Riigikohtu arvamus[1] kriminaalmenetluse seadustiku muudatuste väljatöötamiskavatsuse (digitõendid) kohta

Esmalt ei saa nõustuda VTK-s toodud käsitlusega, mille järgi võimaldavad KrMS § 32 ja § 215 uurimisasutustele pea piiramatut juurdepääsu inimeste e-postkastide sisule. Riigikohus on selgitanud, et KrMS § 32 lg-le 2 ja § 215 lg-le 1 toetudes saab nõuda teavet siis, kui selle teabe nõudmist (ega väljastamist) ei piira muud õigusaktid, sh PS § 43 teisest lausest tulenev piirang (RKKK 08.06.2026, 1-22-7314/268, p 22). Kohtuasjas nr 3-1-1-93-15 ei asunud Riigikohus seisukohale, et pärast isiku e-postkasti jõudmist ei ole e-kiri enam ühelgi juhul käsitatav kommunikatsiooniprotsessis oleva sõnumina ega kuulu seetõttu PS §-s 43 sätestatud sõnumisaladuse kaitsealasse. Kohus selgitas, et sõltumata sellest, kas e-kiri on saajani jõudnud, võib sellega tutvumine olla käsitatav kommunikatsiooniprotsessi sekkumisena siis, kui tutvumiseks ei kasutata kirja saaja (ega saatja) e-posti kontot, vaid juurdepääsu kommunikatsiooniprotsessi käigus tekkivale infole (nt teenusepakkuja juures säilitatavat e-kirja faili koopiat), mille üle kirja saajal ega saatjal kontrolli ei ole (RKKK 20.11.2015, 3-1-1-93-15, p-d 102 ja 103). Sellisel juhul on teavet lubatud koguda *üksnes kohtu loal*. Väljaspool kommunikatsiooniprotsessi olevatele kirjadele laieneb aga PS § 26 kaitseala, millesse võib sekkuda *seaduses sätestatud juhtudel ja korras*.

VTK-ga võib seega nõustuda selles, et õiguslik alus e-postkastide sisu väljanõudmiseks peaks olema seaduses selgelt sätestatud. Olukorras, kus KrMS § 90[1] lg 2 nõuab eeluurimiskohtuniku luba pelgalt tehnilist laadi liiklus- ja asukohaandmete saamiseks, ei saa side sisu puudutavate andmete väljanõudmisele kehtida leebemad nõuded (viidatud 1-22-7314/268, p 23).

EK (suurkoda) on leidnud, et mobiiltelefoni või muusse nutiseadmesse salvestatud andmetele omaniku tahte vastane juurdepääs on tõsine eraelu puutumatuse riive, mis vajab kohtu eelnevat luba (EKo 04.10.2024, C-548/21). VTK-s pakutakse e-postkastidest ja nutiseadmetest tõendite kogumise üle kohtuliku kontrolli tagamiseks välja kaks võimalikku lahendust: kas KrMS § 91 lg-s 1 toodud läbiotsimise mõiste muutmist selliselt, et selle objektiks saaksid olla ka andmekandjad ja nutiseadmed *või* nutiseadmetelt tõendite kogumiseks ja serveriandmete väljanõudmiseks eraldi regulatsiooni loomist. Esimene variant ei pruugi olla kõige sobivam e-postkastide sisu väljanõudmisega kaasnevate probleemide lahendamiseks. Teise variandi puhul ei anta VTK-s aimu sellest, milline kavandatav regulatsioon olema saaks.

Seoses nutiseadmetesse sisenemisega on Riigikohus selgitanud, et kuigi enese mittesüüstamise privileeg ei kohusta isikut oma PIN-koodi andma, ei ole põhimõtteliselt välistatud andmetele ligipääsu saamine ka sunni abil – seda nt olukorras, kus autentimine toimub biomeetrilise (nt sõrmejälje või näo) tuvastuse kaudu. Sel viisil andmetele ligipääs nõuaks aga vastavat luba ja regulatsiooni menetlusseaduses, mida seni kehtestatud ei ole. (Vt lähemalt RKKK 14.06.2022, 1-20-1208, p-d 50–52.)

Küsimus sellest, kuidas arvutisüsteemides olev teave menetlejani jõuab (sh kohtuliku kontrolli tingimus), on aga vaid üks osa probleemist. Lisaks tuleb tegeleda elektroonilistel andmekandjatel sisalduva teabe äravõtmise ja uurimise ulatusega ehk küsimusega toimingu proportsionaalsusest.[2] Õiguskirjanduses on leitud, et teabe äravõtmise ülemäärasust soosib see,

[1] Riigikohtu arvamus ei väljenda Riigikohtu siduvat seisukohta. Riigikohus kujundab siduvaid seisukohti ainult kohtuasjade menetlemisel Riigikohtus.

[2] Riigikohus juhtis juba 2017. aastal tähelepanu sellele, et kehtiva regulatsiooni ülevaatamine ja muutmine digitaalsete tõendite kogumise ja kasutamise eripärast tulenevalt on vajalik. Arvestades igapäevaselt digitaalselt

et puudub täpsem regulatsioon, millisel viisil peab toimuma digitaalsete andmekandjate äravõtmine nii läbiotsimise, vaatluse kui ka nõudekirja alusel.[3] Eeltoodu kõneleb teise lahendusvariandi kasuks.

VTK-s tõstatatud küsimustele vastame järgmiselt:

1. Millised on tüüpilised või iseäranis markantsed juhtumid praktikas, kus kavandatava seadusemuudatusega oleks potentsiaal ebasoovitavateks kõrvalmõjudeks ning millised on teie ettepanekud regulatsiooniks, mis neid kõrvalmõjusid aitaksid vältida?

Kui kavandatav seadusemuudatus tegeleb üksnes andmetele juurdepääsu saamisega ja jätab kõrvale toimingu proportsionaalsuse küsimuse, võib soovimatuks tagajärjeks olla see, et menetleja saab juurdepääsu kogu nutiseadmes või pilveteenuses sisalduvale teabele, kuigi uurimise seisukohalt on asjakohane vaid kitsas osa andmetest. Vältimaks isikute põhiõigustesse ebaproportsionaalset sekkumist, peaks loodav regulatsioon sisaldama nõudeid andmete sihipäraseks filtreerimiseks ning uurimise eesmärgiga mitteseotud andmete eraldamiseks. Loodava normistiku kitsaskohad võivad ilmneda iseäranis juhtudel, mis hõlmavad mh privilegeeritud ja konfidentsiaalse olemusega teavet (sh terviseandmeid ja pangasaladust). Seetõttu tuleb rõhutada VTK-s tehtud tähelepanekut, et tagada tuleb selle kooskõla loodava ametiprivileegide regulatsiooniga. Samal ajal ei tohi aga unustada, et ka nn ametiprivileegide eelnõu ei kata kõiki eriliiki isikuandmed, mis väärivad samaväärset kaitset.

2. Kas ja millised peaksid olema need erandolukorrad, kus nutiseadmes olevaid andmeid peaks saama läbi vaadata seadme omaniku tahtest sõltumatult ka ilma kohtu või prokuratuuri eelneva loata?

Sellised erandid saaksid olla pigem kitsad ning seotud kas vahetu ohuga inimese elule või tervisele (nt röövitud isiku asukoha väljaselgitamine, terroriakti või vägivallakuriteo ärahoidmine) või teatud asjaoludel (näiteks raskemate kuritegude puhul) tõendite hävimise riskiga (nt andmeid on võimalik kaugelt kustutada). Need juhud peavad alluma kohtulikule järelkontrollile. Kuid ka selliste erandite puhul tuleb arvestada privilegeeritud teabe erisustega. Niisugustel juhtudel peaks tõendi hävitamise riski tõttu kohtu eelneva loata ja omaniku tahtest sõltumatu andmete *läbi vaatamine* olema pigem lubamatu ning sellele tuleks eelistada andmetest *koopia tegemist* ilma võimaluseta nende sisuga enne kohtu luba (sh tutvumise ulatus) tutvuda.

3. Millised elektrooniliste tõendite kogumise olukorrad lisaks e-postkastide sisu väljanõudmisele serveripidajalt vajaksid kriminaalmenetluse seadustikus analoogiliselt reguleerimist?

Loodav regulatsioon peaks hõlmama lisaks e-postkastidele ka erinevaid sõnumirakendusi, sotsiaalmeedia- ja muid kontosid ning pilveteenuseid.

---

edastatavate, säilitatavate jm viisil töödeldavate andmete mahtu, on vajalik sätestada seaduses nt arvuandmete kogumise ja tõendina kasutamise tingimused ning puudutatud isikute menetlusgarantiid (vt ka nt EIKo 14.03.2013 Bernh Larsen Holding AS jt *vs*. Norra; EIKo 03.09.2015 Servulo ja Associados – Sociedade de Advogados, RL *vs*. Portugal).

[3] L. Aiaots. Kas suured andmemassiivid on tõendite kullaauk või kriminaalmenetluse hukatus?, Juridica 1-2/2025, lk 70.