EESTI ADVOKATUUR
ESTONIAN BAR ASSOCIATION

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

Teie 29.05.2026 nr 8-3/4289-1
Meie 16.06.2026 nr 1-8/26/70-1

Eesti Advokatuuri seisukohad KrMS muudatuste väljatöötamiskavatsuse (digitõendid) osas

Lugupeetud Liisa-Ly Pakosta

Täname, et olete advokatuurile arvamuse avaldamiseks edastanud KrMS muudatuste väljatöötamiskavatsuse (digitõendid). Esitame teile selle osas advokatuuri seisukohad.

Digitaalse andmekandja puhul ei seisne põhiõiguste riive peamine moment seadme äravõtmises, vaid eelkõige andmestiku sisulises läbivaatamises, mis võib hõlmata isiku kogu digitaalset elukäiku, sealhulgas aastatepikkust suhtlust, e-kirju, pilveandmeid, tervise- ja pangateavet, asukohaajalugu, advokaadisuhtlust, ajakirjandusallikate andmeid ning kolmandate isikute teavet. Selline sekkumine riivab intensiivselt nii eraelu puutumatust kui ka isikuandmete kaitset ning erineb olemuslikult füüsilise eseme leidmisest või äravõtmisest.

Kriminaalmenetluse seadustik ei sisalda detailset eriregulatsiooni e-postkastide, pilvekontode ega muude suuremahuliste digitaalsete andmekogumite läbivaatamise kohta. Euroopa Liidu Kohtu praktika, sealhulgas kohtuasjad C-548/21 (C.G. v Bezirkshauptmannschaft Landeck) ja C-746/18 (H.K. v Prokuratuur), rõhutavad, et elektroonilise side andmetele ja muule digitaalsele andmestikule juurdepääs peab olema allutatud tõhusatele menetluslikele tagatistele ning proportsionaalsuse ja vajalikkuse hindamisele. Samalaadseid põhimõtteid eraelu puutumatuse kaitsel ja riive õigustamisel kajastab ka Euroopa Inimõiguste Kohtu praktika, sealhulgas lahend Macharik v. the Czech Republic (51409/19).

Ka Riigikohus on rõhutanud lahendis RKKKo 18.06.2021 otsus nr 1-16-6179, et elektrooniliste andmete kogumisel ja läbivaatamisel tuleb arvestada erilise intensiivsusega põhiõiguste riivet ning tagada piisavad menetluslikud garantiid.

Samuti tuleb seaduse tasandil selgelt reguleerida, millistel tingimustel ja millises menetluskorras on lubatud kohustada isikut võimaldama juurdepääsu tema digiseadmes olevatele andmetele. See hõlmab nii biomeetriliste tunnuste (nt näotuvastus või sõrmejälg) kasutamist seadme avamiseks kui ka kohustust avaldada parool, PIN-kood või muu juurdepääsutunnus. Arvestades selliste meetmete intensiivset põhiõiguste riivet, ei saa nende kasutamine olla lubatud igas menetluses ega kõigi andmete puhul. Samas on võimalik seaduses

ette näha erandlikud ja selgelt piiritletud juhtumid, kus selliste meetmete kasutamine on põhjendatud. Selles kontekstis pakub olulist võrdlusmaterjali ka Euroopa Inimõiguste Kohtu lahend Minteh vs. Prantsusmaa (23624/20, 19.05.2026).

Keskne küsimus ei ole üksnes see, kas muuta läbiotsimise mõistet või luua eraldi regulatsioon, vaid see, kas digitaalset andmestikku käsitatakse seaduses kvalitatiivselt erineva objektina võrreldes füüsilise esemega. Põhjendatud on eraldi regulatsiooni loomine, mis tunnistab digitaalse andmestiku eripära ning sätestab selle läbivaatamiseks kõrgendatud nõuded. Samas ei tohi regulatsioon piirduda üksnes e-postkastide või üksikute tehniliste lahendustega. VTK-s toodud kitsas käsitlus, mis keskendub e-postkastile ja nutiseadmele, ei kajasta tegelikku olukorda, kus isiku jaoks oluline teave paikneb sageli hajusalt erinevates keskkondades ning on omavahel põimunud. Samavõrd kaitset vajavad pilve- ja serverilahendustes hoitavad failid, pildid, videod, sõnumirakenduste suhtlus ning varukoopiad. Seetõttu peab regulatsioon olema tehnoloogiliselt neutraalne ning hõlmama kõiki olukordi, kus menetleja saab ligipääsu isiku sisulisele andmestikule, sõltumata selle vormist või asukohast, ning e-postil ei ole põhjendatud eristaatust võrreldes muu digitaalse teabega.

Arvestama peab, et erinevalt füüsilistest esemetest kaasneb digitaalsete andmetega alati ulatuslikult metaandmeid. Nende abil on võimalik saada detailset teavet isiku eraelu kohta ning teha tema käitumise, harjumuste ja sidemete osas kaugeleulatuvaid järeldusi. Andmekaitse Inspektsioon on oma juhendmaterjalis selgitanud metaandmete olemust järgmiselt:

„*Lihtsustatult on metaandmed andmed, mis sisaldavad teavet muude andmete kohta. See on teave, mis tekib siis, kui kasutatakse erinevaid infotehnilisi lahendusi ja süsteeme ning mis annab teada, kes, mida, kus, millal ja kuidas tegi. Metaandmed tekivad ja talletatakse teenuste tarbimisel ja IT-protsesside käivitamisel väga mitmes punktis ja erinevatel tehnilistel tasemetel: (1) kasutaja enda arvuti, (2) organisatsiooni kohtvõrgu administreerija, (3) andmesides osalevad võrguseadmed, (4) internetiteenuse osutaja jpt. […] Seega iga kord kui inimesed suhtlevad, tekivad metaandmed. Saates teineteisele tekstsõnumeid, vesteldes veebis või helistades, tekib selle suhtluse kohta mingi teave, mis ei ole suhtlus ise*.“[1]

Selliste metaandmete kättesaadavus koos kaasaegsete otsinguprogrammide, tulevikus üha enam ka tehisintellekti ja suurandmete analüüsi võimekusega, loob võimaluse profileerida isiku käitumist ja liikumist aastakümnete taha. Algoritmide abil on andmekogumitest võimalik eraldada kindla asukoha, ajahetke, seose või muu parameetri alusel isikuga seotud asjaolusid, tuvastades ja rekonstrueerides fakte 10, 20 või isegi 30 aasta tagusest minevikust.

Ehkki teatud erakordselt raskete kuritegude puhul võib selline tagasiulatuv analüüs olla uurimise huvides põhjendatud ja vältimatu, on taoliste otsingute puhul alati vajalik läbi viia proportsionaalsuse test. Proportsionaalsuse põhimõte nõuab, et kui luba küsitakse konkreetse teo uurimiseks, peab ka andmete läbivaatuse ulatus ajaliselt ja sisuliselt olema rangelt piiritletud, mitte muutuma võimaluseks teostada isiku mineviku üldist ja piiramatut kontrolli. Seadus peab kehtestama normatiivsed piirangud ja menetluslikud garantiid, mis oleksid praktikas rakendatavad ka olukorras, kus andmetöötlusprogrammid ning tehisintellekti poolt pakutavad võimalused on üha kiiremas arengus.

Õiguslik regulatsioon peab selgelt eristama seadme või andmekandja valduse võtmist, andmete kopeerimist ja andmete sisulist läbivaatamist, kusjuures viimast tuleb käsitada iseseisva ja

[1] AKI juhis „Metaandmed ja privaatsus“, kättesaadav: https://www.aki.ee/sites/default/files/dokumendid/metaandmed.pdf

kõige intensiivsema põhiõiguste riivena. Kooskõlas Euroopa Kohtu praktikaga ei ole väga tundliku või ulatusliku digitaalse andmestiku puhul prokuratuur piisavalt sõltumatu kontrolliorgan, mistõttu peab sellise läbivaatamise lubamine üldjuhul kuuluma kohtule. Sõltumatu eelkontrolli nõuet rõhutavad nii lahendid C-548/21 ja C-746/18 kui ka Riigikohtu praktika. Erandolukorrad peavad olema kitsalt piiritletud ning nende kujundamisel on asjakohane lähtuda KrMS § 126^4 lg 3 regulatsioonist, mis võimaldab edasilükkamatutel juhtudel toimingu tegemist kohtuniku loal taasesitamist võimaldaval viisil ning nõuab kirjaliku loa vormistamist 24 tunni jooksul.

Lisaks peab regulatsioon terviklikult käsitlema meetme lubatavuse tingimusi, proportsionaalsuse põhimõtte järgimist ning tõhusaid õiguskaitsevahendeid juhuks, kui sekkumine on olnud õigusvastane. Oluline on arvestada enese mittesüüstamise privileegi toimega, eriti olukordades, kus isikut võidakse kohustada võimaldama juurdepääsu andmetele biomeetriliste tunnuste, näiteks näo või sõrmejälje abil, või avaldama paroole karistusähvardusel. Selliste meetmete lubatavus peab olema piiratud üksnes erandlike ja selgelt määratletud juhtumitega ning vastama rangetele põhiseaduslikele ja konventsioonipõhistele kriteeriumidele, mida peegeldab ka Euroopa Inimõiguste Kohtu praktika.

Samuti tuleb seaduses ette näha erireeglid kutsesaladuste ja muu privilegeeritud teabe kaitseks, sealhulgas advokaadisaladuse, arstisaladuse ja ajakirjandusallikate kaitse tagamiseks, ning arvestada kolmandate isikute õigustega olukordades, kus nende andmed satuvad menetlustoimingute esemeks. Regulatsioon peab ühtlasi katma olukorrad, kus uurimisasutus pääseb seadme kaudu ligi pilveteenustele või kasutajakontodele, mille andmed ei paikne füüsiliselt seadmes.

Kokkuvõttes peab uus regulatsioon lähtuma arusaamast, et digitaalse andmestiku sisuline läbivaatamine kujutab endast iseseisvat ja kõrge intensiivsusega põhiõiguste riivet, mille regulatsioon peab oma olemuselt lähenema pigem jälitustoimingutele kui tavapärasele läbiotsimisele. Samal ajal peab regulatsioon olema tehnoloogiliselt neutraalne ja terviklik, hõlmates kogu kaasaegset andmekeskkonda ning tuginema Euroopa Kohtu, Euroopa Inimõiguste Kohtu ja Riigikohtu praktikas kujunenud põhimõtetele, eeskätt sõltumatu eelkontrolli, proportsionaalsuse ja tõhusa põhiõiguste kaitse nõuetele.

Lugupidamisega

allkirjastatud digitaalselt

Imbi Jürgen
Esimees

Merit Aavekukk-Tamm 6979 253
merit.aavekukk-tamm@advokatuur.ee