



Teekond jälgimisühiskonda? Isikuandmete kogumine ja kasutamine Eesti riigis

Paul Keres, Andri Rohtla



**Põhimõtte
Koda**

**„I believe that which grows in shadow
but withers in the light of day,
does not belong on the vine.“***

– Senaator Robert Kinsey, USA telesari „Stargate SG-1“

* Usun, et see, mis varjus kasvab,
kuid päevavalgel närbub,
ei vääri kohta viinapuul.

Sisukord

Raporti eesmärk	5
Põhijäreldused	7
Sissejuhatus.....	9
Digiriigist andmeriigini	9
Mida tähendab „jälgimisühiskond“	9
Jälgimine ja usaldus	10
Põhiseadus ja Euroopa Liidu õigus	11
Raporti põhiväide ja ülesehitus	11
Riigi andmekogud ja andmete kogumise viisid	12
Isik ja perekond	12
Vara ja ettevõtlus	13
Tervis	14
Liikumine	14
Sideandmed: kõigi inimeste liiklus- ja asukohaandmete kohustuslik valimatu kogumine	15
Raha ja maksud	16
Haridus ja töö	17
Õiguskaitse	17
Andmekogude koosmõju	18
Ettepanekud	19
Andmete juurdepääs: kes, millal ja millise põhjendusega .	20
Haldusjärelevalve	20
Väärteomenetlus	22
Kriminaalmenetlus	22

Julgeolekuasutused	23
Mõistete lahtisus	23
Infomonopol	23
Kohtu luba kui prognoosotsus	24
Analüüs: neli kitsaskohta	25
Ettepanekud	27
 Andmete kasutamine: vabatahtlikkusest riskipõhise	
 järelevalveni ja edasi menetluseni	28
Müüt „nõusolekust“	28
Riskipõhine järelevalve	29
Massiline andmetöötlus ja ohtu ennetav haldusmenetlus	29
Järelevalvest karistuseni	30
Andmete kasutamine haldusmenetluslikuks ennetamiseks	31
Analüüs: eesmärk, mis on pidevas muutumises	33
Ettepanekud	33
 Salajase jälgimise ulatus ja kontroll	35
Ametlik statistika	35
Teavitamine	36
Riigikohtu seisukohad teavitamise puudujääkidest	36
Teabehange ja jälitustoimingud: samad tegevused, erinev kaitse	37
Kontrollimehanismid	38
Tsiviilkontrolli taandumine	39
Ettepanekud	40
 Kokkuvõte	42

Raporti eesmärk

Raportis käsitletakse isikuandmete kogumist ja kasutamist riigikorralduse praktilise küsimusena. Autorid lähtuvad seisukohast, et eraelu kaitse on riigi igapäevase toimimise lahutamatu osa ning eraelu puutumatuse piisav tagatus on isikuvabaduse sisulise mõistmise eelduseks.

Raport ei sea kahtluse alla digiriigi vajalikkust. Eesti e-riigi lahendused on kolme aastakümne jooksul säästnud inimeste ja ettevõtete aega, vähendanud halduskoormust ning lihtsustanud riigiga suhtlemist paljudes eluvaldkondades. Andmete ühekordse küsimise põhimõte, X-tee ja elektroonilised registrid on avaliku halduse olulised saavutused. Küsimus on üksnes selles, kas õiguslikud ja institutsionaalsed piirangud on pidanud sammu andmete hulga ja kasutusviiside kasvuga ning ametiasutuste üha laieneva huviga saada järjest rohkem andmeid järjest enamateks eesmärkideks.

Raportis kaalutakse turvalisuse, halduse tõhususe ja eraelu kaitse omavaheolist vahekorda. Need huvid ei välista üksteist, kuid nende tasakaal ei kujune iseenesest, vaid on alati kellegi otsuse tulemus, mida saab ka muuta. Kui üks huvidest hakkab süsteemselt teisi üle kaaluma, näiteks seetõttu, et andmete riskikasutus on tehniliselt lihtne, selle aluseks on pealtnäha vaieldamatu legitiimne eesmärk ning selle piiramine on poliitiliselt ebamugav, on ka see kellegi valik, mille eest tuleb vastutust kanda.

Raport lähtub neljast põhimõttest, millest tulenevad andmetöötluse tasakaalustatud alused.

- **Vajalikkus ja proportsionaalsus.** Riik ei tohi koguda andmeid üksnes seetõttu, et see on tehniliselt võimalik või et andmed võivad kunagi kasulikuks osutuda. Igal kogumisel ja igal päringul peab olema konkreetne eesmärk ning kogumise ulatus peab olema eesmärgiga mõistlikus vahekorras. Mida tundlikum on andmestik, seda kaalukam peab olema põhjus seda koguda ja kasutada.
- **Läbipaistvus inimese jaoks.** Inimene peab mõistliku vaevaga aru saama, milliseid andmeid tema kohta kogutakse, millisest registrist need pärinevad ja kes neid on vaadanud. Ilma selleta ei toimi ükski teine põhimõte, sest õigust, mille riivist inimene teada ei saa, ei saa ta ka kaitsta.
- **Sõltumatu ja sisuline kontroll.** Kontroll peab olema sõltumatu sellest, kes andmeid kasutab, ja see peab olema sisuline, mitte vormiline. Loakontroll, mis piirdub taotlusele allkirja andmisega, ei ole sisuline kontroll, nagu ei ole seda ka järelevalve, mis ei näe kõige suurema riivega toiminguid.

- **Inimese võimalus oma õigusi tegelikult kasutada.** Seaduses kirjas olev õigus tutvuda enda andmetega, nõuda nende parandamist või vaidlustada enda kohta tehtud otsus, peab olema päriselt kasutatav ja maksmapandav. Seda ei tohi takistada salastatus, teavitamata jätmine, menetluse keerukus ega lihtsalt see, et inimene ei tea juhtunust.

Nendest põhimõtetest lähtudes käsitletakse raportis järjest nelja küsimust. Esmalt selgitatakse, milliseid andmeid Eesti riik inimese kohta kogub ([1. peatükk](#)), seejärel seda, kes ja millisel alusel neile ligi pääseb ([2. peatükk](#)), edasi seda, kuidas kogutud andmeid järelvalves ja menetlustes kasutatakse ([3. peatükk](#)), ning viimaks seda, kui kaugele ulatub salajane teabe kogumine ja kui tõhus on selle üle teostatav kontroll ([4. peatükk](#)). Iga peatüki lõpus on esitatud ettepanekud.

Põhijäreldused

Eesti ei ole politsei riik ning autoritel puudub teave, et riigiasutused jälgiksid kodanikke süstemaatiliselt pahatahtlikult. Samas on Eestis kujunenud andmetöötuse süsteem, millel on jälgimisühiskonna struktuursed tunnused: andmeid kogutakse rutiinselt ja ilma inimese sisulise valikuvõimaluseta, neid kasutatakse inimeste liigitamiseks riskikategooriatesse, tähelepanu on suunatud võimalikule tulevasele teole ning riik teab inimesest palju, inimene riigist aga vähe.

Probleemi tuum on andmekogude koosmõju. Rahvastikuregister, kinnistusraamat, tervise infosüsteem, maksuandmed ja töötamise register on igaüks eraldi põhjendatud, kuid X-tee kaudu on registritevahelise andmeliikluse takistused tehniliselt kadunud, samal ajal kui regulatsioonid on jäänud registripõhiseks. Puudub üldnorm, mis piiraks mitme andmekogu riskasutust ühe isiku kohta, ning keegi ei vastuta profiili eest, mis tekib õiguspäraste päringute tulemuste liitmisel. Logid on ebaühtlased, sageli lühiajalised ega näita päringu eesmärki.

Kõige laiaulatuslikum kahtlusest sõltumatu kogumine toimub sideandmete puhul. Elektroonilise side seaduse § 111¹ kohustab sideettevõtjaid säilitama kõigi kasutajate liiklus- ja asukohaandmeid ühe aasta jooksul, kuigi Euroopa Kohus ja Riigikohus on sellise üldise säilitamise Euroopa Liidu õigusega vastuolus olevaks tunnistanud. Seadust ei ole muudetud ning andmestik on endiselt kättesaadav julgeolekuasutustele. Seda saab pidada privaatsusõiguse tahtlikuks ja teadlikuks rikkumiseks. Samamoodi võimaldab POLIS-e põhimäärus koguda määratlemata hulgal teavet määratlemata isikute ja objektide kohta üksnes seetõttu, et need võivad olla seotud mis tahes õigusrikkumisega.

Juurdepääs andmetele tugineb usaldusele asutuse vastu, mitte tegelikult toimuvale ja toimivale kontrollile. Valdav osa päringutest tehakse igapäevase haldusjärelvalve käigus, sageli üksnes viitega asutuse pädevusele. Põhjendust enne päringut ei nõuta, andmete väljastaja ei pea päringu põhjendatust sisuliselt kontrollima ning Riigikohtu sõnastatud piiranguid rakendatakse alles vaidluse korral. 2026. aastal avalikuks tulnud terviseandmete päringute juhtumid näitasid, et tundlike andmete töötlemise erikord praktikas sisuliselt ei toimi.

Ühel eesmärgil kogutud andmed liiguvad edasi riskimudelitesse, sealt järelvalvesse ning edasi väärteo- või kriminaalmenetlusse, ilma et eesmärgi muutumist kordagi eraldi hinnataks. Riigi tähelepanu algab pidevalt toimivas riskimudelil ammu enne menetlust, mil inimesel puudub õigus olla teavitatud või ära kuulatud või kus tal oleks kaebeõigus. Järelevalves sunni ähvardusel antud teave võib jõuda süüteomenetlusse ning Riigikohtu praktikast tulenevad tagatised rakenduvad alles tagantjärele.

Kontroll on kõige nõrgem seal, kus riive on kõige varjatud. Julgeolekuasutuste teabehanketoimingud kattuvad sisuliselt kriminaalmenetluse jälitustoimingutega, kuid teabehanke alused, uuritavate tegude ja isikute ring on määratlemata, enamik toiminguid tehakse asutuse juhi loal salastatud korras, kohtuloo saamise standard on madalam kui kriminaalmenetluses, statistikat ei avaldata ning teavitamine võib saabuda alles pärast kuni 50-aastase salastatuse lõppu. Õiguskantsleri ja Riigikogu erikomisjoni juurdepääs on piiratud või määratlemata ning ministrid on asunud oma haldusala asutusi kontrollimise asemel õigustama.

Teabehanke peamine väljund ei ole kriminaalmenetlus, vaid haldusmenetluslik ennetamine, mille käigus edastatakse hinnanguid teistele asutustele või tööandjatele. Tagajärjeks võib olla näiteks töösuhte lõpetamine, kuid inimene enamasti ei saa teada otsuse tegelikku põhjust ega saa seda tõhusalt vaidlustada.

Lahendus ei seisne digiriigi lammutamises. Vaja on, et iga päring tundlike andmete saamiseks oleks enne tegemist põhjendatud, et inimene saaks teada, kes tema andmeid vaatas ja miks, et sõltumatu organ teeks päringutele sisulist pistelist kontrolli, et logid oleksid täielikud ja auditeeritavad ning et teabehanke loakord ja teabe edastamine väljaspool süüteomenetlust viidaks kriminaalmenetlusega võrreldavale tasemele. Eesti digiriik on ehitatud usalduse peale, aga õigusriigi põhimõtted nõuavad, et seda usaldust saaks igal suvalisel hetkel testida, et veenduda seaduslikkuses.

Sissejuhatus

Digiriigist andmeriigini

Eesti riigikorraldus on viimase kolme aastakümne jooksul üldjoontes hästi toiminud. Riik on üles ehitanud põhiseaduslikud institutsioonid ja professionaalse avaliku halduse ning omandanud rahvusvaheliselt tunnustatud digiriigi maine. Samal ajal on ühiskond ning majandus- ja julgeolekukeskkond kiiresti muutunud ning koos sellega on muutunud ka riigi teadmiste maht oma kodanike kohta.

1990. aastate alguses keskenduti riigi andmetaristu loomisele ehk sellele, kuidas luua usaldusväärsed registrid kodanike, kinnisasjade ja ettevõtete kohta. Rahvastikuregister, äriregister ja kinnistusraamat loodi selleks, et riik teaks, kes on kes ja kellele mis kuulub, mitte inimeste jälgimiseks. 2000. aastatel lisandusid elektrooniline isikutuvastus, X-tee andmevahetuskiht ja põhimõte, et riik ei küsi inimeselt andmeid, mis tal juba olemas on. 2010. aastatel laienes andmestik tervise, liikumise, maksete ja hariduse valdkonda. 2020. aastateks on riigi käsutuses olevate andmete põhjal võimalik keskmise inimese elu rekonstrueerida päeva täpsusega, tuvastades vähese vaevaga tema elukoha, abikaasa, suhtlusringi, terviseprobleemid, piiriületused ja kiiruskaamerast möödumised, sissetuleku ja töökoha.

Sellist tulemust ei ole keegi teadlikult otsustanud. Iga register loodi eraldi, iga seadus võeti vastu eraldi ning iga liidestus X-teega oli omaette võetuna põhjendatud samm. Nende koosmõju ja sellest tulenevad kasutusvõimalused, sealhulgas kuritarvitamise oht, on aga kvalitatiivselt uus nähtus. Seetõttu on raporti esimene põhitähelepanek, et Eesti andmekogude probleem seisneb ennekõike nende koosmõjus, millest ühelgi asutusel ei ole terviklikku ülevaadet ja mille eest ükski asutus selget vastutust ei kannaks.

Mida tähendab „jälgimisühiskond“

Jälgimise kui võimu teostamise viisi filosoofiline käsitlus on mõistest endast tunduvalt vanem. Inglise filosoof ja õigusreformija Jeremy Bentham kavandas 18. sajandi lõpus panoptikoni ehk ringikujulise vangla, mille keskel asuvast vaatetornist saab valvur jälgida kõiki kambreid, ilma et kinnipeetavad teaksid, kas neid parasjagu jälgitakse. Benthami eesmärk oli tõhus ja odav järelevalve, kuid tema olulisim tähelepanek seisnes selles, et jälgimise pidev võimalikkus muudab inimese käitumist ka siis, kui teda tegelikult ei jälgita, mistõttu tuli välistada, et jälgitav saaks järelevalve puudumises veenduda. Prantsuse filosoof Michel Foucault laiendas panoptikoni ideed ühiskonnale tervikuna ning näitas, et kaasaegne võim toimib suurel määral nähtamatu vaatluse, registreerimise ja normaliseerimise kaudu. George Orwelli romaan „1984“ (1949) kirjeldas sama suundumust hoiatava düstoopiana. Raporti seisukohalt on

selles käsitluses oluline mõte, et jälgimise mõju ei sõltu üksnes andmete tegelikust kasutamisest, vaid ka inimese teadmisest, et tema kohta võidakse igal ajal teavet koguda ja seda vaadata. Paratamatult mõjutab see inimese käitumist juba iseenesest – inimesed, kes usuvad ennast olevat jälgimise all, kipuvad käituma nii, nagu nad arvavad, et neilt oodatakse ja nagu on korrektne.

Tänapäevane mõiste „jälgimisühiskond“ (ingl surveillance society) on teaduskirjanduses kasutusel alates 1980. aastatest. See ei tähenda tingimata poliitriiki ega totalitaarset režiimi. Jälgimisuuringute klassikud kirjeldavad pigem olukorda, kus isikuandmete süstemaatiline kogumine, salvestamine ja töötlemine on muutunud igapäevase halduskorralduse rutiinseks osaks. Inimese kohta kogutakse andmeid seetõttu, et ta kasutab teenuseid, liigub, teenib tulu ja käib arsti juures, mitte tingimata seetõttu, et teda milleski kahtlustatakse.*

Üldiselt võib tuua esile kolm tunnust, mis eristavad jälgimisühiskonda rutiinsest teabehaldusest. Esimene neist on sorteerimine, mille puhul liigitatakse inimesi andmete alusel riskantseteks ja riskivabadeks ning kontrollimist vajavateks ja mittevajavateks. Teine on ennetav loogika, mille puhul on tähelepanu suunatud võimalikule tulevasele teole ja piir süütu ning kahtlustatava vahel hägustub. Kolmas on asümmeetria, mis tähendab, et asutus teab inimesest palju, inimene asutusest aga vähe, ning see on süsteemi ülesehituse tulemus.

Eesti õiguskorras tuleb seega kontrollida, kas need kolm tunnust on olemas. Küsimus, kas Eestist on saamas jälgimisühiskond, on empiiriline ning sellele saab vastata hinnates, kui palju andmeid kogutakse, kui hõlpsasti neile ligi pääseb ja kui tõhus on selle üle teostatav kontroll.

Jälgimine ja usaldus

Eesti digiriigi edu on rajanenud usaldusel. Inimesed on andnud riigile andmeid eeldusel, et riik kasutab neid üksnes lubatud eesmärgil ning et nende kasutamise üle teostatakse järelevalvet. Kui ilmneb, et andmeid kasutatakse eesmärkidel, millest inimest ei teavitatud, või et keegi ei kontrolli, kes ja mis põhjusel päringuid teeb, usaldus väheneb ning koos sellega väheneb ka valmisolek digilahendusi kasutada.

Läbipaistvus ja kontroll on digitaalse õigusriigi eeltingimused. Riik, mis suudab näidata, kes ja mis põhjusel inimese andmeid vaatas, võib endale lubada ulatuslikumat andmetöötlust kui riik, mis seda näidata ei suuda. Tervise infosüsteemi ja riigiportaali andmejälgija on samm õiges suunas, kuid need lahendused on ebaühtlased ning kõige intensiivsemate riivete puhul puuduvad sootuks.

* D. Lyon. Surveillance Society: Monitoring Everyday Life. Buckingham: Open University Press 2001; D. Lyon. Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination. London: Routledge 2003; K. D. Haggerty, R. V. Ericson. The surveillant assemblage. – British Journal of Sociology 2000/51(4), lk 605–622; S. Zuboff. The Age of Surveillance Capitalism. New York: PublicAffairs 2019.

Põhiseadus ja Euroopa Liidu õigus

Põhiseadus kaitseb eraelu mitmest aspektist. Põhiseaduse § 26 kaitseb perekonna- ja eraelu puutumatust, § 33 kodu puutumatust, § 43 sõnumisaladust ning § 19 üldist vabadusõigust, millest Riigikohus on tuletanud ka informatsiooni enesemääramise õiguse ehk isiku õiguse teada ja mõjutada, mida riik tema kohta teab. Ükski neist õigustest ei ole absoluutne, kuid põhiseaduse § 11 järgi peab iga piirang olema seaduslik ja demokraatlikus ühiskonnas vajalik ega tohi moonutada piiratava õiguse olemust.

Euroopa õigus lisab sellele kaks kihti. Euroopa Liidu põhiõiguste harta artiklid 7 ja 8 kaitsevad eraelu ja isikuandmeid eraldi õigustena, isikuandmete kaitse üldmäärus (GDPR) ja õiguskaitsevaldkonna andmekaitse direktiiv sätestavad töötlemise põhimõtted ning Euroopa Kohus on mitmes otsuses andnud nendele põhimõtetele konkreetse ja õiguskaitseasutustele sageli koormava sisu. Kolmanda kihi moodustavad Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikkel 8 ning Euroopa Inimõiguste Kohtu praktika salajase jälgimise kohta.

Sellest tuleneb, et riik võib andmeid koguda ja kasutada, kuid peab iga kord suutma põhjendada õiguslikku alust ja eesmärki, näidata, et sama eesmärki ei ole võimalik saavutada vähem riivaval viisil, ning tagada, et nende asjaolude esinemist kontrollib sõltumatu isik. Kui mõni neist eeldustest on täitmata, on tegemist õigustamata põhiõiguse riivega.

Raporti põhiväide ja ülesehitus

Raporti põhiväide koosneb neljast osast. Esiteks kogutakse Eestis andmeid väga suures mahus ja valdavalt ilma, et inimesel oleks sisuline valikuvõimalus, sest andmeid kogutakse seaduse alusel, teenuse saamise või tavapärase ühiskonnale eeldusena või automaatselt. Teiseks ei jää kogutud andmed sinna, kuhu need koguti, vaid liiguvad X-tee ja õiguslike juurdepääsualuste kaudu asutuste vahel ning neid säilitatakse viisil ja eesmärkidel, milleks neid algselt ei kogutud. Kolmandaks kasutatakse andmeid riskianalüüsis, haldusjärelvalves ning väärteo- ja kriminaalmenetluses ka inimese enda vastu, sageli ammu enne seda, kui ta on formaalselt mõne menetluse osaline. Neljandaks on kontroll andmete kasutamise üle nõrk ja ebaühtlane, olles kõige tugevam seal, kus riive on nähtavam, ja nõrgem seal, kus riive on varjatud, kuid sageli ka kõige intensiivsem.

Igale väitele vastab raporti üks peatükk. Esimeses peatükis kaardistatakse Eesti andmekogud ja andmete kogumise viisid. Teises peatükis käsitletakse juurdepääsu andmetele, sealhulgas seda, kes andmeid küsib, millisel alusel ja kes selle üle kontrolli teostab. Kolmandas peatükis analüüsitakse andmete liikumist kogumisest riskianalüüsini ja sealt edasi menetlusse. Neljandas peatükis käsitletakse kõige intensiivsemat riivet ehk salajast teabe kogumist jälitus- toimingute ja julgeolekuasutuste teabehanke kaudu. Kokkuvõttes on esitatud järeldused ja ettepanekud.

Riigi andmekogud ja andmete kogumise viisid

Enne kui rääkida sellest, kes andmetele ligi pääseb, tuleb teada, millised andmed üldse olemas on. Õiguslikuks lähtekohaks on avaliku teabe seaduse määratlus, mille kohaselt on andmekogu riigi, kohaliku omavalitsuse või muu avalik-õigusliku isiku või avalikke ülesandeid täitva eraõigusliku isiku infosüsteemis töödeldavate korrastatud andmete kogum, mis luuakse seadusest, selle alusel antud määrusest või lepingust tuleneva ülesande täitmiseks.* Seega on andmekogu õiguslik institutsioon, mille olemasolu, eesmärk, andmekoosseis ja vastutav töötleja peavad olema õigusaktiga kindlaks määratud.

Justiits- ja Digiministeeriumi juhendis on rõhutatud, et isikuandmeid töötlev andmekogu tuleb asutada seadusega ning mida intensiivsem on riive, seda täpsem peab olema regulatsioon seaduse tasandil. Eri liiki isikuandmete (sealhulgas terviseandmete), maksu- ja pangasaladuse ning profiilianalüüsi puhul ei piisa üldisest volitusest andmekogu pidada, vaid seaduses endas tuleb sätestada, milliseid andmeid, millisel eesmärgil ja millistel tingimustel töödeldakse (vrd ka IKS ning GDPR art 6 lg 3 ja art 9). Nii säilitab parlament kontrolli selle üle, mida täitevvõim inimeste kohta teab.

Teine lähtekoht on tehniline, kuid õiguslikult vähemalt sama oluline. Andmevahetus riigi infosüsteemi kuuluvate andmekogude vahel toimub X-tee kaudu.** X-tee on turvaline andmevahetuskiht, mitte andmekogu ega andmeladu. Samas teeb just see kiht võimalikuks, et üks register saab peaaegu takistusteta teiselt andmeid küsida. Ajalooliselt on X-tee kaudu olnud ühendatud muu hulgas liiklusregister, ehtisregister, maksukohustuslaste register, piiriületuste andmekogu, karistusregister, viisaregister, tolli põhiinfosüsteem, töötajate register ja kinnistusraamatu päringusüsteem (loetelu ei ole ammendav).

Isik ja perekond

Kõige põhilisem andmestik puudutab seda, kes inimene on. Rahvastikuregister sisaldab nime, isikukoodi, sünniaega ja -kohta, kodakondsust, elukohta, perekonnaseisu, andmeid vanemate, abikaasa ja laste kohta, samuti teovõime piiranguid ja surmaandmeid. Perekonnaseisuandmed – sünd, abiolu, lahutus, surm – kantakse registrisse perekonnaseisuasutuse kaudu. Dokumendiregistris

* Avaliku teabe seadus § 43¹ lg 1. Vt ka Justiits- ja Digiministeeriumi juhend andmekogude asutamise ja kasutuselevõtu kohta.

** <https://www.ria.ee/riigi-infosusteem/andmevahetuse-platvormid/andmevahetuskiht-x-tee>

hoitakse andmeid isikut tõendavate dokumentide kohta ning nende juurde kuuluvat biomeetriat ehk näokujutist ja sõrmejälgi.

Rahvastikuregistri roll on eriline. Andmekaitse Inspeksiooni juhendmaterjal kirjeldab selle eesmärki kui järjepideva ja õigusliku tähendusega alusandmestiku loomist, mida teised andmekogud saavad kasutada.* Rahvastikuregister on kogu süsteemi selgroog, sest peaaegu iga teine register seob oma kirjed isikukoodi kaudu just selle andmestikuga. Sama juhend rõhutab, et laiemal andmekasutusel tuleb arvestada algset kogumise eesmärki ja andmete tundlikkust, kuid just see piir kipub praktikas hägustuma.

Andmete allikad on siin mitmetahulised. Osa andmeid esitab inimene ise (elukohateade), osa kolmas isik (sünni registreerimine haiglas, abielu registreerimine), osa tekib automaatselt teiste registrite kaudu. Biomeetria on seejuures erijuhtum, sest see kogutakse dokumenditaotlusel, kuid sisulist valikut inimesel ei ole, sest dokumendita ei ole Eestis võimalik elada.

Biomeetria ei ole siiski üksnes dokumendiregistri lisafunktsioon. Automaatse biomeetrilise isikutuvastuse süsteem ehk ABIS on eraldi andmekogu, mis on X-tee kaudu liidestatud muu hulgas isikut tõendavate dokumentide andmekogu, viisaregistri, elamis- ja töölubade registri, rahvusvahelise kaitse andmise registri ning sissesõidukeeldude registriga, samuti on tal süüteomenetluse otseliides. Isikut tõendava dokumendi taotleja kohta kantakse ABIS-esse foto või näokujutis ja sõrmejäljekujutised. Kriminaal- ja väärteomenetluses daktüloskopeerimisel (sõrmejälje võtmisel) ja näokujutise võtmisel saadud biomeetrilisi andmeid säilitatakse 40 aastat ning seejärel arhiiviosas veel 35 aastat; viisamenetluse biomeetrilisi andmeid hoitakse aktiivselt viis aastat ja seejärel arhiivis 50 aastat. See tähendab, et dokumenti taotledes kogutud biomeetria, välismaalaste menetlustes kogutud biomeetria ja süüteomenetluses kogutud biomeetria on osa ühest tehnilisest taristust, mille kasutamist kontrollitakse valdavalt asutusesiselt ja logide kaudu.

Vara ja ettevõtlus

Kinnistusraamat kogub, säilitab ja avalikustab teavet kinnisomandi tekkimise, üleandmise, asjaõigustega koormamise ning nende muutmise ja lõpetamise kohta. Kanded on teadlikult avalikud, sest see tagab kinnisvarakäibes õiguskindluse. Ühtlasi tähendab see, et inimese kinnisvara, hüpoteegid ja kaudselt ka majanduslik olukord on kättesaadavad viisil, mis muudes valdkondades oleks mõeldamatu.

Äriregister sisaldab andmeid osaluste, juhatuse liikmelisuse, tegelike kasusaajate ja majandusaasta aruannete kohta. Tegelike kasusaajate andmekogu logib päringu tegija nime, isikukoodi, päringu aja ja andmekoosseisu, kuid

* Andmekaitse Inspeksiooni juhendmaterjal „Andmeladude olemus ja selle funktsioonid“, lk 20.

logiandmeid säilitatakse üksnes kuni üks aasta, mis muudab hilisema kontrolli praktiliselt võimatuks. Liiklusregister seob inimese sõidukitega. Relvaregister seob inimese loa, relva, laskemoona, tervisetõendi, karistusregistri, POLIS-e, maksukohustuslaste registri ja kaitseväekohustuslaste registri andmetega; logiandmeid säilitatakse kolm aastat ning isikustatud andmed on asutusesiseks kasutamiseks. Ehitisregister on üldjuhul avalik ja selle andmeid säilitatakse alaliselt; samas logifaile säilitatakse vaid üks aasta. Laevade infosüsteem seob laeva ja omaniku andmed rahvastiku-, äri-, liiklusregistri ja laevakinnistusraamatu andmetega ning avalikustab registriosa andmed laeva ja omaniku kohta. E-residentsuse register lisab sellele majandusandmestikule välisriigi kodaniku digitaalse identiteedi ja taustakontrolli kihi.

Tervis

Tervise infosüsteemis koondatakse haiglate ja perearstide saadetud saatekirjad, epikriisid, diagnoosid, uuringutulemused ja pildid. Retseptikeskuses on andmed väljakirjutatud ja väljaostetud ravimite kohta, mis võimaldab diagnoosi järeldada ka siis, kui diagnoos ise ei ole kättesaadav. Sotsiaalkaitse infosüsteemides ja Töötukassa registrites on töövõime hindamise, puude raskusastme, rehabilitatsiooni, erihooletamise ja hüvitiste andmed. Patsiendiandmeid sisaldavat tervise infosüsteemi tuleb eristada tervishoiukorralduse infosüsteemist, mis on tervishoiutöötajate, proviisorite, farmatseutide, tegevuslubade ja tervise infosüsteemi juurdepääsuõigusega isikute register. Viimase andmeid säilitatakse 30 aastat pärast isiku surma või tegevusloa lõppemist ning logisid seitse aastat.

Terviseandmed on eriliiki isikuandmed, mille töötlemiseks on vaja selget õiguslikku alust ja tõhusaid kaitsemeetmeid. Praktikas on erandid siiski laiad. 2026. aastal avalikuks tulnud TEHIK-uga seotud juhtumid näitasid, et tervise infosüsteemist võidi andmeid väljastada kriminaalasja numbri alusel, ilma et väljastaja oleks sisuliselt hinnanud konkreetse isiku andmete väljanõudmise vajadust. Samuti ilmnes, et andmejälgija ei anna terviseandmete kasutamisest täielikku ülevaadet, kuna osa päringuid ei kajastu seal üldse ning eri logide säilitamine ja kuvamine ei ole omavahel kooskõlas. Seetõttu ei saa tervise infosüsteemi pidada hästi toimiva läbipaistvuse näiteks. Pigem nähtub sellest vajadus sätestada seaduses kohustus märkida päringus konkreetne õiguslik alus, eesmärk ja põhjendus ning tagada võimalus hiljem kontrollida, kas need tegelikult esinesid.

Liikumine

Liikumisandmed on kategooria, mis on viimase kümnendiga kõige rohkem kasvanud ja mille kogumisel on inimese osalus kõige väiksem. POLIS-e ennetava tegevuse andmestik sisaldab automaatse liiklusjärelvalve süsteemi salvestisi ja numbrituvastuskaamerate salvestisi. Numbrituvastuskaamera salvestis ei piirdu sõiduki numbriga, vaid sinna jäädvustatakse ka mootorsõidukis viibinud isiku kujutis, sõiduki registreerimisnumber ning pildistamise

aeg ja koht. Kui sellist salvestist ei kanta teise andmestikku, säilitatakse seda 45 päeva. Kui see seotakse mõne muu andmestikuga, säilitatakse seda vastava andmestiku tähtaja lõpuni. Piirikontrolli andmekogus säilitatakse piiriületuse andmeid kümme aastat ning neid kasutatakse siseturvalisuse ja avaliku korra tagamiseks. Broneeringuinfo süsteem kogub lennureisijate marsruudi, kaasreisijad, makseviisi ja kontaktandmed ning PNR-andmeid säilitatakse formaalselt viis aastat, kuid Euroopa Kohtu praktika nõuab, et pikaajaline säilitamine oleks seotud objektiivse riskiga, mitte kõikide reisijate andmete üldise säilitamisega.

Siin ilmneb kõige selgemalt erinevus üksiku andmepunkti ja nende põhjal moodustuva mustri vahel. Kui üks kaamerapilt näitab üksnes, et sõiduk oli teatud ajal teatud kohas, siis samade andmete pikem aegrida võimaldab tuvastada isiku töö-, elu- ja suhtlusharjumused. Sama kehtib piiriületuste kohta. Üksik piiriületus on üksik fakt, kuid kümne aasta piiriületuste andmed võimaldavad isikut profileerida. ABIS-e viisaandmete 5 + 50 aasta pikkune ja PNR-andmete viie aasta pikkune säilitustähtaeg näitavad, et liikumise ja piiriületusega seotud andmestikku tuleb käsitada pikaajaliselt säilitatava andmekogumina, mitte lühiajalise operatiivteabena.

Euroopa Liidu liikumisandmete süsteemid tugevdavad seda suundumust. EES, ETIAS, VIS ja nendega seotud ühine identiteedihoidla seovad reisidokumendi, isikuandmed ja teatud juhtudel biomeetrilised andmed ühtseks piirihalduse ja julgeoleku taristuks. Euroopa Kohtu PNR-praktika järgi ei saa reisijate andmete pikaajalist üldist säilitamist õigustada pelgalt mugavuse või abstraktse ennetushuviga; säilitamine peab olema seotud konkreetse, objektiivselt tuvastatava riskiga.*

Sideandmed: kõigi inimeste liiklus- ja asukohaandmete kohustuslik valimatu kogumine

Kõige laiaulatuslikum automaatne andmekogumine toimub erasektori andmekogudes. Elektroonilise side seaduse § 111¹ kohustab sideettevõtjat säilitama andmeid, mis võimaldavad tuvastada side allika ja sihtpunkti, side kuupäeva, kellaaja ja kestuse, sideteenuse liigi, kasutaja terminalseadme ning terminal-seadme asukoha. Andmeid säilitatakse üks aasta alates side toimumise ajast. Kohustus ei sõltu kahtlusest ega menetlusest ning kehtib iga telefoni- ja internetiteenuse kasutaja kohta, sõltumata sellest, kas tema suhtes on kunagi mingit menetlust alustatud. Riik paneb sideettevõtjatele kohustuse hoida andmed tema jaoks valmis, et õiguskaitse- ja julgeolekuasutused saaksid need hiljem elektroonilise side seaduse § 112 alusel välja nõuda.

* Euroopa Parlamendi ja Nõukogu direktiiv (EL) 2016/681 (PNR-direktiiv). Vt sideandmete ja massilise andmesäilituse kohta nt C-511/18, C-512/18 ja C-520/18, La Quadrature du Net jt. Vt ka Euroopa Andmekaitseinspektori (EDPS) seisukohad keskandmekogude vajalikkuse hindamise ja kaitsemeetmete kohta.

Riigikohus on selgitanud, et elektroonilise side seaduse § 111¹ äärmiselt avara sõnastuse tõttu tuleb sideettevõtjale pandud kohustusi käsitada liiklus- ja asukohaandmete üldise ja vahet tegemata säilitamisena, mis hõlmab kõiki kasutajaid ja kõiki seadmeid, ning et säte on selles osas vastuolus Euroopa Liidu õigusega. Euroopa Liidu õigusega vastuolus olevat sätet ei saa kohaldada. Seadust ei ole asjassepuutuvas osas aga muudetud ning sideettevõtjad jätkavad kõigi klientide andmete säilitamist, viidates sellele, et seadus kohustab neid seda tegema.

Selle andmestiku ulatust on raske üle hinnata. Euroopa Kohus on rõhutanud, et liiklus- ja asukohaandmed võimaldavad koosvõetuna teha väga täpseid järeldusi inimese igapäevaelu harjumuste, elukoha, liikumiste, sotsiaalsete suhete ja tutvusringkonna kohta ning koostada profiili, mis on eraelu puutumatus seisukohalt sama tundlik kui sideseansi sisu ise. Sideandmete kogumine on seega jälgimisühiskonna tunnuste kõige puhtam näide, sest kogumine on üldine ja kahtlusest sõltumatu, toimub inimese teadmata ja tema valikut küsimata, riik on selle delegeerinud eraettevõtjatele ning see jätkub ka pärast seda, kui kõrgeim kohus on selle Euroopa Liidu õigusega vastuolus olevaks tunnistanud.

Raha ja maksud

Maksukohustuslaste register koondab Maksu- ja Tolliameti hallatavad rakedused ja alamregistrid. Sellesse kuuluvad lisaks tavapärastele deklaratsioonide ja maksuvõlaandmetele ka näiteks hasartmängu mängimise piirangutega isikute nimekiri ning ehitusplatside pääsulogid, mis sisaldavad sisenemise ja väljumise kellaegu, tuvastuskaartide koode, objektil viibimise kestust sekundites ning sõiduki registreerimisnumbrit. Registri üldandmeid säilitatakse kümme aastat pärast isiku surma või juriidilise isiku lõppemist, alamregistre andmeid sõltuvalt liigist ühest kuni 75 aastani. Auditlogi sisaldab kasutaja nime, aega ja päringu või kande objektiks olnud andmekoosseisu, kuid mitte päringu eesmärki, ning seda säilitatakse kaks aastat. Rahapesu Andmebüroo andmekogu RABIS on veel kontsentreeritum andmeladu, kuhu kantakse teated, tehingu osapooled, pangakontod, tehingu summa, vara päritolu ning andmed rahvastikuregistrist, karistusregistrist, e-toimikust, äriregistrist, maksukohustuslaste registrist, kinnistusraamatust, liiklusregistrist, tegelike kasusaajate andmekogust ja POLIS-est.

Finantsandmeid ei esita peaaegu kunagi inimene ise. Need esitab tööandja, pank, makseasutus või raamatupidaja, kellel on sageli seadusest tulenev kohustus jätta inimene andmete edastamisest teavitamata. Rahapesu tõkestamise teatamiskohustusega kaasneb avaldamiskeeld, mistõttu inimene ei tea, et tema tehingust on teatatud. RABIS-e põhimäärusest nähtub, kui ulatuslik selline teabe kogumine võib olla. Andmeid võivad esitada nii kohustatud isikud kui ka isik, kes edastab teavet kahtlase või ebahariliku tehingu kohta, vastutav töötaja teeb päringuid ka Euroopa Liidu ja rahvusvahelistesse infosüsteemidesse ning logisid säilitatakse kümme aastat, kuid päringu eesmärki ei pea ka seal eraldi märkima.

Haridus ja töö

Eesti hariduse infosüsteem sisaldab andmeid õppeasutuste, õpilaste ja üliõpilaste, õpitulemuste, lõpetamise ja kvalifikatsioonide kohta. Töötukassa registrid sisaldavad andmeid töötuse, töövõime, teenuste ja hüvitiste kohta. Sotsiaalkaitse infosüsteem sisaldab pensionide, riiklike toetuste, ohvriabi, erihoolekande, rehabilitatsiooni, abivahendite, puude raskusastme ja töövõime andmeid. Pensioniandmeid säilitatakse 75 aastat pärast isiku surma; lapse puude otsuse andmeid säilitatakse 60 aastat pärast viimase otsuse kestuse lõppu; logiandmeid säilitatakse viis aastat. Töötukassa on sotsiaalkaitse infosüsteemile andmeandja muu hulgas töövõime hindamise otsuste, eksperdiarvamuste, töövõimetoetuse, tööturuteenuste ja töötuna arveloleku kohta.

Esmapilgul võivad need andmestikud näida vähem tundlikena kui tervise- või liikumisandmed, kuid tegelikult kirjeldavad need inimese sotsiaalmajandusliku olukorra muutumist ajas, sealhulgas seda, kas ja kui kauaks ta jäi töötuks, millist toetust ta sai ja kas ta katkestas õpingud. Riskianalüüsi seisukohalt on selline andmestik kasutuskõlblik ning just selle põhjal tehtud liigitusi on kõige keerulisem vaidlustada.

Õiguskaitse

Politsei andmekogu POLIS sisaldab ühiseid infoobjekte (isik, ettevõtte, aadress, sõiduk, sidevahend, ese, dokument ja relv), süüteomenetluse andmeid, haldustegevuse andmeid, ennetava tegevuse andmeid, reageeriva tegevuse andmeid, otsimise andmeid, arestimajade andmeid ja jälitusmenetluse andmestikku. Ennetava tegevuse andmestikus on eriti oluline „hinnanguline ohumärke“ isiku või aadressi kohta, mis on seotud toimepandud või tõenäoliselt tulevikus toime pandava õiguserikkumisega. Majutusteenuse kasutajate andmete alusel tehakse automaatpäring otsimise andmestikku, Interpoli andmekogudesse, Schengeni infosüsteemi ja julgeolekuasutusele. Julgeolekuasutusel on juurdepääs kõigile POLIS-e andmestikele talle seadusega pandud ülesannete täitmiseks. Jälitusmenetluse andmestikku säilitatakse 25 aastat ning arhiivis veel 50 aastat.

Õiguskaitse andmekogudel on kolm eripära. Esiteks sisaldavad need andmeid isikute kohta, kellele ei ole kunagi süüdistust esitatud, nagu tunnistajad, kannatanud, kontaktisikud ja menetlusvälised isikud, kelle andmed on toimikusse sattunud juhuslikult. Teiseks sisaldavad need andmeid, mida ei ole kohtuotsusega kinnitatud, näiteks kahtlustusi, hinnanguid, märkusi, riskihinnanguid ja ohumärkeid, mille faktiline alus võib olla kontrollimata. Kolmandaks hõlmab osa andmekogusid suletud julgeoleku alasüsteeme. Teenistus- ja tsiviilrelvade registris on eraldi Kaitsepolitseiameti relvaregister, mis ei vaheta andmeid registri teiste osade ega teiste andmekogudega ning mille üle teostab järelevalvet Kaitsepolitseiamet ise. ABIS-e kasutamist kontrollitakse vähemalt kord aastas juhuvaliku alusel, kuid näiteks õiguskantsleril puudub juurdepääs pooleliolevatele teabehanketoimingutele ja salastatud meetoditele. Selliste andmete säilitamine ja hilisem kasutamine on õiguslikult tundlikum kui jõustunud karistuse kohta käivate andmete säilitamine, kuid praktikas ei eristata neid piisavalt.

Andmekogude koosmõju

Eraldi võetuna ei pruugi ükski eespool kirjeldatud andmekogu põhjustada ülemäära riivet. Rahvastikuregister on vajalik, kinnistusraamat peab olema avalik, tervise infosüsteem aitab päästa elusid ja maksuandmed on vajalikud maksude kogumiseks. Probleem tekib siis, kui need süsteemid on omavahel ühendatud selliselt, et ühe päringuga on võimalik saada ülevaade, mida ükski register eraldi ei sisalda.

Rahvastikuregistrist saab teada inimese elukoha ja perekonna, töötamise registrist tööandja, maksukohustuslaste registrist sissetuleku ja maksukäitumise, ehitusplatside pääsulogidest tööobjektidel viibimise aja, liiklusregistrist sõiduki, kinnistusraamatust kinnisvara ja hüpoteegid, numbrituvastuskaameratest liikumismustri, retseptikeskusest kaudselt terviseseisundi, piirikontrolli andmekogust reisi, ABIS-est biomeetria ning POLIS-est varasemad kontaktid politsei või järelevalvetega. RABIS näitab koosmõju eriti selgelt, sest selle põhimäärus lubab töödelda andmeid rahvastikuregistrist, karistusregistrist, e-toimikust, äriregistrist, maksukohustuslaste registrist, kinnistusraamatust, liiklusregistrist, tegelike kasusaajate andmekogust ja POLIS-est. Iga üksik päring on õiguslikult põhjendatav, kuid nende koosmõju loob profiili.

Õiguslikult tuleb siin tuvastada kaks lünka. Esiteks puudub üldnorm, mis piiraks mitme andmekogu riskasutust ühe isiku kohta, sest piirangud on sätestatud registre kaupa, mitte isikust lähtudes. Teiseks ei ole kellelgi terviklikku ülevaadet, kuna iga vastutav töötaja vastutab oma registri eest, kuid registre koosmõjul tekkiva uue kvaliteediga andmestiku eest ei vastuta keegi. Riigi infosüsteemi haldussüsteem (RIHA) on küll registre register, kuid see on loodud haldusotstarbel ega hinda põhiõiguste riivet.

Eeltoodust tulenevalt leiavad autorid, et probleemi tuum on koosmõjus. Jälgimisühiskonnale on iseloomulik, et registrevahelise andmevahetuse piirangud on kadunud või nõrgenenud, samal ajal kui järelevalve on jäänud pealiskaudseks ja registripõhiseks.

Sama kehtib järelevalve kohta. Andmekogude logid on ebaühtlased, sest näiteks ehitisregistri logisid säilitatakse üks aasta, relvaregistri omi kolm aastat, maksukohustuslaste registri omi kaks aastat, RABIS-e omi kümme aastat, ABIS-e omi kümme aastat ja tegelike kasusaajate andmekogu omi kuni üks aasta. Mõnes logis on päringu objektiks olnud andmekoosseis, mõnes ainult kasutaja ja aeg, mõnes töötlemise sisu, kuid sageli ei ole logis päringu eesmärki. Kui logi ei näita, miks andmeid vaadati, saab hiljem kontrollida ainult seda, kes vaatas ja millal, mitte seda, kas vaatamine oli põhjendatud.

Ettepanekud

- **Luua ja avaldada riigi andmekogude koondülevaade**, mis on koostatud üldsusele, mitte infosüsteemi haldajale arusaadaval viisil ning milles selgitatakse, milliseid andmeid iga andmekogu sisaldab, kust need pärinevad, kui kaua neid säilitatakse ja millistel asutustel on neile juurdepääs. RIHA andmed on olemas, kuid praegusel kujul ei ole need üldsusele arusaadavad.
- **Viia läbi süsteemne andmete minimeerimise ülevaatus**, kus iga andmekogu puhul tuleks põhjendada, miks iga andmestik on vajalik, ja loobuda nendest, mille vajalikkust põhjendada ei suudeta. Praegu on vaikumisi eeldus andmete säilitamise kasuks.
- **Vaadata üle säilitustähtajad**. Mitme registri puhul on tähtajad kas määramata või määratud ilma seoseta eesmärgiga, milleks andmeid koguti. Eriti puudutab see liikumisandmeid ja õiguskaitse andmekogudes olevaid andmeid isikute kohta, kelle suhtes menetlust ei alustatud või kes jäeti süüdistuseta.
- **Kehtestada ristkasutuse ja logimise reegel andmesubjekti, mitte registri tasandil**. Kui ühe menetluse raames tehakse päringuid mitmesse andmekogusse, tuleb see eraldi dokumenteerida ja põhjendada ning tagada, et seda saab hiljem isikupõhiselt kontrollida. Igas päringus tuleb märkida vähemalt õiguslik alus, eesmärk, põhjendus, andmekoosseis, päringu tegija ja aeg. Neid andmeid tuleb säilitada piisavalt kaua, et järelevalve ei sõltuks juhusest ega sellest, kas isik jõuab kaebuse õigeaegselt esitada.

Andmetele juurdepääs: kes, millal ja millise põhjendusega

Eraelu intensiivne riive leiab aset hetkel, mil keegi andmeid vaatab, mistõttu on juurdepääsu regulatsioon põhiõiguste kaitse seisukohalt koguni olulisem, kui kogumise regulatsioon. Just siin ilmnevad ka Eesti õiguskorra puudused kõige selgemalt.

Juurdepääsu õiguspärasuse hindamisel lähtub raport neljast kriteeriumist. Esiteks tuleb hinnata eesmärki ehk seda, milleks andmeid küsitakse ja kas see on seotud andmete kogumise algse eesmärgiga. Teiseks tuleb hinnata nõutavat põhjendamise standardit ehk seda, kas päringu tegija peab selgitama, miks ta vajab just neid andmeid just selle isiku kohta, või piisab viitest üldisele pädevusele. Kolmandaks tuleb hinnata tundlikele andmetele kohaldatavat erikorda ehk seda, kas pangasaladus, maksusaladus, terviseandmed ja sideandmed on kaitstud rangemalt kui muud andmed ning kas see erikord on sisuline või üksnes vormiline. Neljandaks tuleb hinnata kontrolli päringu vajalikkuse üle ehk seda, kas päringu põhjendatust hindab enne või pärast päringut keegi väljaspool päringut tegijat.

Nende kriteeriumide alusel hinnates ilmneb, et enamikus olukordades on kõik neli tagatist ebapiisavad.

Haldusjärelevalve

Avalikus arutelus seostatakse andmetele juurdepääsu peaaegu alati kuritegevuse ja julgeolekuga, kuid selline käsitlus on eksitav. Kõige rohkem pärinuid teevad haldusorganid tavapärase haldusjärelevalve käigus, kontrollides näiteks maksude tasumist, toetuste saamise õigust, tööohutust, tarbijakaitse nõuete täitmist või kutsetegevuse reeglite järgimist. Just haldusjärelevalves puutub tavaline inimene riigi andmetöötlusega kõige tõenäolisemalt kokku ning just siin on kaitsemeetmed kõige nõrgemad.

Selles valdkonnas on suurim andmetöötleja Maksu- ja Tolliamet. Tema käsutuses on deklaratsioonid, töötamise register, pankade aruandlus, liiklusregistri andmed, kinnistusraamat, äriregister ja hulk muid allikaid ning lisaks on tal maksukorralduse seaduse alusel õigus nõuda teavet nii maksukohustuslaselt kui ka kolmandatelt isikutelt. Samuti tuleb esile tõsta Rahapesu Andmebürood, kes kogub krediidi- ja finantseerimisasutustelt teateid kahtlaste ja ebatavaliste tehingute kohta ning analüüsib neid. Finantsinspeksioon teostab järelevalvet finantssektori üle ning Tarbijakaitse ja Tehnilise Järelevalve Amet, Terviseamet, Tööinspeksioon ja Andmekaitse Inspeksioon oma pädevusvaldkondades. Kohalikud omavalitsused ja hüvitisi maksvad asutused, sealhulgas Sotsiaalkindlustusamet, Töötukassa ja Tervisekassa, kontrollivad toetuste ja hüvitiste saamise aluseid.

Riigikohus on haldusjärelvalves esitatavate teabenõuete lubatavuse piire selgitanud. Maksuhalduri poolt menetlusvälisele isikule esitatud teabenõuet puudutavas asjas leidis kohus, et nõutav teave peab olema seotud läbiviidava maksumenetlusega ning kui seos ei ole andmete iseloomu järgi äratuntav, peab maksuhaldur selgitama, milles see seisneb (RKHK 3-16-2324/18). Seega peab haldusorgan näitama konkreetse seose konkreetse menetlusega ning viide üldisele pädevusele ei ole piisav.

Samas lahendis rõhutas kohus ka proportsionaalsuse põhimõtet. Füüsilise isiku piiritlemata kohustamine tõendada oma varasemate sissetulekute päritolu ei ole proportsionaalne, vaid nõue tuleb ajaliselt ja/või esemeliselt piiritleda. Haldusorgan ei saa seega nõuda inimeselt üldiselt selgitust, kust ta oma raha sai, vaid nõue peab olema seotud konkreetse perioodi või konkreetse varaga.

Nendest seisukohtadest nähtub, kus probleem täpsemalt seisneb. Kohtupraktika nõuab seost menetlusega ja nõude piiritletust, kuid seda nõuet rakendatakse alles siis, kui isik teabenõude vaidlustab. Enamik teabenõudeid kohtusse ei jõua, sest vaidlemine on kulukas ja aeganõudev ning võib tuua kaasa haldusorgani veelgi suurema tähelepanu, mida isik soovib vältida. Seega on õigulik standard küll olemas, kuid selle tegelik rakendamine sõltub sellest, kas isikul on vaidlemiseks piisavalt ressursi.

Andmekaitse Inspeksioon on sellele suundumusele juba aastaid tähelepanu juhtinud. Inspeksiooni 2015. aasta aastaraamatus nimetati probleemina kavatsust anda kindlustusseltsidele otsejuurdepääs e-tervise andmetele ning maksuhalduri soovi saada sideettevõtjatelt sideandmeid ja riskihindamiseks juurdepääs kõikidele andmekogudele. Inspeksioon pidas neid kavatsusi ülemääraseks.* Kuigi need näited pärinevad kümne aasta tagant, on nende loogika asjakohane ka praegu. Kui asutus soovib andmeid analüüsida, kipub tema huvi laienema võimalikult suurele andmehulgale, mitte üksnes rangelt vajalikule.

Rahapesu Andmebüroo tegevus on riskipõhine ning kohustatud isikud, sealhulgas pangad, makseasutused, notarid ja teatud tehingute puhul advokaadid, peavad hindama kliendi riski ja teatama ebatavalistest tehingutest. Riskipõhisus on küll rahvusvaheliselt tunnustatud standard, kuid sellega kaasneb madal teatamiskünnis, mistõttu võib inimene sattuda analüüsi objektiks ilma ühtegi ebaseaduslikku tegu toime panemata.

* Vt Andmekaitse Inspeksiooni aastaraamat 2015.

Väärteomenetlus

Haldusjärelevalve ja karistamise piir on Eesti õiguses hägusem, kui üldiselt arvatakse. Sama asutus, kes teostab järelevalvet, on sageli ka kohtuväline menetleja, kellel on õigus väärteo eest karistada. Nii kontrollib Tööinspeksioon töötingimusi ja karistab nende rikkumise eest, maksuhaldur kontrollib deklaratsioone ja menetleb maksualaseid väärteid ning politsei teostab liiklusjärelevalvet ja menetleb liiklusväärteid.

Praktikas võib järelevalvemenetluses kogutud teave liikuda väärteomenetlusesse. Järelevalvemenetluses on isikul sageli kohustus aidata kaasa menetluse läbiviimisele ja anda haldusorganile sunnivahendi kohaldamise ähvardusel teavet, väärteomenetluses on ta aga menetlusalune isik, kellel on õigus vaikida. Seejuures ei pruugi isik aru saada, millal tema menetlusseisund muutus.

Kriminaalmenetlus

Kriminaalmenetluses on andmetele juurdepääs korraldatud kolmel tasandil. Esimesel tasandil on päringud, mille puhul luba ei ole vaja ja uurimisasutus võib pöörduda andmekogu poole ning saada andmeid oma pädevuse alusel. Siia kuulub enamik päringuid riigi andmekogudesse, nagu rahvastikuregister, liiklusregister, äriregister ja karistusregister. Teisel tasandil on toimingud, mis nõuavad prokuratuuri luba. Kolmandal tasandil on toimingud, mis nõuavad eeluurimiskohtuniku luba, eelkõige sõnumisaladust või kodu puutumatust riivavad jälitustoimingud.

Suurem osa kriminaalmenetluses kasutatavatest andmetest saadakse esimesel tasandil ehk ilma kohtuliku kontrollita, samas kui kohtulik kontroll on ette nähtud toimingutele, mida seadusandja pidas kõige intensiivsemaks riiveks. See hinnang anti aga ajal, mil andmekogude koosmõju oli tunduvalt väiksem. Praegu võib päring kümnesse registrisse anda isiku kohta rohkem teavet kui 1990. aastatel tehtud salajane pealtkuulamine, ilma et keegi väljaspool uurimisasutust sellest teada saaks.

Erandiks on side- ja asukohaandmed, kus Euroopa Liidu õigus on seadnud selge piiri. Euroopa Kohus otsustas Eesti eelotsusetaotluse alusel tehtud lahendis Prokuratuur, et juurdepääs elektroonilise side liiklus- ja asukohaandmetele, mis võimaldavad teha täpseid järeltõlkeid inimese eraelu kohta, peab olema piiratud raske kuritegevuse vastase võitluse või avalikku julgeolekut ähvardava tõsise ohu ennetamisega (EKo 02.03.2021, C-746/18; vt ka RKKKo 18.06.2021, 1-16-6179). Lisaks peab sellisele juurdepääsule eelnema kohtu või sõltumatu haldusorgani eelkontroll.

Sama lahendi teine osa on Eesti jaoks veelgi olulisem. Euroopa Kohus leidis, et prokuratuur, kes juhib kriminaalmenetlust ja võib hiljem esindada riiklikku süüdistust, ei ole eelkontrolli mõttes piisavalt sõltumatu (EKo C-746/18, H. K. vs. Prokuratuur). Selle seisukoha põhjus on struktuurne, sest sama asutus ei saa olla üheaegselt menetluse juht ja menetlustoimingute seaduslikkuse sõltumatu kontrollija.

Julgeolekuasutused

Kõige intensiivsem juurdepääs andmetele toimub julgeolekuasutuste seaduse (JAS) alusel tehtavate teabehanketoimingute raames. Tegemist on paralleelse režiimiga, mille meetodid kattuvad kriminaalmenetluse jälitustoimingutega, kuid mille põhiõiguste tagatised on oluliselt nõrgemad.

Mõistete lahtisus

Kriminaalmenetluse seadustik sätestab jälitustoimingute tegemiseks konkreetsed alused, milleks on kuriteo tõkestamine, tagaotsitava leidmine, konfiskeeritava vara leidmine ja kriminaalmenetluses teabe kogumine (KrMS § 126² lg 1; KrMS §-d 126⁵–126⁹). Esiteks ei ole JAS-is selliseid aluseid. Teabehanketoiminguid reguleerivad üksnes julgeolekuasutuste üldine eesmärk, s.o riigi julgeoleku tagamine põhiseadusliku korra püsimisega, ning väga üldiselt sõnastatud ülesanded (JAS § 2 ja § 6).

Teiseks puudub tegude kataloog, mille uurimiseks teabehanketoiminguid teha võib. Kui kriminaalmenetluses on jälitustoimingud lubatud üksnes seaduses loetletud kuritegude ehk nn kuritegude kataloogi tõendamiseks (KrMS § 126² lg 2),* siis teabehanke puhul ammendavat kataloogi ei ole ning piiriks on taas vaid seaduse eesmärk ja asutuse ülesanded.

Kolmandaks ei ole piiritletud subjektide ring. Kriminaalmenetluse seadustik määrab kindlaks, kelle suhtes jälitustoiminguid teha võib (KrMS § 126² lg 3). JAS-is sellist piirangut ei ole. Erinevalt jälitustoimingutest võib teabehanketoiminguid teha ja teavet varjatult koguda sisuliselt igaühe kohta. Praktiline tagajärg on see, et kui ühe inimese kohta teabe kogumine on põhjendatud, puudub regulatsioon, mis piiraks tema pereliikmete, sõprade või tuttavate jälgimist selle inimese kohta teabe saamiseks.

Seega on probleem sisuline. Määratlemata õigusmõisted on õiguskorras tava-pärased ja sageli vältimatud, kuid nende sisustamine peab olema kontrollitav. Kui intensiivse riive alus, uuritavate tegude ring ja isikute ring on kõik määratlemata ning neid sisustab asutus ise, ei jää alles ühtegi sisulist ja kontrollitavat õiguslikku piirangut.

Infomonopol

Julgeolekuasutuste puhul ei seisne probleem üksnes määratlemata õigusmõistetes. Muudel juhtudel annab määratlemata õigusmõiste sisule lõpliku hinnangu kohus, kuid riigi julgeoleku puhul on kohus jätnud selle hinnangu haldusorgani ehk julgeolekuasutuse pädevusse. Halduskohtupraktikas on JAS

* Tuleb möönda, et see kataloog on aastatega järjest laienenud ja praeguseks muutunud peaaegu kõikehõlmavaks.

§ 6 tõlgendatud nii, et hinnang selle kohta, millest ja kellest tuleneb oht riigi julgeolekule, kuulub Kaitsepolitseiameti pädevusse (RKHKo 3-17-1026, p 33). Seega on asutusel endal praktikas ainuõigus hinnata, mis ja kes kuulub tema ülesannete alla, ning kohtul on vähe alust seda hinnangut sisuliselt kontrollida.

Samas lahendis leidis Riigikohus, et määratlemata õigusmõistete sisustamise õigus ja kohustus lasub menetluse eest vastutaval haldusorganil. Uurimis- põhimõttest tulenevalt on just see haldusorgan see, kes otsustab, kas ja milliseid täiendavaid tõendeid koguda, ning vastutus menetluse tulemuse õiguspärasuse eest jääb temale.

Nende kahe seisukohaga koosmõjus kujuneb Eesti õiguskorras järgmine olukord. Formaalselt vastutab otsuse eest haldusorgan, kes peab määratlemata õigusmõiste ise sisustama ja vajaduse korral täiendavaid tõendeid koguma. Sisuliselt tugineb hinnang aga teabele, mida valdab ja hindab julgeolekuasutus ning millega isik ei saa tutvuda ja mida ta ei saa tõhusalt vaidlustada. Seetõttu tekib julgeolekuasutusel isiku üle täielik infomonopol, mille tagajärjel võib isik teada saada, et teda peetakse julgeolekuohuks, ilma et talle avaldataks selle hinnangu põhjuseid.

Kohtu luba kui prognoosotsus

Osa teabehanketoiminguid nõuab halduskohtu luba. Selliste toimingute hulka kuuluvad sõnumisaladuse piiramine ning ruumi, hoone, piirdega ala, sõiduki või arvutisüsteemi varjatud läbiotsimine (JAS § 27 lg 1). Esmapilgul on see sarnane kriminaalmenetluse kohtuloaga, kuid sisuliselt on loa andmise standardid erinevad.

Halduskohtu loa puhul on tegemist prognoosotsusega. Kohtupraktikas on teabehanke tegemise eelduseks olevat põhjendatud kahtlust kirjeldatud kui prognoosi, mis tugineb kindlaks tehtud faktilistele asjaoludele, kuid mis ei kajasta tõsikindlat teadmist ähvardavast ohust (TlnRKo 16.06.2015, 3-12-983, p 10). Ka õiguskirjanduses on rõhutatud, et tegemist on oma olemuselt tõenäosusel põhineva prognoosotsusega.*

Kriminaalmenetluses kehtib jälitusloale rangem standard. Riigikohus on leidnud, et jälitustoimingu loast peab nähtuma, millistest konkreetsetest asjaoludest ja tõenditest lähtub põhjendatud kuriteokahtlus ning milliste konkreetse juhtumi asjaolude põhjal on mõistlik eeldada, et muude tõendikogumisviiside kasutamine on välistatud (RKKKm 14.12.2017, 1-17-7077, p 71). Ringkonnakohtud on seda nõuet järjekindlalt rakendanud ning lugenud ebapiisavaks põhjendused, mis on esitatud üksnes järelduse vormis või mida saaks kasutada igas sama liiki kriminaalasjas (TrtRKo 28.09.2021, 1-19-6293, p 61–62 ja 126). Seega on mõlema loa eelduseks põhjendatud kahtlus, kuid

* J. Jäätma. Ohutõrjeõigus politsei- ja korrakaitseõiguses: kooskõla põhiseadusega. Tartu: Tartu Ülikooli Kirjastus, lk 173.

teabehanke puhul rajaneb see üksnes tõenäosusel, kriminaalmenetluses aga konkreetsetel asjaoludel ja tõenditel, millele lisandub kohustus põhjendada, miks muud tõendikogumisviisid ei ole piisavad. Teabehankeloa andmise standard on seetõttu oluliselt madalam.

Ülejäänud teabehanketoimingud ei vaja kohtu luba. Varjatud jälgimist, isiku samasuse varjatud tuvastamist, sideandmete kogumist ja asja varjatud läbi-vaatust võib teha julgeolekuasutuse juhi või tema volitatud ametniku loal (JAS § 27 lg 3). Probleem ei piirdu sellega, et loa annab asutus ise. Julgeolekuasutuse juhi loa andmise kord on kehtestatud asutuse sisemise töökorraldusega ja on riigisaladus, mistõttu ei ole väljastpoolt võimalik veenduda, millised piirangud ja põhjendamiskohustused sellele loale kehtivad ega isegi seda, kas need on üldse olemas. PS § 11 järgi peab põhiõiguse piirang olema demokraatlikus ühiskonnas vajalik ega tohi moonutada piiratava õiguse olemust ning Riigikohtu praktika kohaselt tuleb piirangu proportsionaalsust hinnata sobivuse, vajalikkuse ja mõõdukuse astmel. Asutusesisene luba võib olla eesmärgi saavutamiseks sobiv, sest see võimaldab kiiresti reageerida. Vajalikkuse astmel jääb aga vastuseta küsimus, miks ei piisaks sama tõhusast, kuid vähem riivavast abinõust, näiteks sõltumatust eelkontrollist või kiireloomulistel juhtudel kohtu järelkontrollist, nagu see on ette nähtud kriminaalmenetluses samade toimingute puhul. Mõõdukuse astmel tuleb arvestada, et riive on varjatud ja kestuselt piiramata ning isik ei saa sellest üldjuhul teada. Kui ka loa andmise kord on salastatud, ei ole väljastpoolt võimalik kontrollida, kas kaalumine üldse toimus.

Kui menetlust juhtiv prokuratuur ei ole Euroopa Kohtu hinnangul sõltumatu eelkontrolli andja, on asutuse juht, kes annab loa oma asutuse toimingule, sõltumatusest veel kaugemal. Seega puudub valdava osa teabehanketoimingute üle asutuseväline eelkontroll.

Analüüs: neli kitsaskohta

Eeltoodu põhjal saab välja tuua neli kitsaskohta, mis läbivad kogu juurdepääsuregulatsiooni.

Esiteks pääseb andmetele ligi ka väiksema raskusega asjades. Avalikus arutelus käsitletakse juurdepääsu andmetele erandliku ja möödapääsmatu meetmena raskete kuritegude ja julgeolekuohtude puhuks. Tegelikult on valdav osa päringuid seotud maksukontrolli, toetuste kontrolli, liiklusjärelvalve ja muude igapäevaste haldusülesannetega. Enamik neist on seaduslikud ja vajalikud, kuid kaitsemeetmeid ei saa kujundada eeldusel, et andmete saamiseks tehakse päringuid harva.

Teiseks on põhjendamise nõue madal. Suure osa päringute puhul piisab viitest asutuse pädevusele ja menetluse olemasolule. Riigikohtu sõnastatud nõue, et seos menetlusega peab olema äratuntav või selgitatud, kehtib küll formaalselt, kuid seda rakendatakse üksnes vaidluse korral. Puudub mehhanism, mis kohustaks päringu tegijat põhjendust enne päringut kirja panema, ning praegu küsitakse põhjendust tagantjärele, kui üldse.

Kolmandaks on tundlike andmete erikord ebaühtlane. Iga tundlikku andmekategooriat tuleb hinnata eraldi. Pangasaladus on kaitstud krediitiasutuste seadusega, kuid erandite loetelu on pikk ja hõlmab maksuhaldurit, õiguskaitseasutusi, Rahapesu Andmebürood ja järelevalveasutusi. Erikord on formaalselt olemas, kuid see suunab juurdepääsu pigem kindlatesse kanalitesse, kui seda piirab. Riigikohus on küll selgitanud, et maksuhalduri päring pangale pangakonto väljavõtte saamiseks peab olema põhjendatud ning andmetöötlus peab vastama isikuandmete kaitse üldmääruse nõuetele, mis on kogumise eesmärgist erineva töötlemise puhul ranged (RKHKo 3-21-1530, p 67–68), kuid praktikas kontrollitakse nende nõuete täitmist eelkõige tagantjärele ja vaidluse korral. Sama kehtib maksusaladuse kohta, sest maksukorralduse seadus kehtestab küll saladuse hoidmise kohustuse, kuid lubab andmeid edastada pikale loetelule asutustest.

Terviseandmete puhul on erikord näiliselt sisulisem, sest andmetele juurdepääs logitakse ja isik saab teatud ulatuses näha, kes tema andmeid vaatas. 2026. aastal avalikuks tulnud TEHIK-uga seotud juhtumid näitavad siiski, et see nähtavus ei ole täielik ning andmete väljastaja ei pruugi õiguskaitseasutuste päringute põhjendatust sisuliselt kontrollida. TTKS § 59³ lg 7 lai sõnastus ja Riigikohtu seisukoht, et KrMS-i üldine nõudeõigus ei ole patsiendisaladuse väljanõudmiseks iseseisev alus, näitavad, et eriliiki isikuandmete puhul ei piisa tehnilisest logimisest. Õiguslik alus ja põhjendus peavad olema kontrollitavad enne andmete väljastamist.

Kõige vastuolulisem on sideandmete erikord. Kehtiv ESS § 111¹ kohustab sideettevõtjat üldjuhul säilitama ühe aasta jooksul väga laia hulka liiklus- ja asukohaandmeid kõigi kasutajate ja seadmete kohta. Riigikohus on selgitanud, et ESS § 111¹ äärmiselt avara sõnastuse tõttu tuleb selle sättega sideettevõtjale pandud kohustusi käsitada liiklus- ja asukohaandmete üldise ja vahet tegemata säilitamisena, ning on lugenud direktiivi 2002/58/EÜ art 15 lõikega 1 vastuolus olevaks ESS § 111¹ lg-s 2 telefoni- ja mobiiltelefoniteenuse ning telefonivõrgu ja mobiiltelefonivõrgu teenuse osutajatele ette nähtud säilitamiskorralduse (ESS § 111¹ ja § 112; JAS § 27 lg 3; vrd RKKKo 1–24-4898/33, p 22). Selle tulemusel on tekkinud õiguslikult ebaselge olukord, kus sideandmete kasutamine kriminaalmenetluses on rangelt piiratud, kuid üldine säilitamiskohustus on seaduses alles ja julgeolekuasutuste juurdepääs andmetele on säilinud. Sideandmeid kasutatakse kriminaalmenetlustes seejuures ka lihtsalt info saamiseks, kuigi tõendina neid enam ilmselge perspektiivituse tõttu ei esitata.

Neljandaks probleemiks on see, et juurdepääsuõiguse omajat usaldatakse täielikult ja paistab levivat mõtteviisi, et andmete väärkasutamine on teatud asutuste puhul välistatud. Kõige üldisem järeldus siit on, et Eesti süsteem tugineb usaldusele asutuse vastu, mitte kontrollile asutuse üle. Kui asutusele on antud juurdepääsuõigus, eeldatakse, et ta kasutab seda õiguspäraselt. Sisuline eelkontroll toimub peamiselt seal, kus seadus nõuab kohtu luba, ehk väga väikese osa päringute puhul. Päringu saaja kontrollikohustus on ebaühtlane. Maksukohustuslaste registri põhimäärus nõuab, et Maksu- ja Tolliamet veenduks mõistlike pingutustega andmesaaja õiguses andmeid saada, kuid

pangasaladuse regulatsioonis on täitmisregistri kaudu esitatud päringu puhul krediitiasutuse kontrollikohustus sisuliselt välistatud. Järelkontroll toimub logide kaudu, kuid logisid vaadatakse valdavalt alles kaebuse korral. Ennetav, pisteline ja sõltumatu kontroll, mille käigus kontrollitaks juhuvalimi alusel päringute põhjendatust, praktiliselt puudub.

Ettepanekud

- **Kehtestada tundlike andmete (terviseandmed, sideandmed, pangasaladus, maksusaladus, õiguskaitse operatiivandmed ja biomeetria) puhul seaduse tasandil ühtne päringu põhjendamise ja logimise standard.** Päringu tegija peab enne päringut fikseerima menetluse, õigusliku aluse, eesmärgi, põhjenduse ja vajaliku andmekoosseisu. Põhjendus logitakse koos päringuga.
- **Kehtestada päringu saajale kontrollikohustus.** Andmekogu vastutav töötleja või andmete valdaja peab mõistlike pingutustega veenduma, et päringu tegijal on õigus andmeid saada ja et päringus on piisav põhjendus. Põhjendatud kahtluse või õigusliku aluse puudumise korral ei tohi andmeid väljastada. Selline standard on juba maksukohustuslaste registri põhimääruses olemas ning see tuleks laiendada ka pangasaladusele, terviseandmetele ja õiguskaitse andmekogudele.
- **Luu sõltumatu eel- või pistekontrolli mehhanism.** Kus kohtu eelluba ei ole proportsionaalne, peab sõltumatul organil, näiteks Andmekaitse Inspeksioonil või muul eraldi loodud üksusel, olema õigus ja kohustus teha päringute juhuvalimi sisulisi järelkontrolle ning avaldada tulemused koondkujul.
- **Laiendada inimese õigust teada tema kohta tehtud päringutest.** Tervise infosüsteemi andmejälgija mudel tuleb laiendada teistele andmekogudele, nähes ette põhjendatud ja ajaliselt piiratud erandid käimasolevate menetluste kaitseks. Erand peab lõppema koos menetluse või salastamisvajaduse lõppemisega, mitte jääma määramata ajaks kestvaks pimedaks alaks.

Andmete kasutamine: vabatahtlikkusest riskipõhise järelevalveni ja edasi menetluseni

Eelmises peatükis käsitleti seda, kes andmetele ligi pääseb. Käesolevas peatükis analüüsitakse andmete liikumist, mille käigus ühel eesmärgil kogutud andmed jõuavad riskipõhisesse andmeanalüüsi, sealt järelevalvesse ja lõpuks menetlusse, mis võib lõppeda karistusega. Ükski etapp ei pruugi eraldi võetuna olla õigusvastane, kuid tervikuna muudab just see liikumine andmete kogumise jälgimiseks.

Müüt „nõusolekust“

Avalikus arutelus kasutatakse sageli sõna „nõusolek“ nii, nagu oleks see andmetöötluse peamine alus. Riigi andmetöötlemises see peaaegu kunagi nii ei ole. Eristada tuleb kolme kogumisviisi, mis näevad inimese jaoks sarnased välja, kuid on õiguslikult täiesti erinevad.

Esimene kogumisviis on seaduse alusel kohustuslik kogumine. Rahvastiku-registri kanded, maksudeklaratsioonid, töötamise registri kanded, piiri-ületuse registreerimine ja tervise infosüsteemi saadetavad epikriisid tekivad kõik seaduse alusel, mistõttu ei saa nõusolek siin olla õiguslik alus. Kui seadus kohustab andmeid töötleva, oleks nõusoleku küsimine eksitav, sest keeldumine ei muudaks midagi. Õiguslikult on see korrektne, kuid küsimus on selles, kas inimene saab aru, et tal valikut ei ole.

Teine kogumisviis on vaikimisi nõusolekuga ehk opt-out mudel. Mitmes süsteemis on andmete jagamine vaikimisi sisse lülitatud ja inimene võib selle välja lülitada; tüüpnaide on tervise infosüsteemi andmete sulgemine. Formaalselt on valik olemas, kuid praktikas kasutavad seda vähesed, sest nad ei tea sellest, ei oska seda leida või kardavad, et sulgemine kahjustab ravi. Seega suunab vaikimisi seade käitumist tugevalt.

Kolmas kogumisviis on teenuse saamise tingimusena antav nõusolek. Selleks et saada toetust, hüvitist, luba või teenust, tuleb anda nõusolek andmete töötlemiseks või esitada andmeid, mida ilma taotluseta ei esitataks. Õiguslikult on küsitav, kas selline nõusolek on GDPR-i tähenduses vabatahtlik, kui alternatiiviks on teenusest ilmajäämine.

Neid kolme kogumisviisi ei tohi segi ajada. Kui seadus kohustab andmeid töötleva, ei saa nõusolek olla õiguslik alus ning hinnata tuleb seaduse enda proportsionaalsust. Otsustav on, kas inimesel oli sisuline valik, ja enamikus eespool kirjeldatud olukordades seda ei olnud.

Riskipõhine järelevalve

Riskipõhine järelevalve on viimase kümnendi haldusreformi keskne idee ja see on iseenesest mõistlik. Järelevalveasutuste ressurss on piiratud; selle suunamine sinna, kus rikkumise tõenäosus on suurem, on ratsionaalsem kui juhuslik või kõikehõlmav kontroll. Maksu- ja Tolliamet kasutab riskianalüüsi maksukontrolli suunamiseks. Rahapesu Andmebüroo töötab definitsiooni järgi riskipõhiselt. Sotsiaalkindlustusamet ja Töötukassa kasutavad andmeanalüüsi hüvitiste väärkasutuse tuvastamiseks.

Riskianalüüs iseenesest ei ole probleem. Probleem tekib kolmel tingimusel, mis on Eestis sageli korraga täidetud. Esimene tingimus on, et inimene ei tea, milliste andmete alusel ta riskikategooriasse paigutati. Riskimudelite sisu on tavaliselt asutusesisene teave ning avaldamata jätmist põhjendatakse sellega, et muidu saaks mudelit vältida. See on osaliselt õige, kuid tulemuseks on olukord, kus inimene ei saa tõhusalt vaidlustada liigitust, mille sisu talle ei avaldata.

Teine tingimus on eri andmekogude andmete ristkasutamine. Riskimudel, mis kombineerib maksuandmeid, töötamise registrit, kinnistusraamatut, liiklusregistrit ja sotsiaaltoetuste andmeid, teeb täpselt seda, mida 1. peatükk kirjeldas koosmõjuna, ja teeb seda süstemaatiliselt. Iga andmeallikas eraldi võib töötada õiguspäraselt, kuid mudelit kui tervikut ei ole kunagi eraldi hinnatud ega reguleeritud.

Kolmas tingimus on, et riskiskoor toob kaasa intensiivse kontrolli või ebasoodsa otsuse. Siin on vahe oluline. Kui skoor üksnes suunab ametniku tähelepanu ja edasise kontrolli teeb ning põhjendab inimene, on riive mõõdukas. Kui otsuse sisuline alus on aga skoor ise, näiteks toetuse peatamisel või kontrolli algatamisel, mida ilma skoorita poleks tehtud, on tegemist automatiseeritud töötlusel põhineva otsusega, millele GDPR seab eraldi nõuded. Inimene peab saama teada loogika põhielemendid, töötlemine peab piirduma vajalikuga ning tal peab olema õigus otsus vaidlustada ja nõuda inimese sekkumist (GDPR art 5, 13–15 ja 22; õiguskaitsevaldkonnas direktiiv (EL) 2016/680 art 11).

Siinkohal tuleb meenutada, et Andmekaitse Inspeksioon kritiseeris juba 2015. aastal maksuhalduri kavatsust saada riskihindamiseks juurdepääs kõikidele andmekogudele. Kümne aasta jooksul on andmeanalüüsi tehniline võimekus mitmekordistunud, kuid selle õiguslik raamistik on jäänud sisuliselt samaks. Eesti õigus ei käsitle riskianalüüsi iseseisva andmetöötamise liigina, millel oleks oma eesmärk, proportsionaalsuse hindamine ja järelevalve.

Massiline andmetöötlus ja ohtu ennetav haldusmenetlus

Eespool nimetatud POLIS-e põhimäärusest nähtub, et avaliku korra ja siseturvalisuse tagamiseks töötleb PPA väga suurt andmemahutu mitte ainult ohuolukordade lahendamiseks, vaid ka tulevaste ohtude ennetamiseks. POLIS võimaldab seega grupeerida inimesi, ettevõtteid, aadresse, sõidukeid ja muid andmepunkte tõenäosuse järgi, et neist võib oht tekkida, mitte üksnes

olemasoleva ohu alusel. Sellise andmetöötluse puhul on suur oht, et see muutub ebaproportsionaalseks ja sisuliselt varjatud jälgimiseks.

Põhimääruses on sätestatud kaks väga laialivalguvat andmestikku, mille puhul on raske aru saada, millistel kriteeriumidel isik või objekt neisse satub.

Esiteks kogub POLIS andmeid ühiste infoobjektide andmestikku, mis hõlmab kaheksat liiki subjekte või objekte – isikut, ettevõtet, aadressi, sõidukit, sidevahendit, eset, dokumenti ja relva. Nende kohta kogutavate andmete maht on aga lahtine, sest iga liigi juures on märke täiendav teave, mille alla mahub ükskõik missugune detail kellegi või millegi kohta.

Teiseks peab POLIS ennetava tegevuse andmestikku, kuhu märgitakse juhtumite, isikute, ettevõtete ja aadresside kohta mitmesugust teavet. Teavet kogutakse muu hulgas nende isikute, juhtumite ja aadresside kohta, mis tõenäoliselt võivad olla seotud õiguserikkumistega. Põhimääruse järgi koosneb ennetava tegevuse andmestik automaatse liiklusjärelvalve süsteemi ja numbrituvastuskaamerate teabest, kuid ka piirkondlikest infoteadetest. Viimast mõistet pole defineeritud, mistõttu võib ka see teave olla ükskõik mis.

Seega töötleb PPA POLIS-e kaudu määratlemata mahus andmeid määratlemata isikute ringi kohta, kes kirjeldamata põhjusel võivad olla seotud õigusrikkumistega. Seejuures tuleb rõhutada, et POLIS ei ole suunatud üksnes süütegudele, vaid õigusrikkumistele, mis hõlmavad mis tahes avalik-õigusliku normi rikkumist alates parkimisnõuetest kuni haljastus- või mürareegliteni. Eeltoodust tulenevalt leiavad autorid, et POLIS vastab sisuliselt kõigile sissejuhatuses kirjeldatud jälgimisühiskonna tunnustele.

Järelevalvest karistuseni

Andmete teekonna kolmas etapp on üleminek järelevalvest menetlusse, mis toimub kolmes suunas korraga. Esimene suund on haldusakt, mille puhul tehakse riskianalüüsi või järelevalve tulemusena otsus, näiteks maksuotsus, toetuse tagasinõue, loa peatamine või ettekirjutus. Sellist otsust saab vaidlustada ja haldusmenetluse seaduse järgi peavad põhjendused olema kirjas. Praktikas jääb riskianalüüsi roll põhjendustes aga sageli nähtamatuks, sest otsus kirjeldab tuvastatud asjaolusid, kuid ei ütle, miks just see inimene kontrolli alla sattus.

Teine suund on väärteomenetlus, mida käsitleti 2. peatükis ja milles sama asutus, kes kogus teabe järelevalves, menetleb sageli ka väärtegu. Kolmas suund on kriminaalmenetlus, kus järelevalve käigus kogutud materjal võib anda aluse kuriteoteateks või saada tõendiks.

Just siin ilmneb Eesti õiguskorra üks teravamaid probleeme kõiges selles, mis puudutab enese mittesüüstamise privileegi. Põhiseaduse § 22 lg 3 kohaselt ei tohi kedagi sundida tunnistama iseenda vastu. Sama põhimõte sisaldub Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklist 6 tulenevas õiguses

õiglasele kohtumenetlusele. Kriminaalmenetluses on olukord selge, sest kahtlustataval on õigus vaikida ning vaikimisest ei tohi teha tema kahjuks järeldusi.

Haldusjärelvalves on olukord vastupidine. Maksukorralduse seadus, korra-kaitseseadus ja valdkondlikud järelvalveseadused panevad isikule kaasaaitamiskohustuse, mille kohaselt peab ta esitama dokumente, selgitusi ja andmeid. Keeldumise korral võib tema suhtes kohaldada sunniraha või teda väärteokorras karistada. Seega on isik järelvalvemenetluses kohustatud teavet andma.

Vastuolud tekivad siis, kui järelvalves kohustuslikus korras antud teave liigub edasi süüteomenetlusesse. Formaalselt ei ole inimest sunnitud tunnistama iseenda vastu süüteomenetluses, sest teabe andis ta haldusmenetluses. Sisuliselt on tulemus aga sama, sest riik sai sunni abil teabe, mida süüteomenetluses ei oleks tohtinud sunniga saada. Euroopa Inimõiguste Kohtu praktika on selles küsimuses pikk ja nüansirikas, kuid selle põhisuund on, et privileeg ei kao üksnes seetõttu, et teave koguti formaalselt teises menetluses.

Riigikohus on selle piiri nüüdseks tõmmanud, leides, et haldusmenetluses karistuse ähvardusel saadud tõendid on kriminaalmenetluses lubamatud (RKKKo 1-22-3234, p 22–23). Tegemist on olulise tagatisega, kuid sisuliselt on see kriminaalmenetluslik õiguskaitsevahend, mis rakendub tagantjärele tõendi lubatavuse hindamisel. Haldusorganite praktikat see iseenesest ei muuda ja seadust ei paranda, sest järelvalves nõutakse sunni ähvardusel endiselt teavet, mida võidakse hiljem süüteomenetluses kasutada, ning privileegi rikkumine tuvastatakse alles siis, kui isik oskab ja suudab seda kriminaalmenetluses vaidlustada. Seega ei saa järelvalvemenetluse subjekt ka praegu kindel olla, et tema koostöö ei pöördu tema vastu.

Andmete kasutamine haldusmenetluslikuks ennetamiseks

Julgeolekuasutuste puhul ei piirdu andmete kasutamine süüdistuse esitamisega ega isegi kriminaalmenetluse alustamisega. Kaitsepolitsei ameti endine juhtivtöötaja Eerik Heldna on teadusajakirjas *Juridica* selgitanud, et teabehanke käigus kogutakse infot julgeolekut ohustavate kuritegude kohta eelkõige selleks, et neid haldusmenetluses ennetada. See seisneb pädevate asutuste informeerimises, et need saaksid võtta ennetavaid meetmeid muu hulgas regulatsiooni, korralduse või personaliotsuste valdkonnas. Sama käsitluse järgi on teabehankelist infot Eestis kriminaalmenetluses tõendiks vormistatud väga üksikutel kordadel, kuid haldusmenetluslike meetoditega on ennetatud kordades rohkem kuritegusid; korruptsiooni valdkonnas jääb KAPO uuritavate kriminaalasjade arv aastas alla kümne, kuid olulisemaks peetakse kogutud teabe alusel ennetatud ohtlike korruptsiooniilmingute hulka.* Kui teabehanke

* E. Heldna. Julgeolekuasutuste kogutud informatsiooni kasutamine kriminaalmenetluses ja jagamine uurimisasutustega. – *Juridica* X/2016, lk 718–726.

peamine väljund on haldusmenetluslik ennetamine, jääb suurem osa kogutud teabe kasutamisest piiramata kriminaalmenetluses kasutada olevate tõrje-õiguste poolt.

Riigi vaates võib see olla vähem koormav kui kriminaalmenetlus. Eesmärk on sekkuda enne kuriteo ettevalmistus- või katsestaadiumisse jõudmist ja valida abinõu, mis piirab põhiõigusi võimalikult vähe. Isiku vaates võib mõju siiski olla sama tugev kui karistus. Kui julgeolekuasutus edastab teisele asutusele või tööandjale hinnangu, et isikuga seondub julgeoleku- või korrupsioonirisk, võib tagajärjeks olla loa andmata jätmine, teenistussuhte lõpetamine, tööülesannete muutmine või muu eluliselt oluline otsus. Sellise otsuse võib formaalselt teha teine asutus või tööandja, kuid sisulise impulsi annab julgeolekuasutuse hinnang, mille aluseks olevat teavet otsustaja ega isik ise sageli kontrollida ei saa. Seda võimu saab julgeolekuasutuste prestiiži abil kuritarvitada ja tekitada kannatusi inimestele, kes pole toime pannud ühtegi õigusvastast tegu. See oht ei ole abstraktne ning taolisi juhtumeid leidub ka autorite enda praktikast.

See loob ka erilise vaidlustatavuse probleemi. Julgeolekuasutus ei tee isiku kohta tingimata haldusakti, mida saaks vaidlustada. Teabe saaja teeb oma otsuse ise, kuid tugineb hinnangule, mille lähteandmed on salastatud ja mille sisustamine kuulub julgeolekuasutuse infomonopoli. Nii võib tekkida olukord, kus sisulise hinnangu andja ei vastuta otsuse eest, asetsedes väljaspool kohtulikku kontrolli, ja formaalne otsustaja ei saa hinnangut sisuliselt kontrollida ning ei vastuta, kuna võib usaldada julgeolekuasutusi. Kui isik ei tea, et otsuse tegelik põhjus oli julgeolekuasutuse edastatud teave, ei saa ta kasutada ka tava-päraseid kaitsevahendeid: õigust olla ära kuulatud, õigust tutvuda tõenditega ja õigust otsust kohtus vaidlustada.

Haldusmenetluslik ennetamine ei ole iseenesest õigusvastane. Vastupidi, osa julgeolekuohtudest tulebki tõrjuda enne, kui need muutuvad karistatavaks teoks. Probleem tekib siis, kui sellise ennetuse tulemusena sekkutakse sügavalt inimese tööellu, liikumisvabadusse või majandustegevusse, ilma et seadus sätestaks teabe edastamise aluse, edastamise ulatuse, faktide ja hinnangute eristamise kohustuse, isiku teavitamise korra ning võimaluse sõltumatuks kontrolliks. Kirjeldatud probleem on Eestis akuutne. Kui kriminaalmenetluses tuleb isikut kogutud teabega üldjuhul tutvustada, siis haldusmenetlusliku ennetuse puhul võib sama intensiivselt kogutud teave mõjutada inimese elu ilma ühegi nähtava menetluseta.

Analüüs: eesmärk, mis on pidevas muutumises

Tuleb tõdeda, et andmed kogutakse ühel eesmärgil, kuid need jõuavad teise eesmärgini, ilma et eesmärgi muutmist oleks kordagi eraldi otsustatud või põhjendatud.

Andmete liikumist tuleb hinnata tervikuna. Tööandja kannab töösuhte töötamise registrisse, sest seadus kohustab teda seda tegema, ning registreerimise eesmärk on töösuhete arvestus ja maksude kogumine. Seejärel jõuavad andmed maksuhalduri riskimudelisse, kus nende eesmärk on juba kontrolli suunamine. Samal ajal võivad need olla jõudnud ka POLIS-esse, kus nii töötaja, tööandja kui ka nendega seotud aadressid ja sõidukid võidakse märkida tõenäoliselt õiguserikkumisega seotuks. Kui mudel tõstab isiku esile, alustatakse järelevalvemenetlust, milles isik on kohustatud selgitusi andma, ning need selgitused ja kogutud materjal võivad olla aluseks väärteo- või kriminaalmenetlusele, mille eesmärk on karistamine. Ühelgi selle ahela etapil ei hinnata, kas maksuarvestuse eesmärgil kogutud andmete kasutamine karistusmenetluses on proportsionaalne.

GDPR-i eesmärgipiirangu põhimõtte peaks selle ahela katkestama või vähemalt sellele kontrollpunkte seadma. Riigikohus on rõhutanud, et kogumise eesmärgist erinev andmetöötlus peab vastama GDPR-i rangetele nõuetele ning et näiteks maksuhalduri päring pangale kontoväljavõtte saamiseks peab olema põhjendatud (RKKHo 3-21-1530, p 67–68). Halduspraktikas see põhimõtte siiski andmete liikumise ahelat ei katkesta, sest iga üleminek on eraldi seadusega lubatud ja seega formaalselt õiguspärane ning nõuete täitmist kontrollitakse alles vaidluse korral. Eesmärgipiirangust on praktikas saanud nimekiri eranditest.

Teine tähelepanek puudutab ajahetke. Klassikaliselt algab menetlus siis, kui riigil on alus kahtlustada. Andmepõhises järelevalves algab tähelepanu aga palju varem, riskimudelil, mis töötab pidevalt ja mille suhtes inimene pole keegi, keda teavitada. Inimene saab sellest teada alles siis, kui tähelepanust on saanud menetlus, ning selleks ajaks teab riik temast rohkem, kui tema teab sellest, mida riik teab.

Ettepanekud

- **Algatada viivitamata POLIS-es toimuva andmetöötluse terviklik järelkontroll ning täiendada POLIS-e põhimäärust.**
- **Piirata eesmärgi muutmist.** Seaduses tuleb sätestada, et andmete kasutamiseks muul kui kogumise eesmärgil on vaja eraldi õiguslikku alust, milles on nimetatud konkreetne uus eesmärk, ning et üldine viide asutuse pädevusele ei ole piisav. Eelkõige puudutab see järelevalvetoimingute käigus kogutud andmete kasutamist karistusmenetluses.

- **Teavitada inimest riskianalüüsi põhjal alustatud kontrollist.** Kui kontrolli algatamise ajend oli riskianalüüs, peaks inimene vähemalt üldisel kujul teadma, millised andmekategooriad mudelisse sisendiks olid. Käimasoleva menetluse kaitseks võib teavitamist edasi lükata, kuid mitte ära jätta.
- **Piirata järelevalves kohustuslikus korras antud teabe kasutamist süüteomenetluses.** Seadusandja peaks Riigikohtu seisukoha, et haldusmenetluses karistuse ähvardusel saadud tõendid on kriminaalmenetluses lubamatud, seaduses sõnaselgelt sätestama ning panema haldusorganitele kohustuse selgitada isikule enne sunni abil teabe nõudmist, kas ja kuidas võidakse teavet karistusmenetluses kasutada, selle asemel et jätta rikkumise heastamine kriminaalmenetluses tagantjärele lahendada.
- **Kehtestada riskimudelitele eraldi läbipaistvus- ja auditeerimisnõue.** Mudeli eesmärk, kasutatavad andmekategooriad, valideerimine ja mõjuhindang peavad olema dokumenteeritud ning sõltumatu järelevalveasutusele kättesaadavad ka siis, kui mudeli täpsed parameetrid ei ole avalikud.

Salajase jälgimise ulatus ja kontroll

Seni käsitletud andmetöötuse eesmärk pole olnud selle inimese eest varjamine. Käesolev peatükk käsitleb andmetöötust, mis on korraldatud nii, et inimene ei tea sellest midagi ja sageli ei saagi teada. Siin on riive kõige intensiivsem ja kontroll kõige nõrgem, mis ei ole juhus, sest just varjatuse tõttu puuduvad korrigeerivad abinõud, mis mujal toimivad.

Ametlik statistika

Esimene asi, mida salajase jälgimise ulatuse hindamiseks on vaja, on statistika. Ilma selleta on arutelu hinnangute vahetamine. Käesoleva raporti koostamise käigus kasutati Siseministeeriumi andmetel põhinevat, avalikult sotsiaalmeedias avaldatud ülevaadet õiguskaitseasutuste jälitustegevuse trendidest aastatel 2017–2025.* Selle järgi langes jälitustoiminguteks antud lubade arv 2017. aasta 2889-lt 2025. aastaks 771-ni. Isikute arv, kelle suhtes jälitusluba anti, langes samal perioodil 2178-lt 472-ni. Lisaks neile riivati 2025. aastal jälitustoiminguga veel 369 isikut, kelle suhtes jälitusluba ei antud. See viimane arv on oluline, sest näitab, et salajane jälgimine puudutab 2025. aasta andmetel tunduvalt rohkem inimesi kui üksnes neid, kelle suhtes luba formaalselt anti.

Sama ülevaate kohaselt koostati 2025. aastal jälitustoimingust teavitamiseks 2373 teadet. Teavitamine lükati kohtu loal edasi 104 isiku puhul ning prokuratuuri loal jäeti teavitamata 35 isikut. Kuna andmed pärinevad avalikust sotsiaalmeediapostitusest, mitte ametlikust aastaaruandest, tuleb neid käsitada üksnes indikatiivsena. Siiski nähtub neist, et isegi kriminaalmenetluse rangema korra puhul ei ole teavitamine alati vahetu ega täielik.

Samas on oluline arvestada statistika piiridega. Need arvud puudutavad kriminaalmenetluse jälitustoiminguid. Need ei hõlma JAS-i alusel tehtavat teabehanget, julgeolekuasutuse juhi loal tehtavaid toiminguid ega haldusmenetluslikku ennetamist, mille kohta võrreldavat avalikku statistikat ei avaldata ja seetõttu ei ole avalikkusel sellest võimalik mitte midagi teada. Seega ei saa kriminaalmenetluse lubade arvu langusest järeldada, et salajase teabe kogumise kogumaht või riive tegelik ulatus oleks samas ulatuses vähenenud.

* Igor Taro Facebooki postitus.

Teavitamine

Kriminaalmenetluses on teavitamise kord selge. Jälitustoimingu aluseks olnud loa tähtaja möödumisel tuleb isikut üldjuhul viivitamata teavitada ning tema soovil tuleb talle kogutud teavet tutvustada (KrMS § 126¹³ ja § 126¹⁴). Teavitamise täpsem kord on sätestatud määrusega, mille kohaselt teavitab jälitusasutus viivitamata isikut, kelle suhtes jälitustoiming tehti, samuti isikut, kelle perekonna- või eraelu puutumatust jälitustoiminguga oluliselt riivati ja kes on menetluse käigus tuvastatud. Teates tuleb märkida jälitustoimingu tegemise aeg ja liik, tutvustava asutuse kontaktandmed ning tähtaeg, mille jooksul on võimalik materjalidega tutvuda.

Teavitamisel on kaks eesmärki. Esiteks võimaldab see inimesel oma õigusi kaitsta, sest kui ta riivist ei tea, on kaebeõigus illusoorne ja sisutu. Teiseks distsiplineerib see jälitusasutust, kuna toiming, millest tuleb hiljem teavitada, tehakse hoolikamalt kui toiming, mis jääb igaveseks varjatuks.

Teavitamiste ja tehtud toimingute arvu võrdlus oleks kõnekas näitaja, kuid selleks peaksid mõlemad arvud olema usaldusväärselt kättesaadavad ning raportis kasutatud allikad sellist võrdlust ei võimalda. Autorite hinnangul viitab teavitamata jätmise erandite lai sõnastus sellele, et erandit ei kohaldata praktikas erandlikult. Tegemist on siiski hinnanguga, mitte tuvastatud faktiga, ning selle kontrollimiseks tuleb ametlikud andmed avaldada.

Riigikohtu seisukohad teavitamise puudujääkidest

Riigikohus on teavitamise küsimust käsitlenud põhimõttelisel tasandil. 20. märtsi 2014. aasta otsusega tunnistas põhiseaduslikkuse järelevalve kolleegium põhiseadusvastaseks ja kehtetuks kriminaalmenetluse seadustiku rakendamise seaduse § 25¹ lõike 2, kuna see ei näinud ette tõhusat ja sõltumatut kontrolli selle üle, kas inimese teavitamata jätmine tema õigusi puudutavast jälitustoimingust on põhjendatud (RKPJKo 3-4-1-42-13).

Otsuse põhjendused on raporti seisukohalt üliolulised. Riigikohus rõhutas, et jälitustoimingutega kogub riik salaja isikuandmeid, mida ta hiljem kasutab ja säilitab, ning et põhiõiguste riive võib kesta aastaid pärast toimingu lõppemist, kuna riive kestab seni, kuni andmeid säilitatakse ja kasutatakse. Seetõttu ei piisa üksnes toimingu loa kontrollist, vaid kontrollida tuleb ka andmete edasist kasutamist ning seda, kas isikule jäetakse teatamata asjaolud, mida ta peaks teadma.

Sama loogikat on Riigikohus järginud ka kaitseväeluure volituste kontekstis. Riigikohus leidis, et Kaitsevägele antud varjatud meetmed võivad menetluslike tagatiste olemasolu korral olla põhiseaduspäraseid, kuid põhiseadusega on vastuolus tõhusa kontrolli puudumine selle üle, kas isik jäetakse varjatud jälgimisest teavitamata. Seadus peab tagama tõhusad menetluslikud tagatised, mis välistavad meelevaldse teavitamata jätmise (RKPJKo 5-19-38/15).

Nendest kahest lahendist tuleneb selge põhiseaduslik standard, mille kohaselt on varjatud jälgimine lubatav, kuid teavitamata jätmine peab olema sõltumatult kontrollitav. Standard on küll sõnastatud kriminaalmenetluse ja kaitsevääluure kontekstis, kuid järgmises alapeatükis käsitletav teabehanke režiim sellele praegusel kujul ei vasta.

Teabehange ja jälitustoimingud: samad tegevused, erinev kaitse

Kriminaalmenetluse seadustikus on ammendavalt loetletud seitse jälitustoimingut, milleks on varjatud jälgimine, võrdlusmaterjali varjatud kogumine ja esmauuringute tegemine, asja varjatud läbivaatus ja asendamine, postisaadetise varjatud läbivaatus, teabe salajane pealtkuulamine ja -vaatamine, kuriteo matkimine ning politseiagendi kasutamine (KrMS §-d 126⁵–126⁹). Julgeolekuasutuste seaduse alusel tehtavate teabehanketoimingute raames on lubatud piirata sõnumisaladust ning kodu, perekonna- ja eraelu puutumatust ning kaasata isik salajasele koostööle. Nende piirangute teostamiseks kasutatavad meetodid kattuvad sisuliselt sõna-sõnalt kriminaalmenetluse jälitustoimingutega (JAS §-d 24¹, 25, 26 ja 28 võrdluses KrMS §-dega 126⁵–126⁹).

See ei ole üksnes autorite hinnang. Riigikohtu põhiseaduslikkuse järelevalve kolleegium on toimingute samasusele korduvalt osutanud ning kasutanud julgeolekuasutuste seaduses sätestatu kohta koguni väljendit „kriminaalmenetluse väline jälitustegevus“ (RKPJKo 3-4-1-42-13, p 36; RKPJKo 5-19-38/15, p 74). Kui toimingud on sisuliselt samad ja riive intensiivsus inimese põhiõigustele on sama, peaks ka kaitse olema võrreldav. Võimalik vastuväide on, et ohutõrjel ja süüteomenetlusel on erinevad eesmärgid. Riigikohtu kasutatud väljend näitab aga, et kohus käsitleb neid toiminguid sisult samana sõltumata seadusest, mille alusel neid tehakse. Inimese jaoks on riive sama, olgu eesmärk ohu ennetamine või kuriteo tõendamine. Eesmärkide erinevus võib õigustada erinevat korraldust, näiteks teistsugust toimingute ringi või teavitamise ajastust, kuid madalamat kaitsetaset see ei õigusta. Tegelikuses erineb kaitse viies olulises punktis.

Esiteks tohib kriminaalmenetluses jälitustoiminguid teha eranditult prokuratuuri või eeluurimiskohtuniku loal (KrMS § 126⁴). Teabehanke puhul on halduskohtu luba vajalik üksnes osa toimingute tegemiseks ning ülejäänud toimingute puhul annab loa julgeolekuasutuse juht või tema volitatud ametnik, kusjuures loa andmise kord on riigisaladus (JAS § 27 lg-d 1 ja 3). Nagu eespool selgitatud, erineb ka kohtuloo standard, sest teabehankeloo aluseks on tõenäosusel põhinev prognoosotsus, jälitusloa aluseks aga konkreetsetel asjaoludel ja tõenditel põhinev kuriteokahtlus.

Teiseks on teabehanketoimingute puhul teavitamiskohustus olemas üksnes teatud juhtudel ja alles pärast teabe salastatuse kustumist (JAS §-d 29 ja 21¹). Teabehankega kogutud teabe võib salastada kuni 50 aastaks, kuid pool sajandit hiljem saabuv teavitus ei taga kaebeõigust ega distsiplineeri asutust.

Kolmandaks on kriminaalmenetluses inimesel õigus soovi korral jälitustoimikuga tutvuda. Teabehanke puhul tutvustamiskohustust ei ole üldse. Julgeolekuasutuste ülesannete iseloomu arvestades ei ole tutvustamine alati põhjendatud, kuid tutvustamise regulatsiooni täielik puudumine tähendab, et ka siis, kui tutvustamine oleks võimalik ilma ühtegi kaitstavat huvi kahjustamata, ei ole selleks mingit menetluslikku teed.

Neljandaks on kriminaalmenetluses jälitustoimingu protokollimine kohustuslik ja jälitustoimiku pidamise kord on kehtestatud Vabariigi Valitsuse määrusega (KrMS § 126¹⁰ ning jälitustoimiku pidamise ja säilitamise korda reguleeriv Vabariigi Valitsuse määrus). Teabehanke puhul sätestab seadus kohustuse säilitada teavet teabehanke toimikutes ja toimiku avamise kriteeriumid on kehtestatud siseministri määrusega, kuid konkreetne regulatsioon toimingu kokkuvõtete vormi ja toimikusse kandmise kohta puudub. Kuna ka see kord võib olla riigisaladus, ei ole väljastpoolt võimalik hinnata, kas dokumenteerimise nõuded on jälitustoimingutega võrreldavad.

Viiendaks on Euroopa Kohus ja Riigikohus leidnud, et elektroonilise side seaduses sätestatud andmete säilitamise regulatsioon on osaliselt vastuolus Euroopa Liidu õigusega ning sellel alusel säilitatud sideandmete kasutamine kriminaalmenetluses on välistatud (EKo C-746/18 Prokuratuur; RKKKo 18.06.2021, 1-16-6179). Nagu eespool selgitatud, ei ole ESS § 111¹ tervikuna kehtetuks tunnistatud. Julgeolekuasutus võib aga samu andmeid sideettevõtjalt teabehanke korras välja nõuda julgeolekuasutuse juhi loa alusel ning sideettevõtja on kohustatud need väljastama. Selle tulemusel jääb Euroopa Kohtu praktikaga vastuolus kogutud andmestik kättesaadavaks just sellele asutusele, kelle tegevuse üle teostatakse kõige vähem kontrolli.

Kontrollimehhanismid

Salajase jälgimise kontroll peaks Eestis toimuma neljal tasandil, milleks on parlamentaarne järelevalve, õiguskantsler, Andmekaitse Inspeksioon ja kohtud. Igaüht eraldi vaadates ilmneb, et ükski neist ei kata just seda ala, kus riive on kõige intensiivsem. Riigikogu julgeolekuasutuste järelevalve erikomisjon teostab järelevalvet julgeolekuasutuste üle ja on rikkumise avastamisel kohustatud edastama materjalid uurimisasutusele või õiguskantslerile (JAS § 36). Avalikkuse jaoks piirdub komisjoni töö tulemus kord aastas Riigikogule esitatava ülevaatega. Need ülevaated on lühikesed ega sisalda teavet teabehanketoimingute kohta. Komisjonil on küll õigus kutsuda välja isikuid ja nõuda dokumente (JAS § 36 lg 3), kuid seaduses ei ole määratletud, millistele dokumentidele see õigus laieneb. Komisjoni juurdepääs teabehanketoimingute materjalidele on seega eeldatav, mitte tagatud.

Õiguskantsleril puudub juurdepääs julgeolekuasutuse tegevuse salajasel või täiesti salajasel tasemel salastatud meetoditele ning pooleliolevatele teabehanketoimingutele.* Kuna JAS ei sea teabehanketoimingute kestusele piirangut, tähendab „poolelioleva toimingu“ erand, et järelevalveorganil võib puududa juurdepääs just sellele teabele, mis kajastab kehtvat rikkumist. Andmekaitse Inspeksiooni pädevus julgeolekuasutuste andmetöötluse osas on piiratud ning tema põhitähelepanu on suunatud üldisele andmekaitsele.

Kohtulik kontroll on tugev, kuid ainult seal, kus seadus nõuab kohtu luba, ehk vaid üksikute toimingute puhul, ning ka seal kontrollib kohus toimingut eelnevalt, mitte tagantjärele sisuliselt. Tagantjärele kohtusse pöördumiseks peab inimene riivist teadma, mis viib tagasi teavitamise probleemi juurde. Selle tulemusel tekib kontrolli tühimik, sest julgeolekuasutus teeb kõige intensiivsemad riived oma juhi loal, nende kohta statistikat ei avaldata, neist ei teavitata ja nende dokumenteerimise kord on salastatud. Just nende toimingute kohta ei anna ükski neljast kontrollimehhanismist sisulist tagasisidet ning põhjus on seaduse ülesehituses, mitte mehhanismides endis.

Tsiviilkontrolli taandumine

Lisaks neljale nimetatud mehhanismile peaks õiguskaitse- ja julgeolekuasutuste üle tsiviilkontrolli teostama ka ministeerium, kelle valitsemisalasse asutus kuulub, ning valdkonna eest poliitiliselt vastutav minister. 2026. aasta arutelud terviseandmete väljanõudmise üle näitavad aga, et ministrid ei ole seda rolli täitnud kriitilise kontrollijana, vaid on asunud oma haldusala asutuste tegevust õigustama. Probleemi on käsitletud mitte õigusvastase tegevusena, mis tuleb lõpetada ja mille eest tuleb vastutada, vaid üksnes puuduliku õigusliku alusena, mis tuleb seadusega luua.

Siseminister Igor Taro tellis 2026. aasta juunis PPA-lt ja Kaitsepolitseiametilt terviseandmete päringute ülevaatus. Selle käigus selgus, et kaitsepolitsei tegi 13 kuu jooksul päringuid umbes 13 000 inimese terviseandmete kohta, PPA 2139 päringust 135 ei olnud õiguspärased või vajasis täiendavat kontrolli ning PPA oli kasutanud retseptiandmeid isiku võimaliku asukoha tuvastamiseks, mida amet ise pidas ebaproportsionaalseks. Sellest hoolimata leidis minister, et päringuid tehakse tööalastest vajadustest, riigi andmekogude üle teostatav järelevalve on usaldusväärne ja asutuste igapäevane sisekontroll toimib tõhusalt; muutmist vajab tema hinnangul eelkõige seadus (ERR, 07.08.2026). Juulis 2026 külastas minister kaitsepolitseid ja kinnitas pärast juhuvalikuga lõpetatud toimikutega tutvumist, et on veendunud ameti õiguspärases tegutsemises (ERR, 17.07.2026). Sama mustrit näitab numbrituvastuskaamerate juhtum: pärast õiguskantsleri ja Andmekaitse Inspeksiooni kriitikat peatati

* ÕKS § 11¹ lg 6 p-d 1–4: õiguskantsleril ei ole juurdepääsu salastatud välisteabele või riigisaladusele, mis puudutab salajasele koostööle kaasatud isikut, julgeolekuasutuse salajase või täiesti salajase taseme meetodeid, JAS §-des 25 või 26 sätestatud viisil veel lõppemata teabe kogumist või rahvusvahelisi ühisoperatsioone ja välispartneri teavet ilma edastaja nõusolekuta.

kaamerate kasutamine „vajalike seaduste muutmiseni“, mitte ei hinnatud, kas ja kui ulatuslikult oli aastaid kogutud andmestik üldse lubatav.

Sotsiaalminister Karmen Joller, kelle vastutusalasse kuuluvad tervise infosüsteem ja seda haldav TEHIK, vastas Eesti Arstide Liidu pöördumisele, et TEHIK ei ole midagi valesti teinud, sest tegutses kehtiva seaduse järgi, ning et PPA, kelle töötajad nõudsid terviseandmeid kohati ilma piisava põhjendusega, on oma praktikad juba muutnud. Seejärel suunas minister tähelepanu arstidele, kes jagavad patsientide andmeid sotsiaalmeedias (ERR, 2026). Samal ajal näeb tema ministeeriumi eelnõu ette kolme suure terviseandmete kogu – retseptikeskuse, Tervisekassa raviarvete andmekogu ja tervise infosüsteemi – ühendamise, mis koosmõjus juurdepääsureeglitega pigem laiendab kui kitsendab andmetele juurdepääsu (ERR, 12.10.2026).

Mõlema ministri sõnavõttudes puudub samas igasugune tunnistus selle kohta, et isikute põhiõigusi on rikutud. Ilma piisava aluseta tehtud päringuid ja andmete kogumist käsitletakse justkui vormistusvea või halva seaduse probleemina, mitte põhiõiguste riivena, mille eest keegi vastutab. Kui lahendus seisneb vaid aluse loomises seni toimunud tegevusele, muutub seadusloome õigusvastase praktika tagantjärele seadustamiseks ja kinnimätsimiseks, mitte põhiõiguste kaitseks. Tsiviilkontroll, mis näeb oma ülesannet valitsemisala asutuse kaitsmises, ei ole kontroll, vaid selle puudumine.

Siiski tuleb rõhutada asjaolu, mis avalikus arutelus sageli tähelepanuta jääb. Julgeolekuasutuste olemasolu ja ulatuslikud volitused on Eesti julgeolekuolukorras põhjendatud ning Kaitsepolitseiametil peab olema õigus teavet varjatult koguda. Küsimus on üksnes selles, kas selle õiguse kasutamise üle peab olema samasugune kontroll nagu sisuliselt samade toimingute üle kriminaalmenetluses. Kehtiv õigus vastab sellele küsimusele eitavalt, ilma et selleks oleks muud põhjendust kui asjaolu, et kaks korda sätestati eri seadustes eri aegadel.

Ettepanekud

- **Tõhustada teavitamist.** Teabehanketoimingute puhul tuleb kehtestada teavitamiskohustus, mis ei sõltu üksnes salastatuse kustumisest, ning näha ette sõltumatu kontroll selle üle, kas teavitamata jätmine on konkreetsel juhul põhjendatud. Sama põhimõtte peab kehtima juhul, kui teabehanke või jälitustegevuse käigus kogutud teavet kasutatakse haldusmenetluslikuks ennetamiseks, sealhulgas teise asutuse või tööandja teavitamiseks.
- **Avaldada korrapäraselt aastaaruandeid, milles esitatakse koondkujul andmed jälitustoimingute, teabehanketoimingute ja haldusmenetlusliku ennetuse kohta,** sealhulgas lubade arv, toimingute liigid ja kestus, teavitamiste ja teavitamata jätmiste arv ning nende juhtumite arv, mil julgeolekuasutuse kogutud teave edastati ennetava meetme võtmiseks teisele asutusele. Koondandmete avaldamine ei kahjusta ühegi toimingu salajasust, kuid võimaldab hinnata, kas haldusmenetluslik ennetamine on erand või tavapärane töövahend.

- **Ühtlustada teabehankeloa standard kriminaalmenetluses kehtivaga.** Loal tuleb märkida konkreetsed asjaolud, millest tuleneb põhjendatud kahtlus, ning põhjendada, miks ei ole võimalik saada teavet muul, vähem riivaval viisil. Julgeolekuasutuse juhi loal tehtavate toimingute ring tuleb seaduses selgelt piiritleda ning kõige intensiivsemad neist tuleb allutada kohtulikule eelkontrollile. Asutusesisese loa andmise kord ei tohi olla täielikult kontrollimatu riigisaladus. Isikul, kelle suhtes toiminguid tehti ja luba anti, peab olema võimalik nende põhjendustega tutvuda ja neid vaidlustada.
- **Määratleda seaduses teabehanketoimingute alused, uuritavate tegude ring ja subjektide ring senisest konkreetsemalt ning lisada eraldi kord teabe edastamiseks väljaspool süüteomenetlust.** Kui julgeolekuasutus edastab teavet teisele asutusele või tööandjale haldusmenetlusliku ennetuse eesmärgil, peab seadus sätestama edastamise aluse, andmekoosseisu, põhjendamise kohustuse, faktide ja hinnangute eristamise ning isiku teavitamise ja vaidlustamise korra.
- **Täpsustada õiguskantsleri ja Riigikogu erikomisjoni juurdepääsu ning luua eraldi sõltumatu JAS-i järelevalvenõukogu.** Õiguskantsleri seaduse § 11¹ lõike 6 piirangud tuleb üle vaadata nii, et õiguskantsleril oleks tegelik juurdepääs ka salastatud meetoditele ja pooleliolevatele toimingutele, kui kontrolli eesmärk on hinnata põhiõiguste riivet. Järelevalvenõukogul peab olema õigus teha juhuvalimil põhinevaid kontrole, tutvuda teabe edastamise juhtumitega ja avaldada avalikke koondülevaateid.

Kokkuvõte

Raporti lähtekohaks oli küsimus, kas Eestist on saamas jälgimisühiskond. Eesti ei ole politsei- ja autoritel puudub teave selle kohta, et riigiasutused jälgiksid (vähemalt süstemaatiliselt) kodanikke pahatahtlikult. Samas on Eestis kujunenud andmetöötuse süsteem, millel on jälgimisühiskonna struktuursed tunnused. Andmeid kogutakse rutiinselt ja ilma isiku sisulise valikuvõimaluseta, neid kasutatakse isikute liigitamiseks riskikategooriatesse, tähelepanu on suunatud võimalikule tulevasele teole ning riigi ja isiku teadmised teineteise kohta on sügavalt ebavõrdsed. Selliste suundumuste düstopiliste tagajärgede üle mõtiskleb linatöös „Minority Report“ (2002).

Esimene ja kõige olulisem järeldus on, et probleem seisneb andmekogude koostöös. Rahvastikuregister, kinnistusraamat, tervise infosüsteem, maksu- andmed ja töötamise register on igaüks eraldi võetuna põhjendatud ning enamik neist on hästi hallatud. Tehniliselt on registritevahelised takistused aga kadunud, samal ajal kui õiguslik kaitse on jäänud registripõhiseks. Keegi ei vastuta ülevaate eest, mis tekib kümne õiguspärase päringu tulemuste liitmisel. Seadusandja peab pöörama tähelepanu just sellele järjest kasvavale lõhele tehnilise võimekuse ja õigusliku kontrolli vahel.

Seda olukorda iseloomustab hästi POLIS. POLIS-es töödeldakse väga suurt hulka andmeid ning selle kaks andmestikku on reguleeritud sedavõrd ebamääraste reeglite ja eesmärkidega, et põhimääruse alusel ei ole võimalik andmetöötuse proportsionaalsust hinnata. Põhimäärus võimaldab koguda määratlemata isikute ja objektide kohta määratlemata hulgal teavet üksnes seetõttu, et nad võivad olla seotud avalik-õigusliku normi rikkumisega.

Teine järeldus puudutab riigi sekkumise ajahetke. Klassikalise õigusriigi loogika kohaselt hakkab riik isikule tähelepanu pöörama siis, kui selleks on tekkinud alus, näiteks kahtlus, taotlus või menetlus. Andmepõhises halduses algab tähelepanu varem, pidevalt toimivas riskimudelil, mille suhtes isikul ei ole menetlusseisundit, mis annaks õiguse olla teavitatud või ära kuulatud. Ajaks, mil isik saab teada, et teda kontrollitakse, on riik juba otsustanud ta kontrolli alla võtta, ning ka siis ei avaldata talle, milline riskiloogika ta esile tõstis. Menetluslikud tagatised hakkavad kehtima alles menetluse alustamisest ehk pärast kõige olulisemat otsust, mida isik ei saa vaidlustada.

Kolmas järeldus on, et avalik kontroll on kõige nõrgem seal, kus riive on kõige varjatud. Haldusjärelevalve üle on kohtulik kontroll küll olemas, kuigi see rakendub harva, ning kriminaalmenetluses on ette nähtud kohtu eelluba, teavitamiskohustus ja õigus tutvuda jälitustoimikuga. Julgeolekuasutuste teabehankes on toimingud sisuliselt samad ja riive sama intensiivne, kuid enamiku toimingute puhul puuduvad asutuseväline luba, avalik statistika, tegelik teavitamine ja tutvumisõigus ning järelevalveasutuste juurdepääs on piiratud või määratlemata. Riigikohus on kahel korral leidnud, et teavitamata jätmine peab olema sõltumatult kontrollitav, kuid teabehanke kord seda nõuet ei täida.

Neljas järeldus puudutab eesmärgi vahetumist. Maksuarvestuseks kogutud andmed jõuavad riskimudelisse, mudel käivitab järelevalve ja järelevalves kohustuslikus korras antud selgitused jõuavad väärteo- või kriminaalmenetlusesse. Iga üleminek on eraldi seadusega lubatud, kuid ahelat tervikuna ei ole keegi proportsionaalsuse seisukohalt hinnanud. Riigikohus on küll leidnud, et haldusmenetluses karistuse ähvardusel saadud tõendid on kriminaalmenetluses lubamatud (RKKKo 1-22-3234, p 22–23) ning et eesmärgist erinev andmetöötlus, sealhulgas pangaväljavõtete nõudmine, peab olema põhjendatud ja vastama GDPR-i rangetele nõuetele (RKKKo 3-21-1530, p 67–68). Need on aga tagantjärele rakenduvad õiguskaitsevahendid, mis ei muuda haldusorganite igapäevast praktikat ega kaitse isikut kuritarvituste eest enne nende toimumist.

Viies järeldus puudutab julgeolekuasutuste haldusmenetluslikku ennetustegevust. Kaitsepolitsei ameti endine juhtivtöötaja on erialakirjanduses rõhutanud, et teabehanke käigus kogutud teavet kasutatakse sageli pädevate asutuste teavitamiseks, et need saaksid rakendada ennetavaid meetmeid, mitte kriminaalmenetluses tõendina. Kui meede seisneb loa kaotuses, ametist kõrvaldamises või töösuhte lõpetamises, võib tagajärg olla isiku jaoks sama kaalukas kui karistus, kuid tal puuduvad karistusmenetluses või haldusmenetluses tavapäraselt kehtivad kaitsevahendid. Seetõttu ei piisa jälitustoimingute ja teabehankelubade korra muutmisest, vaid eraldi tuleb reguleerida, millal ja kuidas võib julgeolekuasutus kogutud teavet teisele asutusele või tööandjale edastada.

Lahendus ei seisne digiriigi lammutamises. Andmekogude kaotamine või X-tee piiramine kahjustaks inimesi rohkem kui praegune olukord ega lahendaks ühtegi raportis kirjeldatud probleemi, sest haldus muutuks aeglasemaks, kuid kontrollilüngad jääksid samaks. Lahendus on viieosaline ja järgib sissejuhatuses sõnastatud põhimõtteid.

Esiteks on vaja sisukamat põhjendamist. Iga päring tundlikele andmetele tuleb põhjendada enne selle tegemist ning põhjendus peab nimetama menetluse, eesmärgi ja selle, miks just neid andmeid vajatakse. Tegemist on miinimumiga, ilma milleta ei ole hilisem kontroll üldse võimalik.

Teiseks on vaja läbipaistvust. Inimene peab saama teada, kes tema andmeid vaatas ja miks, ning tervise infosüsteemi andmejälgija näitab, et tehniliselt on see lahendatav. Käimasolevate menetluste kaitseks on erandid vajalikud, kuid need peavad olema ajaliselt piiratud ja lõppema koos menetlusega.

Kolmandaks on vaja sõltumatut kontrolli. Kus kohtu eelluba ei ole proportsionaalne, peab sõltumatu organ tegema päringutele sisulist pistelist järelekontrolli ja avaldama tulemused koondkujul. Teabehanke puhul, kus riive on kõige intensiivsem, tuleb loakord viia kriminaalmenetlusega võrreldavale tasemele ning järelevalveorganite juurdepääs seaduses selgelt sätestada.

Neljandaks tuleb tagada päringute tegelik auditeeritavus. Logid peavad olema täielikud, piisavalt kaua säilitatud ja masinloetavad, et neid saaks süstemaatiliselt analüüsida. Koondstatistika päringute arvu kohta asutuse, andmekogu ja õigusliku aluse kaupa tuleb avaldada regulaarselt, sest mõõtmata ei ole võimalik hinnata, kas olukord paraneb või halveneb.

Viiendaks tuleb reguleerida teabe edastamine väljaspool süüteomenetlust. Kui julgeolekuasutus kasutab kogutud teavet haldusmenetluslikuks ennetamiseks ja edastab selle teisele asutusele või tööandjale, peab seadus sätestama edastamise aluse, põhjendamise ja dokumenteerimise kohustuse, faktide ja hinnangute eristamise ning isiku teavitamise ja vaidlustamise korra. Toimingu nimetus ei muuda selle mõju, mistõttu peab igal toimingul, mis mõjutab isiku tööelu või õigusi, olema nähtav ja kontrollitav menetluslik raamistik.

Need ettepanekud ei nõua põhiseaduse muutmist ega digiriigi ümberehitamist. Need nõuavad, et riik kohtleks oma andmetöötlust ja varjatud teabekogumist sama tõsiselt kui muid võimu teostamise vorme, kohaldades neile põhjendamiskohustust, läbipaistvust, sõltumatut kontrolli ja vaidlustatavust. Eesti digiriik on ehitatud usalduse peale, kuid usaldus, mida ei saa kontrollida, on pelgalt lootus. Raporti lõppsõnum on, et praegu on veel aeg asendada lootus kontrollitava usaldusega, enne kui raporti pealkirjas esitatud küsimusest saab tõdemus.

Paul Keres on Eesti vandeadvokaat ja advokaadibüroo LEVIN partner. Keres on lõpetanud Tartu Ülikooli õigusteaduskonna ning kuulub alates 2010. aastast Eesti Advokatuuri. Oma advokaaditöös on Keres osalenud mitmetes suuremahulistes ja ühiskondlikult olulistes kohtuasjades. Muu hulgas on ta esindanud Vabariigi Valitsust pensionireformi põhiseaduslikkust puudutanud menetluses Riigikohtus ning osalenud Justiitsministeeriumi tellimisel nn punamonumentide eemaldamist puudutava seaduse põhiseaduspärasuse analüüsimisel. 2017. aastal tunnustas Eesti Advokatuur Paul Kerest Aasta Advokaadi tiitliga. Tema tegevuses ühenduvad pikaajaline kohtuvaidluste kogemus, äri- ja finantsõiguse tundmine ning kokkupuude põhimõtetelise põhiseaduslike ja avaliku võimu küsimustega.

Andri Rohtla on Eesti vandeadvokaat, kes on spetsialiseerunud kohtuvaidlustele ning eelkõige kriminaal- ja väärteomenetlusele. Ta on osalenud mitmetes suuremahulistes ja avalikku tähelepanu pälvinud kriminaalasjades, sealhulgas Tallinna Sadama kriminaalasjas. Rohtla on lõpetanud Tartu Ülikooli õigusteaduskonna bakalaureuse- ja magistriõppe ning kuulub alates 2020. aastast Eesti Advokatuuri. Vandeadvokaadina tegutseb ta 2024. aastast. Lisaks advokaaditööle on Rohtla osalenud õiguspoliitilises arutelus, käsitledes muu hulgas kriminaalmenetluse, prokuratuuri pädevuse ning sideandmete kogumise ja põhiõiguste kaitse küsimusi. Ta on osalenud Eesti Advokatuuri esindajana ka sideandmete kogumist puudutava seaduseelnõu ettevalmistamisega seotud aruteludel.

Raporti tellis MTÜ Põhimõtte Koda.
Täname abi eest Jaan Tõnissoni Postimehe Fondi ja Postimehe raamatukirjastust.

Keeletoimetaja Lea Arme
Kujundaja Kalle Müller
Kujunduskontseptsioon: Karl-Kristjan Nigesen
Projektijuht Veiko Lukmann

Väljaande autoriõigus:
Paul Keres, Andri Rohtla ja MTÜ Põhimõtte Koda, 2026

Kõik õigused on kaitstud. Selle raporti ühtegi osa ei tohi reprodutseerida ega edastada ühelgi kujul ega ühegi vahendiga ilma autoriõiguse omaja kirjaliku loata.

ISBN 978-9908-50-165-9 (pdf)
ISSN (Põhimõtte Koja raportid ja mõttepaberid) 3125-5302