



RAHAPESU ANDMEBÜROO

Liisa-Ly Pakosta
Justiits- ja Digiministeerium
info@justdigi.ee

Teie 29.05.2026 nr 8-3/4289-1

Meie 16.06.2026 nr 1.2-3/77-2

**Arvamus seoses väljatöötamiskavatsusega,
mis puudutab e-postkastide ja nutiseadmetes
sisalduvate andmete tõendina kogumist
süüteomenetluses**

Täname võimaluse eest avaldada arvamust seoses väljatöötamiskavatsusega, mis puudutab e-postkastide ja nutiseadmetes sisalduvate andmete tõendina kogumist süüteomenetluses (VTK). Kokkuvõtlikult mõistame kavandatava regulatsiooni vajalikkust ning esitame alljärgnevad omapoolsed kommentaarid ja tähelepanekud.

VTK seab eesmärgiks luua elektroonsete tõendite kogumiseks õiguslik raamistik, mis ühelt poolt kaitseb eraelulisi andmeid õiguskaitseasutuste ebaproportsionaalse sekkumise eest ja teisalt võimaldab asjakohasel juhul kasutada neid andmeid süüteomenetluses lubatava tõendina. Kavandatav regulatsioon peab seejuures olema kooskõlas Euroopa Liidu Kohtu ning Euroopa Inimõiguste Kohtu praktikaga.

Kirjeldatud eesmärk on Eesti süüteomenetluse kontekstis meie hinnangul kahtlemata oluline, eriti arvestades hiljutist kohtupraktikat, kus Riigikohtu kriminaalkolleegium asus 8. juuni 2026 lahendis nr 1-22-7314 kokkuvõtlikult seisukohale, et e-postkasti sisu teenusepakkuvalt pärimise puhul ei anna kriminaalmenetluse seadustiku (KrMS) § 32 lõige 2, § 90¹ lõige 1 ja § 215 lõige 1 kõnealuse teabe kogumiseks seaduslikku alust (vt lahendi punkt 20). Ehkki Rahapesu Andmebüroo (RAB) ei ole uurimisasutus ja meie ülesandeks on tulenevalt rahapesu ja terrorismi rahastamise tõkestamise seaduse (RahaPTS) § 54 lõike 1 punktist 10 samas seaduses sätestatud väärtegade menetlemine, on tõstatatud probleemistik ja vajadus asjakohase õigusliku raamistiku kehtestamiseks kahtlemata aktuaalne ka väärtemenetluse kontekstis. Ehkki väärtemenetluse seadustik (VtMS) näeb võrreldes KrMS-iga ette eriregulatsiooni, siis ühtsetest põhimõtetest lähenemine kogu süüteomenetluse kontekstis on vältimatult vajalik ning palume sellega seaduseelnõu koostamisel kindlasti arvestada.

VTK-s on toodud võimalike lahendustena välja kaks alternatiivi. Neist esimene kätkeb endas olemasoleva läbiotsimise mõiste laiendamist nii, et läbiotsimise objektiks saaksid olla ka andmekandjad ja nutiseadmed. Teise alternatiivi kohaselt sätestatakse nutiseadmetelt tõendite kogumine ja serveriandmete väljanõudmine eraldi regulatsiooniga, mis võimaldab elektroonliste tõendite eripära täpsemalt arvestada ning sobitub paremini kavandatava ametiprivileegide regulatsiooniga. Oleme seisukohal, et uue regulatsiooni loomine oleks märkimisväärselt põhjendatum ning eelistatum lahendus. Olemasoleva läbiotsimise mõiste laiendamine võib

tunduda intuiitiivselt lihtsam, kuid võiks pikemas perspektiivis tekitada palju rohkem õigusselgusetust, samuti probleemkohti ja selgusetuid küsimusi varasema ohtra läbiotsimisi puudutava kohtupraktika tõlgendamisest uue käsitlese järgi jne. Uue lahenduse loomist oleks mõistlik alustada õigusselguse huvides serveriandmete, andmekandjate ja nutiseadmete defineerimisest, mille järel on võimalik kujundada vastavate elektrooniliste tõendite eripära arvestav regulatsioon.

VTK-s on esitatud muu hulgas küsimus selle kohta, 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. Samuti küsitakse, millised elektrooniliste tõendite kogumise olukorrad lisaks e-postkastide sisu väljanõudmisele serveripidajalt vajaksid kriminaalmenetluse seadustikus analoogiliselt reguleerimist. Juhime mõlema küsimuse kontekstis tähelepanu, et lisaks e-postkastide sisule on tõenditena üha asjakohasemad erinevate, sh krüpteeritud suhtlusrakenduste vahendusel saadetud sõnumid (nt Telegram, Signal). Nende eripära on ühelt poolt see, et teenuseosutajal endal ei olegi tihti võimalik vestluse sisu edastada, kuna tegemist on nn *end-to-end encryption*'iga, mis tähendab, et ainus võimalik juurdepääs on nutiseadme valdaja enda kaudu, vähem ebaoluline ei ole siin kontekstis ka mõne teenuseosutaja ebatõenäoline koostöö õiguskaitseasutustega. Ühtlasi on laialdaselt levinud võimalus seadistada teatud perioodi järel isekustuvaid sõnumeid, mis toob kaasa aegkriitilisuse. Teisalt tähendab üha kasvav pilveteenuste kasutamine, et andmeid on võimalik kustutada soovi korral distantsilt, sh kustutada kogu nutiseadme sisu. See tähendab, et põhjendatud oleks valida lähenemine, kus teatud edasilükkamatutel juhtudel, kus vastasel korral oleks tõenäoline andmete kustumine jms aegkriitilised kaalutlused, oleks sarnaselt hetkel kehtiva läbiotsimise regulatsiooniga (KrMS § 91 lõiked 5 ja 6) võimalik saada eeluurimiskohtuniku luba tagasiulatuvalt menetlustoimingu lubatavaks tunnistamise määрусega.

Täname võimaluse eest arvamust avaldada ja osaleme meeleldi edaspidistes teemakohastes aruteludes.

Lugupidamisega

(allkirjastatud digitaalselt)

Ingrid Muul
osakonnajuhataja
Rahapesu Andmebüroo juhi ülesannetes