EESTI ADVOKATUUR
ESTONIAN BAR ASSOCIATION

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

Teie 29.05.2026 nr 8-1/4286-1
Meie 11.06.2026 nr 1-8/26/74-1

Eesti Advokatuuri seisukohad KrMS, VTMS, ESS jt seaduste muutmise seaduse eelnõu osas (nn sideandmete eelnõu) osas

Lugupeetud Liisa-Ly Pakosta

Täname, et olete advokatuurile arvamuse avaldamiseks edastanud KrMS, VTMS, ESS jt seaduste muutmise seaduse eelnõu (nn sideandmete eelnõu). Advokatuur esitab teile üldised tähelepanekud eelnõu osas ning kokkuleppel lisana detailsema analüüsi eelnõu sätete kaupa.

1. Üldine hinnang eelnõu osas

Eelnõu on võrreldes varasemate versioonidega küll paranenud, kuid tekitab jätkuvalt mitmeid olulisi õiguslikke ja sisulisi küsimusi. Need puudutavad eelkõige säilitamiskohustuste ulatust, kohaldamise lävendeid, sõltumatu kontrolli olemasolu ning regulatsiooni kooskõla Euroopa Liidu õigusega.

Positiivsena tuleb esile tõsta loobumist varasemast üldisest sideandmete säilitamiskohustusest ning liikumist lahenduse poole, kus riik kasutab eelkõige andmeid, mida sideettevõtjad juba oma tegevuse käigus töötlevad ja säilitavad. See lähenemine vähendab võrreldes varasema regulatsiooniga põhiõiguste riive ulatust ning arvestab paremini Euroopa Kohtu praktikast tulenevaid nõudeid.

Samas jääb eelnõu mitmes keskse tähtsusega küsimuses probleemseks. Esiteks on mitmed säilitamiskohustuste ja andmete kasutamise aluseks olevad lävendid liiga madalad ega piirdu piisavalt selgelt raske kuritegevuse või tõsiste julgeolekuohtudega. Teiseks on korrakaitselised eesmärgid määratletud liiga laialt, võimaldades meetmete kohaldamist ka olukordades, mis ei õigusta nii intensiivset põhiõiguste riivet. Kolmandaks ei taga eelnõu piisavat sõltumatut eelkontrolli ning riigi julgeoleku erand ei ole piisavalt selgelt piiritletud. Nende puuduste tõttu tekivad tõsised küsimused regulatsiooni vastavuse kohta Euroopa Kohtu väljakujunenud praktikale.

2. Euroopa Kohtu praktikast tulenevad piirangud ja riigi julgeoleku erandi probleemid

Rõhutame, et Euroopa Kohtu praktikast tulenevad väga selged piirid sideandmete säilitamisele ja kasutamisele. Üldine ja vahet tegemata säilitamine on lubatav üksnes erandina riigi

julgeoleku kaitseks olukorras, kus esineb tõeline, tõsine ja ettearvatav oht, ning sedagi ajutiselt ja rangete tingimuste alusel (vt liidetud kohtuasjad C-511/18, C-512/18 ja C-520/18, La Quadrature du Net jt.). Lisaks peab selline meede alluma kohtu või sellega võrdsustatud sõltumatu asutuse eelkontrollile. Samuti on Euroopa Kohus rõhutanud, et liiklus- ja asukohaandmetele juurdepääsu saab õigustada üksnes võitluses raskete kuritegude vastu või avalikku julgeolekut ähvardava suure ohu ennetamisel ning see peab üldjuhul puudutama konkreetseid isikuid (C-746/18, H.K vs Prokuratuur).

Sellest lähtuvalt on problemaatiline eelnõus sisalduv lahendus, mille kohaselt saab riigi julgeoleku huvides lausalise sideandmete kogumise otsustada Vabariigi Valitsus. Euroopa Kohtu praktika kohaselt (liidetud kohtuasjad C-511/18, C-512/18 ja C-520/18, La Quadrature du Net jt) peab sellise otsuse tegema kohus või sõltumatu haldusorgan, milleks Vabariigi Valitsus kui täidesaatva võimu organ ei kvalifitseeru. Samuti on küsitav eelnõus sätestatud madal lävend („ohu ennetamine“) ning võimalus pikendada meetmete kohaldamist, mis võib viia erandi muutumiseni sisuliselt reegliks. Ka kuuekuuline periood on ebaproportsionaalselt pikk, eriti arvestades, et kriminaalmenetluses, kus uuritakse juba konkreetseid kahtlustusi, on jälituslubade kestus märkimisväärselt lühem.

Sihistatud säilitamise regulatsioon ESS § 111[1] alusel tekitab täiendavaid probleeme. Eelnõu võimaldab andmete säilitamist mitte ainult kriminaalmenetluse, vaid ka korrakaitselistel eesmärkidel, sealhulgas „korrarikkumise kõrvaldamiseks“. Selline lähenemine on jällegi vastuolus Euroopa Kohtu praktikaga, mis lubab andmete säilitamist ja kasutamist üksnes raskete kuritegude või tõsiste julgeolekuohtude korral. Korrakaitseline ohuennetamine hõlmab oma olemuselt ka väga madala kaaluga rikkumisi ning ei saa õigustada ulatuslikku põhiõiguste riivet. Sama probleem puudutab ka julgeolekualast lävendit, kus kasutatakse „ohu“ mõistet üldises tähenduses, mis ei vasta Euroopa Kohtu nõudele käsitleda üksnes eriti tõsiseid ohte riigi julgeolekule. Lisaks ei ole eelnõus ette nähtud piisavat sõltumatut eelkontrolli. Säilitamiskohustust saab kehtestada prokuratuuri, PPA või julgeolekuasutuse otsusega, mis ei vasta Euroopa Kohtu praktikas nõutud sõltumatu kontrolli standardile. Ka kohtuloa olemasolu ei lahenda iseenesest probleemi, kui materiaalõiguslikud lävendid on liiga madalad või ebaselged. Euroopa Kohtu praktika kohaselt peab ka kohtulik kontroll olema sisuline, mitte pelgalt formaalne, ning luba saab anda üksnes piisava raskusastmega juhtudel.

3. Säilitamise alused, mõisteprobleem ja juurdepääsu lävend

Eelnõu kõige haavatavamaks kohaks on mõiste „ärilisel eesmärgil säilitatavad andmed“, millele kogu regulatsioon üles on ehitatud. Kuigi eristus ärilistel ja seadusest tulenevatel põhjustel säilitatavate andmete vahel on kontseptuaalselt arusaadav, tunnistab ka seletuskiri, et praktikas ei pruugi nende kahe kategooria vahel alati selget piiri olla. Kui tulevikus ei ole võimalik usaldusväärselt kindlaks teha ega tõendada, millisel alusel konkreetseid andmeid säilitati, muutub kogu regulatsiooni keskne eeldus küsitavaks ning järelevalve selle üle oluliselt raskendatuks. Sellest tulenevalt võiks kaaluda, kas süsteem ei peaks veelgi selgemalt lähtuma põhimõttest, et lisaandmete kogumine ja säilitamine on lubatud üksnes erandjuhtudel ning selgelt määratletud ja põhjendatud õigusliku aluse olemasolul, mitte üldiseks ettenägemiseks või võimaliku tulevase vajaduse katmiseks.

Oluline on rõhutada ka seda, et kohtu loa olemasolu ei lahenda iseenesest kõiki Euroopa Kohtu praktikast tulenevaid probleeme. Euroopa Kohus ei ole keskendunud üksnes sellele, kes loa annab, vaid ka sellele, millistel sisulistel tingimustel tohib luba anda. Kohtulik kontroll ei tohi taanduda formaalseks kinnituseks. Juurdepääs liiklus- ja asukohaandmetele eeldab

materiaalõiguslikult piisavalt kõrget lävendit. Euroopa Kohus on kohtuasjas C 746/18 rõhutanud, et kuritegevuse vastu võitlemise eesmärgil peaks juurdepääs põhimõtteliselt piirduma nende isikute andmetega, keda kahtlustatakse raske kuriteo kavandamises, toimepanemises või sellega seotud olemises. Sellest tulenevalt peaks kohtul olema võimalik luba anda üksnes olukorras, kus tegemist on piisava raskusastmega kuritegevuse või sellega võrreldava ohuga. Vastasel juhul muutub kohtulik kontroll olemuslikult formaalseks.

Just samast lähtepunktist vaadatuna tekitab tõsiseid küsimusi sideandmete kasutamine väärteomenetluses ning korrakaitselistel eesmärkidel. Euroopa Kohtu praktikast ei nähtu, et liiklus- ja asukohaandmete kasutamist oleks võimalik põhjendada pelgalt üldise ohuennetuse, korrarikkumise kõrvaldamise või tavapärase haldusjärelevalve vajadusega. Sellised eesmärgid ei vasta sellele raskusastmele, mida Euroopa Kohus peab vajalikuks sellise intensiivse põhiõiguste riive õigustamiseks.

4. Andmekoosseis, seadmetunnused ja profileerimise risk

Sarnased küsimused tekivad ka ESS § 111² alusel nimetatud seadmetunnuste puhul. IMSI, IMEI, SUPI, SUCI ning muud võrguidentifikaatorid võivad praktikas võimaldada väga detailset seadmepõhist ja kaudselt ka isikupõhist profileerimist. Kuigi neid käsitletakse tehniliste andmetena, ei kõrvalda see nende potentsiaalset mõju isiku eraelu puutumatusele. Seetõttu vajab täiendavat põhjendamist nii sellise andmekoosseisu vajalikkus kui ka see, milliste konkreetsete meetmetega välditakse nende andmete kasutamist isiku käitumise, liikumismustrite ja suhtlusvõrgustiku detailseks profileerimiseks.

Eraldi tähelepanu väärib ka reaalajas asukoha tuvastamise regulatsioon. Liiklus- ja asukohaandmete põhjal on võimalik teha väga ulatuslikke ja täpseid järeldusi inimese eraelu, harjumuste, liikumiste, suhtlusvõrgustiku ja elustiili kohta. Mida lähemale liigub meede reaalajas jälgimisele, seda intensiivsem on põhiõiguste riive ning seda tugevamad peavad olema nii meetme põhjendus kui ka selle kohaldamise tingimused ja lävend. Sama tähelepanek kehtib ka Vabariigi Valitsuse määruse kavandis loetletud andmekoosseisu kohta. Kärjetunnused, tugijaamade asukohad, roaminguandmed, IP-aadressid ning sideseansside algus- ja lõpuaeg võimaldavad koos analüüsituna koostada inimese liikumisest ja suhtlusmustrist äärmiselt detailse ja tervikliku pildi. Seetõttu ei ole küsimus üksnes selles, kas andmeid säilitatakse, vaid ka selles, kui ulatuslikku isikuprofiili on nende andmete põhjal võimalik hiljem rekonstrueerida. Just see aspekt nõuab regulatsioonis eriti selget põhjendust ja ranget piiritlemist.

5. Andmekaitse nõuded, logimine ja andmesubjekti teavitamine

ESS § 112 regulatsioon tekitab olulisi küsimusi ka isikuandmete kaitse üldmääruse (IKÜM) valguses. Sideettevõtjad peavad tagama, et andmete töötlemine, sealhulgas edastamine, oleks seaduslik ja läbipaistev. Eelnõu võib aga panna nad olukorda, kus nad on sunnitud oma kohustusi rikkuma. Lisaks puudub piisav logimiskohustus sideettevõtja poolel, mistõttu ei ole hiljem võimalik kontrollida, milliseid andmeid, kellele ja millisel alusel edastati. See omakorda muudab andmesubjekti õiguste teostamise praktikas äärmiselt keeruliseks. Seetõttu võiks kaaluda, kas ka sideettevõtjal peaks olema kohustus säilitada teave selle kohta, milliseid andmeid, kellele ja millisel õiguslikul alusel väljastati. Lisaks on lahendamata andmesubjekti hilisema teavitamise küsimus. Kui inimene ei saa kunagi teada, et tema andmeid kasutati, muutub ka õigusvastase kasutamise vaidlustamine suuresti teoreetiliseks. Teavitamine peaks vajadusel olema küll edasilükatav, kuid põhimõtteliselt automaatne. Teavitamata jätmine peaks olema põhjendatud erand, mis allub sõltumatule kontrollile.

6. Andmete kasutamine teistes menetlustes

Oluline probleem on andmete hilisema kasutamise võimalus. Eelnõus tuleb selgelt välistada olukord, kus julgeoleku eesmärgil kogutud andmeid kasutatakse hiljem kriminaalmenetluses nn tagaukse kaudu. Kui sideandmeid kogutakse ja säilitatakse JAS-i alusel, tuleb välistada ka olukord, kus nende andmete kasutamiseks kriminaalmenetluses koostatakse teabehanke kokkuvõte, mida seejärel KrMS § 63 lõike 1^1 alusel riigi peaprokuröri loal käsitatakse kriminaalmenetluses tõendina. Samuti ei nähtu Euroopa Kohtu praktikast, et sideandmete kasutamine väärteomenetluses või tavapäraste korrakaitseliste ülesannete täitmisel oleks lubatav.

7. Andmete säilitamistähtaegadest

Tähelepanu väärib ka asjaolu, et väga erinevatele andmekategooriatele nähakse eelnõus ette ühesugune säilitamistähtaeg (ESS § 111^1 lg 5). Eelnõust ei nähtu seejuures selgelt, millistel objektiivsetel kriteeriumidel põhineb selline ühtne lähenemine ega miks peaksid eri laadi ja erineva tundlikkusega andmeliigid alluma samale säilitusperioodile. Arvestades, et andmekategooriate olemus ja nendest tulenev põhiõiguste riive intensiivsus võivad oluliselt erineda, eeldaks selline lahendus selget ja veenvat põhjendust.

Lugupidamisega

allkirjastatud digitaalselt

Imbi Jürgen
Esimees

Lisa:

Eelnõu sätete detailsed kommentaarid eelnõu failis

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