TARTU ÜLIKOOL
ÕIGUSTEADUSKOND
Avaliku õiguse osakond

Krista Tuulik

PRIVAATSUSÕIGUS JA ISIKU SIDEANDMETE KASUTAMINE TEABE VARJATUD KOGUMISEL JULGEOLEKU TAGAMISE EESMÄRGIL

Magistritöö

Juhendaja
Anna-Maria Osula, PhD

Tallinn
2023

SISUKORD

SISSEJUHATUS

Juba 75 aastat on üksikisikute isikliku informatsiooni kaitsmist püütud ühel või teisel moel reglementeerida, kuid sellest hoolimata tajutakse tänapäeval privaatsusega seotud probleeme sageli suuremana kui kunagi varem.[1]

Ühelt poolt võib privaatsust lihtsustatuna kirjeldada kui midagi, mis võimaldab isikul hoida teavet või andmeid salajas ehk konfidentsiaalsena ning otsustada, kellega ja millistel tingimustel neid jagada. Saladus aga on midagi, mida ei teata ega kavatseta teistega jagada.[2]

Teiselt poolt on privaatsus keeruline termin, mis hõlmab küsimusi alates inimeste füüsilise keha terviklikkusest kuni maine ja isiklike andmeteni, olles samas huvipakkuv mitme valdkonna esindajatele, sh psühholoogidele, õigusteadlastele, politoloogidele ja poliitikakujundajatele. Rääkimata inseneridest ja arvutiteadlastest, kes on samuti huvitatud privaatsusega seonduvatest probleemidest, kuna peavad sageli eraisikute privaatsuse kaitsmiseks otsustama, kuidas luua ja konfigureerida tooteid või lubada isikliku teabe, piltide või andmete jagamist.[3]

Koroonakriis murdis arusaama, et on olemas digitaalsed ettevõtted ja muud ettevõtted. Mitmed eluvaldkonnad, kus oli vaja jälgida töötajate tööaega või tegevusi, andmestusid kiires tempos. Ühtlasi kasvas erinevate valdkondade ja neis osalevate inimeste andmejalajälg. Nii oli aastal 2022 maailmas üle 4,6 miljardi aktiivse internetikasutaja. Ainuüksi Google'i keskkonnas tehti iga päev 3,5 miljardit otsingut, saadeti enam kui 333 miljonit e-kirja ning maailmas tekkis igas sekundis iga inimese kohta 1,7 megabaiti andmeid.[4]

Enamus suure kasutusväärtusega andmetest kuulub tänapäeval suurtele tehnoloogiaettevõtetele, mille teenustest sõltub hulk ettevõtteid ja kodanikke. Neil ettevõtetel on ligipääs erisugustele kasutajate poolt teenuste tarbimise käigus loodud andmetele.[5] Digiajastul on inimesed usaldanud oma andmed, nende töötlemise ja suhtluse hiiglaslikele tehnoloogiaettevõtetele (nt Apple, Google, Meta, Microsoft või Eestis Telia ja Elisa jne), luues nii ka uue põlvkonna seirevahendajaid. Need vahendajad on suured ja võimsad ettevõtted inimeste ning valitsuse vahel,

[1] Murumaa-Mengel, M. Pruulmann-Vengfeld, P., Laas-Mikko, K. Privaatsusõigus inimõigusena ja igapäevatehnoloogiad. Tartu Ülikool 2014, lk 14.
[2] Manjikian, M. Cybersecurity Ethics. 1st ed. Taylor and Francis. 2017. Kättesaadav: https://www.perlego.com/book/1573596/cybersecurity-ethics-an-introduction-pdf (26.11.2022).
[3] *Ibidem*.
[4] Andmeühiskonna tulevik. Stsenaariumid aastani 2035. Raport. Tallinn: Arenguseire Keskus 2022, lk 13.
[5] *Ibidem,* lk 16.

mis aitavad piirata valitsuse järelevalvet. See on uus normaalsus, et need tehnoloogiaettevõtted haldavad/kaitsevad meie „digitaalseid“ kehasid ja valitsused meie „füüsilisi“ kehasid.[6]

Inimestele meeldisid ja meeldivad eelpool mainitud võrgustikud ning platvormid nagu Google või Facebook, sest need on kasutamiseks tasuta. Samas tuleb järjest enam mõista ja endale tunnistada, et sotsiaalmeedia ei ole kaugeltki tasuta. Inimesed ei ole enam lihtsalt kasutajad, vaid nende isiklik teave on kaup, mida saab osta ja müüa ning seega võrgustike ja platvormide omanike tuluallikas.[7] Keegi, kes omab juurdepääsu isiku elektroonilisele teekonnale, võib seda ära kasutada, kas isikliku kasu saamise eesmärgil või inimeste kui üksikisikute turvalisust ja julgeolekut ähvardavatel asjaoludel.

Nii näiteks oli Mark Zuckerberg ehk Facebooki (tänane Meta), millel oli 2022. aastal ca 2,9 miljardit aktiivset kasutajat[8], asutaja just see ettevõtja, kes müüs kasutajate poolt vabatahtlikult antud isikuandmeid edasi Cambridge Analyticale, Ühendkuningriigi ettevõttele, mis pakkus „valimishaldusteenuseid“, sealhulgas andmekaevet, andmevahendust ja andmeanalüüsi, ning spetsialiseerus USA „valimisturgudel“ töötades Donald Trumpi presidendikampaania toetajaks.[9]

Seega on informatsioon, sh isiklik teave, nii demokraatlikus kui ka autokraatlikus ühiskonnas üks olulisemaid ressursse, mida on tänapäeval aina keerulisem hallata, et tagada riiklikul tasandil oma kodanike kaitse küberruumi ohtude eest. Nüüdseks ongi perioodil, kus arvuteid hakati kasutama isikuandmete töötlemiseks, riiklikud ja rahvusvahelised privaatsusuuringud ning arutelud keskendunud peaasjalikult isikut tuvastava teabe privaatsusele.[10]

Euroopa Liit on asunud Atlandi-ülese julgeoleku ja andmekaitse töörühmas seisukohale, et „kodanike, ettevõtjate ja juhtivate poliitikute erasuhtluse massiline jälgimine on vastuvõetamatu“[11]. Üksikisikute kontrolli puudumine oma andmetele juurdepääsu üle teeb üha

---

[6] Rozenshtein, A. Z. Surveillance Intermediaries. Stanford Law Review 70, no 1. January 2018, lk 105.

[7] Alexandrou, A. Cybercrime and Information Technology. 1st edn. Taylor and Francis, 2021. Kättesaadav https://www.perlego.com/book/2529243/cybercrime-and-information-technology-theory-and-practice-the-computer-network-infostructure-and-computer-security-cybersecurity-laws-internet-of-things-iot-and-mobile-devices-pdf?queryID=31aa299c18a9cab249710d228d37509d&index=prod_BOOKS&gridPosition=1 (26.11.2022).

[8] Andmeühiskonna tulevik. Stsenaariumid aastani 2035. Raport. Tallinn: Arenguseire Keskus 2022, lk 13.

[9] Choudry, A. Activists and the Surveillance State. 1st edn. Pluto Press, 2018. Kättesaadav: https://www.perlego.com/book/840005/activists-and-the-surveillance-state-learning-from-repression-pdf (26.11.2022).

[10] Eesti rahvusvahelises julgeolekukeskkonnas. Teabeamet 2017, lk 37. Kättesaadav:.https://www.valisluureamet.ee/doc/raport/2017-et.pdf (03.12.2022).

[11] Lott, A. Põhiseadusliku korra kaitseks teostatav jälitustegevus Eestis. Analüüs. Põhiseaduslikkuse Järelevalve Kolleegium. 2015, lk 3. Kättesaadav:

suuremat muret, mille tulemusena on selle vajaduse rahuldamiseks vastu võetud mitmeid määrusi, millest üldine andmekaitsemäärus[12] on peamine näide Euroopa kodanike andmekaitsest, edendamaks vaadet üksikisikute, mitte suurettevõtete huvidele.[13]

Eesti Põhiseaduse[14] (edaspidi: PS) preambulist tuleneb Eesti riigi kohustus kindlustada ja arendada riiki, mis on rajatud vabadusele, õiglusele ja õigusele. Sellise riigi toimimiseks on oluline tagada stabiilne keskkond, milles isikud saavad teostada oma põhiõigusi ja vabadusi. PS-i preambulist ning §-st 14 tuleneva põhiõiguste ja vabaduste kaitse tagamise kohustuse täitmiseks peab riik kindlustama sisese ja välise rahu, tagades samas muu hulgas PS-i §-des 26, 33 ning 43 sätestatud eraelu ja kodu puutumatuse ning sõnumisaladuse kaitse.[15]

Teiselt poolt on kommunikatsiooni saladusesse sekkumine, mis on Eesti Vabariigi PS-iga enam piiratud kui sekkumine perekonna- ja eraellu, limiteeritud ning raskendab põhiseadusliku ehk julgeoleku kaitset võimaldades kommunikatsiooni saladusesse sekkuda üksnes kuriteo tõkestamiseks või tõe väljaselgitamiseks kriminaalmenetluses.[16]

Samas on julgeolek, mis põhiseaduslikus mõistes on riigi seisund, kus riigi suveräänsust ja tema põhiseaduslike institutsioonide demokraatlikku toimimist ei rikuta, tänases Euroopas teema number üks. 2022. aasta veebruaris rikkus Venemaa Ukraina demokraatlikku toimimist, alustades sõjalist agressiooni, mis tuli Euroopa Liidu riigipeadele üllatusena.

Eesti Vabariigi luureasutuste nagu Välisluureamet ja Kaitsepolitseiamet üks peamisi ülesandeid on anda riigi juhtkonnale eelhoiatus võimalikest kriisidest ning kogutud ja kinnitatud info pinnalt avada ning selgitada rahvusvaheliste sündmuste arengute, sh mõjutustegevuse, diplomaatia, energeetika ja muude valdkondade mõju riigi julgeolekule.[17] Juba 2022. aasta Välisluureameti avalikus raportis[18] oli väide: „Venemaa loob 2022. aasta veebruari teiseks pooleks tingimused ja

---

https://www.riigikohus.ee/sites/default/files/elfinder/%C3%B5igusalased%20materjalid/pkk_jlitustegevuse_anals.pdf (03.12.2022).

[12] Euroopa Parlamendi ja nõukogu 27. aprill 2016. aasta määrus EL 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). ELT 2016 L 119, lk 33.

[13] Zichichi, M.; Ferretti, S.; D'Angelo, G.; Rodríguez-Doncel, V. Data Governance through a Multi-DLT Architecture in View of the GDPR. Cluster Computing volume 25, 2022, lk 4515.

[14] Eesti Vabariigi põhiseadus. – RT I, 15.05.2015, 2.

[15] Lott, lk 3.

[16] Jaanimägi, K. Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. Sihtasutus Juridicum 2020, Laos. S § 43/20 lk 525.

[17] Eesti rahvusvahelises julgeolekukeskkonnas. Välisluureamet 2022. Kättesaadav: https://raport.valisluureamet.ee/et/eessona (13.01.2023) .

[18] Eesti rahvusvahelises julgeolekukeskkonnas. Välisluureamet 2022. Kättesaadav: https://raport.valisluureamet.ee/et/eessona (13.01.2023) .

valmisoleku, et alustada täieulatuslikku sõjalist rünnakut Ukraina vastu“ ja täpselt nii ka läks. Asjade nii täpne ennustamine tugineb paljuski põhjalikule luuretegevusele, mis tänapäeval põhineb suuresti elektroonilise side võrkudest saadaval informatsioonil ja on kirjeldatav terminiga signaalluure. Luure, eesti keeles ka teabehanke, definitsioonid on tehnoloogiaajastul jäänud paljuski samaks, kuid lisandunud on nn küberkomponent ja elektroonilised keskkonnad, kus jälgijad jälgitava teadmata toimetada saavad ilma, et jälgitaval selle kohta infot oleks.

Võttes arvesse viimase kahe aastakümne tehnoloogilisi ja sotsiaalseid arenguid elektroonilise side vallas, on Euroopa õigusinstitutsioonid leidnud, et tänapäevased sideandmed võivad avaldada palju isiklikku teavet. Samas võimaldavad need andmed võimuorganitel läbi sotsiaalsete võrgustike kaardistamise, asukoha ning interneti jälgimise luua isikust pildi ja saada ülevaade selle kohta, kellega inimene suhtleb.

Euroopa Kohus (edaspidi: EK) ja Euroopa Inimõiguste Kohus (edaspidi: EIK) on viimase kümne aasta jooksul menetlenud mitmeid isiku sideandmete kasutamise õiguslikku raamistikku puudutavaid küsimusi. Esimese olulise kohtulahendina võib välja tuua aastast 2014 pärineva *Digital Rights Ireland jt*[19], kus leiti, et julgeolekuinstitutsioonidele võimaldatakse ebaproportsionaalset sekkumist Euroopa Liidu põhiõiguste hartaga[20] tunnustatud privaatsusõigusesse. Nimetatud lahend sai ka aluseks Euroopa Liidu õigusregulatsiooni muutmisele.[21] *Digital Rights Ireland* ja ka mitmete hilisemate sideandmete kasutamist käsitlevate lahendite tulemusena on välja kujunenud EK kohtupraktika sideettevõtete poolt kogutavate andmete kasutamiseks jälitustegevuses. Ka EIK on viimastel aastatel kujundanud antud valdkonna õiguspraktikat läbi julgeoleku tagamise vajadusest lähtuvate sideandmete kogumise ja kasutamise juhtumite.

Põhinedes eelnevale on autoril tekkinud küsimus, kas riigil on õigus kasutada julgeoleku tagamisel, sh luure teostamisel, kodanike isiklikke andmeid ning põhjustada sellega inimeste privaatsuse ja eraelu puutumatuse rikkumine. Eelnevast lähtuvalt teadvustas autor magistritöö uurimisprobleemi – kas sellised väärtused nagu privaatsuse garanteerimine ja julgeoleku tagamine vastanduvad teineteisele ning kuidas on Euroopa Liidu ühises õigusruumis sätestatud regulatsioon

[19] EKo 08.04.2014, liidetud kohtuasjad C-293/12 ja C-594/12, *Digital Rights Ireland Ltd.* ECLI:EU:C:2014:238.
[20] Euroopa Liidu põhiõiguste harta. ELT C 326. 26.10.2012. Kättesaadav: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A12012P%2FTXT (26.11.2022).
[21] Tunnistati kehtetuks Euroopa Parlamendi ja nõukogu 15. märts 2006. aasta direktiiv 2006/24/EÜ, mis käsitleb üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist

üksikisiku sideandmete kasutamiseks luuretegevuse kaudu julgeolekuliste eesmärkide tagamiseks.

Seega on magistritöö eesmärgiks selgitada välja, kas demokraatia printsiipe austava ja euroopalikke põhimõtteid tunnustava Eesti Vabariigi õigusregulatsioon julgeoleku tagamisel läbi teabe varjatud kogumise ehk (signaal)luure on kooskõlas Euroopa Liidu üksikisiku sideandmete kaitse õiguspõhimõtetega?

Eesmärgi saavutamiseks püstitas autor järgmised uurimishüpoteesid:

> H1 – Eesti siseriiklik ega ka Euroopa Liidu seadusandlus ei sätesta kindlaid reegleid sideandmete säilitamiseks ja töötlemiseks signaalluure raames.
>
> H2 – Julgeoleku aspektidest tulenevalt on õigustatud kodanike elektrooniliste sideandmete privaatsuse puutumatuse riive.

Hüpoteeside paikapidavuse kontrollimiseks formuleerusid järgmised peamised uurimisvaldkonnad: privaatsusõigus, isiku elektroonilised sideandmed, turvalisus, julgeolek, teabe varjatud kogumine ehk teabehange, sh täpsemalt signaalluure.

Kuigi üldistamise huvides kasutab autor terminit isikuandmete ja teabe varjatud kogumine, mille alla liigituvad ka sellised eestikeelsed terminid nagu teabehange, luure, sh signaalluure, seire, spionaaž ning jälitustegevus, siis on antud töö raames on oluline neid eristada. Oluline on eristada ka isikuandmetega seotud mõisteid, sest EL-i alusreglementatsiooni definitsioonid erinevad Eesti õiguspraktikas kasutatavatest, mille ühe näitena võib tuua Andmekaitseinspektsiooni isikuandmete klassifikatsiooni.

Teema avamiseks püstitas autor alljärgnevad alaküsimused:

- Milline on privaatsuse mõiste ja definitsioon ning privaatsuse tagamise instrumendid Euroopa Liidus ja Eesti Vabariigis?
- Kuidas ja milliste institutsioonide tegevusega tagatakse Eesti Vabariigis julgeolek ja millised on nende institutsioonide funktsioonid, õigused ja kohustused?
- Kuidas reguleeritakse eraisikute sideandmete kaitset julgeoleku tagamise seisukohalt teabe varjatud kogumisel Euroopa Liidu ja Eesti Vabariigi seadusandluses?

Töö autorile teadaolevalt ei ole akadeemilistes uurimistöödes varem käsitletud isiku sideandmete kaitse küsimusi riigi julgeoleku tagamiseks teostatava teabe varjatud kogumise kontekstis lähtuvalt Euroopa Liidu andmekaitse regulatsioonist ning sellest tulenevat mõju liikmeriikide, sh

Eesti siseriiklikule regulatsioonile. Käsitletud on küll üksikisiku sideandmete kaitse ühtset regulatsiooni Euroopa Liidus[22] ja uuritud sideandmete kasutamise õiguspärasust, sh ka sideandmete kasutust kriminaalmenetluses, mille kohta on Eesti Riigikohtul ka Euroopa Kohtu Suurkojalt lahend[23].

Teema on keeruline, tundlik ning suuresti kaetud riigisaladuse sätetega, kuid vajab siiski demokraatlikus ühiskonnas õigusselguse huvidest kantuna mõistlikult läbipaistvat reguleeritust.

Hüpoteeside kontrollimiseks ja uurimisküsimustele vastuste leidmiseks tutvus töö autor kehtivate Euroopa Liidu sideandmete kaitse regulatsioonidega, seadusloome käigus esitatud seletuskirjade, õigusalase teaduskirjanduse ja -artiklite, rahvusvahelise kohtupraktika, praktikute ja teoreetikute õigusalaste arvamusartiklite, julgeolekuasutuste avalikult kättesaadavate ja tegevust käsitlevate analüüside, raportite, Euroopa Kohtu, Euroopa Inimõiguste kohtu ja Eesti kohtulahendite, erinevate autorite koostatud magistri- ja doktoritöödega ning muu dokumentatsiooniga. Eelnevast lähtuvalt oli empiiriliseks uurimismeetodiks kombineeritud dokumendianalüüs kohtupraktikast, seadusandlusest ja teoreetilisest kirjandusest.

Arvestades, et töö autoril puudub riigisaladuse luba, mis võimaldaks ligipääsu ametkondlikuks kasutamiseks mõeldud ning riigisaladusega kaitstud dokumentidele, siis lähtus autor töö kirjutamisel ainult avalikult kättesaadavatest allikatest. Selle kitsenduse korvamiseks pöördus autor erinevate valdkondlike ekspertide poole avamaks täiendavalt probleemsete valdkondade tagamaid ning toetamaks tööle seatud eesmärkide saavutamist ning koostas eelnevalt intervjuu küsimused. Kokku pöördus autor intervjuu saamiseks kolmeteistkümne erineva ameti ja institutsiooni esindaja poole, kellest kaheksa nõustusid intervjuu andmisega. Kolm välja valitud eksperti ei soovinud vastata tulenevalt antud teema tundlikkusest ja kaks eksperti loobusid vastamisest, sest ei pidanud ennast valdkonna eksperdiks. Tulenevalt asjaolust, et mõned eksperdid soovisid anonüümsust, siis konkreetsete ekspertide nimesid ja ametikohti antud töös välja ei tooda. Kasutatud allikmaterjalide loetelus on toodud intervjuude kuupäevad, kuid töö sisulises osas viidatakse intervjuude käigus saadud selgitustele ja põhjendustele ilma otsest allikat nimetamata. Autor tänab kõiki kaasaaitajaid, kes olid valmis selgitusi jagama, andes sellega oma suure panuse töö valmimisse.

[22] Schasmin, P. (2016); Sehver, K.H. (2017); Jõesaar, C. (2019); Antson, A (2019).
[23] EKo 02.03.2021, C-746/18 *HK vs Prokuratuur* ECLI:EU:C:2021:152.

Autor on töö üles ehitanud neljas peatükis. Töö esimene ja teine peatükk aitavad mõtestada töö peamiste uurimisvaldkondade teoreetilisi lähtekohti. Esimeses peatükis käsitleb autor privaatsusõiguse mõistet, olemust ning isikuandmete, sh elektrooniliste isikuandmete, liigitust. Töö teises peatükis keskendub autor julgeoleku mõistele ja kirjeldab seda Eesti Vabariigis tagavate asutuste olemust ja rolle. Täiendavalt avatakse mõisted jälitustegevus ja luure ning peatutakse detailsemalt luureandmete kogumiseks kasutatavatel luuredistsipliinidel ehk luuremeetoditel, sealhulgas käesoleva töö kontekstis olulisel signaalluurel. Töö kolmandas peatükis annab autor ülevaate sideandmete kasutamise õiguslikust raamistikust Euroopa Liidus ja Eesti Vabariigis. Neljanda peatüki fookuses on teabe varjatud kogumise õiguspärasus jälitustoimingute teostamise ja julgeoleku tagamise eesmärgil.

Antud töö panus ühiskonnale on eelkõige Eesti isikuandmete töötlemist käsitleva seadusandluse kitsaskohtade väljaselgitamine. Lisaks Eesti õigusruumile saab analoogia alusel teha järeldusi ja tõmmata paralleele ka muude Euroopa Liidu liikmesriikide seadusandlike aktide analüüsiga, tagamaks kooskõla Euroopa Liidu ja Euroopa Inimõiguste Kohtu seisukohtadega, Euroopa inimõiguste ja põhivabaduste kaitsekonventsiooni ning ÜRO inimõiguste ülddeklaratsiooniga.

1. PRIVAATSUSÕIGUSE JA ISIKU SIDEANDMETE OLEMUS

Üksikisiku sideandmed on osa isiku informatsioonilisest privaatsussfäärist, moodustades omakorda osa privaatsusõigusest kui ühest kompleksemast põhiõigusest. Käesolevas peatükis annab autor ülevaate privaatsusõiguse mõistest ja selle olemusest ning isikuandmete, sh elektrooniliste isikuandmete liigitusest kui töö teoreetilistest seisukohtadest.

1.1. Privaatsusõiguse ja isikuandmete olemus

1948. aastal sätestati rahvusvahelisel tasemel esmakordselt ÜRO inimõiguste ülddeklaratsiooni[24] artiklis 12 õigus eraelu puutumatusele järgnevas sõnastuses: „Kellegi era- ja perekonnaellu, kodu puutumatusse või kirjavahetusse ei tohi meelevaldselt sekkuda ega teotada kellegi au ja head nime. Igaühel on õigus saada seaduselt kaitset sellise sekkumise või teotamise korral.“ Umbes samal ajal, aastal 1950 sõnastati Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni[25] artiklis 8 eraelu puutumatuse lähtekoht järgmiselt: „Igaühel on õigus sellele, et austataks tema era- ja perekonnaelu ja kodu ning korrespondentsi saladust. Võimud ei sekku selle õiguse kasutamisse muidu, kui kooskõlas seadusega ja kui see on demokraatlikus ühiskonnas vajalik riigi julgeoleku, ühiskondliku turvalisuse või riigi majandusliku heaolu huvides, korratuse või kuriteo ärahoidmiseks, tervise või kõlbluse või kaasinimeste õiguste ja vabaduste kaitseks.“

Sellele järgnes 1966. aastal ÜRO Kodaniku- ja poliitiliste õiguste rahvusvaheline pakt[26], mille artikkel 17 ütleb kokkuvõtvalt järgmist: „… kellegi isiklikku või perekonnaellu ei tohi meelevaldselt või ebaseaduslikult vahele segada /…/ kirjavahetuse saladusele, aule ja reputatsioonile ei tohi meelevaldselt või ebaseaduslikult kallale kippuda.“

Lisaks neile nimetatud õigusaktidele kaitsevad ka mitmed rahvusvahelised juhendid ja raamistikud, näiteks Majanduskoostöö ja Arengu Organisatsiooni juhend aastast 1980, isikute eraelu puutumatust[27] eesmärgiga kaitsta ka üle piiri edastavaid isikuandmeid[28]. Peaaegu igas riigis

[24] Inimõiguste ülddeklaratsioon. ÜRO Peaassamblee. Kättesaadav: http://www.un.org/en/universal-declaration-human-rights (26.11.2023).
[25] Euroopa inimõiguste ja põhivabaduste kaitse konventsioon. – RT II 1996, 11, 34.
[26] ÜRO kodaniku- ja poliitiliste õiguste rahvusvaheline pakt. – RT II 1994, 10, 11.
[27] Solove, D. Understanding Privacy. Harvard University Press, 2010. lk 1109. Kättesaadav: https://www.perlego.com/book/1148540/understanding-privacy-pdf (26.11.2022).
[28] Organization for Economic Cooperation and Development: Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. Kättesaadav: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188 (27.11.2022).

püüavad arvukad siseriiklikud statuudid, konstitutsioonid/põhiseadused ja kohtuotsused kaitsta eraisikute privaatsust ning mitmete riikide põhiseadustes on privaatsus sätestatud põhiõigusena.[29]

Siseriiklikust aspektist lähtudes sätestab PS kõige olulisemad riigisisesed küsimused – riigi õiguskorra ja rahvusvahelise õiguse suhte, riikluse ja selle õiguskorra aluseks olevad õiguse üldpõhimõtted ning igaühe õigused ja vabadused ehk suhte inimõigustega.[30] Lisanduvad valdkonnad, mis liberaalses ja demokraatlikus õigusriigis on tavapäraselt põhiseadusliku regulatsiooni esemeks: põhiõigused, mis sätestavad avaliku võimu lubatud toimimisulatuse suhetes eraisikuga ja riigikorraldus, sh riigivõimu funktsioonid, põhiseaduslikud organid ja muud olulised allüksused ning nende pädevus.[31]

PS-i kui ühe olulisema Eesti riigi õigusakti teises peatükis on sõnastatud isikute põhiõigused, vabadused ja kohustused. PS § 26 sätestab igaühe õiguse perekonna- ja eraelu puutumatusele, nn privaatsusõiguse, mis annab kõigile õiguse seaduse kaitsele isiklikku või perekonnaellu meelevaldse sekkumise eest ning teeb seadusandjale ülesandeks kaitsta seaduse jõuga isiklikku ja perekonnaelu.[32]

PS § 26 sõnastamisel on lähtutud Euroopa Liidu põhiõiguste harta (edaspidi: harta)[33] artiklitest 7 ja 8, kus on kajastatud igaühe õigus tema era- ja perekonnaelu ning kodu, sõnumite saladuse ja isikuandmete kaitseks.[34] Sama põhimõte on sätestatud ka ÜRO kodaniku ja poliitiliste õiguste rahvusvahelise pakti artiklis 17.[35]

Inimestele pühendunud ja inimkeskses ühiskonnas tohib praktilistes konfliktiolukordades põhiõigustest kõige vähem piirata inimväärikust, mida Eesti Riigikohus[36] on nimetanud kompleksseks põhiõiguseks. Inimväärikuse elementideks on eeskätt õigus heale nimele, õigus õiguslikule võrdsusele kõigi teiste inimestega, õigus inimlikule identiteedile, informatsioonilise enesemääramise õigus, õigus kehalisele puutumatusele, õigus mitte olla hirmul enese ja oma lähedaste eksistentsi kui julgeoleku pärast.[37]

[29] www.privacy.gov.au/publications/oecdgls.doc (26.11.2022).
[30] Maruste, R. Martensi klausli idee mõjust tänapäevasele riigi- ja karistusõigusele. Inimõiguste aastaraamat 2021, lk 248.
[31] Ernits, M. Konkreetne normikontroll de *lege lata* ja de *lege ferenda*. Juridica 8/2001, lk 572.
[32] Jaanimägi, K. PSK § 26/1, lk 387.
[33] Euroopa Liidu põhiõiguste harta..
[34] Jaanimägi, lk 387.
[35] ÜRO Kodaniku- ja poliitiliste õiguste rahvusvaheline pakt. RT II 1994, 10, 11.
[36] RKKKo 26.08.1997, 3-1-1-80-97.
[37] Vallikivi, H. PSK § 19/3, lk 271.

Kuigi nimetatud õiguste kaitse ja riigi julgeoleku saavutamine ei pruugi põhimõtteliselt ega faktiliselt olla vastandlikud, siis tegelikkuses on alates 11. september 2001 (paremini tuntud kui 9/11, kui leidis aset Al-Qā'idah' terrorirünnakute seeria Ameerika Ühendriikide vastu) sõnad „inimõigused" ja „julgeolek" hakanud kollektiivses kujutluses tähistama peaaegu ületamatut vastandumist. Selle vastandumise keskmeks on dilemma, kuidas tagades julgeolekut kaitsta vabadust eiramata seejuures selle olemust ning vältides inimõiguste rikkumist?[38]

Kuigi privaatsuse mõiste on väga kompleksne ja keeruline[39], siis ulatub privaatsuse kui väärtuse tähtsus tagasi ammustesse aegadesse, kuna juba Piiblis, Vana-Kreeka kirjutistes, Muhamedi ütlustes ja juudi keeles on ära toodud privaatsuskontseptsioonid[40], mida on tunnustatud erinevates kultuurides ja erinevatel ajaloolistel perioodidel. Samas on ikka ja jälle arutluse all küsimus privaatsusesse sobivast sekkumisest, kus käsitletakse enamasti avaliku ja erasektori, riigi ja ühiskonna ning indiviidi ja ühiskonna vahelisi suhteid.[41]

Privaatsuse mõiste defineerimisel on David Solove[42] toonud välja kuus aspekti: 1) õigus olla rahule jäetud (unustatud), 2) piiratud ligipääs füüsilisele isikule, 3) saladuse hoidmine, st teiste eest varjamine, 4) kontroll isikliku informatsiooni üle, 5) õigus isikupärale, st individuaalsuse ja isiku kaitse ja 6) õigus intiimsusele.

Kesksel kohal on andmesubjekti kontroll enesekohase informatsiooni üle, mille aluseks on liberalistlik enesemääratlemise idee ehk isik on iseennast määratlev ja vaba otsustama, millised väärtused on tema jaoks olulised ning kes ja millisel määral saab juurdepääsu teda puudutavale informatsioonile ja võimaluse seda kasutada.[43]

Privaatsus on üksikisikute ja ühiskondade jaoks oluline väärtus ning eesmärk järgnevatel põhjustel: 1) privaatsus võimaldab inimestel arendada end erakorraliste isikutena, kes on vabad avalikust kontrollist ja hinnangutest; 2) privaatsus võimaldab luua suhteid teiste inimestega usalduse ja intiimsuse taseme loomise kaudu; 3) privaatsus aitab luua võrdsust, luues tingimused,

[38] Lazarus, L.; Goold, B.J. Security and Human Rights: The Search for a Language of Reconciliation. 2017. Arvutivõrgus kättesaadav: https://lawexplores.com/introduction-security-and-human-rights-the-search-for-a-language-of-reconciliation/ (26.11.2022).
[39] Murumaa-Mengel, lk 11.
[40] Denemark, R.A.; Marlin-Bennett, R. The International Studies Encyclopedia Wiley-Blackwell Print 2017, Arvutivõrgus kättesaadav: https://www-oxfordreference-com.ezproxy.utlib.ut.ee/view/10.1093/acref/9780191842665.001.0001/acref-9780191842665-e-0168?rskey=6HvpO9&result=2 (10.12.2022).
[41] *Ibidem*.
[42] Solove, D. J. Conceptualizing Privacy. California Law Review, 2002. vol 90, lk 1092.
[43] Murumaa-Mengel, lk 17.

kus igaüks saab ise otsustada, kui palju endast ja mis tingimustel avaldab; 4) privaatsus aitab luua kohti, kus inimesed tunnevad end turvaliselt ja kaitstuna, et täita ühiskonnas olulisi funktsioone.[44]

Eristada võib kolme privaatsuse sfääri: 1) informatsiooniline privaatsus (ingl *informational privacy*), 2) füüsiline või ruumiline privaatsus (ingl *physical 13rivacy)* ja 3) otsustusprivaatsus (ingl *decisional privacy*).[45] Lähtuvalt sellest, et antud magistritöö kontekstis keskendub autor informatsioonilisele privaatsusele, on alljärgnevalt toodud mõned detailsemad lähenemised sellele privaatsussfäärile.

Eesti õiguses on isiku informatsioonilise enesemääratlemise õigus tagatud läbi PS § 26 ehk läbi eraelu puutumatuse[46], mille kohaselt informatsiooniline enesemääramine tähendab igaühe õigust ise otsustada, kas ja kui palju tema kohta andmeid kogutakse ja salvestatakse. Seeläbi on eraelu kaitse üheks oluliseks valdkonnaks ka isikuandmete kaitse.[47]

Riigikohtu halduskolleegium (kohtuasi 3-3-1-3-12), on samuti märkinud, et eraelu puutumatuse riivena käsitatakse muu hulgas isikuandmete kogumist, säilitamist, kasutamist ja avalikustamist.[48] Piirangud andmetöötlusele tulenevad informatsioonilise enesemääramise õigusest, ehk PS § 19 lg 1-st, mille kohaselt on isikul võimalus ise otsustada, kas ja millises ulatuses tema enda kohta käivaid andmeid kogutakse ja salvestatakse.[49]

Õigus privaatsusele tähendab, et inimestel on õigus mitte olla jälgitav ilma vastava nõusolekuta või teadmata ning saada teavet, kui ollakse jälgimise all saamaks oma elus luua privaatseid kohti, kus neid ei jälgi ei teised isikud ega rühmad või asutused, näiteks valitsus.[50]

1.2. Isikuandmete mõiste ja kaitse elektroonilise side andmete töötlemisel

Järgnevalt käsitleb autor EL-i poolt määratletud isikuandmetega seotud põhimõisteid, mille tundmine on oluline isiku sideandmete kogumise ja töötlemisega kaasneva probleemistiku detailseks mõistmiseks.

[44] Manjikian, (26.11.2022).
[45] Murumaa-Mengel, lk 9.
[46] Mikiver. M.; Tikk, E. Informatsioonilise enesemääramise õiguse tagamise diskretsiooniotsused haldusmenetluses. Juridica 4/2005, lk 250.
[47] Jaanimägi, K. PSK § 26/24, lk 394.
[48] RKHKo 12.07.2012, 3-3-1-3-12, p 19.
[49] Jaanimägi, lk 394.
[50] Manjikian, (26.11.2022).

Isikuandmed on määratletud 1995. aastal direktiiviga 95/46/EÜ [51] (edaspidi: direktiiv 95/46) artikli 2 punktis a, mille kohaselt on isikuandmeteks igasugune teave tuvastatud või tuvastatava füüsilise isiku kohta. Tuvastatav isik on omakorda isik, keda saab otseselt või kaudselt tuvastada, näiteks isikukoodi põhjal või ühe või mitme tema füüsilisele, füsioloogilisele, vaimsele, majanduslikule, kultuurilisele või sotsiaalsele identsusele omase joone põhjal. Üldmäärus 2016/679 täiendas määratlust artikli 4 punktis 1 määratlustega nimi, asukohateave, võrguidentifikaator või geneetiline tunnus.

Isikuandmete töötlemise mõiste tuleneb direktiivi 95/46[52] artikli 2 punktist b olles iga isikuandmetega tehtav tegevus või toiming või toimingute kogum, olenemata sellest, kas see on automatiseeritud või mitte, näiteks kogumine, salvestamine, korrastamine, säilitamine, kohandamine või muutmine, väljavõtete tegemine, päringu teostamine, kasutamine, üleandmine, levitamine või muul moel avaldamine, ühitamine või ühendamine, sulgemine, kustutamine või hävitamine. Hilisem isikuandmete töötlemise üldmäärus 2016/679[53] täpsustab artikli 4 punkt 2-s isikuandmete töötlemist automatiseeritud või automatiseerimata toiminguks, lisades kriteeriumitena edastamise, levitamise või muul moel kättesaadavaks tegemise teel avalikustamise.

Õiguslikult tuleb vahet teha kolme andmekategoorial – liiklus-, asukoha- ja kliendiandmed, sest Euroopa Kohus käsitleb üksnes liiklus- ja asukohaandmeid, kuid mitte kliendiandmete säilitamist.[54]

Sideandmetena, sh ka elektroonilise side andmetena, käsitletakse kõige üldisemalt liiklus- või asukohaandmeid ja nendega seotud teavet, mis on vajalik abonendi või kasutaja kindlakstegemiseks[55]. Liiklusandmete (ingl *traffic data*) ja asukohaandmete (ingl *location data*) määratluse on toodud direktiiv 2006/24 ehk e-privaatsuse direktiivi[56] artikli 2 lg 2-s. Antud mõistete selgitused leiab direktiivi 2002/58 artiklist 2, mille punktile b vastavalt on liiklusandmed need andmed, mida töödeldakse side edastamiseks elektroonilises sidevõrgus või sellise edastamisega seotud arveldamiseks ja asukohaandmed on artikli 2 punkt c kohaselt need

[51] Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. EÜT 1995 L 281, lk 362.
[52] *Ibidem*.
[53] Määrus 2016/679, lk 32.
[54] Virks, K. Sideandmed ja nende säilitamise olulisus. Juridica 8/2018, lk 582.
[55] Direktiiv 2006/24, lk 56, artikli 2 lõige 2 punkt 1.
[56] Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatuse ja elektroonilise side direktiiv ehk e-privaatsuse direktiiv. ELT 2002 L 201, lk 520.

elektroonilises sidevõrgus töödeldavad andmed, mis näitavad üldkasutatavate elektrooniliste sideteenuste kasutaja lõppseadme geograafilist asukohta.

Sideseansi jooksul tekivad sisuandmed ja metaandmed. Sisuandmete alla kuuluvad nn ümbriku metafoori kasutades privaatsem osa teabest, st see, mis on ümbriku sees[57]. Näiteks sotsiaalmeedia kasutajakontode sisu puudutavad andmed.[58] Metaandmeteks nimetatakse enamasti teavet elektroonilise või digitaalse salvestise kohta, mis tekib ja talletatakse teenuste tarbimisel ning IT-protsesside käivitamisel väga mitmes punktis ja erinevatel tehnilistel tasemetel: 1) kasutaja enda arvuti, 2) organisatsiooni kohtvõrgu administreerija, 3) andmesides osalevad võrguseadmed, 4) internetiteenuse osutaja jpt tasemetel.[59]

Metaandmed on „andmete andmed" ehk kõik need andmed, mis ei kuulu otseselt suhtluse sisusse (kuigi piirid nende kahe vahel ei ole alati selged) nagu helistatud telefoninumbrid, kõne kestus, helistaja ja adressaadi asukoht jne[60] andmed, mida vajab sideteenuse osutaja teenuse eest arvete koostamiseks.[61]

Andmete kasutaja mõiste tuleneb direktiivi 2006/24 artikli 2 punktist b, mille kohaselt on kasutajaks juriidiline või füüsiline isik, kes kasutab üldkasutatavat elektroonilist sideteenust isiklikel või ärilistel eesmärkidel, ilma et ta oleks tingimata ise kõnealust teenust tellinud.

Eesti Riigisaladuse ja salastatud välisteabe seadus[62] (edaspidi: RSVS) § 3 punkt 8 avab mõiste andmete töötlemine järgnevalt – teabe või teabekandja koostamine, märgistamine, kogumine, hoidmine, säilitamine, vedamine, reprodutseerimine, edastamine, hävitamine, nendest väljavõtete tegemine, nendega tutvumine või muu teabe või teabekandjaga tehtav toiming, sõltumata toimingu teostamise viisist või kasutatavatest vahenditest. Andmete töötlussüsteemi mõiste on avatud § 3 punktis 9 järgnevalt – tehnilised vahendid, mida kasutatakse teabe elektrooniliseks töötlemiseks.

[57] Laos, S PSK § 43/10, lk 521.
[58] Tsemin, A.; Antson, A. Kas anonüümsed kommentaatorid saavad side andmete kasutamise regulatsiooni valguses rahulikult magada? Juridica 7/2022, lk 473.
[59] Metaandmed ja privaatsus. Juhis organisatsioonidele ja kodukasutajale seaduse rakendamisel. Andmekaitseinspektsioon 2015, lk 4.
[60] European Commission for Democracy through Law (Venice Commission), 2015, lk. 12. Kättesaadav arvutivõrgus: http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)006-e (26.11.2022).
[61] Laos, S. PSK § 43/8, lk 520.
[62] Riigisaladuse ja salastatud välisteabe seadus. – RT I, 06.05.2020, 36.

Põhinedes Eesti Andmekaitseinspektsioonile[63] jaguneb isikuandmete liigitus Eesti õiguspraktikas kolmeks. Kuigi üldmäärus 2016/679[64], mis kohaldus[65] alates maist 2018, määratleb ainult kaks isikuandmete liiki: tavalised andmed ehk teave inimese ehk füüsilise isiku kohta, millega saab teda otse või kaudselt tuvastada (nimi, isikukood, asukohateave, võrguidentifikaatorid, st andmed, mis aitavad viia füüsilise isikuni, füüsilised, füsioloogilised, vaimsed, majanduslikud, kultuurilised ja mistahes muud tuvastamist võimaldavad tunnused ja nende kombinatsioonid)[66] ja tundlikud isikuandmed, mis ei ole üldmääruses eraldi loetletud, kuid on määratletavad isiku privaatelule suuremat ohtu valmistavate andmetena, mis ei kuulu eriliiki isikuandmete loetellu. Tundlikeks loetakse samuti neid andmed, mille avaldamisega kaasneb oht elule ja tervisele, identiteedivargusele ning kaasneb varaline ja mainekahju jms. Kolmandaks liigituseks on nn eriliiki isikuandmed (varasema Eesti määratluse kohaselt delikaatsed isikuandmed), millest ilmneb rassiline või etniline päritolu, poliitilised vaated, usulised või filosoofilised veendumused või ametiühingusse kuulumine, füüsilise isiku kordumatuks tuvastamiseks kasutatavad biomeetrilised andmed (sõrmejälje-, peopesajälje- ja silmaiirisekujutised), geneetilised, samuti terviseandmed või andmed füüsilise isiku seksuaalelu ja seksuaalse sättumuse kohta[67].

Tänapäeval toimub sõnumite vahetamine valdavalt elektroonilise side kaudu, mis võimaldab signaalide edastamist ja suunamist kaabli kaudu, samuti raadio, optiliste või muude elektromagnetiliste vahenditega. Enim kasutatavateks elektroonilise side võrkudeks on andmeside-, mobiiltelefoni-, kaabellevivõrk ja elektrikaablisüsteem.[68]

Mõiste elektroonilise side võrk tuleneb Euroopa Parlamendi ja Nõukogu direktiivi EL 2018/197 11. detsember 2018, millega kehtestatakse Euroopa elektroonilise side seadustik[69] artiklist 2, mille kohaselt on selleks ülekandesüsteemid, mis võivad, aga ei pruugi põhineda püsitaristul või kesksel juhtimisel ning vajaduse korral lülitus- ja marsruutimisseadmed ja muud vahendid, sealhulgas võrguelemendid, mis ei ole aktiivsed, aga mis võimaldavad edastada signaale kaabli kaudu, raadio teel, optiliselt või muude elektromagnetiliste vahendite abil, kasutades sealhulgas satelliitvõrke, püsivõrke (ahel- ja pakettkommuteeritud võrgud, k.a internet) ja mobiilsidevõrke,

[63] https://www.aki.ee/et/eraelu-kaitse/isikuandmed-ja-tootlemine (26.11.2022).
[64] Määrus 2016/679
[65] Üldmääruse puhul on tegemist EL-i otsekohalduva õigusaktiga, kuid teatud küsimustes jäeti liikmesriikidele kaalutlusõigus riigisiseselt täpsustada, kehtestada ja säilitada üldmääruses sätestatud isikuandmete töötlemisega seotud küsimusi.
[66] Määrus 2016/279 artikkel 4 lg 1.
[67] *Ibidem* artikkel 9 lg 1.
[68] Kask, O.; Laos, S PSK § 43/2, lk 518.
[69] Euroopa Parlamendi ja nõukogu direktiivi EL 2018/197 11. detsember 2018, millega kehtestatakse Euroopa elektroonilise side seadustik (uuesti sõnastatud). ELT 2018 L 321, lk 99.

elektrikaabelsüsteeme, kui neid kasutatakse signaalide edastamiseks, raadio- ja teleringhäälinguvõrke ning kaabeltelevisioonivõrke, olenemata sellest, millist teavet nende kaudu edastatakse.

PS § 43 kohaselt on igaühel õigus tema poolt või temale posti, telegraafi, telefoni või muul üldkasutataval teel edastatavate sõnumite saladusele. Seega kaitse tõhususe eesmärgil hõlmab kaitseala kõiki sõnumi edastamise viise ja vahendeid. Õigus sõnumite saladusele tagatakse infole, mida edastatakse üldkasutataval teel, milleks on sideteenus, mida sideettevõte pakub sideteenuse turul üldistel alustel kõigile isikutele.[70] Erandeid võib kohtu loal teha kuriteo tõkestamiseks või kriminaalmenetluses tõe väljaselgitamiseks seadusega sätestatud juhtudel ja korras.[71]

EL-i põhiõiguste harta artikkel 7 kohaselt on igaühel õigus, et austataks tema era- ja perekonnaelu, kodu ja edastatavate sõnumite saladust ning artikkel 8 lg 1 omakorda sätestab füüsiliste isikute kaitse andmete töötlemisel, mida võib käsitleda ka põhiõigusena[72] järgnevalt – „igaühel on õigus oma isikuandmete kaitsele". Seda põhimõtet täiendab lg 2, kus öeldakse, et selliseid andmeid tuleb töödelda asjakohaselt ning kindlaksmääratud eesmärkidel ja asjaomase isiku nõusolekul või muul seaduses ettenähtud õiguslikul alusel.[73]

Harta artikli 52 lõikes 1 on kirjas, et „hartaga tunnustatud õiguste ja vabaduste teostamist tohib piirata ainult seadusega ning arvestades nimetatud õiguste ja vabaduste olemust. Proportsionaalsuse põhimõtte kohaselt võib piiranguid seada üksnes juhul, kui need on vajalikud ning vastavad tegelikult liidu poolt tunnustatud üldist huvi pakkuvatele eesmärkidele või kui on vaja kaitsta teiste isikute õigusi ja vabadusi".[74]

Eesti Riigikohus on leidnud, et füüsiliste isikute kaitse isikuandmete töötlemisel on käsitatav põhiõigusena[75]. Selle põhiõiguse lahutamatuks osaks on andmesubjekti õigus tutvuda isikuandmetega, mida saab piirata üksnes seadusega ning PS § 44 lg-s 3 sätestatud alustel, s.o teiste inimeste õiguste ja vabaduste /…/ samuti kuriteo tõkestamise, kurjategija tabamise või kriminaalmenetluses tõe väljaselgitamise huvides.[76] Andmesubjekti isikuandmetega tutvumise õiguse piirangud sisalduvad isikuandmete kaitse seaduse §-s 20.

[70] Kask, O., Laos, S PSK § 43/3, lk 518.
[71] *Ibidem.*
[72] RKHKo 3-3-1-84-15, 10.05.2016 p 21.
[73] Põhiõiguste harta art 8.
[74] Põhiõiguste harta art 52 lg 1.
[75] RK 3-3-1-84-15 p 21.
[76] RKHKo 3-3-1-84-15, 10.05.2016 p 21.

PS § 26 ja Euroopa inimõiguste konventsiooni (edaspidi EIÕK) artikkel 8 lg 2 kohaselt on igaühel õigus perekonna- ja eraelu puutumatusele/austamisele ning ametivõimud ei sekku selle õiguse kasutamisse muidu, kui a) kooskõlas seadusega ja kui see on b) demokraatlikus ühiskonnas vajalik[77] 1) riigi julgeoleku, 2) ühiskondliku turvalisuse või 3) riigi majandusliku heaolu huvides, 4) korratuse või kuriteo ärahoidmiseks, 5) tervise või kõlbluse või 6) kaasinimeste õiguste ja vabaduste kaitseks.

PS § 19, mille lg 1 tagab õiguse vabale eneseteostusele, on üldisem säte, mis mängib samuti rolli eraelu privaatsuse kaitsmisel.[78] Mitmed eraelu tahud, mis kuuluvad EIÕK artikkel 8 kaitse alla, on PS-s kaitstud spetsiaalsete põhiõigustega – au ja hea nimi (§ 17), kodu puutumatus (§ 33), sõnumite saladus (§ 43). Perekonna- ja eraelu üksikud tahud võivad kuuluda ka §-des 27 ja 42, samuti § 44 lg-s 2 sõnastatud põhiõiguste kaitsealasse. PS § 26 kui üldsätet tuleb kohaldada juhul, kui kaitsmist vajav erasfääri kuuluv hüve ei ole PS-s kaitstud mõne erisättega. Kui erisäte on olemas, siis tuleb kohaldada vastavat erisätet ja § 26, kui üldisem säte peab taanduma.[79]

Olles andnud ülevaate privaatsusõigusest ning seda reguleerivatest õigusaktidest, keskendub autor alljärgnevas peatükis julgeoleku olemusele, selle tagamisega tegelevatele asutustele, nende funktsioonidele ning nende funktsioonide täitmiseks kasutatavatele meetoditele, sh avab mõisted jälitustegevus, luure, seire ja luuredistsipliinid.

[77] Vajadus demokraatlikus ühiskonnas on käsitletav proportsionaalsuse testina.
[78] Jaanimägi, K. PSK § 26/5, lk 388.
[79] Jaanimägi, K. PSK § 26/14, lk 390.

2. JULGEOLEKU OLEMUS JA TAGAMISE MEETODID

Julgeolek on sotsiaalne konstruktsioon, mis on loodud läbi diskursiivse praktika ja sotsiaalse interaktsiooni.[80] Vabaduste ja turvalisuse/julgeoleku omavahelist dilemmat ning riigi tekkimist kui kompromissi inimeste individuaalsete vabaduste ja kollektiivse turvalisuse vahel, kus iga kehtestatud seadus osutub individuaalse vabaduse kontekstis piiravaks, käsitles esimesena väidetavalt Thomas Hobbes juba 16. sajandil.[81]

Tänases ühiskonnas on esile kerkinud asümmeetrilised ohud, mis ei tunne riigipiire ja mille allikad on raskesti tuvastatavad, kuid mille mõju julgeolekule on samaväärne kui traditsioonilistel julgeolekuohtudel. Eestis kui demokraatlikele printsiipidele tuginevas riigis on põhiseaduslike väärtuste tagamine enesestmõistetav. Samas on demokraatial, turumajandusel, õigusriigil ja inimõigustel põhineva väärtusruumi üleilmne mõju vähenemas, sest meid ümbritsevat ärevat keskkonda ilmestavad külmutatud relvakonfliktid, kasvav radikaliseerumine, mitmetahuline terrorism, rahvusvahelise õiguse valikuline rakendamine, riigipiiride vägivaldne muutmine, rände kasutamine hübriidse ründevahendina ning vaenulik sekkumine riikide demokraatlikesse protsessidesse ja siseasjadesse.[82]

Euroopa Liidu vahetus läheduses asub mitu ka Eesti Vabariigi julgeolekule võimalikku mõju avaldavat konfliktikollet, mis panevad proovile ka kogu maailma julgeoleku. Lisaks mõjutavad julgeolekut üha ilmsemalt majanduskeskkonna ebakindlus, organiseeritud kuritegevus ja korruptsioon ning tehnoloogia arenguga seotud ohud, sh küberruum ja selles toimuv.[83]

Enamik internetitehnoloogiaid on ühendatud omavahel kasutades poliitilisi ja kultuurilisi piire ületavaid servereid. Need tehnoloogiad pakuvad laia valikut teenuseid ja ressursse, mis on vaid ühe hiirekliki kaugusel. Sellised eelised nagu pilvandmetöötlust kasutav odav salvestusruum, kiire ühenduvus e-kaubandust kasutavate ettevõtetega ja juurdepääs valitsusasutustele on ülemaailmselt kättesaadavad sekunditega. Lisaks hüvedele pakuvad need tehnoloogiad suurepärast keskkonda sellisteks tegevusteks nagu häkkimine ja teabe vargus.[84] Toimingud digitaalses keskkonnas, mille ebasoovitava tegevuse mõju ei pruugi avalduda tingimata vahetult

[80] Kärtna, L.A. Euroopa Liidu Somaalia merepiraatluse julgeolekustamine. Tartu Ülikool 2014. lk 8.
[81] Reissar, M. Privaatsus vs turvalisus: riigiteooriate konflikt küberkuritegevuse ja tehnoloogiaajastul. Tartu Ülikool 2021. lk 15.
[82] Riigikaitse arengukava 2022 – 2023. Riigikantselei 2021. lk 8.
[83] Eesti julgeolekupoliitika alused. Lisa Riigikogu otsusele „Eesti julgeolekupoliitika alused“ heakskiitmine. - RT III, 06.06.2017, 2.
[84] Alexandrou, (29.11.2022).

ja füüsiliselt, võivad ulatuda üle riigipiiride, sest andmed võivad üheaegselt paikneda mitme riigi territooriumil ning neid on võimalik hetkega liigutada ühest asukohast või ka riigist teise, pannes nii proovile riigi suveräänsuse, jurisdiktsiooni ja küberoperatsioonide omistamist käsitlevate reeglite rakendamise. [85]

Antud peatükis keskendub autor julgeoleku mõistele ja kirjeldab seda vastavalt Eesti Vabariigis julgeolekut tagavate asutuste olemusele ja funktsioonidele. Täiendavalt avab autor teabe varjatud kogumisega seotud valdkonnad nagu jälitustegevus ja luure ning peatub detailsemalt luureandmete kogumiseks kasutatavatel luuredistsipliinidel ehk luuremeetoditel, sealhulgas käesoleva töö kontekstis olulise mõiste kesksel teemal ehk signaalluurel.

2.1. Julgeoleku olemus ja luureasutuste roll

Järgnevas alapeatükis keskendub autor mõistete julgeolek, oht ning luureasutus avamisele, et mõista nende rolli võimalikus privaatõiguse riives seoses isiku sideandmete kasutamisega.

Klassikaliselt võib julgeolekut defineerida kui vabadust hirmust, teatava muretuse või rahu seisundit[86]. Eesti keeles kasutatav mõiste julgeolek sarnaneb paljude teiste keeltega (nt saksa, inglise, prantsuse keelega) ja selle sisuks on kaitstus ohtude vastu.

Julgeoleku ese ehk õigushüve, mida julgeolek kaitseb, on kõige üldisemalt isiku (sh isiku tegevuse) ja asja seisundi kaitse.[87] Samas võib julgeolekut (ja ka turvalisust) laiemas käsitluses mõtestada kui isiku või asja või isiku positsiooni edasikestmist ehk olemasoleva seisundi kaitsena või ka kui isiku võimalust teostada oma põhiülesandeid ja täita oma põhifunktsioone ehk tegevuse kaitsena. Subjektidena võib käsitleda üksikisikut või siis indiviididest moodustunud sotsiaalset gruppi ehk kogukonda, kus kogukonnana võib mõista rahvast riigi mõistes. See omakorda toob sisse mõistena rahvuslik ja riiklik/riigi julgeolek, viies välja riigi militaarse kaitseni.[88]

Riigi julgeolek on riigi seisund, kus riigi suveräänsust ja tema põhiseaduslike institutsioonide demokraatlikku toimimist ei rikuta PS-iga vastuolus oleval viisil. Tegelik olukord, kus riigi

[85] Kaska, K.; Aasmann, L. Julgeolekuasutuste roll küberjulgeoleku tagamisel ja seda mõjutavad suundumused rahvusvahelises õiguses. Juridica 2/2020, lk 102–116, lk 108.
[86] Mälksoo, M. Akadeemilised julgeoleku-uuringud sõja ja rahu vahel. Akadeemia 2009 nr. 9, lk 1768 Kättesaadav arvutivõrgus: https://www.digar.ee/viewer/et/nlib-digar:104149/162371/page/73 (10.12.2022).
[87] Jäätma, J. Julgeoleku mõiste. Juridica 2/2020, lk 73.
[88] *Ibidem,* lk 72.

suveräänsus ja põhiseaduslike institutsioonide võime täita oma PS-st tulenevaid ülesandeid ei ole mõjutatud muul kui PS-s määratud viisil.

Põhiseaduslikku korda ohustava tegevuse ennetamiseks ja tõkestamiseks on vaja koguda ning töödelda asjakohast teavet, tõkestada vaenulikku luure- ja mõjutustegevust. Kui põhiseaduslikku korda ohustab eelkõige konstitutsiooniliste normide mittetunnustamine või nende süstemaatiline eiramine, siis riigi julgeolekut ohustab mistahes tegevus, mis on suunatud riigi säilimise ja toimimise vastu.[89]

Riigi julgeolek erineb mõistest „põhiseaduslik kord" sellegi poolest, et tegemist on tegeliku olukorraga ehk rikkumise või selle ohu puudumisega. Sõjaliste ohtude ennetamiseks ja kollektiivkaitse õigeaegseks rakendamiseks peab riigil olema toimiv luure ja eelhoiatus.[90]

Eesti Vabariigis mõistetakse julgeoleku all omariikluse ja selle järjepidevuse säilitamist ennetades ja tõkestades ohte ning vajadusel kiiresti ning paindlikult neile vastu astudes.[91] Riigi julgeoleku tagamist teostatakse läbi julgeolekupoliitika, mille eesmärgiks on kindlustada riigi iseseisvus ja sõltumatus, rahva ja riigi kestmine, territoriaalne terviklikkus, põhiseaduslik kord ja elanikkonna turvalisus, teostades seda põhiõigusi ja -vabadusi järgides ning põhiseaduslikke väärtusi kaitstes.[92] Julgeolekuasutuste tegevust ei nimetata jälitustoiminguteks, vaid laiemas plaanis võib meetmeid julgeoleku tagamiseks käsitleda kavandatava[93] kuriteo tõkestamisena.[94] Samas on riigi julgeolek põhiseaduse sätte ja vaimu kohaselt väärtus, mida saab tunnustada kui põhiõiguse piiramise legitiimset eesmärki.[95]

Ohtu defineeritakse kui isikut, süsteemi või ühiskonda kahjustada võiva sündmuse võimalikku põhjust, näiteks isik, objekt ja aine.[96] Korrakaitseseaduse[97] § 5 lg 2 kohaselt on oht olukord, kus ilmnenud asjaoludele antava objektiivse hinnangu põhjal võib pidada piisavalt tõenäoliseks õigushüve kahjustamist, kuid KorS § 1 lg 5 ei kohaldata julgeolekuasutuste tegevusele julgeolekuasutuste seadusest tulenevate ülesannete täitmisel, välja arvatud kuriteo tõkestamine. Seega hõlmavad julgeolekuoht ja korrakaitsealane oht selliseid elemente nagu 1) avalikku korda

[89] Kask, O. PSK § 129/3, lk 888.
[90] Eesti julgeolekupoliitika alused, lk 2.
[91] *Ibidem,* lk 2.
[92] *Ibidem,* lk 2.
[93] KarS järgi riigivastase.
[94] Laos, S. PSK § 43/20, lk 520.
[95] Aasa, B. Eesti Vabariigi põhiseaduse kommentaarid. Eesti Teaduste Akadeemia Riigiõiguse Sihtkapital 2022, p 104.
[96] https://xn--snaveeb-10a.ee/search/unif/dlall/dsall/oht/1 sõjanduse, julgeoleku- ja kaitsepoliitika terminibaas.
[97] Korrakaitseseaduse. - RT I, 06.08.2022, 16.

ähvardava ohu ennetamine, 2) ohukahtluse korral ohu väljaselgitamine, 3) ohu tõrjumine ja 4) avaliku korra rikkumise kõrvaldamine[98], oma olemuselt erinevat laadi.

Lääneriikide julgeolekuteenistused liigituvad kolme suuremasse gruppi: politseilist tüüpi julgeolekuteenistused[99]; luure ja riigisisese julgeolekuteenistuse ülesandeid ühendavad teenistused[100] ja politseiliste õigusteta riigisisesed julgeolekuteenistused[101] Väiksematele riikidele on omane julgeolekuliste ja politseiliste funktsioonide ühendamine.[102]

Eesti Vabariik lähtub riigikaitse laiemast käsitusest, mis koondab sõjalised ja mittesõjalised võimed, tegevused ja ressursid nii avalikust, era- kui ka kolmandast sektorist[103]. Nende rakendamise alused lõi 2016. aastal jõustunud Riigikaitseseadus[104], sätestades riigikaitse juhtimise ja planeerimise alused, mis võimaldavad riiki kaitsta ja juhtida sarnastel põhimõtetel nii rahu ajal kui ka väljaspool seda.[105]

Luureasutuste[106] tegutsevad seaduse alusel, esindades riigi valitsust ja nende peamisteks ülesanneteks on anda riigi juhtkonnale eelhoiatus kriisides, avada rahvusvaheliste sündmuste (sh mõjutustegevuse, diplomaatia, energeetika ja muude valdkondade) arengute tausta ning selgitada, kuidas need arengud mõjutavad riigi julgeolekut.[107]

Eesti Vabariigis on julgeolekuasutuste tegevuse eesmärk Julgeolekuasutuste seaduse (edaspidi: JAS) § 2 lõike 1 kohaselt „tagada riigi julgeolek põhiseadusliku korra püsimisega mittesõjaliste ennetavate vahendite kasutamise abil ning julgeolekupoliitika kujundamiseks ja riigikaitseks vajaliku teabe kogumine ja töötlemine“.[108] Antud ülesanne hõlmab riigi julgeoleku tagamist, sh teabe kogumist ja töötlust digitaalse taristu kaudu, ka küberruumist lähtuvate ohtude suhtes, millel on potentsiaal ohustada põhiseaduslikku korda või riigikaitset.[109]

---

[98] Jäätma, J. Ohutõrjeõigus politsei – ja korrakaitseõigused: kooskõla põhiseadusega. Tartu Ülikool 2015, lk 18.
[99] nt Põhjamaades, Prantsusmaal, Eestis, Lätis, Poolas, Ameerika Ühendriikides.
[100] nt Beneluxi maades, Sloveenias, Leedus.
[101] nt Saksamaa, Suurbritannia.
[102] Heldna, E. Julgeolekuasutuste kogutud informatsiooni kasutamine kriminaalmenetluses ja jagamine uurimisasutustega. Juridica 10/2016, lk 718.
[103] Eesti julgeolekupoliitika alused, lk 3.
[104] Riigikaitseseadus. – RT I, 09.08.2022, lk 18.
[105] Riigikaitseseaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu seletuskiri. Kättesaadav: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/44178720-02b2-4d30-8707-d7dcf606dcee.
[106] Eesti mõistes Kaitsepolitseiamet ja Välisluureamet.
[107] Eesti rahvusvahelises julgeolekukeskkonnas. Välisluureamet 2022. Kättesaadav: https://raport.valisluureamet.ee/et/eessona (04.12.2023).
[108] Sinisalu, S.; Virks, K. Õige vähe õige paljust ehk turvalisuse ja julgeoleku mõningatest tahkudest õiguse laia tõlgenduse kontekstis. Juridica 5/2022, lk 364–365.
[109] Kaska, K.; Aasmann, L. Julgeolekuasutuste roll küberjulgeoleku tagamisel ja seda mõjutavad suundumused rahvusvahelises õiguses. Juridica 2/2020 lk 102–116, lk 104.

JAS § 5 kohaselt on Eesti Vabariigis julgeolekuasutusteks Kaitsepolitseiamet ja Välisluureamet.[110] Kaitsepolitseiamet (edaspidi: KAPO)[111] on struktuuriliselt Siseministeeriumi valitsusasutus. Ameti ülesandeks on riigi sisejulgeoleku tagamine teabe kogumise ja ennetusvahendite kasutamise abil, süütegude uurimine Vabariigi Valitsuse määrusega[112] kehtestatud ulatuses ning meetmete rakendamine Eesti Vabariigi vastu suunatud luure- ja õõnestustegevuse ennetamiseks[113].

Ameti peamised tegevusvaldkonnad ja ülesanded on sätestatud KAPO põhimääruse[114] peatükis 2 § 7 ja 8 JAS §-is 6. JAS-i kohaselt kuuluvad ülesannete hulka: riigi põhiseadusliku korra ja territoriaalse terviklikkuse vägivaldse muutmise ärahoidmine vastavalt JAS § 6 p 1; riigi vastu suunatud luuretegevuse ennetamine ja tõkestamine JAS § 6 p 2 kohaselt (va JAS § 7 lõike 1 punktides 2 ja 3 nimetatud juhtudel); JAS § 6 p 2^1 tulenevalt terrorismi ärahoidmine ja selleks vajaliku teabe kogumine ja töötlemine; JAS § 6 p 2^2 kohaselt riigi julgeolekut ohustava korruptsiooni ärahoidmine ja tõkestamine ning selleks vajaliku teabe kogumine ja töötlemine[115]. Lisaks juba nimetatutele ka JAS § 6 p 3 kohaselt ka kuritegude tõkestamine, mille kohtueelne uurimine on KAPO pädevuses (va JAS § 7 lõike 1 punktides 2 ja 3 nimetatud juhtudel). Põhimääruse § 8-s on ülesannete loetelu detailsemalt lahti kirjutatud, kusjuures nimetatud punkt 8 viitab omakorda tagasi eelpool mainitud JAS-ile ning teabe kogumise funktsioonile.

Välisluureameti (edaspidi: VLA), mis kuulub Kaitseministeeriumi[116] valitsemisalasse, missioon on kaitsta Eesti riiki väliste julgeolekuohtude eest[117]. Välisluureameti põhimääruse § 8[118] kohaselt on ameti tegevusvaldkonnaks riigi julgeoleku ja põhiseadusliku korra tagamine, sealhulgas selleks vajaliku teabe kogumine ja töötlemine, vastuluure teostamine ning riigisaladuse ja salastatud välisteabe kaitse korraldamine ja kontrollimine. Ameti ülesanded on sätestatud määruse § 9 ning JAS §-is 5.

---

[110] Julgeolekuasutuste seadus. – RT I, 27.05.2022, 30.

[111] Kaitsepolitsei tegevuspõhimõtted ja suunad tulenevad järgnevatest raamdokumentidest: „Eesti Vabariigi põhiseadus“, „Eesti Vabariigi julgeolekupoliitika alused“, „Strateegiline ohuhinnang Eesti Vabariigi julgeolekule“, „Eesti turvalisuspoliitika põhisuunad“, „Siseministeeriumi valitsemisala ja ameti arengukavad“, „Korruptsioonivastane strateegia“, „Eesti terrorismivastase võitluse põhialused“, „Riigikaitse strateegia“, „Kriminaalpoliitika arengusuunad“.

[112] Vabariigi Valitsuse määrus. Politsei- ja Piirivalveameti ja Kaitsepolitseiameti vaheline uurimisalluvus. – RT I, 07.05.2019, 4.

[113] https://kapo.ee/et/content/ulesanded-ja-eesmargid/ (04.12.2023).

[114] Kaitsepolitsei põhimäärus. – RT I, 07.11.2014, 1.

[115] Jõustus aastal 2013.

[116] Kaitseministeeriumi põhimäärus. – RT I, 27.08.2022, 2, § 6 lg 2, p 3.

[117] Eesti rahvusvahelises julgeolekukeskkonnas. Välisluureamet 2018, lk 3.

[118] Välisluureameti põhimäärus. – RT I, 17.12.2021, 12.

Lisaks on VLA ülesanded ja pädevus on määratletud JAS § 7-s riigi julgeoleku ja põhiseadusliku korra tagamisel, milleks on: riigile välis-, majandus- ja riigikaitsepoliitika kujundamiseks ning riigikaitseks vajaliku välisriike, välismaiseid tegureid või tegevust puudutava teabe kogumine ja töötlemine vastavalt JAS § 7 lg 1 p 1-le; vastuluure teostamine riigi välisesinduste või väljaspool riigi territooriumit asuvate struktuuride kaitseks ja ka teenistujate, koostööle kaasatud isikute ja valduse kaitseks tulenevalt JAS § 7 lg 1 p 2 ja 3-st ning JAS § 7 lg 1 p 4 kohaselt elektroonilise teabeturbe ning eriside korraldamine ja kontrollimine. Viimati mainitud ülesanne on täpsemalt sätestatud Riigisaladuse ja salastatud välisteabe seaduse[119] (RVSV) § 23-s.

Kuigi julgeoleku- ja korrakaitseasutuste tegevust ühendavaks märksõnaks varjatus, siis julgeolekuasutuse eesmärgiks on leida oht, st ohtu ennetada ohutõrje ennetamistegevuse kaudu, aga korrakaitseasutuse eesmärgiks on teadaolev oht tõrjuda otsese ohutõrje abil.

Ohtude ärahoidmiseks ehk ennetamiseks, sh riigi toimimisele ohtlike kuritegude tõkestamiseks ning riigi julgeoleku tagamiseks rakendatakse erinevaid meetmeid. Nendest üheks on varjatud teabe kogumine ehk luure, mille erinevatest distsipliinidest annab autor ülevaate järgmises alapeatükis.

2.2. Varjatud andmete kogumine ja jälgimistegevus

Mõistmaks varjatud meetoditega teabe kogumise olemust on autori hinnangul oluline avada mitmed valdkonnaga seotud mõisted nagu jälgimine ehk seire; luuretegevus ja luure ehk tänapäevases mõistes teabehange ning luuretegevuste klassifikatsioon läbi luuredistsipliinide ehk luuremeetodite, mille hulka kuulub antud uurimistöö seisukohalt olulisim luuredistsipliin ehk signaalluure.

Salajased uurimismeetodid määratleti Eesti seadusandluses esmakordselt 1993. aastal, kui valitsuse määrusega kinnitati operatiivtehniliste erimeetmete rakendamise ajutine kord[120] (tunnistati 1994. aastal kehtetuks Riigikohtu põhiseaduslikkuse järelevalve kohtukolleegiumi poolt[121]).[122]

[119] Riigisaladuse ja salastatud välisteabe seadus. – RT I, 06.05.2020, 36.
[120] Riigi Kaitsepolitseiameti põhimääruse ja Operatiivtehniliste erimeetmete rakendamise ajutine kord. - RT I 1993, 53, 734.
[121] RKPJKo 12.01.1994, III-4/A-2/94.
[122] Lõhmus, U. Quo vadis, kriminaalmenetlus? Juridica 3/2020, lk 205.

Terminit jälgimine ehk seire[123] (ingl *surveillance*) kasutavad Ameerika, eelkõige USA õigussüsteemis[124] õigusteadlased, et viidata isiku- või ametialase teabe volitamata, st teadliku nõusoleku puudumiseta, kogumisele ja sellega seotud tegevustele nagu kogutud teabe volitamata avaldamine või jagamine.

Seiretegevus hõlmab endas erinevatel motiividel põhinevaid erinevat tüüpi tegevusi (vt. tabel 1), mida viivad läbi erinevad osapooled, kelleks võivad olla eraisikud, ettevõtted, rahvusriigid ja valitsusvälised osalejad. Seiret iseloomustab ka asjaolu, et seire võib olla seaduslik, ebaseaduslik või mõnel juhul ka ebapiisavalt reguleeritud.[125]

Tabel 1. Seiretegevuses osalemise motiivid[126]

Teostaja	**Motiiv**	**Tegevus**
Eraisikud	anda õiguskaitseorganitele vihjeid ja informatsiooni	sotsiaalmeedia jälgimine pärast olulise sündmuse toimumist
Ettevõtted	tagada töötajate jälgimise kaudu efektiivsus ja ettevõtte ressursside sihipärane kasutamine	töötajate tegevuse jälgimine, kasutades GPS tehnoloogiat ja elektroonilist seiret
Rahvatervise ametnikud	tagada ühiskonnas tervishoiu turvalisus	üksikisikute ja gruppide tervise jälgimine
Valitsusasutused	selgitada välja valitsusvastase tegevusega hõlmatud isikud	tarkvara kasutamine eraisikute e-kirjade ja sotsiaalmeediapostituste jälgimiseks
	üksikisikute/kodanike vastase terrorismi ennetamine	elektroonilise kommunikatsiooni jälgimiseks
	psühholoogilises „sõjas“ osalemine; vastase valimissüsteemi õõnestamine	kandidaatide ja nende meeskondade elektroonilise suhtluse monitooring
Valitsusasutused ja ettevõtted	tuvastada töötajad, kellest võib kujuneda nn sisemine oht	ettevõtte protsesse/poliitikaid eiravate ja rahulolematute töötajate tuvastamine

Allikas: Manjikan, 2017.

Seire ehk jälgimisega on tegemist ka juhul, kui valitsusasutus või ettevõte tegeleb elektroonilise valvega, omades selleks sidekanalit (juhtme- või raadiosidekanalit) ning kasutab elektroonilist, mehaanilist või muud seireseadet. Oluliseks aspektiks on see, et jälgitaval isikul võib olla

[123] Eesti õigekeelsussõnaraamat 2018 *püsikontroll, pidev millegi seisundi jälgimine.* Kättesaadav: http://www.eki.ee/dict/qs/index.cgi?Q=seire&F=A (27.11.2023).
[124] Chapter 50 of US Criminal Code, *Section 180*. Kättesaadav https://www.govinfo.gov/app/collection/uscode/2021/title50/-1 (17.11.2022).
[125] Manjikian, (26.11.2022).
[126] *Ibidem*.

põhjendatud ootus privaatsusele, mis tähendab, et teabe kogumiseks õiguskaitselistel eesmärkidel oleks üldjuhul vaja volitust ehk luba.[127]

Täiendavalt on oluline eristada terminoloogiliselt luuret, teabehanget ja jälitustegevust, millest tulenevalt toob töö autor järgnevalt välja eelpool mainitud mõistete erinevused.

Eesti Keele Instituudi militaarterminite oskussõnastikus defineeritakse luuret (ka seire, avastamine, reke ehk kohaluure) kui tegevust, mille eesmärk on vaatluse või muude avastamismeetodite abil hankida informatsiooni vaenlase või võimaliku vaenlase tegevuse ja ressursside kohta või andmeid määratud maa-ala meteoroloogiliste, hüdrograafiliste või geograafiliste näitajate kohta.[128]

Luure ehk luuramine on valitsuse ja organisatsioonide poolt igasuguse informatsiooni kogumine, mis on vajalik riigi juhtkonnale strateegiliste otsuste langetamiseks riigikaitse, välispoliitika ja majanduse vallas.[129] Luureandmed, mida enamasti kogutakse varjatult välismaal[130], sisaldavad informatsiooni, mis võib olla nii avalik kui privaatne kui ka kogutud nii avalikest kui ka salajastest allikatest või mõlema kombinatsioonist.[131]

Terminit luure (ingl *intelligence)* kasutatakse nii luuretegevuse kui ka luuretegevuse tulemi ehk luureteabe vastena, viidates samuti luurega tegelevatele organisatsioonidele järgnevalt:

- luureteave – luureandmete töötlemise ja analüüsi tulemus, mida on vaja olukorrast arusaamiseks ja otsuste langetamiseks;
- luuretegevus – tegevuskeskkonda ning vastaspoole võimeid ja kavatsusi puudutava info kogumine ja töötlemine, mille tulemiks on luureteave;
- luureorganisatsioon – luureandmete kogumise ja/või töötlemisega tegelev organisatsioon.[132]

Luureandmete kogumise meetodeid nimetatakse sageli ka luureandmete kogumise distsipliinideks või „INT"-deks (ingl *Intelligence Collection Disciplines*)[133]. Põhinedes USA luureühenduste organisatsiooni liigitusele võib INT-e liigitada, kas lähtudes

[127] Manjikian, (26.11.2022).
[128] https://sonaveeb.ee/search/unif/dlall/mil/luure/1 (15.01.2023).
[129] Purre, M. Riigireetmine ja riigireetur. Juridica 2/2020, lk 82.
[130] Heldna, lk 719.
[131] Purre, lk 82.
[132] Taktikatasandi luure käsiraamat. Eesti Kaitsevägi. 2020, lk 6.
[133] Clark. R. M. Guide to the Study of Intelligence. Perspectives on Intelligence Collection. Journal of U.S. Intelligence Studies. Association of Former Intelligence Officers. Volume No 2. 2013, lk 47–53.

kogumisfunktsioonide lähtekohast, st milline organisatsioon millist meetodit kasutab või tuginedes analüütilisele lähtekohale, mis põhineb kahel erineval informatsiooni kogumise allikal: sõnaline allikas (näiteks avatud allikad, inimluure jne) ja mittesõnaline allikas (näiteks elektrooniliste allikate luure, radarluure jne). Nende kahe kogumisallika oluline erinevus seisneb eelkõige hilisemas erinevas hinnangute andmises analüüsiprotsessi käigus, kus näiteks sõnalisel allikal põhinev meetod võimaldab hinnata kavatsusi, kuigi inimesed ühe sõnalise luure allikana võivad ka valetada, mittesõnaline aga mitte.[134]

Tuginedes rahvusvahelisele kirjandusele, Eesti sõjaajaloolase Ivo Juurvee[135] liigitusele, FBI klassifikatsioonile[136], NATO allikatele [137] ja valdkondlike ekspertide kommentaaridele võib koostada alljärgneva luuremeetodite loetelu, kus sisalduvad nii nn klassikalised ehk ajaloolised luuredistsipliinid kui ka tänastest tehnoloogia arengutest tulenevad distsipliinid:

- Inimallika luure (ingl *human intelligence* – HUMINT) on avalikkuse huvi enim köitev ja kõige tuntum luureandmete kogumise viis, mis seisneb inimeste kasutamises luuretegevuseks, sealhulgas allikate värbamises võõrriigi kodanike hulgast.
- Piltluure (ingl *imagery intelligence* – IMINT) – huvipakkuvate objektide pildistamine või vaatlus (nt laevadelt, lennukitelt, satelliitidelt, droonidelt, sh fotoaparaatide ja telefonidega tehtud pildid) ja hilisem kirjeldamine, mis sobib erinevate rajatiste kohta teabe kogumiseks ja vajadusel lahingukahjude hindamiseks.
- Avalike allikate luure (ingl *open source intelligence* – OSINT) – ajakirjanduse, kirjanduse, sh ka ametlike väljaannete ja seadusloome, foorumite, info portaalide (sh nii avalikult kättesaadavad kui ka tasulised) pidev jälgimine ja analüüs.
- Signaalluure (ingl *signals intelligence* – SIGINT) – sidevõrkude kaardistamine ja pealtkuulamine. Tänapäevases redaktsioonis on signaalluure eelkõige defineeritud kui telefonide, interneti ja raadiosignaalide jälgimine ehk varjatud jälitus[138], mis hõlmab paljuski seda, mida tänapäeval seostatakse sõnaga „küber“[139] ning valdkondlike ekspertide käsitluses teave, mille allikas on võõras elektromagnetlaine (signaal, kiirgus vms) jagunedes omakorda:

[134] Clark, R. M. lk 47-53.
[135] Juurvee, I. Riigisaladuse kaitse Eesti Vabariigis 1918–1940, lk 17.
[136] https://usnwc.libguides.com (11.01.2023).
[137] AJP 2 Allied Joint Intelligence, Counter Intelligence And Security Doctrine Detsember 2016 Edition A Version 2.
[138] Eesti rahvusvahelises julgeolekukeskkonnas. Välisluureamet 2018, lk 38.
[139] *Ibidem*, lk 54.

- sideluure (ingl *communications intelligence* – COMINT[140]) – üksikisikute telefonivestlustest, tekstisõnumitest ja erinevat tüüpi võrgusuhtlusest kogutud teave eelkõige kõne-, teksti- ja signaaliedastuste kohta;
- elektrooniline luure (ingl *electronic intelligence* – ELINT) – kajastab kaasaegsete relvade ja jälgimissüsteemide elektroonilist väljundit ja mida saab jagada omakorda veel tehniliseks (ingl *Technical ELINT* ehk *TechELINT*) ja operatiivseks (ingl *Operational ELINT* ehk *OpELINT*)[141] elektrooniliseks luureks,
- radarite luure (ingl *radar intelligence* – RADINT) – luureandmed, mida kogutakse radarite abil;[142]
- võõraste aparatuurisignaalide luure (ingl *foreign instrumentation signals intelligence* – FISINT) on seotud kosmose-, maapealsete ja maa-aluste süsteemide testimise ja operatiivse kasutuselevõtuga;[143]
- küberluure (ingl *cyber intelligence* – CYBINT) – SIGINT-i alamliik, mis sõltub riigi asutustest ja struktuurist. Näiteks tuginedes Välisluureameti käsitlusele, on signaalluure ja küberluure erinevad luuredistsipliinid[144].

- Sotsiaalmeedialuure (ingl *social media intelligence* – SOCMINT) on erinevalt eelnevatest meetoditest[145] uus meetod ning seisneb inimfaktori kasutamises (nn human intelligence – HUMINT-i tänapäevane versioon) nii passiivse tegevusena kui sekkumisena.

Eelnevat loetelu võib nimetada ka nn üksikmeetodil põhinevateks luuredistsipliinideks. Neid täiendavad järgnevad nn kombineeritud luuredistsipliinid:

- Andurluure[146] (ingl *measurement and signatures intelligence* – MASINT), mis on suhteliselt vähetuntud info kogumise distsipliin. MASINT-i defineeritakse sarnaselt relvastusoperatsioonide defineerimisele relvajõudude (näiteks maa-, õhu- ja merejõudude) vahendusel.[147] MASINT on seotud relvade võimekuse ja tööstusliku

[140] https://www.techtarget.com/whatis/definition/COMINT-communications-intelligence.
[141] Bernard, R. L. Electronic Intelligence (ELINT) at NSA. Center for Cryptologic History. National Security Agency. 2009, lk 1. Kättesaadav: https://permanent.access.gpo.gov/gpo7719/elint.pdf (22.01.2023).
[142] https://akit.cyber.ee/term/1687 (15.01.2023).
[143] https://akit.cyber.ee/term/1674 (15.01.2023).
[144] Välisluureameti aastaraamat 2018, lk 57.
[145] Juurvee, I. 100 aastat luuret ja vastuluuret Eestis. Post Factum, lk 9.
[146] Tõlge põhineb https://sonaveeb.ee/search/unif/dlall/mil/MASINT/1 (15.01.2023).
[147] Wiritz. J.J; Rosenwasser. J.J. From Combined Arms to Combined Intelligence: Philosophy, Doctrine and Operations. Intelligence and National Security. Vol. 25, No. 6, 725–743, Routledge. December 2010, lk 726.

tegevusega hõlmates õhu- ja õhusõidukite IMINT ja SIGINT kogumissüsteemidest kogutud andmete täiustatud töötlemist ja kasutamist.

- Telemeetriline luure (ingl *telemetry intelligence* – TELINT) – kasutatakse mõnikord relvade poolt katsete ajal edastatavate andmete tähistamiseks. Nii TELINT kui ka ELINT võivad olla SIGINT-i tüübid ja aidata kaasa MASINT-ile. [148]
- Georuumiline luure (ingl *geospatial intelligence* – GEOINT), mille raames tuginedes Wiritz ja Rosenwasserile [149] saadakse teavet konkreetse asukohaga seotud piltide andmete analüüsi abil.

Spionaažiks loetakse luuretegevust, mis keskendub info hankimisele küll varjatud meetoditega, kuid erineb luurest, sest on keelatud selle tegevuse objektiks oleva riigi seadustega.[150] See on protsess, mille käigus saadakse teavet, mis ei ole tavaliselt avalikult kättesaadav, kasutades inimallikaid (agendid) või tehnilisi vahendeid (nt arvutisüsteemidesse häkkimine). Spionaaž võib hõlmata ka püüdeid mõjutada otsustajaid ja arvamuskujundajaid võõrvõimu huvide kasuks.[151]

Magistritöö kirjutamise ajal läbi viidud ekspertintervjuude käigus märkis üks luurevaldkonna ekspert, et mõiste signaalluure ei ole käesoleval ajal Eestis enam sisuliselt kasutusel. Selle asemel räägitakse JAS §-des 25 ja 26 sätestatud viisil kogutud teabest, mida omakorda reguleerivad julgeolekuasutuste (KAPO ja VLA) määrused.

Enne 2003. aastat oli JAS-i § 7 lg 2 kohaselt Teabeameti (nüüdne VLA) ülesandeks koguda KAPO taotlusel KAPO pädevuse piires või kaitseväe ülesannete täitmiseks teavet elektroonilisel ehk signaalluure viisil.

2003. aastal jõustunud JAS-i redaktsioonis oli väljend „signaalluure viisil“ asendunud elektroonilisel viisil teabe kogumise väljendiga ning redaktsiooni seletuskirjas viidatakse vajadusele viia sisse muudatused ja täiendused tulenevalt Riigisaladuse ja salastatud välisteabe seadusest[152] (edaspidi: RSS) ning täpsustada normitehnilised ebatäpsused kehtivast õiguskorras (JAS/RSS), sh korrastada terminoloogiat st viia JAS/RSS kooskõlla.[153] RSS § 3 p 10 sätestab

[148] https://usnwc.libguides.com (11.01.2023).
[149] Wiritz. J.J; Rosenwasser. J.J. From Combined Arms to Combined Intelligence: Philosophy, Doctrine and Operations. Intelligence and National Security. Vol. 25, No. 6, Routledge. December 2010, lk 726.
[150] Taktikatasandi luure käsiraamat. Eesti Kaitsevägi 2020, lk 39.
[151] Purre, M. Riigireetmine ja riigireetur. Juridica 2/2020, lk 82 .
[152] Riigisaladuse ja salastatud välisteabe seadus. - RT I, 06.05.2020, 36.
[153] Riigisaladuse seaduse ja julgeolekuasutuste seaduse muutmise seadus. Seletuskiri § 2 p 1–3.

mõiste elektrooniline teabeturve – riigisaladuse või salastatud välisteabe käideldavuse, salajasuse ja terviklikkuse tagamise töötlussüsteemis.

Rootsi signaalluure agentuuri käsitluse kohaselt on signaalluure luuredistsipliin, mida algselt kasutati raadiosignaalide pealtkuulamiseks ja analüüsiks. Tänaseks on signaalluurest kujunenud üldtermin, mille alla käib elektrooniline ja sideluure. Enimkasutatavad elektroonilise side võrgud on andmeside-, mobiiltelefoni-, kaabellevivõrk ja elektrikaablisüsteem. Signaalluure erineb politsei ja korrakaitselises tegevuses kasutatavast varjatud jälgimisest selle poolest, et on ennetava iseloomuga ning tihti vähem piiritletud, samuti ei pruugi see olla suunatud ainult sisejulgeolekule. Suurel hulgal sõnumite sisu puudutavaid andmeid ning metaandmeid kogutakse eri viisidel ning analüüsitakse arvutite abil valitud kriteeriumide järgi. Filtreerimise aluseks võivad olla inimeste nimed, keeled, võtmesõnad, kommunikatsiooni teekonnad ja muud tehnilised andmed.[154]

Signaalluure võib hõlmata nn tavalise suhtluse jälgimist ja hõlmata juurdepääsu nii interneti- ja telekommunikatsioonikanalite sisule kui ka metaandmetele, kus kogutakse luureandmeid nähtuse või konkreetse isiku või rühma kohta.[155]

Erineval viisil kogutakse väga suur hulk sisu- ja metaandmeid.[156] Seejuures eristatakse masskogumist ehk automatiseeritud andmete kogumise protsessi, mille käigus saadakse väga suur hulk sideandmeid ehk side- ja metaandmeid[157] ja sihtkogumist, mis põhineb konkreetsetel faktidel ehk põhjendatud kahtlusel, on täpselt sihitud isikutele või rühmadele ning seotud otseselt kuritegevusega või rahvusliku julgeoleku küsimustega.[158]

Teabehanke mõiste tuleneb JAS § 9 lg 2 ning hõlmab riigi julgeoleku (mitte avaliku korra) seisukohast kõige ohtlikumate kuriteoliikide ennetamist veel enne kuriteo ettevalmistamise staadiumisse jõudmist. See eristab teabehanget oluliselt kriminaalmenetluse seadustikus (edaspidi: KrMS) reguleeritud jälitustegevusest. Nii kriminaalmenetluse välise (eelkõige organiseeritud kuritegevuse tõkestamiseks) kui ka kriminaalmenetluses kuriteo avastamiseks tehtava jälitustegevuse siht on siiski kurjategijate vastutusele võtmine. Teabehanke korral on tegemist haldusmenetluse eriliigiga, kus halduskohtunik lahendab ilma prokurörita küsimuse

[154] Euroopa Nõukogu, Venice Commission Report on the Democratic Oversight of Signals Intelligence Agencies, 2015. Kättesaadav: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)011-e (24.10.2021).
[155] *Ibidem*, lk 34.
[156] *Ibidem*, lk 38.
[157] *Ibidem*, lk 38.
[158] Bulk Collection of Signals Intelligence: Technical Options. Computer Science and Telecommunications. BoardNational Academy of Sciences. 2015.

isiku põhiõiguste vs riigi julgeolek ning ilma karistusõiguslikult karistatavasse staadiumisse jõudmata. Teabehange muutub jälitustegevuseks juhul, kui mingil põhjusel ei olnud haldusmenetluse ennetavad meetmed piisavad ning tarvitusele tuleb võtta tugevamalt vabadusi piirav meede ehk kriminaalmenetlus, kus isiku põhiõiguste piiramiseks annab Eestis jälitusasutusele loa maakohtu kohtunik prokuratuuri kaudu juhul, kui tegevuse eesmärgiks on tõendi hankimine süüteo toimepanemise kohta.[159]

Luure- ja jälitustegevuse erinevuse võib vastavat tegevust läbi viivate ametite lõikes tuua välja järgmiselt. Luuramise käigus kogutakse teavet varjatult peamiselt välismaal ning selle tegevuse esmaseks ülesandeks on aidata riigi juhtkonnal langetada strateegilisi otsuseid riigikaitse, välispoliitika ja majanduse valdkondades, mis on ühtlasi VLA esmane ülesanne. VLA tegevus ei ole seotud ühegi konkreetset liiki kuriteo ennetamisega ning seda tegevust ei oleks ka võimalik piirata kuriteokoosseisuga. KAPO ülesanne on nii riigi sees iseseisvalt teabehanke käigus hangitud info alusel kui ka muu hulgas VLA hangitud teabe alusel ennetada julge oleku ohte ja viia vajadusel läbi kriminaalmenetlus juba toimunud, riigi julgeolekut ohustava kuriteo avastamiseks, mida ei õnnestunud ennetada. Seega on KAPO ja VLA tegevus suunatud eri ülesannete täitmisele.[160]

Globaliseerumisprotsesside ja interneti loomise tulemusena ei ole enam kerge eristada sise- ja välisturvalisuse ohte. Tulenevalt sellest on luure järelevalve üks olulisemaid arenguid viimastel aastatel olnud asjaolu, et signaalluure ei ole enam seotud ainult sõjalise ja välisluurega, vaid puutub teatud määral kokku ka sisejulgeoleku valdkonnaga. Eelnevast tulenevalt võib signaalluure nüüdsest hõlmata ka tavalise telekommunikatsiooni jälgimist, mida nimetatakse seireks ja millel on oluliselt suurem potentsiaal mõjutada individuaalseid inimõigusi ja põhjustada privaatsusõiguse riivet.[161]

Järgnevas peatükis keskendub magistritöö autor sideandmete kasutamisele süütegude tõkestamisel *versus* julgeoleku tagamisel ning sellest tulenevale võimalikule privaatsusõiguste riivele.

[159] Heldna, lk 720.
[160] *Ibidem,* lk 719.
[161] Venice Commission, lk 3.

3. SIDEANDMETE KASUTAMISE ÕIGUSLIK RAAMISTIK

Kui eelnevates peatükkides keskendus autor privaatsuse kontseptsiooni, julgeoleku olemuse, luureditstipliinide ning julgeolekuasutuste eesmärkide avamisele, siis käesolevas peatükis käsitleb autor Euroopa Liidu õiguslikku raamistikku, Euroopa Kohtu (EK) ja Euroopa Inimõiguste Kohtu (EIK) seisukohti ning praktikat ja Eesti Vabariigi seadusandlust isikuandmete kasutamise õiguspärasuse tagamiseks ning nende tõlgendamist julgeoleku tagamise eesmärgil.

Selleks, et paremini mõista varjatud teabe kohumise erinevust jälitustoiminguga kuritegude avastamiseks ja julgeoleku tagamiseks käsitleb töö autor ühe alapeatükina ka Elektroonilise side seadust (edaspidi: ESS) ja sellega volitatud tegevusi andmepäringute osas.

3.1. Euroopa Liidu õiguslik raamistik ja praktika üksikisiku sideandmete kasutamiseks

Kuni 2018. aasta maikuuni oli peamiseks õigusaktiks EL-is andmekaitse vaates Euroopa Parlamendi ja Nõukogu 24. oktoobri 1995. aasta direktiiv 95/46/EÜ[162] (direktiiv 95/46) üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumine, millega loodi EL-is terviklik andmekaitsesüsteem. Selle õigusakti kohaldamisalaks oli eelkõige siseturg ning see oli pigem seotud muude ametiasutuste kui õiguskaitseasutuste tegevusega.

2009. aastal algasid ELi andmekaitse eeskirjade ajakohastamise vajaduse arutelud ning eelnevast lähtuvalt võeti 2016. aastal vastu isikuandmete kaitse üldmäärus 2016/679, mis on liikmesriikides otsekohalduv alates 25. maist 2018, kui tühistati varasem andmekaitsedirektiiv. Kuigi isikuandmete kaitse üldmäärus on vahetult kohaldatav, siis siiski eeldati, et liikmesriigid ajakohastavad oma olemasolevaid riiklikke andmekaitseseadusi, et viia need määrusega täielikku vastavusse, kuid kajastades ka kaalutlusruumi. Nii direktiivi 95/46 kui ka üldmääruse 2016/679 reguleerimisalasse ei kuulunud õiguskaitseasutustes isikuandmete töötlemist reguleerivad eeskirjad.

[162] Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta, EÜT 1995 L 281.

2008. aastal lahendati see küsimus EL-i nõukogu raamotsusega 2008/977/JSK[163] kriminaalasjades tehtava politsei- ja õigusalase koostöö raames töödeldavate isikuandmete kaitse kohta. Samas jäi selle õigusakti kohaldamisalast välja riigisisene isikuandmete töötlemine õiguskaitseasutustes.

Olukorra lahendas direktiiv Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta direktiiv (EL) 2016/680, 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[164] (edaspidi: direktiiv 2016/680) ja mis tunnistas kehtetuks raamotsuse 2008/977/JSK, tunnistades avaliku julgeolekuga seotud andmetöötluse eripära ja sätestades ka andmekaitse erieeskirjad kriminaalasjades tehtava õiguskoostöö ning politseikoostöö valdkonnas.[165]

Arvestades telefoni-, mobiilside, interneti- ja digitaalteenuste arengust ning vajadust kasutajate õigust eraelu puutumatusele ja konfidentsiaalsuse austamisele nn elektroonilise side sektoris, sätestati direktiiv 2002/58/EÜ[166], milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (nn eraelu puutumatuse ja elektroonilise side direktiiv ehk e-privaatsuse direktiiv).[167]

EK, kes on pädev otsustama, kas liikmesriik on täitnud ELi andmekaitseõigusaktidest tulenevaid kohustusi, ja tõlgendama ELi õigusakte, et tagada nende mõjus ja ühtne kohaldamine kõigis liikmesriikides[168] on viimase pea kümne aasta jooksul menetlenud isikuandmete säilitamise ja neile juurdepääsu eelotsusetaotlusi. Neist otsustest on kujunenud elektroonilise sideandmete õigusloome seisukohast olulised tähised. Järgnevalt käsitleb autor olulisemaid otsuseid ajalises järjestuses.

Juba 2014. aastast on pärit töös varasemalt mainitud kohtuotsus, mida tuntakse nimega *Digital Rights Ireland* jt, millega tunnistati kehtetuks direktiiv 2006/24, kuna leiti, et see võimaldab

[163] Nõukogu raamotsus 2008/977/JSK kriminaalasjades tehtava politsei- ja õigusalase koostöö raames töödeldavate isikuandmete kaitse kohta, ELT 2008 L 350.
[164] Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta direktiiv (EL) 2016/680, 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, ELT L 119, 4. mai 2016.
[165] Euroopa andmekaitseõiguse käsiraamat (2018)Euroopa Liidu Põhiõiguste Amet ja Euroopa Nõukogu 2020, lk 31–33.
[166] Direktiiv 2002/58.
[167] Euroopa andmekaitseõiguse käsiraamat. lk 34–35.
[168] *Ibidem*, lk 36.

ebaproportsionaalset sekkumist Euroopa Liidu põhiõiguste harta artiklitega 7 ja 8 tunnustatud õigustesse.

2016. aastal järgnes kohtuotsus *Tele2 Sverige ja Watson* jt[169], milles tõlgendati direktiivi 2002/58 artikli 15 lõiget 1 koostoimes artiklitega 7 ja 8 ning aastast 2018. pärineb kohtuotsus *Ministerio Fiscal*[170], kus samuti käsitleti ja kinnitati direktiivi 2002/58 artikli 15 lõike 1 tõlgendust ehk koostoimet harta artiklitega 7 ja 8.

2020. aastal järgnesid kohtuotsused *La Quadrature du Net* jt C-511/18 ja C-512/18 ja *Privacy International*. C-623/17. Samasse aastasse kuulub kohtuotsus Ordre des barreaux francophones et germanophone jt C-520/18, kus on kättesaadav kohtujuristi ettepanek, kuid mitte kohtuotsus.

Eelmisel 2022. aastal lisandusid G.D C-140/20 (Iirimaa) ja liidetud kohtuasjad *VD ja SR* (Prantsusmaa) C-339/20 ja C-397/20, kus isikuandmete töötlemist ja eraelu puutumatust elektroonilise side sektoris käsitleti taas lähtuvalt harta artiklitest 7, 8 ja 11 ning artikli 52 lg 1-st.

Kõigis eelpool nimetatud kohtuasjades on eelkõige probleemiks direktiivi 2002/58 kohaldamine riigi julgeoleku ja terrorismivastase võitlusega seotud tegevustele ning liikmesriikide õigus piirata eraelu puutumatust, mida vastav direktiiv kaitseb,[171] mis on ka antud uurimustöö keskseks probleemiks, ehk kas riigi julgeoleku kaalutlustel on õigustatud üksikisiku sideandmete kogumine, töötlemine/kasutamine.

Harta artiklites 7, 8 ja 11 tunnustatud õiguseid lubab harta artikli 52 lg 1 nende õiguste teostamisel piirata, tingimusel, et piirangud on ette nähtud seaduses, arvestavad nimetatud õiguste olemust, on proportsionaalsuse põhimõtte kohaselt vajalikud ja vastavad tegelikult EL poolt tunnustatud üldist huvi teenivatele eesmärkidele või vajadusele kaitsta teiste isikute õigusi ja vabadusi.[172]

Seega direktiivi 2002/58 artikli 15 lõike 1 tõlgendamine lähtuvalt hartast eeldab, et võetakse arvesse ka harta artiklites 3[173], 4[174], 6[175] ja 7[176] tunnustatud õiguste olulisust ning seda, milline

[169] EKo 21.12.2016, liidetud kohtuasjad C-203/15 ja C-698/15, *Tele2 Sverige AB* ECLI:EU:C:2016:970.
[170] EKo 02.10.2018, C 207/16, *Ministerio Fiscal,* ECLI:EU:C:2018.
[171] EKo 22.06.2021 C-718/19. *Ordre des barreaux francophones et germanophone,* ECLI:EU:C:2021:505, kohtujurist M. C. Sànchez-Bordona. Ettepanek.
[172] EKo 06.10.2020, liidetud kohtuasjad C-511/18, C-512/18 ja C-520/18. *La Quadrature du Net,* ECLI:EU:C:2020:791.
[173] Õigus isikupuutumatusele.
[174] Piinamise ning ebainimliku või alandava kohtlemise või karistamise keeld.
[175] Õigus vabadusele ja turvalisusele.
[176] Era- ja perekonnaelu austamine.

tähtsus on riigi julgeoleku kaitse ning raske kuritegevuse vastu võitlemise eesmärkidel, mis aitavad kaasa teiste isikute õiguste ja vabaduste kaitsele.[177]

Isikuandmete kaitse üldmääruse 2016/679 kohaldamisala erandeid, mis on ette nähtud selle määruse artikli 2 lõikes 2, punktis d „…määrust ei kohaldata, kui isikuandmeid töötlevad pädevad asutused süütegude tõkestamise, uurimise, avastamise või nende eest vastutusele võtmise ja kriminaalkaristuste täitmisele pööramise, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmise ja nende ennetamise eesmärgil“ tuleb pädevate asutuste poolt tõlgendada kitsalt[178] ning vastavalt määruse põhjendusele 19 eeskätt süütegude tõkestamisel ja avastamisel

Liikmesriigid võivad anda pädevatele asutustele direktiivi 2016/680 tähenduses muid ülesandeid, mida ei täideta tingimata süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmise ja ennetamise eesmärgil. Muudel eesmärkidel toimuv isikuandmete töötlemine niivõrd, kuivõrd see on liidu õiguse kohaldamisalas üldmäärus 2016/679kohaldamisalasse.

Pädevateks asutusteks loeb direktiiv 2016/680 artikli 3 punkt 7-ga defineeritult:
a) avaliku sektori asutus, kes on pädev süütegusid tõkestama, uurima, avastama või nende eest vastutusele võtma või kriminaalkaristusi täitmisele pöörama, sealhulgas kaitsma avalikku julgeolekut ähvardavate ohtude eest ja neid ohte ennetama, või
b) muu asutus või üksus, kes teostab liikmesriigi õiguse kohaselt avalikku võimu süütegude tõkestamise, uurimise, avastamise või nende eest vastutusele võtmise ja kriminaalkaristuste täitmisele pööramise, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmise ja nende ennetamise eesmärgil.

Üldmääruse 2016/679 artikkel 23 lõike 1 kohaselt võib seadusandliku meetmega piirata artiklites 12–22 ja artiklis 34, samuti artiklis 5 sätestatud kohustuste ja õiguste ulatust, kuivõrd selle sätted vastavad artiklites 12–22 sätestatud õigustele ja kohustustele, kui selline piirang austab põhiõiguste ja -vabaduste olemust ning on demokraatlikus ühiskonnas vajalik ja proportsionaalne meede, et tagada a) riigi julgeolek; b) riigikaitse; c) avalik julgeolek; d) süütegude tõkestamine, uurimine, avastamine ja nende eest vastutusele võtmine või kriminaalkaristuste täitmisele pööramine, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmine ja nende

[177] C-511/18, *La Quadrature du Net,* p 122.
[178] EKo 21.06.2022 C-817/19, *Ligue des droits humains vs Conseil des ministres*, ECLI:EU:C:2022:491, p 70.

ennetamine (punktid e kuni j, mida artikkel 23 sätestab jäävad hetkel välja toomata, sest ei ole seotud käesoleva uurimistöö valdkonnaga).[179]

Kohtuasjas *Privacy International* (seostuvad ka lahendid *Digital Rights Ireland* jt, *Tele2,)* leidis EK, et direktiivi 2002/58 artikli 1 lõiget 3, artiklit 3 ja artikli 15 lõiget 1 tuleb lähtuvalt Euroopa Liidu Liitumisleping artikli 4 lõikest 2 tõlgendada nii, et selle direktiivi kohaldamisalasse kuuluvad liikmesriikide õigusnormid peavad võimaldama riigivõimu kandjal panna elektroonilise side teenuste osutajatele riigi julgeoleku kaitsmise eesmärgil kohustus edastada julgeoleku- ning luureteenistustele liiklus- ja asukohaandmeid.[180]

Samas lahendis (*Privacy International)* leidis EK, et direktiivi 2002/58 artikli 5 lõikes 1 sätestatud keeld sidet ja sellega seotud liiklusandmeid salaja pealt kuulata hõlmab elektroonilise side teenuste osutajate poolt liiklus- ja asukohaandmete mis tahes viisil kättesaadavaks tegemist avaliku võimu asutustele, näiteks julgeoleku- ja luureteenistustele, ning nimetatud andmete säilitamist nende asutuste poolt, olenemata sellest, kuidas neid andmeid hiljem kasutatakse.[181]

Elektroonilise side vahendite kasutajatel on põhimõtteliselt õigus eeldada, et nende side ja sellega seotud andmed jäävad anonüümseks ja neid ei salvestata, kui nad ei ole selleks oma nõusolekut andnud[182], kuid artikli 15 lõige 1 lubab liikmesriikidel teha erandeid direktiivi artikli 5 lõikes 1 ette nähtud põhimõtetest ja kohustusest tagada isikuandmete konfidentsiaalsus ja sellele vastavatest kohustustest /…/ kui selline piiramine on demokraatlikus ühiskonnas vajalik, otstarbekas ja proportsionaalne meede selleks, et tagada riigi julgeolek, riigikaitse ja avalik julgeolek või kuritegude või elektroonilise sidesüsteemi volitamata kasutamise ennetamine, uurimine, avastamine ja kohtus menetlemine. Selleks võivad liikmesriigid muu hulgas võtta seadusandlikke meetmeid, millega nähakse ette andmete säilitamine piiratud aja jooksul, kui see on mõnel nimetatud põhjusel õigustatud, kuid samas on oluline, et erand neid andmeid salvestada muutuks reegliks.[183]

2002/58 artikli 15 lõike 1 kolmandast lausest lähtub, et liikmesriikidel on lubatud kehtestada selle direktiivi artiklites 5, 6 ning 9 ette nähtud õigusi ja kohustusi piiravaid seadusandlikke meetmeid ainult juhul, kui see on kooskõlas liidu õiguse üldpõhimõtetega ning proportsionaalsuse

[179] EKo 06.10.2020 C-623/17, *Privacy International vs Secretary of State for Foreign and Commonwealth Affairs*, ECLI:EU:C:2020:790, p 14.
[180] *Ibidem,* p 40.
[181] *Ibidem,* p 58.
[182] *Ibidem,* p 57.
[183] C-623/17*, Privacy International,* p 58–59.

põhimõttega[184] ning need peavad olema sätestatud seaduses.[185] Side ja sellega seotud liiklusandmete konfidentsiaalsuse põhimõttest kõrvalekaldumise kord demokraatlikus ühiskonnas peab olema „vajalik, otstarbekas ja proportsionaalne“ ning vastavalt direktiivi põhjendusele 11 isegi „rangelt“ proportsionaalne kavandatud eesmärgiga.[186]

Vastavalt EK väljakujunenud praktikale on eraelu puutumatuse põhiõiguse kaitsmiseks nõutud, et isikuandmete kaitse erandid ja piirangud piirduksid sellega, mis on tingimata vajalik. Peale selle ei tohi üldisest huvist lähtuvat eesmärki taotledes jätta võtmata arvesse, et see peab olema kooskõlas põhiõigustega, mida meede puudutab. Seega on oluline saavutada tasakaal nimetatud eesmärgi ning asjasse puutuvate huvide ja õiguste vahel.[187]

Proportsionaalsuse nõude järgimiseks peavad õigusaktis olema ette nähtud selged ja täpsed reeglid, mis reguleerivad asjaomase meetme ulatust ja kohaldamist ning kehtestatud miinimumnõuded, millest tulenevalt on isikutel, kelle isikuandmetega on tegu, piisavad tagatised, mis võimaldavad nende andmeid tõhusalt kaitsta kuritarvitamise ohu eest. See õigusakt peab olema riigisiseses õiguses õiguslikult siduv ja sisaldama, millistel asjaoludel ja tingimustel võib selliste andmete töötlemist meedet rakendada, tagades seeläbi, et riive piirdub sellega, mis on tingimata vajalik. Selliste tagatiste olemasolu on veel vajalikum, kui isikuandmeid töödeldakse automatiseeritult ja kui sellega kaasneb suur oht, et neile andmetele pääsetakse juurde ebaseaduslikult.[188]

EK väljakujunenud praktika kohaselt on liiklus- ja asukohaandmete edastamine kolmandale isikule harta artiklitega 7 ja 8 tagatud põhiõiguste riive, olenemata sellest, kuidas neid andmeid hiljem kasutatakse.[189] Artikliga 7 kaitstud põhiõiguse korral tuleb liiklus- ja asukohaandmete edastamist julgeoleku- ja luureteenistustele pidada eriti raskeks riiveks[190], sest suure koguse liiklus- ja sideandmete ning nende andmega kaasneda võidava tundliku teabe säilitamine võib kujutada endast ohtu kuritarvitamisele ja õigusvastasele juurdepääsule.[191]

Samas on ELL artikli 4 lõikes 2 sätestatud, et riigi julgeolek jääb iga liikmesriigi ainuvastutusse. See vastutus tugineb esmatähtsale huvile kaitsta riigi põhifunktsioone ja ühiskonna põhihuve ning

[184] *Ibidem,* p 60.
[185] *Ibidem,* p 65.
[186] *Ibidem,* p 66.
[187] *Ibidem,* p 67.
[188] *Ibidem,* p 68.
[189] *Ibidem,* p 70.
[190] C-623/17*, Privacy International,* p 71.
[191] *Ibidem,* p 73.

hõlmab erinevate tegevuste, näiteks terrorism, ennetamist ja mahasurumist, mis võivad tõsiselt destabiliseerida riigi põhilisi põhiseaduslikke, poliitilisi, majanduslikke või sotsiaalseid struktuure. Seda eriti juhul, kui need kujutavad endast otsest ohtu ühiskonnale, elanikkonnale või riigile kui sellisele.[192] Riigi julgeoleku tagamine on tähtsam, kui direktiivi 2002/58 artikli 15 lõikes 1 nimetatud teised eesmärgid, sealhulgas eesmärk võidelda üldiselt kuritegevuse ja ka raske kuritegevusega või kaitsta avalikku julgeolekut. Eesmärk kaitsta riigi julgeolekut võib seega eeldusel, et järgitakse muid harta artikli 52 lõikest 1 tulenevaid nõudeid, põhjendada meetmeid, mis toovad kaasa raskemaid põhiõiguste riiveid.[193]

Seega peavad juurdepääsu liiklus- ja asukohaandmetele reguleerivad liikmesriigi õigusnormid lähtuma objektiivsetest kriteeriumidest, et määratleda asjaolud ja tingimused, mille esinemise korral saab riigi pädevatele ametiasutustele anda juurdepääs kõnealustele andmetele.[194] EK on seisukohal, et õigusnormid, mis võimaldavad andmeid üldiselt ja vahet tegemata avaliku võimu asutustele edastada, tähendavad üldise juurdepääsu andmist.[195] Juhul, kui siseriiklikud õigusnormid panevad elektroonilise side teenuste osutajatele kohustuse teha julgeoleku- ja luureteenistustele liiklus- ja asukohaandmete üldise ja vahet tegemata edastamise teel kättesaadavaks tegemise, väljub see piiridest, mis on tingimata vajalik ja seda ei saa pidada demokraatlikus ühiskonnas põhjendatuks.[196]

Kohtujuristi ettepanekut[197] andmete avamiseks, töötlemiseks ja säilitamiseks lähtuvalt riikliku julgeoleku tagamise vajadusest direktiivis 2002/58 arvesse võetud kahes vaates. Ühelt poolt on see liikmesriikide kõikide riigi julgeolekuga seotud tegevuste direktiivi kohaldamisalast väljajätmise alus. Teiselt poolt on see direktiiviga 2002/58 ette nähtud õiguste ja kohustuste piiramise aluseks ning rakendatav seadusega eraõigusliku või kaubandusalase tegevuse suhtes, mis ei ole seotud era- või äritegevusega ning mis ei kuulu võimulolija tegevuse valdkonda. Seega võti direktiivi 2002/58 artikli 1 lõikes 3 ette nähtud välistamise piiritlemiseks on see, et seda ei kohaldata tegevuse suhtes, mida teostavad enda nimel avaliku võimu organid riigi julgeoleku tagamiseks, nõudmata eraõiguslike isikute koostööd ja seega kehtestamata neile kohustusi nende ettevõtluse juhtimiseks.

[192] *Ibidem,* p 74.
[193] *Ibidem,* p 74.
[194] *Ibidem,* p 78.
[195] *Ibidem,* p 80.
[196] C-623/17*, Privacy International,* p 81 – põhjendatuks nagu nõuab direktiivi 2002/58 artikli 15 lõige 1, tõlgendatuna ELL artikli 4 lõike 2 ning harta artiklite 7, 8 ja 11 ning artikli 52 lõike 1 alusel.
[197] EKo 06.10.2020 C-623/17*, Privacy International vs Secretary of State for Foreign and Commonwealth Affairs,* ECLI:EU:C:2020:790, kohtujuristi M. Sànchez-Bordona ettepanek, p 77 ja 79.

Loetelu avaliku võimu organite tegevustest, mille puhul on tehtud isikuandmete töötlemise üldisest korrast erand, tuleb tõlgendada ainult kitsalt. Mõistet „riigi julgeolek", mis jääb vastavalt ELL artikli 4 lõikele 2 iga liikmesriigi ainuvastutusse, ei või laiendada teistele sektoritele, mis on avalikule elule rohkem või vähem lähedased.[198] Sellisel piiritlemisel saab lähtuda raamotsusest 2006/960/JSK, milles eristatakse ühelt poolt õiguskaitseasutusi laias mõttes, mis on muu hulgas „riiklik politsei-, tolli- või mõni teine asutus, mida siseriiklike õigusaktidega on volitatud avastama, ennetama ja uurima süütegusid või kuritegelikku tegevust ning kasutama oma volitusi ja võtma sunnimeetmeid selliste tegevuste puhul", ja teiselt poolt „asutusi või üksusi, mis tegelevad eelkõige riikliku julgeoleku küsimustega".[199]

Direktiivi 95/46 ja direktiivi 2002/58 puhul on oluline järjepidevus kaitse eesmärgis, sest kummagi eesmärk ei ole kaitsta põhiõigusi selles konkreetses valdkonnas, milles liikmesriikide tegevus ei „kuulu liidu õiguse reguleerimisalasse".[200] Direktiivi 2002/58 põhjenduse 11 kohaselt on riikide pädevus julgeoleku valdkonnas ainult juhul, kui nad teostavad pädevust otse ja oma vahenditega. Seevastu juhul, kui isegi kui tegemist on riigi samade julgeoleku kaalutlustega, kuid abiks on vaja eraõiguslikke isikuid, kellele pannakse teatavad kohustused, siis tähendab see sisenemist EL õiguse ehk direktiivi 2002/58 ja üldmäärus 2016/679 reguleerimisalasse, mille eesmärgiks on eraõiguslikelt isikutelt nõutav eraelu puutumatuse kaitse.[201]

Lisaks EK-le on üksikisiku sideandmete kasutamise temaatikat käsitlenud ka EIK, kus viimased lahendid *Centrum för Rättvisa v. Sweden*[202], *Big Brother Watch and Others*[203] ning *Ekimdzhiev and Others v. Bulgaria*[204] käsitletavad sideandmete massjälgimist ja töötlemist luure valdkonnas ning eristavad sellise tegevust kriminaalmenetluses isikustatud jälitustoimingute teostamisest. Luure eesmärgiks on riigi julgeolekule kohaste ohtude tuvastamine, mistõttu on see laiema ulatusega ning eeldab kõrgemat salastatust pikema perioodi vältel.[205]

EIK hiljutises kohtuasjas *Centrum för Rättvisa*[206] ning sellega analoogses kohtuasjas *Big Brother* Watch[207] tõdeti, et sideandmete hankimine hulgi pealtkuulamise teel võib seega olla sama riivav,

[198] C 623/17, *Privacy International*, kohtujurist ettepanek M. Sànchez-Bordona, p 80.
[199] *Ibidem,* p 82.
[200] *Ibidem,* p 84.
[201] *Ibidem,* p 85.
[202] EIKo 25.05.2021, nr 35252/08 *Centrum för Rättvisa v. Sweden.*
[203] EIKo 25.*05.2021, nr 58170/13, 62322/14, 24960/15 Big Brother Watch and Others v. The United Kingdom.*
[204] EIKo 11.01.2022 nr 70078/12, *Ekimdzhiev and Others v. Bulgaria*.
[205] https://www.vm.ee/uudised/inimoiguste-kohus-selgitas-sideandmete-massjalgimisele-signaalluure-kontekstis-kohalduvaid.
[206] EIKo 35252/08, *Centrum för Rättvisa*, p 256.
[207] EIKo *58170/13, Big Brother Watch,* p 342.

kui side sisu hulgi omandamine, mistõttu tuleb nende pealtkuulamist, säilitamist ja otsimist ametiasutuste poolt analüüsida samade kaitsemeetmete alusel, mida kohaldatakse sisu suhtes.[208]

EIK seisukohtadele põhinedes on signaalluure režiimide hindamine keeruline, sest tänapäeval toimub peaaegu kogu suhtlus digitaalses vormis ning läbi globaalsete sidevõrkude, kasutades kiiremaid ja odavamaid võimalusi ning osutamata suurt tähtsust riigipiiridele. Nii on mitteisikustatud jälgimisel väga lai ulatus nii riigi sees kui ka väljaspool riiki. Erinevalt kriminaalmenetluses kasutatavast isikustatud jälgimisest kasutatakse välisluures riigi julgeoleku tagamise eesmärgil eelkõige massjälgimist. EIK leidis, et arvestades ohte (näiteks ülemaailmne terrorism, narkokaubandus, inimkaubandus, laste seksuaalne ärakasutamine jne), mille eest riigid peavad oma elanikkonda kaitsma ning seda, et nendes tegudes osalevad isikud kasutavad suhtluseks internetti ja püüavad jälgimist takistada kasutades kõrgetasemelist tehnoloogiat, on riikidel lai kaalutlusõigus otsustamaks, milline süsteem on vajalik riigi julgeoleku tagamiseks.[209]

Kohtuasjas *Centrum för Rättvisa*[210] hindas EIK jälgimise õiguspärasust ning leidis, et õiguspärasuse määratlemisel peab arvesse võtma isikustatud jälgimise puhul rohkem kriteeriume kui ainult EIK poolt varasemalt sätestatud „*Weberi* kuus kaitsemeedet“, mis lähtuvad printsiipidest „seaduslik” ja „vajadusel” nagu on selles valdkonnas väljakujunenud lähenemisviis.[211]

Weberi kuus kriteeriumit pärinevad ajast, mil tehnoloogia kasutamine inimeste suhtlusvahendina tänasest erinev. Omavaheline kommunikatsioon on tänaseks suundunud võrku, mis võimaldab olulisemalt suuremal määral ja teistsuguses kvaliteedis sideandmete tekkimist ning seega tuleb sideandmete massjälgimisel ja isikustatud jälgimisel kohaldada kaasaegseid põhimõtteid.[212]

---

[208] EIKo nr 70078/12, *Ekimdzhiev and Others,* p 394–395.

[209] https://www.vm.ee/uudised/inimoiguste-kohus-selgitas-sideandmete-massjalgimisele-signaalluure-kontekstis-kohalduvaid.

[210] *Centrum för Rättvisa* suhtleb igapäevaselt üksikisikute, organisatsioonide ja ettevõtetega Rootsis ja välismaal e-posti, telefoni ja faksi teel. Suur osa sellest suhtlusest on eraelu puutumatuse seisukohast eriti tundlik, sest organisatsioon täidab oma ülesandeid valitsusvälise organisatsioonina, mis kontrollib riigi osalejate tegevust, usub ta, et on oht, et tema sidet on pealt kuulatud ja kontrollitud signaalluure abil.

[211] EIKo 04.12.2015, nr 47143/06, *Roman Zakharov v. Russia*, p 236 ja EIKo 18.05.2010, nr 26839/05, *Kennedy vs the United Kingdom*, p 155.

[212] EIKo 35252/08, *Centrum för Rättvisa*, p 225.

EIK tõi sisse uute oluliste kaitsemeetmetena aspekti, et siseriiklik regulatsioon peab olema määratlenud ka sõltumatud järelevalveasutused koos volituste loeteluga ning sõltumatu järelkontrolli organi kõrvalekallete tuvastamiseks.[213]

Eelnevale põhinedes võib kokkuvõtvalt esitada kriteeriumid, millele siseriiklik regulatsioon nii sideandmete kui ka sideandmetega seotud andmete massjälgimise teostamiseks peab vastama, järgnevalt:

1. süütegude loetelu, mille korral on isikute lubatud varjatud isikuandmete kogumine;
2. isikute ringi määratlemine, kelle puhul on lubatud varjatud isikuandmete kogumine;
3. piirangud jälitustegevuse kestvusele;
4. kogutud andmetega tutvumise/uurimise, kasutamise ja säilitamise kord;
5. ettevaatusabinõud andmete edastamisel teistele isikutele;
6. jälitustegevusega saadud andmete kustutamise või hävitamise kord;[214]
7. sõltumatu järelevalveasutuse määramise kord ja volituste loetelu;
8. *ex post* järelkontrolli määratlemine ja volituste defineerimine.

Harta artikkel 8 riive on põhjendatud, kui on kohaldatud kõiki eelpoolmainitud kaitsemeetmeid. See tähendab, et siseriiklikul tasandil tuleb igas protsessi etapis hinnata meetmete vajalikkust ja proportsionaalsust, määratleda toimingu eesmärk ja ulatus, taotleda sõltumatu asutuse luba, kohaldada järelevalve ning *ex post* kontrollimeetmed.[215]

Kohtuasjas *Centrum för Rättvisa* oli tegemist massjälgimisega EIK möönis, et tulenevalt tehnoloogia arengust, tuleb sideandmete massjälgimise hindamisel kohandada tavalisele isikustatud jälgimisele kohaldatavaid põhimõtteid. Massjälgimise puhul on küll ühelt poolt suur oht kuritarvitusteks, kuid teisalt suurem vajadus salastatuse järele. EIK nõustus, et isikustatud jälgimisel ja massjälgimisel on palju erisusi, kus massjälgimine on suunatud piiriülesele suhtlusele, mida ei ole võimalik kontrollida muul viisil. Erinev on ka andmete kogumise eesmärk, kus isikustatud jälgimist kasutatakse kuritegude uurimisel, massjälgimist eelkõige välisluures, et hoida ära küberrünnakuid, spionaaži ja terrorismi. Kuigi ka massjälgimine võib olla suunatud konkreetsetele isikutele, ei jälgita sellisel juhul nende isikute seadmeid, vaid nendeni jõutakse massandmetele valikukriteeriumide kohaldamisel.[216]

---

[213] *Ibidem,* p 275.
[214] *Ibidem,* p 249.
[215] EIKo *58170/13, Big Brother Watch,* Legal summary, p II.
[216] https://www.vm.ee/uudised/inimoiguste-kohus-selgitas-sideandmete-massjalgimisele-signaalluure-kontekstis-kohalduvaid.

Süütegude ja isikute loetelu ja põhjendatud kahtluse kriteerium ei ole ka EIK-i hinnangul välisluured lihtsasti määrateltavad lihtsasti määratletavad, kuid ülejäänud – jälgimise tähtaeg, andmete uurimise, kasutamise ja säilitamise kord, andmete jagamisel võetavad ettevaatusabinõud ja andmete kustutamise või hävitamise tingimused on ka massjälgimise e luuretegevuse korral asjakohased.[217]

Siinkohal tähendab kvaliteetne õigusloome seda, et siseriiklik õigus ei pea olema mitte ainult selle kohaldamisel juurdepääsetav ja ettenähtav, vaid ka tagama, et salajasi jälgimismeetmeid rakendatakse ainult juhul, kui see on demokraatlikus ühiskonnas vajalik ning eelkõige sätestades piisavad ja tõhusad kaitsemeetmed ning tagatised kuritarvitamise vastu.[218]

EIK seisukoht on, et ka kuritegude ärahoidmisel ja avastamisel peab kommunikatsiooniandmete töötlemine olema vältimatult vajalik selle eesmärgi saavutamiseks ja seadus peab määratlema tingimused, mis õigustavad konkreetse ohu tõrjumiseks konkreetsete isikute sõnumite saladuse riivet, mitte aga lubama sekkumist määratlemata hulga inimeste kommunikatsiooniandmetesse.[219]

Käesolev uurimistöö kontrollib Eesti õiguskorra vastavust eelmainitud EIK kohtulahenditega formuleeritud järeldustele peatükis 4.2.

3.2. Eesti Vabariigi õiguslik raamistik üksikisiku sideandmete kasutamiseks

Alates maist 2018 on Eestis isikuandmete kaitse õiguses keskne roll üldmäärusel 2016/679, mis loob üldised raamid isikuandmete töötlemisele. Eesti siseriiklikuks õigusaktiks on Isikuandmete kaitse seadus (edaspidi IKS), mis tulenevalt üldmäärusega antud diskretsioonist, täpsustab ja täiendab üldmääruse küsimusi ulatuses, milles liikmesriikidele on vastav õigus antud.

Uue IKS-iga võeti üle Euroopa Parlamendi ja Nõukogu direktiiv 2016/680, 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. Ühtlasi tunnistati kehtetuks nn „õiguskaitseasutuste direktiiv“ ehk nõukogu raamotsus 2008/977/JSK2.[220]

[217] *Ibidem.*
[218] EIKo 04.12.2015, nr 47143/06, *Roman Zakharov v. Russia.*
[219] Laos, S. PSK § 43/25, lk 528.
[220] Isikuandmete kaitse seaduse eelnõu. Seletuskiri, lk 3 Kättesaadav: https://www.aki.ee/sites/default/files/dokumendid/reform/iks_sk_21.03.18.pdf.

IKS-i üheks eesmärgiks oli ka üle võtta nn õiguskaitseasutuste direktiiv, mis kehtestab andmekaitsereeglid politsei ja teiste pädevate asutuste tegevusele väljaspool piiriülest koostööd. Need kohalduksid politsei ja teiste pädevate asutuste tegevusele ning olid varem reguleeritud lisaks IKS-ile menetlusseadustikes sätestatud eranditega. Võrreldes varasema raamotsusega on direktiivi kohaldamisala laiem, hõlmates kogu andmetöötlust pädevate asutuste poolt juhul, kui selline andmetöötlus leiab aset asutuste põhiülesannete täitmise raames.[221]

Sarnaselt isikuandmete kaitse üldmääruse reguleerimisalaga jääb IKS-i reguleerimisalast välja isikuandmete töötlemine järgneval kolmeks grupiks koondatud põhjusel: põhiseaduslike institutsioonide ülesannete täitmine; Kaitseväe ja Kaitseliidu tegevus riigi sõjalisel kaitsmisel ja selle ettevalmistamisel ning Kaitseministeeriumi ja Riigikantselei tegevus riigi sõjalise kaitse planeerimisel; julgeolekuasutuste tegevus riigi julgeoleku tagamisel, mis seisneb eelkõige teabehanke raames isikuandmete töötlemises.[222]

Seega antud uurimistöö kontekstis, mis on suunatud julgeoleku tagamise funktsiooni täitmisele, ei kohaldu IKS ega isikuandmete kaitse üldmäärus 2016/679.

13. detsember 2018 algatati ka IKS-i rakendamise seaduse (IKSrs)[223] eelnõu, millega tehti muudatusi 126 seadusesse viimaks need vastavusse isikuandmete kaitse üldmäärusega 2016/679 ja ühtlustada neid õiguskaitsevaldkonna direktiiviga 2016/680.[224]

Isikuandmete töötlemise seisukohast oli oluliseim aspekt, kuidas avalik võim töötleb isikuandmeid. Tulenevalt PS § 26 on isikuandmete kaitse oluline osa põhiõigusest perekonna- ja eraelu kaitsele ning igaühe õigusest vabale eneseteostusele, kuhu võib sekkuda üksnes seaduses sätestatud juhul ja korras tervise, kõlbluse, avaliku korra või teiste inimeste õiguste ja vabaduste kaitseks, kuriteo tõkestamiseks või kurjategija tabamiseks, sest igaühe õigust vabale eneseteostusele tuleb rakendada kooskõlas seaduse ning teiste inimeste õiguste ja vabadustega.[225]

IKSrs eelnõu menetlemise raames käsitleti järgmisi peamisi küsimusi[226]: avaliku võimu eesmärk töödelda isikuandmeid ja isikuandmete töötlemise põhjendatus, sh kas isikuandmete töötlemise eesmärgid on piisavalt selged; isikuandmete töötlemise ulatus ning selle vastavus minimaalsuse põhimõttele, st minimaalne vajalik ulatus avaliku võimu soovitava eesmärgi täitmiseks ja

[221] *Ibidem,* lk 4.
[222] *Ibidem*, lk 4.
[223] Isikuandmete kaitse seaduse rakendamise seadus. – RT I, 13.03.2019, 2.
[224] IKSrs seletuskiri. Sissejuhatus.
[225] *Ibidem*.
[226] Isikuandmete kaitse seaduse eelnõu. Seletuskiri. Sissejuhatus.

töötlemise ulatuse põhjendatus; andmete töötlemise tähtajad tulenevalt eesmärgipärasusest ja minimaalsest vajalikkusest ning arhiveerimine ja kustutamine.

Muudetavate seaduste hulka kuulusid muude õigusaktide seas ka julgeolekuasutuste seadus ja kriminaalmenetluse seadustik.

2004. aastal võeti vastu Elektroonilise side seadus[227] (edaspidi ESS), mis jõustus 2005 ja mida on tänaseks väga mitmeid kordi muudetud. ESS sätestab valdkondlikult vajalikud mõisted vastavalt: § 2 p 5 elektroonilise ehk side ettevõtja[228], § 2 p 6 elektroonilise side teenus[229], § 2 p 8 elektroonilise side võrk[230] jm. Lisaks mõistetele toodi välja nõuded üldkasutatavatele elektroonilise side võrkudele ja teenustele, kontaktandmete otseturustuseks kasutamisele, raadioside pidamisele, raadiosageduste ja numeratsiooni haldamisele ja raadioseadmele ning ka valdkondlikule järelevalvele.

Justiitsministeerium seaduseelnõu ettevalmistajana oli veendumusel, et ESS on kooskõlas Euroopa Parlamendi ja Nõukogu üldmäärusega 2016/679.[231] Lisaks ESS-ile on isikuandmete kaitse valdkond „tihedas seoses menetlusseadustike ning isikuandmete kaitse üldregulatsiooniga. Näiteks sideandmete säilitamise regulatsioon ei käsitle reaalajas toimuvat andmetöötlust (nt hädaabinumbrile helistaja positsioneerimine, abivajaja asukoha tuvastamine ilma hädaabikõneta jt) ega jälitustegevuse raames teostatavaid toiminguid. Lisaks ei puuduta sideandmete säilitamise reeglid sõnumi sisu, vaid üksnes sideseansiga seotud metaandmeid“.[232]

Andmete turvalisuse ja kaitse on avatud peatükis 10, kus § 102 sätestab sideettevõtja andmekaitse üldpõhimõtted. Vastavalt § 102 lg 1-le on sideettevõtja kohustatud hoidma saladuses kõiki talle sideteenuse osutamise käigus teatavaks saanud andmeid kliendi ja teiste isikute kohta, kes ei ole sõlminud lepingut sideteenuse osutamiseks, ent kes kasutavad sideteenust kliendi nõusolekul ning seda nii: 1) sideteenuse kasutamise üksikasjade kohta; 2) sõnumi sisu ja vormi kohta; 3) sõnumi edastamise aja ja viisi kohta. Lõige 2 kohaselt võib eelpool mainitud andmeid avaldada üksnes

[227] Elektroonilise side seadus. – RT I, 27.02.2022, 3.
[228] … on isik, kes osutab lõppkasutajale või teisele üldkasutatava elektroonilise side teenuse osutajale üldkasutatavat elektroonilise side teenust.
[229] … on kokkulepitud tingimustel elektroonilise side võrgu kaudu osutatav teenus, milleks on internetiühenduse teenus, isikutevahelise side teenus või muu teenus, mis seisneb tervikuna või peamiselt signaalide edastamises, kuid mis ei ole meediateenus.
[230] vt lk 16.
[231] Elektroonilise side seadus. Seletuskiri. Sisukokkuvõte.
[232] Elektroonilise side seaduse ja sellega seonduvalt teiste seaduste muutmise eelnõu väljatöötamiskavatsus (sideandmete säilitamine ja kasutamine) Eelnõu 31.10.2018.

kliendile ja kolmandale isikule ka kliendi nõusolekul, va ESS §-des 112, 113, 114^1 ja 114^2 juhtudel.

2008. aastal täiendati ESS-i §-dega 111^1, 112^1 ja 114^1 ning muudeti §-e 112 ja 113 ning sätestati sideandmete säilitamise ja edastamise kohustus, mille kohaselt peavad telefoni- ja mobiiltelefoniteenuse ning telefonivõrgu ja mobiiltelefonivõrgu teenuse osutajad ehk sideettevõtjad säilitama ühe aasta jooksul kõik teenuse kasutajate sideandmed.

Üheks olulisemaks §-iks kujunes § 111^1, mis ilma oluliste muudatusteta sisaldab direktiivi artiklites 5, 6, 7 ja 12 sõnastatut, kuid erinevalt direktiiviga ettenähtust avardas Eesti seadusandja sideandmete töötlemise eesmärki ja kasutusala,[233] võimaldades § 111^1 lg 11-s avaliku võimu asutustel st loetletud õiguskaitse-, julgeoleku-, jälitus- ja järelevalveasutustel juurdepääsu ESS § 111^1 lg 2 ja 3 kohaselt säilitatud andmetele sideteenuse kohta. § 111^1 lg 11 sätestab kohustuse need andmed edastada järelpärimise korral paragrahvis loetletud õiguskaitse, julgeoleku, jälitus- ja järelevalveasutustele.

ESS § 112 sätestab omakorda, et kui § 111^1 lg 11 loetletud/nimetatud asutused esitavad järelepärimise, siis on sideettevõtja kohustatud kiireloomuliste järelepärimiste puhul esimesel võimalusel, kuid hiljemalt kümne tunni möödumisel ja muudel juhtudel kümne tööpäeva jooksul järelepärimise saamisest arvates, kui nimetatud tähtaegade järgimine on järelepärimise sisust tulenevalt võimalik, andma järelepärimise teinud asutusele teavet ESS § 111^1 lg 2 ja 3 nimetatud andmete kohta. Tulenevalt ESS § 112 lg 3-st peab tagama jälitus- ja julgeolekuasutustele ning Politsei- ja Piirivalveametile Politsei ja piirivalve seaduses sätestatud alusel mobiiltelefonivõrgus kasutatavate terminalseadmete asukoha tuvastamise (nn positsioneerimine) reaalajas.[234] ESS § 113 aga volitab jälitus- või julgeolekuasutusele juurdepääsuks sidevõrgule vastavalt jälitustoimingu teostamiseks või sõnumi saladuse õiguse piiramiseks.

2013. aastal muudeti nn jälituspaketi raames ESS-i ning § 106 lg 3-e ning varasemast määratlusest, kus vastavalt ESS § 112 toodud jälitus- või julgeolekuasutuse järelpärimisele antav teave sai laiema määratluse ning uues redaktsioonis jäi vaid „… § 112 kohaselt esitatud järelepärimised ja antud teave …“. Alates 2013. aastast ei ole sideandmete päring enam jälitustoiming ning on sätestatud eraldi KrMS § 90^1-ga.[235]

[233] Lõhmus, U. Elektroonilise side metaandmete säilitamise ja kasutamise saaga uued peatükid Juridica 3/2021, lk 168.
[234] Laos, S PSK § 43/8, lk 520.
[235] Intervjuu seadusloome eksperdiga.

Muudeti ka ESS § § 111^1 lg 11-t, kus algsele sätestatutele, et andmeid „edastatakse ainult jälitus- või julgeolekuasutusele, Finantsinspektsioonile ja kohtule“, muutus volitatud asutuste ring laiemaks. Käesolevaks hetkeks on ESS § § 111^1 lg 11-ga andmepäringuid tegema volitatud institutsioonide ja ametite ring väga lai, hõlmates uurimis- ja jälitusasutusi, erinevaid kohtuinstantse, järelevalveasutusi ja ameteid.

Aastal 2018 pöördus Eesti Riigikohtu kriminaalkolleegium samas kohtuasjas EK poole eelotsuse saamiseks kohtumäärusega1-16-6179.[236] Märtsis 2021 jõudis Euroopa Kohtu Suurkoda kohtuasjas H.K vs Prokuratuur[237] otsuseni, et Eesti riigisisesed õigusnormid on vastuolus direktiivi 2002/58 artikli 15 lõiget 1 koostoimes harta artiklitega 7, 8 ja 11 ning artikli 52 lõikega 1, mis võimaldavad ametiasutustele kuritegude ennetamise, uurimise, avastamise ja kohtus menetlemise eesmärgil juurdepääsu liiklus- või asukohaandmete kogumile, millest võib saada teavet elektroonilise side vahendi kasutaja sideseansside või tema kasutatavate lõppseadmete asukoha kohta ja teha tema eraelu kohta täpseid järeldusi, ilma et see juurdepääs piirduks menetlustega, mille eesmärk on võitlus raske kuritegevuse vastu või avalikku julgeolekut ähvardava suure ohu ärahoidmine, ning seda sõltumata sellest, millise ajavahemiku kohta on andmetele juurdepääsu taotletud, ning selle ajavahemiku kohta kättesaadavate andmete hulgast ja liigist. [238] direktiivi 2002/58 artikli 15 lõiget 1 koostoimes harta artiklitega 7, 8 ja 11 ning artikli 52 lõikega 1 tuleb tõlgendada nii, et sellega on vastuolus riigisisesed õigusnormid, mis annavad prokurörile, kelle ülesanne on juhtida kohtueelset kriminaalmenetlust ja vajaduse korral esindada hilisemas menetluses riiklikku süüdistust, pädevuse anda ametiasutusele kriminaaluurimise läbiviimiseks liiklus- ja asukohaandmetele juurdepääsu luba.[239]

Tulenevalt eeltoodud EK otsusest algatati 2021. aasta mais KrMS-i muudatus. Võrreldes varasemalt kehtiva õigusega lisandus, et kohus peab sideandmete päringute tegemiseks luba andes võtma arvesse kuriteo raskust ja laadi, st sideandmete päringu loa saamiseks peab prokuratuur kõigepealt tegema põhistatud taotluse kohtule. Taotluse põhjal peab olema võimalik tuvastada, et sideandmete päring on vältimatult vajalik kriminaalmenetluse eesmärgi saavutamiseks ning kohus hindama, kas loa andmine on kuriteo raskust ja laadi arvestades põhjendatud ja ega sellega ei

[236] EKKKm 12.11.2018 1-16-6179.
[237] C-746/18 *HK vs Prokuratuur.*
[238] C-746/18, *H.K. vs Prokuratuur,* p 45.
[239] C-746/18, *H.K. vs Prokuratuur*, p 59.

riivata põhjendamatult isiku õigusi. Kui kohus otsustab loa anda, siis on loal ka täpne kuupäevaline ajavahemik, mille kohta on lubatud päring teha.[240]

Lisaaspektina oli käsitluse all ka nn raske kuriteo, kui tänaseni määratlemata õigusmõiste ja sellele definitsiooni ehk määratluse leidmine.[241] Advokatuuri esindaja oli seisukohal, et menetletav KrMS-i muudatus on puudulik lahendus, sest probleem ei ole mitte ainult selles, kes lube väljastab (varasemalt prokuratuur ja uues redaktsioonis kohus) ja mis on raske kuritegu, vaid selles, et sideandmeid üldse kogutakse (mis oli ka Riigikohtu seisukoht) ja kellel on kehtiva seadusandluse kohaselt õigus sideandmete päringute taotlusi teha. Samas oli prokuratuuri esindaja seisukohal, et uue redaktsiooniga lahendatakse EK lahendis välja toodud prokuratuuri lubade andmise probleemi ning laiema õiguse päringute tegemiseks ja sideandmete kogumiseks saab edasi lükata.

Seega 2021 jõustunud redaktsiooni kohaselt saab sideandmeid kriminaalmenetluses kasutada üksnes kohtu loal. Seadusesse lisati ka kuritegude loetelu, mille menetlemisel on võimalik sideandmete kohta päringuid teha. Need muudatused vähendavad oluliselt sideandmete kasutamist kriminaalmenetluses. Tulenevalt rakendatud muudatustest ja EK lahenditest on väidetavalt sideandmete kasutamine ka vähenenud.[242]

Justiitsministeeriumi seisukoht oli, et kui sideandmete säilitamise kohustus üldse ära kaotada, siis nimetatud sätet, mille järgi sideandmete päringuid saab teha üksnes kohtu loal, on ikkagi vaja, sest sideteenuse osutajad säilitavad teatud andmeid enda otstarbeks. Nende andmete kasutamine kriminaalmenetluses ei ole ebaseaduslik, küll aga on nende andmete kasutamiseks vajalik kohtu kontroll. Seega, annab säte võimaluse küsida kriminaalmenetluses välja neid sideandmeid, mis on tekkinud sideettevõtete äritegevuse käigus, mida ei ole spetsiaalselt säilitatud riigi poolt sätestatud säilitamiskohustuse täitmiseks ja mille säilitamine ei ole olnud ebaseaduslik. Nn sihistatud sideandmete säilitamise puhul tuleb sideettevõtjate seisukohast põhjalikult kaaluda, milline see peaks olema reaalselt tehniliselt teostatav andmete kogumise lahendus.[243]

Kuigi väga mitmed institutsioonid (EK, RK) ja õigusteadlased on seisukohal, et ESS on § 111[1] on vastuolus EL sideandmete säilitamise ja kasutamise aluspõhimõtetega, ei viidud 2021 detsembris jõustunud ESS-i redaktsioonis sisse kooskõla tagavaid muudatusi. Seisuga 2023 märts

[240] Riigikogu õiguskomisjoni istungi protokoll nr 95, 17.05.2021.
[241] Riigikogu õiguskomisjoni istungi protokoll nr 98, 03.06.2021.
[242] Riigikogu õiguskomisjoni istungi protokoll nr 104, 13.09.2021.
[243] *Ibidem.*

peab töö autor tõdema, et jätkuvalt kestab olukord, mille tõi aastatel 2016 ja 2021 esile Uno Lõhmus, et pigem on valitud EK otsuste jälgimise põhimõte.

Ka seadusandja ise on seaduseelnõu seletuskirjas märkinud, et ESS regulatsiooni kohaldamisala ja eesmärgid on oluliselt laiemad kui ülevõetava direktiivi eesmärk, mis on suunatud raskete ning organiseeritud kuritegude vastu võitlemisele. ESS aga kehtestab võimalused vastava teabe kasutamiseks näiteks väärteomenetluses, mis ei lähtu algsest direktiivi eesmärgist, et andmeid kasutataks ainult raskete kuritegude menetlemiseks.[244]

Nii nagu U. Lõhmusega aga juba aastal 2016 kommenteeris ja ka hiljem esitas küsimuse, siis kas ja millised argumendid õigustavad eraelu puutumatuse ja andmekaitse õiguse nõrgemat kaitset Eesti Vabariigis võrreldes EK kommunikatsiooni liiklus- ja asukohaandmete säilitamise ja neile juurdepääsu tagamise regulatsioonidega.[245]

Ühe võimaliku põhjusena tõi Lõhmus seda valdkonda mõned aastad hiljem kajastades, et eesmärgiks võis olla soov võita võimalikult palju aega süütegude avastamiseks ja uurimiseks konkreetsete riigiasutuste muude ülesannete täitmise arvelt. Samas leiab see aset põhiõiguste kaitse arvelt. Autori hinnang on sarnane U. Lõhmuse seisukohaga, et seaduse muutmisega viivitamist on võimalik õigustada mõnda aega vajadusega, et saada suurem selgus, kuidas tõlgendada liidu õigusloomet ning lootes määruse vastuvõtmisele, mis alandaks metaandmete säilitamise ja riigiasutustele kättesaadavaks tegemise nõudeid.[246] Samas on see ootus kestnud juba piisavalt kaua ning vajab siiski nüüdseks riigipoolset õiguslikku sekkumist, et tagada demokraatiale iseloomulik ja vajalik õigusselgus.

Antud seisukoht sai kinnitust ka käesoleva uurimistöö raames valdkondlike ekspertidega läbi viidud intervjuude käigus, kus Eesti siseriikliku seadusloome eest vastutavate institutsioonide eksperdid möönsid, et kehtiv ESS vajab üle vaatamist, kuid hetkel puudub arusaam, kuidas saavutada olukord, kus ühest küljest oleks tagatud riigi julgeolek ja teisest küljest sideettevõtjate klientide privaatsus. Kehtib seisukoht, et kuna, EK-s on menetluses mitmeid eelotsuste taotlusi,

[244] Elektroonilise side seaduse ja sellega seonduvalt teiste seaduste muutmise eelnõu väljatöötamiskavatsus (sideandmete säilitamine ja kasutamine). Kättesaadav: https://eelnoud.valitsus.ee/main/mount/docList/947260b9-64e7-4190-9319-32ecac6e6f83#DX0ym4oy. (18.02.2023.)
[245] Lõhmus, U. Repliik. H. Kalmo. Põhiseaduse Põkkumine Euroopa Liidu põhiõiguste Hartaga. Juridica 4/2016, lk 293.
[246] Lõhmus, U. 2021, lk 168.

siis jälgitakse ELi institutsioonide vastavaid arenguid, kuni nii sideandmete säilitamise kui ka kasutamise ja lubatud kohaldamisala osas täpsema selguseni jõudmiseni.

Töö autori arvates, on mõistetav soov oodata EK-lt võimalikult palju asjakohaseid lahendeid, kuid kui juba väga mitmetes kohtulahendites aastate jooksul on formuleeritud vastuolud liidu alusregulatsiooniga ja ka Eesti siseriiklikud instantsid on vastuoludest teadlikud, millele lisandub Riigikohtu kriminaalkolleegiumi 18.06.2021 otsus[247], kus tõdetakse ESS-i vastuoluEuroopa Liidu direktiivi 2002/58 artikli 15 lõikega 1 ning seni kuni Eesti õigus ei ole Euroopa Liidu õigusega kooskõlla viidud, ei saa ilma õigusliku aluseta säilitatud sideandmeid kriminaalmenetluse eesmärkidel kasutada.

[247] Riigikogu õiguskomisjoni istungi protokoll 07.12.2021 ja RKKKo nr 1-16-6179.

4. ISIKUANDMETE KOGUMINE RIIGI JULGEOLEKU TAGAMISEKS

Käesolevas peatükis keskendub töö autor varjatud teabe kogumisele, mille alla liigitub ka signaalluure. Varjatud meetoditega kogutakse teavet mitte ainult teabehankes luuretegevust läbi viies, vaid ka kriminaalmenetluses kuritegude avastamise eesmärgil jälitustegevuses. Käesolevas töös kuritegude avastamiseks jälitustegevuse läbimiimiseks sideandmete kasutamisel ei peatuta, Eestis kehtivast regulatsioonist ja selle kitsaskohtadest sai antud lühiülevaade eelnevas peatükis.

4.1. Varjatud teabe kogumise meetodid

Varjatud teabe kogumise meetodid ja vahendid on sätestatud JAS-is, mille § 28 kohaselt sätestab, kas sise- või kaitseminister minister need määrusega, mis esitatakse Riigikogu julgeolekuasutuste järelevalve komisjonile[248] teadmiseks.

Nendeks määrusteks on:

- Kaitsepolitseiameti poolt teabe varjatud kogumisel kasutatavad meetodid ja vahendid ning teabetoimiku pidamise ja säilitamise kord;[249]

KAPO saab piirata isiku õigusi sõnumi saladusele tulenevalt määruse §-ist 1 kasutades telegraafi, telefoni või muu tehnilise sidekanali kaudu (või muul viisil) edastatava sõnumi või muu teabe pealtkuulamist, -vaatamist või salvestamist vastavate tehniliste vahendite või kohaldatud tehnoloogiate abil. Kodu, perekonna või eraelu puutumatuse õiguse piiramine on lubatud tulenevalt määruse § 2 p 4-st, kasutades selleks andmete kogumist elektroonilise side võrgu kaudu edastatavate sõnumite fakti, kestuse, viisi ja vormi ning edastaja või vastuvõtja kohta.

- Välisluureameti poolt teabe varjatud kogumisel kasutatavad meetodid ja vahendid.[250]

Nimetatud määruse § 2 p 6 annab VLA-le volitused elektroonilise side võrgu kaudu edastatava sõnumi ning muu teabe pealtkuulamiseks, -vaatamiseks ja salvestamiseks ning punkt 7 elektroonilise side võrgu kaudu edastatava sõnumi edastamise fakti, kestuse, viisi ja vormi ning edastaja või vastuvõtja asukoha andmete jälgimiseks ja salvestamiseks.

[248] Koosseis määratakse JAS § 10 lg 3 kohaselt riigikaitseseaduse alusel (RiKS) ning selle kinnitab Vabariigi Valitsus vastavalt RiKS § 4 lg 3-le. Vastavalt RiKS § 4 lg 4-le ning juhib komisjoni tööd peaminister.
[249] Kaitsepolitseiameti poolt teabe varjatud kogumisel kasutatavad meetodid ja vahendid ning teabetoimiku pidamise ja säilitamise kord. – RT I, 02.08.2017, 7.
[250] Välisluureameti poolt teabe varjatud kogumisel kasutatavad meetodid ja vahendid. – RT I, 28.06.2017, 9.

Julgeolekuasutuste töö suunamine ja ühtlustamine toimub vastavalt JAS § 9 lg1-le peaministri ja valdkondlike ministrite (sise- või kaitseminister), kelle valitsemisalas asuvad julgeolekuasutused, omavahel järjepideva koostöö raames. Vastavalt JAS § 9 lg 2-le kehtestab Vabariigi Valitsus oma korraldusega igal aastal riigisaladusega piiratud riigi julgeolekuteabe hanke ja analüüsi kava, millega sätestatakse julgeolekuasutuste ja Kaitseväe ülesanded kaitseväeluure teostamisel ning kogutava teabe vastavalt selle olulisusele.

JAS-iga reguleeritud vastuluure ja teabehanke kaalutlustel toimuvad riiklikud sekkumised põhiseadusliku korra kaitseks on mitmefunktsioonilised, sh nii preventiivsetel kaalutlustel ohtude tõrjumine ehk ohutõrjeõiguslik sekkumine (mida reguleerivad KorS, PPVS ja muud seadused, kokku rohkem kui 160 dokumenti[251]) kui ka sekkumine repressiivsetel kaalutlustel karistamise eesmärgil ehk süüteomenetluslik sekkumine (reguleerivad KrMS ja VTMS).[252]

Kui EIÕK art 8, mille kaitsealasse sõnumite saladus konventsioonis kuulub, lubab sekkuda sõnumisaladuse kaitsealasse riigi julgeoleku, ühiskondliku turvalisuse, riigi majandusliku heaolu, tervise, kõlbluse ning kaasinimeste õiguste ja vabaduste kaitse eesmärgil, siis PS piirab riigivõimu võimalusi sekkuda sõnumite saladusse tunduvalt enam kui EIÕK. Nimelt on PS § 26 järgi sõnumite saladusse sekkumine isegi enam piiratud kui sekkumine perekonna- ja eraellu. Sõnumisaladusse sekkumine ehk riive, mille legitiimsed eesmärgid kaitsevad õigust sõnumi saladusele, kuid raskendavad PS-s tunnustatud väärtuste nagu riigi julgeolek kaitset, on õigustatud üksnes kohtu loal ja kahe järgneva eesmärgi saavutamiseks:

1) kuriteo tõkestamiseks;

2) kriminaalmenetluses tõe väljaselgitamiseks.[253]

Eelneva sekkumise laiendamiseks on sõnumite saladuse kaitsega seotud mõistete laiendavat tõlgendust kasutatud erinevates seadustes[254] ning seadusandja ja senine kohtupraktika käsitleb kaitsealana üksnes üldkasutataval teel edastamisprotsessis olevaid sõnumeid.[255]

Seega, sõltumata sõnumite saladuse ning era- ja perekonnaelu puutumatuse kaitseala täpsest piiritlemisest peab seadusandja arvestama sõnumite saladusega puutumuses olevate riivete

[251] Korrakaitseseaduse muutmise ja rakendamise seaduse eelnõu seletuskiri. Kättesaadav: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/2445bcfe-b04d-40c8-932e-db51253abea3/Korrakaitseseaduse%20muutmise%20ja%20rakendamise%20seadus (24.02.2023).
[252] Pärnamägi. I. Riikliku sekkumise eesmärgi kindlakstegemise praktiline pool. Mitmefunktsiooniliste meetmete probleem. Juridica 3/2019, lk 189.
[253] Laos, S. PSK § 43/13, lk 522.
[254] nt kuriteo tõkestamine JAS §-s 4.
[255] Laos, lk 522

intensiivsusega nüüdisaegses infoühiskonnas ning sõltuvalt asjaoludest kehtestama ka era- ja perekonnaelu kaitseks kohtu loa nõude.[256] Sõnumite saladuse õiguse piiramise täpsemad alused ja menetluskord on reguleeritud JAS-i ja KrMS-ga.[257]

Ebapiisav regulatsioon on vastuolus PS §-s 13 sätestatud õigusselguse põhimõttega.[258] Õigusselgus tähendab seda, et seadused ja muud õigusaktid peavad olema piisavalt selged ja arusaadavad, et isikul oleks mõistlik võimalus riigi tegevust ette näha ja kohandada oma tegevust sellele vastavalt. Õigusselgusetu olukorraga takistab seadusest tulenevate kohustuste kindlakstegemist ja täitmist.[259]

Õigusselgusetu olukord takistab seadusest tulenevate kohustuste kindlakstegemist ja täitmist.[260] Riigil on PS § 14 järgi kohustus luua põhiõiguste kaitseks kohased menetlused, mis tagaks isiku õiguste tõhusa kaitse. PS § 14 sisaldab isiku subjektiivset õigust nõuda ja riigi, eelkõige seadusandja objektiivset kohustust, kehtestada normid, mis piisava tõenäosusega ja piisaval määral tagaks põhiõiguste teostumise ning kaitse.[261]

Isiku kohta varjatult teabe kogumist ja selle edasist töötlemist võib üldjuhul pidada isiku õiguste intensiivseks ja riigivõimu omavoli ohtu sisaldavaks riiveks, mis esitab normide õigusselgusele kõrgendatud nõudeid. Riigikohus on rõhutanud, et jälitustegevust reguleeriv seadus peab nägema ette jälitustoimingute tegemiseks selged alused ja menetluskorra, mis on jälitustegevuse seaduslikkuse kontrollimise eelduseks.[262]

4.2. Sideandmete kasutamine julgeoleku tagamiseks

Järgnevalt analüüsib uurimistöö autor sideandmete kasutamise õiguspärasust Eesti seadusandluses julgeoleku tagamise eesmärkidel, mille üheks meetmeks on luuretegevuse (sh signaalluure) kaudu teabehange. Analüüs on teostatud põhinedes Eesti siseriiklikule regulatsioonile julgeoleku valdkonnas, mis sätestab tingimused isiku elektrooniliste sideandmete töötlemisele. Analüüsi eesmärk on aru saada, kas kõik EIK poolt välja toodud kriteeriumid,

[256] Laos, S PSK § 43/13, lk 522.
[257] Laos, S PSK § 43/14, lk 522.
[258] RKPJKo 19.12.2019, 5-19-38, p 2.
[259] *Ibidem,* p 68.
[260] *Ibidem*, p 67.
[261] *Ibidem*, p 99.
[262] *Ibidem*, p 69.

millele siseriiklik seadusandlus peab vastama, on kaetud ka Eesti siseriiklikus regulatsioonis, et tagada vajalike kaitsemeetmete olemasolu harta artikkel 8 riive lubatavus ja vajalik õigusselgus.

Julgeoleku tagamine ja kuritegevuse vastu võitlemine eesmärgiks on kaitsta igaühe inimõigusi ja põhivabadusi. Andmekaitse ja privaatsusõiguse küsimused ei tohi takistada turvalise elukeskkonna ning põhiõiguste kaitset ja vastanduda turvalisuse tagamisele. Isikutel on ühelt poolt õigus nõuda riigi mittesekkumist, kuid samas õigus nõuda riigilt kaitset .[263]

Nagu eelnevalt mainitud, siis jääb isikuandmete kaitse seaduse ja isikuandmete kaitse üldmääruse reguleerimisalast välja isikuandmete töötlemine nendes valdkondades, mis ei kuulu EL õiguse kohaldamisalasse. Üheks selliseks valdkonnaks on julgeolekuasutuste tegevus riigi julgeoleku tagamisel.

Julgeolekuasutuste tegevus eelkõige teabehankes ei kuulunud IKS-i ja isikuandmete kaitse üldmääruse reguleerimisalasse. Õiguslünga täitmiseks on need sätestatud JAS-is ning sõnastatud juhindudes kehtivast õigusest, PS-ist, EIÕK-st, IKS-st, üldmäärusest ja kohtupraktikast. Samas on piirangud sätestatud mitteammendava loeteluna.[264]

2018. aastal, kui Eestis kehtivat seadusandlust sooviti viia vastavusse isikuandmete kaitse üldmäärusega 2016/679 ja ühtlustada õiguskaitsevaldkonna direktiiviga 2016/680,[265] oli üks muudetav seadus JAS, mille normide koostamisel lähtuti eelkõige isikuandmete kaitse konventsiooni[266] peatükist II, mis sätestatab andmekaitse põhiprintsiibid (osalisriikide kohustused, andmete liigid, kvaliteedi, andmeturve ja tagatised andmesubjektile) ning konventsiooni lisaprotokollist[267] (lisandub õiguspärasuse mõõde).

Lisanduvateks põhimõteteks olid seletuskirjale põhinedes[268], et teabe kogumisel ja töötlemisel:

- ei või kahjustada isiku põhiõigusi ülemääraselt, võrreldes julgeolekuasutuse taotletava eesmärgiga;
- ei või ohustada isiku elu ja tervist, põhjendamatult ohustada vara ja keskkonda ega põhjendamatult riivata muid isikuõigusi;

[263] Sinisalu, A.; Virks, K. Õige vähe õige paljust ehk turvalisuse ja julgeoleku mõningatest tahkudest õiguse laia tõlgenduse kontekstis. Juridica 5/2022, lk 364.
[264] Isikuandmete kaitse seaduse rakendamise seadus. Seletuskiri - RT I, 13.03.2019, 2, Eelnõu § 26.
[265] IKSrs seletuskiri. Sissejuhatus.
[266] Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon. – RT II 2001, 1.
[267] Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni muutmise protokoll. – RT II, 03.07.2020, 2.
[268] IKSra seletuskiri, lk 33.

- teavet töödeldakse ja säilitatakse nii kaua, kui see on vajalik julgeolekuasutuse ülesande täitmiseks ja kooskõlas julgeolekuasutuse tegevuse eesmärgiga;
- teavet kogutakse ja töödeldakse viisil, mis tagab selle turvalisuse[269].

JAS reguleerib ka isikuandmete töötlemisega kaasnevaid andmesubjekti õiguste piiranguid, mis on isikuandmete kaitse üldmääruse artikli 23 lõike 1 alusel lubatud liikmesriigil kehtestada seadusandliku meetmega riigi julgeoleku tagamise eesmärgil.[270]

Julgeoleku ehk õigushüve ja põhiseadusliku korra tagamise kaitseks sätestab JAS vastavalt § 1 lg 1-le julgeolekuasutuste pädevused, täpsustades need § 1 lg 1^1-s[271]. Selle kohaselt teostab julgeolekuasutus isikuandmete, sealhulgas eriliiki isikuandmete töötlemist ja andmesubjekti õiguste piiramist. Lisaks tuuakse välja piiramise alused ning isikuandmete töötlemise nõuete täitmise üle järelevalve teostamise kord.

JAS § 3 lg 1 p 3 kohaselt kogub ja töötleb julgeolekuasutus teavet, sealhulgas isikuandmeid, kui see on vajalik tema ülesannete täitmiseks, lähtudes seejuures põhimõttest, et teabe kogumise ja töötlemise viis, ulatus ning tulenevalt JAS § 3 lg 1 p 1 ei või kohaldatavad korralduslikud ja tehnilised kaitsemeetmed kahjustada isiku põhiõigusi ülemäära, võrreldes julgeolekuasutuse taotletava eesmärgiga, ohustada isiku elu ja tervist põhjendamatult, ohustada vara ja keskkonda ega põhjendamatult riivata muid isikuõigusi. Julgeolekuasutuste tegevuse põhimõtteid reguleerivas sättes, e JAS-i § 3 lg 2-s sätestatud *ultima ratio* e äärmise abinõu põhimõte laieneb kogu julgeolekuasutuste tegevusele, mille hulka kuulub ka isikuandmete töötlemine. Eriti täpselt on sätestatud julgeolekuasutuse tegevuse põhimõtted, mis peavad sisaldama ka väga konkreetselt julgeolekuasutuste kohustusi andmesubjekti õiguste igakülgseks tagamiseks.[272]

2018. aastal täiendati JASi §-i 1 lg-ga 1^1, mis täpsustas seaduse reguleerimisala, st kuna isikuandmete kaitse seaduse ja isikuandmete kaitse üldmääruse reguleerimisalast jäi välja julgeolekuasutuste tegevus riigi julgeoleku tagamisel ning selle raames isikuandmete töötlemine, siis sätestati julgeoleku tagamiseks isikuandmete töötlemise eriregulatsioon JAS-is, kus on sätestatud ka järelevalve teostamine andmekaitsenõuete täitmise üle, ehk nn selge erisus isikuandmete kaitse seaduses sätestatud riiklikust ja haldusjärelevalvest.[273]

[269] Turvalisuse all käsitletakse kaitset loata või ebaseadusliku töötlemise eest ning juhusliku kadumise, hävimise või kahjustumise eest, rakendades asjakohaseid tehnilisi või korralduslikke meetmeid.
[270] IKSra seletuskiri, lk 33.
[271] Jõustunud 2019 JAS-i redaktsiooniga.
[272] IKSrs seletuskiri, lk 33.
[273] *Ibidem.*

4.2.1 Järelevalve teostamise korraldus

Vastavalt JAS 36 lg 1-le teostab järelevalvet julgeolekuasutuste tegevuse üle Riigikogu julgeolekuasutuste järelevalve komisjon (erisus IKS-ist, mille korral teostab Andmekaitse Inspektsioon riiklikku ja haldusjärelevalvet[274]), mis on Riigikogu erikomisjon ja keda teavitavad julgeolekuasutuste tegevusest vastavalt JAS 36 lg 2-le peaminister ja asjaomane minister. Mainitud komisjon on vastavalt JAS 36 lg 2 p 6-le seaduserikkumise avastamise korral kohustatud edastama vastavad materjalid uurimisasutusele või õiguskantslerile.

Efektiivne kontroll (jälitus- ja) julgeolekuvaldkonna üle on demokraatia ja õigusriigi toimimise eelduseks, kuuludes jälitustegevuse õiguspärasusega seotud menetlusgarantiide hulka.[275] Õiguskantsleri seadus[276] (ÕKS) § 1 lg 9 kohaselt teostab õiguskantsler järelevalvet põhiõiguste ja -vabaduste järgimise üle täidesaatva riigivõimu asutuste poolt varjatult isikuandmete ja nendega seonduva teabe kogumise, töötlemise, kasutamise ja järelevalve korraldamisel.

ÕKS ei sätesta oma kehtivas redaktsioonis sõnaselgelt õiguskantsleri järelevalvepädevust jälitus- ja julgeolekuteabe varjatud töötlemise, sh isikuandmete varjatud töötlemise üle, kuid see ei tähenda, et õiguskantsleril puuduks võimalus jälitus- ja julgeolekuteabe andmete varjatud töötlemise üle teostada järelevalvet.[277] Eelkõige jälitusasutuste (KrMS § 126^2 lg 1) ja julgeolekuasutuste (JAS § 5) poolt isikuandmete ja nendega seonduva teabe kogumist, kasutamist ning muud töötlemist, mis toimub eesmärgiga varjata andmete töötlemise fakti ja sisu andmesubjekti eest.

Järelevalveobjektiks on varjatud töötlemise üle teostatav järelevalve korraldus (kontrollisüsteem), st järelevalve süsteemi terviklik ja efektiivne toimimine, olles osaks õiguskantsleri ombudsmanijärelevalvest. [278]

2018. aastal sätestati julgeolekuasutuste ülesannete täitmiseks vajalik eriregulatsioon isikuandmete töötlemisele lisades JAS-i lause § 21 lg 2 – riikliku järelevalve teostamisel võib kohaldada JAS § 21^1 lõikes 3 sätestatud andmesubjekti õiguste piiranguid,[279] kuid arvesse tuleb võtta KorSi ja JAS-i kohaldamisala erinevust, kus julgeolekuasutuste tegevus on seotud kuriteo

[274] IKSra seletuskiri, lk 39.
[275] EIKo 02.01.2013 nr 22491/08, *Sefilyan vs. Armeenia,* p 12.
[276] Õiguskantsleri seadus,.- RT I, 26.05.2020, 11.
[277] Seletuskiri õiguskantsleri seaduse täiendamise seaduse eelnõule, lk 2.
[278] *Ibidem,* lk 3.
[279] IKSra seletuskiri, lk 34.

tõkestamisega, aga JAS-i kohaselt on kuriteo tõkestamine kuriteo ärahoidmine mis tahes seaduslikul viisil enne selle toimepanemist.

Järelevalve kohustus (nii sõltumatu järelevalve määramise kord kui ka hilisem *ex post* kontroll) on üks EIK poolt välja toodud olulistest aspektist, millele peab vastama liikmesriigi siseriiklik regulatsioon. Eesti siseriiklikus seadusandluses on järelevalveorganitele volituste andmine kajastatud JAS § 36-s. Kontroll kogutud, töödeldud ja kasutatud andmete osas andmesubjekti kohta, mida julgeolekuasutus oma põhitegevuse käigus saab, täites JAS-ist tulenevaid põhiülesandeid, kuulub õiguskantsleri ja Riigikogu julgeolekuasutuste järelevalve komisjoni pädevuse hulka..[280] Seega saame kokkuvõtlikult ütelda, et järelevalvekohustus on Eesti siseriiklikus seadusandluses tagatud.

4.2.3 Andmete kogumise alus ja ulatus

2019. aastal kehtima hakanud JAS-i redaktsiooni täiendati §-ga 21^1, millega sätestatakse julgeolekuasutuste poolt töödeldava teabe liikide näitlikustav loetelu, töötlemiseks õigustatud isikud, andmesubjekti õiguste piiramiseks vajalike meetmete näilikustav loend ja selle alused ning erisused kogutud teabe töötlemiseks ja säilitamiseks.[281]

JAS § 21^1 annab julgeolekuasutusele õiguse piirata andmesubjekti õigusi ning koguda ja töödelda oma ülesannete täitmiseks muu hulgas järgmist: 1) isikuandmeid; 2) eriliiki isikuandmeid; 3) anonüümitud andmeid; 4) üldsusele suunatud ja avalikest allikatest kättesaadavaid andmeid. Lg 1 täpsustab, et kui see on vajalik tema ülesannete täitmiseks tulenevalt JAS § 3 lg 1-st. PS §-dest 3, 11 ja 26 tulenevalt tuleb eriregulatsiooni loomisel sätestada, millist liiki isikuandmeid julgeolekuasutuste poolt töödeldav teave hõlmab ning seega täpsustatakse § 21^1 lõikega 1, et julgeolekuasutus võib oma ülesannete täitmiseks või täitmise tagamiseks töödelda muu hulgas isikuandmeid, eriliiki isikuandmeid, isikustamata andmeid, üldsusele suunatud ja avalikest allikatest kättesaadavaid andmeid. § 21^1 lg 2 järgi toimub teabe kogumine ja töötlemine vahetult julgeolekuasutuse (st tehes seda ise) või selleks volitatud asutuse või koostööle kaasatud isiku poolt.

Andmesubjekti õiguste piiramise alus ja ulatus, mis võib olla vajalik julgeolekuasutuste ülesannete täitmisel riigi julgeoleku tagamiseks tulenevalt JAS § 6-ga KAPO-le ja JAS § 7-ga

[280] IKSra eletuskiri, lk 3.
[281] Isikuandmete kaitse seaduse rakendamise seadus. Seletuskiri. – RT I, 13.03.2019, 2 eelnõu § 26.

VLA-e seadusega pandud (omakorda isikuandmete kaitse üldmääruse artikli 23 lõike 1 alusel) tuleneb § 21[1] lg 3-st, kus p 1 kohaselt on julgeolekuasutusel õigus saada teada andmesubjekti isikuandmete automatiseeritud või automatiseerimata töötlemisest, sh milliseid isikuandmeid töödeldakse, samuti töötlemise eesmärki, õiguslikku alust, ulatust ja põhjust. § 21[1] lg 2 kohaselt on õigus saada teada isikuandmete vastuvõtjad ja avaldatavate isikuandmete kategooriad ning teavet selle kohta, kas isikuandmed edastatakse välisriigile või rahvusvahelisele organisatsioonile; p 3 sätestab säilitamise tähtaja või tähtaja määramise kriteeriumeid; p 4 isikuandmete töötlemise tehnilised ja korralduslikud kaitsemeetmed ning p 5 julgeolekuasutuse õiguse tutvuda kogutud ja töödeldavate isikuandmetega. p 6 omakorda kajastab õigust nõuda isikuandmete töötlemise piiramist; p 7 nõuda isikuandmete ülekandmist, p 8 esitada vastuväiteid andmete töötlemise kohta ning p 9 julgeolekuasutuse õiguse saada teavet ka isikuandmetega seotud rikkumiste kohta. [282]

JAS-i § 3 ja §-dega 6 ja 7 koosmõjus hõlmab ülesannete täitmist kuriteo tõkestamiseks JAS-i § 4 tähenduses ning isiku (sh andmesubjekti enda) õiguste ja vabaduste kaitseks. Selguse huvides on need alternatiivsed alused normi tekstis ka eraldi välja toodud, andes parema selguse JAS-i §-st 32 tuleneva teabe andmise kohustuste täitmiseks. Lisaks on reguleeritud olukorrad, kus julgeolekuasutustel on kohustus anda infot muule asutusele või isikule nende ülesande täitmiseks, kui teabe andmine ei sea ohtu julgeolekuasutuse ülesande täitmist.[283]

Andmesubjekti õiguste piirangute kehtestamine üldmääruse tuginedes artiklis 23 sätestatule ning artikli 23 lõike 1 alusel on piirangud kohaldatavad ka julgeolekuasutuse tegevusele sellises valdkonnas, mis võib kuuluda liidu õiguse kohaldamisalasse, kuid piirangu kohaldamise vajadus vastab riigi julgeoleku tagamise eesmärgile. JAS § 21[1] lg 4 võimaldab andmesubjekti õigusi piirata ainult juhtudel, kui piiramata jätmine võib: 1) kahjustada julgeolekuasutuse ülesannete täitmist; 2) takistada kuriteo tõkestamist; 3) kahjustada andmesubjekti või teise isiku õigusi ja vabadusi.[284]

JAS § 21[1] lg 5 võimaldab julgeolekuasutus kogutud teavet töödelda nii JAS-s kui muus seaduses sätestatud ülesande täitmiseks või täitmise tagamiseks, mille on tinginud julgeolekuasutusele eriseadusega pandud ülesanded,[285] kuid mille õigus on hetkel normina tuletatav tõlgendamise teel.

[282] Isikuandmete kaitse seaduse rakendamise seadus. Seletuskiri RT I, 13.03.2019, 2 eelnõu § 26.
[283] *Ibidem*.
[284] *Ibidem*.
[285] Nt välismaalaste seaduses sätestatud Kaitsepolitseiameti pädevus viisamenetluses osalemisel, välismaalase Eestis ajutise viibimise, Eestis elamise ja Eestis töötamise ning Eestist eemal viibimise asjaolude üle kontrolli teostamine või muust seadusest tuleneva riikliku järelevalve ülesande täitmine, julgeolekukontroll riigisaladuse ja salastatud välisteabe seaduse alusel.

Eriseadustega pandud ülesanded (n riiklik järelevalve, mida antud uurimistöö ei hõlma) tulenevad JAS-s sätestatud julgeolekuasutuste põhitegevuse eesmärkidest, milleks on riigi julgeoleku tagamine. Seega tuleb ka praktikas võimaldada julgeolekuasutustel olemasoleva teabe kasutamist selle ülesande täitmiseks[286].

Andmete kogumise alus ja ulatus on Eesti siseriiklikus seadusandluses kajastatud. EL-i seadusandlus lubab julgeoleku tagamise eesmärgil isikuandmeid koguda ja töödelda, sest vastavalt määruse 2016/679 artiklil 23 p 1-le võib vastutava töötleja või volitatud töötleja õiguste ulatust piirata, kui see on vajalik, et tagada riigi julgeolek.

4.2.3. Piirangud kogutud andmete säilitamise kestvusele ja kogumise kord

JAS § 21^1 lg 5 sätestab kogutud andmetele ajapiirangu, mille kohaselt julgeolekuasutus võib säilitada nii JAS-i kui muu seaduse alusel kogutud teavet nii kaua, kui see on tema JAS-s sätestatud ülesannete (st põhiülesannete) täitmiseks vajalik või kuni vajadust edasiseks töötlemiseks ei saa välistada.

Eesti seadusandlus (JAS) lubab julgeolekuasutustel säilitada andmeid võimalikult kaua. Samas direktiiv 2002/58 artikkel 15 kohaselt tuleks ka riigi julgeoleku (sh riigikaitse, avaliku korra kriminaalkuritegude) tagamise eesmärgil rakendada liikmesriigina seadusandlikke meetmeid, ning sätestada andmete säilitamine piiratud aja jooksul.

Viimase aspektina sätestab JAS § 21^1 lg 7 eelmainitud andmete töötlemise erisused. Julgeolekuasutus võib kohaldada isikuandmete töötlemist riikliku järelevalve käigus, samuti ka julgeolekuasutuse ametniku ja töötaja teenistusse või tööle võtmisel ning teenistuse või töötamise ajal, mis ei olnud antud töö uurimisobjektiks.

JAS § 25 lg 1 järgi on julgeolekuasutusel õigus piirata isiku sõnumisaladust, kui lg 2 kohaselt on piisavad andmed ettevalmistatava või toimepandava kuriteo kohta ning piiramine toimub vastavalt JAS § 25 lg 3 punkt 2-le elektroonilise side võrgu kaudu edastatava sõnumi või muu teabe pealtkuulamise, -vaatamise või salvestamisega. Erinevalt KAPO-st ei ole VLA jälitusasutus ning tema esmaseks ülesandeks ei ole kuritegude avastamine ja tõkestamine selle tavalises tähenduses, vaid vastuluure Eesti Vabariigi välis-, majandus- ja riigikaitsepoliitika kujundamiseks

[286] KrMS § 63 lg 1^1 kohaselt Julgeolekuasutuste seaduse alusel kogutud teabe tõendina esitamise kriminaalmenetluses otsustab riigi peaprokurör, arvestades käesoleva seadustiku § 126^1 lõikes 2 ja § 126^7 lõikes 2 nimetatud piiranguid.

ning riigikaitseks vajaliku teabe kogumine. Seda võib laiemas plaanis käsitada, kui meetmeid julgeoleku tagamiseks kavandatava kuriteo tõkestamiseks (üldjuhul KarS järgi riigivastase kuriteo).[287]

JAS §-25-s sätestatud juhtudel ja JAS § 27-s sätestatud korras on julgeolekuasutustel õigus piirata sõnumite saladust (JAS § 26), kui on olemas piisavad andmed ettevalmistatava või toimepandava kuriteo kohta, mida ei seostata toimingu kuriteo raskusastmega.[288] Vastavalt JAS § 27 lg 1 peab julgeolekuasutuse juht esitama halduskohtu esimehele või tema määratud halduskohtunikule põhjendatud kirjaliku taotluse vastava loa saamiseks, kus näidatakse ära nimetatud õiguse piiramise viis (edasilükkamatul juhul, kui esineb oht riigi julgeolekule ja nimetatud luba ei ole võimalik taotleda, siis võib tulenevalt JAS § 27 lg 2^1 toimingu teha halduskohtu loal, mis on antud taasesitamist võimaldaval viisil esitades taasesitamist võimaldava taotluse halduskohtu esimehele või tema määratud halduskohtunikule esimesel võimalusel, kuid hiljemalt toimingu alustamisele järgneval päeval). JAS § 27 lg 2 kohaselt otsustatakse loa andmine viivituseta ning luba antakse kuni kaheks kuuks. Luba võib pikendada iga kord sama tähtaja võrra. Tegemist on kuriteo määratlemisega ainsuses, mitte kuritegevus üleüldiselt, vaid konkreetset liiki kuriteo ettevalmistamiseks või toimepanemiseks tuleb taotleda luba halduskohtult.

See omakorda tähendab, et väljaspool kriminaalmenetlust on KAPO-l ja VLA-l kuriteo tõkestamiseks laialdasemad volitused sõnumite pealtkuulamisel ja -vaatamisel, kui seda on uurimisasutusel. Kahe seaduse (JAS ja KrMS) erinevad standardid sisult sarnaste toimingute osas tekitavad praktikas vaidlusi eelkõige KrMS § 63 lg 11 kohaldamisel.[289]

EIK oma lahendites leiab, et vajalik on määratleda piirangud jälitustegevuse kestvusele ja mida Eesti regulatsioonis annab halduskohus kaheks kuuks (vajadusel pikendamise võimalusega) ning seega selles aspektis on Eesti regulatsioon kookõlas EIK ootustega. Andmete säilitamisse ajaraami on Eesti seadusandja aga jätnud lahtiseks ning mille puhul EIK näeb ette konkreetset määratlemist.

4.2.4. Süütegude loetelu andmete kogumise lubamiseks

Üks olulisemaid ja ühtlasi keerulisemaid aspekte ka EIK seisukohast on määratleda süütegude loetelu, mille puhul on lubatud varjatud isikuandmete töötlemine. Kui Eesti siseriiklik seadusandlus sätestab KrMS-i ette menetluskorra ja süütegude loetelu, mille puhul on lubatav

[287] Laos, S PSK § 43/20, lk 522.
[288] *Ibidem.*
[289] *Ibidem.*

varjatud jälitustegevus, siis JAS-is sellist süütegude loetelu ei ole sätestatud. Käesoleva uurimistöö peatükis 2.2. sai välja toodud VLA ja KAPO tegevuse olemuslik erinevus, mis seisnes selles, et VLA tegevus ei ole seotud ühegi konkreetset liiki kuriteo ennetamisega ning seda tegevust ei piirata kuriteokoosseisuga.

Tõlgendamise teel võib selleni jõuda läbi JAS § 2-s sätestatud julgeolekuasutuste tegevuse eesmärkide ja §-des 6 ja 7 sätestatud julgeolekuametite eesmärkide. Selline tõlgenduslik tuletamine ei vasta aga EIK-i poolt välja toodud lähtekohale õigusselguse tagamisel. Toimingu tegemiseks vajaliku loa andmise kord on läbi halduskohtu esimehe positsiooni sätestatud. Samuti nõue igakordseks loa taotlemiseks konkreetse kuriteo (mitte kuritegude) kohta.

Vastavalt JAS § 28-le kehtestab vahendid ja meetodid varjatud teabe kogumiseks ja tulenevalt JAS § 30 ka kogutud teabe kohta avatud teabetoimiku pidamise ja säilitamise korra asjaomane minister oma määrusega. Nimetatud määrus esitatakse järelevalvet teostavale institutsioonile ehk Riigikogu julgeolekuasutuste järelevalve komisjonile teadmiseks.

Julgeolekuasutuste poolt kasutatavad meetmed andmete kogumiseks teabehanke valdkonnas ei ole EIK poolt käsitlemist leidnud. EK on (kohtujuristi ettepanek lahendis Privacy International) sätestanud, et kogumine peaks toimuma otse ja oma vahenditega, st mitte pärides sideteenuseid osutavate ettevõtete poolt teenuse osutamise käigus kogutud andmeid. JAS § 28 kohaselt on kasutatavad meetmed julgeolekuettevõtete valdkondlike ministrite otsustuspädevuses.

Uurimistöö käigus läbi viidud luurevaldkonnaga lähemalt seotud ekspertide intervjuudes selgus, et konkreetsed teabehankega andmete kogumise meetodid ja viisid on fikseeritud, kuid kuuluvad riigisaladusega kaetud informatsiooni alla.

4.2.5. Andmesubjekt teavitamine toimingust ja andmete säilitamine

Isiku, kelle õigust sõnumi saladusele piiratakse, teavitamine või mitteteavitamine on reguleeritud JAS §-is 29. Toimingu tegemisest teavitamine on õigusselguse tagamise seisukohalt oluline aspekt nii EIK-le kui EK-le ning vastav kord on piisava detailsusega EL tasandil kajastamist leidnud.

JAS §-i 30 kohaselt säilitatakse kogutud teave teabetoimikutes, mis avatakse iga juhtumi kohta eraldi. Toimiku pidamise ja säilitamise kord kehtestatakse valdkondliku ministri määrusega. Magistritöö kirjutamise hetkel Kaitseministeeriumi dokumendiregistrist kättesaadava 2017. aasta

Kaitseministri määruse[290] § 5 alusel säilitatakse toimik Välisluureametis, mis tagab selle säilimise, sellele juurdepääsu ning selle hävitamise või avalikule arhiivile üleandmise arhiiviseaduses, riigisaladuse ja salastatud välisteabe seaduses ning nende alusel kehtestatud õigusaktides sätestatud korras. RSVS § 9 p 4 järgi julgeolekuasutuse ülesannete täitmisel varjatult kogutud teave ning selle kogumist kajastav teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut, salastatakse täiesti salajasel või madalamal tasemel kuni 50 aastaks. Teabekandjad, mille salastatus on kustunud, antakse tulenevalt RSVS § 38 lg 1-st üle Rahvusarhiivile. Juhtudel, kui isik, kelle suhtes jälitustoiming tehti või kelle perekonna- või eraelu puutumatust jälitustoiminguga riivati, nõuab eriliiki isikuandmeid käsitleva teabe hävitamist ning seda teavet ei ole enam vaja avalike ülesannete täitmiseks, siis RSVS § 38 lg 2 kohaselt ei anta üle teabehankega või jälitustoiminguga kogutud teavet sisaldava infot Rahvusarhiivile ja hävitatakse teabekandja eriliiki isikuandmeid käsitlev osa viisil, mis teeb võimatuks selles sisaldunud teabe taastamise. RSVS § 38 lg 3 sätestab erandid, mille puhul võib hävitada teabekandjad enne salastatuse lõppu.[291]

EIK-i üks õigusselguse kriteeriumitest on andmete säilitamise ja kustutamise kord ning see on Eesti siseriiklikus regulatsioonis loodud läbi valdkondliku ministri määruse ja RSVS-i.

4.2.6. Suhtlus teiste isikute ja rahvusvaheliste partneritega

JAS sätestab §-i 31 lg 1-s julgeolekuasutuste õiguse oma ülesannete täitmiseks pöörduda riigi- või kohaliku omavalitsuse või avalik-õigusliku isiku poole teabe saamiseks. Tulenevalt § 31 lg 2-st võib teavet andnud asutus ja isik kohaldada isikuandmeid sisaldavat teavet töödeldes JAS § 21^1 lg 3 sätestatud piiranguid.

Avaliku teabe seaduse alusel asutatud andmekogu andmetele on julgeolekuasutustel seadusega pandud ülesannete täitmiseks juurdepääs vastavalt JAS § 31^1. JAS-i § 32-ga sätestatakse juhud, millal julgeolekuasutuse ülesannete täitmisel saadud teavet võib ja peab kolmandatele osapooltele, sh välisriigi või rahvusvahelisele organisatsioonile edastama. Julgeolekuasutuse ülesannete täitmisel saadud teabe peab edastama teisele riigiasutusele ja füüsilisele või juriidilisele isikule, kui see on vajalik terrorikuriteo tõkestamiseks või on seotud terrorikuriteo toimepanemise ohuga ning sellist teavet võivad julgeolekuasutus kui ka andmesaaja töödelda

[290] Kaitseministri määrus. Välisluureameti teabetoimiku pidamise ja säilitamise kord: 2017. Kättesaadav: https://adr.rik.ee/kmin/dokument/8422668.
[291] Seletuskiri Riigisaladuse ja salastatud välisteabe seaduse eelnõu. – RT I 2007, 16, 77, jõust. 01.01.2008.

andmesubjekti nõusolekuta[292]. Teavet saanud asutus või isik võib kohaldada isikuandmeid sisaldavat teavet töödeldes JAS § 21^1 lg 3 sätestatud andmesubjekti õiguste piiranguid vastavalt JAS § 32 lg 4.

JAS sätestab teabe saamise alused teistelt riigivõimu asutustelt ja institutsioonidelt ning rahvusvahelistelt lepingupartneritelt. Samas on sisse toodud, et terrorikuriteo tõkestamise eesmärgil on julgeolekuasutusel õigus edastada andmesubjekti puudutavat informatsiooni ilma andmesubjekti nõusolekuta nii füüsilistele kui juriidilistele isikutele. Kui julgeolekuasutuste poolt andmete kogumine otse ja oma vahenditega on mõistetav julgeoleku asutuse ülesannete täitmiseks, siis magistritöö kirjutajale jääb arusaamatuks, miks lubab Eesti seadusandlus kogutud andmete jagamist kolmandate osapooltena, sealhulgas nii füüsiliste kui juriidiliste isikutega.

ELi seadusandlus lubab julgeoleku aspektidest ajendatuna kehtestada liikmesriikidel endil siseriikliku seadusandluse isikuandmete töötlemise julgeoleku tagamiseks. Tulenevat EIK viimastest lahenditest (sh 2021 ja hilisemad) on EL-i kohtusüsteemil siiski eeldused, millele kvaliteetne, isikule mõistetav ja õigusselge siseriiklik regulatsioon peab vastama. JAS-i viimane redaktsioon pärineb enne käesolevas töös käsitletud EIK lahendid *Centrum för Rättvisa vs Sweden*, *Big Brother Watch and Others* ning *Ekimdzhiev and Others v. Bulgaria*. Nüüdseks väljakujunenud EK kohtupraktika kohaselt on nõutud, et põhiõiguste kaitse erandid piirduksid sellega, mis on tingimata vajalikud. EIK omakorda on oma lahendites jõudnud kaheksale seisukohale, millele siseriiklik regulatsioon peab vastama, et tagada olukord, kus siseriiklik õigus on kohaldamisel juurdepääsetav, ettenähtav ja tagab, et salajasi jälgimismeetmeid rakendatakse ainult juhul, kui see on demokraatlikus ühiskonnas vajalik. Lisaks on sätestatud piisavad ja tõhusad kaitsemeetmed ning tagatised kuritarvitamise vastu.

Teabe varjatud kogumise, ehk luure, mille alla koonduvad kõik luuredistsipliin, sh signaalluure, kaitseregulatsioon tuleneb Eesti siseriiklikus seadusandluses eelkõige JAS-ist. JAS sätestab valdavas osas EIK- poolt loetletud kaitsemeetmed, kuid neid, mida ka EIK peab raskesti saavutatavateks – süütegude ja isikute loetelu – ei ole Eesti seadusandluses määratletud. Lisaks jätab Eesti seadusandlus julgeolekuasutustele võimaluse andmete säilitamiseks ja töötlemiseks määratlemata ajaks sõnastades selle „nii kaua, kui see on vajalik," EL-i normid näevad ette konkreetse ajalise määratluse, ehk andmete säilitamise piiratud aja jooksul. Piirangud jälitustegevuse kestvusele, kasutamisele, säilitamise-hävitamise kord, koostöö teiste

[292] Politsei ja piirivalve seaduse ning päästeteenistuse seaduse muutmise ning sellega seonduvalt teiste seaduste muutmise seadus. Seletuskiri, lk 42.

institutsioonidega ja järelevalve on Eesti õigusruumis leitavad erinevatest regulatsioonidest nagu JAS-is, ministri määrus ja RSVS leitavad.

EIK-i viimased kohtulahendid on toonud ELi seisukohtadesse uusi seisukohti seoses teabe varjatud kogumisega seotud õigusregulatsiooni eeldustele. Selleks, et tagada Eesti õigusregulatsiooni kooskõla EL-i aluspõhimõtetega tuleb seadusandjal tagada muudatuste sisse viimine siseriiklikkusse seadusandlusesse.

KOKKUVÕTE

Demokraatliku ühiskonna üheks tunnusjooneks on isikuvabaduste olemasolu. Eesti kui demokraatliku riigi elanikena ei mõtle me igapäevaselt oma õigustele ja vabadustele, sest võtame seda kõike iseenesest mõistetavana. Samas elame maailmas, kus kasutame üha rohkem ja rohkem kõikvõimalikke elektroonilisi suhtluskanaleid ja platvorme, millest on saanud tänaseks vahendajad inimeste ning valitsuse vahel. Arvestades viimase kahe aastakümne tehnoloogilisi ja sotsiaalseid arenguid elektroonilise side vallas, on Euroopa Inimõiguste Kohus leidnud, et tänapäevased sideandmed võivad avaldada palju isiklikku teavet. Kogudes andmeid hulgi, saab võimuorgan vajadusel läbi sotsiaalsete võrgustike kaardistamise, asukoha jälgimise, interneti sirvimise jälgimise ja suhtlusmustrite kaardistamise kaudu luua isikust intiimse pildi ning ülevaate selle kohta, kellega see inimene on suhelnud.

Käesoleva magistritöö uurimisprobleem lähtus üksikisiku elektroonilise side andmete privaatsuse tagamise ja riigi julgeoleku tagamisest Euroopa Liidu ühises õigusruumis ja sellest tulenevalt Eesti Vabariigis luuretegevuse kaudu julgeolekuliste eesmärkide tagamiseks.

Autori uurimiseesmärgiks oli välja selgitada, kas demokraatia printsiipe austava ja euroopalikke põhimõtteid tunnustava Eesti Vabariigi õigusregulatsioon julgeoleku tagamisel läbi teabe varjatud kogumise ehk (signaal)luure on kooskõlas Euroopa Liidu üksikisiku sideandmete kaitse õiguspõhimõtetega?

Magistritöö autor püstitas kaks keskset uurimishüpoteesi: Euroopa Liidu ja Eesti siseriiklik ja seadusandlus ei sätesta kindlaid reegleid sideandmete säilitamiseks ning töötlemiseks signaalluure raames ja julgeoleku aspektidest tulenevalt on õigustatud kodanike elektrooniliste sideandmete privaatsuse puutumatuse riive.

Hüpoteeside paikapidavuse kontrollimiseks keskendus autor järgnevatele töö seisukohast olulistele teemadele nagu privaatsus, julgeolek ning teabe varjatud kogumine, mille mõistete ja kontseptsioonidest arusaamine on vajalik.

Privaatsus on oma olemuselt väga kompleksne kontseptsioon, kuhu kaasajal on lisandunud uue olulise aspektina küberkomponent. Privaatsuse, mille osaks on ka informatsiooniline enesemääratlusõigus, keskmeks jääb isiku kontrolli omamine enesekohase informatsiooni üle, sh ka elektroonilised sideandmed, olles osa isiku privaatsussfäärist. Seega on oluline mõista ka isiku

sideandmete struktuuriloogikat, mis on EL-i õigusruumis mõnevõrra erinev kui Eesti siseriiklikus seadusandluses.

Järgmine oluline teemavaldkond on turvalisus ja julgeolek. Julgeolek on olemuselt sotsiaalne konstruktsioon, kus juba aastatuhandeid on filosoofid diskuteerinud individuaalsete vabaduste ja kollektiivse turvalisuse tasakaalu üle. Sarnaselt privaatsuse kontseptsiooniga on tehnoloogia areng ja küberkomponendi lisandumine toonud uusi aspekte ka julgeoleku ja turvalisuse käsitlustesse. Valdkond on kiiresti arenev, seega ei ole veel välja kujunenud ühest ja üheselt mõistetavat terminoloogiat. Julgeoleku esemeks on õigushüve, mida võib kitsamas tähenduses käsitleda kui isiku ja asja seisundi kaitset ning laiemas käsitluses isiku ja asja olemasoleva positsiooni edasikestmist eesmärgiga täita oma põhiülesandeid ja -funktsioone. Lähtuvalt uurimiseesmärgist käsitles autor julgeoleku olemust ja selle tagamise meetodeid ning luure kui julgeolekuasutuste töövahendi olemust.

Riigi tasandil on julgeoleku esemeks riigi kui sellise püsimine, et täita oma põhiülesandeid ja -funktsioone. Eesti Vabariigis mõistetakse sellena omariikluse püsimist ja järjepidevuse tagamist ennetades ning takistades korrakaitselisi ja julgeolekulisi ohte kui isikut, süsteemi või ühiskonda kahjustada võivate sündmuste põhjuseid.

Põhiseaduslikku korda ohustava tegevuse ennetamiseks ja tõkestamiseks tuleb koguda ning töödelda teavet vaenuliku poole luure- ja mõjutustegevusest. Ohtude väljaselgitamise üheks meetodiks on jälgimine ehk seire, mida iseloomustab üldjuhul seiratava volituse puudumine selliseks tegevuseks. Eesti julgeolekuasutuste sellist tegevust tähistatakse terminitega luure, seire või teabehange. Tänapäeval on kasutusel üldterminina pigem teabehange, mis omakorda jaguneb luuremeetoditeks või -distsipliinideks, mille üheks alammeetmeks on signaalluure. Signaalluure omakorda hõlmab side-, elektrooniliste kanalite, radarite, aparatuurisignaalide ja küberluuret. Käesoleva uurimistöö mõistes kasutas autor katusmõistena teabe varjatud kogumist, mis koondas enda alla ka signaalluure kui ühe luuredistsipliini.

Eesti Vabariigis on julgeolekuasutusteks Kaitsepolitseiamet (KAPO) ja Välisluureamet (VLA). KAPO ülesandeks on riigi sisejulgeoleku tagamine teabe kogumise ja ennetusvahendite kasutamise abil, süütegude uurimine ning meetmete rakendamine Eesti riigi vastu suunatud luure- ja õõnestustegevuse ennetamiseks. VLA ülesanne on tagada riigi julgeolek põhiseadusliku korra püsimiseks mittesõjaliste ennetavate vahendite kasutamise abil ja julgeolekupoliitika kujundamiseks ning riigikaitseks vajaliku teabe kogumine ja töötlemine, sh teabe kogumine ja töötlus küberruumis, st digitaalse taristu kaudu.

Kolmas ja privaatsust ning julgeolekut siduv alateema on eraisikute privaatsuse reguleerimine EL-i ja Eesti Vabariigi seadusandluses, sh kas EL-i otsekohalduvad määrused omavad rolli Eesti siseriiklikus õiguskaitses ja direktiivid on üle võetud siseriiklikku seadusandlusesse; kuidas on mõjutanud ja mõjutavad EK ning EIK kohtulahendid Eesti siseriiklikku seadusandlust ja selle kujunemist.

Uurimiseesmärkide saavutamise käigus selgusid alljärgnevad asjaolud: üksikisiku isikuandmete kaitse valdkonnas on viimase kolmekümne aasta jooksul toimunud pidev areng; aastal 2018 jõustusid viimane isikuandmete kaitset reguleeriv üldmäärus 2016/679 ja õiguskaitse valdkonna direktiiv 2016/680. Kuigi isikuandmete üldmäärus on küll otsekohalduv, eeldati, et liikmeriigid ajakohastavad siseriiklikke andmekaitseseadusi, et viia need määrusega vastavusse.

Institutsiooniks, mis on võimeline ja pädev otsustama, kas liikmesriik on täitnud ELi andmekaitseõigusaktidest tulenevad kohustused ning tõlgendama ELi õigusakte, on EK. Alates 2014. aastast ja nn märgilisest kohtulahendist *Digital Rights Ireland* on lisandunud hulk kohtupraktikaid, mille raames on menetletud erinevate liikmesriikide institutsioonide, õiguskaitseasutuste, ametite, sh jälitusasutuste ja julgeolekuasutuste isikuandmete kogumise/töötlemise ja kasutamisega seotud juhtumeid erinevates Euroopa liikmesriikides.

Selleks, et mõista varjatud teabe kogumise ja jälitustegevuse erinevusi, käsitleb töö autor lühidalt ka Elektroonilise side seaduse puudujääke. Euroopa Kohtu Suurkoda on Eesti Riigikohtu taotlusel teinud otsuse, kus on välja toodud Elektroonilise side seaduse vastuolu EL-i seadusandlike seisukohtadega. Vaatamata sellele kohtuotsusele ja asjaolule, et ka õigusteadlased on juhtinud tähelepanu ebakohtadele, ei ole Eesti seadusloomes muutmismenetlust algatatud. Käesoleva uurimistöö kirjutamise käigus intervjueeris töö autor mitmeid valdkondlikke eksperte ning ka nemad möönsid, et vastuolu on olemas ja vajab seadusandluses muudatuste sisseviimist, kuid muudatusmenetlust ei ole algatatud. Põhjuseks toodi soov oodata hetkel EK menetluses olevate kohtuasjade lahendeid, et muudatused saaks tuleneda nendes lahendites toodud seisukohtadest.

Eesti siseriiklikus seadusandluses on julgeolekuasutuste õigused isikute sideandmete kogumiseks ja töötlemiseks koondatud Julgeolekuasutuste seadusesse, kus on sätestatud ka piirangud jälitustegevuse kestvusele, reguleeritud koostöö ja andmevahetus teiste ametkondade, ettevõtete ja välispartneritega ning ühtlasi järelevalve kord ja institutsioonid.

EIK tõi 2021. aasta kohtulahendis *Centrum för Rättvisa v. Sweden* välja kaheksa olulist kriteeriumit, millele liikmesriikide seadusandlus peab vastama põhjendamaks Euroopa Liidu põhiõiguste harta

artikkel 8 riivet. Sellest tulenevalt peab ka Eesti siseriiklik regulatsioon määratlema: süüteod ja isikute ringi, mille korral on varjatud isikuandmete kogumine põhjendatud; kehtestama ajalise piirangu andmete kogumisele ja kogutud andmete säilitamisele; määratlema kogutud andmete kasutamise, kustutamise ja hävitamise põhimõtted, ettevaatusabinõud andmete edastamisel teistele isikutele ning järelevalve korra koos volituste loeteluga.

Analüüsides Eesti siseriiklikku seadusandlust ja selle kooskõla eelpool loetletud EIK kriteeriumitega, jõudis töö autor järeldusele, et Eesti seadusandluses ei ole määratletud süütegude ja isikute loetelu, mille korral varjatud teabehange on põhjendatud. EIK on samuti pidanud süütegude ja isikute ringi määratlemist kõigist aspektidest kõige raskemini saavutatavateks. Teise olulise erinevusena toob töö autor välja kogutud andmete säilitamise määratlemise. Eesti seadusandluses on julgeolekuasutuste õigus andmeid säilitada, sh vajadusel võimalus ka töödelda määratlemata. Seaduse sõnastus „nii kaua, kui see on vajalik“ erineb Euroopa institutsioonide seisukohast, kus eeldatakse konkreetset ajalist määratlemist. Ootused jälitustegevuse kestvusele määratlemisele, kasutamise-säilitamise-hävitamise kord, koostöö teiste institutsioonidega ja järelevalve on Eesti õigusruumis leitavad erinevatest regulatsioonidest nagu JAS, valdkondliku ministri määrus ja RSVS.

Tulenevalt viimastest Euroopa Kohtu ja Euroopa Inimõiguste Kohtu lahenditest vajab Eesti siseriiklik õigusregulatsioon, sh ESS ja JAS, muutmist ning Euroopa Liidu lähtekohtadega kooskõlla viimist, tagamaks Euroopa Liidu põhiõiguste harta artiklist 8 ja Eesti Vabariigi PS § 26-st tulenev õigus isikuandmete kaitsele. EIK kaheksast vajalikust kaitsemeetmest on JAS-is, õiguskantsleri seaduses ja valdkondlike ministrite määrustes kaetud enamik. Samas on EIK seisukohal, et õigusselgus on tagatud vaid juhul, kui kaetud on kõik kaheksa. Seega on vaja Eesti seadusandluses määratleda ka kaks puuduvat kriteeriumit ehk süütegude ja isikute loetelu ning konkretiseerida säilitamise ja töötlemise ajamääratlus.

Kokkuvõtteks teeb autor järelduse, et magistritöös püsitatud hüpoteesid leidsid kinnitust osaliselt. Vastavalt EK väljakujunenud praktikale on nõutud, et põhiõiguste kaitse erandid piirduksid ainult tingimata vajalikega. EIK on omakorda oma lahendites defineerinud kaheksa kaitsemeedet, millele peab vastama siseriiklik regulatsioon, tagamaks olukord, kus siseriiklik õigus on kohaldamisel juurdepääsetav, ettenähtav ja tagab, et salajasi jälgimismeetmeid rakendatakse ainult juhul, kui see on demokraatlikus ühiskonnas vajalik. Lisaks peavad olema sätestatud piisavad ja tõhusad kaitsemeetmed ning tagatised kogutud andmete kuritarvitamise vastu. Ei Euroopa Liidu ega Eesti siseriiklik seadusandlus sätesta kindlaid reegleid sideandmete säilitamiseks ja töötlemiseks signaalluure raames, kuid need tulenevad EK ja EIK kohtulahenditest. Tulenevalt julgeoleku tagamise aspektidest on kodanike elektrooniliste

sideandmete privaatsuse ja eraelu puutumatuse riive, sh isikuandmete kogumine, säilitamine ja kasutamine, õigustatud. Nimelt, EL-i aluslepingutes ehk esmases õiguses austab põhiõiguste harta eraelu puutumatuse õigust isikuandmete kaitsele, kuid kodanike julgeoleku tagamine jäetakse liikmesriigi ainuvastutusse.

Üldmäärus 2016/679 võimaldab piirata seadusandliku meetme direktiiviga 2016/680 pädevateks loetud asutustel andmesubjekti õigusi isikuandmete kogumisel/töötlemisel, kui selline piirang on vajalik ja proportsionaalne meede riigi julgeoleku tagamiseks.

Sellega hindab autor, et magistritööle püstitatud uurimiseesmärk on saavutatud ja töö järeldused võimaldavad vastavatel ametkondadel viia õigusselguse saavutamiseks Eesti siseriiklik seadusandlus vastavusse Euroopa Liidu regulatsioonidega.

SUMMARY

Privacy policy and processing of personal communication data for the purposes of security using signals intelligence.

One feature of a democratic society is the existence of personal freedoms. As residents of Estonia as a democratic state, we do not think about our rights and freedoms daily as we take it all for granted. At the same time, we live in a world where we are increasingly using all kinds of electronic communications channels and platforms, which have now become intermediaries between people and government Due to the technological and social development of electronic communications over the last two decades, the European Court of Human Rights has found that modern communications data can reveal a lot of personal data. When collecting data the institution can create an intimate picture of a person, if necessary, by mapping social networks, tracking location, tracking internet browsing and mapping communication patterns, and an overview of who the person has interacted with.

The research problem of this Master's thesis is based on ensuring the privacy of personal electronic communications data and ensuring national security in the common legal space of the European Union and, consequently, ensuring security objectives through intelligence activities in the Republic of Estonia.

The aim of the author's research was to find out whether the legal regulation of the Republic of Estonia follows the principles of democracy and recognises the principles of Europe in ensuring security through the collection of hidden information, i.e. (signals)intelligence and does it comply with the legal principles of the European Union for the protection of personal data?

The author of the Master's thesis raised two central research hypotheses: the national and legal regulations of the European Union and Estonia do not set out specific rules for recording and processing communications data within the framework of signal intelligence, and due to security aspects, the privacy of citizens' electronic communications data can be violated.

In addition following research topics that were important to understand: such as privacy, security and the collection of information had to be covered.

To verify the validity of the hypotheses and find answers to research questions, the author of the work studied the existing European Union regulations on the protection of communications data, explanatory notes submitted in the course of legislative drafting, legal literature and articles, international case law, legal opinion articles of practitioners and theorists, publicly available

analyses of security authorities, judgments of the European Court of Justice, the European Court of Human Rights and Estonian court decisions, master's and doctoral papers. Based on the above, the empirical method of research was a combined analysis of documents from case-law, legislation, and theoretical literature.

Given that the author of the work does not have a state secret permit that would allow access to documents intended for official use and are protected by state secrets, the author had to rely only on publicly available sources to carry out the research. To compensate this restriction, the author turned to several sectoral experts to open the areas of concern in the form of interview. In total, the author turned to thirteen representatives of different agencies and institutions for an interview, eight of whom agreed to carry out the interview. The three selected experts did not wish to respond due to the sensitivity of the subject matter and two experts withdrew from responding because they did not consider themselves to be experts in the field. Because some experts requested anonymity, the names, and positions of specific experts in this work will not be specified. The list of source materials used contains the dates of the interviews, but the substantive part of the work refers to the explanations and reasons received during the interviews without naming the direct source.

Privacy is by its very nature a very complex concept and a new important aspect of cyber component has been added. The right for privacy, which includes the right to self-determination of information, is the person's control over self-identified information, including electronic communications data, as part of the person’s privacy area. It is therefore also important to understand the structural logic of personal data, which Estonian jurisdiction is somewhat different compared to EU law.

The next important issue is security. Security is essentially a social construct. The philosophers have debated the balance between personal freedoms and collective security for millennia. Similarly, to the concept of privacy, technological developments and the addition of a cyber component have also brought new aspects approaches. The field is still developing and doing it rapidly, so the common terminology has not yet been developed. A item of security in the narrowest sense, may be regarded as protection of the status of a person and thing and, in the broadest sense, as continuation of the current position of the person and thing with the aim of performing its principal functions. Based on the purpose of the investigation, the author discussed the nature of security and the methods of ensuring it and intelligence as a tool of security authorities.

At national level, the object of security is the enduring of the state as such and the performance of its main functions. In the Republic of Estonia, this means ensuring the continuity of statehood and preventing security threats that could damage a person, system or society.

Information on the intelligence and influence activities of a hostile party shall be collected and processed in order to prevent and prevent activities endangering the constitutional order. One method of identifying threats is surveillance. Surveillance is generally characterised by a lack of supervised powers for such activities.

Intelligence as a whole contains different methods or disciplines, in English called INT-s, one of which is signal intelligence or SIGINT. SIGINT, that includes communications, electronic channels, radars, apparatus signals and cyber intelligence, is a specific interest on current research.

In the Republic of Estonia, the security authorities are the Estonian Internal Security Service (KAPO) and the Estonian Foreign Intelligence Service (VLA). The task of KAPO is to ensure the internal security of the state by collecting information and using prevention tools, investigating offences and implementing measures to prevent intelligence and subversion activities against the Estonian state. The function of the VLA is to ensure national security by using non-military preventive means to maintain the constitutional order and the collection and processing of information necessary for the development of security policy and national defence, including the collection and processing of information in cyberspace, i.e. through digital infrastructure.

The third sub-topic binding on privacy and security is the regulation of the privacy of private persons in the legislation of the European Union and the Republic of Estonia, including whether the directly applicable regulations of the European Union have a role in Estonian law enforcement and the directives have been transposed into national legislation. How the decisions of the Court of Justice of the European Union (EC) and the European Court of Human Rights (ECHR) have affected Estonia's national legislation and its development.

In order to achieve the objectives of the investigation, the following facts have emerged: in the area of the protection of personal data of persons, there has been a steady development over the last thirty years. In 2018, the last General Data Protection Regulation 2016/679 and Law Enforcement Directive 2016/680 entered into force. Although the GDPR is directly applicable, Member States were expected to update national data protection laws in order to bring them into line with the Regulation.

The institution capable and competent to decide whether a Member State has fulfilled its obligations under EU data protection legislation and to interpret EU legislation is the EC. Since

2014 and the so-called 'significant judgment' in Digital Rights Ireland has included a number of case-laws concerning the collection/processing and use of personal data by institutions, law enforcement authorities, authorities, including supervisory authorities and security authorities in different European Member States.

In order to understand the differences between the collection of hidden information and surveillance activities, the author of the work also briefly addresses the shortcomings of the Electronic Communications Act. At the request of the Supreme Court of Estonia, the Court of Justice has ruled on the conflict of the Electronic Communications Act with the legislative positions of the European Union. Despite this judgment and the fact that legal scholars have also pointed out the shortcomings, no amendments have been initiated in Estonian legislation. In the course of writing this research, the author of the paper interviewed several experts in the field, and they also admitted that there is a contradiction and that changes in the legislation are needed, but no amendment procedure has been initiated. The reason for this was the desire to wait for the judgments in the cases currently pending in EC, so that the amendments could result from the positions set out in these judgments.

In Estonian national legislation, the rights of security authorities for the collection and processing of personal communications data are consolidated in the Security Authorities Act, which also provides for restrictions on the duration of surveillance activities, regulated cooperation and exchange of data with other bodies, companies and foreign partners, and also the procedure for supervision and surveillance institutions are present.

Most of the necessary from the eight protection measures outlined by the EHRC are provided for in Estonian legislation.

In the 2021 judgment *Centrum för Rättvisa v. Sweden,* the ECHR developed minimum requirements that should be set out in law to avoid abuses of power and that have to be met by national legislation to ensure fair safeguards against the justification of the breach of Article 8 of the Charter of Fundamental Rights of the European Union. Consequently, Estonian national regulation must also define: the nature of offences and definition of the categories of people liable to have their communications intercepted; a limit on the duration of interception; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which intercepted data may or must be erased or destroyed; and the procedure for supervision together with the list of powers.

Those which the ECHR considers difficult to achieve – the list of offences and persons – have not been defined in Estonian legislation. Estonian legislation leaves the possibility for security authorities to store and process data for an unspecified period by formulating it – as long as it is necessary, although the position of the European institutions is to define a specific time frame. Criteria – restrictions on the duration of surveillance activities, the procedure for use, preservation and destruction, co-operation with other institutions and supervision can be found in the Estonian legislation in different laws and acts such as JAS, regulation of the sectoral minister and RSVS.

Based on the latest judgments of the EC of Justice and the ECHR, Estonia's national legal regulation, including Electronic Communications Act and Security Authorities Act, needs to be amended and brought into line with the European Union's sources in order to ensure the right to the protection of personal data arising from Article 8 of the Charter of Fundamental Rights of the European Union and § 26 of the Constitution of the Republic of Estonia. The majority of the eight necessary protection measures of the EHRC are covered by the Act and Security Authorities Act, the Chancellor of Justice Act and sectoral ministerial regulations. At the same time, the ECHR is of the opinion that legal clarity is ensured only if all eight are covered. Thus, it is also necessary to define two missing criteria in Estonian legislation, i.e., the list of offences and persons, and to specify the definition of storage and processing time.

In conclusion, the author concludes that the hypotheses of current Master’s thesis were partially confirmed. In accordance with the established practice of the EC, it is required that exceptions to the protection of fundamental rights have to be limited to what is strictly necessary. The ECHR, in turn, has defined in its decisions eight safeguards to be met by national regulation in order to ensure that national law is accessible, predictable in application and to ensure that secret surveillance measures are implemented only where necessary in a democratic society. In addition, adequate and effective safeguards must be in place against the abuse of the data collected. The national legislation of the European Union or Estonia does not provide for specific rules for the storage and processing of communications data within the framework of signal intelligence, but they arise from the judgments of the EC and the ECHR. Due to security aspects, it is justified to infringe the privacy and privacy of citizens' electronic communications data, including the collection, storage and use of personal data. Namely, in the EU Treaties, or primary law, the Charter of Fundamental Rights respects the right to privacy to the protection of personal data but ensuring the security of citizens is left to the responsibility of the Member States.

General Regulation 2016/679 allows, by means of a legislative measure, the authorities designated competent by Directive 2016/680 to restrict the rights of data subjects in the collection/processing of personal data where such a restriction is necessary and proportionate to ensure national security.

The author assesses that the research objective established for the Master's thesis has been achieved and that the conclusions of the thesis allow the respective agencies to bring the Estonian national legislation into conformity with the regulations of the European Union in order to achieve legal clarity.

KASUTATUD MATERJALID

Kasutatud kirjandus

1. Alexandrou, A. Cybercrime and Information Technology. 1st edn. Taylor and Francis, 2021. Kättesaada: vhttps://www.perlego.com/book/2529243/cybercrime-and-information-technology-theory-and-practice-the-computer-network-infostructure-and-computer-security-cybersecurity-laws-internet-of-things-iot-and-mobile-devices-pdf?queryID=31aa299c18a9cab249710d228d37509d&index=prod_BOOKS&gridPosition=1 (26.11.2022)
2. Bernard, R. L. Electronic Intelligence (ELINT) at NSA. Center for Cryptologic History. National Security Agency. 2009, Kättesaadav: https://permanent.access.gpo.gov/gpo7719/elint.pdf (22.01.2023).
3. Bulk Collection of Signals Intelligence: Technical Options. Computer Science and Telecommunications BoardNational Academy of Sciences. 2015. Kättesaadav: https://nap.nationalacademies.org/catalog/19414/bulk-collection-of-signals-intelligence-technical-options. (06.01.2023).
4. Choudry, A. (2018) Activists and the Surveillance State. 1st edn. Pluto https://www.perlego.com/book/840005/activists-and-the-surveillance-state-learning-from-repression-pdf .
5. Clark, R. M. Guide to the Study of Intelligence. Perspectives on Intelligence Collection. Journal of U.S.
6. Intelligence Studies. Association of Former Intelligence Officers. Volume. Number 2. Fall/Winter 2013. lk 47–53.
7. Denemark, R.A., Marlin-Bennett, R. The International Studies Encyclopedia Wiley-Blackwell Print. Published online: 2017. https://www-oxfordreference-com.ezproxy.utlib.ut.ee/view/10.1093/acref/9780191842665.001.0001/acref-9780191842665-e-0168?rskey=6HvpO9&result=2. (10.12.2022)
8. Ernits, M. Konkreetne normikontroll de *lege lata* ja *de lege ferenda*. Juridica VIII 2001, lk 572–596.
9. Heldna, E. Julgeolekuasutuste kogutud informatsiooni kasutamine kriminaalmenetluses ja jagamine uurimisasutustega. Juridica X/2016, lk 718–726.

10. Jaanimägi, K. Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. Madise, Ü jt (toim) Kommenteeritud väljaanne 5, Sihtasutus Juridicum 2020.
11. Juurvee, I. Riigisaladuse kaitse Eesti Vabariigis 1918–1940. Tartu Ülikool 2013
12. Juurvee, I. 100 aastat luuret ja vastuluuret Eestis. Post Factum 2018.
13. Jäätma, J. Julgeoleku mõiste.Juridica 2/2020, lk 771–78.
14. Jäätma, J. Ohutõrjeõigus politsei- ja korrakaitseõigused: kooskõla põhiseadusega. Tartu Ülikool 2015.
15. Kaska, K., Aasmann, L. Julgeolekuasutuste roll küberjulgeoleku tagamisel ja seda mõjutavad suundumused rahvusvahelises õiguses. Juridica 2/2020, lk 102–116.
16. Kergandberg, E. Luurates „Teeme ära“ meeskonnaga kevadisel jälitusmaastikul. Juridica 3/2020, lk 214.
17. Kärtna, L.A. Euroopa Liidu Somaalia merepiraatluse julgeolekustamine. Tartu Ülikool 2014.
18. Lazarus.L., Goold, B.J. Security and Human Rights: The Search for a Language of Reconciliation https://lawexplores.com/introduction-security-and-human-rights-the-search-for-a-language-of-reconciliation/ (26.11.2022)
19. Lott, A. Põhiseadusliku korra kaitseks teostatav jälitustegevus Eestis. Analüüs. Põhiseaduslikkuse Järelevalve Kolleegium. 2015.
20. Lõhmus, U. jt Eesti Vabariigi põhiseaduse kommentaarid. Eesti Teaduste Akadeemia Riigiõiguse Sihtkapital 2022.
21. Lõhmus, U. Elektroonilise side metaandmete säilitamise ja kasutamise saaga uued peatükid. Juridica 3/2021, lk 167–179.
22. Lõhmus, U. Repliik. H. Kalmo. Põhiseaduse Põkkumine Euroopa Liidu põhiõiguste Hartaga. Juridica 4/2016, lk 292–293.
23. Lõhmus, U. Quo vadis, kriminaalmenetlus? Juridica 3/2020, lk 198–209.
24. Manjikian, M. Cybersecurity Ethics. 1st ed. Taylor and Francis.2017. https://www.perlego.com/book/1573596/cybersecurity-ethics-an-introduction-pdf (26.22.2022)
25. Maruste, R. Martensi klausli idee mõjust tänapäevasele riigi- ja karistusõigusele. Inimõiguste aastaraamat 2021. Lk 247–267.
26. Mikiver, M., Tikk, E. Informatsioonilise enesemääramise õiguse tagamise diskretsiooniotsused haldusmenetluses. Juridica IV/2005, lk 250–258.
27. Murumaa-Mengel, M., Pruulmann-Vengfeld, P., Laas-Mikko, K. Privaatsusõigus inimõigusena ja igapäevatehnoloogiad. Tartu Ülikool 2014.

28. Mälksoo, M. Akadeemilised julgeoleku-uuringud sõja ja rahu vahel. Akadeemia 2009 nr 9, lk 1768. https://www.digar.ee/viewer/et/nlib-digar:104149/162371/page/73. (10.12.2022)
29. Purre, M. Riigireetmine ja riigireetur. Juridica 2/2020, lk 79–89.
30. Pärnamägi, I. „Riikliku sekkumise eesmärgi kindlakstegemise praktiline pool. Mitmefunktsiooniliste meetmete probleem.“ Juridica 3/2019, lk 189–204.
31. Reissar, M. Privaatsus vs turvalisus: riigiteooriate konflikt küberkuritegevuse ja tehnoloogiaajastul. Tartu Ülikool 2021.
32. Rozenshtein. A. Z., Surveillance Intermediaries. Stanford Law Review 70, no. 1, January 2018, lk 99–190.
33. Sinisalu, S. Virks, K. Õige vähe õige paljust ehk turvalisuse ja julgeoleku mõningatest tahkudest õiguse laia tõlgenduse kontekstis. Juridica 5/2022, lk 360–367.
34. Solove, D.J. Conceptualizing Privacy. California Law Review,, 2002/90, lk 1087–1155. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=313103 (26.11.2022).
35. Solove, D.J. Understanding Privacy. Harvard University Press. 2010 https://www.perlego.com/book/1148540/understanding-privacy-pdf (26.11.2022).
36. Tsemin, A., Antson, A. Kas anonüümsed kommentaatorid saavad side andmete kasutamise regulatsiooni valguses rahulikult magada? Juridca 7/2022, lk 473–483.
37. Virks, K. Sideandmed ja nende säilitamise olulisus. Juridica 8/2018. lk 581–596.
38. Wiritz, J.J., Rosenwasser. JJ. From Combined Arms to Combined Intelligence: Philosophy Doctrine and Operations. Intelligence and National Security. Vol. 25, No. 6, Routledge December 2010, lk 725–743.
39. Zichichi, M., Ferretti, S., D'Angelo, G., Rodríguez-Doncel, V. Data governance through a multi-DLT architecture in view of the GDPR. Cluster Computing volume 25, 2022, lk 4515–4542.

Rahvusvahelised ja EL-i õigusaktid

40. ÜRO Inimõiguste ülddeklaratsioon, võetud vastu ÜRO Peaassamblee https://www.un.org/en/about-us/universal-declaration-of-human-rights (26.11.2022).
41. Euroopa Liidu põhiõiguste harta. 2010/C 83/02.
42. Euroopa Liidu toimimise lepingu konsolideeritud versioon. – ELT C 326, 26.10.2002.

43. Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta, EÜT 1995 L 281, lk 355–374.
44. Euroopa Parlamendi ja nõukogu 27. aprill 2016. aasta määrus EL 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). ELT 2016 L 119, lk 1–88.
45. Nõukogu raamotsus 2008/977/JSK kriminaalasjades tehtava politsei- ja õigusalase koostöö raames töödeldavate isikuandmete kaitse kohta, ELT 2008 L 350.
46. Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta direktiiv EL 2016/680, 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, ELT L 119, lk 89–131.
47. Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatuse ja elektroonilise side direktiiv ehk e-privaatsuse direktiiv. ELT 2002 L 201, lk 514–524.
48. Euroopa Parlamendi ja nõukogu 15. märts 2006. aasta direktiiv 2006/24/EÜ mis käsitleb üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist ja millega muudetakse direktiivi 2002/58/EÜ. ELT 2006 L 105, lk 54–63.
49. Euroopa Parlamendi ja nõukogu direktiivi EL 2018/197 11. detsember 2018, millega kehtestatakse Euroopa elektroonilise side seadustik (uuesti sõnastatud). ELT 2018 L 321, lk 36–201.

Eesti Vabariigi õigusaktid

50. Eesti Vabariigi Põhiseadus. – RT I, 15.05.2015, 2.
51. Eesti julgeolekupoliitika alused. Lisa Riigikogu otsusele „Eesti julgeolekupoliitika alused“ heakskiitmine. – RT III, 06.06.2017, 2.
52. Elektroonilise side seadus. – RT I, 27.02.2022, 3
53. Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni. – RT II 1996, 11, 34
54. Julgeolekuasutuste seadus. – RT I, 31.12.2022, 11.
55. Kaitseministeeriumi põhimäärus. – RT I, 27.08.2022.

56. Kaitsepolitsei põhimäärus. – RT I, 07.11.2014,
57. Kaitsepolitseiameti poolt teabe varjatud kogumisel kasutatavad meetodid ja vahendid ning teabetoimiku pidamise ja säilitamise kord. – RT I, 02.08.2017, 7.
58. Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon. – RT II 2001, 1,
59. Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni muutmise protokoll. – RT II, 03.07.2020, 2.
60. Isikuandmete kaitse seaduse rakendamise seaduse. – RT I, 13.03.2019, 2.
61. Kaitseministri määrus. Välisluureameti teabetoimiku pidamise ja säilitamise kord: 2017 https://adr.rik.ee/kmin/dokument/8422668.
62. Kodaniku- ja poliitiliste õiguste rahvusvaheline pakt. – RT II 1994, 10, 1.
63. Korrakaitseseaduse. – RT I, 06.08.2022, 16.
64. Kriminaalmenetluse seadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seadus. – RT I, 29.06.2012.
65. Riigisaladuse ja salastatud välisteabe seadus. – RT I, 06.05.2020, 36.
66. Riigikaitseseadus. –RT I, 09.08.2022, 18.
67. Riigi Kaitsepolitseiameti põhimääruse ja Operatiivtehniliste erimeetmete rakendamise ajutise korra kinnitamine. – RT I 1993, 53, 734.
68. Vabariigi Valitsuse määrus. Politsei- ja Piirivalveameti ja Kaitsepolitseiameti vaheline uurimisalluvus. – RT I, 07.05.2019, 4.
69. Välisluureameti põhimääruse. – RT I, 17.12.2021, 12.
70. Välisluureameti poolt teabe varjatud kogumisel kasutatavad meetodid ja vahendid. – RT I, 28.06.2017, 9.
71. Õiguskantsleri seadus. – RT I, 26.05.2020, 11.
72. ÜRO Kodaniku- ja poliitiliste õiguste rahvusvaheline pakt. – RT II 1994, 10, 11.

Seaduseelnõude seletuskirjad

73. Elektroonilise side seaduse ja sellega seonduvalt teiste seaduste muutmise eelnõu väljatöötamiskavatsus (sideandmete säilitamine ja kasutamine) EELNÕU 31.10.2018 https://eelnoud.valitsus.ee/main/mount/docList/947260b9-64e7-4190-9319-32ecac6e6f83#n1wMfuem.
74. Elektroonilise side seadus. Seletuskiri. Sisukokkuvõte.https://www.just.ee/sites/www.just.ee/files/elfinder/article_files/ehitusseadustiku_eelnou_seletuskiri_2013.pdf .

75. Isikuandmete kaitse seaduse eelnõu. Seletuskiri. https://www.aki.ee/sites/default/files/dokumendid/reform/iks_sk_21.03.18.pdf.
76. Isikuandmete kaitse seaduse rakendamise seadus. Seletuskiri RT I, 13.03.2019, 2 https://www.riigiteataja.ee/akt/113032019002.
77. Korrakaitseseaduse muutmise ja rakendamise seaduse eelnõu. Seletuskiri. https://www.riigikogu.ee/tegevus/eelnoud/eelnou/2445bcfe-b04d-40c8-932edb51253abea3/Korrakaitseseaduse%20muutmise%20ja%20rakendamise%20seadus.
78. Politsei ja piirivalve seaduse ning päästeteenistuse seaduse muutmise ning sellega seonduvalt teiste seaduste muutmise seadus. Seletuskiri. https://www.riigikogu.ee/tegevus/eelnoud/eelnou/2d545b21-de81-4a18-8aec-d4de49d36d63.
79. Riigikaitseseaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu. Seletuskiri. https://www.riigikogu.ee/tegevus/eelnoud/eelnou/44178720-02b2-4d30-8707-d7dcf606dcee.
80. Riigisaladuse ja salastatud välisteabe seaduse eelnõu. Seletuskiri. https://www.riigikogu.ee/tegevus/eelnoud/eelnou/305b4804-a456-3cb8-935e-5fb113ff2f40/Riigisaladuse%20ja%20salastatud%20v%C3%A4listeabe%20seadus.
81. Seletuskiri isikuandmete kaitse seaduse rakendamise seaduse eelnõu juurde https://www.riigikogu.ee/tegevus/eelnoud/eelnou/9d1420bb-b516-4ab1-b337-17b2c83eedb1.

Kohtulahendid

82. RKKKo 18.06.2021 1-16-6179.
83. EKKKm 12.11.2018 1-16-6179.
84. RKHKo 10.06.2016 3-3-1-84-15
85. RKKKo 23.02.2015 3-1-1-51-14.
86. RKHKo 12.07.2012 3-3-1-3-12.
87. RKKKo 26.08.1997 3-1-1-80-97.
88. EKo 21.06.2022 C-817/19, *Ligue des droits humains vs Conseil des ministres,* ECLI:EU:C:2022:491.
89. EKo 22.06.2021 C-718/19. *Ordre des barreaux francophones et germanophone,* ECLI:EU:C:2021:505, kohtujurist M. C. Sànchez-Bordona. Ettepanek.

90. EKo 02.03.2021, C-746/18 *HK vs Prokuratuur,* ECLI:EU:C:2021:152.
91. EKo 06.10.2020 C-623/17*, Privacy International vs Secretary of State for Foreign and Commonwealth Affairs,* ECLI:EU:C:2020:790.
92. EKo 06.10.2020, liidetud kohtuasjad C-511/18, C-512/18 ja C-520/18. *La Quadrature du Net*, ECLI:EU:C:2020:791.
93. EKo 06.10.2020 C-623/*17 Privacy International vs Secretary of State for Foreign and Commonwealth Affairs,* ECLI:EU:C:2020:790, kohtujurist M. C. Sànchez-Bordona.ettepanek.
94. EKo 02.10.2018, C-207/16, Ministerio Fiscal, ECLI:EU:C:2018:788.
95. EKo 21.12.2016, liidetud kohtuasjad C-203/15 ja C-698/15, Tele2 Sverige AB ECLI:EU:C:2016:970.
96. EKo 08.04.2014, liidetud kohtuasjad C-293/12 ja C-594/12, Digital Rights Ireland Ltd. ECLI:EU:C:2014:238.
97. EIKo 11.01.2022 nr 70078/12, Ekimdzhiev and Others v. Bulgaria.
98. EIKo 25.05.2021, nr 35252/08 Centrum för Rättvisa v. Sweden..
99. EIKo 25.05.2021, nr 58170/13, 62322/14, 24960/15 Big Brother Watch and Others v. The United Kingdom.
100. EIKo 04.12.2015, nr 47143/06, Roman Zakharov v. Russia.
101. EIKo 02.01.2013 nr 22491/08, Sefilyan vs. Armeenia.
102. EIKo 26.06.2006, nr 54934/00, Weber ja Saravia vs Germany.
103. EIKo 18.05.2010, nr 26839/05, Kennedy vs the United Kingdom.

Muud allikad

104. Andmekaitse ja infoturbe leksikon. Cybernetica 2011-2023 https://akit.cyber.ee/. (15.01.2023)
105. Andmeühiskonna tulevik. Stsenaariumid aastani 2035. Raport. Tallinn: Arenguseire Keskus. 2022. https://arenguseire.ee/wp-content/uploads/2022/12/2022_andmeyhiskonna-tulevik_raport.pdf (05.01.2023).
106. Eesti rahvusvahelises julgeolekukeskkonnas 2022. https://raport.valisluureamet.ee/et/eessona (13.01.2023).
107. Eesti rahvusvahelises julgeolekukeskkonnas 2018. https://raport.valisluureamet.ee/et/eessona (13.01.2023).
108. Eesti rahvusvahelises julgeolekukeskkonnas 2017. https://www.valisluureamet.ee/doc/raport/2017-et.pdf (13.01.2023).

109. Eesti õigekeelsussõnaraamat 2018. http://www.eki.ee/dict/qs/index.cgi?Q=seire&F=A (28.1.2022).
110. Euroopa andmekaitseõiguse käsiraamat. 2018 väljaanne. Euroopa Liidu Põhiõiguste Amet ja Euroopa Nõukogu 2020. https://www.aki.ee/sites/default/files/inspektsioon/rahvusvaheline/juhised/fra-coe-edps-2018-handbook-data-protection_et.pdf (27.12.2022).
111. Euroopa Nõukogu, Venice Commission Report on the Democratic Oversight of Signals Intelligence Agencies, 2015. https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)011-e (24.01.2023)
112. Chapter 50 of US Criminal Code, Section 1801 https://www.govinfo.gov/app/collection/uscode/2021/title50/-1 (28.12.2022).
113. Küberturvalisuse strateegia 2019-2022. Majandus- ja Kommunikatsiooniministeerium kuberturvalisuse_strateegia_2019-2022_0.pdf (03.02.2023).
114. Metaandmed ja privaatsus. Juhis organisatsioonidele ja kodukasutajale seaduse rakendamisel. Andmekaitseinspektsioon 2015. https://www.aki.ee/sites/default/files/dokumendid/metaandmed.pdf (06.01.2023).
115. Organization for Economic Cooperation and Development: Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188 www.privacy.gov.au/publications/oecdgls.doc (06.01.2023).
116. Riigikaitse arengukava 2022–203. Riigikantselei 2021. https://www.riigikantselei.ee/el-poliitika-julgeolek-ja-riigikaitse/julgeoleku-ja-riigikaitse-koordineerimine (14.01.2023).
117. Riigikogu õiguskomisjoni istungi protokoll nr 95, 17. mai 2021.
118. Riigikogu õiguskomisjoni istungi protokoll nr 104, 13. september 2021.
119. Riigikogu õiguskomisjoni istungi protokoll 07. detsember 2021.
120. Taktikatasandi luure käsiraamat. Eesti Kaitsevägi 2020.
121. The International Studies Encyclopedia. Edited by: Robert A. Denemark and Renée Marlin-Bennett Wiley-Blackwell Print 2017.https://www-oxfordreference-com.ezproxy.utlib.ut.ee/view/10.1093/acref/9780191842665.001.0001/acref-9780191842665-e-0168?rskey=6HvpO9&result=2. (10.12.2022)
122. https://sonaveeb.ee/search/unif/dlall/mil/luure/1 (15.01.2023).

Ülevaade ekspertintervjuudest:

1. Intervjuu luurevaldkonna eksperdiga 02..01.2023.
2. Intervjuu jälitustegevuse eksperdiga 05.01.2023.
3. Intervjuu seadusloome eksperdiga 16.01.2023.
4. Intervjuu luurevaldkonna eksperdiga 18.01.2023.
5. Intervjuu luurevaldkonna eksperdiga 29.01.2023.
6. Intervjuu seadusloome eksperdiga 15.02.2023.
7. Intervjuu jälitustegevuse eksperdiga 16.02.2023.
8. Intervjuu jälitustegevuse eksperdiga 03.28.2023.