



## Kaitsepolitseiamet

Siseministeerium  
info@siseministeerium.ee

Justiits- ja Digiministeerium  
info.delta@justdigi.ee

Teie 01.06.2026 1-7/173-1  
Meie 15.06.2026 nr 3920-2

### Arvamus sideandmete säilitamise ja kasutamise eelnõule

Kaitsepolitseiamet toetab sideandmete säilitamise ja kasutamise probleemistiku terviklahendust. Oleme seisukohal, et regulatsioon peab võimaldama pädevatel asutustel kaitsta nii riigi julgeolekut kui avastada ja tõendada toime pandud kuritegusid. Seetõttu esitame eelnõu kohta järgmised olulisemad märkused ja ettepanekud. Konkreetsed sõnastusettepanekud oleme valmis esitama eelnõu edasistel aruteludel.

#### Terminite selgus

Kehtiva õiguse kohaselt käsitletakse sideandmete elektroonilise side seaduse (ESS) § 111<sup>1</sup> lõigetes 2 (telefon- ja mobiiltelefoni teenuse andmed) ja 3 (internetiühenduse ja elektronposti andmed) loetletud andmeid, mida sideettevõtjad peavad riigi jaoks säilitama. Rõhutame, et tegemist on side tehniliste ehk metaandmetega, mis kirjeldavad sideühenduse toimumist, mitte kõne, sõnumi või muu kommunikatsiooni sisu. Samuti ei tähenda nende andmete kasutamine reaajas jälgimist, vaid tegemist on nõ ajalooliste andmetega, mis võimaldavad analüüsida juba toimunud side sündmusi tagantjärele.

Sideandmed hõlmavad muu hulgas:

- infot selle kohta, kelle vahel side toimus (näiteks telefoninumbrid, IP-aadressid);
- side alguse ja lõpu aega ning kestust;
- kasutatud sidekanalit (kas tegemist on kõne, SMS, andmeside, internetiteenusega);
- sidepidamiseks kasutatud seadme või ühenduse tehnilisi tunnuseid;
- seadme või ühenduse ligikaudset asukohta side toimumise hetkel.

Õigusselguse ja Euroopa Kohtu ning Riigikohtu praktika ühetaoliseks rakendamiseks on vaja selgelt eristada:

- a) lõppkasutaja tuvastamist võimaldavaid andmeid ehk *subscriber data* – lihtsustatult öeldes on tegemist lepinguliste andmetega, kust nähtuvad telefoni või internetiühenduse teenuse numbri ja seadme omaniku andmed või muud tunnused;
- b) liiklusandmeid ehk *traffic data* – lihtsustatult öeldes on tegemist andmetega, kust nähtub, mis ajal konkreetne number helistas teisele numbrile;
- c) asukohaandmeid ehk *location data* – lihtsustatult öeldes on tegemist kärjeinfoga, kust selgub, millise mobiilimasti piirkonnas kõne alustati.

Kui kehtiv ESS käsitleb sideandmetena ka lepingulisi andmeid ehk telefoninumbrit ja omanikku, siis Euroopa Kohus ei ole selliste andmete säilitamise ja kasutamise kohta etteheiteid teinud. Euroopa Kohus käsitleb üksnes liiklus- ja asukohaandmete säilitamist ja kasutamist. Seetõttu toetame eelnõuga kavandatud ESS §-s 111<sup>2</sup> sätestatud lõppkasutaja tuvastamiseks vajalike

andmete eraldi reguleerimist, kuid vastav paragrahv peab võimaldama ka kõne või sõnumi vastuvõtja isikuandmete tuvastamist. Ei saa tekkida olukorda, kus pädev asutus saab õiguslikult tuvastada ainult helistaja telefoninumbri omanikku, kuid ei saa kontrollida, kellele kuulub kõnet või sõnumit vastuvõttev number.

Samuti leiame, et ESS-is ja kriminaalmenetluse seadustikus (KrMS) tuleb sideandmete kontekstis kasutada ühesuguseid termineid. Kehtivas KrMS § 90<sup>1</sup> lõikes 1 ja eelnõus KrMS § 90<sup>1</sup> pealkirjas kasutatakse sõnastust „identifitseerimistunnustega seotud andmed“. Seevastu kavandatud ESS muudatustes on kasutusel „lõppkasutaja tuvastamiseks vajalikud andmed“. Olukorras, kus mõeldakse samu andmeid, tuleb terminid ühtlustada. Kaitsepolitseiameti ettepanek on kasutada „lõppkasutaja tuvastamiseks vajalikud andmed“.

### **Sideandmete säilitamine ja kasutamine riigi julgeoleku eesmärgil**

Kaitsepolitseiamet on seisukohal, et Eesti Vabariigi põhiseaduse (PS) ja Euroopa Liidu aluslepingu artikli 4 lõikega 2 („riigi julgeoleku kaitse on iga liikmesriigi ainuvastutuses“) on kooskõlas sideoperaatorite poolt kõigi nende klientide ja teenuse kasutajate sideandmete (nii kliendi andmed kui liiklus- ja asukohaandmed) üldine ja ühetaoline säilitamine. Põhiõiguste kaitse kontekstis on oluline reguleerida nendele andmetele juurdepääs, sest üksnes sideandmete analüüsist on võimalik teha järeldusi isiku suhtluse kohta. Olukorras, kus sideandmeid säilitavad sideettevõtted enda süsteemides ja riigi poolt neid ei töödeldaks, on põhiõiguste riive minimaalne ning võimalike kuritarvituste vältimiseks peavad sideettevõtted järgima e-privaatsuse direktiivis sätestatud nõudeid (direktiiv 2002/58/EÜ, artiklid 4–6, 9).

Leiame, et Eesti Vabariigi iseseisvus, sõltumatus ja territoriaalne terviklikkus on ülekaalukad põhjendused, et tagada üldine ja ühetaoline sideandmete olemasolu.

Euroopa Kohus on 2020. aasta lahendis La Quadrature du Net jt (C-511/18, C-512/18 ja C-520/18) leidnud, et riigi julgeoleku kaitse eesmärgil on kooskõlaseadusandlikud meetmed, kus elektroonilise side teenuse osutajatele tehakse ettekirjutus säilitada liiklus- ja asukohaandmeid üldiselt ja vahet tegemata olukordades, kus asjaomane liikmesriik seisab silmitsi riigi julgeolekut ähvardava suure ohuga, mis osutub tõeliseks ja vahetuks või ettearvatavaks (p 168). Taoline kohtu seisukoht ei arvesta aga Venemaa Föderatsiooni (VF) sõjalisest doktriinist tulenevate pikaajaliste eesmärkidega. Tuleb arvestada, et VF on varasemalt initsieerinud mitmeid mõjutustegevuse operatsioone (sh erinevad katsed mõjutada valimistulemusi) ja agressiooni rünnakuid (nt Gruusia 2008, Ukraina 2014), mis 24.02.2022 eskaleerus Ukrainas täiemahuliseks sõjategevuseks ja kestab jätkuvalt. Olukorras, kus VF on sõjaliselt rünnanud Ukrainat ja pannud toime erinevaid hübriidrünnakuid Euroopas, on äärmiselt oluline mõista, et VF-ist lähtuv oht on pikaajaline, kus kasutatakse erinevaid meetodeid oma eesmärkide saavutamiseks. Eesti julgeolekupoliitika alustes<sup>1</sup> on märgitud, et VF on Eestile ja Euroopale eksistentsiaalne oht. Kaitsepolitseiameti ülesanne on kaitsta Eesti põhiseaduslikku korda ja julgeolekut ning nende ülesannete täitmiseks on vaja tagada ühetaoline ja üldine sideandmete olemasolu. Igasugune muude kriteeriumite alusel, nt geograafilised piirkonnad, isikute või ametialade loetelude põhine andmete säilitamine läheb meie hinnangul vastuollu PS §-s 12 sätestatud võrdsuse põhimõttega. Ühtlasi annab nõ sihistatud või geograafiline säilitamine vaenulikele välisriigile võimaluse planeerida enda tegevusi selliselt, et nende tegevused ei jääks sideandmete säilitamise kohustuse alla.

Juhul, kui seadusandja soov on loobuda seadusest tulenevast üldisest sideandmete säilitamiskohustusest ja kehtestada riigi julgeoleku eesmärgil andmete säilitamine Vabariigi Valitsuse korraldusega (eelnõu ESS § 111<sup>3</sup>), on kaitsepolitsei ettepanek sätestada vastava Vabariigi Valitsuse korralduse tähtjaks kaks aastat, mida on võimalik kahe aasta kaupa pikendada. Eesti julgeolekukeskkonda hindab kõige kõrgemal tasemel Riigikogu heakskiiduga dokument Eesti julgeolekupoliitika alused. Dokumendi julgeolekukeskkonna kirjeldus tugineb mh julgeolekuasutuste ohuhinnangutele, mida on viimastel aastatel koostatud kahe-kolme aastase

---

<sup>1</sup> Riigikogu poolt heaks kiidetud 10.06.2026.

välbaga. Meie hinnangul annab 2-aastane tähtaeg ka sideettevõtetele kindluse, et nad ei pea näiteks iga 3 või 6 kuu tagant tegema arendusi, mis on seotud andmete säilitamise ja mitte-säilitamise sisse-välja lülitamisega. Tuleb arvestada, et tekkinud kulud kantakse edasi riigile.

### **Sideandmete säilitamine ja kasutamine raske kuritegevuse vastase võitluse eesmärgil**

Kaitsepolitseiamet on seisukohal, et uurimisasutused ei tohiks sideandmete puhul kuritegevuse vastases võitluses sõltuda sideettevõtete ärielistest eesmärkidest. Tuleb arvestada, et sideettevõtete äriks ei ole andmete säilitamine, mistõttu seadusest tuleneva kohustuse puudumisel ei pruugita enam andmeid säilitada või säilitatakse oluliselt vähem andmeid ja lühema tähtaja jooksul. Samuti tuleb arvestada, et Eestis on kolm suuremat sideettevõtet, kelle peakontorid ei asu Eestis. Seadusest tuleneva andmete säilitamise kohustuse puudumine annab peakontoritele võimaluse kulude kokkuhoiu eesmärgil loobuda ärielistel eesmärkidel andmete säilitamisest. Samuti on oht, et erinevad ettevõtted säilitavad erinevaid andmeid ning erineva tähtaja jooksul. Taoline killustatud lahendus ei taga uurimisasutustele süütegude menetlemiseks ja tõendamiseks vajalikke andmeid. Seeläbi ei kannata mitte ainult kurjategijate tabamine, vaid kahjustada saavad ka kannatanute õigused, sest tulevikus võib teatud kuritegude lahendamine ja süüdlaste tabamine sõltuda sellest, millise sideettevõtte klient oli kahtlustatav ja/või kannatanu. Kaitsepolitseiameti hinnangul läheb taoline olukord vastuollu PS §-s 12 sätestatud võrdsuse põhimõttega. Seetõttu teeme ettepaneku kehtestada ESS-s ka kuritegevuse vastase võitluse eesmärgil sideandmete säilitamise kohustus.

Raske kuritegevuse vastase võitluse eesmärgil andmete säilitamist võimaldavad ka Euroopa Kohtu otsused. Ka eelnevalt viidatud 2020. aasta lahendis La Quadrature du Net jt leidis kohus, et lubatud on: „seadusandlikud meetmed, mis näevad ette riigi julgeoleku kaitsmise, raskete kuritegude vastu võitlemise ja avalikku julgeolekut ähvardava suure ohu ennetamise eesmärgil liiklus- ja asukohaandmete eesmärgipärase säilitamise, mis on objektiivsete ja mittediskrimineerivate asjaolude alusel piiritletud vastavalt andmesubjektide kategooriatele või geograafilise kriteeriumi põhjal ja ajaliselt piiratud tingimata vajalikuga, kuid mida on võimalik pikendada“ (p 168).

Kaitsepolitseiamet on seisukohal, et raske kuritegevuse vastase võitluse eesmärgil tuleb liiklus- ja asukohaandmeid säilitada järgmiste kriteeriumite põhjal:

- 1) Eesti riigipiiri piirkonnas (kuni 10 km) ja saartel asuvate tugijaamade leviala andmed;
- 2) riigikaitseobjektide ja teatud elutähtsate teenuste osutajate piirkonnas asuvate tugijaamade leviala andmed;
- 3) kuritegevuse statistika alusel põhjendatud piirkonnas asuvate tugijaamade leviala andmed;
- 4) anonüümse ettemakstud kõnekaardi sideteenuse andmed;
- 5) välisriigi abonendi rändlusteenuse kasutaja andmed.

Punktides 1–3 nimetatud kriteeriumid määratakse kindlaks Politsei- ja Piirivalveameti ja Kaitsepolitseiameti või siseministri ettepanekul Vabariigi Valitsuse poolt ning punktides 4 ja 5 nimetatud andmete puhul kehtib seadusest tulenev kohustus.

Kaitsepolitseiameti hinnangul on raske kuritegevuse vastase võitluse eesmärgil sideandmete säilitamiseks ja kasutamiseks õigusliku aluse loomine suurema ühiskondliku hüvega kui näiteks eelnõus sätestatud andmete säilitamine konkreetse menetluse tarbeks (§ 111').

### **Juurdepääs sideandmetele**

Arvamuse avaldamiseks saadetud eelnõu versioonis ei ole enam sätteid, mis reguleerisid, kellele peavad sideettevõtted andmeid edastama. Kuigi päringute õiguspärasuse eest vastutab päringu tegija, on õigusselguse huvides põhjendatud sätestada ESS-s asutused, kellele sideettevõtte peab andmeid avaldama. Pädevate asutuste välja toomine ESS-s annab sideettevõtetele selguse, kes ja mis seaduse kohaselt võivad neilt andmeid pärida. Samasugune põhimõte on

kirjas krediidasutuste seaduses (KAS § 88). Arvestades asutuste ülesandeid ja sideandmete olulisust nende ülesannete täitmisel, tuleks ESS-s kindlasti sätestada teabe andmise kohustus:

- 1) uurimisasutusele, jälitusasutusele, prokuratuurile ja kohtule kriminaalmenetluse seadustiku kohaselt;
- 2) julgeolekuasutusele julgeolekuasutuste seaduses sätestatud ülesannete täitmiseks ning riigisaladuse ja salastatud välisteabe seaduses nimetatud julgeolekukontrolli teostamiseks;
- 3) kohtule kohtumenetlust reguleerivates seadustes ettenähtud juhtudel ja korras.

Kokkuvõttes oleme seisukohal, et arvamuse avaldamiseks saadetud eelnõu vajab oluliselt muutmist ja täiendamist. Arvestades kohtupraktikast tulenevaid piiranguid sideandmete kasutamisele kriminaalmenetlustes on ennekõike vaja kiiret lahendust, et sideandmeid oleks võimalik tõendina kriminaalmenetlustes kasutada.

Lugupidamisega

(allkirjastatud digitaalselt)

Margo Palloson  
peadirektor