SISEMINISTEERIUM

Pr Liisa-Ly Pakosta
Justiits- ja Digiministeerium

Teie: 29.05.2026 nr JDM/26-0647/-1K

Meie: 26.06.2026 nr 1-7/171-3

Siseministeeriumi arvamus e-postkastide ja nutiseadmete andmete tõendina kogumist käsitleva väljatöötamiskavatsuse kohta

Siseministeerium on tutvunud väljatöötamiskavatsusega, mis käsitleb e-postkastides ja nutiseadmetes sisalduvate andmete tõendina kogumist süüteomenetluses, ning toetab eesmärki luua elektrooniliste tõendite kogumiseks selgem õiguslik raamistik. Leiame, et kehtiv regulatsioon vajab ajakohastamist, kuna Euroopa Kohtu praktikast tulenevate nõuetega arvestamata jätmine viib olukorrani, kus siseriikliku praktika järgi tehtud toiminguid hinnatakse õigusvastaseks ning nende tulemusena saadud tõendid tunnistatakse lubamatuks.

Euroopa Kohus on lahendis C-548/21 *Bezirkshauptmannschaft Landeck* leidnud, et juurdepääs mobiiltelefonis sisalduvatele andmetele võib kujutada endast olulist põhiõiguste riivet, kuna mobiiltelefon võib sisaldada muu hulgas sõnumeid, fotosid, veebilehitsemise ajalugu ning liiklus- ja asukohaandmeid, mille põhjal on võimalik teha väga täpseid järeldusi inimese eraelu kohta. Seetõttu peab Euroopa Kohtu hinnangul olema juurdepääs mobiiltelefonis sisalduvatele andmetele seaduses piisavalt selgelt ja täpselt sätestatud ning alluma üldjuhul (välja arvatud põhjendatud kiireloomulistel juhtudel) kohtu või sõltumatu haldusasutuse eelkontrollile.

1. Siseministeeriumi hinnangul on tänapäevase nutiseadme sisu vaatamisel ulatuslik eraelu riive pigem reegel kui erand, sest nutiseade koondab sageli inimese suhtluse, dokumendid, fotod, kontaktid, liikumisandmed, veebikasutuse ja muu eraelulise teabe viisil, mis annab inimese eraelust terviklikuma ja detailsema pildi kui paljude tavapäraste füüsiliste esemete või ruumide läbiotsimine. Seetõttu peame põhjendatuks allutada nutiseadme, arvuti või muu digitaalse andmekandja sisu vaatlemine põhimõtteliselt kriminaalmenetluse seadustikus (edaspidi *KrMS*) sätestatud läbiotsimise regulatsioonile. Mööname, et digitaalse andmekandja sisu vaatlemise allutamine otse KrMS §-s 91 sätestatud läbiotsimise regulatsioonile, näiteks läbiotsimise objekti laiendamisega digitaalsele keskkonnale, läheks vastuollu Riigikohtu senise käsitusega, mille kohaselt arvutisüsteeme läbi ei otsita ning andmekandjal sisalduva teabega tutvumine toimub läbi KrMS §-s 86 sätestatud vaatluse, mistõttu peame võimalikuks kahte lahendust.

    a) Esimese võimaliku lahendusena näeme seaduses kuriteokoosseisude loetlemist, mille puhul on seadusandja juba hinnanud, et digitaalse andmekandja sisuga tutvumine on riive intensiivsust arvestades üldjuhul proportsionaalne. Lahendus lähtub analoogia korras KrMS § 99^1 loogikast, milles teatud raskusastmega kuritegude puhul on seadusandja pidanud võrdlusmaterjali võtmist igal juhul põhjendatuks, nähes leebemate rikkumiste puhul meetme kohaldamise vajaduse hindamise menetleja kaalutluseks.

Analoogse lahenduse korral saaks seadusandja eelnevalt määratleda olukorrad, kus riive on üldjuhul põhjendatud, jättes muudel juhtudel toimingu lubatavuse hindamise kohtule. Digitaalse andmekandja sisu vaatluse puhul võiks selline lävend olla seotud näiteks raskete kuritegudega või kuritegudega, mille puhul on lubatud jälitustoimingud.

Rakendajatele oleks selline lahendus lihtsam kui igakordne kohtu loa taotlemine, vähendaks kohtu, prokuratuuri ja uurimisasutuste töökoormust ning võimaldaks menetluses kiiremini edasi liikuda. Samas mööname, et selline lahendus ei pruugi olla kooskõlas *Bezirkshauptmannschaft Landeck* punktis 102 väljendatud põhimõttega, et mobiiltelefonis sisalduvatele andmetele juurdepääs peab olema allutatud kohtu või sõltumatu haldusasutuse eelkontrollile.

b) Teise võimaliku lahendusena näeme eriregulatsiooni kehtestamist digitaalse andmekandja sisu vaatlusele, lähtudes KrMS-is sätestatud läbiotsimise regulatsiooni põhimõtetest. Selline lahendus võtaks arvesse Riigikohtu praktikat ehk toiming jääks liigilt vaatluseks, kuid digitaalse andmekandja sisu vaatlus allutataks üldreeglina kohtu loale, erandina KrMS § 91 lg 3 loogika kohaselt edasilükkamatul juhul tagantjärele kohtulikule kontrollile.

Praktiliselt on eriregulatsioon põhjendatud sellega, et digitaalse andmekandja sisu läbivaatamine erineb olemuslikult koha või asja läbiotsimisest. Reeglina ei viibi menetlusosaline digitaalse andmekandja vaatluse juures, kuna andmetega tutvumine ei toimu tavaliselt vahetult andmekandja äravõtmise hetkel, andmete kopeerimine ja sisuline läbivaatamine võib võtta märkimisväärselt aega ning mõnel juhul võib olla vajalik seadme saatmine ekspertiisi või välisriiki avamiseks või kopeerimiseks. Seetõttu peaks eriregulatsioon arvestama, et digitaalse andmekandja kopeerimine ja läbivaatamine ei ole ajaliselt võrreldav koha või asja läbiotsimisega ning võib sõltuvalt andmemahust, seadme lukustusest või ekspertiisivajadusest kesta oluliselt kauem.

Edasilükkamatu juhu erand on vajalik olukorras, kus viivitus võib muuta andmete säilitamise või hilisema vaatlemise võimatuks. Praktikas võib see puudutada näiteks olukorda, kus sõnumirakenduse vestluse kustutab teine osapool, e-posti kontole logitakse sisse teisest seadmest või seade kustutab andmed automaatselt, näiteks pikema kasutamata seismise või ebaõnnestunud avamiskatsete järel. Samuti võib kiire andmete säilitamine olla vajalik juhul, kui seadmes võivad sisalduda andmed veel tuvastamata või kinni pidamata kuritegeliku grupi liikmete kohta.

2. Rõhutame, et digitaalse andmekandja äravõtmist ja kopeerimist tuleb selgelt eristada andmekandja sisu või sisu koopia vaatlemisest. Kohtu loa nõue peaks puudutama andmetega sisulist tutvumist, mitte andmekandja äravõtmist ega andmete säilitamiseks vajalikku kopeerimist. Uurimisasutusel peab olema võimalik andmekandja ära võtta ning säilitada nii andmekandja sisu koopia kui vajaduse korral ka andmekandja ise enne kohtult loa saamist, sest vastasel juhul võib tõendusteave kaduda, muutuda või muutuda hiljem kontrollimatuks.

Kui kohtu luba oleks vaja juba andmekandja äravõtmiseks või kopeerimiseks, muudaks see menetluse põhjendamatult koormavaks ning võib takistada tõendite säilimist (seadet ei ole võimalik õigeaegselt isoleerida et andmete muutumist välistada). Digitaalsete tõendite puhul tuleb arvestada nende muutumise ja hävimise riskiga. Näiteks võib WhatsAppi või muu sõnumirakenduse vestlusi kustutada ka vestluse teine osapool ning telefoniga seotud e-posti kontole võib olla võimalik sisse logida teisest seadmest ja seal olevaid andmeid muuta või kustutada. Samuti võib tõendusteave kaduda seadme või konto tehniliste

seadistuste tõttu, näiteks juhul, kui andmed kustuvad automaatselt kindla aja möödumisel või ebaõnnestunud avamiskatsete järel. See on eriti oluline olukorras, kus seadmes võivad sisalduda andmed veel tuvastamata või kinni pidamata kuritegeliku grupi liikmete kohta. Seetõttu palume Euroopa Kohtu praktikast tulenevat loavajadust mitte tõlgendada laiendavalt.

Seadmele või andmetele juurdepääsu võimaldamise küsimuses peame oluliseks eristada tehnilise juurdepääsu loomist andmete sisulisest vaatlemisest. Näiteks PUK-koodi või muu tehnilise juurdepääsu eelduse kasutamine ei tähenda iseenesest õigust seadme sisuga tutvuda. Sideettevõtjalt PUK-koodi küsimist tuleks käsitada tehnilise eeldusena vaatluse võimaldamiseks, mitte iseseisva juurdepääsuna seadme sisule. Samas tuleks regulatsioonis selgelt läbi mõelda, millal ja millistel tingimustel võib isikult nõuda aktiivset kaasabi ning millal saab selline kaasabi olla üksnes vabatahtlik pärast õiguste, sealhulgas enese mittesüüstamise privileegi selgitamist.

Samuti palume arvestada, et digitaalse andmekandja sisu ei ole võimalik osaliselt kopeerida või enne koopia tegemist eraldada üksnes menetluse seisukohalt vajalik teave. Uurimisasutus võib küll üldiselt teada, millist liiki teavet otsitakse, kuid enne andmete läbivaatamist ei ole võimalik täpselt teada, kus vajalik teave paikneb, millisel kujul see esineb või milliste andmete koosmõjus selle tõenduslik tähendus ilmneb. Seetõttu tehakse koopia andmekandja sisust tervikuna ning menetluse seisukohalt asjakohane teave eraldatakse ja vormistatakse tõendina alles hilisema läbivaatamise käigus.

Näiteks narkokuritegude puhul võib suhtlus olla konspireeritud, kasutades varjatud tähendusega väljendeid või emotikone. Üksiku sõnumi või pildi tähendus selgub alles kontekstis, koosmõjus muu teabega. Seetõttu ei ole enne sisuga tutvumist võimalik usaldusväärselt otsustada, millised andmed on menetluse seisukohalt vajalikud ja millised mitte. Märksõnade või faililiikide põhine eelfilter võib sellise teabe välja jätta, kuid samas tuua esile suure hulga andmeid, millel menetluse esemega seos puudub.

Samal põhjusel ei tohiks loa ulatust siduda jäiga ajapiiranguga. Mõnes menetluses võib oluline olla ka varasem suhtlus või muu pikema aja jooksul kogunenud teave, näiteks kuritegeliku ühenduse püsivuse, liikmete omavahelise seose või rollijaotuse tõendamiseks. Loa ulatus peaks lähtuma konkreetsest menetlusvajadusest, mitte abstraktsest ajalisest piirist.

Märgime, et tervikliku koopia tegemine ei tähenda, et kogu koopias sisalduv teave muutub tõendiks või et seda võib kasutada väljaspool konkreetse menetluse eesmärki. Euroopa Parlamendi ja nõukogu direktiivi (EL) 2016/680, mis reguleerib isikuandmete töötlemist õiguskaitseasutustes süütegude tõkestamise, avastamise, uurimise ja menetlemise eesmärgil, art 4 lg 1 p-de b, c ja e järgi tuleb isikuandmeid töödelda kindlaksmääratud ja õiguspärasel eesmärgil, asjakohases ja vajalikus ulatuses ning säilitada üksnes nii kaua, kui see on vajalik. Sama loogika on sätestatud isikuandmete kaitse seaduse § 14 lg 1 p-des 2, 3 ja 5. Seetõttu tuleb tõendina vormistada üksnes menetluse seisukohalt asjassepuutuv teave ning asjassepuutumatut materjali ei tohi kriminaaltoimikusse lisada ega kasutada menetlusväliselt.

3. Eraldi rõhutame vajadust säilitada võimalus tutvuda digitaalse andmekandja sisuga isiku teadliku ja vabatahtliku nõusoleku alusel. See ei asendaks kohtu loa üldreeglit, vaid võimaldaks piiratud ulatuses tutvuda konkreetse sisuga olukorras, kus isik ise soovib seda uurimisasutusele näidata. Isikul võib olla põhjendatud huvi näidata näiteks konkreetset

vestlust, fotot, dokumenti, IMEI-koodi või muud piiritletud teavet, et kahtlustust ümber lükata või vältida ulatuslikumaid menetlustoiminguid.

Nõusoleku küsimust tuleks käsitleda muuhulgas seetõttu, et Euroopa Kohtule on kohtuasjas C-313/26 esitatud eelotsusetaotlus, milles küsitakse liikmesriikide seisukohtu selles, kas politsei võib kriminaaluurimise raames ära võetud mobiiltelefonis sisalduvate andmetega tutvuda andmesubjekti nõusoleku alusel ilma kohtu või sõltumatu haldusasutuse eelneva loata ning kas nõusoleku korral võib tutvuda üksnes konkreetsete andmetega või kogu mobiiltelefonis sisalduva teabega.

Meie hinnangul peaks nõusoleku alusel tutvumine olema lubatud üksnes piiratud ja selgelt määratletud ulatuses. Nõusolek peab olema teadlik, vabatahtlik ja piiritletud, st isikule peab olema selgitatud õigust vaikida ehk õigust mitte aidata kaasa enda süüstamisele ning talle peab olema selge, millise teabega tutvutakse (nõusolek konkreetse sisuelemendi vaatamiseks ei anna alust laiendada vaatlust kogu andmekandja sisule). Näiteks võib isik soovida näidata uurimisasutusele konkreetset vestlust, fotot või dokumenti, mis tema hinnangul lükkab kahtlustuse ümber või selgitab tema käitumist. Sellisel juhul peaks meie hinnangul olema võimalik tutvuda selle konkreetse sisuga isiku teadlikul ja vabatahtlikul nõusolekul ning vajaduse korral jäädvustada menetluse seisukohalt asjakohane osa. See aitaks vältida kogu andmekandja sisu kopeerimist ja läbivaatamist kohtu loa alusel, sest nõusolek konkreetse vestluse, foto või dokumendi vaatamiseks ei anna alust laiendada vaatlust kogu seadmele või muule andmekandjal sisalduvale teabele. Kui piiratud vaatluse käigus ilmneb viide muule kuriteole või vajadus andmekandja ulatuslikumaks läbivaatamiseks, tuleks edasine juurdepääs lahendada üldises korras ehk kohtu loa alusel.

4. E-postkastide osas jääme varasemalt väljendatud seisukoha juurde, et teenuseosutaja hallatavas arvutisüsteemis asuvast e-kirjast koopia tegemine peaks toimuma prokuratuuri taotlusel ja kohtu loal. Seda seisukohta toetab Riigikohtu praktika, eelkõige 08.06.2026 otsus nr 1-22-7314/268, milles Riigikohus leidis punktides 20–25, et teenuseosutaja juures säilitatava e-postkasti sisu väljanõudmiseks ei anna KrMS § 32 lg 2, § 90[1] lg 1 ega § 215 lg 1 piisavat õiguslikku alust. Sama otsuse punktides 22–23 rõhutas Riigikohus, et kui tehnilist laadi liiklus- ja asukohaandmete saamiseks on nõutav eeluurimiskohtuniku luba, ei saa side sisu puudutavate andmete väljanõudmisele kehtida leebemad nõuded.

   Samas peame oluliseks eristada olukorda, kus uurimisasutus tutvub e-kirjadega isiku valduses oleva arvuti, telefoni või muu digitaalse andmekandja kaudu ning olukorda, kus e-kirjade sisu soovitakse saada teenuseosutaja või muu kolmanda isiku hallatavast serverist. Esimesel juhul on tegemist digitaalse andmekandja sisu vaatlusega, millele peaks kohalduma eespool kirjeldatud digitaalse andmekandja vaatluse eriregulatsioon. Teisel juhul on tegemist teenuseosutajalt sisuandmete väljanõudmisega, mille puhul toetame eraldi kohtu loa aluse sätestamist.

   Regulatsiooni kujundamisel võiks meie hinnangul lähtuda Euroopa Parlamendi ja nõukogu 12.07.2023 määruse (EL) 2023/1543 loogikast, mille kohaselt eristatakse elektrooniliste tõendite puhul andmete säilitamist ja andmete esitamist. Andmete säilitamise eesmärk on hoida ära nende kustutamine või muutmine, kuid säilitamine ei anna veel õigust andmete sisuga tutvuda. E-postkasti sisuandmete saamiseks peab olema eraldi kohtu luba.

   Samuti tuleks eristada küsitavate andmete liiki. Kasutaja tuvastamisega seotud andmed, näiteks konto või kasutaja kindlakstegemiseks vajalikud andmed, ei ole riive intensiivsuselt võrreldavad e-kirjade sisuga. E-kirjade sisu annab otsese ülevaate inimese suhtlusest ja eraelust ning selle väljanõudmine peab seetõttu alluma rangemale kontrollile.

Eraldi vajab läbimõtlemist tööandja või muu haldaja juures asuvate e-kirjade väljanõudmine. Riigikohtu 08.06.2026 otsus nr 1-22-7314/268 käsitles teenuseosutaja juures säilitatavat e-postkasti sisu ega lahendanud küsimust, kas ja millistel tingimustel võivad nõuded erineda olukorras, kus e-kirjad asuvad tööandja või ametiasutuse hallatavas keskkonnas. Ametialaste süütegude menetlemisel on oluline, et seadus annaks ka sellisteks olukordadeks selge aluse.

5. Regulatsioon ei peaks piirduma üksnes e-postkastide ja nutiseadmetega. Sama küsimus võib tekkida näiteks arvutite, tahvelarvutite, väliste kõvaketaste, mälupulkade, pilvekontode, võrguketaste, sõnumirakenduste, häälsõnumite, fotode ja videote puhul. Vajalik teave ei pruugi asuda üksnes seadme füüsilises mälus, vaid võib olla sünkroniseeritud pilvekontole, sõnumirakendusse või tööandja võrgukettale. Seetõttu võiks VTK edasises menetluses kaaluda nutiseadme asemel laiema mõiste kasutamist, näiteks arvutisüsteem või digitaalne andmekandja või mõni muu tehnoloogianeutraalsem, abstraktsem koondmõiste.

6. Kolmandate isikute andmete puhul leiame, et nende sisaldumine digitaalses andmekandjas või e-postkastis ei saa iseenesest välistada andmetega tutvumist. Tänapäevased suhtlusvahendid sisaldavad paratamatult ka teiste isikute andmeid ning näiteks grupiviisilise kuriteo puhul on need andmed vajalikud teiste toimepanijate, rollijaotuse või kuriteo asjaolude tuvastamiseks. Küsimus ei peaks seega olema selles, kas kolmandate isikute andmete olemasolu välistab juurdepääsu, vaid selles, kuidas tagada nende eesmärgipärane ja proportsionaalne kasutamine.

   Mõistame, et kolmandate isikute andmete töötlemine suurendab põhiõiguste riivet ja vajab selgeid tagatisi. Samas peaks leidtõendi kasutamine olema lubatud ka digitaalkeskkonnas, kui see avastatakse õiguspärase vaatluse käigus. Leiame, et digitaalse keskkonna puhul tuleks lähtuda samast loogikast nagu koha või asja läbiotsimisel. Lubamatu kalastamine peab olema välistatud, kuid õiguspärase toimingu käigus ilmnenud asjakohane tõend ei peaks muutuma lubamatuks üksnes põhjusel, et see puudutab muud kuritegu või kolmandat isikut.

Lugupidamisega

(allkirjastatud digitaalselt)

Igor Taro
siseminister