3. Privaatsus, isikuandmete kaitse ja tehnoloogia

Mitmes meie kultuuriruumis inimõigusi käsitlevas põhidokumendis, nagu Euroopa inimõiguste ja põhivabaduste konventsioon[1] , Euroopa Liidu põhiõiguste harta[2] ning Eesti Vabariigi põhiseadus[3] , pole terminit *privaatsus* otsesõnu kasutatud. Selle asemel sätestavad Euroopa inimõiguste konventsioon (art 8), Euroopa Liidu põhiõiguste harta (art 7) ja Eesti põhiseadus (§-d 26, 33, 43) perekonna- ja eraelu ning kodu puutumatuse ja sõnumisaladuse kaitse.

Privaatsust mainitakse siiski eraldi mitmes teises inimõiguste kaitset käsitlevas olulises rahvusvahelises dokumendis, näiteks ÜRO inimõiguste ülddeklaratsioonis (artikkel 12). Selget privaatsuse definitsiooni otsides jääme aga hätta, sest privaatsuse mõiste ei ole üheselt defineeritud ning võib hõlmata mitmeid sotsiaalseid ning kultuurilisi mõõtmeid, samuti mõjutab õiguse piire näiteks tehnoloogia areng.[4] Selle peatüki autorid pooldavad laiahaardelist lähenemist, mille järgi kuuluvad privaatsusõiguse alla perekonna-, eraelu ning kodu puutumatus ja sõnumisaladuse kaitse.

Tuleb nentida, et tehnoloogia tormiline areng on kaasa toonud olukordi, kus nii Euroopa kui ka kodumaistel kohtutel on keeruline selgelt piiritleda sõnumisaladuse, perekonna- ja eraelu ning kodu puutumatuse kaitsealasid. Selge piiritlemise asemel liigub rahvusvaheline kohtupraktika paindlikuma lähenemise suunas, kus teatud inimõiguste vahel on nii tihe seos, et näiteks Euroopa Inimõiguste Kohus ei püüagi alati kaitsealasid eristada ning võib tunnistada mõlema õiguse üheaegset riivet.[5] Nimetatud õiguste kaitsealade ning tõlgendamise kohta on ohtralt kohtupraktikat.[6]

Lisaks eespool nimetatud neljale inimõigusele – perekonna-, eraelu ning kodu puutumatus ja sõnumisaladuse kaitse – tuleb eraldi tähelepanu pöörata isikuandmete kaitse õiguslikule regulatsioonile. Esimene rahvusvaheline andmekaitsele keskendunud riikidevaheline leping oli isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon, mis võeti vastu 1981. aastal.[7] Isikuandmete kaitset on mainitud ka Euroopa Liidu põhiõiguste harta artiklis 8.

Samas tuleb märkida, et inimõigusena ei mainita isikuandmete kaitset ei Euroopa inimõiguste konventsioonis ega ka Eesti põhiseaduses. See aga ei tähenda, et isikuandmete kaitse oleks jäetud tähelepanuta ning isikud kaitseta. Näiteks Euroopa Inimõiguste Kohus on arvukates lahendites märkinud, et kuigi inimõiguste konventsiooni artikli 8 lõike 1 sõnastusest *expressis verbis* isikuandmete kaitset kui eraldiseisvat õigust ei leia, on ka isikuandmete kaitse küsimused artikli 8 kaitsealas. [8]

Näiteks kohtuasjas S. ja Marper *vs*. UK leidis Euroopa Inimõiguste Kohus, et isikuandmete (antud juhul sõrmejälgede ning DNA näidiste) kogumist ning säilitamist olukorras, kus neid enam uurimiseks ei kasutatud, võib pidada artiklis 8 sätestatu rikkumiseks.[9] Euroopa Inimõiguste Kohus tuvastas artiklis 8 sätestatud nõude ebaproportsionaalse rikkumise ka kohtuasjas Peck *vs*. Ühendkuningriik. See puudutas juhtumit, kus meedias avaldati hagejast turvakaamerate poolt avalikus ruumis salvestatud video ilma tema nõusolekuta ja tema identiteeti varjamata.[10]

Euroopa Liidu kõige olulisem isikuandmete kaitset reguleeriv dokument on Euroopa Parlamendi ja nõukogu isikuandmete kaitse üldmäärus, mis hakkas Euroopa Liidu liikmesriikides kehtima 2018. aastal.[11] Üldmäärus sisaldab mitu keskset põhimõtet, nagu näiteks õigus olla unustatud ja võimalikult väheste andmete kogumise põhimõte. Uudsena on üldmääruses välja toodud õigus andmete ülekandmisele, profileerimisega seotud õigused ning ka lõimitud ning vaikimisi andmekaitse põhimõte, mida varasemast Euroopa Liidu õigusest sellisel kujul ei leia.

Nende põhimõtete sisustamine uute tehnoloogiate valguses on tõstatanud mitmeid õiguslikke küsimusi ka juba enne üldmääruse vastuvõtmist. Näiteks õigus olla unustatud tõusis terava tähelepanu alla 2014. aastal kohtuasjas Google *vs*. AEPD ja Mario Gonzàles. Euroopa Kohus leidis siis, et otsingumootorite haldajaid tuleb käsitada isikuandmete vastutavate töötlejatena ning et kui isikuandmed on nende töötlemise kunagisi eesmärke ning möödunud aega arvestades ülemäärased ning pole parajasti asjakohased, peab otsingumootori haldaja need isikuandmed otsingutulemuste seast kõrvaldama.[12]

Inimõiguste omavahelised piirid on hägustunud, aga riigid on arendanud digitaalse ühiskonna uute õiguspõhimõtete tõlgendusi. Näiteks arendas Saksa Liidukonstitutsioonikohus 1983. aastal uue põhiõigusena õiguse informatsioonilisele enesemääramisele. Selle kohaselt on isikul õigus teada tema kohta käivate andmete kogumisest ja otsustada oma andmete üle. Saksa Liidukonstitutsioonikohus sõnastas

2008. aastal veel ühe tehnoloogia arenguga tugevalt seotud põhiõiguse: õiguse infotehnoloogiasüsteemide konfidentsiaalsusele ja terviklikkusele.13 Selle kohaselt võivad julgeolekuasutused varjatult jälgida IT-süsteemide kasutamist ning pääseda ligi salvestatud andmetele ainult siis, kui tegu on ohuga põhilistele õigushuvidele ning kohtu loal.

Pidades silmas uusi tehnoloogiaid, rõhutavad privaatsusõiguse kaitse tähtsust ka mitmed teised rahvusvahelised organisatsioonid. Näiteks on ÜRO inimõiguste ülemvoliniku büroo võtnud tähelepanu alla privaatsuse kaitse, pöörates eraldi tähelepanu tehnoloogia ja privaatsusega seotud teemadele, nagu massjälgimine, isikuandmete kaitse, DNA andmekogud, avaandmed ning suurandmed.14 Alates 2013. aastast on ÜRO vastu võtnud mitu resolutsiooni pealkirjaga „Õigus eraelu puutumatusele digitaalajastul“15 , mis on tõmmanud rahvusvahelist tähelepanu tehnoloogia rollile inimõiguste kaitsmisel ning rikkumisel ning on märkimisväärne just oma globaalse haarde poolest. Teema olulisuse tõttu alustas ÜRO-s tegevust ka eraelu puutumatuse õiguse eriraportöör, kelle üks tööülesanne on koguda infot eraelu puutumatuse ja uute tehnoloogiatega seotud tavade ja kogemuste kohta, jagada ja edendada riikide parimaid tavasid ning tuvastada võimalikke murekohti. Valdkonna konkreetsem käsitlemine ÜRO tasandil on märk sellest, et teadlikkus inimõiguste ning tehnoloogia valupunktidest on riikides suurenenud, kuid samas jätkuvad mitmetes riikides just tehnoloogia toel selged inimõiguste rikkumised.

3.1. Isikuandmete kaitse

Isikuandmete kaitse on tehnoloogia arenguga muutunud üha olulisemaks. Aastatega on Euroopa Liidu regulatsioon arenenud aina nüansirikkamaks ning samas mõjutanud ka teiste regioonide ning riikide andmekaitseõiguse arengut (nn Brüsseli efekt).16

Eelmises alapeatükis mainisime, et Euroopa Liidu keskne isikuandmete kaitsele pühendatud instrument on Euroopa Liidu isikuandmete kaitse üldmäärus. Üldmääruse kohaselt vastutab isikuandmete „vastutav töötleja“ selle eest, et isikuandmete töötlemisel jälgitaks üldmääruses sätestatud põhimõtteid17 , olenemata sellest, milliseid tehnoloogiaid on isikuandmete töötlemisel kasutatud. Kuivõrd isikuandmete kaitsega seotud õiguslikke küsimusi on rohkem, kui siin peatükis jõuame katta, toome järgnevalt kolm näidet üldmääruse rakendamisel tekkinud küsimuste kohta.

Esiteks on uute tehnoloogiate puhul keeruline määratleda, kas kogutavad ja töödeldavad andmed kuuluvad isikuandmete kaitse üldmääruse mõistes isikuandmete alla või millal on need n-ö piisavalt anonüümseks muudetud ning seeläbi üldmäärus neile ei kohaldu. Näiteks IP-aadresside puhul leidis Euroopa Kohus, et nii staatilised kui ka dünaamilised IP-aadressid võivad olla üldmääruse mõistes isikuandmed, sest need võivad viia füüsilise isiku tuvastamiseni, kes nimetatud IP-aadressi kasutab.18 Samas on endiselt ebaselge, kas näiteks plokiahela tehnoloogias kasutatavad räsid vastavad samuti üldmääruse isikuandmete definitsioonile või tuleks neid käsitada anonüümitud teabena.19 See omakorda mõjutab otseselt tehnoloogia- ja teenusepakkujate õigusi ja kohustusi ning samal ajal ka tehnoloogiate kasutajate kaitset.

Teise näitena saab tuua suurandmed ning tehisintellekti kasutamisega seotud küsimused. Siin on peamised õiguslikud probleemid seotud töödeldavate isikuandmete mahu ja mitmekesisuse ning töötlemise tingimuste ja tulemustega. Näiteks võib olla keeruline kindlaks määrata andmete omanikku, kui kogutakse ja töödeldakse suuri andmekogusid, mis koosnevad mitmestest allikatest ning on salvestatud erineval kujul ning mille töötlemine ei pruugi alati toimuda algselt määratud eesmärkidel. Samuti võib probleeme tekitada vastutava ja volitatud töötleja kindlaksmääramine ning täpsete volituste ning kohustuste defineerimine, kui andmeid töötlevad nutikad masinad ja tarkvara. Oluline on ka otsustada, millistel eesmärkidel võidakse tulemusi kasutada ning kuidas õiguslikult käsitleda tehisintellekti tehtud otsuseid, mis põhinevad tehisintellekti enda välja töötatud andmetöötlusel.20

Kolmandaks, uute tehnoloogiate igapäevane kasutuselevõtt tekitab erinevaid arusaamu isikuandmete töötlemise lubatavuse kohta. Isikuandmete kaitse üldmäärus nimetab ühe töötlemise alusena andmesubjekti nõusoleku. Üldmääruse kohaselt peab nõusolek olema antud viisil, millega andmesubjekt kinnitab „vabatahtlikult, konkreetselt, teadlikult ja ühemõtteliselt nõusoleku teda puudutavate isikuandmete töötlemiseks“.21 Sotsiaalmeedia, mitmesuguste elektrooniliste teenuste ning tehnoloogiate kontekstis saab aga küsida, kas nõusolek andmete töötlemiseks vastab alati üldmääruses nimetatud tingimustele. Kas andmesubjekti nõusolek on vabatahtlik ehk kas andmesubjekt on saanud valida (nt kas ta soovib personaliseeritud reklaame)? Kas nõusolek on konkreetne ja teadlik ehk kas andmesubjekt kui teenuse kasutaja mõistab täiel määral, kuidas kasutatakse tema andmeid või kellele neid edastatakse (nt mis tingimustel saavad

andmetele ligipääsu kolmandad isikud või riigid)? Andmesubjekti teadlikkus on seotud ka läbipaistvuse nõudega, mille kohaselt peab vastutav töötleja teavitama andmesubjekti tema isikuandmete töötlemise viisidest ning eesmärkidest „kokkuvõtlikult, selgelt, arusaadavalt ning lihtsasti kättesaadavas vormis, kasutades selget ja lihtsat keelt“22 , mille rakendamine keeruliste tehnoloogiliste lahenduste puhul võib osutuda väljakutseks.

3.2. Sideandmete säilitamine

Inimõiguste kaitse ja turvalisuse tagamise vahel tasakaalu leidmine on alati olnud keeruline ülesanne ning tehnoloogia kiire areng võib kaalukausi veelgi enam uppi lüüa.

Ilmekas näide selle kohta on pikalt kestnud debatt sideandmete säilitamise tingimuste üle. Nimelt kuulutas Euroopa Kohus 2014. aastal Euroopa Liidu sideandmete säilitamise direktiivi 2006/24 kehtetuks.23 Euroopa Kohus küll nentis, et sideandmete säilitamine on eesmärgipärane kuritegevuse ja kuritegude, eriti organiseeritud kuritegevuse ennetamisel, uurimisel, avastamisel ja kohtus menetlemisel, kuid leidis, et direktiiv hõlmas üldistatult kõiki isikuid ning kõiki elektroonilise side vahendeid ja liiklusandmeid, ilma et raskete kuritegude vastu võitlemise eesmärki arvestades oleks ette nähtud mingit eristamist, piirangut või erandit.24 Seega puudusid direktiivis reeglid, mis reguleeriksid Euroopa Liidu põhiõiguste harta artiklites 7 ja 8 ette nähtud inimõiguste riive ulatust, ning kohus tõdes, et direktiiv tõi kaasa Euroopa Liidu õiguskorras nende inimõiguste ulatusliku ja väga raske riive, ilma et see riive oleks täpselt piiritletud sätetega, mis lubaksid tagada, et riive piirdub vaid vältimatult vajalikuga.25 Samuti ei näinud direktiiv muu hulgas ette piisavalt garantiisid, mis võimaldaksid tagada säilitatavate andmete tõhusa kaitsmise juhuks, kui keegi soovib salvestatud andmeid kuritarvitada.26 Kohtule ei olnud meelepärane veel see, et direktiiv ei nõudnud andmete säilitamist EL-i territooriumil ning seetõttu ei saanud pidada täiel määral tagatuks, et vajalikke andmekaitse ja andmeturbega seotud nõuete täitmist saab kontrollida sõltumatu asutus.27

Euroopa Kohus on neid küsimusi arutanud ka hiljem ning kinnitas ka 2016. aastal, et liikmesriigid võivad kehtestada õigusnormistiku, mis võimaldab raske kuritegevuse vastu võitlemise eesmärgil ennetavalt säilitada liiklus- ja asukohaandmeid, kui säilitatavate andmete liigid, asjasse puutuvad sidevahendid ja isikud ning säilitamise kestus on piiratud rangelt vajalikuga ning kui on tagatud, et riigi pädevatele

ametiasutustele antakse juurdepääs säilitatavatele andmetele ainult rangelt vajalikus ulatuses.[28] Ka rõhutas kohus andmetele juurdepääsu saamise eeltingimusena kohtu või sõltumatu haldusasutuse eelneva kontrolli vajalikkust, mis tehakse juurdepääsu taotleva asutuse põhjendatud taotluse alusel, mis omakorda on ennekõike esitatud kuriteo ennetamise, avastamise või menetlemise raames.[29] Samasuguse tulemuseni jõudis kohus ka 2020. aastal käsitletud asjades, kui leidis, et üldine sideandmete säilitamine ei ole EL-i õigusega kooskõlas, kuigi on võimalikud erandid: sideandmeid võib säilitada näiteks riigi julgeoleku kaalutlustel ja kindla aja jooksul, kui säilitamine on valikuline ja piiratud, või kui andmed puudutavad konkreetset rasket kuritegu või terrorirünnakut.[30]

Vaatamata eespool nimetatud Euroopa Kohtu otsustele kehtis Eestis endiselt õigusnormistik, mis kohustas teenuseosutajaid säilitama aasta aega kõigi kasutajate sideandmed (näiteks sideseansi algus ja lõpp, kasutatud teenus, kellega ühendust peeti jne) ning need seaduses sätestatud tingimustel edastama riigi uurimis-, jälitus- või julgeolekuasutustele, prokuratuurile, kohtule või teistele seaduses määratud asutustele.[31] Olukord muutus alles pärast Euroopa Kohtu 2021. aastal tehtud otsust. Selles otsuses täpsustati, et üldine sideandmete säilitamine on EL-i õigusega vastuolus, kui sideandmetele juurdepääs ei piirdu menetlustega, mille eesmärk on võitlus raske kuritegevuse vastu või avalikku julgeolekut ähvardava suure ohu ärahoidmine, ning olenemata sellest, millise ajavahemiku andmetele on juurdepääsu taotletud ning olenemata selle ajavahemiku kohta kättesaadavate andmete hulgast ja liigist ning samuti siis, kui puudub kohtu või sõltumatu haldusasutuse eelnev kontroll.[32] Seejärel otsustas Riigikohus, et Eestis kehtiv andmete laussäilitamine ning nende andmete kasutamist reguleeriv kord on vastuolus EL-i õigusega ning seetõttu on välistatud kriminaalmenetluse eesmärkidel sideandmete säilitamine ja kasutamine nii kaua, kuni Eesti pole viinud oma sellekohast õigusnormistikku vastavusse EL-i õigusega.[33]

3.3. Jälitustoimingud

Ulatuslikud inimõiguste, sealhulgas sõnumisaladuse kaitse riived võivad kaasneda ka jälitustoimingutega[34] , mille läbiviimise vahendid ja võimekus kasvavad tehnoloogia arenguga samas rütmis. Eraldi tuleb käsitleda piiratud isikustatud jälgimist ning tehnoloogia arenguga võimalikuks saanud elektroonilist lausjälgimist.

Euroopa Inimõiguste Kohus on kohtuasjas Klass jt *vs.* Saksamaa rõhutanud, et salajane jälgimine, sealhulgas kommunikatsiooni jälgimine, tuleb tasakaalustada

tõhusate ja piisavate tagatistega võimalike kuritarvituste vastu ning et üksikisikute lausjälgimist ei saa õigustada luure- ning terrorismivastase võitlusega.35 Sarnase seisukoha on Euroopa Inimõiguste Kohus võtnud kohtuasjas Szabó ja Vissy *vs.* Ungari. Kohus on öelnud, et ka terrorismikuritegude ärahoidmisel ja avastamisel peab kommunikatsiooniandmete töötlemine olema vältimatult vajalik selle eesmärgi saavutamiseks ja seaduses tuleb sätestada tingimused, mis õigustavad konkreetse ohu tõrjumiseks konkreetsete isikute sõnumite saladuse riivet, mitte aga lubama sekkumist määratlemata hulga inimeste kommunikatsiooniandmetesse.36

Euroopa Inimõiguste Kohus kinnitas kohtuasjas Kopp *vs.* Šveits, et sõnumisaladuse piiramise juhud ja kord peavad olema täpselt ja arusaadavalt sätestatud seaduses. 37 Kohtuasjas Weber ja Saravia *vs*. Saksamaa analüüsis kohus Saksamaal kehtinud telekommunikatsiooni pealtkuulamise korda ning lisas täpsustusena kuus kaitsemeedet isikustatud jälgimise kohta kriminaalmenetluses. Kohtu hinnangul tuleb õigusnorme sätestades arvestada: 1) milliste süütegude puhul võib jälitustegevust kasutada; 2) milliste isikute suhtes võib jälitustegevust teostada; 3) millised on piirangud jälitustegevuse kestusele; 4) milline on saadud andmete uurimise, kasutamise ja säilitamise kord; 5) millised on ettevaatusabinõud andmete teistele isikutele edastamise korral; 6) milline on jälitustegevusega saadud andmete kustutamise ja hävitamise kord. Pärast põhjalikku analüüsi leidis kohus, et hagejate vaidlustatud pealtkuulamine oli riigi määratud eesmärke arvestades demokraatlikus ühiskonnas vajalik.38

Kohtuasjas Roman Zakharov *vs*. Venemaa rõhutas Euroopa Inimõiguste Kohus, et mobiiltelefonikõnede salajast pealtkuulamist reguleerivad normid peavad andma üksikisikule võimaluse kindlaks teha, kas tema kõnesid on pealt kuulatud, ning üksikisikul peab olema juurdepääs õiguskaitsevahenditele.39

Jälitustoimingute puhul võib ristuda eraelu puutumatuse kaitsealaga ka sõnumisaladuse kaitseala. Kuivõrd Eesti põhiseaduse järgi on sõnumisaladusse sekkumine rohkem piiratud kui perekonna- ja eraellu sekkumine, on Riigikohus korduvalt käsitlenud kahe kaitseala piiritlemise küsimust. Riigikohus on leidnud, et sõnumisaladuse kaitsealas on vaid need sõnumid, mis on parajasti kommunikatsiooniprotsessis, ning isiku valduses olev ülejäänud informatsioon, nagu e-kiri või selle mustand, on kaitstud põhiseaduse §-ga 26.

Eraelu kaitsealasse kuuluvad ka sõnumi metaandmed, millest ei selgu sõnumi sisu. 40 Kohus põhjendas seda sellega, et sõnumi teeloleku ajal, kui sõnum on väljunud

saatja valdusest ning pole veel adressaadini jõudnud, on sõnum isiku mõjusfäärist väljas ning ta ei saa seda kolmandate isikute eest kaitsta.[41] Interneti vahendusel edastatud sõnumid on teel vaid väga lühikest aega ning seetõttu leiavad s õnumisaladuse mõiste laiema tõlgenduse pooldajad, et saatmisele kuuluvad ja kohale jõudnud sõnumid väärivad samaväärset kaitset nagu kommunikatsiooniprotsessis olevad sõnumid. Kuidas näiteks oleks muidu kaitstud e-kiri, mille saatja on välja saatnud ning ootab lugemist, olles salvestatud teenusepakkuja serverisse? Või kuidas on kaitstud e-kiri, mida meelega pole välja saadetud, vaid mis ootab lugemist e-kirja kontol, millele võib ligi pääseda igaüks, kes teab õiget kasutajanime ja parooli? Seega ei tohiks sõnumi kaitse sõltuda sellest, kas sõnum on tehtud saajale kättesaadavaks, vaid sellest, kas isik soovib sõnumi sisu jätta avalikustamata. Sõnumisaladuse kaitseala laiemat tõlgendust toetavad ka Euroopa inimõiguste konventsiooni ja harta sõnastus ja rakenduspraktika.[42]

Jälitustoiminguid võivad elektroonilisi vahendeid kasutades teha ka luure- või julgeolekuasutused ning mitmetest lahvatanud skandaalidest teame, et mitte ainult riigisiseselt.[43] Rahvusvaheline õigus riikidevahelist luuretegevust otseselt ei keela, küll aga võib rahvusvahelist õigust rikkuda viis, kuidas luuretegevust läbi viiakse. Seejuures pole oluline, kas tegu on n-ö traditsiooniliste vahendite abil tehtud või küberluurega (*cyber espionage*).

Küberluures kasutatakse mitmesuguseid viise, kuidas andmeid koguda ka teise riigi territooriumil viibimata. Näiteks võib mõne toote tootmisel riistvarasse sisestada koodi, mis muudab võimalikuks riistvara kaugjälgimise. Samuti võib konkreetsete isikute seadmete operatsioonisüsteemid nakatada pahavaraga, mille abil saab ligi seadmetesse salvestatud andmetele või pealt kuulata seadmete kaudu toimuvat suhtlust. Lisaks võib kasutada andmepüüki ehk kalastamisrünnet, et kätte saada salasõnad, mille abil süsteemidesse sisenedes varjatult vajalikku infot koguda. Oluline on, et teatud elemendid, nagu näiteks tekitatud füüsiline kahju või operatsioonisüsteemide toimimise halvamine, võivad kätkeda rahvusvahelise õiguse reeglite (näiteks suveräänsuse või mittesekkumise printsiibi) rikkumist.[44]

Huvipakkuvad on hiljutised Euroopa Inimõiguste Kohtu otsused, mis puudutavad riikide massilise signaaliluure[45] regulatsiooni ning elektroonilist lausjälgimist. Näiteks hindas Euroopa Inimõiguste Kohtu suurkoda kohtuasja Centrum för Rättvisa *vs.* Rootsi otsuses, et arvestades ohte, millega riigid peavad silmitsi seisma, ning seda, et nende tegude toimepanijad ning osalised kasutavad suhtluseks internetti ning samas püüavad oma internetisuhtluse jälgimist takistada kõrgetasemelise

tehnoloogiaga, on riikidel kaalutlusõigus otsustada, millist süsteemi vajab riik julgeolekuohtude väljaselgitamiseks ning turvalisuse tagamiseks. Kohus analüüsis mitme kriteeriumi alusel, kas õigusaktides, millele toetudes signaaliluure teel jälgitakse sidekanalite kaudu edastatavat kommunikatsiooni ja metaandmeid, on ette nähtud piisavalt kaitsemeetmeid, et kaitsta elanikke võimalike riigipoolsete kuritarvituste eest.

Olulise arenguna möönis Euroopa Inimõiguste Kohus, et pidades silmas tehnoloogia arengut, tuleb sideandmete massjälgimise hindamisel arvestada tavalisele isikustatud jälgimisele kohaldatavaid põhimõtteid, mida kohus oli sätestanud eespool mainitud Weber ja Saravia *vs*. Saksamaa kohtuasjas. Lisaks täpsustas kohus elemente, mida riigisisene õigusnormistik peab nii sideandmete kui ka sideandmetega seotud andmete massjälgimisel kajastama. Kuigi kohus kiitis üldiselt heaks Rootsi lausjälgimist reguleeriva õigusnormistiku, tuvastati ka kolm puudujääki: 1) puudusid selged reeglid selle kohta, kuidas hävitada andmeid, mis ei sisalda isikuandmeid; 2) õigusnormistikus, mis puudutas kogutud andmete jagamist kolmandate riikidega, puudus viide üksikisiku privaatsuse olulisusele; 3) puudus toimiv *ex post facto* kontroll. Sellest lähtuvalt otsustas kohus, et Rootsi õigusnormistik rikub Euroopa inimõiguste konventsiooni artiklis 8 sisalduvat privaatsusõigust.[46]

Sarnaseid küsimusi käsitleti ning samasugust lähenemist kohaldati Euroopa Inimõiguste Kohtu asjas Big Brother Watch jt *vs*. Ühendkuningriik, milles suurkoda otsustas, et Suurbritannia on üksikisikute lausjälgimisega rikkunud konventsiooni artikleid 8 ja 10. Kohus viitas artikli 8 rikkumist tuvastades kolmele puudujäägile: massjälgimise loa andja ei olnud täitevvõimust sõltumatu; sideandmete massjälgimise luba ei sisaldanud piisavaid otsingukriteeriume; konkreetse isikuga seotud otsingukriteeriumidele ei pidanud eelnevalt taotlema luba.[47]

Kuigi seda Euroopa Inimõiguste Kohtu otsust saab pidada inimõiguste kaitsele pühendunud organisatsioonide suureks võiduks, sest mõlema otsuse kohaselt tuvastas kohus artikli 8 rikkumise, kardavad kriitikud, et seesuguste otsustega normaliseeritakse lausjälgimine, sest lausjälgimist ennast ei peetud ebaproportsionaalseks.[48] Seoses piiriüleste jälitustoimingute lubatavusega tuleb eraldi ära märkida murranguline Saksa Liidukonstitutsioonikohtu otsus, mille kohaselt peab ka piiriüleste jälitustoimingute tegemine olema kooskõlas Saksamaa põhiseadusega. Liidukonstitutsioonikohtu otsusega tunnistati seega 2020. aastal kehtinud vastav regulatsioon õigusvastaseks.[49]

3.4. Läbiotsimine

Tehnoloogia levik ja areng on muutnud ka teiste kriminaalmenetluses tõendite kogumiseks kasutatavate toimingute tegemist. Näiteks ei sisalda Eesti õigus elektrooniliste teabekandjate läbiotsimise käigus äravõtmise ja läbivaatuse kohta eriregulatsiooni.50 Teabekandja äravõtmine eraldivõetuna ei riiva sõnumisaladust, kuid üldjuhul on toimingu eesmärk saada teada edastatud sõnumite sisu, mistõttu on teabekandja äravõtmine vähemalt puutumuses sõnumisaladusega. Samuti võib teabekandja uurimine tekitada mitmeid küsimusi, nagu läbiotsitavate andmete mahu piiritlemine ning läbiotsimisest teavitamine.51 Seetõttu ei ole kehtivate õigusnormide tõlgendamine üheselt arusaadav. See toob kaasa õigusliku ebaselguse, avara tõlgendamis- ning tegutsemisruumi, sealhulgas ka inimõiguste kaitse suhtes. Kuna tänapäeval vahetatakse sõnumeid valdavalt elektrooniliste sidevahendite kaudu ning palju andmeid salvestatakse elektroonilistele andmekandjatele, tekib õigustatud ootus, et tehnoloogia arengut arvestades tuleks ajakohastada ka kriminaalmenetluse vastava sisuga õigusnormistik.52

Olulise aspektina tuleb vaadelda ka andmete asukoha problemaatikat, sest aina rohkem tekib olukordi, kus kohtueelses menetluses kogutavad tõendid ei asu asja menetleva riigi territooriumil või polegi nende füüsilist asukohta võimalik tuvastada. Näitena võib tuua pilvetehnoloogiad, kus andmete salvestamine ainult kasutaja koduriigi territooriumil on pigem erand kui reegel ning kus peegeldatud andmebaaside, eri serverite ning rakenduste tõttu ei suuda tihtipeale isegi teenuse osutajad täielikult identifitseerida andmete tegelikku asukohta.

Elektrooniliste tõendite kogumisel võidakse kriminaalmenetluses kasutada nn kaugläbiotsimist, mida tehakse (arvuti)süsteemis ning mida laiendatakse selle (arvuti)süsteemi kaudu teistesse, mujal asuvatesse (arvuti)süsteemidesse või mida tehakse kriminaalmenetlust teostava uurimisasutuse (arvuti)süsteemi kaudu. Selline otsene ligipääs andmetele on märksa kiirem kui traditsiooniline rahvusvaheline kriminaalkoostöö, kuid võib lisaks teise riigi suveräänsuse rikkumisele tekitada küsimusi ka üksikisiku inimõiguste kaitse kohta.

- 1Inimõiguste ja põhivabaduste kaitse konventsioon. – RT II 2010, 14, 54. Konventsioonile kirjutati alla 4. novembril 1950, see jõustus 3. septembril 1953. Konventsiooni on ratifitseerinud kõik 47 Euroopa Nõukogu liikmesriiki.
- 2Euroopa Liidu põhiõiguste harta 30.03.2010. – ELT C 83/02.
- 3Eesti Vabariigi põhiseadus. – RT I, 15.05.2015, 2.

- 4Privaatsusõiguse ulatust annab olemuslikult hästi edasi 1890. aastal avaldatud kuulus fraas, mille kohaselt tähendab see mõiste eelkõige „õigust olla jäetud üksi“. Warren, S. D., Brandeis, L. D. Right to privacy. – Harvard Law Review 1890–1891/4 (5), lk 193. Privaatsusõiguse kujunemise kohta vt Lõhmus, U. Põhiõigused kriminaalmenetluses. Tallinn: Juura 2014, lk 301−312.
- 5Lõhmus, lk 307.
- 6Euroopa Inimõiguste Kohtu kontekstis privaatsusõiguse ning digitaalse ajastu puutepunkte uuriv ülevaateartikkel: Çınar, Ö. H. The current case law of the European Court of Human Rights on privacy: challenges in the digital age. – The International Journal of Human Rights 2021/25 (1), lk 26−51.
- 7Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon. – RT II 2001, 1, 3.
- 8EIK, 44787/98, P. G. ja J. H. vs. Ühendkuningriik, 25.09.2001; EIK, 59842/00, Vetter vs. Prantsusmaa, 31.05.2005; EIK, 71611/01 Wisse vs. Prantsusmaa, 20.12.2005; EIK, 52019/07, L. H. vs. Läti, 29.04.2014.
- 9EIK, 30562/04, 30566/04, S. ja Marper vs. Ühendkuningriik, 04.12.2008.
- 10EIK, 44647/98, Peck vs. Ühendkuningriik, 28.01.2003.
- 11Euroopa Parlamendi ja nõukogu 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). Koos üldmäärusega võttis EL vastu ka direktiivi riigiasutustes isikuandmete õiguskaitse eesmärgil töötlemise kohta, millega kehtestatakse andmekaitse eeskirjad ja põhimõtted, mis reguleerivad isikuandmete töötlemist süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil. Euroopa Parlamendi ja nõukogu 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 ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK.
- 12EK, C-131/12, Google Spain SL ja Google Inc. vs. Agencia Española de Protección de Datos (AEPD) ja Mario Costeja González, ECLI:EU:C:2014:317.
- 13BVerfG, 1 BvR 370/07 ja 1 BvR 595/07. 27.02.2008. – https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20 (19.12.2021). Nimetatud õigus on eesti keelde tõlgitud ka kui „õigus infotehnoloogiasüsteemide konfidentsiaalsusele ja puutumatusele“; vt ka

Lõhmus, lk 305.

- 14 ÜRO inimõiguste ülemvoliniku büroo. Privaatsuse eriraportöör. – https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx, (28.03.2021).
- 15 Viimati: ÜRO Peaassamblee. Resolution on the right to privacy in the digital age. A/HRC/RES/42/1. 26.09.2019.
- 16 Bradford, A. The Brussels Effect: How the European Union Rules the World. – New York: Oxford University Press 2020. Isikuandmete kaitse üldmäärus, artikkel 5, p 2.
- 17 Isikuandmete kaitse ülmäärus, artikkel 5, p 2.
- 18 EK, C-582/14, Patrick Breyer vs. Saksamaa, ECLI:EU:C:2016:779.
- 19 Finck, M., Pallas, F. They who must not be identified – distinguishing personal from non-personal data under the GDPR. – International Data Privacy Law 2020/10 (1).
- 20 Loe lähemalt: Euroopa Liidu Põhiõiguste Amet ja Euroopa Nõukogu. Euroopa andmekaitseõiguse käsiraamat. − Luxembourg: Euroopa Liidu Väljaannete Talitus 2020, ptk 10.
- 21 Isikuandmete kaitse üldmäärus, preambul p 32.
- 22 Isikuandmete kaitse üldmäärus, artikkel 12 lg 1.
- 23 EK, C-293/12, Digital Rights Ireland and Seitlinger and Others, ECLI:EU:C:2014:238.
- 24 Ibid., p-d 43 ja 57.
- 25 Ibid., p 65.
- 26 Ibid., p 66.
- 27 Ibid., p 68.
- 28 EK, C-203/15, Tele2 Sverige, ECLI:EU:C:2016:970, p-d 110, 115, 116, 118, 119.
- 29 Ibid., p 120.
- 30 EK, C-623/17, Privacy International vs. Secretary of State for Foreign ja Commonwealth Affairs jt, ECLI:EU:C:2020:790.; EK, C-511/18, La Quadrature du Net jt vs. Premier minister jt, ECLI:EU:C:2020:791.
- 31 Elektroonilise side seadus. – RT I, 22.10.2021, 15, § 1111.
- 32 EK, C-746/18, Prokuratuur (Conditions d’accès aux données relatives aux communications électroniques), ECLI:EU:C:2021:152.
- 33 RKKK, 1-16-6179, 18.06.2021, p 105.
- 34 Jälitustoiminguid võidakse Eestis teha kriminaalmenetluse seadustiku, julgeolekuasutuste seaduse või Kaitseväe korralduse seaduse alusel. Loe

lähemalt: Jaanimägi, K., Oja, L. Paragrahv 26. – Madise, Ü. (toim). et al. Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. Tartu: Sihtasutus Iuridicum 2020, p 23.

- 35EIK, 5029/71, Klass jt vs. Saksamaa, 06.09.1978.
- 36EIK, 37138/14, Szabó ja Vissy vs. Ungari, 12.01.2016; loe täpsemalt: Laos, Sepp, p 25.
- 37EIK, 13/1997/797/1000, Kopp vs. Šveits, 25.03.1998.
- 38EIK, 54934/00, Weber ja Saravia vs. Saksamaa, 29.06.2006.
- 39EIK, 47143/06, Roman Zakharov vs. Venemaa, 04.12.2015.
- 40RKKK, 3-1-1-51-14, 23.02.2015, p 21.
- 41RKKK, 3-1-1-14-14, 30.06.2014, p-d 816 ja 817; loe täpsemalt: Laos, Sepp, p 5.
- 42Laos, Sepp, p 6.
- 43Näitena võib tuua vihjeandja Edward Snowdeni 2013. aastal avaldatud materjalid, mille kohaselt oli USA riiklikul julgeolekuametil väidetavalt lausjälgimise jaoks ligipääs suurte IT-firmade serveritele ning võimekus valguskaabli kaudu inimesi pealt kuulata ja krüptograafilisi võtmeid murda. Loe täpsemalt: MacAskill, E. et al. NSA Files Decoded: Edward Snowden’s Surveillance Revelations Explained. – The Guardian 01.11.2013.
- 44Schmitt, M. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. – Cambridge: Cambridge University Press 2017, lk 168−174.
- 45Üldtermin, mille alla käib elektrooniline ja sideluure. Enim kasutatavad elektroonilise side võrgud on andmeside-, mobiiltelefoni-, kaabellevivõrk ja elektrikaablisüsteem. Signaaliluure erineb tavapärasest 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 viisil ning analüüsitakse arvutite abil valitud kriteeriumide järgi. Filtreerimise aluseks võivad olla inimeste nimed, keeled, võtmesõnad, kommunikatsiooni teekonnad ja teised tehnilised andmed. Loe täpsemalt: 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 (24.10.2021).
- 46EIK, 35252/08, Centrum för Rättvisa vs. Sweden, 25.05.2021.
- 47EIK, 58170/13, 62322/14 ja 24960/15, Big Brother Watch jt vs. Ühendkuningriik, 25.05.2021.

- 48Milanovic, M. The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för rättvisa. − EJIL:Talk! 26.05.2021. – https://www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/ (13.09.2021).
- 49BVerfG, 1 BvR, 2835/17, 19.05.2020.
- 50Kuigi KrMS § 91 ei nimeta otsesõnu teabekandjat kui läbiotsimise objekti, võidakse läbiotsimise käigus teabekandjad (nt arvuti kõvaketas, e-kirja väljatrükk, mobiiltelefon) ära võtta ning rakendada vaatlust. Kriminaalmenetluse seadustik. – RT I, 08.07.2021, 9.
- 51Lõhmus, lk 312–313.
- 52Laos, Sepp, p 15; Lõhmus, lk 312–313.