise vajadust, seda eelkõige tulenevalt üha arenevast tehnoloogiast. Iga isiku põhiõiguseks on õigus eraelu puutumatusele, milleks on ka isikuandmete töötlemine. Järgnevalt analüüsitakse isikuandmete kaitse õiguslikku regulatsioon tulenevalt Euroopa Liidu ja Eesti õiguskorrast ning uuritakse, millised on võimalikud jõustamismeetmed riiklikul järelevalvel.

Teises peatükk analüüsitakse, milline on käesoleval ajal võimalik vastutus isikuandmete nõuete rikkumisel Eestis. Autor annab ülevaate, millised teod on karistatavad tulenevalt IKS-st ning millised nõuded tulenevad kehtivast direktiivist 95/46/EÜ. Autori hinnangul võib probleemiks olla direktiivi üldsõnalisus, mis on tinginud rohke eelotsuste küsimise Euroopa Kohtult (*edaspidi EK*). Autor käsitleb erinevaid vastutuse liike Eesti õiguses ning keskendub vastutusele süüteomenetluse raames, analüüsides muuhulgas ka Andmekaitse Inspektsiooni (*edaspidi* AKI) praktikat. Töös on kasutatud ka Riigikohtu ja Euroopa Inimõiguste Kohtu (*edaspidi EIK*) tõlgendamise praktikat.

Kolmandas peatükis uuritakse 25. maist 2018. a kehtima hakkavast andmekaitse üldmäärusest tulenevaid sanktsioone ja jõustamismeetmeid. Autor käsitleb haldustrahvide sätete ülevõtmist Eesti õigusesse ning uurib haldussunni võimalikku rakendamist Eestis väärteomenetluse korras. Viimaks annab autor hinnangu andmekaitse üldmääruses sätestatud sanktsioonide, st eelkõige kõrgete trahvimäärade rakendamise võimalikkusele Eesti õiguses. Autor analüüsib võimalikke probleeme ning hindab uue isikuandmete kaitse seaduse eelnõu vastavust üldmäärusele. Erinevalt direktiivist on määrus otsekohalduv, mis annab riigile senisest oluliselt vähem ruumi kaalutlusotsuste tegemiseks EL õiusest tulenevate normide rakendamisel.

Arvestades magistritöö olemust ning mahupiiranguid keskendub autor oma töös eelkõige andmekaitsereformiga kaasnevatele muudatustele Eesti õiguses. Töö põhirõhk on kehtiva õigusraamistiku ja rakenduspraktika valguses analüüsida võimalused andmekaitse üldmäärusest tulenevate rangete sanktsiooninormide rakendamiseks Eestis. Käesoleva töö teemakäsitlusest jääb välja põhilised muudatused seoses üldmääruse kohaldamisega ning keskendub põhiliselt sanktsioonide ülevõtmise probleemidele Eesti õigusesse.

Töö teema on valitud, kuna isikuandmete kaitse on väga oluline ning seoses isikuandmete kaitse reformiga ka päevakajaline ja aktuaalne. Antud teema on õiguslikult vähe käsitlust leidnud.

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

1. ISIKUANDMETE KAITSE ÕIGUSLIK RAAMISTIK

1.1. Isikuandmete kaitse olemus

Kuigi tehnoloogia võib kujutada endast ohtu, võib tehnoloogia ka pakkuda lahendust privaatsuse kaitsmisel.[13] Tehnoloogia võib tõhustada andmete kaitsmist ning anda uusi teadmisi automatiseeritud andmetöötluses. Tänu uuenenud tehnoloogiale on võimalik tagada parem andmekaitse, kuna andmete töötlemine on muutunud turvalisemaks ning võimaldab kontrollida andmetöötlejate tegevust. Tehnoloogia abil võib suurest hulgast üksikasjalikest andmetest midagi aru saada – kombineerida erinevaid andmeid nii, et iseenesest vähetähtsad andmed muutuvad oluliseks, ning koguda ja levitada andmeid üle kogu maailma. Igal juhul peab andmekaitse aspekt olema infosüsteemide hindamisel osa nii selle kaudu, kuidas süsteem aitab tagada paremat andmekaitset, kui ka selle kaudu, missuguseid võimalikke ohte see esile toob ja kuidas nende vastu võidelda tõhusalt ja samas proportsionaalselt.[14] Kiirelt areneva tehnoloogiaga peab sammu pidama privaatsusõigus ja andmekaitse, esitades samas väljakutseid ka õigussüsteemile, et rakendada tõhusalt õigusnorme. Tehnoloogia on kindlasti loonud uue keskkonna, milles tuleb andmekaitset rakendada.[15] Moodne informatsiooni- ja kommunikatsioonitehnoloogia võimaldab uusi viise, kuidas suhelda, jagada ja koguda infot. Elame infoühiskonnas ja informatsioon liigub tänapäeval kiiresti ning see on omaette väärtus. Tehnoloogia arenguga on andmed muutunud väga väärtuslikuks, sest suuri andmehulki on võimalik kasutada mitmete erinevate teenuste pakkumiseks. Paljud ettevõtted, sh erinevad teenusepakkujad omavad suurel hulgal andmeid isikute kohta, mis nad on saanud otseselt või kaudselt isikute endi käest. Otseselt võib näitena tuua Facebook, Instagram, Twitter ja paljud teised suhtlusvõrgustikud, kus isikud ise oma andmeid on ettevõttele andnud või kaudselt kasutades mõnda teenusepakkujat, näiteks Google.

Isikuandmete kaitse põhiliseks eesmärgiks on üksikisiku privaatsuse kaitse. Seega on andmekaitse keskmes andmesubjekt ehk isik, kelle andmeid töödeldakse ning isikuandmete töötlemisega on tegu alati siis, kui tehakse midagi inimese kohta käivate andmetega. Põhiõigus

[13] S. Gutwirth, Y. Poullet, P. D. Hert, C. Terwangne, S. Nouwt Editors „Reinventing Data Protection?“, .Springer Science+Business Media B.V.2009.
[14] K. Nyman Metcalf. Inimõiguste Instituut. Uuring 2014,.
Arvutivõrgus:
https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2013/13-07-18_Smart_borders_EN.pdf (18.01.2018).
[15] G. Gonzales Fuster, S. Gutwirth, P. de Hert (2010) „). From Unsolicited Communications to Unsolicited Adjustments“:: G. Gutwirth, Y. Poullet & P. de Hert (toim.) *Data Protection in a Profiled World,* Springer, Dordrecht/London (105-117), lk 107-109.

andmekaitsele on tuletatud õigusest eraelu puutumatusele - isik peab ise saama otsustada kellele ta oma eraeluga seotud andmeid avaldab. Siiski tuleb ka arvestada, et erinevatel põlvkondadel on erinevad arusaamad ja oskused isikuandmetega seotud ohtude tunnetamiseks, eelkõige suhtlusvõrgustike ja meedia kaudu. Meedia all käsitleme siinkohal nii päeva- ja nädalalehti ning tele- ja raadiokanaleid, samuti blogisid, netifoorumeid ja suhtlusvõrgustikke. Mõlemad võivad sisaldada ajakirjandusliku eesmärgiga artikleid ning meelelahutuslikku osa. Oluliseks erinevuseks on asjaolu, et ajakirjanduslikul eesmärgil on lubatud isikuandmeid avalikustada ka ilma inimese enda nõusolekuta.[16]

Isikuandmete definitsioon ise on väga lai, hõlmates kogu teavet, mida võib isikuga, kas kaudselt või isegi väga kaudselt seostada. Mõneti on selline laiaulatuslik kaitse põhjendatud, arvestades tänapäeva informatsiooni kättesaadavuse lihtsust ja ulatust.[17] Isikuandmete mõiste laieneb mistahes vormis teabele: see võib esineda sõnadena, numbritena, graafiliselt, fotona või helina. Isikuandmeteks on nii objektiivne teave, nt mingi aine sisaldus veres, kui ka subjektiivne teave – arvamused ja hinnangud.[18] Andmed võivad mõjutada isiku eraelu, mis peaks olema tulenevalt Põhiseadusest puutumatu ja mille üle isikud peavad ise otsustama. Selleks, et teave kujutaks endast isikuandmeid, ei pea see olema tingimata tõene.[19] 1981. aastal vastu võetud Euroopa Nõukogu isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni nr 108 (*edaspidi konventsioon 108 või andmekaitsekonventsioon*)[20] artiklis 2 punktis a on antud isikuandmete definitsioon, mille kohaselt mõistetakse isikuandmetena mis tahes informatsiooni tuvastatud või tuvastatava isiku (andmesubjekti) kohta.

Andmekaitse kui õigusharu ei keskendu mitte andmete kaitsele, vaid kaitseb inimest, see tähendab isiku õigust informatsioonilisele enesemääratlusele.[21] Moodsa kommunikatsioonitehnoloogia arenedes muutub oht üksikisiku eraelu puutumatusele ja informatsioonilisele enesemääramisõigusele üha teravamaks. Informatsiooniline enesemääramine tähendab seda, et igal isikul on õigus ise otsustada, kas ja kui palju andmeid

[16] Andmekaitse Inspektsioon. Isikuandmete avalikustamine meedias. 19.11.2015. Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Juhised/meediavaidlusse%20sekkumise%20kriteeriumid.pdf (02.04.2018).
[17] J.Antonova. Isikuandmete kaitse kohtueelses kriminaalmenetluses Eestis. Tartu: 2015, lk 9.
[18] Andmekaitse Inspektsioon. Isikuandmete töötlemine töösuhtes. 26.05.2014. Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikuandmed%20t%C3%B6%C3%B6suhetes%20juhendmaterjal26%2005%202014_0.pdf (02.04.2018).
[19] Artikli 29 alusel asutatud andmekaitse töörühm. Arvamus 4/2007 isikuandmete mõiste kohta, lk 6. Arvutivõrgus: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf (18.01.2018)).
[20] Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon. - RT II 2001, 1, 3.
[21] M. Männiko. Juura 2011, lk 56.

tema kohta kogutakse ja salvestatakse, seetõttu on just eraelu kaitse seisukohalt üheks oluliseks valdkonnaks isikuandmete kaitse.[22] Õigus kontrollida enda kohta käivat informatsiooni ehk nn informatsioonilise enesemääramise õigus on isikuandmete kaitse põhimõtete alus. Termin "informatsiooniline enesemääramisõigus" (*das Recht auf informationelle Selbstbestimmung*) on esimest korda defineeritud Saksamaal. Täpsemalt pärineb selline õigus 1983. aasta kohtulahendist[23], kus Saksa Föderaalkohus asus seisukohale, et tulenevalt põhiseadusest on igaühel õigus ise määrata, kellele isikuandmeid üle anda ning kellel lubada neid töödelda. Konkreetselt üksikisiku õigust omada kontrolli enda kohta käivate andmete kasutamise üle.

Maailmas esimene andmekaitset reguleeriva õigusakti võeti vastu Saksamaa Föderatiivses Vabariigis Hesseni liidumaal 1970.[24] Järgmisena võtsid seaduse vastu Rootsi (1973), Ameerika Ühendriigid (1974), Saksamaa (1977) ning Prantsusmaa (1978).[25] Nii Euroopa Nõukogu kui ka Majanduskoostöö ja Arengu Organisatsioon (*edaspidi OECD*) on vastu võtnud reelid isikuandmete kaitseks, mis olid olulised andmekaitse valdkonna edasiarendamisel rahvusvahelisel tasandil. 1980. aastal võttis OECD vastu resolutsiooni, millega kehtestati juhised privaatsuse kaitse ja isikuandmete piiriülese edastamise kohta (*Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*)[26], seda juhendit täiendati 2013. aastal.[27] Juhise artikkel 1 p c annab isikuandmete definitsiooni: "Isikuandmed on andmed tuvastatud või tuvastatava isiku kohta (andmesubjekt)".

Euroopa nõukogu parlamentaarse Assamblee 1970. a resolutsiooni „Deklaratsioon massikommunikatsioonimeedia ja inimõiguste kohta"[28] punktis 15 on õigus eraelu puutumatusele määratletud kui õigus elada omaenda elu minimaalse sekkumisega. Redaktsiooni peamine tähelepanu on pööratud isiku eraellu sekkumisele ajakirjanduse poolt,

[22] Ü. Madise jt (toim). Eesti Vabariigi Põhiseadus. Komm vlj. 4. tr. Tallinn: Juura 2017, § 26 / 24.
[23] Saksamaa Föderaalse Konstitutsioonikohtu otsus 15.detsembrist 1983, viitenumber: 1 BvR 209, 269, 362, 420, 440, 484/83; C. DeSimone. Pitting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive. - German Law Journal 2010/11, No. 3, p 29.
[24] F. Boehm. Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Springer Verlag, Berlin Heidelberg, 2012, lk 20.
[25] D. Banisar. Models for protecting privacy. – The Door into the Other Side. Budapest: Adatvédelmi Biztos Irodja, 2001, lk 177.
[26] OECD. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Arvutivõrgus: http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (31.01.2018).
[27] OECD. The OECD privacy framework. AvailableArvutivõrgus: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf, (31.01.2018).
[28] Euroopa Nõukogu Parlamentaarse Assamblee resolutsioon 428 (1970)). Declaration on mass communication media and Human Rights. Arvutivõrgus: http://assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewPDF.asp?FileID=15842&lang=en (31.01.2018).

kuid siiski leiab käsitlemist ka vajadus kaitsta privaatsust laiemalt. Isiku kujutise äratundmatuks muutmise võimalusele on tähelepanu juhtinud Euroopa Inimõiguste Kohus nt asjas *Peck vs. the United Kingdom.*[29]

1.2. Õigus isikuandmete kaitsele põhiõiguste kontekstis

EL õiguskorras on andmekaitse saanud justkui eraldiseisvaks põhiõiguseks, mida tähtsuse poolest on kohati võrreldav eraelu puutumatusega.[30] Juba peale II Maailmasõda muutus oluliseks inimõiguste kaitse põhimõte. Selle tulemusena sätestati õigus eraelu puutumatusele 1948. aastal ÜRO inimõiguste deklaratsiooni[31] artiklis 12, mis käsitleb era- ja perekonnaelu austamist. Artikli kohaselt ei tohi meelevaldselt sekkuda kellegi era- ja perekonnaellu, kodupuutumatusse või kirjavahetusse ega teotada kellegi au ja head nime. Igal inimesel on õigus seaduse kaitsele selliste vahelesegamiste ja rikkumiste eest. 1950. aastal võeti vastu Euroopa inimõiguste ja põhivabaduste kaitse konventsioon[32] (*edaspidi* EIÕK), mis jõustus aastal 1953[33]. Õigus isikuandmete kaitsele tuleneb artiklist 8, millega tagatakse kõikidele õigus era- ja perekonnaelu, kodu ja korrespondentsi puudumise austamisele ning kehtestatakse tingimused, mille puhul on põhjendatud kõnealuse õiguse piiramine.[34] Euroopa Liidu toimimise lepingu[35] artikkel 16 sätestab, et igaühel on õigus oma isikuandmete kaitsele. Samuti on isikuandmete kaitse aluseks ka Euroopa Liidu Põhiõiguste Harta[36] (*edaspidi harta*) artikkel 8, mis sätestab õiguse isikuandmete kaitsele iseseisva põhiõigusena.

Õiguskirjanduses on selgitatud, et andmesubjekt peab saama võimalikult palju oma isikuandmete töötlemist mõjutada, selles osaleda ja seda kontrollida ning seetõttu on andmekaitsereeglite hulgas alati ka nõue, et andmesubjektil peab olema võimalik kindlaks teha tema isikuandmete töötlemise juhud, tutvuda tema kohta töödeldavate andmetega, nõuda valede

[29] EIKo 28.01.2003, nr 44647/98, *Peck vs. the United Kingdom,* p 80.
[30] M. Tzanou. Data protection as a fundamental right next to privacy? „Reconstructing" a not so new right. – International Data Privacy Law. Vol. 3. No 2. 2013, p 88.
Available: http://idpl.oxfordjournals.org.ezproxy.utlib.ee/content/3/2/88.full.pdf+html?sid=9cd0e47e-7e17-48fb-9d57-8bf05406e48f. (31.01.2018).
[31] Ühinenud Rahvaste Organisatsioon. Inimõiguste ülddeklaratsioon. Arvutivõrgus: http://www.un.org/en/documents/udhr/, (31.01.2018).
[32] Inimõiguste ja põhivabaduste kaitse konventsioon. – RT II 2010, 14, 54.
[33] The Council of Europe. A Convention to protect your rights and liberties.
Available: https://www.coe.int/en/web/human-rights-convention/ (31.01.2018).
[34] Handbook on European Data Protection Law. Luxembourg: Publications Office of the European Union. 2014, p 17.
[35] Euroopa Liidu leping ja Euroopa Liidu toimimise lepingu konsolideeritud versioon. – ELT C 326, 26.10.2012.
[36] Euroopa Liidu Põhiõiguste Harta, ELT C 83, 30.03.2010, lk 389-403.

andmete parandamist jms. Need nõuded peavad muutma isikuandmete töötlemise võimalikult avatuks ja läbipaistvaks.[37] Erinevalt EIÕK-st ja PS-st nimetab harta eraldi õiguse era- ja perekonnaelu puutumatusele (art 7) ning õiguse isikuandmete kaitsele (art 8). Harta artikkel 7 sätestab õiguse isikuandmete kaitsele kui autonoomse põhiõiguse.[38] Õigus isikuandmete kaitsele ei keela andmete töötlemist ega kaitse isikut andmetöötluse kui sellise eest, vaid kaitseb ebaseadusliku ja/või ebaproportsionaalse andmete töötlemise eest.[39] Seega võivad EL riigid piirata õiguste ja kohustuste ulatust üksnes juhul, kui selline piiramine on vajalik ja proportsionaalne abinõu selleks, et kaitsta avalikke erahuvisid, nt riiklikku julgeolekut, võimaldada kriminaalkuritegude uurimist, tagada riigikaitset või avalikku korda.

Eesti õiguskorras on õigus isikuandmete kaitsele tagatud PS tasandil. PS-s on kajastatud eraelu puudutavad sätted. Kuigi PS ei sätesta eraldiseisvat õigust isikuandmete kaitsele, on see hõlmatud eelkõige PS paragrahviga 26, mis sätestab õiguse eraelu puutumatusele. Tulenevalt §-st 26 on igaühel õigus perekonna- ja eraelu puutumatusele. Riigikohus on oma otsuses sedastanud, et eraelu puutumatuse riivena käitatakse muu hulgas isikuandmete kogumist, säilitamist, kasutamist ja avalikustamist.[40] Põhiõigused kehtivad eelkõige eraisiku ja avaliku võimu kandja vahelistes suhetes, kusjuures esimene on suhte õigustatud, teine kohustatud pool.[41] PS § 19 sätestab, et igaüks peab oma õiguste ja vabaduste kasutamisel ning kohustuste täitmisel austama ja arvestama teiste inimeste õigusi ja vabadusi ning järgima seadust. PS § 19 lõikes 2 sisaldub nii üldine teiste inimeste õiguste ja vabaduste järgimise kohustus kui ka põhimõte, mis määrab kindlaks põhiõiguste kehtivuse põhiõiguste kandjate omavahelistes suhetes.[42] Riigiasutused, kohalikud omavalitsused ja nende ametiisikud ei tohi kellegi perekonna- ega eraellu sekkuda muidu, kui seaduses sätestatud juhtudel ja korras tervise, kõlbluse, avaliku korra või teiste inimeste õiguste ja vabaduste kaitseks, kuriteo tõkestamiseks või kurjategija tabamiseks.[43] Eraeluliste andmete kogumisele ja töötlemisele suunatud toimingud, mille puhul peab silmas pidama PS § 26 riive proportsionaalsust, on ette nähtud ka

[37] T. Ilus. Andmesubjekti osaluse põhimõte Euroopa Nõukogu konventsioonide ning EIK lahendite valguses. – Juridica, 2005 / 8, lk 522.
[38]S. Rodota. Data Protection as a Fundamental Right. - Gutwirth, S. jt (toim). Reinventing Data Protection? Springer Science+Business Media B.V., 2009, lk 79.
[39] P. De Hert, P., S. Gutwirth. Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action. - Gutwirth, S. jt (toim). Reinventing Data Protection? Springer Science+Business Media B.V., 2009, lk 3.
[40] RKHKo 3-3-1-3-12, p19.
[41] EV PS komment § 19 / 17.
[42] EV PS komment § 19 / 15.
[43] H. Kranich. Ühiskonna (eba) normaalne areng ja inimõigused. Nimede kohtulahendites avalikustamise näide. - Juridica 2015 / 4, lk 283.

korrakaitselistel eesmärkidel, näiteks Politsei ja piirivalve seaduses[44], Korrakaitseseaduses[45] (*edaspidi KorS*), Julgeolekuasutuste seaduses[46], Vangistusseaduses[47], samuti võivad ulatuslikud eraelu riived kaasneda jälitustoimingutega. PS § 26 kaitsealas on ka andmed igasuguse sõnumi saatmise kohta. Paragrahvi 26 esimeses lauses on sätestatud tõrjeõigus, mis annab põhiõiguse kandjale õiguse oodata, et riik ei sekku tema perekonna- ja eraellu ning kohustab riiki sekkumisest hoiduma. Põhimõtteliselt on kõik, mida PS § 26 tõrjeõigusena kaitseb riigi eest, kaitstav ka kolmandate isikute rünnete eest.[48] PS § 26 sõnastamisel on selgeks eeskujuks olnud Inimõiguste ja põhivabaduste kaitse konventsiooni (*edaspidi EIÕK*)[49] artikkel 8.[50] Artiklis nr 8 on märgitud, et igaühel on õigus sellele, et austatakse tema era- ja perekonnaelu ja kodu ning korrespondentsi saladust. EIK on leidnud, et kuigi EIÕK artikli 8 eesmärk on kaitsta isikuid avaliku võimu omavolilise sekkumise eest, ei tähenda see üksnes riigi kohustust hoiduda sellisest rikkumisest: niisuguse eelkõige negatiivse kohustuse kõrval võivad selles loomupäraselt positiivsed kohustused era- või perekonnaelu tegelikuks austamiseks.[51] Eraelu hõlmab EIK käsitluses ka võimude poolt isiku kohta avaliku informatsiooni kogumise ja talletamise teabetoimikutes.[52]

PS § 26 esimese lause kaitseala võib riivata iga sellega kaitstud õigusliku positsiooni ebasoodne mõjutamine riigi poolt, aga ka riigi kaitsekohustuse täitmata jätmine.[53] Paragrahvi 26 teises lauses on eraelu piiriklausel sätestatud kitsamalt kui EIÕK art 8 lõikes 2. EIÕK art 8 lg-s 2 on sätestatud, et ametivõimud ei sekku art 8 esimeses lõikes tagatud õiguse kasutamisse muidu kui kooskõlas seadusega ja kui see on demokraatlikus ühiskonnas vajalik riigi julgeoleku, ühiskondliku turvalisuse või riigi majandusliku heaolu huvides, korratuse või kuriteo ärahoidmiseks, tervise või kõlbluse või kaasinimeste õiguste ja vabaduste kaitseks. Antud juhul on art 8 teine lõige sõnastatud liiga avaralt, et võimaldab riivata perekonna- ja eraelu puutumatust peaaegu igal mõeldaval põhjusel. Paragrahvi 26 teise lause kohaselt võib sekkuda perekonna- ja eraellu tervise, kõlbluse, avaliku korra või teiste inimeste õiguste ja vabaduste kaitseks, kuriteo tõkestamiseks või kurjategija tabamiseks. Seega on sätestatud kvalifitseeritud

[44] Politsei ja piirivalve seadus. - RT I 2009, 26,159 ... RT I, 06.07.2017, 6.
[45] Korrakaitseseadus. - RT I, 22.03.2011, 4 ... RT I, 02.12.2016, 6.
[46] Julgeolekuasutuste seadus. - RT I 2001, 7, 17 ... RT I, 05.05.2017, 2.
[47] Vangistusseadus. - RT I 2000, 58, 376 ... RT I, 09.03.2018, 19.
[48] EV PS komment § 26 / 19.
[49] Inimõiguste ja põhivabaduste kaitse konventsioon. - RT II 2000, 11, 57.
[50] EV PS komment § 26 / 19.
[51] EIKo 13.06.1979, nr 6833/74, *Marckx vs.* Belgia, p 20.
[52] EIKo 04.05.2000, 2834/95, *Rotaru vs Rumeenia*, p 43.
[53] EV PS komment § 19 / 19.

seadusereservatsioon, mis lubab eraelu riivata üksnes seadusega või seaduse alusel ja PS § 26 teises lauses kindlaks määratud põhjustel.[54]

EIÕK ega PS ei kasuta mõistet "isikuandmete kaitse", vaid terminit "eraelu puutumatus", mis on oma olemuselt laiem. Euroopas rõhutatakse andmekaitset reguleerides eelkõige üksikisiku privaatsuse kaitse vajadust. Privaatsust peetakse siin üheks põhiliseks inimõiguseks, samaväärseks õigustega eneseteostusele, mõttevabadusele ning sõnavabadusele.[55] Euroopa Nõukogu Parlamentaarse Assamblee resolutsioonis nr 428 (1970) määratletakse eraelu kui õigust elada omaenda elu minimaalse sekkumisega, sellele lisati resolutsiooniga nr 1165 (1998) õigus kontrollida enda kohta käivat informatsiooni.[56]

Isikuandmeteks loetakse ainult füüsilise isiku kohta käivaid isikuandmeid. Siiski on õiguskirjanduses peetud võimalikuks selliseid olukordi, kus isikuandmeteks võib erandkorras käsitleda ka sellist juriidilise isiku kohta käivat teavet, mis sisaldab selget viidet füüsilisele isikule, näiteks kui ettevõtte ärinimi sisaldab selle omaniku pärisnime. EIK on leidnud, et EIÕK artikli 8 kaitseala on mõnel juhul vajalik laiendada ka juriidilistele isikutele.[57] Samuti on märkinud EK, et mõistet „eraelu" tuleks tõlgendada nii, et see hõlmaks füüsiliste ja juriidiliste isikute ameti- ja ärialast tegevust.[58] Kuigi tundub, et eraelu saab olla vaid füüsilisel isikul, kaitseb põhiõigus teatud ulatuses ka juriidilist isikut. Selline eraelu kaitse juriidilistele isikutele saab tekkida siiski juhul, kui kaitset vajav õiguslik positsioon jääb välja PS erisätetee kaitse alt, milleks võib olla ka PS §-ga 43 tagatud sõnumite saladus. Üldreegel on siiski nii Eesti, EL ja Euroopa Nõukogu (*edaspidi EN*) õigusest tulenevalt see, et isikuandmed on eeskätt ainult füüsilise isiku kohta käiv teave.

Mõningatel juhtudel võivad isikuandmed olla kaitstud ka PS § 43 alusel, mis sätestab õiguse sõnumisaladusele. PS on õigus sõnumisaladusele sätestatud eraldiseisva põhiõigusena, kuigi sisuliselt on sõnumisaladus üks eraelu osa.[59] Siiski sätestab PS erinevad tingimused sõnumisaladuse ja eraelu puutumatuse riivamiseks. Sõnumisaladust on lubatud riivata piiratud juhtud - ainult kohtu loal kuriteo tõkestamiseks või kriminaalmenetluses tõe väljaselgitamiseks.

[54] EV PS komment § 26 / 27.
[55] T. Ilus. Isikuandmete kaitse olemus ja arengusuunad. Juridica 2002 / 7, lk 442.
[56] EV PS komment § 26 / 4.
[57] EIKo 16.12.1992, nr 13710/08, *Niemietz vs.* Saksamaa, 16.12.1992, p 30; EIKo 16.04.2002, nr 37971/97, *Société Colas Est jt vs.* Prantsusmaa, 16.04.2002, p 41.
[58] Kohtuasi nr EKo 14.02.2008, C-450/06, *Varek Sa vs.* Belgia, 14.02.2008, p 48.
[59] Näiteks Euroopa Inimõiguste ja Põhivabaduste kaitse konventsioonis kaitstakse sõnumisaladust samas sättes (art 8) eraelu ja kodu puutumatusega.

Samas kui eraelu puutumatust võidakse seadusega piirata lisaks ka tervise, kõlbluse, avaliku korra või teiste inimeste õiguste ja vabaduste kaitseks. Seega PS kontekstis kaitstakse töötaja eraelu ja õigust sõnumisaladusele ning tunnistatakse töötaja õigust otsustada andmete kogumise ja levitamise üle. Kokkuvõtvalt saame öelda, et nii seadusandja kui ka andmete töötlejad peavad arvestama, ei isikuandmete töötlemise reeglid asetuvad põhiseaduslikku raamistikku ning PS seab isikuandmete töötlemisele omad nõuded. Andmete kaitsmine põhiõigustega ei tähenda veel andmete töötlemise keeldu, vaid paneb riigile töötlemise reguleerimise ja selle vajalikkuse kaalumise kohustuse. Laiem isikuandmete põhiõiguslik kaitse tähendaks sisuliselt riigi kohustust olla ettevaatlik kõigi isiku kohta käivate andmetega ümberkäimisel.[60]

1.3. Isikuandmete kaitse õiguslik regulatsioon

Andmekaitse peamiseks ülesandeks on privaatsuse tagamine.[61] Isikuandmete kaitse reguleerimisel on liikmesriigid seotud Euroopa Liidu õigusega.

Fred H. Cate on välja toonud neli Euroopa andmekaitsele omast joont[62]:

1) seadused laienevad nii avalikule kui erasektorile;
2) reguleeritud on väga lai ring andmetöötlusoperatsioone, muuhulgas andmete kogumine, säilitamine, kasutamine ning levitamine;
3) seadusest tulenevad andmete töötlejaile erinevad aktiivset tegutsemist nõudvad kohustused (sageli nt kohustus registreerida andmete töötlemine riigiasutuses);
4) valdkondlike piiranguid on vähe või üldse mitte – seadused laienevad kõikidele töötlemisjuhtudele andmesubjektide erisusest sõltumata.

Euroopa Liidus on isikuandmete töötlemisega seotud mõisted, õigused ja kohustused on koondatud ühte üldregulatsiooni, milleks on direktiiv 95/46/EÜ. Direktiivi 95/46/EÜ eesmärk on EL siseturu edendamine ning sellest tulenevalt näeb direktiiv ette liikmesriikide õiguse harmoniseerimise.[63] Direktiivi 95/46/EÜ artiklis 6 on sätestatud, et isikuandmeid võib kasutada vaid täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel. Artikkel 7 sätestab 6 võrdse tähtsusega õiguslikku alust. Artikli 28 kohaselt peavad liikmesriigid ellu kutsuma

[60] I. Pilving. Õigus isikuandmete kaitsele. Juridica 2005 / 8, lk 536.
[61] Euroopa andmekaitseinspektor P. Hustinxi kõne 2. mail 2004 Euroopa Parlamendi ees, lk 1.
[62] F. H. Cate. Privacy in the information age. Washington, D.C: Bookings Institution Press, 1997, lk 32-33.
[63] P. Hustinx. EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation. Avaldatud kõne, 2014, lk 9. Arvutivõrgus: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2014/14-09-15_Article_EUI_EN.pdf (18.01.2018).

järelevalveasutuse, kes vaatab läbi kõigi isikute või kõnealuseid isikuid esindava ühenduse esitatud avaldused nende õiguste ja vabaduste kaitse kohta seoses isikuandmete töötlemisega ning teavitav andmesubjekte avalduse tagajärgedest.

Antud juhul on Euroopas andmekaitse rakendumisel väga oluline roll andmekaitse järelevalve riiklikel institutsioonidel, kes peaksid tagama seaduses sätestatud nõuete jõustamise. Isikuandmete kaitse seadus [64] (*edaspidi IKS*) § 32 kohaselt on Eestis selliseks organisatsiooniks Andmakaitse Inspektsioon (*edaspidi* AKI). Muuhulgas on AKI ülesandeks soovituslike juhiste andmine isikuandmete kaitse seaduse rakendamiseks.[65] Järelevalvemenetluse läbiviimisel lähtub AKI nii IKS-ist kui KorS-st. IKS § 33 lg 5 kohaselt on AKI antud võimalus algatada järelevalvemenetluse kaebuse alusel või omal algatusel. Selle kohaselt on AKI-l järelevalve menetluse algatamiseks jäetud kaalutlusruum, samuti kaalutlusõigus järelevalvemenetluse lõpetamise üle. Lisaks eelnevale on Riigikohtu halduskolleegium märkinud, et AKI-l on kaalutlusõigus, kas jääda kaebuse piiridesse või kontrolliulatust enda initsiatiivil laiendada.[66]

Eesti õigus põhineb suuresti nii EN kui EL õigusel. 2008. aastal viidi Eestis läbi kolme seadust hõlmav reform, mille tulemusel võeti vastu uus IKS, millega võeti üle nii kehtiv direktiiv 95/46/EÜ kui ka konventsioon 108. Seaduse eesmärk oli parandada 2003. aasta 1. oktoobril jõustunud isikuandmete kaitse seaduse rakendamisel ilmnenud kitsaskohad. Senise IKS regulatsioonist ei olnud praktikas kavandatud kujul rakendunud eraeluliste isikuandmete töötlemisest AKI teavitamine ning see oli eelnõust väljajäetud. Isikute põhiõiguste tõhusama kaitse huvides vajas reguleerimist seni IKS kohaldamisalast välistatud õiguspäraselt avalikuks kasutamiseks antud isikuandmete töötlemine. Üle oli vaja vaadata isikukoodi töötlemise põhimõtted, samuti isikuandmete töötlemine teaduslikel ja statistilistel eesmärkidel.[67] Erinevalt varasemalt kehtivast seadusest ei ole IKS kohaldamisalast enam välistatud õiguspäraselt avalikuks kasutamiseks antud isikuandmete töötlemist. Siiski märgiti eelnõus, et andmesubjektile peab jääma ka avalikustatud andmete suhtes üldjuhul nõuete esitamise õigus, eelkõige õigus nõuda oma isikuandmete parandamist ja andmete avalikustamise lõpetamist, samuti tekitatud kahju hüvitamist.[68] Isikuandmete mõistet muudeti eelnõus võrreldes

[64] Isikuandmete kaitse seadus. – RT I 2007,24,127 … RT I, 06.01.2016,10.
[65] IKS § 33 lg 1 p 5.
[66] TKHKoRKHKo 3-3-1-85-15, p 29.
[67] Isikuandmete kaitse seaduse eelnõu seletuskiri. Arvutivõrgus: http://webcache.googleusercontent.com/search?q=cache:ZpXneFC7l0oJ:www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/IKS%2520SELETUSKIRI%2520%25281%2529.rtf+&cd=1&hl=et&ct=clnk&gl=ee&client=firefox-b (31.01.2018)
[68] *Ibid*, 59.

varasemalt kehtinud IKS-ga, tuues isikuandmete erilist kaitset vajava alaliigina välja üksnes delikaatsed isikuandmed.

IKS kohaldub kogu Eestis toimuvate isikuandmete töötlusele, va riigisaladuse töötlemine ja isiklikuks tarbeks andmete töötlemine. Isikuandmete mõiste on defineeritud IKS § 4 lg 1 – mille kohaselt on isikuandmed on mis tahes andmed tuvastatud või tuvastatava füüsilise isiku kohta, sõltumata sellest, millisel kujul või millises vormis need andmed on.[69] Isikuandmete töötlemine on iga isikuandmetega tehtav toiming, sealhulgas isikuandmete kogumine, salvestamine, korrastamine, säilitamine, muutmine ja avalikustamine, juurdepääsu võimaldamine isikuandmetele, päringute teostamine ja väljavõtete tegemine, isikuandmete kasutamine, edastamine, ristkasutamine, ühendamine, sulgemine, kustutamine või hävitamine, või mitu eelnimetatud toimingut.[70] Isikuandmete töötlemisel tuleb järgida kindlaid põhimõtteid, mis aitavad saavutada andmekaitse eesmärke. Need on seaduslikkuse, eesmärgikohasuse, minimaalsuse, kasutuse piiramise, andmete kvaliteedi, turvalisuse ja andmesubjekti osaluse põhimõtet.[71] Rääkides minimaalsuse põhimõttest, tuleb märkida, et IKS-s ei ole ühtegi konkreetset sätet säilitamistähtaegade piiramise kohta, kuigi vastav põhimõte on konventsioonis 108 (art 5 p e) ning direktiivis 95/46/EÜ (art 6 lg 1 p e). Säilitamistähtaja piiramise põhimõte (*principle of limited retention of data*) tähendab, et andmeid tohib säilitada andmesubjekti tuvastamist võimaldaval viisil üksnes niikaua, kui see on vajalik sätestatud eesmärgi saavutamiseks, seejärel tuleb andmed kustutada.[72] IKS rakendatakse väga erinevates olukordades, näiteks kui isikuandmeid töödeldakse ajakirjaniku või riigiasutuse poolt, aga ka tööandjale, kes uurib oma töötaja kohta käivat teavet. Kriminalamenetlusele ja kohtumeneltusele kohaldatakse IKS-i menetlusseadustikes sätestatud eranditega. IKS eesmärk on kaitsta isikuandmete töötlemisel füüsilise isiku põhiõigusi- ja vabadusi, eelkõige õigust era elu puutumatusele. Seadust ei kohaldata, kui isikuandmeid töötleb füüsiline isik isiklikul otstarbel ja siis, kui isikuandmeid üksnes edastatakse läbi Eesti territooriumi, ilma et neid andmeid Eestis muul viisil töödeldakse.[73]

[69] IKS § 4 lg 1.
[70] IKS § 5.
[71] M. Männiko, 2011, lk 44-47.
[72] Handbook on European Data Protection Law. Luxembourg: Publications Office of the European Union. 2014. Arvutivõrgus: http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf (15.12.2017).
[73] IKS § 2 lg 1.

Alates 25. maist 2018 rakendatakse Euroopa Liidus isikuandmete kaitse üldmäärust (*General Data Protection Regulation* – GDPR), mille eesmärk on anda eraisikutele suuremat kontrolli oma isikuandmete üle ning tagada ühtlane andmekaitse tase kogu EL-s. Üldmäärusega tunnistatakse kehtetuks seni valdkonda reguleerinud ja Eesti õigusesse üle võetud direktiiv 95/46/EÜ. Direktiiv 95/46/EÜ kehtestati 1995. aastal ning ei suuda arvestada kõigi tänapäeva tehnoloogiatega, näiteks pilveandmetöötluse erisustega.[74] Üldmääruse eesmärk on kaitsta kõiki EL kodanikke privaatsuse ja andmekaitse rikkumise eest, mis on oluliselt muutunud peale 1995. aasta direktiivi 95/46/EÜ kehtestamist. Erinevalt direktiivist ei nõua üldmäärus, et riikide valitsused võtaksid seadusandlikke õigusakte ning seega oleksid need otseselt siduvad ja kohaldatavad[75] ning kehtib sellisena nagu see on vastu võetud. Oluline on sedastada, et erinevalt seni kehtinud direktiivist on uue õigusakti puhul tegemist määrusega. Määrus on EL õiguses otsekohalduv õigusakt, samas kui direktiiv on õigusakt, mis seab eesmärgi, mida kõik EL liikmesriigid peavad saavutama.[76]

Positiivse hinnangu üldmäärusele annab Brandenburgi Liidumaa andmekaitseinspektor Dagmar Hartge, kes tõstab esile ka *lex loci solutionis'*e põhimõtte määrusega seadustamist. [77] Selle tulemusena kohaldub üldmäärus kõikidele EL ühisturul tegutsevatele ettevõtetele, olenemata nende asukohast. See tähendab, et võrreldes varasemast kohaldatakse EL andmekaitsereegleid ka näiteks selliste suurte korporatsioonide suhtes, kes tegutsevad Euroopa turul, kuid kelle peamine asukoht ei ole EL-is. Samuti hindab Hartge positiivselt määruses kinnistatud *one-stop-shop*-mehhanismi[78], mille kohaselt on ettevõtte ühtseks kontaktpunktiks üldiselt tema asukohajärgne andmekaitseinspektsioon, andmesubjekti ühtseks kontaktpunktiks aga tema elukohajärgne andmekaitseinspektsioon.[79]

Kehtima hakkav üldmäärus jätab liikmesriikide seadusandjatele ka piiratud ulatuses vabadust. Siiski on riigisisesel seadusandjal üldmääruse puhul võimalus sätestada oma õiguses üksnes

[74] N. Robinson, H. Graux, M. Botterman, L. Valeri. Review of the European Data Protection Directive. Cambridge: RAND, 2009, p 36. AvailableArvutivõrgus: http://www.hideproject.org/downloads/review_of_eu_dp_directive.pdf, (31.01.2018).
[75] Blackmer, W.S. (5 May 2016). GDPR: Getting Ready for the New EU General Data Protection Regulation. Information Law Group. InfoLawGroup LLP.
[76] Euroopa Liidu lepingu ja Euroopa Liidu toimimise lepingu konsolideeritud versioonid ELT C 59, 7.6.2016, art 288.
[77] Brandenburgi Liidumaa andmekaitse ja dokumentidega tutvumise õiguse inspektori Dagmar Hartge seisukoht, lk 1.
Arvutivõrgus: https://www.bundestag.de/blob/409390/086370264cba2c233daa84d841ce6c12/a-drs-18-24-92-data.pdf (18.01.2018)
[78] DagmarD. Hartge seisukoht, lk 9..
[79] P. K. Tupay. Juridica 2016 / 4, 238.

need aspektid, mida üldmäärus ei reguleeri ja kus üldmäärus on jätnud liikmesriigile otsustusõiguse. Avaliku sektori paindlikkus tähendab riigi võimalust kehtestada teatud valdkondades oma regulatsioon sh rahvuslik julgeolek, riigikaitse, avaliku korra kaitse, kriminaalmenetlus.[80] Üldmääruse sisulise ja territoriaalse kohaldamisala ulatus on toodud üldmääruse artiklites 2 ja 3 ning nende sätete puhul ei ole jäetud EL liikmesriikidele otsustusõigust riigisisese õiguses üldmääruse täiendamiseks.

Üldmäärusega kehtestatakse füüsiliste isikute senisest tugevamad õigused saada teavet, õigus andmetega tutvuda ja õigus andmete kustutamisele. Isikuandmete kaitse üldmäärus soodustab andmete vaba liikumist digitaalsel ühtsel turul, kõrvaldades direktiivist tulenenud õigusraamistiku killustatust. Digitaalse ühtse turu eest vastutav Euroopa Komisjoni asepresident Andrus Ansip on öelnud: „/…/meie digitaalne tulevik peab rajanema usaldusele ja iga inimese privaatsust tuleb kaitsta. ELi tugevamad isikuandmete kaitse normid saavad reaalsuseks 25. mail. See on suur samm edasi ja meie eesmärk on, et reform oleks kõigi jaoks edukas/…/“[81]. Määruse eesmärk on kaasajastada ja ühtlustada isikuandmete käsitamise nõudeid kõigis liikmesriikides. Kaitstes paremini eurooplaste privaatsust, suurendatakse tarbijate usaldust ja turvatunnet ning luuakse samal ajaluusi võimalusi ettevõtjatele, eriti väikeettevõtetele. Üldmäärusega tagatakse ühtlane ja järjepidev andmekaitse normide kohaldamine kõigis liikmesriikides eesmärgiga lõpetada olukord, kus erinevad liikmesriigid rakendavad andmekaitse direktiivi eri viisil.

Määruse eesmärgiks on seatud isikute põhiõiguste, seega privaatsuse, tagamine. Määrus nõuab isikuga seonduvate andmete töötlemiseks siseriikliku õiguse tuge, sealhulgas isiku enda nõusolekut. Andmesubjekt peab saama võimalikult palju oma isikuandmete töötlemist mõjutada, selles osaleda ja kontrollida. Näiteks avaliku võimu kandjatele on usaldatud suures mahus isikuandmeid, näiteks erinevad riiklikud andmebaasid ja riigi poolt osutatavad e-teenused, siis peab nende andmete töötlemine olema õiguspärane ja selge ka andmesubjektidele.

[80] J. Antonova, M. Mikiver. Andmekaitsest õigusloomejuristile. 22.09.2016. Arvutivõrgus: https://www.just.ee/sites/www.just.ee/files/andmekaitse_koolituse_slaidid.pdf (31.01.2018).

[81] Euroopa Komisjon.European Commission. Commission publishes guidance on upcoming new data protection rules. Arvutivõrgus: http://europa.eu/rapid/press-release_IP-18-386_en.htm (05.0103.03.2018)).

1.4. Riiklik järelevalve ja jõustamismeetmed

Isikuandmete kaitse seadus reguleerib isikuandmete töötlemise tingimusi ja korda, riiklikku järelevalvet isikuandmate töötlemise üle ning sätestab vastutuse töötlemise nõuete rikkumise eest. Vastutus isikuandmete töötlemisnõuete rikkumise eest jaguneb kolmeks: haldus-, väärteo- ja kriminaalvastutus.

Kui andmesubjekt leiab, et isikuandmete töötlemisel rikutakse tema õigusi, on tal õigus pöörduda AKI või kohtu poole, kui seaduses ei ole sätestatud teistsugust vaidlustamise korda.[82] Eraelu puutumatuse rikkumisel on võimalik pöörduda tsiviilkohtusse või algatada kriminaalmenetlus politseis. Tsiviilkohtusse on võimalik esitada kaebus teabe levitaja vastu, kui isiku eraelu on tehtud avalikuks ilma põhjuseta. Kriminaalmenetluse algatamiseks on alust, kui delikaatsed isikuandmed on avaldatud ebaseaduslikult. Isikuandmete töötlemise nõuete rikkumisel võib kohus rakendadavastutusena kas kriminaal- või tsiviilvastutust. Sõnumisaladuse rikkumist ja isikuandmete ebaseaduslikku avaldamist võidakse karistada vaid rahatrahviga. Kuid sõnumisaladuse rikkumist isiku poolt, kellel on oma tööülesannete tõttu juurdepääs sõnumitele ning delikaatsete isikuandmete ebaseadusliku avaldamise eest, kui see avalikustati isikliku kasu eesmärgil või põhjustas isikule olulist kahju, võib karistada ka vangistusega.[83] Seega teatud eriti rasked rikkumised kvalifitseeritavad kuritegudeks. Kriminaalkaristused sisaldavad tihti ka lisapiiranguid, näiteks keeldu töötada tulevikus teatud ametikohal.

Tsiviilkohtusse esitatakse hagi, kui keegi, näiteks mõni väljaanne on rikkunud isiku õigust eraelu puutumatusele. Sellisel juhul on isikul võimalik nõuda õiguskaitsevahendite kohaldamist, eelkõige kahju hüvitamist. Selleks võib olla rahaline hüvitis või kohustus isikuandmete töötlemine lõpetada, isikuandmeid parandada ja kustutada. Seejuures peab olema tagatud proportsionaalsus isiku eraelu puutumatuse kaitse ja sõnavabaduse piiramise vahel. Eraisiku ees vastutab ning kahju hüvitab alati vastutav töötleja, näiteks ajakirjandusväljaanne.

Väärteokaristuse määramisel lähtutakse väärteomenetluse seadustikus ettenähtud menetluskorrast ning süü määramisel on aluseks karistusseadustiku üldosas sätestatu. Erinevalt

[82] IKS § 22.
[83] Karistusseadustik. – RT I 2001,61,364 … RT I , 30.12.2017,29. § 156-157[1].

kuriteost ei ole väärteo puhul oluline tahtlus ning väärteona on karistatav nii tahtlik kui ettevaatamatu tegu.

Direktiivi 95/46/EÜ artiklist 22 (põhjenduspunkt 55[84]) tuleneb, et enne vaidluse suunamist kohtule tuleb andmesubjektidele anda võimalus pöörduda riikliku andmekaitseasutuse poole. AKI saab kaebuse alusel kohaldada nõudeid rikkunud isikuandmete töötleja suhtes haldussunnivahendeid ning teatud juhtudel kohaldada rikkuja suhtes väärteokaristust. Siiski on AKI korrakaitseorgan ja peab lähtuma KorS § 4 lg-s 2 sätestatud reeglitest, mistõttu sekkub AKI eraõiguslikesse suhtesse ainult kindlatel tingimustel. Isikute subjektiivsete õiguste kaitsmine on kohtuvõimu funktsioon. Vaid erandlikel juhtudel sekkub AKI omal algatusel ajakirjandusse kaebepõhiselt ning sekkumise korral on võimalik teha väljaandele soovitus/ettekirjutus/ettepanek ning reeglina ei mõista välja kahjuhüvitisi ega vii ajakirjanike suhtes läbi väärteomenetlusi.[85] Siinkohal juhib autor tähelepanu asjaolule, et kõnealuse KorS § 4 lg 2 reegli rakendamine andmekaitsealaste rikkumiste korral võib tuua kaasa EL andmekaitsereeglite rikkumise, kuivõrd direktiiv 95/46/EÜ ei näe ette eraõiguslike vaidluste välistamist järelevalveasutuse pädevusest, kui töötlemine toimus andmekaitseseaduste rakendusalas. Kuivõrd antud probleem ei haaku käesoleva magistritöö teemaga, ei peatu autor sellel küsimusel pikemalt.

Kuna IKS käsitleb isikuandmete töötlemist nii eraõiguslikes kui ka avalik-õiguslikes suhetes, siis kohaldatakse vastutuse aluste ja korra suhtes Võlaõigusseadust[86] või Riigivastutuse seadust[87]. Täpsustades siinkohal AKI pädevust, on oluline, et kui isikuandmeid töötleb riigiasutus ning ei suuda isikuandmete kaitse nõudeid piisavalt täita, ei saa järelevalveasutuse tegevus tõkestada isikuandmete töötleja seadusest, välislepingust või EL määrusest tulevate ülesannete täitmist ega rakendada tema suhtes Asendustäitmise ja sunniraha seaduses[88] (*edaspidi* ATSS) ettenähtud sunnivahendeid. Seega, kui isikuandmete kaitse alase ettekirjutuse adressaat on riigiasutus, ei või sunnivahendit rakendada.

[84] Siseriiklikes õigusaktides tuleb sätestada õiguskaitsevahendid juhuks, kui vastutav töötleja ei austa andmesubjektide õigusi; igasuguse kahju, mida üksikisikule võib põhjustada ebaseaduslik töötlemine, peab kompenseerima volitatud töötleja, kuid ta võidakse sellest kohustusest vabastada, kui ta tõestab, et ta ei ole kahju eest vastutav, seda eelkõige juhul, kui ta tuvastab andmesubjekti süü või kui tegemist on vääramatu jõuga; kõigi isikute suhtes, kes ei järgi käesoleva direktiivi põhjal võetud meetmeid, tuleb rakendada sanktsioone, olenemata sellest, kas tegemist on eraõiguslike või avalikõiguslike isikutega;
[85] AKI. Isikuandmete avalikustamine meedias. 19.11. 2015.
[86] Võlaõigusseadus. – RT I, 2001,81,487 ... RT I, 31.12.2017, 8.
[87] Riigivastutuse seadus, - RT I 2001, 47, 260 ... RT I, 17.12.2015, 76.
[88] Asendustäitmise ja sunniraha seadus, - RT I 2001, 50, 283 ... RT I, 12.07.2014, 29.

ATSS § 5 lg 1 on sätestatud, et sunnivahendi adressaat on füüsiline isik või eraõiguslik või avalikõiguslik juriidiline isik, keda on ettekirjutusega kohustatud nõutavat tegu tegema või keelatud teost hoiduma. Sunnivahendi adressaat on ka isik, kelle suhtes rakendatakse ATSS §-s 12 sätestatud ettekirjutuseta asendustäitmist. Sunnivahendit ei rakendata riigiasutuse suhtes. Ettekirjutuse täitmise tagamiseks kasutab AKI sunniraha ATSS sätestatud korras. Senise praktika kohaselt lisatakse ettekirjutusele hoiatus sunniraha rakendamise kohta. Sunniraha rakendamise hoiatus peaks olema efektiivne vahend, mis sunniks teabevaldajat seadusest tulenevaid kohustusi täitma. Peale sunniraha sisse nõudmist on teabevaldaja ettekirjutuse täitnud. Haldussundi kohaldatakse üldreeglina vastutava töötleja suhtes, sest just ettevõtja kui vastutav töötleja peaks tagama andmete töötlemise nõuetest ja seadustest kinnipidamise. Siiski on võimalik ka haldussunni rakendamine volitatud töötleja suhtes, kui volitatud töötleja on rikkunud spetsiifiliselt temale pandud kohustused. Haldussund ei ole karistus, vaid haldusjärelevalve meede, millega juhitakse puudujääkidele tähelepanu ja antakse võimalus need parandada.

2. VASTUTUS ISIKUANDMETE KAITSE NÕUETE RIKKUMISTE EEST EESTI KEHTIVAS ÕIGUSES

2.1. Andmekaitseõiguse jõustamine Eestis

Andmekaitse reeglid ei ole suunatud ainult andmete kasutaja keelamisele ja piiramisele. Väga oluline on ka andmesubjekti jätkuv osalemine tema andmete töötlemise protsessis. Andmetöötlusega kokku puutuvad isikud ei tohi seega unustada, et kui andmed on kogutud, ei tähenda see töötleja piiramatut voli nende kasutamiseks – andmesubjektide huvid on ka töötlemise ajal kaitstud. Oluline on meeles pidada, et ka andmete vaatamine ja neile ligipääsu võimaldamine on andmete töötlemine. Asjaolu, et isikuandmete kaitse on põhiõigus, ei tähenda veel andmete töötlemise keeldu, vaid paneb riigile töötlemise reguleerimise ja selle vajalikkuse kaalumise kohustust. Laiem isikuandmete põhiõiguslik kaitse tähendaks sisuliselt riigi kohustust olla ettevaatlik kõigi isiku kohta käivate andmetega ümberkäimisel.[89] Arvestades andmete kaitsmise vajalikkust ja riigil lasuvat kohustust on üheks andmete kaitse elemendiks ka jõustamismeetmed ja sanktsioonid, mille kaudu andmesubjektil on võimalik oma subjektiivseid õigusi kasutada. Andmete töötleja jaoks tähendab see vastutust andmekaitsealaste rikkumiste eest.

2.1.1. Vastutuse regulatsioon IKS-is

Eestis reguleerib vastutust andmekaitsealaste rikkumiste eest eelkõige IKS, kus on määratletud vastutus väärteo korras. IKS § 42 sätestab vastutuse delikaatsete isikuandmete töötlemise registreerimiskohustuse, isikuandmete kaitse turvameetmete või isikuandmete töötlemise muude nõuete rikkumise eest[90], seega on võimalikud kolm olukorda, millal isik saab toime panna isikuandmete kaitse alase väärteo:

1) registreerimiskohustuse rikkumine - praegu kehtiva regulatsiooni kohaselt tuleb delikaatsete isikuandmete töötlemisel määrata isikuandmete töötleja poolt isikuandmete kaitse eest vastutav isik või registreerida delikaatsete isikuandmete töötlemine AKI-is;[91]
2) turvameetmete rikkumine – isikuandmete kaitseks tuleb rakendada turvameetmeid (tehnilisi ja organisatsioonilisi) nende tahtmatu või volitamata töötlemise, avalikuks tuleku või hävimise eest.[92] Turvameetmete hindamisel tuleb arvestada isikuandmete

[89] I. Pilving. Juridica 2005 / 8, lk 536.
[90] IKS § 42.
[91] IKS § 27.
[92] Dirktiivi 95/46/EÜ art 17.

töötlemisega seotud riskide ja ohuga, mida delikaatsemad andmed seda kõrgemad peavad olema turvameetmed. Isikuandmete töötleja poolt rakendatud turvameetmed hõlbustavad ka AKI järelevalve teostamist;

3sikuandmete töötlemise muude nõuete rikkumine – uute tehnoloogiate kasutamisest võivad tuleneda teatavad ohud andmesubjekti õigustele ja vabadustele. Olenevalt töötlemise laadist ja ulatusest võivad tekkida ohud, mida seaduses ei ole võimalik kindlaks määrata, vaid tuleb lahendada juhtumipõhiselt. Selle sätte alla paigutuvad ka karistused nn uudishimupäringute eest, ehk olukorrad, kus andmete töötlemise õigust omavad isikud ületavad oma volitusi või tegutsevad tööülesannetest väljaspool, sooritades ebaseaduslikke päringuid uudishimust.[93]

Delikaatsete isikuandmete töötlemise nõuete rikkumisel, kui ka rikkumise korral, kui isikule on tehtud ettekirjutus ja isik pole seda täitnud, määratakse rahatrahv. AKI-l on õigus teha isikuandmete töötlejale ettekirjutus ning ettekirjutuse mittetäitmisel võib inspektsioon rakendada sunniraha.[94] Sunnivahendi rakendaja peab valima sunnivahendi, mis isikut võimalikult vähe kahjustades sunnib teda täitma talle ettekirjutusega pandud kohustust. U. Klopets on märkinud: "/.../ettekirjutuse, asendustäitmise ja sunniraha eesmärk on rikkumisele eelnenud olukorra taastamine, sest väärteokaristust kohaldatakse tagasiulatuvalt/…/".[95]

Praegu kehtiv IKS kehtestab ühetaolise vastutuse. IKS sätestab trahvi määramise võimaluse nii tahtliku rikkumise kui ka hooletuse puhul. Tahtluse defineerimisel saame lähtuda karistusõiguse teooriast, mille järgi on tahtlus toimepanija poolt süüteokoosseisule vastavate teo faktiliste asjaolude teadmine ja tahtmine.[96] Ettevaatamatus on tähelepanematu ja kohusetundetu käitumine, seejuures hoolsuskohustuse rikkumine ehk hooletus.[97]

IKS § 42 lg 1 sätestab vastutuse isikuandmete töötlemise muude nõuete eiramise eest. Isikuandmete avalikustamine on üks isikuandmete töötlemise viise ning isikuandmete avalikustamine võib andmesubjekti õigusi kõige enam kahjustada. Andmesubjekti õigused on sätestatud IKS §-des 19, 21 ning õigusi on piiratud § 20 lg 1 ja § 21 lg 3. Isikuandmete

[93] AKI: rohkelt tuleb karistada rahvastikuregistri väärkasutajaid. – Äripäev. 20.05.2013. Arvutivõrgus: http://www.ituudised.ee/uudised/2013/05/20/andmekaitse-rohkelt-tuleb-karistada-rahvastikuregistri-vaarkasutajaid (02.02.2018).
[94] IKS § 40.
[95] U. Klopets. Asendustäitmise ja sunniraha rakendamise analüüs. Tallinn: Justiitsministeerium 2011, lk 9. Arvutivõrgus: http://www.just.ee/uuringud.
[96] P. Pikamäe. KarS § 16 / 4. – Pikamäe, P., Sootak, J. Karistusseadustik. Komm vlj. Tallinn: Juura, 2015.
[97] P. Pikamäe. KarS § 18/ 2.

töötlemisele ajakirjanduse eesmärgil kehtestab eriregulatsiooni IKS § 11 lg 2, mille kohaselt võib isikuandmeid ilma andmesubjekti nõusolekuta ajakirjanduslikul eesmärgil töödelda ja avalikustada meedias kui selleks on ülekaalukas avalik huvi ning see on kooskõlas ajakirjanduseetika põhimõtetega. IKS § 11 lg 2 kohaldamisel tuleb arvestada EIK praktikat väljendusvabaduse ja eraelu tasakaalustamisel. Eraelu puutumatust ja ajakirjandusvabadust on EIK pidanud võrdseteks põhiõigusteks, mille kaal peaks olema põhimõtteliselt sama.[98] Sõnavabaduse piiramise proportsionaalsust hinnates tuleb arvesse võtta ka kohaldatud karistuse liiki ja raskust.[99] Kohaldatavad karistused võivad vähendada ajakirjanduse soovi osaleda arutelus avalikku huvi pakkuvate küsimuste üle. Ajakirjandusvabadus oleks olulisel määral pärsitud, kui meedias võiks isikuga seotud teavet töödelda ja avaldada üksnes isiku nõusolekul.

Isikuandmete avalikustamisega meedias ei tohi siiski kahjustada andmesubjekti õigusi. Kuna ajakirjanduslikul eesmärgil võib isikuandmeid töödelda ilma andmesubjekti nõusolekuta, tuleb iga juhtumi puhul eraldi hinnata, kas avalik huvi kaalub üle isiku õiguste kaitse vajaduse. Seega tuleb IKS § 11 lg 2 kohaselt riive puhul leida tasakaal eraelu puutumatuse ning avaliku huvi ja teiste isikute õiguste vahel.[100]Avaliku huvi puudumist võiks sedastada näiteks juhul, kui avaldatakse eraelu detaile, mis kuidagi ei seondu avaliku huviga ega aita kaasa ühiskondlikule debatile. Ka Riigikohtu halduskolleegium on märkinud, et eraelu puutumatuse riivena käsitatakse muu hulgas isikuandmete kogumist, säilitamist, kasutamist ja avalikustamist.[101] Kui PS § 26 „eraelu“ hõlmab ka õigust enesekujutamisele, tuleks selle all mõista eelkõige õigust oma kujutisele ja sõnale. Õigus oma kujutisele kaitseb üksikisikut tema näitamise vastu meedias ning õigus sõnale tagab seda, et isikule ei omistataks avaldusi, mida ta pole teinud. Isikul peab olema õigus ise otsustada, kas ja millisel viisil ta tahab end avalikkuse ees kujutada ning kas ja mil määral tohivad kolmandad isikud muuta tema isiksuse avaliku arutelu esemeks. Halduskolleegium on selgitanud, et investori tegevus börsil ei ole selgelt eraeluline ega avalik, vaid skaala keskel asuv tegevus.[102] Kolleegium nõustub, et kolmandale isikule ettekirjutuse tegemine kaebaja isikuandmete eemaldamiseks viidatud edetabelist tähendaks lubamatut sekkumist ajakirjandusvabadusse.

[98] EIKo 07.02.2012, 39954/08, *Alex Springer AG vs* Saksamaa, p 87; EIKo 07.07.2012, 40660/08, *Von Hannover vs* Saksamaa nr 2.
[99] EIKo, 07.02.2012, 39954/08, *Axel Springer AG vs*. Saksamaa, p 95.
[100] RKHko 3-3-1-85-15, p 21.
[101] RKHKo 3-3-1-3-12, p 19.
[102] RKHKo 3-3-1-85-15, p 24.

Sarnaselt IKS § 42 lg-ga 1, mis sätestab isikuandmete kaitse turvameetmete nõuete rikkumise eest rahatrahvi, on sama koosseis reguleeritud ka KarS § 157^1 lg 1, kus on sätestatud ebaseadusliku juurdepääsu võimaldamise eest rahatrahv. Juurdepääsu võimaldamise näitena võib tuua juhtumi kui infosüsteemis autentimiseks vajalikud esemed või salasõnad antakse üle teisele isikult. Andmete avaldamine või juurdepääsu võimaldamine on igal juhul ebaseaduslik, kui selleks ei ole saadud andmesubjektilt kehtivat luba või puudub seadusest tulenev alus (IKS § 10 lg 1).[103] Omakasu motiiv tähendab soovi saada mistahes ainelist kasu raha, asja, vara, varalisest kohustusest vabanemise vms näol.[104] Kahju käesoleva koosseisu tähenduses saab seisneda varalises kahjus, mille määr pole tähtis. Samuti on rahalise karistuse või kuni kolmeaastase vangistusega karistatav teise isiku identiteedi ebaseaduslik kasutamine, s.t kui edastatakse teise isiku isikuandmeid tema nõusolekuta, võimaldatakse neile juurdepääs või kasutatakse neid eesmärgiga varjata kuritegu või luua teise isikuna esinemise teel temast teadvalt ebaõige ettekujutus ja tekitatakse kahju teise isiku seadusega kaitstud õigustele või huvidele.

IKS § 42 kaitsealasse kuulub ka isikuandmete kaitse, mis puudutab töötaja ja tööandja vahelisi suhteid. IKS § 14 lg 1 p 4 järgi on isikuandmete töötlemine lubatud andmesubjekti nõusolekuta, kui isikuandmeid töödeldakse andmesubjektiga sõlmitud lepingu täitmiseks või lepingu täitmise tagamiseks, välja arvatud delikaatsete isikuandmete töötlemine. See tähendab, et tööandjal on õigus töödelda töötaja isikuandmeid, kuivõrd see on vajalik töölepingu täitmiseks. Samas ei saa töölepingus ega töösisekorra reeglites siiski ette näha selliseid isikuandmete töötlemisi, mis oleks vastuolus IKS või teiste seadustega. Soome õiguskorrast saab tuua näite tööõiguse valdkonnast: tööandja tohib oma töötaja koha andmeid koguda eelkõige otse töötajalt endalt või töötaja nõusolekul teistest allikatest.[105] Ühe hiljutise kohtulahendi tegi ka EIK, mis puudutas privaatsus töökohal.[106] EIK on leidnud, et töötaja e-posti konto jälgimine on rikkunud tema õigust eraelu puutumatusele ja kirjavahetusele EIÕK artikkel 8 tähenduses.

[103] A. Nõmper. KarS § 157^1 /3.3 – 3.5.
[104] J. Sootak. KarS § 58/ / 2.
[105] Act on the Protection of Privacy inPrivacyin Working Life, 477/2001, 08.06.2001.
[106] EIKo, 12.01.2016, 61496/08, *Bárbulescu vs* Rumeenia, p35.

2.1.2. Direktiivist 95/46/EÜ tulenev vastutus

Isikuandmete kaitse on valdkond, mille reguleerimisel on liikmesriigid seotud EL õigusega. EL õiguse tõlgendamise õigus on Euroopa Kohtul ning seetõttu on EK praktika abiks liikmesriigi vastavate seaduste tõlgendamisel ja kohaldamisel.[107] Vastavalt direktiivile 95/46/EÜ kaitsevad liikmesriigid isikuandmete töötlemisel füüsiliste isikute põhiõigusi ja vabadusi ning eelkõige nende õigust eraelu puutumatusele.[108] Direktiivi 95/46/EÜ põhjenduspunkti 8 kohaselt on direktiivi eesmärk viia isikuandmete töötlemisega seotud üksikisikute õiguste ja vabaduste kaitse kõigis liikmesriikides samale tasemele. Siiski ei kohaldu direktiiv 95/46/EÜ isikuandmete töötlemise suhtes, kui seda teeb füüsiline isik isiklikel või kodustel eesmärkidel.[109]

EK on märkinud, et kuivõrd direktiivi 95/46/EÜ sätted reguleerivad isikuandmete töötlemist, mis võib riivata põhivabadusi ja eriti õigust eraelu puutumatusele, tuleb nende tõlgendamisel lähtuda põhiõigusest.[110] Vajadusel tuleb tõlgendada andmekaitse sätteid ka õigusmõistmise käigus. EK on põhjendanud liikmesriikide kohustust direktiivi 95/46/EÜ täpsustada järgmiselt: „/…/andmekaitsedirektiivi sätted ise on paratamatult üldised, sest direktiiv peab reguleerima suurt hulka erinevaid olukordi, kuid direktiivis sisalduvate nõuete teatav paindlikkus on põhjendatud/…/“[111].

EK on ka selgitanud, et kuigi direktiivi 95/46/EÜ sätted näivad olevat sisu poolest tingimusteta ja piisavat täpsed, võivad isikud siiski neile riigisiseses kohtus vaidluses riigi vastu tugineda, seda ka juhul, kui riik on direktiivi valesti üle võtnud või jätnud selle riigisisesesse õigusesse üle võtmata. Näiteks võib tuua direktiivi artikli 7 punkti f, mis käsitleb isikuandmete töötlemist õigustatud huvi alusel, tõlgenduse. Kuigi liikmesriikidel on direktiivi 95/46/EÜ kohaselt mõnede sätete rakendamisel kaalutlusruum, näeb artikli 7 punkt f ette tingimusteta kohustuse.[112] Artikli 7 punkt f on piisavalt täpne ja vahetu õigusmõjuga. Kohus märkis, et riigisisesed õigusnormid, mis kehtestavad andmesubjekti nõusolekuta isikuandmete

[107] E. Rohtmets. Isikuandmete kaitse küsimused Euroopa Kohtu eelotsustes. Andmesubjekti õiguste kaitse. Kohtupraktika analüüs. Tartu: Riigikohtu õigusteabe osakond 2013.
Arvutivõrgus: :http://www.riigikohus.ee/vfs/1455/Andmesubjekti%20oigused_EK_analuus.pdf, lk 5 (05.01.2018).
[108] Direktiivi 95/46/EÜ art 1.
[109] Direktiivi 95/46/EÜ art 3.
[110] EKo 20.05.2003, C-465/00, C-138/01 ja C-139/01, *Rechnungshof vs Österreichischer Rundfunk* jt, p 68.
[111] EKo 06.11.2003, C-101/01, *Lindqvist vs* Rootsi .
[112] EKo 24.11.2011, C-468/10 ja C-469/10, p 44.

töötlemiseks täiendavad normid, on vastuolus artikli 7 punktida f. Tulenevalt direktiivist 95/46/EÜ tuleb kaitset igasuguse isikuandmete töötlemise suhtes rakendada ühtselt kõigis liikmesriikides. Liikmesriikidel on jäetud diskretsioon direktiivi sätteid ülevõetavate riigisiseste õigusaktide ulatuse laiendamiseks nendele valdkondadele, mis ei kuulu direktiivi 95/46/EÜ kohaldamisalasse.

E. Rohtmets ja L. Kanger on 2011. aastal tõdenud, et: „/…/Eesti isikuandmete kaitse seadus võtab direktiivi 95/46/EÜ üle samas printsipiaalsuse astmes, kui on direktiiv ise. Riigisisese õigusega direktiivi eriti ei täpsustata, kuigi seda lubab otsesõnu direktiivi 95/46/EÜ artikkel 5 ja toonitab EK/…/"[113].

Nagu eespool mainitud on direktiivi 95/46/EÜ sätted üldised ja teatav paindlikkusega. Siiski on oluline,et Eestis oleksid IKS-i sätted üheselt mõistetavad nii andmete töötlejatele, kui ka andmesubjektidele, sh nende õigused ja kohustused peavad olema täpselt ja selgelt piiritletud ja reguleeritud. Samas on õige, et teatud küsimustes on jäetud liikmesriikidele kaalutlusõigus riigisiseselt täpsustada andmekaitsedirektiivis isikuandmete töötlemisega seotud küsimused, kui EL tasandil ei oleks ühtse regulatsiooni kehtestamine vajalik või võimalik. Näitena võib siinkohal tuua kohtumenetluse, mille reeglid on riigiti äärmiselt erinevad ja seega peavad liikmesriigid leidma sellised lahendused isikuandmete kaitse reguleerimiseks, mis sobiks konkreetse riigi õigus- ja kohtusüsteemiga.

Vastutuse osas on oluline direktiivi 95/46/EÜ artikkel 24, mille kohaselt liikmesriigid võtavad sobivaid meetmeid, et tagada direktiivi sätete täielik rakendamine ja sätestavad eelkõige sanktsioonid, mida kohaldatakse direktiivi kohaselt vastuvõetud sätete rikkumise puhul. Direktiivi 95/46/EÜ põhjenduspunkti 55 kohaselt tuleb siseriiklikus õiguses sätestada õiguskaitsevahendid juhuks, kui vastutav töötleja ei austa andmesubjektide õigusi, samuti kõigi isikute suhtes, kes ei järgi direktiivi põhjal võetud meetmeid. Sellistel juhtudeltuleb rakendada sanktsioone, olenemata sellest, kas tegemist on eraõiguslike või avalik-õiguslike isikutega.[114]

Direktiivis 95/46/EÜ on ette nähtud isikuandmete kaitse nõuete mittetäitmise ja rikkumise korral karistus. Kaitsmise põhimõtted peavad kajastuma töötlemise eest vastutavate isikute, riigiasutuste, ettevõtte, esinduse või muude organite suhtes kehtestatud kohustuse.[115] Asjaolu,

[113] E. Rohtmets, L. Kanger, Eesti andmekaitse Euroopa Kohtupraktika peeglis. 2011.
[114] Direktiivi 95/46/EÜ pp 55.
[115] Direktiiv 95/46/EÜ pp 25.

et järelevalveasutus teeb rikkujale pigem meeldetuletusi ja hoiatusi, ei ole iseenesest halb, kuid need meetodid oleksid efektiivsemad, kui neid toetaks efektiivsed jõustamismeetmed, kui rikkuja teistele meetmetele ei allu.[116] Ühiskonnas peab olema tagatud normide reaalne toime, mis tähendab institutsionaliseeritud võimu tegevust normide realiseerimisel.[117]

Iga kohustuse mittetäitmisele järgneb vastutus ning on ette nähtud karistus. J. Sootak on kirjutanud: "/.../ hälbiva käitumise valdkonnas vajab ühiskond selliseid norme, mis mitte ei kirjelda seda käitumist, vaid kirjutavad ette ka ühiskonna reageerimisvormi /.../". Kui käitumist kirjeldav normiosa on *dispositsioon*, siis ühiskonna reageerimisvorm avaldub *sanktsioonis."*[118] Iga sanktsioon ei ole vastutus, kuid vastutus saab eksisteerida vaid sanktsioonide, täpsem alt nende kohaldamise kaudu.[119] Seega on sanktsioon üksnes riigi negatiivne reaktsioon õigust rikkuvale teole. J. Sootak on selgitanud, et sanktsiooni kasutamine sekkumise vahendina tähendab seda, et karistusõigus ei reguleeri inimese käitumist otseselt, vaid mõjutab neid karistusega.[120] Karistusõiguses reageerib riik õigusvastasele teole ning läbi selle reageeringu mõjutatakse isikut ennast, teisi isikuid kui ka üldsust.[121] Väärtegu on pigem manitsus ja korralekutsumine tulevaste kohustuste täitmiseks, kuna kriminaalkaristus sisaldab olulist sotsiaaleetilist etteheidet.[122] J. Sootak on selgitanud: "/.../ väärteokoosseis on vajalik üksnes selliste õiguslike kohustuste sanktsioneerimisel, mille õigeaegse või täieliku täitmata jätmisega kaasneb oluline oht või kahju õigushüvele. Kui kohustust ei ole täidetud ja ka oht või kahju ei ole saabunud, piisab subjekti tegutsema kohustamiseks haldussunnist/…/".[123]

Direktiiv 95/46/EÜ on jätnud liikmesriikidele suures osas valikuvabadust, mille tulemusena on isikuandmete kaitse regulatsioon liikmesriikides erinev. Erinevustest tulenevalt ei ole

---

[116] D. Korff. EC study on implementation of Data Protection Directive. Comparative summary of national laws. Cambrige: September 2002, p 207. – Available: http://www.garanteprivacy.it/documents/10160/10704/Stato+di+attuazione+della+Direttiva+95-46-CE, ...kuup (18.01.2108).

[117] B.-D. Meier.Strafrechtliche Sanktionen. Berlin: Springer, 2001.

[118] R. Kiris, P. Pikamäe, J. Sootak. Sanktsiooniõigus. Tallinn: Juura 2017, lk 15.

[119] *Ibid*, lk 17.

[120] J. Sootak. Karistusõiguse alused. Tallinn: Juura 2003, lk 19.

[121] S. Põllumäe. Mõiste *administrative penalties* riigisisesesse õigusesse ülevõtmine. Tallinn: Juura. Õiguskeel 2015 / 2, lk 27.
Arvutivõrgus:https://www.just.ee/sites/www.just.ee/files/sander_pollumae._moiste_administrative_penalties_riigisisesesse_oigusesse_ulevotmine.pdf (06.03.2018).

[122] V. Krey. Deutsches Strafreecht. Allgemeiner Teil. Bd 1. Stuttgart: Kohlhammer 2001, § 1, vnr 20-21.

[123] J. Sootak. Karistusõigese revisjon kuriteo-, väärteo- ja haldusõiguse piirimail. Juridica 2013 / 4, lk 247.

saavutatud ka direktiiviga 95/46/EÜ soovitud eesmärke.[124] Kuigi direktiiv eraldi halduskaristuse regulatsiooni ette ei näe, on siiski enamik liikmesriike võtnud kasutusele trahvi tegemise võimaluse. Kehtiva direktiivi järgi on igal liikmesriigil võimalik valida trahvide suurus, mis on hetkel riigiti väga erinev. Näiteks Saksamaal on trahvi suurus 50 000 kuni 100 000 eurot[125], Austrias 10 000 kuni 25 000 eurot[126], Lätis on juriidilisele isikule võimalik määrata trahvi kuni 14 000 eurot[127], Iirimaal on trahvi määrasid isegi vähendatud ning hetkel on trahvide suurus 1 000 kuni 50 000 naela. Sloveenias on üksikisikule määratav maksimaalne trahv 830 eurot, samas Suurbritannias ja Hispaanias on maksimaalne trahv 500 000 eurot.[128]

Eestis on vastutus reguleeritud IKS-i 7. peatükis. Isikuandmete kaitse nõuete rikkumise korral on väärteomenetluses võimalik füüsilisele isikule määrata rahatrahv kuni 300 trahviühikut ning juriidilist isikut võib karistada kuni 32 000 euroga. AKI-l on võimalik ettekirjutuse mittetäitmisel võimalik rakendada sunniraha kuni 9600 eurot. Rahatrahvi kohaldamise regulatsioon on ette nähtud KarS § 47, mis sätestab väärteo eest kohaldatava põhikaristusena rahatrahvi nii füüsilise kui juriidilise isiku jaoks. Kui tegu on karistatav väärteona, saab see olla karistatav kuriteona üksnes siis, kui KarS-is on selgelt välja toodud nn kriminaliseerivad tunnused.[129] Vastav regulatsioon on olemas KarS §-ides 157 ja § 157[1].

Suured ettevõtted, näiteks Facebook, Google, Amazon on saanud suuri trahve, kuid üksikisiku andmekaitseõigusi siiski rakendatud ei ole. Näiteks 2017 aasta mais trahvis Eurooopa Komisjon Facebook'i 110 miljoni euroga, juunis 2017 trahvis Euroopa Liit Google't 2,4 miljardi euroga. Andmekaitse nõudeid arvestades võib olla ebarahuldavate seadmete või tarkvara väljavahetamine, samuti turvenõuete rakendamine väga kulukas, mille kõrval trahvide korduv tasumine on ettevõtetele kokkuvõttes odavam. Sellised suured ettevõtted registreerivad oma firmad EL riikidesse, kus trahvid ja karistused on väiksemad ning üldine andmekaitsereeglite

[124] European Comission report. First report on the implementation of the Data Protection Directive (95/46/EC). COM(2003) 265 final. Brussels: 15.05.2003. Available: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52003DC0265#text, (31.01.2018).
[125] Bundesdatenschutzgesetz (BDSG). Arvutivõrgus: https://www.gesetze-im-internet.de/bdsg_1990/ (11.02.2018).
[126] Datenschutzgesetz (DSG). Arvutivõrgus: https://www.digital.austria.gv.at/data-protection-act (05.02.2018).
[127] Fizisko personu datu aizsardzības likums. Arvutivõrgus: https://www.vestnesis.lv/ta/id/4042-fizisko-personu-datu-aizsardzibas-likums (18.01.2018).
[128] European Union Fundamental Rights Agency. Access t odatato data protection remedies, p 21. Arvutivõrgus: http://fra.europa.eu/et (18.01.2018).
[129] Karistusseadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse seletuskiri, 16.07.2013. Arvutivõrgus: https://www.just.ee/sites/www.just.ee/files/elfinder/article_files/karistusseadustiku_ja_sellega_seonduvalt_teiste_seaduste_muutmise_seaduse_seletuskiri.pdf (18.01.2018).

rakendamise praktika leebem. Rikkumistest saadud tulu võib olla kordades suurem, kui neile määratud trahvid. Näiteks paiknevad valdav osa USA päritoluga suurettevõtteid Iirimaal, kus nende peamiseks tegevuseks on isikuandmete töötlemine. Iiri andmekaitseseadus *(Data Protection ACT)* sätestab peale 2003. aasta muudatusi karistustena trahvimäärad 1000-50 000 naela.[130]

Näitena üks hiljutine juhtum, kus Facebook´i sõnul andsid nad Cambridge'i ülikooli psühholoogia professorile loa pääseda ligi nendele kasutajatele, kes laadisid alla tema mobiilirakenduse. Vaatamata sellele, et professori küsitlust tegid ainult 270 000 inimest, pääses ta ligi enam kui 50 miljoni inimese andmetele, sest Facebook lubas professoril saada ka küsitluse täitnud isikute sõprade andmed. Andmete müük on Facebooki üks suurimaid tuluallikaid – kasutajatelt kogutud andmeid müüakse näiteks mobiilirakenduste arendajatele. Juhtum näitab aga, et vaatamata kliendiga sõlmitud andmelepingutele, võivad sotsiaalvõrgustiku kasutajate isiklikud andmed lõpetada ikkagi pahatahtlike kavatsustega kolmandate osaliste käes. [131]

Seega ei ole direktiiviga 95/46/EÜ saavutatud andmekaitse õiguse harmoniseerimist, sealhulgas erinevad väga oluliselt ka isikuandmete töötlemise nõuete rikkumiste eest määratavad sanktsioonid. Selline erineva tasemega andmekaitse õiguse kohaldamine liikmesriikides võib tekitada õiguskindlusetust ning tuua kaasa olukorda, kus ettevõtted valivad oma registreeritud asukohaks selliseid EL riike, kus on andmekaitsealaste reeglite rakenamine lihtsam ning võimalikud sanktsioonid madalamad. See kõik nõrgestab omakorda oluliselt andmesubjekti positsiooni ning võimalust tõhusalt teostada oma andmekaitseõigusest tulenevaid õigusi. Tulenevalt eeltoodust on väga oluline ühtlustada liikmesriikide poolt isikuandmete nõuete rikkumisel määratavaid sanktsioone. Oluline on tagada ühtne regulatsioon Euroopas,ei tekiks ebavõrdne konkurents ettevõtete vahel ning üksikisikul oleks võimalus saada tõhusat kaitset andmete töötlemise reeglite rikkumise korral.

[130] Irish DPA, arvutivõrgus - https://dataprotection.ie/docs/Home/4.htm (02.02.2018)).
[131] Andmeskandaali sattunud Facebook kaotas oma väärtusest 37 miljardit. – Postimees. 20.03.2018. Arvutivõrgus:https://majandus24.postimees.ee/4444519/andmeskandaali-sattunud-facebook-kaotas-oma-vaartusest-37-miljardit (01.04.2018)

2.1.3. Andmekaitse riiklik järelevalve

Direktiivi 95/46/EÜ artikli 28 lg 1 tuleneb järelevalveasutuse sõltumatus. Vältimaks inspektsiooni kuulumist politseiasutustega samasse haldusalasse ja tagada sellega AKI sõltumatus, viidi 1999. aastal siseministeeriumi valitsemisalas loodud asutus 2007. aasta veebruaris üle justiitsministeeriumi valitsemisalasse.[132] Vabariigi valitsuse seaduse[133] § 59 lõike 3 kohaselt on AKI justiitsministeeriumi valitsemisalas, samuti kuuluvad justiitsministeeriumi valitsemisalasse andmekaitse alased küsimused.

Direktiivi artikli 28 lõige 3 nõuab, et järelevalveasutusel peab olemas olema volitus osaleda kohtumenetluses ja volitus juhtida rikkumistele õigusasutuste tähelepanu. E. Rohtmetsa ja L. Kangeri arvates ei ole Vabariigi Valitsuse seaduse § 101 kooskõlas direktiiviga 95/46/EÜ, sest muudel riigiorganitel ei tohiks direktiivi mõtte kohaselt olla riikliku järelevalve menetlusse sekkumise õigust. Nad on seisukohal, et AKI kui sõltumatu järelevalveasutus peab riigiasutuste süsteemis seisma väljaspool ühegi ministeeriumi kontrolli majandusliku, organisatsioonilise ja isikliku sõltumatuse tähenduses, et välistada isikute põhiõiguste kaitse taseme sõltuvus poliitilisest tahtest. Olukorras, kus AKI algatab ekslikult väärteomenetluse ja kohaldab sunniraha põhiseadusliku institutsiooni suhtes või teeb muul põhjusel õigusvastase järelevalveotsuse, peab olema ka tõhus võimalus selle otsuse vaidlustamiseks ja väärpraktika muutmiseks.[134]

Kaebuse eraelu kaitseks AKI-le saab esitada, kui isikuandmeid on väärkasutatud ning rikkuja eirab nõuet lõpetada isiku õiguste rikkumine. Inspektsiooni tegevus on suunatud rikkumise lõpetamisele. Kui teised meetmed ei ole tõhusad, on AKI-l võimalik algatada väärteomenetlus ja määrata trahv. Piiratud juhtudel on ette nähtud ka kriminaalvastutus. Trahvi määramine on AKI õigus, mitte kohtustus.

AKI ülesandeks on tuvastada, kas leidis aset isikuandmete kaitse nõuete rikkumine või tegutses andmete töötleja õiguspäraselt. Näiteks IKS § 11 lg 2 kohaselt võib isikuandmeid avalikustada meedias ka ilma inimese enda nõusolekuta kui on ülekaalukas avalik huvi, avalikustatakse ajakirjanduslikul eesmärgil, seda tehakse kooskõlas ajakirjanduseetika põhimõtetega ning avalikustamine ei kahjusta ülemäära inimese õigusi. Seejuures tuleb arvestada, et inimese

[132] E. Rohtmets, L. Kanger, Eesti andmekaitse Euroopa Kohtupraktika peeglis. 2011.
[133] Vabariigi Valitsuse seadus. – RT I 1995, 94, 1628 ... RT I, 28.12.2017, 19.
[134] E. Rohtmets, L. Kanger, Eesti andmekaitse Euroopa Kohtupraktika peeglis. 2011.

eraeluliste detailide avalikustamine lihtsalt avalikust uudishimust, ei saa käsitleda veel avaliku huvina. AKI sekkub ajakirjandusse kaebusepõhiselt ning vaid erandlikel juhtudel oma algatusel. Eelkõige kui on tegemist alaealisega, tegemist on tõeliselt delikaatsete isikuandmetega, samuti kui rikkumine puudutab suurt hulka inimesi või on korduv.[135] Inspektsiooni peadirektor V. Peep on selgitanud: "/ .../seadus lubab ajakirjanduslikul eesmärgil ülekaaluka avaliku huvi korral isikuandmeid avaldada ka ilma asjaosalise nõusolekuta. ... Pelk uudishimu aga ei ole veel avalik huvi. Seega ajakirjandusvabaduse kaitse ei laiene avaliku uudishimu rahuldamisele kellegi eraelu detailide osas/…/"[136]

Alates 1. jaanuarist 2015 kehtivas IKS-is on seadust täiendatud IKS §-ga 40^1, mis sätestab AKI võimalust esitada taotluse teenistusliku järelevalve korraldamiseks. Lõikest 1 tulenevalt kui isikuandmete töötleja jätab AKI ettekirjutuse täitmata, võib AKI pöörduda isikuandmete töötleja kõrgemalseisva asutuse, isiku või kogu poole teenistusliku järelevalve korraldamiseks või ametniku suhtes distsiplinaarmenetluse algatamiseks. Üksikisiku suhtes, kes rikkus teenistuskohustuste raames töötlemise reegleid, saab läbi viia distsiplinaarmenetluse. Andmekaitsealaste rikkumistel on avaliku sektori ja erasektori vahe selles, et andmetöötlejat kui institutsiooni (riiki ega omavalitsust ega tema asutust) ei saa väärteovastutusele võtta, küll aga personaalselt andmetöötleja ametnikku/töötajat.[137] Haldussundi või väärteokaristust kohaldab inspektsioon üldreeglina ettevõtte suhtes, sest viimane vastutab töötleja nõuetest ja seadusest kinnipidamise eest.

Isikuandmete töötlemise nõuete rikkumise korral on AKI-l võimalik teha ettekirjutusi.[138] Kui riigiasutusest isikuandmete töötleja ei täida ettekirjutust selles määratud tähtaja jooksul, võib AKI pöörduda Halduskohtumenetluse seadustikus[139] sätestatud korras protestiga halduskohutusse.[140] Haldussund ei ole oma olemuselt karistus, vaid haldusjärelevalve meede, millega juhitakse puudujääkidele tähelepanu ning antakse võimalus need parandada. Sõltuvalt IKS § 23 sätestatud rikkuja subjektist tuleb kahju hüvitada kas eraõiguse või riigivastutuse sätete järgi.[141]

---

[135] AKI. Isikuandmete avalikustamine meedias.
[136] *Ibid*,
[137] AKI peadirektori seisukohad uue andmekaitseõiguse kontseptsiooni asjus (koostatud Justiitsministeeriumis 27.04.2017). Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/jum_oigusraamistiku_kontseptsiooni_markused.pdf (08.01.2018).
[138] IKS § 40 lg 1.
[139] Halduskohtumenetluse seadustik, RT I. - 23.03.2011, 3 ... RT I, 28.11.2017, 3.
[140] IKS § 40 lg 4.
[141] RKHKo, 3-3-1-98-06 p 22.

Seni on AKI rikkumistele reageerimiseks kasutanud peamiselt sunniraha, millele eelneb sunniraha hoiatust sisaldav ettekirjutus. Hetkel kehtiva Eesti õiguse kohaselt ei ole sunniraha karistus ATSS § 3 lg 2 kohaselt ning ei käsitata sunnivahendi rakendamist karistusena. ATSS § 1 järgi kujutab haldussund endast ettekirjutust, asendustäitmist ja sunniraha. Ettekirjutuse, asendustäitmise ja sunniraha eesmärk on rikkumisele eelnenud olukorra taastamine, sest väärteokaristust kohaldatakse tagasiulatuvalt.[142] Siiski kehtiva õigussüsteemi kontekstis ei kuulu väärteod aga mitte riigi haldustegevuse, vaid karistusõiguse valdkonda.

AKI on liitunud e-toimiku süsteemiga[143], mida kasutatakse väärteomenetluse läbiviimiseks, sh andmevahetuseks teiste asutustega näiteks karistuse andmete edastamisel Karistusregistrile. E-toimiku süsteemi saab siseneda üksnes ID-kaardiga pädevad ametnikud ja menetlusosalised ise. AKI võrgulehel on ettekirjutused ja vaideotsused avalikult kättesaadavad. Jõustunud väärteootsused registreeritakse karistusregistris[144] ning neile kehtib juurdepääsupiirang.

Erinevalt vaideotsustest ja ettekirjutustest ei ole väärteootsused avalikud, neid saab küsida üksnes teabenõude esitamisega ning jõustunud otsustele kehtib juurdepääsupiirang. Tulenevalt Väärteomenetluse seadustikust (*edaspidi VTMS*) § 62 võib AKI väärteomenetlusega seotud asjaolusid avalikustada üksnes erandlikel juhtudel. Inspektsioon jätab endale õiguse, kui isik viib ise menetlusalase info avalikkuse ette, anda vajadusel oma tegevuse kohta avalikkusele selgitusi ning ei avalda seejuures teavet suuremas ulatuses, kui isik ise eelnevalt on avalikustanud.[145] Eeltoodust tulenevalt ei ole võimalik AKI väärteopraktikat põjalikult analüüsida, kuna materjalid ei ole avalikud.

Vastutus väärteo korras on sätestatud IKS § 42. Isikuandmete töötlemisnõuete rikkumise tuvastamisel on võimalik AKI-l algatada haldusmenetlus ning selle raames kohustada töötlejat isikuandmete töötlemine seadusega kooskõlla viia, tehes vastavale töötlejale ettekirjutuse. Juhul kui ettekirjutust ei täideta, on võimalik täiendavalt määrata ka sunniraha.

Väärteokaristuse puhul lähtutakse VTMS ettenähtud menetluskorrast ning süü määramisel on aluseks KarS üldosas sätestatu. Väärteona on karistatav nii tahtlik kui ettevaatamatu tegu.

[142] U. Klopets. Asendustäitmise ja sunniraha rakendamise analüüs, lk 9.
[143] E-toimik. Arvutivõrgus: http://www.e-toimik.ee/ (12.03.2018)).
[144] Karistusregister. Arvutivõrgus: http://www.rik.ee/et/karisturegister (12.03.2018)).
[145] AKI. Väärteomenetlused. 08.01.2015. Arvutivõrgus: http://www.aki.ee/et/vaarteomenetlused-0 (02.03.2018)).

Seadusandja poolt on ette antud karistuse piirid ning konkreetne karistus jääb väärteomenetleja otsustada, arvestades konkreetse juhtumi asjaolusid. Väärteomenetluse läbiviimist reguleerib VTMS koos Kriminaalmenetluse seadustikuga[146].

KrMS § 214 lg-s 2 ja VTMS-s § 62 lg-s 1 on sätestatud põhimõtted, millega peab andmete avaldamisel arvestama, kui menetlus ei ole lõppenud, st enne otsuse tegemist. Kohtuvälise menetluse kohta võib andmeid avaldada väärteomenetluse, andmesubjekti või avalikkes huvides, seda vastavate piirangutega. Seega üksnes juhul, kui ei kahjustata ülemäära väärteomenetlust, riigi huve või ärisaladust, samuti andmesubjekti ega kolmandate isikute õigusi. Informatsiooni edastamine ei tohi kahjustada ka alaealise huve. Vastava otsuse tegemiseks on kohtuvälisel menetlejal kaalutlusõigus, muuhulgas ka mõiste "avalik huvi" tõlgendamiseks. Eeltoodust tulenevalt tuleb andmete avaldamisel menetlusvälistele isikutele ja kolmandatele isikutele ning nende esindajatele lähtuda VTMS § 62 lg-st 1 kaalutlemise tulemina. Seega on kohtuväline menetleja kohtustatud tagama informatsiooni edastamise ulatuses, mis ei kahjusta väärteomenetlust, samuti isikute seadusega kaitstavaid õigusi ja huve.

J. Sootak on haldussunni ja väärteokaristuse piiritlemisel välja toonud, et väärteokoosseis on vajalik nende õiguslike kohustuste sanktsioneerimisel, mille õigeaegse või täieliku täitmata jätmisega võib kaasneda oluline oht või kahju õigushüvele. Kui kohustust ei ole täidetud ja ka oht või kahju ei ole saabunud, piisab subjekti tegutsema kohustamiseks haldussunnist.[147] J. Sootak on seisukohal, et haldussund on piisav valdkonnas,
kus toimub intensiivne riiklik järelevalve ning rikkumisi on võimalik selle järelevalve käigus kiiresti avastada ja kõrvaldada.[148] Tema arvates väärtegu ja haldussund ei välista teineteist, enne peaks olema haldussund ning haldussunni raames võiks pigem vajadusel sunniraha määra suurendada, mitte kehtestada väärteovastutust.[149]

Eesti siseriiklikus õiguses on väärteokaristuse ja sunniraha iseloom täiesti erinev, sealjuures on sunniraha mõjutusvahend ja mitte karistus.[150] Halduskaristus ja väärteokaristuse eristamisest oleneb see, kas karistust saab rakendada koduvalt ning kas karistus tuleks kanda karistusregistrisse.[151]

[146] Kriminaalmenetluseseadustik. – RT I 2003, 27, 166 ... RT I, 06.07.2017, 6.
[147] J. Sootak. Juridica 2013 / 4, lk 248.
[148] *Ibid*, lk 248.
[149] *Ibid*, lk 248.
[150] RKÜKo 10, 3-2-1-4-13, p 40.
[151] J. Sootak. Juridica 2013 / 4, lk 248.

2.1.4. Karistusõiguslik regulatsioon

Peamine vastutus isikuandmete töötlemisnõuete rikkumise eest on selle isiku ees, kelle andmeid töödeldakse (andmesubjekt). Üldjuhul vastutab rikkumise eest vastutav töötleja ehk enamasti ettevõte, kuid samas ei ole välistatud ka töötaja vastutus, kui ta rikub enda töölepingust tulenevaid kohustusi. Isikuandmete töötleja vastutus on süüline. Andmesubjekti kaebeõiguse realiseerimisel kohtu korras tuleb isikuandmete töötlemise nõuete rikkumise puhul arvestada, et sõltuvalt sellest, millist liiki õigussuhtes isiku õigusi rikuti, peab ta pöörduma kas hagiga maakohtusse (kui tema õigusi rikuti eraõiguslikus suhtes) või kaebusega halduskohtusse (kui tema õigusi rikuti avalik-õiguslikus suhtes). Samuti juhul, kui isiku taotlusel asja uurinud AKI isikuandmete töötlemise nõuete rikkumist ei avastanud ning isik sellega ei nõustu, pidades isikuandmete töötleja tegevust tema õigusi rikkuvaks, saab ta kohtus vaidlustada isikuandmete töötleja tegevust. Kui taotleja leiab, et AKI rikkus isiku taotluse läbivaatamisel ise seadust, võib ta esitada kaebuse halduskohtusse.

Eesti õiguses kasutatakse õigusrikkumiste määratlemisel kahetasandilist lähenemist. Üldterminina kasutatakse mõistet *süütegu*, mis on karistusseadustikus või muus seaduses sätestatud kui karistatav tegu (KarS § 3 lg 1). Süüteod jagunevad omakorda väärtegudeks ja kuritegudeks (KarS § 3 lg 2). Seejuures on mõlema süüteoliigi puhul tegemist riigi poolt õigusvastaseks tunnistatud tegudega, mille eest on ette nähtud karistus. Väärtegude ja kuritegude erinevus seisneb määratava sanktsiooni ranguses ning ette nähtud karistuse liigis. Seejuures mõlema süüteoliigi puhul on võimalik määrata nii rahaline sanktsioon (trahv või rahaline karistus) kui ka vabadusekaotus (arest või vangistus). Väärtegude puhul viib menetluse läbi kohtuväline menetleja, kuritegude puhul juhib kohtueelset menetlust prokuratuur, kuid mõlemale süüteoliigile kohalduvad karistusseadustikus sätestatud üldnormid.[152]

Isikuandmete kaitse nõuete rikkumise eest on ette nähtud karistusõiguslik vastutus. Kuna isiku privaatsusesse sekkumine võib mõjutada suurel määral isiku eraelu, siis on selline tegevus riigi poolt kriminaliseeritud. Isikuandmete ebaseaduslik avaldamine on sätestatud KarS § 157. Kvalifitseeritava süüteo subjekt KarS § 157 järgi saab olla vaid erilise isikutunnusega isik, kelle kriminaalõiguslik vastutus lähtub seadusest tulenevast kohustusest hoida talle kutse- või ametitegevusega teatavaks saanud saladust. Kriminaalkolleegium on täpsustanud, et eraelu

[152] Isikuandmete kaitse uue õigusliku raamistiku kontseptsioon. 18.04.2017.

hõlmab isiku tervet isiklikku elusfääri, kogu tema elukorraldust. Seega on teave isiku elukoha, registreeritud sõidukite ja toimepandud õigusrikkumiste kohta käsitletav eraelu puudutava teabena.[153]

Oluline on kutse- või ametitegevuses teatavaks saanud teave, mis tähendab, et isik ei oleks isikuandmeid teada saanud, kui tal ei oleks vastavat kutse- või ametiseisundit. Isikuandmed peavad käima kellegi teise kohta, see tähendab ükskõik kes, peale kohustuse rikkuja enda. Avaldamine on teabe teatavakstegemine teisele isikule, mis on võimalik igasuguses vormis, tegevuse või tegevusetusega. Avaldamise ebaseaduslikkus on eelkõige andmete avaldamine vastuolu kehtivate nõuetega. Vastuolu võib seisneda nii andmete avaldamise viisi (vajalike turvameetmete kasutusele võtmata jätmine), andmete saajas (saaja ei ole andmete saamiseks õigustatud isik) kui ka muudes asjaoludes. Süüteo subjektiks saab olla üksnes erilise isikutunnusega isik, kellele on seadusega pandud kohustus isikuandmeid mitte avaldada.

Karistusõiguse revisjoni raames peeti oluliseks viia sisse muudatused KarS-is ja haruseadustes eesmärgiga korrastada kuritegude ja väärtegude omavahelist suhet nii KarS-i ja konkreetse haruseaduse vahekorras kui ka KarS-i enda ja haruseaduse piires.[154] Seaduse oluline eesmärk oli laiendada haldussunni – ettekirjutuse, sunniraha ja asendustäitmise rakendusala ning vähendada väärteokoosseisude hulka, kõrvaldada seega ülekriminaliseerimine. Paragrahvi 157[1] uus redaktsioon nägi ette kolm koosseisutegu, mis puudutavad delikaatseid isikuandmeid tingimusel, et need said ebaseaduslikult teatavaks. Andmete töötlemise korra rikkumine on väärtegu IKS § 42 järgi.[155]

KarS § 157[1] reguleerib delikaatsete isikuandmete ebaseaduslikku avaldamist või juurdepääsu võimaldamist. Ebaseaduslikud on andmed, mille avaldamine on vastuolus kehtivate nõuetega, eelkõige vajalike turvameetmete kasutusele võtmata jätmises või andmete saamiseks ei olnud õigustatud isik.[156] Delikaatsete isikuandmete ebaseadusliku avaldamise või neile ebaseadusliku juurdepääsu võimaldamise eest karistatakse rahatrahviga. Seega näeb lõige 1 ette väärteo vastutuse delikaatsete isikuandmete ebaseadusliku avaldamise eest. Sama teo eest, kui see on toime pandud omakasu eesmärgil või kui sellega on tekitatud teisele isikul kahju, karistatakse rahalise karistusega või kuni üheaastase vangistusega[157]. Lõige 2 näeb ette ka

[153] RKKKo 3-1-1-81-08. , p 14.4.
[154] Karistusseadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse seletuskiri, 16.07.2013.
[155] *Ibid*, lk 38.
[156] A. Nõmper. KarS § 157 / 3.4.
[157] KarS § 157[1] lg 2.

kriminaalvastutuse, kui sellega on tekitatud teisele isikule kahju. Kui § 157 ja § 157[1] lg 2 eeldavad tahtlust (vähemalt kaudset) süüteokoosseisu suhtes, siis § 157[1] lg 2 puhul võib isik teo toime panna ka ettevaatamatusest. Seega kohaldatakse Kars § 157 ja § 157[1] lg 1 sarnaselt IKS § 42 isikuandmete töötlemise (muude) nõuete rikkumisel väärteo korras.

J. Salla on märkinud, et hinnates karistuste süsteemi Eestis tervikuna, paistab kriminaalkaristuse puhul silma rahalise karistuse harv kasutamine füüsiliste isikute karistuspraktikas, samas väärteokaristuste puhul domineerib rahatrahv teiste karistuste kõrval selgelt.[158]

2.2. Vastutus andmekaitsealaste rikkumiste eest – praktiline rakendamine Eestis

Tänapäeval muutub isikuandmete kogumine ja töötlemine järjest laiaulatuslikumaks ning sellega seoses väheneb andmesubjekti võimalus kontrollida oma andmete käitlemise üle. Kuna info- ja kommunikatsioonitehnoloogia võimaldavad isikuandmeid massiliselt koguda ja töödelda, kujutab seesugune tegevus ohtu üksikisiku eraelu puutumatusele ning üldisele isiksusõigusele: erinevaid andmeid kombineerides on võimalik luua võrdlemisi terviklik pilt isiku omadustest, harjumustest, suhetest, varalisest seisust jms ning seeläbi kaudselt inimest n-ö jälgida.[159]

AKI kaitseb isikute õigust saada teavet asutuste tegevuse kohta, õigust era- ja pereelu puutumatusele isikuandmete kasutamisel ning õigust pääseda enda kohta kogutud andmete juurde.[160] AKI võtab iga-aastase seire käigus vaatluse alla ühekorraga kümneid ja sadu objekte. Seire viiakse enamasti läbi kirjavahetuse või veebivaatluse teel. Isikuandmete töötlemine tervishoiu- ja sotsiaalsektoris on Andmekaitse Inspektsiooni jaoks kõrgendatud tähelepanu all. Näiteks Terviseameti poolt väljastatava tervishoiuteenuse osutajatele vajaliku tegevusloa taotlemiseks on vajalik delikaatsete isikuandmete töötlemise registreering AKI-s[161].

2014. aasta seire käigus avastati tervishoiusektoris kaks rikkumist. Väärteomenetlused puudutasid kahte arsti, kes vaatasid õigusliku aluseta isikuandmeid e-tervise infosüsteemis.

[158] J. Salla. Karistuse asendamist ja karistusest vabastamist puudutavad muudatused. - Juridica 2014 / 8, lk 593
[159] T. Ilus. Juridica 2005 / 8, lk 522.
[160] AKI. Avaliku teabe seaduse ja Isikuandmete kaitse seaduse täitmisest aastal 2015. Soovitused aastaks 2016. Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/AASTARAAMAT.pdf (05.03.2018).
[161] IKS § 27-29.

Kumbagi arsti karistati kiirmenetluse korras trahviga.[162] 2015. aastal alustas AKI neli väärteomenetlust andmetes uudishimutsenute kohta. Nendest ühes juhtumis oli andmesubjektiks TÜ Kliinikumis ravil olnud E. Savisaar, kelle haigusloo avasid kolm Tartu ülikoolil kliinikumi töötajat.[163] Kaks neist pääsesid noomitusega ja üks vallandati. AKI avalike suhete nõuniku Maire Iro sõnul on terviseandmete vaatamine väärtegu ka siis, kui päringuid tehti paljast uudishimust, ilma saadud andmeid edasi andmata või andmete vaatamisest kasu saamata.[164]

IKS § 26 lg-st 3 tulenevalt on tööandjal seaduslik kohustus tagada isikuandmeid töötlevate isikute väljaõpe isikuandmete kaitse alal. 2016. aastal lõpetas AKI seitse digiloo väärkasutamisega seotud väärteomenetlust. Kõigi nende menetluste raames said tervishoiutöötajad karistatud rahatrahviga. Näiteks Belgia isikuandmete kaitset reguleerivas seaduses on sätestatud, et terviseandmeid kogutakse otse andmesubjektilt; sellest reeglist kõrvalekaldumine on lubatud vaid erandjuhtudel (nt kui isik ei ole võimeline ise oma andmeid avaldama).[165] Erireegel on haiglas viibiva andmesubjekti andmete osas, mis on lubatud lähedastele.

2015. aastal alustas AKI 24 väärteomenetlust, neist 14 korral määrati trahvi. Kõikidel juhtudel oli tegemist isikuandmete kaitse seaduse rikkumisega. Suurim määratud trahvisumma oli 160 eurot, väikseim 16 eurot. Kui kohaliku omavalitsuste veebilehtede seire käigus tuvastatud rikkumiste osa viidi läbi 7 väärteomenetlust, mille rikkumiste sisuks oli delikaatsete isikuandmete juurdepääsu võimaldamine, siis tervise ja politsei infosüsteemis oli rikkumised teised. Kolmest väärteomenetlusest, mis olid läbi viidud meditsiinitöötajate suhtes, vaatasid kõik ilma õigusliku aluseta isikute terviseandmeid tervisesüsteemis. Jahmatamapanev on info, et üks meditsiinitöötaja tegi tervise infosüsteemis 258 õigusliku aluseta päringut. Trahvimäärad olid vastavalt 64, 80 ja 160 eurot. Viis väärteomenetlust alustati 2015. aastal jällegi politsei infosüsteemi POLIS. Huvitav on ka üks väärteomenetlus, mis alustati politsei pressiesindaja

[162] AKI. Avaliku teabe seaduse ja Isikuandmete kaitse seaduse täitmisest aastal 2014. Soovitused aastaks 2015. Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/aastaraamat%202014.pdf (18.01.2018)).
[163] Tartu ülikooli kliinikumis vallandati Savisaare haiguslugu vaadanud töötaja. – Eesti Päevaleht. 09.11.2016. Arvutivõrgus: http://epl.delfi.ee/news/eesti/tartu-ulikooli-kliinikumis-vallandati-savisaare-haiguslugu-vaadanud-tootaja?id=76199069 (18.01.2018)).
[164] Kliinikum vallandas Edgar Savisaare haiguslugu vaadanud töötaja. – Postimees. 09.11.2016. Arvutivõrgus: https://tervis.postimees.ee/3904237/kliinikum-vallandas-edgar-savisaare-haiguslugu-vaadanud-tootaja (08.01.2018).
[165] Art 7 § 5, Law of Detcember 8, 1992 on Privacy Protection in relation to the Processing of Personal Data. , Law of Detcember 8, 1992, Art 7 § 5.

suhtes, kes ei saanud aru, et avaldas delikaatset infot isiku kohta. Politsei pressiesindaja arvates on suitsiid „täiesti tavapärane nähtus, millel ei ole inimese psüühikaga absoluutselt mitte mingit seost".[166] AKI poolt tehtu ülevaatest selgub, et 10 aasta kohta on 13 juhtumit, kus isikuandmete kaitse nõudeid rikkumides on kommentaare andnud kas politsei, prokuratuur või Justiitsministeerium ning millest kahes on avaldatud isiku täisnimi (võimaldades seega lihtsat juurdepääsu sellele teabele ka internetis läbi otsingumootorite ja veebiportaalide).

2016. aastal tegi AKI kaks vaideotsust isikuandmete kaitse asjades. Esimesel juhul jäeti vaie rahuldamata tuginedes KorS-i sätetele. Vaide esitaja soovis AS SL Õhtuleht poolt väljaantava Õhtulehe veebiväljaandes artiklites tema isikuandmeid sisaldava artiklite avaldamise lõpetamist. KorS §-st 4 võib haldusorgan asuda riikliku järelevalve käigus eraõiguslike isikute vahelisi suhteid lahendama ainult kindlatel tingimustel. KorS § 4 lg 2 sätestatud tingimused ei ole alternatiivsed, vaid kõik kolm tingimust peavad olema täidetud.[167]Teine vaideotsus rahuldati osaliselt. AKI esitati kaebus isikuandmeid sisaldava teabe avalikustamise lõpetamiseks interneti leheküljel, täpsemalt kohtulahendite avaldamine Riigi Teataja leheküljel. AKI täpsustab, et IKS § 2 lg 2 kohaldatakse kriminaalmenetlusele ja kohtumenetlusele menetlusseadustikes sätestatud erisustega ning andmete kustutamist reguleerib KaRS § 28.[168]

Puudutatud isik (isik, kelle õigusi on kolmanda isiku õigusvastane tegevus rikkuda) võib aga nõuda, et järelevalveorgan otsustaks järelevalvemenetluse algatamise või järelevalvemeetme rakendamise üle kaalutlusvigadeta, kui järelevalvet sätestav õigusnorm kaitseb ka tema õigushüve. Riigikohtu halduskolleegium on leidnud,[169] et isikul puudub subjektiivne õigus nõuda järelevalvemenetluse algatamist või konkreetse meetme rakendamist kolmanda isiku suhtes, kui pädevus- ja volitusnorm näevad järelevalveorganile ette kaalutlusõiguse nii järelevalvemenetluse algatamiseks kui ka järelevalvemeetme rakendamiseks.

2016. aastal oli AKI-i menetluses mitu juhtumit, kus mobiilisideettevõtete klientide isikuandmed sattusid võõrastesse kätesse just seadmete hoolduse, remondi või asendusseadme väljastamise käigus. Järelevalve käigus tuvastati, et mobiilsideettevõtete ja nende partnerite vahelised lepingud ei käsitle isikuandmete kaitset piisvalt selgesõnaliselt. 2017. aastast on AKI-l ka kaks vaideotsust isikuandmete kaitse asjas. Esimesel juhul keelduti loa andmisest

[166] AKI. Soovitused aastaks 2016. lk 55.
[167] AKI vaideotsus nr 2.1-3/16/1343, 31.08.2016, lk 6.
[168] AKI vaideotsus nr 2.1-1/16/1044, 04.08.2016, lk 10.
[169] RKHKo 3-3-1-44-10, p 15; 3-3-1-29-13, p 17; 3-3-1-42-14, p 12.

isikuandmete töötlemisele teadusuuringus. Keelduti põhjusel, et varasemas uuringus kogutud andmeid uues uuringus ei saa töödelda andmesubjekti võimaldaval kujul.[170] Teisel juhul palus vaide esitaja AKI-l algatada järelevalvemenetlus, kontrollimaks IKS-e täitmist OÜ poolt, vajadusel rakendada haldussundi ning algatada OÜ suhtes väärteomenetlus. Inspektsioon põhjendas vaide rahuldamata jätmist tulenevalt KorS § 4 lg 2 sätestatud tingimustele.[171]

AKI poolt oli 2017. aastal tehtud 19 ettekirjutus-hoiatustest isikuandmete kaitse asjades. Ettekirjutusega kohustati füüsilisest isikust ettevõtjat esitama IKS § 28 lõikes 2 sätestatud tingimustele vastav registreerimistaotlus või teade isikuandmete kaitse eest vastutava isiku määramisest, milles peavad sisalduma vähemalt IKS § 30 lõikes 1 nimetatud andmeid. 19 ettekirjutusest 3 korral pidi AKI tegema veel täiendava hoiatuse. Määratud tähtajaks ettekirjutus-hoiatuse tähtajaks täitmata jätmise korral oli sunniraha 200 eurot. Kahel korral tehti ettekirjutus-hoiatus, mille mittetäitmisel oli sunniraha suurus 1500 eurot. Ühel juhul kohustati OÜ-d kustutama võrgulehelt isikuandmed. Teisel juhul kohustati lõpetama e-posti aadressi kasutamine otseturunduspakkumiste saatmise eesmärgil ning lõpetama isikute kontaktandmete töötlemine otseturunduslikul eesmärgil.[172]

AKI põhiülesanneteks on ka teavitus- ja ennetustöö korraldamine. Läbiviidud seirete käigus avastatud puuduste asjus annab AKI asjaosalistele tagasisidet ja soovitusi, tõsisemate puuduste korral aga alustab järelevalve- või väärteomenetlust. 26.05.2017 viis AKI koostöös Ülemaailmse Andmekaitseasutuste Võrgustikuga GPEN (*Global Privacy Enforcement Network*) läbi seire, mille käigus seirati 21 e-ehituspoe kodulehtesid. 15 ehituspoel oli ebapiisav või üldse puuduolev privaatsuspoliitika või sellekohane teave. 20 e-ehituspoodi ei andnud piisavalt selgitusi, kuidas kasutajate andmeid hoitakse, näiteks milliseid meetmeid on kasutusele võetud isikuandmete kaitseks. 17 e-ehituspoodi ei andnud piisavalt teavet, kas ja kellele võidakse kasutajate andmeid jagada ja väljastada, kuidas toimub isikuandmete edastamisel kullerfirmale. Probleeme oli ka andmete kustutamisega - 15 e-poodi ei suutnud anda selgitust, kuidas kasutaja saaks endaga seotud andmeid ära kustutada e-ehituspoest.[173]

[170] AKI vaideotsus nr 2.1-3/17/1634, 12.09.2017, lk 4.
[171] AKI vaideotsus nr 2.1-3/17/965, 08.05.2017, lk 4.
[172] AKI. Avaliku teabe seaduse ja Isikuandmete kaitse seaduse täitmisest 2016 aastal. Soovitused aastaks 2017. Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/aastaraamat_2016.pdf (5.03.2018)).
[173] AKI. Interneti rehitsemise seire 2017 (GPEN Sweep), 18.09.2017. Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/interneti_rehitsemise_seire_2017_gpen_sweep.pdf (05.03.2018).

AKI vaneminspektori H.-A. Lettensi sõnul on ikka veel e-kauplejate seas üsna levinud, et ostu sooritamisel küsitakse ülemääraselt palju isikuandmeid.[174] Isikuandmete töötlemisel peab lähtuma minimaalsuse põhimõttest – isikuandmeid võib koguda vaid ulatuses, mis on vajalik määratletud eesmärkide saavutamiseks. Sellistel juhtudel on AKI teinud ettekirjutuse ettevõtetele ülemääraselt kogutud isikuandmete kustutamiseks.

Eelpool välja toodud AKI poolt avastatud rikkumist arv on üsna suur, vaatamata AKI poolt korraldatavatele nõustamistele ja juhendamistele. Läbiviidud seirete eesmärk on eelkõige isikuandmete töötlemisel esinevate rikkumistele tähelepanu pöörata ja teavitada. Ka määratavad trahvid ei ole eriti motiveerivad rikkumiste kõrvaldamiseks või edaspidisest rikkumisest hoiduma.

2.3. Väärteo- ja karistusõigusliku vastutuse praktilised näted Eestis

Andmekaitsega seotud rikkumistest saab välja tuua senise IKS-i alusel registreeritud väärtegude arvu ning AKI sunnivahendi rakendamise praktika. 2015. aastal saabus AKI-le kokku 446 kaebust, vaiet või väärteoteadet. IKS § 42 alusel registreeriti 16 väärtegu, mis seisnesid isikuandmete töötlemise nõuete rikkumises. 15 rikkumise puhul määrati karistusena trahv või rakendati sunniraha.[175] Kuna väärteomenetlused, ei ole avalikud, puudub autoril võimalus analüüsida IKS § 42 rakendamist.

IKS § 21 lg 1 kohaselt on andmesubjektil õigus oma isikuandmete töötlejalt nõuda ebaõigete isikuandmete parandamist. Kohtuasjas nr 3-3-1-46-10 esitas vahistatu Tallinna Vangla direktorile kaebuse tema kohta Riikliku kinnipeetavate, arestialuste ja vahistatute registrisse (kinnipeeturegister) tehtud kannete peale. Kolleegium oli seisukohal, et IKS § 21 lg 2 p 3 välistab sõnaselgelt andmesubjekti õiguse nõuda tema kohta kogutud isikuandmete kustutamist või sulgemist, kui andmed on kogutud seaduse alusel. Kuna kinnipeeturegistrisse kogutud andmed on kogutud seaduse alusel (VangS § 5^1 koostoimes põhimäärusega), ei ole kinnipeetaval õigust nõuda tema kohta kogutud isikuandmete kustutamist või sulgemist. Kinnipeeturegistris olevad andmed on ette nähtud ainult ametialaseks kasutamiseks ning neid

[174] AKI, soovitused aastaks 2017, lk 32.
[175] AKI peadirektori seisukohad uue andmekaitseõiguse kontseptsiooni asjus (koostatud Justiitsministeeriumis 27.04.2017). Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/jum_oigusraamistiku_kontseptsiooni_markused.pdf (08.01.2018).

väljastatakse vaid andmekogu põhimääruses sätestatud isikutele (VangS § 5^1 lg 2). Kuna andmete parandamise nõudmine eeldab, et kinnipeetaval oleks juurdepääs tema kohta tehtud kandele, ei saa ta nõuda nende andmete parandamist, mis pole talle saanud õiguspäraselt teatavaks.[176]

IKS osas on halduskolleegium öelnud: "/.../tulenevalt IKS § 4 lg 2 p-st 8 ei loeta andmeid süüteo toimepanemise kohta pärast avalikku kohtuistungit küll enam delikaatseteks, kuid see ei tähenda, et tegemist ei oleks üldse isikuandmetega/.../"[177]. Isik esitas kaebuse, milles palus tunnistada õigusvastaseks tema kohta süüdistavate hinnangute andmine. Antud juhul oli tegemist oli Justiitsministeeriumi ajalehes Vangla Ekspress avaldatud sama ministeeriumi ametniku artikliga. Vaidlustatud artiklites on kaebaja identifitseeritud nimeliselt, neis kajastati kaebaja suhteid vangla juhtkonna ja kaaskinnipeetavatega, samuti tsiteeriti kaebaja peetud telefonikõnede salvestusi ning päevikut. Riigikohus selgitas, et ehkki artiklid avaldati Justiitsministeeriumi haldusala, täpsemalt vanglasüsteemi sisekommunikatsiooni raames, sai sellega suur hulk ametnikke juurdepääsu andmetele. Kolleegium oli seisukohal, et artiklites avaldati kaebaja isikuandmeid.[178] Samuti on kolleegium märkinud, et ainuüksi sellest, et andmed on isiku nõusolekul või seaduse alusel ilma tema nõusolekuta varem mingis vormis avalikustatud, ei saa järeldada, et täiendaval avalikustamisel ei pruugi andmesubjekti jaoks olla olulisi tagajärgi. Andmete esialgne ja korduv avalikustamine võivad toimuda väga erinevas vormis ja väga erineva intensiivsusega, sõltuvalt andmete edastaja isikust, infokanalist, kontekstist, auditooriumist jne.[179] "Mis puutub isiku enda poolt või tema nõusolekul avalikustatud andmetesse, siis tuleb arvestada, et andmesubjekt ei pruugi oma kunagise otsustuse tegemise hetkel olla ette näinud kõiki korduva avalikustamise viise ja nende tagajärgi oma õigustele"[180]. Ebaõigete andmete ümberlükkamist saab nõuda RVastS § 11 lg 1 järgi. Ka Euroopa Inimõiguste Kohus on mitmel korral rõhutanud, et andmete kajastamine kohtumenetluses ei anna blankovolitust andmete avaldamiseks meedias.[181]

Nii Riigikohtu kriminaal- kui ka halduskolleegium on varem asunud seisukohale, et IKS § 4 lg 1 tähenduses on isikuandmetena käsitatavad ka kriminaalmenetluses kogutavad andmed isiku

[176] RKHKRKHKo 3-3-1-46-10, p 16.
[177] RKHKo, 3-3-1-3-12, p 19.
[178] RKHKo, 3-3-1-3-12*Ibid,* p 19.
[179] RKHKo, 3-3-1-3-12, p 24.
[180] *Ibid*, p 25.
[181] EIKo, 17.01.2012, 33497/07, *Krone Verlag jt/ vs* Austria*;*, p 49*;* EIKo, 10.02.2009, 3514/02, *Eerikäinen jt/ vs* Soome p 63.

käitumise kohta teatud ajal ja kohas, samuti andmed tema suhete kohta kolmandate isikutega.[182] Andmete avaldamine asja avalikul arutamisel kriminaalmenetluse seadustiku kohaselt kujutab endast andmete avalikustamist seaduse alusel IKS § 11 lg 1 mõttes. [183] IKS § 11 lg 1 piirab teiste sama seaduse sätete kohaldamist, kuid ei ole ise seaduslik alus andmete töötlemiseks ning IKS § 11 lg-st 1 ei tulene, et juba avalikustatud isikuandmete uueks töötlemiseks ei pea olema seaduslikku alust.[184] Kui isikuandmed on seaduse alusel ilma andmesubjekti nõusolekuta varem mingis vormis avalikustatud (nt andmete avaldamine asja avalikul arutamisel kriminaalmenetluse seadustiku kohaselt), siis ei tähenda see, et edaspidi võib neid isikuandmeid piiramatult ja korduvalt avalikustada. Selline võimalus oleks vastuolus andmetöötluse eesmärgikohasuse, minimaalsuse ja kasutuse piiramise põhimõttega vastavalt IKS § 6 p-d 2-4. Kohtuistungil avaldatud andmete uus avaldamine trükiväljaannetes, televisioonis jm avardab oluliselt teavitatavate isikute ringi ja sellel võivad olla andmesubjekti jaoks olulised tagajärjed.[185]

Kolleegium on selgitanud, et IKS § 11 lg-s 2 sätestatud erand on rakendatav vaid juhul, kui koos esinevad kõik viidatud sättes nimetatud kolm tingimust: avalikustamiseks on ülekaalukas avalik huvi, see on kooskõlas ajakirjanduseetika põhimõtetega ning andmesubjekti ei kahjustata ülemäära. Sama põhimõtet on tsiviilkolleegium kinnitanud 2014 aastal.[186] Oktoobris 2017 rahuldas Riigikohtu tsiviilkolleegium hagi andmeid kõrvaldama kohustamiseks ja mittevaralise kahju hüvitamiseks. [187] Mittevaralise kahju välja mõistetava hüvitise suuruse osas on kolleegium selgitanud oma varasemas lahendis[188]. Kõnealuses lahendis on kolleegium märkinud lisaks juhtumite kohta, kus isiku õigusi rikutakse eraeluliste andmete õigusvastase avaldamisega, et kahjuhüvitamise suuruse kindlaksmääramisel tuleb sel juhul arvestada esmalt rikkumise ulatust (nt seda, kas artikkel avaldati üksnes paberväljaandes või lisaks ka Internetis, kus see jõuab eelduslikult oluliselt suurema hulga lugejateni kui paberväljaandes), samuti muid pressideliktide eripärasid (nt vajadust kaitsta isikuid nende elu sundkommertsialiseerimise eest).

[182] Riigikohtu 3. novembri 2016.a määrus haldusasjas nr 3-3-1-158-16, p7; 20. november 2004. a määrus kriminaalasjas nr 3-1-1-116-14, p18) RKHko, 3-3-1-158-16, p 7.
[183] RKTKo, 3-2-1-159-14, p 14.
[184] RKHKo, 3-3-1-3-12, p 22.
[185] RKTKo, 3-2-1-159-14. , p 15.
[186] *Ibid*, p15.
[187] RKTKo 2-15-16007, p 18.
[188] RKTKo 3-2-1-18-13, p 27.

Saksamaal näitel on Bundesdatenschutzgesetzis (BDSG) hüvitise nõue sätestatud §-s 8, mille järgi peab avalik-õiguslik asutus hüvitama andmesubjektile isikuandmete automatiseeritud kogumise, töötlemise või kasutamisega tekitatud kahju ning seda olenemata süüst[189]. Eraelu puutumatuse rikkumise korral peab andmesubjektile hüvitama ka mittevaralise kahju.[190] Eeltoodud rikkumiste korral on võimalik hüvitis kuni 130 000 eurot.

Õigus sõnale hõlmab nii igat liiki salvestused kui ka kirjalikus vormis edasiantava sõna. Samuti kuulub siia õigus, et isiku kohta ei avaldatakse ebaõigeid asjaolusid.[191] Ebaõigete andmete ümberlükkamise õigus tähendab seda, et väljaanne või ringhäälinguasutus peab avaldatu ümberlükkamiseks võimaldama isikule ümberlükatava teabega võrreldava lehe- või saateruumi.[192] Andmesubjektil peab olema võimalik kindlaks teha tema isikuandmete töötlemise juhud, tutvuda tema kohta töödeldavate andmetega, nõuda valede andmete parandamist.

Eestis on kriminaalvastutus reguleeritud KarS-s. KarS § 157 reguleerib kutse- või ametitegevuse teatavaks saanud isikuandmete ebaseadusliku avaldamise eest isiku poolt, kellel on seadusest tulenev kohtustus andmeid mitte avaldada.[193] Delikaatsete isikuandmete ebaseadusliku avaldamise või neile ebaseadusliku juurdepääsu võimaldamisel karistatakse rahatrahviga. Kui sama tegu on toime pandud omakasu eesmärgil või sellega on tekitatud teisel isikule kahju, on võimalik rahatrahv või isegi vangistus.[194] KarS § 157 lg 1 dispositsioonis kirjeldatud käitumine on kooskõlas KarS § 3 lõikega 4 karistatav väärteona ning võimaldab karistada üksnes rahatrahviga. Piiratud juhtudel on ette nähtud kriminaalvastutus, mis on sätestatud KarS § 157[1].

Kolleegium on asunud seisukohale, et KarS § 157 objektiivsetest tunnustest on hõlmatud üksnes sellise kutse- või ametitegevuses teatavaks saanud teise isiku tervis, eraelu või äritegevust puudutava teabe avaldamine, mis ei ole vastava ametiseisundi ja infosüsteemile juurdepääsuõiguseta isikult kättesaadav.[195] Teabe saladuses hoidmise huvi õigustusest saab aga rääkida vaid siis, kui saladuses hoitavaid andmeid ei saa hankida muul viisil. Andmed registreeritud sõidukite ja õigusrikkumiste kohta on kättesaadavad vaid isikutele, kellel on

[189] BDSG § 8 lg 1.
[190] BDSG § 8 lg 2.
[191] RKTKo 3-2-1-145-07, p 14.
[192] RKTKo 3-2-1-17-05, p 27; 3-2-1-95-05, p 26; 3-2-1-161-05, p 14.
[193] KarS § 157.
[194] KarS § 157[1].
[195] RKKK 3-1-1-81-08, p 14.2.

kutse- või ametitegevusest tulenev juurdepääs vastavatele registritele, muuhulgas ka infosüsteemile KAIRI. Süüdistatav, töötades Põhja Politseiprefektuuri kriminaalosakonna varavastaste kuritegude talituse politseivaneminspektorina omas juurdepääsuõigust politsei arvutivõrgule ja andmekogudele. Isikute eraelu puudutava teabe avaldamisega on rikutud seadusest tulenevat kohustust hoida saladuses teise isiku eraelu puudutavat teavet. K. Lõhmus-Ein on selgitanud: "/…/Konfidentsiaalse info puhul on oluline selle info kvaliteet ja see, kas isik, kellele on info avaldatud, on info kvaliteedist teadlik. Samas tuleks eeldada, et kui isik tegutseb oma kutsetegevuse raames ja saab selle käigus informatsiooni, oskab ta hinnata erineva info kvaliteeti ja oskab eristada infot, mille avaldamine kolmandatele isikutele ei ole lubatud/…/"[196].

KarS § 157 järgi rikkumise tuvastas ka Tallinna Ringkonnakohus kohtuasjas 1-11-2627[197]. Süüdistatav, töötades politseinikuna, omas õigust saada ametialaseks kasutamiseks tööks vajalikku informatsiooni ja ta vastutas selle saladuses hoidmise eest, seega rikkus infosüsteemi KAIRI pidamise korda. Riigikohus on täpsustanud, et eraelu kaitse üheks oluliseks valdkonnaks on isikuandmete kaitse ning eraelu puutumatuse riivena käsitatakse muu hulgas isikuandmete kogumist, säilitamist, kasutamist ja avalikustamist.

Politseiinfosüsteemi KAIRI kasutamise rikkumine tuvastas kriminaalkolleegium ka 2013.a kriminaalasjas.[198] IKS § 26 kohta märkis kriminaalkolleegium, et viidatud sättest ei tulene, et see kohustus laieneb vaid delikaatsetele isikuandmetele. Kohus tuvastas, et juurdepääs KAIRI andmebaasile on süüdistataval tema ametiülesannetest tulenevalt. Töötades politseijuhtivinspektorina, s.o isikuna, kes oli isikuandmete töötleja IKS §-de 5 ja 7 mõttes ning kellel lasus vastavalt IKS §-le 26 kohtustus hoida talle tööülesannete täitmisel teatavaks saanud isikuandmeid saladuses, avaldas ta teistele isikutele eraelu ning äritegevusega seonduvaid andmeid. Tulenevalt KarS § 157 rikkus ta IKS §-s 26 sisalduvat kohustust hoida talle tööülesannete täitmisel teatavaks saanud isikuandmeid saladuses.

IKS § 4 lg 2 p 8 kohaselt on delikaatseteks isikuandmeteks ainult andmed süüteo toimepanemise või selle ohvriks langemise kohta enne avalikku kohtuistungit või õigusrikkumise asjas otsuse langetamis või asja menetluse lõpetamist. Kohtuasjas 3-1-1-41-4

[196] K. Lõhmus-Ein. Eraelu ja selle elementide õiguslik kaitse. Tartu: 2004, lk 98.
[197] Tln RKo, 1-11-2627/57, p 5.3.
[198] RKKKo 3-1-1-56-13, p 14.1.

avaldas isik ebaseaduslikult talle ametitegevuse käigus teatavaks saanud teiste isikute tervist ja eraelu puudutavat teavet. [199] Süüdistatav oli isik, kellele oli riigi poolt pandud võimuesindaja ülesanded, olles ametiisik KarS § 288 mõttes, isikuandmete töötleja IKS §-de 5 ja 7 tähenduses ning kellel lasus IKS § 26 järgi kohustus hoida talle tööülesannete täitmisel teatavaks saanud isikuandmeid saladuses. Kohtulikul arutamisel tuvastatu kohaselt edastas süüdistatav enda ametikoha elektronposti aadressilt õigustamata isikult ebaseaduslikult kirja teel politsei infosüsteemist KAIRI pärinevat kolmanda isiku eraelu puudutavat teavet. Antud kohtuasjas oli tuvastatud, et süüdistatava poolt edastatud teise isiku eraelu puudutavad andmed olid juba varasemalt avalikustatud isikuandmete seaduse alusel, s.t süüdistusakti ja kohtuotsuse avaldamise teel. Kolleegium oli seisukohal, et puudub alus väita, et süüdistatav oli teadlik süüdistuses kirjeldatud teabe varasemast avaldamisest avaliku kohtuistungi käigus. Kooskõlas kohtulikul arutamisel kindlaks tehtuga pidi ta seetõttu võimalikuks pidama, et avaldab saladuses hoitavat teavet ebaseaduslikult, ja seda ka möönma (KarS § 16 lg 4). IKS § 6 p-s 3 minimaalsus põhimõtte täpsem reguleerimine kriminaalmenetluse valdkonnas vähendaks olukordi, kus ametiisikute seadusvastase tegevuse tulemusena on õigustamata isikud saanud kolmandate isikute eraelu puudutavat teavet. Töötades Põhja politseiprefektuuri analüüsi- ja planeerimisbüroo komissarina ning kellele olid riigi poolt pandud võimuesindaja ülesanded, pidi isik täitma kohustust hoida talle tööülesannete täitmisel teatavaks saanud isikuandmeid saladuses.

KarS § 157 sätestatud kuriteo toimepanemises tunnistati isik süüdi 06.11.2013.a otsusega ja talle mõisteti karistuseks rahaline karistus. Isikut süüdistati selles, et töötades Politsei- ja Piirevalveameti Keskkriminaalpolitsei rahapesu andmebüroo (edaspidi RAAB) järelvalvetalituse peaspetsialisti ametikohal, kelle tööülesanneteks oli muuhulgas rahapesumenetleja ametijuhendist tulenevalt analüüsida talle teenistuse juhi poolt määratud kohustatud subjektide sektoritest saabunud rahapesu ja terrorismi rahastamise kahtlusega ning RSS alusel saabunud teateid, nende kvaliteeti ning teavitamise kohustuse täitmist, samuti tegeleda järelevalve käigus välja selgitatud puuduste kõrvaldamisega ning väärteo tunnuste ilmnemisel menetleda kohtuvälise menetlejana väärtegusid. Seega isikuna, kellel on riigi poolt pandud järelevalve ning võimuesindaja ülesanded ning olles ametiisik KarS § 288 mõistes, kasutades ametiseisundit, pani toime ebaseaduslikult teabe varjatud kogumise.[200]

[199] RKKrK 3-1-1-41-14, p 12.1.
[200] Harju Maakohus, 1-13-9441/5.

Vastutuse osas on EIK rõhutanud, et vabaduskaotuslikul karistusel sõnavabaduse teostamise eest on iseenesest heidutav toime. Vabaduskaotuslik karistus sõnavabaduse teostamise eest on kooskõlas EIÕK artikliga 10 ainult erandlikel asjaoludel siis, kui sõnavabaduse teostamisel on rikutud väga oluliselt teisi põhiõigusi, näiteks kui tegemist on vihakõnega või vägivallale õhutamisega.[201] Väljendusvabadus, sealhulgas ajakirjandusvabadus on omaette väärtus. Seda kaitsevad nii PS § 45 kui ka EIÕK artikkel 10. Väljendusvabadus on osa demokraatia põhimõttest. Ilma selleta oleks meil raske vastu astuda võimu omavolile või kuritarvitamisele ning teha põhistatud valikuid.[202] Ka EIK on väljendanud: "/.../oleks eriti mõeldamatu, et kohtuistungite üle ei toimu üldse mingit eelnevat või paralleelset diskussiooni, olgu siis erialaväljaannetes, üldises pressi või rahva seas. Meedia ülesanne ei ole üksnes jagada sellist informatsiooni ja mõtteid, vaid ka avalikkusel õigus neid saada/.../".[203]

Ajakirjanduslikul eesmärgil - tähendab Euroopa Inimõiguste Kohtu praktika kohaselt ideede ja informatsiooni levitamist, mis aitavad edendada debatti demokraatlikus ühiskonnas. EIK praktika kohaselt peab väljendusvabaduse piiramise järele olema rõhuv sotsiaalne vajadus. EIK on pidanud mitmetes asjades otsustama, kas ajakirjandus väljaande karistamine kriminaalmenetlusest pärineva materjali kajastamise eest on kooskõlas EIÕK artikliga 10. Otsustes on nii andmete avaldamise keelu rikkumist, kui väljendusvabaduse õigustamatut piiramist.

Ajakirjanduse soovi anda panus avalikku arutellu üldist huvi pakkuval teemal võivad vähendada ka rahalised karistused. EIK, hinnates kaebajale mõistetud karistuse raskust, leidis, et kuigi rahatrahvid olid leebed, võis neil olla jahutav mõju kaebuse esitanud äriühingule.[204] Kohtuasjas Print Zeitungsverlag GmbH vs. Austria leidis EIK, et mõistetud karistus (2000 euro suurune kompensatsioon kummalegi hagejale ja süüdimõistva kohtuotsuse avaldamine) ei ole sellise raskusastmega, mis muudaks sõnavabadusse sekkumise ebaproportsionaalseks.[205]

EIK on loetlenud ja sisustanud kriteeriumid, mida tuleb sõnavabaduse ja eraelu puutumatuse tasakaalustamisel silmas pidada. Need on: avaldatud materjali panus üldist huvi pakkuvasse debatti, puudutatud isiku tuntus ja avaldatud materjali teema, puudutatud isiku varasem

[201] EIKo, 24.09.2013, nr 43612/10, *Belpietro vs*. Itaalia, EIKo 24.09.2013p22.
[202] Heili Sepp: kaalul on sõnavabadus. – Postimees. 04.02.2017. Arvutivõrgus: https://arvamus.postimees.ee/4001067/heili-sepp-kaalul-on-sonavabadus (08.01.2018).
[203] EIKo, 29.03.2016, nr 56925/08, *Bēdat vs* Śveits, 29.03.2016p35
[204] EIKo 07.02.2012, nr 39954/08, *Axel Springer* AG vs. Saksamaa, p 109.
[205] EIKo 10.10.2013, nr 26547/07, *Print Zeitungsverlag vs. GmbH* vs Austria, p 42.

käitumine, teabe hankimise viis ja teabe tõelevastavus, avaldatud materjali sisu, vorm ja tagajärjed ning mõistetud karistuse raskus.[206]

Riigikohtu menetluses oli 2010. aastal juhtum, kus kostja kasutas õigusvastaselt hageja kujutist ja sekkus hageja eraellu. Kolleegiumi arvates on isiku kujutise kasutamine ilma tema nõusolekuta üldjuhul lubatav vaid selle isiku endaga seotud aktuaalse päevasündmuse kajastamiseks. Sellele lisandub eeldus, et isiku kujutise kasutamine on päevasündmuse kajastamiseks vajalik ning avalikkuse huvi kaalub üle isiku huvi.[207] Kujutise kasutamine ilma nõusolekuta on lubatav, kui hageja oleks pannud toime tõsise õigusrikkumise, millest teavitamine on üldsuse huvides, eelkõige selliste õigusrikkumiste avastamiseks või ärahoidmiseks tulevikus. Isiku kujutise kasutamine võib olla lubatav siis, kui kujutist muudetakse tehniliste vahenditega selliseks, mis ei võimalda isikut tuvastada. Seejuures ei tohi kolleegiumi arvates isiku tuvastamist võimaldada ka kontekst.[208] Oluline on siiski märkida, et lapse õiguste kaitse kaalub üldjuhul üle sõnavabaduse, seda isegi olukorras, kui alaealist kajastatakse seoses raske kriminaalkuriteoga (Ovchinnikov vs Venemaa).[209] Kohtuasjas Krone Verlag GmBG v Austria[210] rõhutas kohus, et lapse kui nõrgema poole seisundi eraelu kaitse on ülimuslik avaliku huvi ees tema eraelu vastu.

Saksa õiguse kohaselt, kui on kontrollimise käigus on avastatud rikkumised, siis võivad sellel olla erinevad tagajärjed. Näiteks, kui ettevõtte andmekaitsevolinik ei ole selleks ülesandeks oma isikuomadustelt sobiv või piisavalt usaldatav, võib järelevalveorgan nõuda tema väljavahetamist. Sellega ähvardatakse suhteliselt sagedasti.[211] Tehniliste-organisatoorsete puuduste puhul saab nende kõrvaldamist nõuda ja läbi suruda haldusakti ja haldustäite abil.[212] Seda menetlust rakendatakse võrdlemisi harva, sest tegu on õiguslikult üsna keeruka ja formaliseeritud haldusmenetlusega. Teatud formaal– nagu ka materiaalõiguslike andmekaitserikkumiste puhul on ette nähtud karistus kas väär- või kuriteo eest.[213] Neid meetmeid rakendatakse ka harva; üldjuhul vaid siis, kui vastutav isik keeldub oma viga

[206] E. Rohtmets. Ajakirjandusvabaduse ja eraelu puutumatuse tasakaal Euroopa Inimõiguste Kohtu praktikas. Kohtupraktika analüüs. Tartu: Riigikohtu õigusteabe osakond 2014. Arvutivõrgus: http://www.riigikohus.ee/vfs/1688/ajakirjandusvabadus_analuus_m2rts2014.pdf (08.01.2018).
[207] RKTKo 3-2-1-152-09, p 13.
[208] RKTKo 3-2-1-152-09, p 14.
[209] EIKo 16.12.2010, 24061/04, *Aleksei Ovchinnikov vs.* Venemaa, p35.
[210] EIKo19.06.2012, 27306/07, *Krone Verlag GmBG vs.* Austria, p20.
[211] Asutuse andmekaitsevoliniku tegevust reguleerivad BDSG §-d 4f ja 4g, tema vallandamist BDSG § 38 lg 5 kolmas lause.
[212] BDSG § 38 lg 5 esimene ja teine lause.
[213] BDSG §-d 43 ja 44, LDSG SH § 44.

tunnistamast. Kõige tõhusamaks meetmeks andmekaitserikkumiste kõrvaldamiseks Saksamaal tuleb pidada formaalset märgukirja – s.t. teatud andmetöötluse vormi õigusevastasuse konstateerimist.[214] Kuigi niisugusel konstateeringul puuduvad otsesed õiguslikud tagajärjed, piisab selleks, et sundida ettevõtet puudust kõrvaldama, sageli juba ähvardusest konstateering avalikustada.[215]

USA-s on suhtumine privaatsuse kaitsesse Euroopa omast märgatavalt erinev. Euroopas on andmekaitse eesmärgiks kaitsta eraisikut nii avaliku kui ka erasektori eest. USA-s aga on privaatsuse kaitse üks väheseid erandeid informatsioonivabaduse suhtes ning USA seadused püüavad üksikisikut kaitsta pigem riigipoolsete kuritarvituste eest informatsioonivabaduse piiramisel, erasektoris kehtivad isikuandmete kasutamise osas vaid teatud eriseadustega sätestatud piirangud.[216] Erinevalt Euroopast ei tulene USA konstitutsioonist otsest õigust privaatsusele.[217]

[214] BDSG § 25, § 38 lg 1 esimene lause, LDSG SH § 42.
[215] T.Weichert. Isikuandmete töötlemine eraõiguslikes suhetes ja järelevalve selle üle finantsteenuste osutajate näitel. – Juridica 2005 / 8, lk 557.
[216] T. Ilus. Juridica 2002 / 7, lk 442.
[217] F. H. Cate, lk 44.

3. VASTUTUS PÄRAST EUROOPA LIIDU ANDMEKAITSEREFORMI

3.1. Vastutus andmekaitse üldmääruse järgi

Isikuandmete kaitse üldmäärusega[218] (*edaspidi üldmäärus)* on asutatud Euroopa Andmekaitsenõukogu[219], mis on artikli 29 töörühma järglane ning oleks võimeline 25. mail 2018 täielikult toimima.[220] Andmekaitsenõukogu on nõuandev organ. Sellesse kuuluvad iga andmekaitse asutuse juhid ja Euroopa andmekaitseinspektor, või nende vastavalt määratud esindajad. Andmekaitsenõukogu aitab tagada, et üldmäärust kohaldatakse ühtselt kogu Euroopa Liidus. Organ annab välja suuniseid isikuandmete kaitse üldmääruse kesksete põhimõtete tõlgendamise kohta, sh sanktsioonide määramise suhtes.

Andmekaitsereform annab EL-ile võimaluse võtta isikuandmete kaitse valdkonnas üleilmne juhtroll, seejuures peavad kõik osalejad täitma oma kohustusi. Austria andmekaitseeksperdi Waltraud Kotschy arvates on üldmäärusega andmesubjektid paremini kaitstud, sh tugevam kaebeõigus ja oluliselt suuremad trahvide ülemmäärad.[221] Üldmäärus kehtib kõigi ettevõtete/äriühingute suhtes, kes töötlevad EL elavate andmesubjektide isikuandmeid, seejuures ei ole oluline ettevõtte asukoht. Üldäärus kohaldub nii EL territooriumil asuvatele kui ka mujal asuvatele ettevõtetele. Üldmäärust kohaldatakse ka EL andmesubjektide isikuandmete töötlemisel nende töötlejate suhtes, kelle ettevõtted ei asu EL-is, see tähendab kaupade ja teenuste pakkumist EL kodanikele. Eelkõige ettevõtted, kes ei ole EL-is asutatud, kuid kes töötlevad ELi kodanike andmeid.[222] Näitena võib tuua olukorda, kui töödeldakse isikuandmeid EL riikide kodanikele kaupade või teenuste müümisel, peab arvestama üldmääruses sätestatut. Üldmäärus kehib ka väljaspool ELi asuvate organisatsioonide kohta, kui nad koguvad või töötlevad ELis asuvaid isikuandmeid. Üldmäärus näeb ette andmekaitsenormide ühtlustamise kogu ELis. Varasemalt oli direktiivis territoriaalne kohaldatavus ebaselge ning vajas EK

[218] 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). ELT L 119, 04.05.2016.
[219] Euroopa Andmekaitsenõukogu on ELi amet. Tal on juriidilise isiku staatus ja tema ülesanne on tagada määruse järjepidev kohaldamine. Andmekaitsenõukogu koosseisu kuuluvad kõigi andmekaitseasutuste juhid ja Euroopa Andmekaitseinspektor või siis nende esindajad.
[220] European Commission, 24.1.2018. Stronger protection, new opportunities -Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018. Arvutivõrgus: https://ec.europa.eu/commission/sites/beta-political/files/data-protection-communication-com.2018.43.3_en.pdf (02.03.2018).
[221] *Ibid*, lk 3.
[222] GDPRi muudatused. Arvutivõrgus: https://www.eugdpr.org/key-changes.html (03.03.2018)

tõlgendamist. Seega, kui isikuandmete töötlemine toimub erinevates EL riikides, on pädev selle EL liikmesriigi andmekaitseasutus, kus asub peamine tegevuskoht, st juhatuse asukoht. Juhul kui ei ole EL-is juhatust, siis loetakse peamiseks tegevuskohaks seda, kus toimub tegelik juhtimistegevus töötlemise eesmärki ja vahendeid käsitlevate otsuste vastuvõtmisel.[223] Eeltoodut kinnitab ka üldmääruse põhjenduspunkt 22.[224]

EL andmekaitsereformi eesmärgiks vajadus tõhusama siseturu ja rangema isikuandmete kaitse järele. EL kohtuasjade kaudu on selgunud, et eri liikmesriikides on erinevaid tõlgendusi/käsitlusi, see on ka põhjuseks miks andmekaitsereform on vajalik. Üldmääruse eesmärgiks on andmetöötleja vastutustundlikkus, et tagada inimeste suhtes seadusliku, õiglase ja läbipaistva andmetöötlusprotsessi. Üldmäärusega muudetakse selgemaks andmete rahvusvahelise edastamise normid ning tagatakse ka väljaspool ELi liikuvate isikuandmete kaitse ja selle kaudu andmekaitse kõrge tase. Uuest õiguslikust raamistikust saavad ühesuguse kasu nii füüsilised isikud, äriühingud, haldusasutused kui ka muud organisatsioonid.

Üldmäärus sätestab teavitamiskohustuse seosese isikuandmete töötlemisnõuete rikkumistega. Dirktiivis 95/46/EÜ on ette nähtud ainult üldine teavitamiskohustus isikuandmete töötlemisest järelevalveasutusele, mis aga ei ole aidanud parandada isikuandmete kaitset. Isikuandmetega seotud rikkumisest teatamisel saab arvesse võtta rikkumise asjaolusid ja seda kas isikuandmed olid või ei olnud kaitstud asjakohaste tehnoloogiliste kaitse meetmetega.[225] Selline teavitamine on oluline ka vastutuse kontekstis, mida autor käsitleb antud peatükis. Kuna isikuandmetega seotud rikkumine, kui seda ei käsitleta õigeaegselt, võib põhjustada füüsilistele isikutele füüsilisi, varalist ja mittevaralist kahju.[226] 2018. aastal kehtima hakkava üldmääruse artikli 33 kohaselt laieneb rikkumisteadete edastamise kohustus kõikidele isikuandmete töötlejatele. Seega kui isikuandmete vastutav töötleja on tuvastanud isikuandmetega seotud rikkumise, mis tõenäoliselt kujutab endast ohtu füüsiliste isikute õigustele ja vabadustele, peab sellest teavitama pädevat järelevalveasutust. Samasugune kohustus laieneb ka volitatud töötlejale, kes peab rikkumisest teavitama vastutavat töötlejat. Rikkumisest teatamine muutub üldmääruse järgi kohustuslikuks kõigis liikmesriikides, vastav regulatsioon on üldmääruse artiklitest 33 ja

[223] Euroopa Komisjon. Mis juhtub, kui me töötleme isikuandmeid eri ELi liikmesriikides? Arvutivõrgus: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/enforcement/what-happens-if-my-company-processes-data-different-eu-member-states_et (02.03.2018).
[224] Üldmääruse pp 22.
[225] Üldmääruse pp 88.
[226] IKS eelnõu 616 SE, lk 39.

34. Sellega parandatakse kaitse taset võrreldes ELis praegu kehtiva olukorraga, kus vastavalt eraelu puutumatust ja elektroonilist sidet käsitlevale direktiivile[227] ning võrgu- ja infosüsteemide turvalisuse direktiivile[228] peavad andmetega seotud rikkumistest teatama ainult elektroonilise side teenuse osutajad, oluliste teenuste operaatorid ja digitaalse teenuse osutajad. Seega teavitasid isikuandmetega seotud rikkumistest Andmekaitse Inspektsiooni vaid elektroonilise sideteenuse osutajad. Vastavat üldmääruse artiklile 33 lg 1 peab teavitamine toimuma põhjendamatu viivituseta ja võimaluse korral 72 tunni jooksul pärast rikkumise teada saamist. Andmetöötleja peab korraldama andmetöötluse viisil, mis võimaldaks rikkumise või riski kiiresti avastada. Artikkel 33 järgi on andmetöötlejal kaalutlusõigus hinnata, millal on tegu ohuga füüsiliste isikute õigustele ja vabadustele.

Üldmääruse põhjenduspunktid 75, 76 ja 85 selgitavad, et erineva tõenäosuse ja tõsidusega ohud füüsiliste isikute õigustele ja vabadustele võivad tuleneda isikuandmete töötlemisest, mille tulemusel võib tekkida füüsiline, materiaalne või mittemateriaalne kahju. Vastavalt artiklile 34 lg 1 peab vastutav töötleja põhjendamatu viivituseta teavitama ka andmesubjekti, kui rikkumise tulemusena tekib füüsiliste isikute õigustele ja vabadustele tõenäoliselt suur oht. Üldmääruses on selgitatud, et kui kahju tekkimise otsese ohu leevendamise vajadusel eeldatakse andmesubjekti kohest teavitamist, siis vajadus rakendada asjakohaseid meetmeid isikuandmetega seonduvate rikkumiste jätkamise või samalaadsete isikuandmetega seonduvate rikkumiste ärahoidmiseks võib õigustada hilisemat teavitamist.[229] Siiski tuleb tähele panna, et tulenevalt artiklist 34 lg 4 kui vastutav andmetöötleja ei pea vajalikuks andmesubjekte informeerida, on järelevalveasutusel siiski õigus vastavalt töötlejalt vastavat teavitamist nõuda.

Trahvid on oluliseks vahendiks, mida järelevalveasutused peaksid sobival juhul kasutama. Küsimus on mitte trahvide kvalifitseerimine viimase võimalusena, vaid ka trahvide määramata jätmine, kuid teiselt poolt mitte kasutada neid viisil, mis vähendaks nende tõhusust vahendina.[230] Meetme täiendamine ei ole alati vajalik teise parandusmeetme kasutamisega. Näiteks järelevalveasutuse sekkumise tõhusus ja hoiatavus, võttes nõuetekohaselt arvesse selle konkreetse juhtumiga proportsionaalsust, võib saavutada ainult trahvi kaudu.[231] Üldmäärusega kehtestatud täitmise tagamise uue korra keskne element on trahvid, mis koos muude artiklis 58

[227] ETL L 154/31.07.2002.
[228] ETL L 105/13.04.2006.
[229] Üldmääruse pp 86.
[230] Article 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, 7.
[231] *Ibid.*

sätestatud meetmetega moodustavad tähtsa osa järelevalveasutuste käsutuses olevatest täitmise tagamise vahenditest.[232]

Üldmääruse artikkel 83 sätestab trahvi/haldustrahvi (inglise keeles *administrative fines*) määramise tingimused. Selleks, et järgida trahvide määramisel järjepidevat lähenemisviisi on andmekaitsenõukogu kokku leppinud, kuidas ühiselt mõista määruse artikli 83 lõikes 2 sätestatud hindamiskriteeriumeid, ning sellepärast nõustuvad andmekaitsenõukogu ja individuaalsed järelevalveasutused kasutama trahvide kohaldamise ja määramise suuniseid ühtse lähenemisviisina.[233]

Trahvid on võimalikud, maksimaalsed määratavad ning kehtivad ka pilveteenuse pakkujate suhtes. Trahvi määramisel tuleb igat juhtumit eraldi hinnata ja võtta arvesse mitmeid tegureid: rikkumise raskusastet ja kestust, mõjutatud andmesubjektide arvu ja neile tekitatud kahju suurust, rikkumise tahtlust, kõiki kahjude leevendamiseks kasutusele võetud meetmeid, samuti koostööd järelevalveasutusega. Määruses on kehtestatud kaks ülemmääraga trahvi, neist üks, 10 miljonit või 2% ettevõtte kogukäibest võib määrata ka juhul, kui vastutav töötleja ei teosta mõjuhinnangut. Üldmääruse kohaselt võib trahvi asemel teha noomituse, mis tähendab võimalust, mida saab kasutada peale juhtumi kõikide asjaolude konkreetset hindamist.[234] Üldmääruses ei ole konkreetsetele rikkumistele kindlat hinda määratud, vaid üksnes ülempiir, st maksimumsumma. Artikli 58 lõike 2 punktide b-j sätetes on täpsustatud, milliseid vahendeid võivad järelevalveasutused vastutava töötleja või volitatud töötleja poolse rikkumisega tegelemiseks kasutada. See tähendab, et üldmääruse rikkumist kõnealuse sättega hõlmatud juhul ei ole veel toimunud.[235] Artiklis sätestatud korraldust tuleb mõista IKS eelnõu § 62 sätestatud ettekirjutuse all.

Üldmääruse artikli 83 lõikes 2 on esitatud loetelu kriteeriumidest, mille kasutamist eeldatakse järelevalveasutuselt nii trahvi määramise vajaduse kui ka trahvi summa hindamisel. Selles ei soovitata samade kriteeriumide korduvat hindamist, vaid sellist hindamist, milles võetakse

[232] Artikli 29 alusel asutatud andmekaitse töörühm. Suunised määruse (EL) 2016/679 kohaste trahvide kohaldamise ja määramise kohta. 03.10.2017. Arvutivõrgus: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237 (18.01.2018).
[233] *Ibid*, lk 4.
[234] Üldmäärus pp 148.
[235] Artikli 29 alusel asutatud andmekaitse töörühm. Suunised määruse (EL) 2016/679 kohaste trahvide kohaldamise ja määramise kohta. 03.10.2017.

arvesse iga konkreetse juhtumi kõiki asjaolusid, nagu on ette nähtud artikliga 83.[236] Kohaldatava sanktsiooni hindamine võib tulla eraldi pärast seda, kui on hinnatud, kas mõnedes riikides on põhiseadusest tulenevate nõuete tõttu tekkinud siseriiklike menetlusnormide rikkumisi. Seepärast võib see piirata sellistes riikides järelevalveasutusejuhi välja antud otsuse eelnõus sisalduvat sisu ja üksikasjalikku teavet.[237]

Üldmääruse artikli 83 lõige 4 sätestab trahvi määramise õiguse kui on rikutud isikuandmete töötlemise järgmisi tingimusi: vastutava või volitatud töötleja kohustuse kohaldada lapse nõusoleku seoses infoühiskonna teenustega, rikutud on töötlemise tingimusi, mille käigus ei nõuta isiku tuvastamist, vastutava töötleja ja volitatud töötleja üldkohustuste rikkumine, ei ole tagatud isikuandmete turvalisust (sh andmesubjekti ja järelevalveasutuse teavitamine rikkumisest), ei ole teostatud andmekaitsealane mõjuhinnang ja eelnev konsulteerimine, andmekaitseametniku kohustuste rikkumine. Samuti sertifitseerimisasutuse ning järelevalvet teostava asutuse kohustuse rikkumised. Üldmääruse artikli 83 lõige 5 sätestab veel isikuandmete töötlemise põhimõtete, nõusoleku andmise tingimuste ning isikuandmete eriliikide töötlemise tingimuste rikkumise. Lisaks kui on rikutud teabe ja juurdepääsu isikuandmetele, õigust parandamisele ja kustutamisele ning õigust esitada vastuväiteid ja automatiseeritud töötlusel põhinevate üksikotsuste tegemisel. Üldmääruse artikli 83 lõiges 5 on isikuandmete kolmandatele riikidele ja rahvusvahelisetele organisatsioonidele edastamise tingimuse rikkumise ning järelevalveasutuse uurimisvolituste ja parandusvolituste mittejärgimise eest õigus määrata trahv. Artikli lõikes 6 on õigus määrata trahv, kui ei ole täitetud järelevalveasutuse korraldusi. Ülevaade ja võrdlus on toodud Lisa 1[238] tabelis.

Üldmääruse artikliga 83 on ette nähtud ühtlustatud lähenemisviis lõigetes 4-6 loetletud kohustuste rikkumisega tegelemiseks. Võrreldes artikli 83 lõikes 4 sätestatud rikkumised on raskusastmelt madalamad kui lõikes 5 toodud rikkumised. Samuti kui ühe konkreetse juhtumi puhul on toime pandud mitu erinevat rikkumist, siis järelevalveasutus saab kohaldada trahve, mis on tõhusad, proportsionaalsed ja heidutavad kõige raskema rikkumise seisukohast. Tõhususe, proportsionaalsuse ja heidutavuse hindamine peab iga juhtumi puhul kajastama ka

[236] *Ibid.*
[237] *Ibid.*
[238] Lisa 1, lk 8984.

valitud parandusmeetmega taotletavat eesmärki, milleks on kas uuesti tagada eeskirjade täitmine või karistada ebaseaduslikku käitumist (või mõlemad).[239]

Üldmääruse artikkel 8 sätestab tingimused, mida kohaldatakse lapse nõusolekule seoses infoühiskonna teenustega. Lapsed üldiselt ei pruugi aru saada ohtudest, tagajärgedest ja kaitsemeetmetes ning sellepärast väärivad laste isikuandmed erilist kaitset.[240] Üldmääruse artikkel 12 sätestab andmesubjekti õigused selge teave, teavitamise ja andmesubjekti õiguste teostamise korra kohta. Isikuandmete töötlemisega seotud teave peab olema kättesaadav, andmesubjekte peab teavitama vastutava töötleja identiteedist ning füüsilisi isikuid tuleb teavitada, kuidas nad saavad andmete töötlemisega seoses oma õigusi kaitsta.[241] See tähendab et, kui on avastatud artiklite 8 ja 12 rikkumine, võib järelevalveasutusel olla võimalik kohaldada neid üldmääruse artikli 83 lõikes 5 sätestatud parandusmeetmeid, mis vastavad raskeime rikkumise kategooriale (art 12).[242] Seega peavad järelevalveasutused juhtumipõhiselt kindlaks tegema ja valima parandusmeetmed, mis on asjaomase juhtumi puhul proportsionaalne.

Artikkel 29 töögrupp on märkinud, et üldmääruse artikli 83 lõikes 4 sätestatud rikkumine, mis oma laadilt kuulub kategooriasse "kuni 10 miljonit eurot või kuni 2% kogu aastakäibest", võib teatavatel tingimustel kvalifitseerida kõrgema taseme (20 miljoni euro) kategooriasse. Seda juhul kui sellisele rikkumisele on eelnenud järelevalveasutuse korralduses, mida vastutav töötleja ei järginud (artikli 83 lõige 6).[243] Üldmääruses on kahe erineva maksimaalse haldustrahvi kehtestamisel juba märgitud, et mõne määruse sätete rikkumine võib olla raskem kui muude sätete rikkumine. Kuid pädevad järelevalveasutused võivad artikli 83 lõikes 2 sätestatud üldiste kriteeriumide alusel juhtumi asjaolusid hinnates otsustada, et konkreetsel juhul on suurem või väiksem vajadus reageerida parandusmeetmega trahvi kujul. Kui trahvi valitakse ühe või mitme asjakohase parandusmeetmena, kohaldatakse üldmääruse (83 lõike 4 ja artikli 83 lõike 6) mitmeastmelist süsteemi, et määrata kindlaks maksimaalne trahv, mis võib vastavalt kõnealuse rikkumise laadile.[244] Artikli 83 lg 6 kohaldamisel peab arvesse võtma siseriiklikke menetlustoiminguid.

[239] Artikli 29 alusel asutatud andmekaitse töörühm. Suunised määruse (EL) 2016/679 kohaste trahvide kohaldamise ja määramise kohta. 03.10.2017.
[240] Üldmääruse pp 38.
[241] Üldmääruse pp 39.
[242] Artikli 29 alusel asutatud andmekaitse töörühm. Suunised määruse (EL) 2016/679 kohaste trahvide kohaldamise ja määramise kohta. 03.10.2017.
[243] *Ibid.*
[244] *Ibid.*

Halduskaristuste määramise praktika kogu Euroopa Liidus on arenev. Järelevalveasutused peaksid võtma meetmeid, et järjepidevust pidevalt parandada. Seda on võimalik saavutada korrapärase teabevahetuse kaudu või muude sündmuste kaudu, mis võimaldavad võrrelda juhtumeid kohalikul, riiklikul ja piiriülesel tasandil.[245]

Saksa BDSGs kohaldatakse üldmääruse artikli 83 lõigete 4-6 kohaste rikkumiste korral haldusõigusrikkumiste seaduse sätteid.[246] Üldmääruse artikli 83 regulatsioon on vastavalt BDSG § 41 (trahvi ja kriminaalmenetluse sätete kohaldamine) ning § 43 (trahvide eesmärk) ning artikkel 84 reguleerib § 42 sätestatud karistusõiguslikke sätteid.[247] Välja on toodud asjaolu, et kui rikutakse üldmääruse mitut sätet, siis trahvi kogusumma ei tohi ületada kõige tõsisemate rikkumiste eest määratud karistust. BDSG § 43 lõikes 1 on tahtliku või ettevaatamatu ning lõikes 2 on tahtliku või hooletuse tõttu andmekaitse rikkumise eest ette nähtud rahatrahv, § 44 on tahtliku rikkumise korral ka vanglakaristus, kui rikkumine on toime pandud isikliku kasu saamise eesmärgil.

3.2. Haldustrahvide rakendamine Eesti õiguses

Üldmääruse rakendamine Eestis tähendab, et üldmäärus on otsekohalduv ning norme ei tohi ümber kirjutada. Selline kohustus tuleneb Euroopa Ühenduse lepingu artikli 249, mille kohaselt kohaldatakse määrust üldiselt, see on tervikuna siduv ja vahetult kohaldatav kõigis liikmesriikides. Vajaduse puudumist määruseid siseriiklikku õigusesse inkorporeerida on kinnitanud ka Euroopa Kohus.[248] Õigusnormid peavad olema täielikus kooskõlas määrusega ning vastuolu korral kehtib alati määrus. Üldmääruse jõustumisel tuleb kehtetuks tunnistada kõik niisugused riigisisesed õigusaktid, mille tulemuseks võiks olla määruse vahetu õigusmõju takistamine. Isikuandmete töötlemine on palju muutunud ning isikuandmete maht on kasvanud, eelkõige vajavad kaitset füüsilised isikuid, kui andmesubjektid. Üldmäärus ei anna õigusi ja kohustusi mitte ainult liikmesriikidele, vaid sellest tulenevad vahetud õigused ja kohustused ka liikmesriikide füüsilistele ja juriidilistele isikutele.

[245] Article 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, 7.
[246] BDSG § 41, trahvi ja kriminaalmenetluse sätete kohaldamine.
[247] BDSG, §-d 41-43.
[248] Euroopa KohusEKo 28.10.2010 otsus kohtuasjas, C-367/09, *Belgisch Interventie- en Restitutiebureau v. SGS Belgium NV, Firme Derwa NV, Centraal Beheer Achmea NV*, p 32.

Advokaat Karmen Turk on toonud näite veebipõhise turunduskampaania kohta: „/…/ turustajate soov on üldjuhul teada klientide kohta võimalikult palju informatsiooni. Üldmääruse alusel peaks töötleja olema võimeline tõendama, et nii meili- kui postiaadressi üheaegne kogumine on eesmärgikohaselt vajalik ning vähim, millega eesmärgini jõuda/…/“[249]. Meeles tuleb pidada, et ka andmebaasides sisalduvad andmed, millega midagi ei tehta, on ka andmete töötlemine.

Võrreldes kehtiva IKS-iga, suurenevad oluliselt isikuandmete töötlemisega seotud rikkumiste eest määratavad karistused. Kehtiva IKS-i kohaselt saab isikuandmete töötlemise nõuete rikkumise eest karistada füüsilist isikut rahatrahviga kuni 1 200 eurot ning juriidilist isikut kuni 32 000 eurot, need on maksimummäärad, mida AKI pole praktikas rakendanud. Sunniraha määr, mida võib AKI ettekirjutuse täitmata jätmise korral rakendada vastavalt määrusele, suureneb 9 600 eurolt 30 000 euroni. Üldmäärus sätestab konkreetsed aspektid, mida järelevalveasutus peab kaaluma karistuse üle otsustamisel.[250] Üldmääruses sätestatud olulisemalt kõrgemad trahvid peaks motiveerima ettevõtteid andmekaitse reeglitest kinni pidama. Nii on ka TÜ andmekaitseõiguse lektor Mari Männiko selgitanud, et „/…/uus määrus kehtestab andmekaitse regulatsiooni rikkumise eest väga kõrged trahvimäärad, see sunnib andmetöötlejaid oma andmekaitsereeglid või nende puudumist hoolega üle vaatama vältimaks trahvimäärasid, mis võivad äritegevusele hukutavalt mõjuda/…/“[251]. Euroopas on just rahaline karistus kõige levinum juriidiliste isikute suhtes kohaldatav karistusliik.[252] Näitena võib tuua Inglismaa lähenemist, kus rahalised karistused võivad olla nii kõrged, et nende tasumise järgselt võib ohtu sattuda juriidilise isiku tegevuse jätkamine, kusjuures on selline võimalus õigusruumis täiesti aktsepteeritav tagajärg.[253] Selline suurem karistusähvardus peaks mõjutama ettevõtjaid kriitilisemalt üle vaatama isikuandmete töötlemise seaduslikud alused ning rakendama igakülgselt turvameetmeid, vältimaks võimalikku väärteovastutust. Senine praktika on näidanud, et kui pole sanktsiooni, ei järgita kohustust. Eelduslikult käituvad isikuandmete töötlejad seaduskuulekamalt kui väärtegude toimepanemise eest on oluliselt suuremad

[249] K. Turk. Andmekaitsemääruse jõustumiseelsete tegevuste TOP 10 – 4. Uudsed andmekaitse põhimõtted. 1910.2016. Arvutivõrgus: https://triniti.ee/andmekaitsemaaruse-joustumiseelsete-tegevuste-top-10-4-uudsed-andmekaitse-pohimotted/ (18.01.2018).
[250] Isikuandmete kaitse seaduse eelnõu seletuskiri. 06.11.2017, lk 58.
[251] M.Männiko. Andmekaitsereform toob hiigeltrahvid. – Äripäev. 09.05.2016. Arvutivõrgus: https://www.aripaev.ee/uudised/2016/05/04/andmekaitsereform-toob-hiigeltrahvid (18.01.2018). M.Männiko. Äripäev. 09.05.2016.
[252] C. Change. Corporate Liability in Europe. Clifford Chance LLP January 2012, p3. Arvutivõrgus: http://www.cliffordchance.com/content/dam/cliffordchance/PDFs/Corporate_Liability_in_Europe.pdf (18.01.2018).
[253] *Ibid*, p. 40.

rahatrahvid. Siiski tuleb arvestada KarS-i üldosas sätestatud põhimõtetega ning olema proportsionaalne, arvestades isiku (juriidilise/füüsilise) majanduslikku seisu.

Justiitsministeerium esitas 2016. aasta lõpus kooskõlastamiseks karistusseadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse väljatöötamiskavatsuse.[254] Eesmärgiks on muudatuste ja täienduste abil viia seadusandlik olukord vastavusse EL õigusest tulenevate nõuetega ning võimaldada Eestis kohaldada EL õigusaktides sätestatud ülemmääradega rahalisi sanktsioone. [255] Seni on EL õigusest tulenevaid kohustusi kohaldada teatud rikkumiste korral kõrgema määraga rahalisi sanktsioone Eesti õiguses üle võetud läbi sunniraha instituudi, mis aga ei pruugi olla kooskõlas EL õigusega ning võib ühtlasi tähendada vastuolu ka Eesti õigusnormidega. Nimelt, nagu autor on varasemat märkinud, ei käsitleta sunniraha Eesti õiguses karistusena, vaid tegemist on haldussunnimeetmega, mille eesmärk ei ole karistuslik. KarS muutmise eelnõus pakuti välja kaks lahendust: haldustrahvide kohaldamise võimaluse sätestamine haldusmenetluses või karistusõiguse regulatsiooni täiendamine. Hetkel on riigikogus 14.03.2018 esimese lugemise läbinud Karistusseadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu.[256] Eelnõuga täiendatakse karistusseadustiku üldosa, et täita EL õigusest tulenevaid nõudeid ja kohaldada teatud rikkumiste eest oluliselt suuremaid rahatrahvi ülemmääraga väärteokaristusi, st haldustrahvide kohaldamist väärteomenetluses.

Üldmääruse artiklis 83 lõigetes 3 ja 4 sätestatud trahve hakatakse Eestis rakendama väärteomenetluses, mis on sätestatud ka üldmääruse põhjenduspunktis 151. Üldmääruse artikli 83 lõikes 2 on välja toodud tingimused, mille järgi saab hinnata VTMS § 3^1alusel, kas antud asjaolud annavad alust väärteomenetluse alustamiseks. Seega on maksimummääras trahvide määramine Eestis üsna erandlik, kuna AKI peab iga juhtumi puhul hindama, kas

[254] Karistusseadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse (EL õiguses sätestatud haldustrahvide kohaldamine Eesti õiguses) väljatöötamiskavatsus. 01.08.2016. Arvutivõrgus: http://eelnoud.valitsus.ee/main/mount/docList/af8feea7-5e75-435b-8152-18ece419983f#ZQPx4ka5 (18.01.2018).
[255] EL õigusaktide keelekasutus ei ole kõnesolevas osas ühtne. Kuna rahatrahv ning rahaline karistus on riigisiseses õiguses konkreetsed karistusõiguslikud mõisted, kasutatakse käesolevas väljatöötamiskavatsuses EL õigusaktides sätestatud trahvide osas mõistet „rahalised sanktsioonid".
[256] Eelnõu 586 SE. Karistusseadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seadus (väärteokaristuste reform, EL-i õigusest tulenevad rahatrahvid) 586 SE. Arvutivõrgus: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/f65acfbc-2656-4fbf-97e1d96582f1fcbe/Karistusseadustiku%20muutmise%20ja%20sellega%20seonduvalt%20teiste%20seaduste%20muutmise%20seadus%20(v%C3%A4%C3%A4rteokaristuste%20reform,%20ELi%20%C3%B5igusest%20tulenevad%20rahatrahvid) (01.04.2018).

väärteomenetluse läbiviimine ning trahvi määramine on konkreetse rikkumise olemust ja iseloomu arvestades vajalik ja proportsionaalne.[257]

Hetkel kehtiva IKS alusel vastutab enamikel juhtudel ettevõte, kelle suhtes AKI kohaldab haldussundi või väärteokaristust. Autori väide tugineb AKI kodulehel avalikult kättesaadavatel ettekirjutus-hoiatustel ning vaideotsustel.[258] Haldussund on haldusjärelevalve meede, millega juhitakse tähelepanu puudujääkidele ning antakse võimalus need parandada. Väärteokaristuse määramisel lähtutakse väärteomenetluse seadustikus ettenähtud menetluskorrast ning süü määramisel on aluseks karistusseadustiku üldosas sätestatu.

Paljudes riikides, kus on võimalik juriidilise isiku karistusõiguslik vastutus, tõusetub küsimus, kas juriidilise isiku vastutuse aluseks peaks olema juriidilise isiku kui organisatsiooni vastutus või juriidilise isikuga seotud indiviidide vastutus.[259] Üldiselt on tegemist tuletatud vastutusega, mille kohaselt saab juriidiline isik olla süüteo eest vastutav ainult siis, kui esineb füüsilise isiku vastutus. Ka Riigikohus on selgitanud, et juriidilise isiku vastutuse aluseks on tuletatud vastuse põhimõte, mille kohaselt juriidiline isik kui õiguslik abstraktsioon saab tegutseda vaid füüsilise isiku kaudu.[260]

IKS eelnõu kohta on AKI peadirektor V. Peep 21.12.2017. aastal avaldanud arvamust ‚et „/…/5. peatükis[261] on toodud erinevaid süüteokoosseise, kuid puuduvad süüteokoosseisud avaliku sektoriga seonduvalt ning kui ametnik teostab päringu uudishimust, siis puudub võimalus tema vastutusele võtmiseks/…/“[262]. Olulise probleemina tõi Peep välja ka raskusi juriidilise isikute vastutusele võtmise väärteo korras. Põhjuseks, miks juriidilisele isikule väärteovastutuse kohaldamine on menetlusreeglite tõttu tihti võimatu, nimetab Peep asjaolu, et vaatamata rikkumise faktile ja juriidilise isikuga seose faktile on tegelikult raske tõendada karistusõiguslikku seost KarS 14 lg 1 alusel. V. Peebu hinnangul ei vasta haldustrahvide

[257] IKS seletuskiri, lk 47.
[258] AKI menetluspraktika. Arvutivõrgus: http://www.aki.ee/et/inspektsioon/menetluspraktika (18.01.2018)).
[259] J.Gobert. A-M.Pascal (editors). European Developments in Corporate Criminal Liability. Routledge, 2014, lk 5.
[260] RKKKo 3-1-1-66-14, p 6; RKKKo 3-1-1-131-04, p 8; RKKKo 3-1-1-22-05, p 12; RKKKo 3-1-1-30-11, p-d 15.1-15.2.
[261] IKS eelnõu 616S E, ptk 6, 12.04.18.
[262] AKI. MEMO haldustrahvidest, 29.05.2017. Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/memo-haldustrahvid.pdf (18.01.2018). AKI. Eelnõule arvamuse avaldamine, 21.12.2017. Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/eelnoule_arvamuse_avaldamine_-_uus_iks.pdf (18.01.2018)

kohaldamine väärteokaristuse kujul üldmääruse nõudele, mille kohaselt peab trahvi määramine igal üksikul juhul olema tõhus (üldmääruse artikkel 83 lg 1 ja 9).

Selle väitega ei saa autor nõustuda. Ka riigiasutus või selle ametnik ei või piiramatult isikuandmeid töödelda piiramatult. Riigi, kohaliku omavalitsuse ja avalik-õigusliku juriidilise isiku vastutuse välistamine tuleneb põhimõttest, et nad tegutsevad avalikes huvides.[263] Avalikku ülesannet täitev asutus, kogu või isik saab isikuandmeid töödelda vaid tal lasuvate kohustuste täitmiseks, samuti on isikuandmete töötlemise seaduslikkust avaliku võimu kandja poolt reguleeritud valdkonnaspetsiifilistes eriseadustes. Rikkumise korral vastutab teo toime pannud ametnik, sest tema tegevus ei saa olla riigi või laiemalt avalikkuse huvides.[264] Siiski ei ole sellise vastuse alusel välistatud riigi poolt asutatud või riigi osalusega äriühingud või sihtasutused. Ka AKI väljatoodud statistika põhjal näha, et näiteks aastal 2015 algatatud väärteomenetlused puudutasid kohalike omavalitsuste veebilehti, samuti meditsiinitöötajaid, kes vaatasid ilma õigusliku aluseta isikute terviseandmeid tervise infosüsteemis ning politsei infosüsteemi ja rahvastikuregistri väärkasutamist.[265]

Kehtiv IKS sätestab isikuandmete töötleja definitsiooni § 7, mille kohaselt on isikuandmete töötleja füüsiline või juriidiline isik, kes töötleb või kelle ülesandel töödeldakse isikuandmeid. IKS § 7 lg 4 kohaselt vastutab vastutav töötja selle eest, et volitatud töötleja täidab isikuandmete töötlemise nõudeid. Volitatud töötleja võib isikuandmete töötlemist edasi volitada üksnes vastutava töötleja kirjalikul nõusolekul.[266] Üldjuhul on isikuandmete töötlejad vastutavad töötlejad, kelle lasub ka vastutus volitatud töötleja nõuetekohase töötlemise eest. Samuti on volitatud töötleja isikuandmete töötlemisel seotud vastutava töötleja juhistega ning tema järelevalve all. Kolmas isik on juriidilisest isikust või asutusest isikuandmete töötleja, kes oma ametiülesandeid täites töötleb isikuandmeid.

Üldmääruse artikli 4 kohaselt on "vastutav töötleja" füüsiline või juriidiline isik, avaliku sektori asutus, amet või muu organ, kes määrab kindlaks isikuandmete töötlemise eesmärgid ja vahendid. Volitatud töötleja on füüsiline või juriidiline isik, avaliku sektori asutus, amet või muu organ, kes töötleb isikuandmeid vastutava töötleja nimel.[267] Lisaks on määratletud

[263] E. Elkind, J. Sootak. Juriidilise isiku vastutus: uued arengusuunad Eesti kohtupraktikas. – Juridica 2015 / 2, lk 672.
[264] *Ibid*, lk 672.
[265] AKI. Avaliku teabe seaduse ja isikuandmete kaitse seaduse täitmisest 2015 aastal.
[266] IKS § 7 lg 5.
[267] Üldmääruse art 4 p 8.

"kolmas isik", kes võivad töödelda isikuandmeid vastutava töötleja või volitatud töötleja nimel.[268] IKS eelnõu § 12 on sätestatud, et termineid eraldi IKS ei defineerita ja kohaldatakse üldmääruse artiklis 4 sätestatud termineid. IKS eelnõu § 61 on viited üldmääruses sätestatud nõuetele, sh üldmääruse artiklile 29, mille rikkumise eest on ette nähtud väärteovastutus. Artiklis 29 on sätestad, et isik, kes töötleb isikuandmeid kas vastutava või volitatud töötleja nimel, peab täitma üldmäärusest tulenevaid nõudeid.[269] Siia alla kuuluvad füüsilised isikud, kes töötlevad isikuandmeid teise isiku nimel ja isikut on võimalik karistada IKS § 62 alusel väärteo korras.

KarS § 14 lg 1 kohaselt on juriidilise isiku kriminaalvastutus võimalik juriidilise isiku organi, tema liikme, juhtivtöötaja või pädeva esindaja poolt juriidilise isiku huvides toime pandud teo eest, tegemist on omistamisnormiga. KarS § 14 lõikest 1 tulenevalt ei erine juriidilise isiku vastutuse alused väärtegude ja kuritegude puhul. Juriidilise isiku vastutuse küsimuse lahendamisel tuleb tuvastada konkreetse teo toimepannud füüsilise isiku käitumises. Seega tuleb välja selgitada, kas selle füüsilise isiku käitumine, kelle tegevust juriidilisele isikule omistatakse, esinevad menetlusalusele isikule omistatud karistatava teo tunnused selle koosseisupärase, õigusvastasuse ja süülisuse näol.[270] Juhul kui puudub üks teo tunnustest, ei ole süüteo omistamine juriidilisele isikule võimalik. Füüsilise isiku toimepandud süüteo omistamiseks juriidilisele isikule on oluline, et see oleks toime pandud juriidilise isiku huvides.[271] Kriminaalkolleegium on selgitanud, et juriidiline isik kui õiguslik fiktsioon saab tegutseda vaid füüsiliste isikute kaudu, mistõttu saab juriidilisele isikule omistada vaid inimeste tegusid.[272] Dogmaatikas valitseb seisukoht, et kuigi KarS-i üldosa sätestab juriidilise isiku vastutuse alused §-des 14 ning § 37, peaksid juriidilise isiku vastutusele laienema ka teised üldosa sätted niivõrd, kui nad ei ole vastuolus juriidilise isiku olemusega. Selle kohaselt vastutabki rikkumise korral juriidiline isik kui organisatsioon. Menetlus ei pea hõlmama organisatsiooni heaks tegutsenud füüsiliste isikute vastutust. Sellest tulenevalt võib juriidiline isik vastutada ka tegevusetusdelikti alusel.[273] Riigikohus mitmes väärteoasjas leidnud, et juhul kui väärteoprotokollist ei tulene, milline isik juriidilise isiku huvides koosseisupärase, õigusvastase ja süülise teo toime pani, siis ei ole võimalik teo omistamine juriidilisele isikule

[268] Üldmääruse art 4 p 10.
[269] IKS seletuskiri, lk 49.
[270] P. Pikamäe. KarS § 14 / 6. Vt ka RKKKo 3-1-1-100-11, p 13; RKKKo 3-1-1-66-14, p 6.
[271] P. Pikamäe. KarS § 14 / 9.1-9.3.
[272] RKKKo 3-1-1-15-14, p 9.
[273] P. Pikamäe. KarS § 14 / 2.

ning teo osas tuleb menetlus lõpetada.[274] KarS eelnõuga täiendatakse KarS § 14 lg 2 teist lauset, mille kohaselt võib ette näha ka ainult juriidilise isiku vastutuse, st juriidilise isiku süüteovastutuse.[275]

Vastupidine näide on Austraaliast, kus juriidiline isik on võimalik otse, ilma juriidilise isikuga seotud füüsilise isiku vastutust tuvastamata, süüteo eest vastutusele võtta juhul, kui juriidilise isiku puudulik organisatsiooniline korraldus viis süüteo toimepanemiseni või ka soodustas seda.[276]

Eeltoodust tulenevalt saab väita, et isikuandmete töötlemise nõuete rikkumise eest vastutab nii vastutav, kui volitatud töötleja, samuti on võimalik karistada füüsilisi isikuid, kes töötlevad isikuandmeid teise isiku nimel, näiteks uudishimust. Karistusõiguses määratud juriidilise isiku definitsioonist tulenevalt saab juriidiline isik vastutada ainult läbi füüsilise isiku tegevuse, samasugune vastutus on juriidilisel isikul isikuandmete nõuete rikkumisel. Mõlemal juhul vastutab juriidiline isik ka tegevusetusdelikti alusel, kui juriidiline isik ei rakenda piisavaid turvameetmeid isikuandmete töötlemisel.

Direktiivi 95/46/EÜ artikkel 24 sätestab liikmesriikidele kohustuse võtta vastu sobivaid meetmeid, et tagada direktiivi sätete täielik rakendamine ning sanktsioonid rikkumise puhuks, see aga on kaasa toonud erinevaid menetlusi ja trahvimäärasid. Näiteks Inglismaa ja Holland kasutavad peamiselt tsiviilõiguslikke ja haldussanktsioone, Belgia tugineb ainult kriminaalmenetlusele.[277] Hert näeb vajadust ühtlustada kriminaalõiguse sanktsioone, mida kasutatakse andmekaitses.[278]

Eesti õiguses oli mõiste "haldusõigusrikkumine" kasutusel kuni 01.09.2002, kui jõustus karistusõiguse reform, mis ühendas haldusõigusrikkumiste regulatsiooni väärteoõiguse nime all karistusõiguse süsteemi. Sellega tehti põhimõtteline õiguspoliitiline otsustus, et isikute

[274] Vt RKKKo 3-1-1-30-11, p 15.1; RKKKo 3-1-1-84-07, p 8; RKKKo 3-1-1-82-04, p 11; RKKKo 3-1-1-9-05, p 8; RKKKo 3-1-1-22-05, p 15; RKKKo 3-1-1-4-06, p 5; RKKKo 3-1-1-19-07, 8.
[275] Karistusseadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seadus (väärteokaristuste reform, EL-i õigusest tulenevad rahatrahvid) 586 SE.
[276] M. Donaldson. R. Watters. „Corporate Culture" as a Basis for the Criminal Liability of Corporations. Prepared by Allens Arthur Robinson for the United Nations Special Representative of the Secretary General on Human Rights and Business. February 2008, lk 1-2. Arvutivõrgus: http://198.170.85.29/Allens-Arthur-Robinson-Corporate-Culture-paper-for-Ruggie-Feb-2008.pdf (18.01.2018).
[277] P. D. Hert, The EU data protection reform and the (forgotten) use of criminal sanctions.
[278] *Ibid.*

karistamine toimepandud õigusrikkumiste eest on karistusõiguse osa ja ei ole osa haldusõigusest.[279] Justiitsministeerium oli seiskohal, et rahatrahvide kohaldamisel on vajalik kujundada ühtne praktika ning selle tagamiseks saab kohtuvälise menetleja juht kasutada VTMS § 10 lg-s 2^1 sätestatud võimalust anda kõrgendatud ülemmääraga rahatrahvi kohaldamiseks üldised juhised.[280] Näitena Saksamaalt, kus sellised juhised on ette nähtud haldustrahvide kohaldamiseks finantsvaldkonnas.[281]

AKI peadirektori arvates tekib vastuolu Euroopa Liidu õigusega, kui sarnaste olukordade jaoks tekitatakse üldmääruses ettenähtud instrumendi kõrvale teine, siseriiklikust õigusest tulenev instrument.[282] Tema ettepanek on „/…/ viia sunniraha üldmääruse artikkel 83 rakendamise sätetesse, selgitada eelnõu tekstis ja ettekirjutuse kattuvust ning riigiasutuse tegevusetuse peale halduskohtusse protesti esitamise sätted/…/".[283] V. Peep on ka varasemalt märkinud, et karistuse eesmärk on eelkõige süüdlase karistamine. Haldustrahvi eesmärk on eelkõige rikkumise toime pannud organisatsiooni heidutamine – välistamaks edaspidised rikkumised ning võtta ette rikkumise riske vähendavaid muudatusi.[284] Üldmääruse artiklist 83 lg 1 ja 8[285] tuleneb nõue, et rikkumise eest trahvimine oleks igal üksikul juhul tõhus, proportsionaalne ja heidutav, kuid tagaks menetlusliku kaitse.

Haldusmenetluse seaduse põhimõtted, mille hulka kuuluvad ka menetlusosaliste arvamuse ja vastuväidete ärakuulamise nõue, tagavad trahvitavale tema õiguste piisava kaitse. Haldusmenetluse vormivabadus, eesmärgipärasus ja elektroonilise asjaajamise võimaldamine tagavad oluliselt lihtsama, kiirema ja tõhusama reageerimise.[286] Riigikohtu üldkogu on väljendanud arvamust, et Eestis erineb haldusmenetlus oluliselt süüteomenetlusest.

---

[279] S. Põllumäe. Karistusõiguse revisjoni ettepanekutest tulenevad muudatused haldussunnivahendites ja haldustrahvi vms meetme võimalus. Memorandum. Justiitsministeerium: 2014, lk 3.
[280] Karistusseadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse (EL õiguses sätestatud haldustrahvide kohaldamine Eesti õiguses) väljatöötamiskavatsus, lk 18.
[281] Bundesanstalt für Finanzdienstleistungsaufsicht. Leitlinien zur Festsetzung von Geldbußen bei Verstößen gegen Vorschriften des Wertpapierhandelsgesetzes, November 2013. Arvutivõrgus: http://www.bafin.de/SharedDocs/Downloads/DE/Leitfaden/WA/dl_bussgeldleitlinien_2013.pdf?__blob=publicationFile&v=6 (18.01.2018).
[282] AKI. Eelnõule arvamuse avaldamine, 21.12.2017. Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/eelnoule_arvamuse_avaldamine_-_uus_iks.pdf (18.01.2018).
[283] *Ibid.*
[284] AKI. Isikuandmete kaitse üldmäärusee (EL) 2016/679 rakendamine, 16.10.2017.
[285] Üldmääruse art 83 lg 8 käesoleva artikli kohaste volituste kasutamise suhtes järelevalveasutuse poolt kohaldatakse kooskõlas liidu ja liikmesriigi õigusega asjakohaseid menetluslikke kaitsemeetmeid, sealhulgas tõhusat õiguskaitsevahendit ja nõuetekohast menetlust.
[286] AKI MEMO haldustrahvidest 29.05.2017.

Karistusliku iseloomuga sanktsioonide kohaldamine haldusmenetluses tähendab, et taolisele menetlusele tuleks laiendada ka kriminaalmenetluses kohalduvaid menetluspõhiõigusi.[287]

Väärteokoosseisud on üldmääruse artikli 83 lõike 4 punktides a-c, lõike 5 punktides a-e ja lõikest 6 tulenevalt. Üldmääruse artikli 83 lõigetes 3 ja 4 sätestatud trahve kohaldatakse väärteomenetluses. Artikli 83 lõike 2 kohaselt tuleb igal konkreetsel juhul trahvi määramise ja selle suuruse üle pöörata tähelepanu sama lõike punktides a-k nimetatud asjaoludele. See tähendab, et artiklis 83 lõikes 2 nimetatud asjaolud on sellised, mis võimaldavad hinnata VTMS § 3^1 alusel, kas väärteomenetluse alustamine on toimepandud väärteo asjaolusid arvesse võttes põhjendatud, vajalik ja mõistlik.

EIK on lähtunud kuriteo autonoomsest mõistest ning sisustanud selle läbi niinimetatud Engeli kriteeriumite. [288] Esimene kriteerium on rikkumise formaalne liigitus siseriiklikus õiguses, teine on rikkumise laad ning kolmas on selle karistuse laad ja raskusaste, mille asjaomane isik võib saada. Esimesest kriteeriumist tulenevalt on AKI seisukohal, et Eesti õiguskorras puuduva haldustrahvi ning väärteomenetlust ei pea kohaldama.[289] Ka suurem osa liikmesriike[290] käsitleb üldmääruse artiklis 83 nimetatud trahve haldusõiguslike trahvidena, kuigi tulenevalt üldmääruse põhjenduspunktis 151 on nimetatud Eesti ja Taani osas erand. Rikkumise laadi osas on AKI märkinud, et artiklis 83 nimetatud rikkumised on oma laadilt haldusõiguslikud rikkumised ning hõlmavad haldussundi, näitena tulenevalt art 83 lg 6 käsitleb järelevalveasutuse korralduse täitmata jätmise. Üldmääruse artikkel 84 sätestab liikmesriigi õigust lisaks haldustrahvidele kehtestada ka karistused.

EK on leidnud, et haldusmenetluses kohaldatud sanktsioonid (inglise keeles *penalty*) võib oma olemuselt olla karistuslik ning kaasa tuua *ne bis idem* põhimõtte rakendumise.[291] EIK on erinevates lahendites pidanud nii Saksa[292], Austria[293], Soome[294] kui ka Läti[295] õiguses haldusrikkumisteks tegusid teatud juhtudel vastavaks kuriteo autonoomsele mõistele

[287] RKÜKo 3-1-1-37-07, p 21.2 jj; RKÜKo 3-4-1-10-04, p 17-18.
[288] EIKo 06.06.1979, nr 5370/72, *Engel jt vs*. Holland, 08.06.1976seeria A, nr 22, punktp 82.
[289] AKI. Isikuandmete kaitse üldmääruse (EL) 2016/679 rakendamine, 16.10.2017. Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/isikuandmete_kaitse_uldmaaruse_el_2016679_rakendamine.pdf (18.01.2018).
[290] BDSG § 41.
[291] EKo 26.02.2013, C-617/10, *Aklagaren* v Hans Akerberg Fransson, C-617/10. p 50
[292] EIKo 21.02.1984, nr 8544/79, *Öztürk v* Saksamaa, p 44.
[293] EIKo 23.10.1995, nr 16841/90, *Pfarrmeier v* Austria, § 30-p 32.
[294] EIKo 23.11.2006, nr 73053/01, *Jussila v* Soome, § 29-p 39.
[295] EIKo 31.07.2007, nr 65022/01, *Zaicevs v* Läti, §p 23, § 50-55.

konventsiooni tähenduses.[296] *Ne bis in idem* rikkumisele on viidatud ka määruse põhjenduspunktis 149.

Üldmäärusest tulenevate kohustuste täitmiseks on Justiitsministeerium pooldanud karistusõiguslikku regulatsiooni. Põhjendusena on välja toodud, et haldusõigusliku lahenduse kasuks otsustamine eeldab kogu senisest haldussunni ja karistusõiguse vaheteost loobumist ning uue tervikliku regulatsiooni koostamist, samas kui karistusõiguslik regulatsioon vajab vaid kehtiva õiguse täiendamist.[297]

Nii üldmäärusest, kui ka siseriiklikust õigusest tuleneb nõue, et sanktsioonide kohaldamisel järgitakse proportsionaalsust. Arvestades ettevõtte tegeliku kandevõimega on sanktsioonide eesmärk on ettevõtet heidutada või sundida, mitte põhjustada ettevõtte maksejõuetust (pankroti). AKI peadirektor Viljar Peep seletab, et isikuandmete töötlemisel rakenduvad rangemad nõuded siis, kui isikuandmete töötlemine toob kaasa riske: „/…/näiteks andmetöötluse suur maht, tundlik sisu, inimeste automatiseeritud profileerimine, automaatotsused, suurte alade kaameravalve, isikuandmete edastamine väljapoole Euroopat/…/".[298] Nõustuda võib, et arvestades Eestis tegutsevate ettevõtete majandustegevust, võib olla kõrgete maksimummääras trahvide kohaldamine erandlik, peab siiski arvestama asjaolu, et AKI teostab järelevalvet, ka piiriülese ettevõtete rikkumistele, kelle aastakäive võib olla väga suur.

Rangete karistuste reguleerimine EL tasandil oli üks andmekaitsereformi eesmärke, sest ainult nii on võimalik kindlustada üldmäärusest tulenevate reeglite ühetaoline rakendamine EL-s. Liikmesriikidel ei ole võimalik kalduda kõrvale määruses sätestatud trahvide summadest, küll aga peab trahvide määramisel tähelepanu pöörama nendele rikkumistele, mille eest vajalik trahv määratakse.[299] Autori hinnangul peaks isikuandmete kaitse olema kõikides liikmesriikides samal tasemel, tagades seeläbi eeskirjade täitmise või rakendades tõhusaid karistusmeetmeid. Kuna mõnedes riikides on põhiseaduslikest nõuetes tulenevalt riiklikud menetlusreeglid erinevad on põhjenduspunkti 151 kohaldamine õigustatud. Siiski tuleb pädeval järelevalve asutusel trahvide ülemmäära üle otsustada iga juhtumi puhul eraldi ning trahvi

[296] Karistusseadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse (EL õiguses sätestatud haldustrahvide kohaldamine Eesti õiguses) väljatöötamiskavatsus, lk 12.
[297] *Ibid*, lk 10.
[298] V. Peep. Andmekaitse uued nõuded ehmatasid ettevõtted ära. – Äripäev. 15.01.2018. Arvutivõrgus: https://www.aripaev.ee/uudised/2018/01/15/andmekaitse-uued-nouded-ehmatasid-ettevotted-ara (03.03.2018).
[299] IKS eelnõu seletuskiri, lk 46.

määramisel isikule (kes ei ole ettevõtja) arvesse võtma üldist sissetulekutaset selles liikmesriigis ja isiku majanduslikku olukorda.

Võrdlusena võib välja tuua ka konkurentsiõiguse, kus trahvimäärad on väga kõrged. Euroopa Komisjon on märkinud, et konkurentsiõiguse rikkumise eest määratud trahvide eesmärk on rikkumist ära hoida, eelkõige karistada ja hoiatada.[300] Trahvid peavad olema tasemel, mis oleks piisavalt hoiatavad. Oluline, et trahvid ei karista mitte ainult mineviku käitumist, vaid takistab ettevõtet ka tulevikus ebaseadusliku käitumise eest.[301] Konkurentsialaste väärtegude trahvide ülemmäära on sagedasti tõstetud, just põhjendusega, et väiksemad karistused ei ole konkurentsirikkumiste puhul mõjusad.

Kõrged trahvimäärad on sätestatud ka turukuritarvituse määruses[302], mille eesmärk on võidelda turukuritarvitamise vastu finantsturgudel ning kauba- ja kaupadega seotud tuletisinstrumentide turgudel. Lisaks turukuritarvituse määrusele on turukuritarvituse korral kohaldatavaid kriminaalkaristusi käsitlevas direktiivis[303] sätestatud nõue, et kõik EL riigid peavad ühtlustama oma seadused, mis käsitlevad turukuritarvitamisega seotud kuritegusid. Sanktsioonid peavad olema karmimad, et oleks hoiatav mõju, samuti ühtlustatud kõigis liikmesriikides. Mõnede riikide ametiasutustel puudusid rakendamiseks tõhusad sanktsioonid, samas kui teistes riikides oli rikkumiste puhul ette nähtud kriminaalkaristus. Eraldi direktiiv karistuse määramise kohta on vajalik eelkõige EL ühtse poliitika tõhustamiseks, arvestades, et rikkumised on suures osas toime pandud piiriüleselt. Turu kuritarvitamise määrus on rikkumise eest ette nähtud maksimummäärad füüsilise isiku puhul 5 miljonit eurot ja juriidilisele isikule 15 miljonit eurot ning liikmesriikidel on õigus kehtestada veel karmimaid halduskaristusi. Eesmärk on tagada liikmesriikides ühine lähenemisviis ja suurendada nende hoiatavat mõju.[304]

Autor on arvamusel, et kõrgendatud rahatrahvi rakendamine andmekaitse rikkumise toimepanijate suhtes on õigustatud. Oluline on märkida isikuandmete töötlemine toimub spetsiifilises valdkonnas, kus tegeletakse isikuandmete töötlemisega ning kus töötavad eriteadmistega inimesed.

---

[300] Euroopa Komisjon, Trahvid konkurentsiõiguse rikkumise kohta. Arvutivõrgus: http://ec.europa.eu/competition/cartels/overview/factsheet_fines_et.pdf (02.02.2018).
[301] MEMO/06/256 European Commission. Competition: revised Commission Guidelines for setting fines in antitrust cases. Arvutivõrgus: http://europa.eu/rapid/press-release_MEMO-06-256_en.htm. (18.01.2018).

[302] Euroopa Parlamendi ja Nõukogu määrus (EL) nr 596/2014, 16.04.2014.
[303] Euroopa Parlamendi ja nõukogu 16. aprilli 2014. aasta direktiiv 2014/57/EL.
[304] Määruse 596/2014, pp 71.

3.3. Üldmääruse artikli 83 rakendamine Eestis

EL on viinud lõpule põhjaliku reformi Euroopa andmekaitse reguleerimise valdkonnas. Ühtlustatud andmekaitsekorra keskmes on andmekaitsenormide täitmise järjepidev tagamine. Määrusega kehtestatud täitmise tagamise uue korra keskne element on trahvid, mis koos muude artiklis 58 sätestatud meetmetega moodustavad tähtsa osa järelevalveasutuste käsituses olevatest täitmise tagamise vahenditest.

Õigusteadlased on seisukohal, et lisaks vahetule kohaldatavusele iseloomustab määruseid nende tervikuna siduvus[305], st määrused kehtivad vahetult ja kogumina kõigis liikmesriikides ning liikmesriigid ei saa jätta teatud osa määrusest kohaldamata. Üldmäärus on küll otsekohalduv, kuid selle rakendamiseks vastavad sätted Eesti õiguses puuduvad. Artikli 83 lg 9 tuleneb riigi kohustus tagada eeskirjad, mis võimaldaksid järelevalveasutusel vastavalt riigisisesele õigusele sätteid kohaldada. Seega eeldavad vahetult kohaldatavad määrused "halduskaristuse" sätestamist riigisiseses õiguses.[306] Eestis, tulenevalt teistest siseriiklikest õigusaktidest ei ole selliste karistuste kohaldamine võimalik. Siiski on liikmesriikidel väga oluline roll andmekaitse üldmääruse nõuete täpsustamisel. Oluline eesmärk on, et isikuandmete töötlemise nõudeid järgitakse ja täidetakse, mitte ei tehta seda vaid suurte trahvide hirmus. Ettevõtjad peaksid oma infosüsteemid üle vaatama ja analüüsima, kas isikuandmete töötlemine on õiguspärane. Kuna andmesubjekti õigused laienevad on oluline detailsemalt reguleerida nõuded andmesubjekti nõusolekule isikuandmete töötlemisel. Delikaatsete isikuandmete töötlemine on keelatud, kui üldmäärus ei sätesta selle jaoks eraldiseisvalt õiguslikku alust.

Juba 2007. aasta IKS eelnõus leiti, et sunniraha ülemmäära tõstmine on vajalik. Oluliseks põhjenduseks peeti asjaolu, et isikuandmeid töötlevad ka väga suured äriühingud (nt kaubandus- ja finantskorporatsioonid jt), kelle puhul näiteks suuremahuliste kliendibaasi töötlemiseks kasutatavate, kuid andmekaitse nõudeid arvestades, ebarahuldavate seadmete või tarkvara väljavahetamine võib olla vägagi kulukas, mille kõrval võiks ka senises maksimaalmääras sunniraha korduv tasumine olla kokkuvõttes odavam. Sunniraha ülemmäära tõstmine ei tähenda, et praktikas rakendatava sunniraha suurus sellega seoses hüppeliselt

[305] J. Laffranque, Euroopa Liidu õigussüsteemi ja Eesti õiguse koht selles. Tallinn: Juura 2006, lk 270.
[306] Sarnaselt on ka Saksamaal kavandatud vahetult kohaldatava MAR halduskaristuste ülevõtmist enda riigisisesesse õigusesse – vt WpHG art 39 muudatused - Deutscher Bundestag. Begründung zum Gesetsentwurf eines Ersten Gesetzes zur Novellierung von Finanzmarktvorschriften auf Grund europäischer Rechtsakt. Drucksache 19/16, lk 18 ja 74. Arvutivõrgus: http://dipbt.bundestag.de/extrakt/ba/WP18/717/71710.html, lk 15 jj.Arvutivõrgus: http://dipbt.bundestag.de/extrakt/ba/WP18/717/71710.html (02.03.2018).

tõuseks, vaid see annab AKI-le üksnes võimaluse rakendada äärmuslikel juhtudel ka sellise suurusega sunniraha, mis tõesti ka täidaks oma eesmärki ehk sunniks isikuandmete töötlejat ettekirjutust täitma. IKS eelnõus märgiti, et rahatrahvi suuruse tõstmine on sarnaselt sunniraha ülemmäära tõstmisele vajalik suurte isikuandmete töötlejate mõjutamiseks hoiduma võimalikest isikuandmete kaitse nõuete rikkumisest.[307] Rahaline karistus on üks efektiivsemaid karistusi, mida rakendatakse juriidilisele isikule, sest juriidiliste isikute tegevuse olulisemaks osaks kasumi teenimine ning rahalise karistuse tasumine on kõige tõhusam ja mõjukam meede.

AKI-le jääb ka tulevikus alles õigus anda rikkumise lõpetamiseks korraldusi/ettekirjutusi. Üldmääruse artikkel 58 lg 2 loetleb järelevalveasutusele antud volitused. Antud sätte tõlgendamisel kohaldab AKI Haldusmenetluse seadusest[308] tulenevaid reegleid art 58 lg 2 kohase ettekirjutuse tegemisel. Üldmääruse artikli 83 alusel määratud trahve saab üldmääruse kohaldamisel määrata Eesti õiguses väärteotrahvidena, seda ka juhul kui viiakse läbi nii haldus- kui ka väärteomenetlus (rikkumise lõpetamisele sundimine ning ühtlasi ka heidutavalt karistamine). Seega saab tulenevalt üldmääruse regulatsioonist AKI kohaldada nii järelevalvet koos sunnirahaga (art 55 lg 2 ja art 83 lg 6), väärteo korras karistamist (art 83 ühekordse trahvid ja art 84 väärteotrahvid) ning sunniraha koos väärteo korras karistamist (rikkumise lõpetamise korraldus ja selle eiramisel korduv sundiv trahv ning samas asjas karistav trahv). Oluline on, et kui üldmääruses on ette nähtud trahvi kohaldamine, siis AKI ei saa jätta trahvi kohaldamata.

Hetkel kehtiva IKS § 40 lg 2 sätestab, et ettekirjutuse mittetäitmisel võib AKI rakendada sunniraha. Üldmääruse artikli 83 lõike 6 kohaselt järelevalveasutuse korralduse täitmatajätmise korral määratakse trahv, mis tähendab eelkõige sunniraha asendumist trahviga. Üldmääruse art 83 lg 7 kohaselt võivad liikmesriigid määrata trahve ka liikmesriigis asutatud avaliku sektori asutusele ja organitele, tegemist on kaalutluskohaga. Siiski on Justiitsministeerium seisukohal, et Eesti kontekstis ei ole mõistlik selliseid norme rakendusseaduses kehtestada ning mõistlikum oleks muid tõhusaid meetmeid rakendada, näiteks rikkumise korral AKI-1 õigust andmete töötlemine peatada.

IKS eelnõu 6. peatükk haakub karistusseadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõuga[309]. Justiitsministeerium on esitanud IKS eelnõu kooskõlastamiseks ning see

[307] IKS eelnõu, 2008.
[308] Haldusmenetluse seadus. – RT I,2001,58,354…RT I, 28.12.2017,21.
[309] Karistusseadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seadus (väärteokaristuste reform, EL-i õigusest tulenevad rahatrahvid) 586 SE.

on Vabariigi Valitsuse poolt 12.04.2018 heaks kiidetud. 6. peatükis on sätestatud väärteokoosseisud, mis tulenevad üldmääruse artiklist 83 tulenevast kohustusest määrata trahvid üldmääruse sätete rikkumise eest. Nimetatud eelnõuga luuakse võimalus EL õiguses sätestatud haldustrahvide kohaldamiseks väärteomenetluses ning võimaldab ette näha teatud rikkumiste eest senisest oluliselt suurema rahatrahvi ülemmääraga väärteokaristusi. Väärteokoosseisud on sätestatud üldmääruse üldmääruse artikli 83 lõike 4 punktides a-c, 5 punktides a-e ja lõikest 6 tulenevalt.[310] Artikkel 83 lõige 6 alusel kohaldatakse korralduse täitmata jätmise korral trahvi sunnirahana. Seda juhul, kui tegu on jätkuva rikkumisega ning järelevalveasutus on andnud korralduse selle lõpetamiseks. Käesoleval ajal kasutab AKI rikkumiste korral sunniraha, millele on eelnenud sunniraha hoiatust sisaldav ettekirjutus.

Samuti ei ole võimalik rakendada sellist mitmeastmelist menetlust, kus sunnirahale eelneb ettekirjutus ja hoiatus, kui on vahetu oht ning see vajab kiiret sekkumist. Riigikohus on selgitanud, et sunnivahendit ei tohi rakendada karistusena. Sunniraha võib rakendada vaid ettekirjutuse täitmisele kallutamiseks.[311] Eestis valitud sunniraha süsteemi ei saa pidada EL õigusaktides sätestatud rahaliste sanktsioonide kohaldamise nõuetele vastavaks, sest sunniraha ei saa rakendada selliste rikkumiste korral, mida ei ole võimalik enam kõrvaldada.[312]

Üldmääruse artikli 83 lõike 2 kohaselt tuleb igal konkreetsel juhul trahvi määramise ja selle suuruse üle pöörata tähelepanu sama lõike punktides a-k nimetatud asjaoludele. Näiteks rikkumise laadile, raskusele, kestusele ja samuti mõjutanud andmesubjektide hulgale ja neile tekitatud kahju suurusele. Üldmääruse artikli 83 lõigetes 3 ja 4 sätestatud trahve kohaldatakse väärteomenetluses. See tähendab, et üldmääruse artiklis 83 lg 2 nimetatud asjaolud on sellised, mis võimaldavad hinnata VTMS § 3^1 alusel, kas väärteomenetluse alustamine on toimepandud väärteo asjaolusid arvesse võttes põhjendatud, vajalik ja mõistlik. Rahatrahvide kohaldamise ühtse praktika tagamiseks on kohtuvälise menetleja juhil võimalik kasutada VTMS § 10 lg-s 2^1 sätestatud võimalust anda kõrgendatud ülemmääraga rahatrahvi kohaldamiseks üldiseid juhiseid.

[310] Isikuandmete kaitse seaduse eelnõu 616 SE seletuskiri, 06.11.2017
[311] RKHK0 3-3-1-72-14, p 14, 27. vt J. Jäätma. Sunniraha kui kohustatud isiku sundimise vahend ja sunnivahend. – Juridica 2015 / 10, lk 720-722.
[312] Karistusseadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse (EL õiguses sätestatud haldustrahvide kohaldamine Eesti õiguses) väljatöötamiskavatsus.

Üldmääruse artiklis 83 sätestatud rikkumiste korral on kohaldatav halduskaristus. Artikkel 83 näeb ette ühtlustatud lähenemisviisi punktides 4-6 sõnaselgelt loetletud kohustuste rikkumisele.[313] Haldustrahvi kõrval jääb liikmesriigile võimalus kehtestada väär- ja kuriteokoosseise, seda rikkumiste kõrval, mille puhul üldmääruse artikkel 83 ei näe trahvimist ette. Määruses ei ole spetsiifilistele rikkumistele sätestatud konkreetset summat, vaid ainult ülempiir (maksimaalne summa). Sellele viitab artikli 83 lõikes 4 loetletud kohustuste rikkumiste suhteliselt madal raskusaste, võrreldes artikli 83 lõikes 5 sätestatuga. Reageerimine artikli 83 lõike 5 rikkumisele peab olema efektiivne, proportsionaalne ja hoiatav ning sõltub siiski juhtumi asjaoludest.[314]

Eesti õigussüsteem ei võimalda määrata trahve (*administrative fines)* üldmääruse sätestatud üldkorra kohaselt. Üldmääruse artiklis 83 lg 9 ja üldmääruse pp-s 151 on ära toodud Eestile oluline erisus üldmäärusest, mis puudutab haldustrahve ja nende kohaldamist. Trahvide suuruse ja määramise osas on eriavamusel A. Nõmper, kelle arvates: „/…/ üldmääruses välja toodud, et Eesti on erandlik Euroopa riik, kus tulenevalt meie teistest õigusaktidest ei ole selliste karistuste kohaldamine üldse võimalik. Seega Eestis jäävad karistused 32 000 euro piiridesse ja tegelikult ei rakendata suuremaid kui mõne tuhandelisi trahve. Seega isikuandmete töötlemise nõudeid ei tule järgida mitte trahvi hirmus, vaid selleks, et olla oma kliendi ja töötajat austav ettevõtja/…/“.[315] Põhjenduspunktis 151 on selgelt välja toodud Eesti õigussüsteemi eripära, mille kohaselt ei võimalda Eesti õigussüsteem määrata trahve üldmääruses sätestatu kohaselt. Sellest tulenevalt on märgitud, et trahve käsitlevaid eeskirju saab kohaldada selliselt, et Eestis määrab trahvi järelevalveasutus (AKI) väärteomenetluse raames, tingimusel et eeskirjade sellisel kohaldamisel nimetatud liikmesriikides on samaväärne toime nagu järelevalveasutuse määratud trahvidel.[316] Eestis paigutatakse haldustrahvid väärteoõiguse ja Taanis kriminaalõiguse alla, ülejäänud liikmesriikides on haldustrahv, st haldusõiguslik sanktsioon. Seega reguleerib andmekaitsemääruse artikkel 83 haldustrahve ning määruse põhjenduspunktist 151 tulenevalt võib rakendada haldustrahve väärteomenetluse kaudu.

[313] Article 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237 (02.03.2018)
[314] *Ibid.*
[315] A. Nõmper. Andmekaitseseadusega kaasnevad suured trahvid on müüt. – Äripäev. 10.11.2016. Arvutivõrgus: https://www.aripaev.ee/uudised/2016/11/10/andmekaitseseadusega-kaasnevad-suured-trahvid-on-muut (02.02.32018).
[316] Isikuandmete kaitse seaduse eelnõu seletuskiri, 06.11.2017.

AKI-l on kaalutlusõigus karistuse kohaldamisel, lähtuda tuleb ka Eesti eripärast. Menetlusreeglite kehtestamine jääb liikmesriigile. Üldmääruse põhjenduspunkt 151 nimetab, et haldustrahvide puudumise tõttu Eestis määrab trahvi järelevalveasutus väärteomenetluse raames. Algselt võib jääda ekslik mulje, et tekib vastuolu artikliga 83 lg 9, mille kohaselt liikmesriigis, kus haldustrahvid puuduvad, algatab trahvi pädev järelevalveasutus ning selle määravad pädevad riiklikud kohtud. Oluline on märkida, et liikmesriigid võivad artiklit kohaldada sellisel viisil, kuid ei ole kohustatud. Karistusseadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse väljatöötamiskavatsuses ning sellel põhinevas eelnõus soovitakse jätta haldustrahvid karistus-, mitte haldusõiguse raamidesse. Väljatöötamiskavatsuses[317] mööndi, et spetsiifiliste valdkondlike normide osas võib haldusorgan-järelevalveasutus olla pädevam ja kiirem hindama rikkumise mõju ja raskust kui politsei, prokuratuur ja kohus. Teisest küljest nenditakse, et haldusmenetlus ei annaks midagi juurde, sest väärteomenetluses ongi reeglina haldusorgan kohtuväline menetleja.

Kehtiv IKS võimaldab väärteo eest kohaldada rahatrahvi. Nii rahalise karistuse (KarS § 44) suurusega, kui ka rahatrahvi suurusega (KarS § 47) seonduv on reguleeritud KarS-is. Kahe trahviliigi erinevus väljendub nende arvutamises. Rahaline karistus mõistetakse päevamäärades ning karistuse lõpliku summa määrab ära süüdlase keskmine päevasissetulek. Väärtegude eest kohaldatav rahatrahv määratakse trahviühikutes ning rahatrahvi lõplik suurus saadakse trahviühikute korrutamisel seaduses üheselt kindlaks määratud rahatrahvi baassummaga.[318] Vastuolu korral KarS § 47 ja muudes seadustes sätestatud väärtegude eest ette nähtud rahatrahvi määrade vahel kohaldatakse väärteo eest rahatrahvi eelnimetatud paragrahvis sätestatud määras.[319] Riigikohus on selgitanud, et selline lahendus tuleneb asjaolust, et üld- ja eriosa sätted ei ole üld- ja erinormi vahekorras, mistõttu nende vahel vastuolu ilmnemise korral kohaldatakse üldosa sätet.[320]

EL õigusaktides sätestatud rahatrahvide kõrge ülemmäär ning samuti ülemmäära arvutamise põhimõtted ei sobitu täielikult karistusõiguse üldosas süütegude eest kohaldatavate karistuste liikide ja määradega. Kuna rahatrahvide ülemmäär ei sobi hetkel riigisisese õigusega, siis on väljatöötamisel karistusseadustiku ja sellega seonduvalt teiste seaduste muutmise seadus.

[317] Karistusseadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse (EL õiguses sätestatud haldustrahvide kohaldamine Eesti õiguses) väljatöötamiskavatsus. 01.08.2016.
[318] P. Pikamäe. KarS § 44 / 1.2.
[319] P. Pikamäe. KarS § 47 / 5.
[320] RKKKo 3-1-1-20-01, p 6.1.

Karistusseadustiku muutmine on plaanis selliselt, et tõstetakse väärteomenetluses rakendatavate trahvide piire. Ette on valmistatud eelnõu[321], millega lisatakse karistusseadustikku paragrahv kõrgendatud ülemmääraga trahvide jaoks. Karistusseadustiku üldosa täiendatakse § 47^1 võimalusega sätestada väärteo eest kõrgendatud ülemääraga rahatrahvi. Rahandusministeerium on IKS eelnõu kooskõlastamisel välja toonud, et kõrgema määraga väärteokoosseisud saavad olla eelnõus üksnes juhul, kui selleks on alus karistusseadustikus.[322] Nimetatud eelnõuga luuakse võimalus EL õiguses sätestatud haldustrahvide kohaldamiseks väärteomenetluses ning võimaldab ette nähtud teatud rikkumiste eest senisest oluliselt suurema rahatrahvi ülemmääraga väärteokaristusi.[323] Seega karistusõiguse üldosa muutmine on vajalik, et oleks võimalik EL-i õigusaktides nõutavaid karistusi karistusseadustiku eriosas ja eriseadustes sätestada ja kohaldada. Eelnõus on rõhutatud, et KarS § 47^1 lg 1 on tegemist erandliku rahatrahvi liigiga, mis sätestatakse väärteo eest põhjendatud juhul ning eeskätt siis, kui see on vajalik Eestile siduva rahvusvahelise kohustuse täitmiseks. Rahvusvahelise kohustuse mõiste ei hõlma üksnes sõlmitud välislepinguid, vaid lisaks Euroopa Liidu õiguse allikaid, mis ei ole tehniliselt Eestile siduvad lepingud, vaid lepingu alusel antud sekundaarõigus.[324]

Kuigi KarS muutmise eelnõu on hetkel Riigikogu menetluses[325], ei pruugita jõuda muudatused maikuuks vastu vtta ja jõustada. Andmekaitse üldmäärus ning hakkab kehtima alates 25. maist 2018 ning AKI on kohustatud rakendama kõrgendatud trahvimäärasid, kuigi KarS § 47^1 ei ole veel vastu võetud. Ühtlasi on küsitav, kas õigeaegselt jõutakse vastu võtta ja jõustada ka IKS[326]. Sellise võimaluse annab vahetu õigusmõju põhimõte, mis tugineb Euroopa Liidu õiguse esmasuse põhimõttele ja lubab õigusnormide kollisiooni lahendada Euroopa Liidu õigusnormi vahetu kohaldamisega konkreetses olukorras. Siin tuleb aga arvestada, et kuigi määrus on vahetult kohaldatav, ei pruugi kõigil sätetel olla vahetu õigusmõju. Vahetust õigusmõjust saame

[321] Karistusseadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seadus (väärteokaristuste reform, EL-i õigusest tulenevad rahatrahvid) 586 SE, lk 24.
[322] Rahandusministeerium, 29.12.2017. Isikuandmete kaitse seaduse eelnõu kooskõlastamine, lk 12. Arvutivõrgus: http://eelnoud.valitsus.ee/main#sK371WfU (02.02.2018).
[323] Isikuandmete kaitse seaduse eelnõu seletuskiri, 06.11.2017.
[324] Analoogiliselt selgitusi KarS § 8 kohta – Riigikogu XII koosseisu seaduseelnõu 393 SE seletuskiri, lk 5
[325] Viide Riigikogu menetlus: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/f65acfbc-2656-4fbf-97e1-d96582f1fcbe/Karistusseadustiku%20muutmise%20ja%20sellega%20seonduvalt%20teiste%20seaduste%20muutmise%20seadus%20(v%C3%A4%C3%A4rteokaristuste%20reform,%20EL-i%20%C3%B5igusest%20tulenevad%20rahatrahvid) (16.04.2018)
[326] Viide Riigikogu menetlusele: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/e14c5e2f-b684-4aa4-a7dd-ffb76f63f395/Isikuandmete%20kaitse%20seadus (18.04.2018).

rääkida juhul kui määruse normid on sõnastatud selgelt ega jäta võimudele diskretsioonivõimalust.[327]

H. Jüriöö on oma magistritöös välja toonud, et sanktsioonid, mida liikmesriigid on kohustatud määruste täitmiseks tagama on erinevad nii sanktsiooni rakendamise menetluses kui sanktsiooni suuruses, kus erisused ulatuvad miljonitesse eurodesse ning taga ühtset EL õiguse kehtestamist liikmesriikides.[328]

EL õiguse rakendamine sõltub liikmesriigi rakendusasutusest- ja meetmetest, mille rakendamine siseriiklikul tasandil on oluliseks meetodiks EL õiguse vahetu ja ühetaolise kohaldamise tagamine. Antud kohustus tuleneb ELTL artiklitest 4 ja 291. ELTL artikli 291 lg 1 sätestab, et liikmesriigid võtavad vastu kõik siseriikliku õiguse meetmed, mis on vajalikud liidu õiguslikult siduvate aktide rakendamiseks. See kohustab liikmesriikide rakendusasutusi ennekõike võtma kõik meetmed, mis on vajalikud ühenduse õiguse rakendamiseks ja täitmiseks nende jurisdiktsioonis.[329]

Siinkohal saab näite tuua Saksamaa kriminaalõigusest, kus keeldutakse tunnistamast, et juriidilist isikut on võimalik kriminaalvastutusele võtta.[330] Saksamaal on leitud, et juriidilise isiku kriminaalvastutusele võtmine on vastuolus karistusõiguses kehtiva põhimõttega, et karistus peab olema suunatud teo tegeliku toimepanija vastu. Karistuste süsteem ei ole kohaldatav organisatsiooniliste süüdistatavate suhtes ning et juriidilisel isikul puudub n-ö mõistus, mistõttu pole juriidilise isiku süü küsimus üldse võimalik. [331] Juriidiliste isikute vastutusele võtmine on Saksamaal reguleeritud üldklauslina. [332] Siiski on Saksamaa kohtud määranud juriidilistele isikutele nende kriminaalse tegevuse eest karistuseks suuri rahatrahve. Lisaks sellele, et rahatrahvid mõjuvad märkimisväärselt ettevõtte mainele, peetakse Saksamaal väärteoõiguse alusel määratud rahatrahvi vähemalt sama efektiivseks kui olukorras, kui juriidilisel isikul tuleks vastutada karistusõiguse alusel kuivõrd ka karistusõiguses on juriidilise

[327] EK otsusEKo 11.01.2001.a asjas, C-404/98, Azienda Agricola Monte Arcosu.-, p 27.
[328] H. Jüriöö. Euroopa Liidu määruste vahetu ja ühetaolise rakendamise probleemid Euroopa Parlamendi ja nõukogu määruse nr 261/2004 näitel. Tartu: 2016, lk 58-68.
[329] M. Acceto ja S. Zlepting, The Principle of Effectiveness: Rethinking Its Role in Community Law, European Public Law, 11.3 (2005), lk. 387.
[330] C. Change. Corporate Liability in Europe. Clifford Chance LLP January 2012, p. 1. Arvutivõrgus: http://www.cliffordchance.com/content/dam/cliffordchance/PDFs/Corporate_Liability_in_Europe.pdf (02.02.2018) C. Change. January 2012, p. 1.
[331] H. L. Leigh. The Criminal liability of corporations and other groups: a comparative view. Michigan Law Review, Vol 80, No 7. jun 1982, p. 1509.
[332] E. Elkind, J. Sootak. Juridica 2005 / 10, lk 673.

isiku peamiseks karistusliigiks rahatrahv. [333] Saksamaal on välistatud juriidilise isiku kriminaalvastutus, sest see ei vasta põhiseaduslikule süüpõhimõttele. Samas näeb Saksa väärteoseadustik (OWiG) juriidilistele isikutele sanktsioonina ette rahatrahvi, mis võib ulatuda ühe miljoni euroni.[334]

IKS eelnõuga muudetakse senist delikaatsete isikuandmete kategooriat, mida hakatakse nimetama isikuandmete eriliigiks. Riigikohus juhtis tähelepanu, et KarS § 157[1] näeb kehtivas õiguses ette väärteokaristuse delikaatsete isikuandmete ebaseadusliku avaldamise eest.[335] Kavandatav paragrahv näeb ette kõrgendatud ülemmääraga rahatrahve nii füüsilistele kui juriidilistele isikutele. Kõik EL-i õigusaktid ei reguleeri, kumb rahatrahvi ülemmäär tuleks karistuse mõistmisel aluseks võtta, kui väärteo eest on ette nähtud mitmel alusel arvutatava rahatrahvi ülemmäär (IKS eelnõu ptk 6, fikseeritud ülemmäär 10 000 000 eurot kui ka juriidilise isiku käibe protsendist sõltuv ülemmäär). Sellisel juhul peaks eelistama kõrgemat ülemmäära ning selline nõue on EL-i õigusaktides ka välja toodud. (nt läbipaistvusdirektiiv art 28b lg 1 p c).[336] EL-i õigusest tulenevate kohustute täitmiseks ei ole alati võimalik väärteokoosseisu sätestamist vältida. Olukorras, kus tegemist on oma iseloomult kõrvaldatava seaduse nõuete rikkumisega, on põhimõtteliselt võimalik näha ette EL-i õiguses sätestatud rahaliste sanktsioonide suurustele vastav sunniraha. Samas ei ole välistatud, et mõni olemuselt kõrvaldatav seaduse nõuete rikkumine toob kaasa piisava ohu või kahju, et vajalik on väärteokoosseisu sätestamine.

IKS eelnõu 6. peatükis nähakse ette vastutuse sätted. Eelnõu §-id 61-69 on sätestatud väärteokoosseisud viidetega üldmääruse artiklitele. IKS-is sisalduv väärtegude regulatsioon moodustab KarS suhtes eriosa. Arvestades isikute võrdse kohtlemise printsiipi ei tohi eriosa norm raskendada isiku olukorda, võrreldes üldosa normiga.[337] Seaduses peavad olema kirjeldatud süüteo tunnused. Ka KarS lähtub süüteomõistest, mille järgi on süüteokoosseis esimene tase teo karistamise tuvastamisel.[338] Esimesena esitatakse küsimus, kas tegu, mis on seotud inimese käitumisega, kuulub süüteokoosseisu. IKS eelnõus ei ole ühtegi koosseisu välja

[333] C. Change, Januar 2013. p5.
[334] Vt, H. J. Hirsch. Juriidiliste isikute kriminaalvastutusest. – Juridica 1996 / 1, lk 17–18; J. Pradel. Juriidiliste isikute kriminaal- vastutus. Tähelepanekuid Euroopa riikide seadusandluse kohta. – Juridica 1999 / 8, lk 370 jj; E. Samson. Kriminaalkaristus majandusette- võtetele. – Juridica 1999 / 8, lk366 jj.
[335] Riigikohtu arvamus isikuandmete kaitse seaduse eelnõu kohta, 20.12.2017. Arvutivõrgus: http://eelnoud.valitsus.ee/main#OgPd2TPg (02.02.2018).
[336] Karistusseadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seadus (väärteokaristuste reform, EL-i õigusest tulenevad rahatrahvid) 586 SE, lk 26.
[337] J. Sootak. KarS § 2 / 4.
[338] J. Sootak. KarS § 12 / 2.

toodud, millise isikuandmete töötlemise rikkumise korral, sh teo või tegevusetuse korral on ette nähtud trahv. Karistusõiguslikult peaksid süüteokoosseisud olema välja toodud, kuigi määrus otseselt välistab sätete seadusesse ümberkirjutamise. Samuti ei näe autor võimalust IKS eelnõus määratleda eraldi sätted füüsilise ja juriidilise isiku karistamiseks, kuna üldmääruses ei ole eraldi sellist nõuet ettenähtud. Üldmääruse artikkel 4 sätestab vastutava töötaja ja volitatud töötaja definitsiooni, kelleks võib olla füüsiline või juriidiline isik, kes vastutavad isikuandmete töötlemise nõuete rikkumise korral ning neile on võimalik kohaldada ülemmääras trahvi. Olukorras, kus füüsilisest isikust töötlejale saaks uue IKS regulatsiooni kohaselt määrata väiksema ülemmääraga trahvi, ei pruugi olla kooskõlas üldmäärusest tulenevate reeglitega.

Töö autor arvab, et riiklik andmekaitsejärelevalve on tõhus, kuna võimaldab kohaldada mõjusaid sanktsioone andmekaitsereeglite rikkumise korral, st kõrgemaid trahvimäärasid. Kuigi ka varasemalt on Eesti õigusesse üle võetud kõrgema määraga trahve, tulenevalt EL õigusest, näiteks Väärtpaberituru[339] seadus või Krediidiasutuste seadus[340], siis seda on tehtud läbi sunniraha instituudi. Käesoleval juhul selline käsitlus ei sobi, kuna sunniraha kohaldamine eeldab eelnevat ettekirjutust või hoiatust, sunniraha on ennetav meede ning ei ole käsitletav karistusena. Üldmääruses sätestatud artikli 83 lõigete 4-6 kohustuste rikkumise eest trahv. Seega on ette nähtud sanktsioon selliste isikuanmdmete töötlemise nõuete rikkumiste eest, mid ei ole võimalik ära hoida ega heastada. Siiski on autori hinnangul problemaatiline, kuidas kõrgendatud rahatrahvi määr paigutub Eesti karistusõiguslikku süsteemi. Samuti ei ole autori hinnangul IKS eelnõu vastutuse sätted kooskõlas määrusega ning võivad olla sobimatud ka Eesti karistusõiguse süsteemi nõudeid arvestades, kuivõrd kosseisukirjeldustest ei ole üheselt selge, milliste tegude suhtes on rakendatud väärteovastutus.

[339] Väärtpaberituru seadus. – RT I 2001,89,532…RT I, 30.12.2017,43.
[340] Krediidiasutuste seadus. – RT I 1999,23,348…RT I, 30.12.2017,3.

KOKKUVÕTE

Õigus privaatsusele ja eraelule on kaitstud kui inimõigus, mis on reguleeritud nii riikide põhiseaduste kui ka rahvusvaheliste konventsioonide kaudu. Arenev tehnoloogia on loonud ulatuslikult võimalusi andmete laialdaseks töötlemiseks ning andmesubjekt ei pruugi teadagi, et tema andmeid töödeldakse ja mis eesmärkidel seda tehakse. Andmesubjektil on mitmeid õigusi, mis võimaldavad tal kontrollida oma isikuandmete töötlemist, kuid vaatamata nende õiguste olemasolule sõltub andmekaitsereeglite tegelik rakendamine muuhulgas ka sellest, kas ja milliseid sunnimeetmeid saab andmesubjekt töötleja suhtes rakendada.

Käesoleva töö eesmärgiks oli uurida, millised jõustamismeetmed on Eestis kasutusel, kuidas neid praktikas kohaldatakse, hinnata nende efektiivsust ning vaadelda, kas kehtiv süsteem sobib kokku arengutega EL-is ning millisel viisil on Eestil võimalik täita EL andmekaitse üldmäärusest tulenevaid kohustusi ja kindlustada andmesubjekti õiguste tõhus jõustamine.
Autor püstitas hüpoteesi, mille kohaselt Eesti õiguses ei ole piisavalt tõhusaid meetmeid andmekaitseõiguse jõustamiseks ning olemasolev sanktsioneerimise süsteem ei täida EL õigusest tulenevaid nõudeid.

Töö esimeses peatükis selgitati välja ja analüüsiti isikuandmete kaitse põhilisi eesmärke ja olemust. Isikuandmeteks on mistahes teave tuvastatud või tuvastatava isiku kohta ning isikuandmete töötlemine on iga isikandmetega tehtav toiming, sealhulgas kogumine säilitamine, muutmine, avalikustamine, päringute teostamine, kasutamine, edastamine, kustutamine jt. Selleks, et teave kujutaks endast isikuandmeid, ei pea see olema tingimata tõene. Isikuandmete töötlemine peab olema võimalikult avatud ja läbipaistev. Andmesubjektil peab olema võimalik kontrollida enda kohta töödeldavate andmetega, sh nõuda valede andmete kustutamist või parandamist. Keegi ei või meelevaldselt sekkuda teise isiku eraellu. Õigus isikuandmete kaitsele ei tähenda andmete töötlemise keeldu, vaid nõuab andmekaitse reeglite ja põhimõtete järgimist ning kaitseb isikut ebaseadusliku töötlemise eest.

Eestis reguleerib isikuandmete kaitset isikuandmete kaitse seadus (IKS), mis sätestab ka vastutuse isikuandmete töötlemise nõuete rikkumise eest. Andmesubjekt võib oma õiguste kaitseks pöörduda riikliku järelevalveasutuse poole. Isikuandmete ebaseaduslikul avalikustamisel on andmesubjektil võimalik esitada kaebus tsiviilkohtusse. Lisaks riiklikule järelevalvele ning tsiviilvastutusele näeb Eesti õiguskord ette ka vastutuse väärteo- või kriminaalkorras. Kriminaalmenetluse algatamiseks on alust, kui delikaatseid isikuandmeid on

avaldatud ebaseaduslikult, omakasu eesmärgil või isikule kahju tekitamisega. Selliste tegude eest võib karistuseks olla rahatrahv või isegi vangistus.

Kontrolli andmekaitsenõuete täitmise üle teostab sõltumatu järelevalveasutus. Eestis on selleks järelevalveasutuseks Andmekaitse Inspektsioon (AKI), kes kohaldab haldussunnina ettekirjutuse mittetäitmisel sunniraha või viib läbi väärteomenetluse, kui esineb süüteokoosseisu tunnuseid. Sunnivahendit siiski ei rakendata riigiasutuste suhtes, mis seab kahtluse alla tõhusate jõustamismeetmete olemasolu riigiasutuste puhul. Esimese peatüki kokkuvõtteks võib öelda, et hetkel kehtivad õigusaktid, mis peavad reguleerima isikuandmete kaitset, on aegunud. 1995. aastal vastu võetud EL andmekaitse direktiiv 95/46/EÜ, mis peab reguleerima ühtselt liikmesriikides isikuandme töötlemist ja nõudeid, ei Täida tänapäeva oludes enam oma eesmärki. Kiire tehnoloogia arenguga on vaja uusi regulatsioone ning käesolev õigusloome on iganenud. Direktiivi eesmärgiks oli luua ühtne regulatsioon kõigis liikmesriikides, kuid kuna riikidele on antud suur otsusediskretsioon, käsitlevad liikmesriigid norme erinevalt ja seega ei ole direktiiv oma eesmärki saavutanud. Kinnitust eeltoodule annab ka Euroopa Kohtule saadetud eelotsuse taotlused ning kohtu tõlgendused direktiivi rakendamiseks, mis annab alust väita, et direktiivi sätted on liialt üldsõnalised. Kuna IKS võtab üle direktiivi ning suuresti lähtub direktiivi sätetest, siis on autor seisukoha, et ka Eesti andmekaitsereeglistik on lünklik.

Teises peatükis käsitles autor, millised vastutuse liigid on ette nähtud isikuandmete kaitse alaste rikkumiste korral. Andmetöötlejad peavad jälgima, et kui andmed on kogutud, ei tähenda see töötlejatele piiramatut õigust nende kasutamiseks. Arvestades andmete kaitsmise vajalikkust ja riigil lasuvat kohustust luua meetmed isikute põhiõiguste kaitseks, on üheks andmete kaitse elemendiks jõustamismeetmed ja sanktsioonid.
IKS sätestab kahte liiki vastutust:

1) vastutus läbi riikliku järelevalve ning sunnimeetmete rakendamise ja
2) vastutus väärteo korras delikaatsete isikuandmete registreerimiskohustuse, isikuandmete turvameetmete või isikuandmete muude nõuete rikkumise eest. Tulenevalt karistusõiguslikust regulatsioonist sätestab IKS andmekaitsenõuete trahvi määramise võimaluse nii tahtliku kui ettevaatamatu rikkumise korral.

Kuigi liikmesriikidel on direktiivi 95/46/EÜ rakendamisel jäetud kaalutlusruum, siis Euroopa Kohus on teatud punktide osas väga täpne. Kokkuvõtvalt võib öelda, et kuna sanktsioonide rakendamise osas on liikmesriikidele jäetud liiga palju kaalutlusruumi ning liikmesriigid saavad

ise valida, mis viisil ja millise meetme kaudu sanktsioonid kehtestada, on trahvide määrad riigiti väga erinevad ega pruugi olla sellise mõjuga, nagu direktiiv nõuab. See omakorda annab võimaluse suurtele ettevõtetele andmekaitsenõuete rikkumiseks ning turvameetmete asemel võib ettevõttele olla soodsam ja kasulikum lahendus trahvi maksmine. Seda probleemi soovitakse lahendada 25.05.2018.a kehtima hakkava EL andmekaitse üldmäärusega. Kuigi AKI võib algatada väärteomenetlust ja määrata trahvi, on praktikas ameti peamiseks tegevuseks ettekirjutuste ja hoiatuste tegemine, st haldussunni kohaldamine. Eelnevalt oli juttu haldussunni kohaldamisest, mis on ettekirjutus rikkumise lõpetamiseks, siis peatüki viimases osa käsitles autor karistusõiguslikku regulatsiooni. Väärtegude ja kuritegude erinevus seisneb sanktsiooni ranguses. Kui väärtegude korral viib menetluse läbi kohtuväline menetleja, siis kuritegusid menetleb kohus ja karistuseks võib olla isegi vabadusekaotus. Rahuldavaks võib pidada asjaolu, et kohtupraktikat analüüsides selgus, et raskemate rikkumiste korral on kohust mõnel juhul rakendanud ka karistusõiguslike sanktsioone.. AKI väärteomenetluse analüüs ei olnud autoril võimalik teha, kuna AKI väärteootsused ei ole avalikud. Siiski vajab nimetamist asjaolu, et andmekaitse alaseid rikkumisi avastati nii politsei kui terviseasutuste spetsialistide seas.

Kolmandas peatükis käsitles autor hetkel kehtivat väärteo- ja karistusõigusliku vastuse regulatsiooni. Autor analüüsis andmekaitse üldmäärusest tulenevaid nõudeid sanktsioonide osas ning hindas reeglite sobivust Eesti õigussüsteemi. Üldmäärus reguleerib üsna täpselt vastutava ja volitatud töötleja vastutuse.

Autor annab ülevaate trahvimäärade võimaliku rakendamise Eesti õiguses ning hindab IKS-i eelnõus pakutud lahenduse vastavust üldmäärusele. Üldmääruses on selgelt välja toodud territoriaalne kohaldamisala, mille järgi vastutavad andmetöötlejad olenemata ettevõtte asukohast, st piiriülesel töötlemise korral on sanktsioonide määrad ja kohaldamine peab olema kõigis liikmesriikides sarnane ja kohaldub ka väljaspool EL-i asutatud ettevõtete suhtes. Kui direktiivi järgi vastutasid ainult vastutavad töötlejad, siis üldmääruse kohaselt vastutavad ka volitatud töötleja, kes töötlevad andmeid vastutava töötleja nimel. Üldmäärus sätestab kõrged trahvimäärad, mis peaks tagama, et andmetöötlejad rakendavad kõiki ennetavaid meetmed andmekaitse nõuete täitmiseks.

Autor toob välja üldmääruse rakendamisega seotud probleeme ning asub seisukohale, et üldmääruse kohaste sanktsioonide rakendamine nõuab Eesti õiguskorras oluliste muudatuste tegemist. Põhiprobleemiks on asjaolu, et Eestis ei ole võimalik rakendada üldmäärusest tulenevaid halduskaristusi, kuivõrd Eesti õiguskord ei tunnusta sellist sanktsiooniliiki. Selles

osas annab üldmäärus Eestile ja Taanile diskretsiooniõiguse kohtumenetluses. Analüüsides üldmääruse võimalikku vastutuse ja sanktsioonide kohaldamist Eesti õiguses on haldustrahve Eesti õiguses võimalik kohaldada väärteomenetluses. Teine probleem, mis vajas analüüsimist, oli füüsilise ja juriidilise isiku vastutus. Kui üldiselt vastutab ettevõtte, kelle nimel vastutav või volitatud töötleja isikuandmeid töötleb, siis üldmääruse järgi saab vastutusele võtta ka töötlejad, kes vaatab isiku andmeid uudishimust. Selleks, et Eestis oleks võimalik kõrgeid trahvimäärasid rakendada, on vajalik muuta karistusseadustiku, loomaks regulatsiooni, mis lubab kõrgendatud trahvimäära rakendamist. Vastav seadusemuudatus on hetkel Riigikogus menetluses. Analüüsides IKS eelnõus sätestatud süüteokoosseisude regulatsiooni leiab autor, et valitud lahendus, kus süüteonormid on sõnastatud läbi viidete vastavatele üldmääruse artiklitele, ei ole Eesti õiguses sobilik ega vasta normi selguse ja karistuse ettenähtavuse põhimõtetele.

Käesoleva töö autor püstitas hüpoteesi, et Eesti õiguses ei ole piisavalt tõhusaid meetmeid andmekaitseõiguse jõustamiseks ning olemasolev sanktsioneerimise süsteem ei vasta täida EL õigusest tulenevaid nõudeid. Kokkuvõttes leiab autor, et hüpotees leidis kinnitust.
Autori hinnangul tuleb Eesti õiguskorras läbi viia mitmeid muudatusi, et saavutada sanktsiooniraamistik, mis oleks kooskõlas nii Eesti õiguse üldpõhimõtetega kui ka EL andmekaitse üldmäärusega. Jõustamismeetmetel on oluline osa andmesubjekti õiguste tagamisel, mistõttu peavad rakendatavad sanktsioonid olema tõhusad. Käesoleval hetkel on Eestis küll võimalik erinevat liiki vastutus, kuid õiguskorras esineb ka mitmeid lünkasid. Andmekaitse üldmääruse rakendamiseks on Eestile antud võimalus kohaldada üldmäärusest tulenevaid haldustrahve meie õigussüsteemile omase väärteomenetluse raames. Siiski kaasneb selle valikuga ka mitmeid probleeme ning autori hinnangul ei taga IKS-i eelnõu vastutust piisaval määral.

SANCTIONS IN THE AREA OF DATA PROTECTION BEFORE AND AFTER DATA PROTECTION REFORM

SUMMARY

The right to privacy and private life is protected as a human right, regulated both through constitutional laws and international conventions. The ever-developing technology has created opportunities for extensive processing of data, whereas the data subject may not know that the data is being processed, and for what purpose. The data subject has a number of rights that allow them to control the processing of personal data, but despite the existence of these rights, the actual implementation of data protection rules depends, among other things, on whether and which coercive measures can be applied to the data processor by the data subject.

This thesis aims at investigating which enforcement measures are applied in Estonia and how it is done in practice, to evaluate their efficiency as well as whether the current system is compatible with the latest developments in the EU and how Estonia can fulfil its obligations under the EU General Data Protection Regulation to ensure effective enforcement of data subject rights. The author hypothesised that Estonian law does not have enough effective measures to enforce data protection law, and the existing sanctioning system does not comply with EU law requirements.

The first chapter of the thesis clarifies and analyses the main goals and the nature of personal data protection. Personal data is any information about an identified or identifiable person, and the processing of personal data is an act involving any personal data, including collection, storage, modification, disclosure, execution, use, transmission, deletion, etc. In order for the information to be considered personal data, it does not necessarily have to be true. The processing of personal data must be as open and transparent as possible. The data subject must be able to verify the processed data, including requiring deletion or editing of incorrect data. No-one can arbitrarily interfere with the privacy of another person. The right to protection of personal data does not imply prohibition on processing data, but requires compliance with the rules and principles of data protection as well as protects a person against unlawful processing.

In Estonia, personal data protection is regulated by the Personal Data Protection Act (PDPA), which also provides for liability for violation of personal data processing requirements. The

data subject may contact the National Supervisory Authority to protect their rights. Unlawful disclosure of personal data means that the data subject is able to lodge a complaint with a civil court. In addition to state supervision and civil liability, the Estonian legal system also provides for liability in misdemeanor or criminal proceedings. There are certain grounds for initiating criminal proceedings, e.g., sensitive personal data has been published illegally, for personal gain or for causing harm to a person. Penalties for such acts include fines or even imprisonment.

Data protection requirements are monitored by an independent supervisory authority. In Estonia, the supervisory authority is represented by the Data Protection Inspectorate (DPI), which applies penalties for failure to comply with a precept or executes misdemeanor proceedings if there are indications of an offense component. However, coercion is not applied to public authorities, which calls into question the existence of efficient enforcement measures for public authorities. To conclude the first chapter, it can be said that the current legislation that regulates the protection of personal data has expired. The Data Protection Directive 95/46/EC, adopted in 1995, which has to regulate uniform processing of personal data in the member states and other relevant requirements, does not fulfil its purpose in today's context. Fast technological developments require new regulations as the legislation in question has become outdated. The aim of the Directive was to create a single regulatory framework in all the member states, but since the countries have been subject to a major decision-making process, the member states are subject to different standards and, therefore, the Directive failed to achieve its primary objective. Confirmation of the foregoing also gives rise to requests for a preliminary ruling from the Court of Justice and interpretations by the Court of Justice for the purpose of implementing the Directive, which gives grounds for arguing that the provisions of the Directive are too general. As the PDPA takes over the Directive and largely follows its provisions, the author is of the opinion that the Estonian data protection rules are incomplete.

In the second chapter, the author discusses which types of liability are applicable to personal data breach violations. Data processors need to ensure that once data has been collected, it does not imply unlimited processing rights to its use. Given the need for data protection and the state's obligation to establish measures to protect the fundamental rights of individuals, enforcement measures and sanctions are one element of data protection.

The PDPA provides for two types of liability:

1) liability through implementation of state supervision and coercive measures, and

2) liability for misdemeanors in regard to recording of sensitive personal data, breach of requirements related to personal data security measures, and other personal data requirements. As a result of penal law, the PDPA provides for imposing a fine on data protection claims in the event of intentional and negligent breach.

Although the member states have a margin of discretion in implementing the Directive 95/46/EC, the European Court is very precise on certain points. To sum it up, since application of sanctions is left to the member states with too much discretion and the member states are free to choose, which sanctions to impose, and by which means, the level of fines varies greatly from one country to another and may not have the same effect as the Directive requires. This, in turn, enables larger companies to violate data protection requirements, and, instead of complying with security measures, companies find it more profitable to pay a fine. This problem will be solved by the EU General Data Protection Regulation, which will enter into force on 25.05.2018. Although the DPI may initiate misdemeanor proceedings and impose fines, precepts and warnings are the agency's main activity, that is, application of administrative compulsion, which is a precept for infringement termination.

The last part of the chapter deals with criminal law regulation. The difference between misconduct and crime lies in the rigor of the sanction. In the case of misdemeanor, proceedings are conducted through extra-judicial proceedings, but criminal proceedings are conducted in court, and imprisonment may also be imposed. It is comforting to realise that as a result of analysing case law, it has become clear that in cases of more serious violations, the court has in some cases also imposed punitive sanctions. The analysis of the DPI misdemeanor procedure could not be performed by the author as the DPI misdemeanor decisions are not publicly available. However, it must be noted that data protection violations were detected among both the police and healthcare professionals.

In the third chapter, the author discusses the current regulation on misdemeanor and punishment. The author analyses the requirements for sanctions under the General Data Protection Regulation and assesses the suitability of the rules for the Estonian legal system. The General Regulation governs strictly the liability of the responsible and authorised data processor.

The author gives an overview of the possible application of fines in Estonian law and assesses the compliance of the solution proposed in the PDPA draft with the General Regulation. The

General Regulation explicitly outlines the territorial scope, according to which data processors, irrespective of the location of the business, are responsible for cross-border processing; the levels of sanctions and their application must be similar in all the member states and also apply to non-EU companies. Under the Directive, only responsible data processors are held liable; however, the General Regulation will also impose liability on authorised data processors who process data on behalf of the main data processor. The General Regulation provides for high fines, which should ensure that data processors take all preventive measures to comply with data protection requirements.

The author outlines the problems associated with the implementation of the General Regulation and is of the opinion that the implementation of sanctions under the General Regulation requires significant changes to the Estonian legal order. The main problem lies in the fact that it is not possible to implement administrative penalties arising from the General Regulation in Estonia, since the Estonian legal system does not recognise this type of sanction. In this regard, the General Regulation gives Estonia and Denmark discretion in court proceedings. When analysing the possible application of liability and sanctions in Estonian law, administrative fines in Estonian law can be applied in misdemeanor proceedings. Another problem that needed to be analysed is the liability of physical and legal persons. If the company, on behalf of which a responsible or authorised data processor handles data, is held liable, then, according to the General Regulation, the latter will also be held liable, even monitoring personal data out of pure interest. In order to be able to apply high fine rates in Estonia, it is necessary to amend the Penal Code to create a regulation that allows for the application of a higher rate. The corresponding amendment to the law is currently pending in Riigikogu. By analysing the provisions of the constituent offence elements set forth in the GDPA draft, the author finds that the chosen solution, where the offence standards are worded through references to the corresponding articles of the General Regulation, is not suitable in Estonian law and does not meet the principles of clarity of the norm or foreseeability of punishment.

The author of this thesis set out the hypothesis that the measures used in Estonian law are not efficient enough to enforce data protection law, and the existing sanctioning system does not meet the requirements of the EU law. All in all, the author finds that the hypothesis was confirmed.

According to the author, a number of changes have to be made in the Estonian legal system in order to achieve a sanctions framework in line with both the general principles of Estonian law

and the EU General Data Protection Regulation. Enforcement measures play an important role in ensuring the rights of the data subject, and, therefore, the sanctions to be imposed must be efficient. At present, there are different liability types in Estonia, but there are several gaps in the legal system. To implement the General Data Protection Regulation, Estonia has been given an opportunity to apply administrative penalties under the General Regulation in the context of misdemeanor procedure specific to our legal system. However, there are several problems with this particular choice, and, according to the author, the PDPA draft does not provide for adequate liability.

LISA 1

Kehtivad karistused (IKS, KarS)	Uus IKS, KarS	Karistatav tegevus (üldmäärus)
IKS § 40 Andmekaitse inspektsiooni ettekirjutus Lg 1 - 1) Käesoleva seaduse täitmise tagamiseks on Andmekaitse Inspektsiooni ametiisikul õigus teha isikuandmete töötlejale ettekirjutusi ja vastu võtta otsuseid. Lg 2 - Käesoleva paragrahvi lõikes 1 nimetatud ettekirjutuse mittetäitmisel võib Andmekaitse Inspektsioon rakendada sunniraha asendustäitmise ja sunniraha seaduses sätestatud korras. Sunniraha ülemmäär on 9600 eurot. Sunniraha ei rakendata riigiasutuse suhtes.	IKS (eelnõu)§ 59 Sunniraha määr Andmekaitse Inspektsiooni ettekirjutuse täitmata jätmise korral on asendustäitmise ja sunniraha seaduses sätestatud korras rakendatava sunniraha kohaldamise igakordne ülemmäär kuni 20 000 000 eurot või ettevõtja puhul kuni 4 protsenti tema eelneva majandusaasta ülemaailmsest aastasest kogukäibest, olenevalt sellest, kumb summa on suurem.	Üldmääruse artikkel 83 Trahvide määramise üldtingimused Lg 6 - Artikli 58 lõikes 2 osutatud järelevalveasutuse korralduse täitmatajätmise korral määratakse kooskõlas käesoleva artikli lõikega 2 trahv, mille suurus on kuni 20 000 000 eurot või ettevõtja puhul kuni 4 % tema eelneva majandusaasta ülemaailmsest aastasest kogukäibest, olenevalt sellest, kumb summa on suurem.
IKS § 42 Isikuandmete töötlemise nõuete rikkumine Lg 1 - Delikaatsete isikuandmete töötlemise registreerimiskohustuse, isikuandmete kaitse turvameetmete või isikuandmete töötlemise	IKS (eelnõu) § 61 Vastutava töötleja ja volitatud töötleja kohustuse rikkumine Lg 1 - Euroopa Parlamendi ja nõukogu määruse (EL) nr 2016/679 artiklites 8, 11, 25–39, 42 ja 43 sätestatud vastutava töötleja või	Artikkel 83 Trahvide määramise üldtingimused Lg 4 - Kooskõlas lõikega 2 võib järgmiste sätete rikkumise eest määrata trahvi, mille suurus on kuni 10 000 000 eurot või

muude nõuete eiramise eest – karistatakse rahatrahviga kuni 300 trahviühikut. Lg 2 - Sama teo eest, kui selle on toime pannud juriidiline isik, – karistatakse rahatrahviga kuni 32 000 eurot.	volitatud töötleja kohustuse rikkumise eest – karistatakse rahatrahviga kuni 10 000 000 eurot. Lg 2 - Sama teo eest, kui selle on toime pannud juriidiline isik, – karistatakse rahatrahviga kuni 10 000 000 eurot või kuni 2 protsenti juriidilise isiku käibest. § 62. Sertifitseerimiskorra rikkumine Lg 1 - Euroopa Parlamendi ja nõukogu määruse (EL) nr 2016/679 artiklites 42 ja 43 sätestatud sertifitseerimiskorra rikkumise eest –karistatakse rahatrahviga kuni 10 000 000 eurot. Lg 2 - Sama teo eest, kui selle on toime pannud juriidiline isik, –karistatakse rahatrahviga kuni 10 000 000 eurot või kuni 2 protsenti juriidilise isiku käibest. § 63. Toimimisjuhendi järgimise üle järelevalve teostamise korra rikkumine Lg 1- Euroopa Parlamendi ja nõukogu määruse (EL) nr 2016/679 artikli 41 lõikes 4	ettevõtja puhul kuni 2 % tema eelneva majandusaasta ülemaailmsest aastasest kogukäibest, olenevalt sellest, kumb summa on suurem: a) vastutava töötleja või volitatud töötleja kohustused artiklite 8, 11, 25-39, 42 ja 43 alusel; b) sertifitseerimisasutuse kohustused artiklite 42 ja 43 alusel; c) järelevalvet teostava asutuse kohustused artikli 41 lõike 4 alusel. Lg 5 – Kooskõlas lõikega 2 võib järgmiste sätete rikkumise eest määrata trahvi, mille suurus on kuni 20 000 000 eurot või ettevõtja puhul kuni 4 % tema eelneva majandusaasta ülemaailmsest aastasest kogukäibest, olenevalt sellest, kumb summa on suurem: a) töötlemise aluspõhimõtted, sealhulgas artiklite 5, 6, 7 ja 9 kohased nõusoleku andmise tingimused; b) andmesubjektide õigused artiklite 12–22 alusel; c) isikuandmete edastamine

	sätestatud toimimisjuhendi järgimise üle järelevalve teostamise korra rikkumise eest –karistatakse rahatrahviga kuni 10 000 000 eurot. Lg 2 - Sama teo eest, kui selle on toime pannud juriidiline isik, –karistatakse rahatrahviga kuni 10 000 000 eurot või kuni 2 protsenti juriidilise isiku käibest. IKS § 64. Isikuandmete töötlemise põhimõtete rikkumine Lg 1 - Euroopa Parlamendi ja nõukogu määruse (EL) nr 2016/679 artiklis 5 sätestatud isikuandmete töötlemise põhimõtete rikkumise eest, sealhulgas Euroopa Parlamendi ja 23 nõukogu määruse (EL) nr 2016/679 artiklites 5, 6, 7 ja 9 sätestatud andmesubjekti nõusoleku andmise korra rikkumise eest, –karistatakse rahatrahviga kuni 20 000 000 eurot. Lg 2 - Sama teo eest, kui selle on toime pannud juriidiline isik, –karistatakse rahatrahviga kuni 20 000 000	kolmandas riigis asuvale vastuvõtjale või rahvusvahelisele organisatsioonile artiklite 44–49 alusel; d) mis tahes kohustused IX peatüki kohaselt vastu võetud liikmesriigi õigusaktide alusel; e) järelevalveasutuse artikli 58 lõike 2 kohase korralduse või ajutise või alalise töötlemispiirangu või andmevoogude peatamise täitmatajätmine või juurdepääsu andmisest keeldumine, rikkudes sellega artikli 58 lõiget 1.

	eurot või kuni 4 protsenti juriidilise isiku käibest. IKS § 65 Andmesubjekti õiguste rikkumine Lg 1 - Euroopa Parlamendi ja nõukogu määruse (EL) nr 2016/679 artiklites 12–22 sätestatud andmesubjekti õiguse rikkumise eest – karistatakse rahatrahviga kuni 20 000 000 eurot. Lg 2 - Sama teo eest, kui selle on toime pannud juriidiline isik, –karistatakse rahatrahviga kuni 20 000 000 eurot või kuni 4 protsenti juriidilise isiku käibest. IKS § 66 Isikuandmete edastamise korra rikkumine Lg 1 - Euroopa Parlamendi ja nõukogu määruse (EL) nr 2016/679 artiklites 44–49 sätestatud isikuandmete edastamise korra rikkumise eest –karistatakse rahatrahviga kuni 20 000 000 eurot. Lg 2 - Sama teo eest, kui selle on toime pannud juriidiline isik, –karistatakse rahatrahviga kuni 20 000 000 eurot või kuni 4 protsenti	

	juriidilise isiku käibest. IKS § 67 Isikuandmete töötlemise korra rikkumine eriolukorras Lg 1 - Käesoleva seaduse 2. peatüki 3. jaos sätestatud isikuandmete töötlemise korra rikkumise eest – karistatakse rahatrahviga kuni 20 000 000 eurot. Lg 2 - Sama teo eest, kui selle on toime pannud juriidiline isik, –karistatakse rahatrahviga kuni 20 000 000 eurot või kuni 4 protsenti juriidilise isiku käibest. IKS § 68 Andmekaitse Inspektsiooni korralduse täitmata jätmine Lg 1 - Euroopa Parlamendi ja nõukogu määruse (EL) nr 2016/679 artikli 58 lõikes 2 sätestatud korralduse täitmata jätmise eest – karistatakse rahatrahviga kuni 20 000 000 eurot. Lg 2 - Sama teo eest, kui selle on toime pannud juriidiline isik, –karistatakse rahatrahviga kuni 20 000 000 eurot või kuni 4 protsenti juriidilise isiku käibest.	

	IKS § 69 Andmekaitse Inspektsiooni juurdepääsu võimaldamise rikkumine Lg 1 - Euroopa Parlamendi ja nõukogu määruse (EL) nr 2016/679 artikli 58 lõikes 1 sätestatud uurimisvolituse alusel antud korralduse täitmata jätmise eest, kui sellega ei võimaldata Andmekaitse Inspektsioonile juurdepääsu isikuandmetele, muule teabele või ruumidele, – karistatakse rahatrahviga kuni 20 000 000 eurot. 24 Lg 2 - Sama teo eest, kui selle on toime pannud juriidiline isik, –karistatakse rahatrahviga kuni 20 000 000 eurot või kuni 4 protsenti juriidilise isiku käibest.	
KarS § 157 Isikuandmete ebaseaduslik avaldamine Lg 1 - Kutse- või ametitegevuses teatavaks saanud isikuandmete ebaseadusliku avaldamise eest isiku poolt, kellel oli seadusest tulenev kohustus andmeid mitte avaldada, ja kui puudub käesoleva	Samaks.	

seadustiku §-s 157[1] sätestatud süüteokoosseis, – karistatakse rahatrahviga kuni 300 trahviühikut. Lg 2 - Sama teo eest, kui selle on toime pannud juriidiline isik, – karistatakse rahatrahviga kuni 32 000 eurot.		
KarS § 157[1] Delikaatsete isikuandmete ebaseaduslik avaldamine Lg 1 - Delikaatsete isikuandmete ebaseadusliku avaldamise või neile ebaseadusliku juurdepääsu võimaldamise eest – karistatakse rahatrahviga kuni 300 trahviühikut. Lg 2 - Sama teo eest, kui see on toime pandud omakasu eesmärgil või kui sellega on tekitatud teisele isikule kahju, – karistatakse rahalise karistuse või kuni üheaastase vangistusega. Lg 3 - Käesoleva paragrahvi lõikes 1 sätestatud teo eest, kui selle on toime pannud juriidiline isik, –	Isikuandmete kaitse seaduse rakendamise seadus (eelnõu) § 25 Karistusseadustiku muutmine Karistusseadustiku §-s 157[1] asendatakse sõna "delikaatsete isikuandmete" sõnadega "eriliiki isikuandmete"	

karistatakse rahatrahviga kuni 32 000 eurot. Lg 4 - Käesoleva paragrahvi lõikes 2 sätestatud teo eest, kui selle on toime pannud juriidiline isik, – karistatakse rahalise karistusega.		
	Karistusseadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seadus (väärteokaristuste reform, EL-i õigusest tulenevad rahatrahvid) „§ 47^1. Kõrgendatud ülemmääraga rahatrahv Lg 1 - Põhjendatud juhul, eelkõige kui see on vajalik Eestile siduva rahvusvahelise kohustuse täitmiseks, võib käesolevas seadustikus või muus seaduses väärteo eest ette näha kõrgendatud ülemmääraga rahatrahvi. Sellisel juhul võib kohus või kohtuväline menetleja väärteo eest kohaldada rahatrahvi kuni: 1) 20 000 000 eurot või	

	2) kolmekordses väärteo tulemusel teenitud kasule või ära hoitud kahjule vastavas summas, kui sellist kasu või kahju on võimalik kindlaks teha. Lg 2 - Juriidilisele isikule võib käesoleva paragrahvi lõikes 1 sätestatud juhul kohus või kohtuväline menetleja väärteo eest kohaldada rahatrahvi kuni: 1) 20 000 000 eurot; 2) kolmekordses väärteo tulemusel teenitud kasule või ära hoitud kahjule vastavas summas, kui sellist kasu või kahju on võimalik kindlaks teha, või 3) 15 protsenti juriidilise isiku või seaduses sätestatud juhul tema konsolideerimisgrupi konsolideeritud käibest.	

KASUTATUD KIRJANDUS

1. Acceto, M., Zlepting, S. The Principle of Effectiveness: Rethinking Its Role in Community Law, European Public Law, 11.3 (2005), lk. 387
2. Banisar. D., Models for protecting privacy. – The Door into the Other Side. Budapest: Adatvédelmi Biztos Irodja, 2001
3. Blackmer, W.S. (5 May 2016). GDPR: Getting Ready for the New EU General Data Protection Regulation. Information Law Group. InfoLawGroup LLP
4. Boehm. F., Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Springer Verlag, Berlin Heidelberg, 2012
5. Bygrave, L.A. Data Privacy Law: An International Perspektive. Oxford Scholarship Online 2014
6. Cate, F. H. Privacy in the information age. Washington, D.C: Bookings Institution Press, 1997
7. Change, C. Corporate Liability in Europe. Clifford Chance LLP January 2012, p3
8. Donaldson, M., Watter, R. „Corporate Culture“ as a Basis for the Criminal Liability of Corporations. Prepared by Allens Arthur Robinson for the United Nations Special Representative of the Secretary General on Human Rights and Business. February 2008, lk 1-2
9. Eesti Vabariigi Põhiseadus. Komm vlj. 4. tr. Tallinn: Juura 2017
10. Elkind, E., Sootak. J. Juriidilise isiku vastutus: uued arengusuunad Eesti kohtupraktikas. – Juridica 2015 / 2, lk 672
11. Gobert, J., Pascal A.-M. (editors). European Developments in Corporate Criminal Liability. Routledge, 2014, lk 5
12. Gonzales Fuster. G., Gutwirth. S., P. De Hert (2010). From Unsolicited Communications to Unsolicited Adjustments: G. Gutwirth, Y. Poullet & P. de Hert (toim.) *Data Protection in a Profiled World*, Springer, Dordrecht/London (105-117)
13. Gutwirth, S., Hert, P. D., Poullet, Y., Terwangne, C., S. Nouwt Editors, Reinventing Data Protection?, Springer Science+Business Media B.V.2009
14. De Hert, P., Gutwirth, S. Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action. – Gutwirht, S. jt (toim). Reinventing Data Protection? Springer Science+Business Media B.V.,2009
15. Handbook on European Data Protection Law. Luxembourg: Publications Office of the European Union. 2014, p 17
16. Hirsch, H. J. Juriidiliste isikute kriminaalvastutusest. – Juridica 1996 /1, lk 17–18

17. Ilus, T. Andmesubjekti osaluse põhimõte Euroopa Nõukogu konventsioonide ning EIK lahendite valguses. – Juridica 2005 / 8, lk 522
18. Ilus, T. Isikuandmete kaitse olemus ja arengusuunad. – Juridica 2002 / 7, lk 442
19. Jäätma, J. Sunniraha kui kohustatud isiku sundimise vahend ja sunnivahend. – Juridica 2015 / 10, lk 720-722
20. Kiris, R., Pikamäe, P., Sootak, J. Sanktsiooniõigus. Tallinn: Juura 2017, lk 15
21. Kranich, H. Ühiskonna (eba) normaalne areng ja inimõigused. Nimede kohtulahendites avalikustamise näide. – Juridica 2015 / 4, lk 283
22. Krey, V. Deutsches Strafreecht. Allgemeiner Teil. Bd 1. Stuttgart: Kohlhammer 2001, § 1, vnr 20-21
23. J. Laffranque, Euroopa Liidu õigussüsteemi ja Eesti õiguse koht selles. Tallinn: Juura 2006, lk 270
24. Leigh, H. L. The Criminal liability of corporations and other groups: a comparative view. Michigan Law Review, Vol 80, No 7. jun 1982, p. 1509
25. Madise, Ü. Jt (toim). Eesti Vabariigi Põhiseadus vlj. Tallinn: Juura 2017
26. Meier, B.-D. .Strafrechtliche Sanktionen. Berlin: Springer, 2001
27. Männiko, M. Õigus privaatsusele ja andmekaitse. Tallinn: Juura 2011
28. Nõmper, A., Tikk, E. Informatsioon ja õigus. Tallinn: Juura 2007
29. Pikamäe, P., Sootak, J. Karistusseadustik. Komm vlj. Tallinn: Juura 2015
30. Pilving, I. Õigus isikuandmete kaitsele. – Juridica 2005 / 8, lk 536
31. Pradel, J. Juriidiliste isikute kriminaal- vastutus. Tähelepanekuid Euroopa riikide seadusandluse kohta. – Juridica 1999 / 8, lk 370 jj
32. Põllumäe, S. Mõiste *administrative penalties* riigisisesesse õigusesse ülevõtmine. Tallinn: Juura. Õiguskeel 2015 / 2, lk 27
33. Robinson, N., Graux, H., Botterman, M., Valeri, L. Review of the European Data Protection Directive. Cambridge: RAND, 2009, p 36
34. Rodota, S. Data Protection as a Fundamental Right. – Gutwirth, S. jt (toim). Reinventing Data Protection? Springer Science+Business Media B.V., 2009, lk 79
35. Salla, J. Karistuse asendamist ja karistusest vabastamist puudutavad muudatused. – Juridica 2014 / 8, lk
36. Samson, E. Kriminaalkaristus majandusette- võtetele. – Juridica 1999 / 8, lk366 jj
37. Sootak, J. Karistusõiguse alused. Tallinn: Juura 2003, lk 19
38. Sootak, J. Karistusõigese revisjon kuriteo-, väärteo- ja haldusõiguse piirimail. Juridica 2013 / 4, lk 247

39. Tupay, P.K. Õigusest eraelule kuni andmekaitse üldmääruseni ehk tundmatu õigus isikuandmete kaitsele. – Juridica 2016 / 4, lk 240
40. Tzanou, M. Data protection as a fundamental right next to privacy? „Reconstructing" a not so new right. – International Data Privacy Law 2013, nr 3 (2)
41. Weichert, T. Isikuandmete töötlemine eraõiguslikes suhetes ja järelevalve selle üle finantsteenuste osutajate näitel. – Juridica 2005 / 8, lk 557

Eesti õigusaktid

1. Asendustäitmise ja sunniraha seadus. – RT I 2001,50, 283 … RT I, 12.07.2014, 29
2. Eesti Vabariigi Põhiseadus. – RT 1992, 26, 349 ... RT I, 15.05.2015, 2
3. Haldusmenetluse seadus. – RT I,2001,58,354…RT I, 28.12.2017,21
4. Halduskohtumenetluse seadustik. – RT I, 23.02.2011,3 … RT I, 28.11.2017, 3
5. Isikuandmete kaitse seadus. – RT I 2007, 24, 127 ... RT I, 06.01.2016, 10
6. Julgeolekuasutuste seadus. – RT I 2001, 7, 17 ...RT I, 05.05.2017, 2
7. Karistusregistri seadus. – RT I, 21.03.2011, 3 ... RT I, 05.12.2017, 4
8. Karistusseadustik. – RT I 2001, 61, 364 ... RT I, 30.12.2017, 29
9. Korrakaitseseadus. – RT I, 22.03.2011, 4 ... RT I, 02.12.2016, 6
10. Krediidiasutuste seadus. – RT I 1999,23,348…RT I, 30.12.2017,3
11. Kriminaalmenetluse seadustik. – RT I 2003, 27, 166 ... RT I, 05.12.2017, 8
12. Politsei ja piirivalve seadus. – RT I 2009, 26, 159 ... RT I, 06.07.2017, 6
13. Riigivastutuse seadus, - RT I 2001, 47, 260 ... RT I, 17.12.2015, 76
14. Vabariigi Valitsuse seadus. – RT I 1995, 94, 1628 ... RT I, 28.12.2017, 19
15. Vangistusseadus. – RT I 2000, 58, 376 … RT I, 09.03.2018, 19
16. Võlaõigusseadus. – RT I, 2001,81,487 ... RT I, 31.12.2017, 8
17. Väärteomenetluse seadustik, - RT I 2002, 50, 313 ... RT I, 30.12.2017, 22
18. Väärtpaberituru seadus. – RT I 2001,89,532…RT I,30.12.2017,43

Euroopa Liidu, rahvusvahelised ja välisriikide õigusaktid

19. Bundesdatenschutzgesetz (BDSG). Arvutivõrgus: https://www.gesetze-im-internet.de/bdsg_1990/ (11.02.2018)
20. Datenschutzgesetz (DSG). Arvutivõrgus: https://www.digital.austria.gv.at/data-protection-act (05.02.2018)
21. Euroopa Liidu leping. – ELT C 115 / 09.05.2008, 13-45

22. Euroopa Liidu lepingu ja Euroopa Liidu toimimise lepingu konsolideeritud versioonid ELT C 326 / 26.10.2012
23. Euroopa Liidu Põhiõiguste Harta, ELT C 83 / 30.03. 2010, lk 389-403
24. Euroopa Nõukogu Parlamentaarse Assamblee resolutsioon 428 (1970) "Declaration on mass communication media and Human Rights". Arvutivõrgus: http://assembly.coe.int/nw/xml/XRef/X2HXrefViewPDF.asp?FileID=15842&lang=en (18.01.2018)
25. Euroopa Parlamendi ja nõukogu direktiiv 2002/58/EÜ, 12. juuli 2002, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv). ELT L 514 / 31.07.2002
26. Euroopa Parlamendi ja Nõukogu direktiiv, 2006/24/EÜ, 15. märts 2006, mis käsitleb üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist ja millega muudetakse direktiivi 2002/58/EÜ. ELTL 105 / 13.04.2006
27. Euroopa Parlamendi ja nõukogu direktiiv 95/46/EÜ, 24.10.1995, üksikute kaitse kohta isikuandmete töötlemisel ja selliste vaba liikumise kohta. ELT L 281 / 23.11.1995, lk 31-50
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 kaitseüldmäärus). – ELT L 119, 04.05.2016. Arvutivõrgus:http://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32016R0679&from=ET (18.01.2018)
29. Fizisko personu datu aizsardzības likums. Arvutivõrgus: https://www.vestnesis.lv/ta/id/4042-fizisko-personu-datu-aizsardzibas-likums (18.01.2018)
30. Inimõiguste ja põhivabaduste kaitse konventsioon. – RT II 2010, 14, 54
31. Irish DPA, arvutivõrgus - https://dataprotection.ie/docs/Home/4.htm (02.02.2018)
32. Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon. – RT II 2001, 1,3
33. 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, 04.05.2016
34. Ühinenud Rahvaste Organisatsioon. Inimõiguste ülddeklaratsioon. Arvutivõrgus: http://www.un.org/en/documents/udhr/ (12.12.2017)

Kohtuotsused

35. EIKo 29.03.2016, nr 56925/08, *Bēdat vs* Šveits
36. EIKo 12.01.2016, 61496/08, *Bárbulescu vs* Rumeenia
37. EIKo 10.10.2013, nr 26547/07, *Print Zeitungsverlag vs. GmbH* vs Austria
38. EIKo 24.09.2013, nr 43612/10, *Belpietro vs* Itaalia
39. EIKo 07.02.2012, 39954/08, *Alex Springer AG vs* Saksamaa
40. EIKo 07.07.2012, 40660/08, *Von Hannover vs* Saksamaa
41. EIKo 17.01.2012, 33497/07, *Krone Verlag jt vs* Austria
42. EIKo 16.12.2010, 24061/04, *Aleksei Ovchinnikov vs.* Venemaa
43. EIKo 10.02.2009, 3514/02, *Eerikäinen jt vs* Soome
44. EIKo 31.07.2007, nr 65022/01, *Zaicevs v* Läti
45. EIKo 23.11.2006, nr 73053/01, *Jussila v* Soome
46. EIKo 28.01.2003, 44647/98, *Peck vs.* the United Kingdom
47. EIKo 16.04.2002, 37971/97, *Société Colas Est jt vs* Prantsusmaa
48. EIKo 16.04.2002, nr 37971/97, *Société Colas Est jt vs* Prantsusmaa
49. EIKo 04.05.2000, 2834/92, *Rotaru vs* Rumeenia
50. EIKo 23.10.1995, nr 16841/90, *Pfarrmeier v* Austria
51. EIKo 16.12.1992, nr 13710/08, *Niemietz vs* Saksamaa
52. EIKo 21.02.1984, nr 8544/79, *Öztürk v* Saksamaa
53. EIKo 13.06.1979, 6833/74, *Marckx vs.* Belgia
54. EIKo 06.06.1979, nr 5370/72, *Engel jt vs*. Holland
55. EKo 26.02.2013, C-617/10, *Aklagaren* v Hans Akerberg Fransson
56. EKo 24.11.2011, liidetud kohtuasjad C-468/10 ja C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) ja Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) vs Administración del Estado
57. EKo 28.10.2010, C-367/09, *Belgisch Interventie- en Restitutiebureau v. SGS Belgium NV, Firme Derwa NV, Centraal Beheer Achmea NV*
58. EKo 14.02.2008, C-450/06, *Varek Sa vs* Belgia
59. EKo 06.11.2003, C-101/01, *Lindqvist vs* Rootsi
60. EKo 20.05.2003, C-465/00, Rechnungshof vs Österreichischer Rundfunk jt, ühendatud C-465/00, C-138/01 ja C-139/01
61. Harju Maakohus, 1-13-9441/5, 06.11.2013
62. Pärnu Maakohus, 1-11-2627/24, 08.05.2012
63. RKHKo, 3-3-1-158-16, 03.11.2016

64. RKHKo 3-3-1-85-15, 23.03.2016
65. RKHK0 3-3-1-72-14, 22.04.2015
66. RKHKo 3-3-1-42-14, 22.10.2014
67. RKHKo 3-3-1-29-13, 23.10.2013
68. RKHKo 3-3-1-3-12, 12.06.2012
69. RKHKo 3-3-1-46-10, 15.09.2010
70. RKHKo 3-3-1-44-10, 13.10.2010
71. RKHKo 3-3-1-98-06, 17.04.2007
72. RKKKo 3-1-1-41-14, 01.10.2014
73. RKKKo, 3-1-1-15-14, 24.03.2014
74. RKKKo 3-1-1-66-14, 13.11.2014
75. RKKKo 3-1-1-56-13, 07.06.2013
76. RKKKo 3-1-1-100-11, 09.12.2011
77. RKKKo 3-1-1-30-11, 12.05.2011
78. RKKKo 3-1-1-81-08, 23.02.2009
79. RKKKo 3-1-1-84-07, 07.12.2007
80. RKKKo 3-1-1-19-07, 07.05.2007
81. RKKKo 3-1-1-4-06, 27.03.2006
82. RKKKo 3-1-1-22-05, 15.04.2005
83. RKKKo 3-1-1-131-04, 14.01.2005
84. RKKKo 3-1-1-9-05, 23.03.2005
85. RKKKo 3-1-1-22-05, 15.04.2005
86. RKKKo 3-1-1-82-04, 28.09.2004
87. RKKKo 3-1-1-20-01, 05.03.2001
88. RKTKo 2-15-16007, 04.10.2017
89. RKTKo, 3-2-1-159-14, 18.02.2014
90. RKTKo 3-2-1-18-13, 26.06.2013
91. RKTKo 3-2-1-152-09, 13.01.2010
92. RKTKo 3-2-1-145-07, 19.02.2008
93. RKTKo 3-2-1-161-05, 31.05.2006
94. RKTKo 3-2-1-17-05, 13.05.2005
95. RKTKo 3-2-1-95-05, 21.12.2005
96. RKÜKo 3-2-1-4-13, 17.12.2013
97. RKÜKo 3-1-1-37-07, 12.06.2008
98. RKÜKo, 3-4-1-10-04, 25.10.2004

99. Saksamaa Föderaalse Konstitutsioonikohtu otsus 15.detsembrist 1983, viitenumber: 1 BvR 209, 269, 362, 420, 440, 484/83
100. Soome kohtuotsus 06.08 1983, 477/2001
101. Tln RnKo, 1-11-2627/57, 24.09.2012

Andmekaitse Inspektsiooni vaideotsused

102. AKI vaideotsus nr 2.1-3/16/1343, 31.08.2016
103. AKI vaideotsus nr 2.1-1/16/1044, 04.08.2016
104. AKI vaideotsus nr 2.1-3/17/1634, 12.09.2017
105. AKI vaideotsus nr 2.1-3/17/965, 08.05.2017

Muud materjalid

106. AKI. Avaliku teabe seaduse ja Isikuandmete kaitse seaduse täitmisest 2016 aastal. Soovitused aastaks 2017. Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/aastaraamat_2016.pdf (5.03.2018)
107. AKI. Avaliku teabe seaduse ja Isikuandmete kaitse seaduse täitmisest aastal 2015. Soovitused aastaks 2016. Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/AASTARAAMAT.pdf (5.03.2018)
108. AKI. Avaliku teabe seaduse ja Isikuandmete kaitse seaduse täitmisest aastal 2014. Soovitused aastaks 2015. Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/aastaraamat%202014.pdf (18.01.2018)
109. AKI. Eelnõule arvamuse avaldamine, 21.12.2017. Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/eelnoule_arvamuse_avaldamine_-_uus_iks.pdf (18.01.2018)
110. AKI. Interneti rehitsemise seire 2017 (GPEN Sweep), 18.09.2017. Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/interneti_rehitsemise_seire_2017_gpen_sweep.pdf (05.03.2018)
111. AKI. Isikuandmete avalikustamine meedias. 19.11.2015. Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Juhised/meediavaidlusse%20sekkumise%20kriteeriumid.pdf (02.04.2018)

112. AKI. Isikuandmete kaitse üldmääruse (EL) 2016/679 rakendamine, 16.10.2017. Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/isikuandmete_kaitse_uldmaarus e_el_2016679_rakendamine.pdf (18.01.2018)
113. AKI. Isikuandmete töötlemine töösuhtes. 26.05.2014. Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikuandmed%20t%C3%B6%C 3%B6suhetes%20juhendmaterjal26%2005%202014_0.pdf (02.04.2018)
114. AKI. MEMO haldustrahvidest, 29.05.2017. Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/memo-haldustrahvid.pdf (18.01.2018)
115. AKI. Rikkumisteated. 13.02.2017. Arvutivõrgus: http://www.aki.ee/et/andmekaitse-reform/rikkumisteated (18.01.2018)
116. AKI: rohkelt tuleb karistada rahvastikuregistri väärkasutajaid. – Äripäev. 20.05.2013. Arvutivõrgus: http://www.ituudised.ee/uudised/2013/05/20/andmekaitse-rohkelt-tuleb-karistada-rahvastikuregistri-vaarkasutajaid (02.02.2018)
117. AKI menetluspraktika. Arvutivõrgus: http://www.aki.ee/et/inspektsioon/menetluspraktika (18.01.2018)
118. AKI. Töötlustoimingute registreerimine. 04.04.2018. Arvutivõrgus: http://www.aki.ee/et/andmekaitse-reform/tootlustoimingute-registreerimine (09.04.2018)
119. AKI. Väärteomenetlused. 08.01.2015. Arvutivõrgus: http://www.aki.ee/et/vaarteomenetlused-0 (02.03.2018).
120. Andmekaitse Inspektsiooni avastus: SEB küsib ainsana mobiilipanga kasutajalt ligipääsu telefoniraamatule. – Delfi. 20.02.2017. Arvutivõrgus: http://kasulik.delfi.ee/news/uudised/andmekaitse-inspektsiooni-avastus-seb-kusib-ainsana-mobiilipanga-kasutajalt-ligipaasu-telefoniraamatule?id=77286196 (18.01.2018)
121. Andmekaitse Inspektsiooni peadirektori ülevaade EL andmekaitsereformi rakendamise seisust Eestis. 14.10.2016. Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/ylevaade_reformist_14102016.pdf (18.01.2018)
122. AKI peadirektori seisukohad uue andmekaitseõiguse kontseptsiooni asjus (koostatud Justiitsministeeriumis 27.04.2017). Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/jum_oigusraamistiku_kontseptsiooni_markused.pdf (08.01.2018).
123. Andmeskandaali sattunud Facebook kaotas oma väärtusest 37 miljardit. – Postimees. 20.03.2018. Arvutivõrgus: https://majandus24.postimees.ee/4444519/andmeskandaali-sattunud-facebook-kaotas-oma-vaartusest-37-miljardit (01.04.2018)

124. Antonova, J. Isikuandmete kaitse kohtueelses kriminaalmenetluses Eestis. Magistritöö. Tartu: Tartu Ülikool, 2015
125. Antonova, J., Mikiver, M. Andmekaitsest õigusloomejuristile. 22.09.2016. Arvutivõrgus: https://www.just.ee/sites/www.just.ee/files/andmekaitse_koolituse_slaidid.pdf
126. Artikli 29 alusel asutatud andmekaitse töörühm. Arvamus 4/2007 isikuandmete mõiste kohta, Arvutivõrgus: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf (18.01.2018)
127. Artikli 29 alusel asutatud andmekaitse töörühm. Arvamus 5/2011 nõusoleku määratluse kohta. 13.07.2011, lk 3. Arvutivõrgus: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_et.pdf (05.01.2018)
128. Artikli 29 alusel asutatud andmekaitse töörühm. Suunised määruse (EL) 2016/679 kohaste trahvide kohaldamise ja määramise kohta. 03.10.2017. Arvutivõrgus: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237 (18.01.2018)
129. Brandenburgi Liidumaa andmekaitse ja dokumentidega tutvumise õiguse inspektori Dagmar Hartge seisukoht, lk 1. Arvutivõrgus: https://www.bundestag.de/blob/409390/086370264cba2c233daa84d841ce6c12/a-drs-18-24-92-data.pdf (18.01.2018)
130. E-toimik. Arvutivõrgus: http://www.e-toimik.ee/ (12.03.2018)
131. European Commission. Commission publishes guidance on upcoming new data protection rules. Arvutivõrgus: http://europa.eu/rapid/press-release_IP-18-386_en.htm (03.03.2018).
132. European Commission. Competition: revised Commission Guidelines for setting fines in antitrust cases. Arvutivõrgus: http://europa.eu/rapid/press-release_MEMO-06-256_en.htm. (18.01.2018)
133. European Commission, 24.1.2018. Stronger protection, new opportunities -Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018. Arvutivõrgus: https://ec.europa.eu/commission/sites/beta-political/files/data-protection-communication-com.2018.43.3_en.pdf (02.03.2018)
134. European Comission report. First report on the implementation of the Data Protection Directive (95/46/EC). COM(2003) 265 final. Brussels: 15.05.2003. Available: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52003DC0265#text, (31.01.2018)
135. European Union Fundamental Rights Agency. Access to data protection remedies, p 21. Arvutivõrgus: http://fra.europa.eu/et (18.01.2018)
136. Euroopa Komisjon. Mis juhtub, kui me töötleme isikuandmeid eri ELi liikmesriikides? Arvutivõrgus: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-

and-organisations/enforcement-and-sanctions/enforcement/what-happens-if-my-company-processes-data-different-eu-member-states_et (02.03.2018).

137. Euroopa Komisjon, Trahvid konkurentsiõiguse rikkumise kohta. Arvutivõrgus: http://ec.europa.eu/competition/cartels/overview/factsheet_fines_et.pdf (02.02.2018)
138. Euroopa Komisjoni ülevaade EL andmekaitsereformist. Arvutivõrgus: http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm (31.01.2018).
139. Fundamental Rights Agency. Access to data protection remedies, p 21.
140. GDPRi muudatused. Arvutivõrgus: https://www.eugdpr.org/key-changes.html (03.03.2018)
141. Heili Sepp: kaalul on sõnavabadus. – Postimees. 04.02.2017. Arvutivõrgus: https://arvamus.postimees.ee/4001067/heili-sepp-kaalul-on-sonavabadus (08.01.2018).
142. Hustinx, P. EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation. Avaldatud kõne, 2014, lk 9. Arvutivõrgus: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2014/14-09-15_Article_EUI_EN.pdf (18.01.2018).
143. Isikuandmete kaitse seaduse eelnõu 616 SE. – Arvutivõrgus: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/e14c5e2f-b684-4aa4-a7dd-ffb76f63f395/Isikuandmete%20kaitse%20seadus (19.04.2018)
144. Isikuandmete kaitse seaduse eelnõu seletuskiri, 2007. Arvutivõrgus: http://webcache.googleusercontent.com/search?q=cache:ZpXneFC7l0oJ:www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/IKS%2520SELETUSKIRI%2520%25281%2529.rtf+&cd=1&hl=et&ct=clnk&gl=ee&client=firefox-b (31.01.2018)
145. Isikuandmete kaitse seaduse eelnõu seletuskiri, 06.11.2017. Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/iks_sk_9.11.17.pdf (18.01.2018)
146. Isikuandmete kaitse uue õigusliku raamistiku kontseptsioon. 18.04.2017. Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/andmekaitse_kontseptsioon_11.04.2017.pdf
147. H. Jüriöö. Euroopa Liidu määruste vahetu ja ühetaolise rakendamise probleemid Euroopa Parlamendi ja nõukogu määruse nr 261/2004 näitel. Tartu: Tartu Ülikool 2016
148. Kanger, L., E. Rohtmets, E. Eesti andmekaitse Euroopa Kohtu praktikapeeglis. –Riigikogu Toimetised nr 23, 2011. Arvutivõrgus: https://rito.riigikogu.ee/eelmised-numbrid/nr-23/eesti-andmekaitse-euroopa-kohtu-praktika-peeglis (18.01.2018)
149. Karistusregister. Arvutivõrgus: http://www.rik.ee/et/karisturegister (12.03.2018)
150. Karistusseadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse seletuskiri, 16.07.2013. Arvutivõrgus:

https://www.just.ee/sites/www.just.ee/files/elfinder/article_files/karistusseadustiku_ja_sellega_seonduvalt_teiste_seaduste_muutmise_seaduse_seletuskiri.pdf (18.01.2018)

151. Karistusseadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse (EL õiguses sätestatud haldustrahvide kohaldamine Eesti õiguses) väljatöötamiskavatsus. 01.08.2016. Arvutivõrgus: http://eelnoud.valitsus.ee/main/mount/docList/af8feea7-5e75-435b-8152-18ece419983f#ZQPx4ka5 (18.01.2018)
152. Karistusseadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seadus (väärteokaristuste reform, EL-i õigusest tulenevad rahatrahvid) 586 SE, lk 11. Arvutivõrgus: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/f65acfbc-2656-4fbf-97e1d96582f1fcbe/Karistusseadustiku%20muutmise%20ja%20sellega%20seonduvalt%20teiste%20seaduste%20muutmise%20seadus%20(v%C3%A4%C3%A4rteokaristuste%20reform,%20ELi%20%C3%B5igusest%20tulenevad%20rahatrahvid) (01.04.2018)
153. Kliinikum vallandas Edgar Savisaare haiguslugu vaadanud töötaja. – Postimees. 09.11.2016. Arvutivõrgus: https://tervis.postimees.ee/3904237/kliinikum-vallandas-edgar-savisaare-haiguslugu-vaadanud-tootaja (08.01.2018)
154. Klopets, U. Asendustäitmise ja sunniraha rakendamise analüüs. Tallinn: Justiitsministeerium 2011, lk 9. Arvutivõrgus: http://www.just.ee/uuringud
155. D. Korff. EC study on implementation of Data Protection Directive. Comparative summary of national laws. Cambrige: September 2002, p 207. – Available: http://www.garanteprivacy.it/documents/10160/10704/Stato+di+attuazione+della+Direttiva+95-46-CE, (02.02.2018)
156. Lõhmus-Ein, K. Eraelu ja selle elementide õiguslik kaitse. Magistritöö. Tartu: Tartu Ülikool, 2004
157. Männiko, M. Andmekaitsereform toob hiigeltrahvid. – Äripäev. 09.05.2016. Arvutivõrgus: https://www.aripaev.ee/uudised/2016/05/04/andmekaitsereform-toob-hiigeltrahvid (18.01.2018)
158. Nyman Metcalf, K. Privaatsusõigus inimõigusena ja igapäevatehnoloogiad. Privaatõiguse ja andmekaitse õiguslikud aspektid. Inimõiguste Instituut. Uuring 2014, V osa lk 82. Arvutivõrgus: https://humanrightsestonia.ee/wp/wp-content/uploads/2014/11/EST-Uuringu-V-osa-Privaat%c3%b5iguse-ja-andmekaitse-%c3%b5iguslikud-aspektid.pdf (31.01.2018).
159. Nõmper, A. Andmekaitseseadusega kaasnevad suured trahvid on müüt. – Äripäev. 10.11.2016. Arvutivõrgus: https://www.aripaev.ee/uudised/2016/11/10/andmekaitseseadusega-kaasnevad-suured-trahvid-on-muut (02.02.32018)
160. OECD. The OECD privacy framework. Available: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf,

161. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Arvutivõrgus: http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

162. Opinion of the European Data Protection Supervisor on the Proposals for a Regulation establishing an Entry/Exit System (EES) and a Regulation establishing a Registered Traveller Programme (RTP), 18 July 2013. Arvutivõrgus: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2013/13-07-18_Smart_borders_EN.pdf (31.01.2018)

163. Peep, V. Andmekaitse uued nõuded ehmatasid ettevõtted ära. – Äripäev. 15.01.2018. Arvutivõrgus: https://www.aripaev.ee/uudised/2018/01/15/andmekaitse-uued-nouded-ehmatasid-ettevotted-ara (03.03.2018)

164. Põllumäe, S.Karistusõiguse revisjoni ettepanekutest tulenevad muudatused haldussunnivahendites ja haldustrahvi vms meetme võimalus. Memorandum. Justiitsministeerium: 2014, lk 3.

165. Rahandusministeerium, 29.12.2017. Isikuandmete kaitse seaduse eelnõu kooskõlastamine, lk 12. Arvutivõrgus: http://eelnoud.valitsus.ee/main#sK371WfU (02.02.2018)

166. Riigikohtu arvamus isikuandmete kaitse seaduse eelnõu kohta, 20.12.2017. Arvutivõrgus: http://eelnoud.valitsus.ee/main#OgPd2TPg (02.02.2018)

167. Riigikogu menetlus: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/e14c5e2f-b684-4aa4-a7dd-ffb76f63f395/Isikuandmete%20kaitse%20seadus (18.04.2018)

168. Rohtmets, E. Ajakirjandusvabaduse ja eraelu puutumatuse tasakaal Euroopa Inimõiguste Kohtu praktikas. Kohtupraktika analüüs. Tartu: Riigikohtu õigusteabe osakond 2014. Arvutivõrgus: http://www.riigikohus.ee/vfs/1688/ajakirjandusvabadus_analuus_m2rts2014.pdf (08.01.2018)

169. Rohtmets, E. Isikuandmete kaitse küsimused Euroopa Kohtu eelotsustes. Andmesubjekti õiguste kaitse. Kohtupraktika analüüs. Tartu: Riigikohtu õigusteabe osakond 2013. Arvutivõrgus: http://www.riigikohus.ee/vfs/1455/Andmesubjekti%20oigused_EK_analuus.pdf, (05.01.2018)

170. Siseministeerium 22.01.2018, Isikuandmete kaitse seaduse eelnõu kooskõlastamine. Arvutivõrgus: http://eelnoud.valitsus.ee/main/mount/docList/1909e111-ca98-4d1b-830a-ee49dea64a97#bXdh4dal (02.03.2018)

171. Tartu ülikooli kliinikumis vallandati Savisaare haiguslugu vaadanud töötaja. – Eesti Päevaleht. 09.11.2016. Arvutivõrgus: http://epl.delfi.ee/news/eesti/tartu-ulikooli-kliinikumis-vallandati-savisaare-haiguslugu-vaadanud-tootaja?id=76199069 (18.01.2018)

172. The Council of Europe. A Convention to protect your rights and liberties. Available: https://www.coe.int/en/web/human-rights-convention/ (31.01.2018)
173. Turk, K. Andmekaitsemääruse jõustumiseelsete tegevuste TOP 10 – 4. Uudsed andmekaitse põhimõtted. 1910.2016. Arvutivõrgus: https://triniti.ee/andmekaitsemaaruse-joustumiseelsete-tegevuste-top-10-4-uudsed-andmekaitse-pohimotted/ (18.01.2018)

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, Piret Muinast,

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

ISIKUANDMETE KAITSE NÕUETE RIKKUMISE SANKTSIONEERIMINE EUROOPA LIIDU ANDMEKAITSEREFORMI VALGUSES,

mille juhendajad on Julia Antonova ja Jaan Sootak,

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

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

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

Tartu, **23.04.2018**