RAHANDUSMINISTEERIUM

proua Pakosta
Justiits- ja Digiministeerium
info@justdigi.ee
Suur-Ameerika 1
10122, Tallinn

Teie 29.05.2026 nr 8-3/4289-1,
JDM/26-0647/-1K

Meie 22.06.2026nr 1.1-11/2366-2

Kriminaalmenetluse seadustiku muudatuste väljatöötamiskavatsus (digitõendid)

Lugupeetud proua Pakosta

Kooskõlastame kriminaalmenetluse seadustiku muudatuste väljatöötamiskavatsuse (digitõendid) järgmiste tähelepanekutega.

Toetame vajadust suurendada õigusselgust ja oleme nõus, et kehtivat regulatsiooni tuleb ajakohastada kooskõlas EL Kohtu ja EIÕK praktikaga. Samas rõhutame, et põhiõiguste kaitse tugevdamine peab säilitama tasakaalu õiguskaitse tõhususega – digitaalsed tõendid on tänapäeval kesksed pea kõigis kuriteoliikides, sh salakaubanduses, maksukuritegevuses, sanktsioonirikkumistes ning narkootiliste ainetega seotud kuritegudes.

Peame põhjendatuks nõuet, et nutiseadmetes ja muudel andmekandjatel sisalduvatele andmetele juurdepääs eeldab üldjuhul kohtu eelnevat luba, kuid samas tuleb regulatsioonis arvestada menetluspraktika eripäradega. Näiteks on tüüpiline olukord andmekandjate äravõtmine isiku kinnipidamisel ilma eelneva planeerimiseta (nt riikliku järelevalve käigus avastatud kuriteokahtlus) ning sellistel juhtudel ei ole eelneva loa taotlemine objektiivselt võimalik. Isikul võib olla kaasas lukustamata või lukustatud nutitelefon ning praeguse praktika kohaselt on võimalik teha seadme vahetu vaatlus, et tuvastada kaasosalised, kauba liikumise asukohad või muud andmed, mis seovad isiku konkreetse kuriteoga. Kui tuleb oodata kohtu luba, võib telefon vahepeal automaatselt lukustuda või on võimalik andmed seadmes eemalt kustutada (nt „Leia minu iPhone“ või Google’i vastav teenus), mille tulemusel lähevad tõendid pöördumatult kaotsi.

Selle vältimiseks tuleks seadusesse luua mehhanism (analoogselt KrMS § 91 lg 5-ga), mis võimaldab uurimisasutusel kiireloomulistel juhtudel andmed koheselt kopeerida (nn „külmutada“) ilma neid sisuliselt läbi vaatamata, ning taotleda kohtu luba andmete analüüsimiseks tagantjärele (nt 24–72 tunni jooksul).

Planeeritud toimingute puhul (eelkõige läbiotsimine) ei ole loa taotlemine reeglina probleemne, kuid praktikas ei ole võimalik taotluses ammendavalt ette näha kõiki toimingute käigus leitavaid andmekandjaid ega kõiki andmeliike. Nutiseadmed sisaldavad väga erinevaid andmeid (nt kõnelogid, suhtlusrakendused, fotod, failid jms) ning tõenduslikult oluline teave

võib ilmneda alles seadme läbivaatamisel. Seetõttu peaks loa ulatus võimaldama koguda kõiki menetletava süüteoga seostatavaid asjakohaseid andmeid, mitte üksnes kitsalt eelnevalt määratletud andmeliike, kuna nende kohapealne selekteerimine ei pruugi olla tehniliselt võimalik.

Samuti on vaja selgust, kas läbiotsimisel (kohtu loal) leitud andmekandjate sisu töötlemiseks tuleb igal juhul taotleda kohtult täiendav luba. Nõue küsida iga üksiku seadme või iga andmeliigi kohta eraldi luba muudaks menetluse põhjendamatult aeganõudvaks. Eriti probleemne on see vahetu kinnipidamise järgselt, kus kiire ligipääs andmekandjatel sisalduvatele andmetele võib olla vältimatult vajalik tõendite säilitamiseks ning kaasosaliste tuvastamiseks. Lisaks tuleb regulatsioonis selgelt määratleda, kas kohtu loa nõue hõlmab üksnes nutiseadmeid (nt mobiiltelefonid, tahvelarvutid) või kogu IT-tehnikat laiemalt, sealhulgas arvuteid, mälupulki, väliseid kõvakettaid ja muid andmekandjaid.

Erandolukordadena tuleb eelkõige käsitleda juhtumeid, kus esineb vahetu oht inimese elule, tervisele või vabadusele, näiteks kui tegemist on kadunud või röövitud isikuga ning kahtlustatava seadmes võib sisalduda reaalajas teave kannatanu asukoha kohta. Sellisel juhul võib isegi lühiajaline viivitus tuua kaasa pöördumatuid tagajärgi. Samuti on põhjendatud erandi kohaldamine terrorismiohu või muude kõrgendatud ohutasemega juhtumite korral, kus on ohus isikute elu või võib toimuda rünnak elutähtsa taristu vastu.

Praktika näitab, et viivitus – sealhulgas kohtu või prokuratuuri loa ootamine – võib kaasa tuua andmete hävimise või kättesaamatuks muutumise ka sellistes menetlustes, mis eeltoodud raskusastme alla ei kuulu. Näiteks võib seade olla avatud ja kohe lukustuda, esineda oht andmete kaugkustutamiseks, tekkida vajadus viivitamatult katkestada võrguühendus, aku tühjenemisel kaduda ligipääs seadmele või aktiveeruda mehhanism, mis muudab andmed kättesaamatuks, samuti võib katkeda aktiivne sessioon või ligipääs pilveteenusele. Sellistes olukordades peaks regulatsioon võimaldama teha viivitamata minimaalsed vajalikud toimingud andmete säilitamiseks (sh kopeerimiseks) ja esmaseks hindamiseks tingimusel, et tegevus dokumenteeritakse ning sellele järgneb tagantjärele kontroll ja andmete edasiseks töötlemiseks loa taotlemine.

Ühe võimalusena võiks kaaluda, et erandi kohaldamise aluseks olevad kuriteoliigid on piiritletud KrMS § 126² lg 2 nn kataloogikuritegude sarnaselt, mis aitaks tagada erandi selguse ja ühtlase kohaldamise praktikas.

Erandite rakendamisel tuleb piirduda vältimatute toimingutega, mis on vajalikud andmete säilitamiseks ja esmaste asjaolude tuvastamiseks. Andmete edasine sisuline läbivaatamine ja kasutamine tõendina peab toimuma kohtu või prokuratuuri loa alusel.

Erand on vajalik ka juhtudeks, kus seadme omanik või seaduslik valdaja annab selgesõnalise ja teadliku nõusoleku andmete läbivaatamiseks. Sellisel juhul ei ole põhjendatud täiendava loa nõudmine, kui nõusolek on nõuetekohaselt vormistatud ja dokumenteeritud.

Lisaks e-postkastidele toimub praktikas päringute kaudu ka muude teenusepakkujate valduses olevate andmete kogumine. Näiteks küsitakse raamatupidamisandmeid raamatupidamistarkvara teenusepakkujalt, kes ei ole andmete omanik, kuid kellel on teenuse osutamise tõttu ligipääs kliendi andmetele. Sarnane olukord esineb ka GPS- või sarnaseid lahendusi pakkuvate ettevõtete puhul, kes näevad oma süsteemides sõidukite liikumistrajektoore ja muid teenusega seotud andmeid.

Kuna digitaalsed tõendid on kriminaalmenetluses kujunenud üheks peamiseks tõendiallikaks, on põhjendatud nende kogumise reguleerimine iseseisvalt, mitte üksnes läbiotsimise regulatsiooni laiendamise kaudu. Samas ei tohiks lähtuda eeldusest, et elektroonilisi tõendeid saab alati sündmuskohal (läbiotsimisel) või kogumise hetkel kitsalt ja käsitsi piiritleda. Seaduses peaks selgelt eristama esmast hindamist, mille eesmärk on tuvastada, kas konkreetne seade või andmeallikas võib olla menetluses asjakohane, ning sellele järgnevat sisulist läbivaatamist (eelneb andmete kopeerimine), andmete kasutamist ja hilisemat säilitamist, sealhulgas nende tutvustamist menetlusosalistele.

Seega vajaksid selgemat reguleerimist vähemalt järgmised olukorrad:
• nutitelefonide ja tahvelarvutite andmete säilitamine, kopeerimine ja läbivaatamine ning hilisem säilitamine ja tutvustamine;
• arvutite, väliste andmekandjate, NAS-ide (võrgu kaudu kasutatav andmesalvesti) ja serverite kopeerimine;
• tööpostkastide, funktsionaalsete postkastide ja isiklike postkastide eristamine;
• pilvekontode, sünkroonitud andmete ja aktiivsete sessioonide (avatud ja kasutuses olev konto või ühendus) kasutamine tõendite kogumisel;
• sõnumi- ja vestlusrakenduste ning sotsiaalmeedia kontode andmete kogumine (nt WhatsApp, Messenger, Facebook jms);
• kustutatud andmete, varukoopiate, cache'i (ajutiselt hoitav info), logide ja metaandmete (nt faili loomise aeg ja muud tehnilised andmed) kogumine;
• olukorrad, kus seadme või konto täpne sisu ja andmete asukoht selgub alles esmase analüüsi (triage'i) käigus.

Lugupidamisega

(allkirjastatud digitaalselt)
Jürgen Ligi
rahandusminister

Virge Aasa 58851493
Virge.Aasa@fin.ee

Anneli Valgma 58851315
Anneli.Valgma@fin.ee