

HUAWEI SEISUKOHT VABARIIGI VALITSUSE MÄÄRUSE EELNÕULE

1. Huawei seisukohtade sissejuhatus ja kokkuvõte

- (1) Väliskaubandus- ja infotehnoloogiaminister algatas 15.11.2019 eelnõu Vabariigi Valitsuse 22. juuni 2006. a määruse nr 140 „Nõuded sideteenuse osutamisele ja sidevõrkude tehnilised nõuded“ muutmiseks (edaspidi: **Määruseelnõu**). Vabariigi Valitsus (edaspidi: **Valitsus**) andis huvirühmadele võimaluse oma Määruseelnõud puudutavate seisukohtade esitamiseks kuni 20.12.2019.
- (2) Huawei Technologies Oy (Finland) Co. Ltd (edaspidi: **Huawei**) soovib esmalt valitsust seisukohtade esitamise võimaluse eest tänada. Huawei on Soome õiguse alusel asutatud äriühing ja kuulub suuremasse Huawei kontserni.¹
- (3) Eesti kõrgtehnoloogiline võimekus on Huawei hinnangul mõjuvatel põhjustel väga muljet avaldav. Eesti on aluseks aina kasvavale arvule digitaalsetele edulugudele nagu Skype, Transferwise ja Bolt, aga ka uuenduslikele e-valitsuse teenustele. Telekommunikatsioonitehnoloogia valdkonnas esirinnas olemine on riigi majandusele palju kasu toonud. Huawei on uhke, et on Eesti operaatorite tehnoloogiapartner.
- (4) Seletuskirjast lähtuvalt on Määruseelnõu eesmärk riigi julgeoleku ja küberturvalisuse tagamine. Huawei on küberturbe tagamisele pühendunud ning väljendab heameelt Eesti Vabariigi Valitsuse sarnase suhtumise üle. Kõnealuses kontekstis on Huawei Euroopa Liidus asutatud äriühinguna pühendunud Euroopa Liidus kehtivate õigusaktide järgimisele. Küberturvalisuse kontekstis teeb Huawei koostööd erinevate ELi liikmesriikidega, et tagada Huawei toodetavate seadmete vastavus erinevates ELi liikmesriikides kehtivatele küberturvalisust puudutavatele kõrgetele standarditele.
- (5) Määruseelnõu praegusest sõnastusest lähtudes, ei panusta Huawei hinnangul Määruseelnõu küberturvalisuse tagamise ning Määruseelnõuga hetkel kavandatava mehhanismi kasutuselevõttu tuleks uuesti hinnata. Huawei'le valmistab muret asjaolu, et juhul, kui valitsus otsustab Määruseelnõuga jätkata eelnõu praeguses sõnastuses, oleks tegemist kahjuliku ülereguleerimisega, millel võivad olla olulised negatiivsed tagajärjed telekommunikatsiooniturule, muu hulgas tagajärjed, mis on seotud toimimise järjepidevusega, õigusliku raamistiku ja majanduslikke tagajärgedega, mille lõpptulemusena lakkaks Eesti telekommunikatsiooniturg toimimast. Mittetoimiv turg, mille sidusrühmadel puudub selgus ning kus konkurents on oluliselt moonutatud, viib omakorda innovatsioonipuuduseni, sealhulgas puuduks turvalisust ja töökindlust parendav innovatsioon. Kõik see päädiks madalama turvalisustaseme ning suuremate kuludega seotud telekommunikatsioonivõrguga, mis võib, tuginedes Määruseelnõu praegusele sõnastusele, lõppkasutajatele vastuvõetamatuks osutada.
- (6) Lisaks eelnevale oleme käesoleva aasta jooksul Eestis toimunud avaliku arutelu põhjal mures, et Määruseelnõu eesmärk võib olla välise surve tõttu Huawei turult kõrvaldada. Ühe olemasoleva tootja turult väljatõrjumine avaldaks Eestile märkimisväärset negatiivset majanduslikku mõju. See negatiivne majanduslik mõju võib ulatuda 300 miljoni euroni. Telekommunikatsioonisektori ülereguleerimise tagajärjed võivad järgnevatel aastatel olla veelgi suuremad.
- (7) Selles kontekstis on Huawei esitanud oma Määruseelnõu tagajärgi ja puudujääke käsitlevad seisukohad ning soovib valitsusele tungivalt kõiki sidusrühmi kaasava suhtluskanali loomist.
- (8) Kokkuvõttes esitab Huawei järgnevad seisukohad:

¹ www.huawei.com/en/

- a. **Õigusaktist tulenevate nõuete sobivus** – Määruseelnõu eesmärk on kehtestada meetmed üldkasutatava elektroonilise side võrgu turvalisuse ja riigi julgeoleku huvidel vastavuse tagamiseks. Praegusel kujul ei võimalda Määruseelnõu anda ühtegi riigi julgeolekut puudutava hinnangut ning võib hoopis võrkude turvalisust, ja seega ka riigi julgeolekut, negatiivselt mõjutada.

Määruseelnõuga soovitakse kehtestada kuni 120 tööpäeva (ca 5,6 kuud) kestev kooskõlastusmenetlus, mis viiakse läbi mis tahes sidevõrgu riist- ja tarkvara suhtes enne kõnealuse riist- ja tarkvara kasutusele võtmist. Elutähtsa teenuse osutamise ootamatu katkestuse korral, näiteks 27. oktoobril Võrus elektrivõrgu toimimisega juhtunu korral, peavad sideettevõtjad olema suutelised kiiresti reageerima, et tagada sidevõrgu toimimise turvalisus ning kõnealuste võrkudega ühendatud muude elutähtsate teenuste toimimise turvalisus. Eespool kirjeldatud kooskõlastusmenetlus ei võimalda võrguettevõtjatel tagada sidevõrkude toimepidevust, vastupidavust ja toimimise turvalisust, mõjutades seega negatiivselt riigi julgeolekut.

Hetkel kehtivate õigusaktide põhjal saavutatakse riigi julgeoleku huvide kaitse ning küberturvalisus avastatud turvaaukude kiire kõrvaldamisega, mis on võimalik tänu ettevõtjate ja telekommunikatsiooniseadmete tootjate koostööle. Praegusel kujul takistaks Määruseelnõuga kavandatav vajalikku kiiret reageerimist.

Lisaks, kuna Määruseelnõu alusel nõutav teave võimaldaks tuvastada üksnes telekommunikatsiooni riist- ja tarkvara tootja ning riistvara põhilise kasutusviisi, pole kõnealuse teabe põhjal võimalik teha järeldusi selle kohta, kas telekommunikatsiooniseade või tarkvara on turvaline ja töökindel ning sellest lähtuvalt ka riigi huvidel kooskõlas.

Riketega riist- ja tarkvara kasutamine ei saa olla kooskõlas riigi huvidel, olenemata kõnealuse riist- või tarkvara tootjast. Eeltoodust saab järeldada, et praegusel kujul pole Määruseelnõu sobiv vahend eelnõus sätestatud eesmärkide saavutamiseks.

Telekommunikatsioonivõrkude ettevõtjatele on seadmeid ja tarkvaratootjaid valides juba praegu tähtsad nii töökindlus kui ka küberturvalisus. Seega, toimiva turumajanduse tingimustes tagab konkurents erinevate sidusrühmade vahel selle, et parimad ja kõrgeima turvalisusastmega seadmetüübid leiavad kasutust telekommunikatsioonivõrkudes. Seega, Määruseelnõu peab vältima sideturu vaba konkurentsi häirivate mehhanismide kehtestamist ning seda nõuab ka elektroonilise side seaduse (edaspidi: ESS)² § 87 lõike 1 punktis 11 sätestatu.

- b. **Vähemkoormavate ja mõõdukamate meetmete olemasolu** - ESS § 87 lõike 2 punkt 4 annab valitsusele volituse võtta vastu määramisi, et kehtestada tehnilised nõuded, mis on vajalikud ESS § 87 lõikes 2 sätestatud eesmärkide saavutamiseks, nt riigi julgeoleku tagamiseks. Kõnealuste tehniliste nõuete kehtestamisele peab eelnema nõuete vajalikkuse kontroll vastavalt § 87 lõike 2 punktile 4. Määruseelnõu praegune sõnastus ja eelnõu seletuskiri ei sisalda teavet selle kohta, kas Määruseelnõus kirjeldatud meetmed on läbinud kõnealuse vajalikkuse kontrolli. Vastuoluline on sealjuures ka asjaolu, et seletuskirja viited riigi julgeolekule mainivad ühtlasi elutähtsaid teenuseid, mille suhtes juba kehtivad õigusaktidega sätestatud nõuded, muu hulgas hädaolukorra seaduse ja küberturvalisuse seadusega kehtestatud nõuded. Eespool toodust saab järeldada, et analüüsitud pole seda, kas olemas on muid meetmeid, mis sobiksid paremini valitsuse vajadustega ning oleksid vähem koormavad ja mõõdukamad turule

² Elektroonilise side seadus, RT I, 13.03.2019, 47. Arvutivõrgus: <https://www.riigiteataja.ee/akt/113032019047>

avaldatava mõju poolest. Eeltoodust tulenevalt saab väita, et Määruseelnõu on vastuolus oma delegatsiooninormiga, mis tuleneb ESS § 87 lõike 2 punktist 4.

- c. **ELi tasandi küberturvalisuse ja telekommunikatsiooniga seonduvate õiguslike arengute kõrvalejätmine** – määruseelnõus pole esitatud analüüsi või seisukohti ELi hõlmavate telekommunikatsioonisektori digitaalse turvalisuse suurendamiseks juba kasutusele võetud meetmete kohta, eelkõige NIS direktiivist³ ja ELi telekommunikatsioonisektori õiguslikust raamistikust, muu hulgas direktiivist 2002/20/EÜ⁴ (loadirektiivist) ja direktiivist (EL) 2018/1972⁵ (Euroopa elektroonilise side seadustikku kehtestavast direktiivist) tulenevate meetmete kohta. Kuna Määruseelnõu ja Määruseelnõu seletuskiri toovad välja selge seose sideteenuste osutamise, elutähtsate teenuste ja riigi julgeoleku vahel, peab Määruseelnõus ühtlasi arvestama juba kehtestatud ELi hõlmavate meetmetega, millega reguleeritakse vastavaid telekommunikatsiooniteenuste aspekte.
- d. **Ebapiisav üleminekuperiood** – Määruseelnõu jõustub 6-kuulise üleminekuperioodi möödumisel. 5G võrgud on ehitatud olemasolevatele 4G võrkudele, mis tähendab, et 5G võrke ettevalmistavate investeeringutega on juba alustatud ning see on kestnud mitmeid aastaid. 6-kuuline üleminekuperiood on ebapiisav selleks, et turul vajalikud muudatused teha, kuna sellega kaasneks viimase kümnendi jooksul tehtud oluliste investeeringute mahakandmine. Määruseelnõuga hetkel ettenähtud ajakava ei võimaldaks ka arvesse võtta teisi ELi tasandi arenguid, näiteks ELi „Toolbox“.
- e. **Mõjuanalüüsi puudumine** – Määruseelnõu koostamisel pole tehtud tegelikult arvestavat mõjuanalüüsi. Seletuskirja praeguses sõnastuses on väidetud, et „eelnõul ei ole puutumust Euroopa Liidu õigusega“. Samas on peaaegu igas seletuskirja peatükis toodud viiteid ELi õigusele ja erinevatele ELi tasandi tegevustele. Eeltoodust olenemata pole Määruseelnõuga kavandatud kooskõlas ELi õiguse üldpõhimõtetega ega ka Määruseelnõu seletuskirjas viidetud EL dokumentides kirjeldatud lähenemisviisiga.

Selguse mõttes tuleb märkida seda, et ELi õigus võimaldab valitsusel EL õigusest läbi erandite kõrvale kalduda, muuhulgas, et tagada avalik kord või julgeolek, kuid asjakohaste kohtulahendite põhjal on selge, et kõnealuseid erandeid tuleb tõlgendada ELi õiguse alusel ning Euroopa Liidu põhiõiguste hartaga sätestatud põhiõiguste kontekstis⁶, arvestades muu hulgas õigust omandile (artikkel 17), ettevõtlusvabadust (artikkel 16) ja diskrimineerimise keeldu (artikkel 20). Asjakohast analüüsi pole tehtud.

Määruseelnõu tooks turuosalistele kaasa kulude olulise suurenemise, mis omakorda kanduks üle lõppkasutajale. Seda pole samuti arvestatud. Määruseelnõul on oluline mõju hetkel kasutusel olevatele telekommunikatsioonivõrkudele, mis toob turuosalistele kaasa kulude olulise suurenemise. Seletuskirjas nenditakse, et „teatavate kulude“, mis sideettevõtjatele tekkida võivad, suurust pole võimalik ette ennustada. Huawei

³ EUROOPA PARLAMENDI JA NÕUKOGU DIREKTIIV (EL) 2016/1148, 6. juuli 2016, meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus.

⁴ Euroopa Parlamendi ja nõukogu 7. märtsi 2002. aasta direktiiv 2002/20/EÜ elektrooniliste sidevõrkude ja -teenustega seotud lubade andmise kohta (loadirektiiv). Arvutivõrgus: <https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32002L0020>

⁵ Euroopa Parlamendi ja nõukogu 11. detsembri 2018. aasta direktiiv (EL) 2018/1972, millega kehtestatakse Euroopa elektroonilise side seadustik (uuesti sõnastatud), EMPs kohaldatav tekst. Arvutivõrgus: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2018.321.01.0036.01.ENG

⁶ Euroopa Liidu põhiõiguste harta. Arvutivõrgus: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12012P/TXT>

hinnangu kohaselt oleks otsene mõju Eesti majandusele on peaaegu 300 miljonit eurot. Näiteks Huawei juba kasutuses olevate seadmete väljavahetamine läheks maksma umbes 150 miljonit eurot. Lisaks, pole välistatud, et valitsusel tuleks kõnealused kulud hüvitada, kuna ettevõtjad peavad antud kulutused tegema valitsusese tegevusest tulenevatel põhjustel.

Seletuskirjas tuuakse välja ka see, et kavandatavast õigusaktist tulenevalt on vajalik eelarvet suurendada ühe inimese palgakulu võrra. Määruseelnõuga kaasnev halduskoormus oleks oluliselt suurem sellest, mis on jõukohane ühele ametnikule. Seega, eeldusel, et suurenenud halduskoormus jääb ühe ametniku kanda, muutub mis tahes turvalisuse hindamise mudeli loomine ebamõistlikuks. See viitab omakorda asjaolule, et Määruseelnõu ei võimalda valitsusel saavutada oma eesmärki, milleks on riigi julgeoleku suurendamine.

- f. **Vastutuse piiritlemine** – puudub selgus telekommunikatsiooniettevõtjate ja seadmete tootjate vastutuses valitsuse kooskõlastustega tark- või riistvara puudutavate turvaintsidentide puhul. Määruseelnõus on esitatud Tarbijakaitse ja Tehnilise Järelevalve Ameti (edaspidi: **TTJA**) „tehnilise dokumentatsiooni kooskõlastamise“ mudel. See mudel hägustab vastutuse tegelikku jaotumist sidusrühmade vahel, täpsemini järelevalveorgani ja ettevõtjate vahel, aga ka erinevate ametiasutuste vahel (näiteks TTJA ja Riigi Infosüsteemi Ameti vahel). Seega, üheselt tuleb kindlaks määrata vastutuse jaotus ja kõiki asjassepuutuvaid sidusrühmi hõlmav kooskõlastamise mehhanism.
- g. **Kaubanduse ja konkurentsi moonutamine** – arvestades suuremate telekommunikatsiooniseadmete müüjate väikest arvu, siis juhul, kui Määruseelnõu tulemusel välistatakse praktikas konkreetne tootja, oleks selle mõju telekommunikatsiooniseadmete tootjate turu konkrentsile märkimisväärne. Lisaks võimendaks seda veelgi 6-kuuline periood, mis kulub seadmete ja tarkvaratootjate väljavahetamisele, mille tulemusel suureneksid sideettevõtjate seadmete väljavahetamisele tehtavad kulutused ja väheneks konkrents telekommunikatsiooniseadmete tootjate vahel. Kokkuvõttes võib see viia turu jagamiseni, mis takistaks kaupade ja teenuste vaba liikumist ELi siseturul.

(9) Huawei on eespool esitatud väidete kohta käivad täpsemad seisukohad esitanud allpool (punkt 2 ja järgnev).

(10) Eeltoodule tuginedes on selge, et riigi julgeoleku tagamiseks on vajalik teistsugune lähenemine. Huawei hinnangul oleks Määruseelnõu vastu võtmine kahjulik ülereguleerimine. Selle asemel, kui valitsus soovib kehtestada läbivaatusmehhanismi, soovitame valitsusel jätkata dialoogi telekommunikatsioonisektori osalejatega ning teiste asjaomaste sidusrühmadega, eesmärgiga leida faktidel põhinev lähenemine, mille puhul faktid on kontrollitavad ja kontroll põhineb ühistel standarditel, nagu näiteks *Network Equipment Security Assurance Scheme*⁷ (eesti k: Võrguseadmete Turvalisuse Tagamise Skeem), mis määratakse ühiselt 3GPP ja GSMA organisatsioonide poolt. Valitsus peab tagama, et mis tahes läbivaatusmehhanism on läbipaistev ja mõistlikult tõhus.

2. Õigusaktist tulenevate nõuete sobivus

(11) Määruseelnõuga kehtestatakse kuni 120 tööpäeva kestev kooskõlastusmenetlus, mis koosneb järgnevast:

⁷ Arvutivõrgus: <https://www.gsma.com/security/network-equipment-security-assurance-scheme/>.

- a. Enne telekommunikatsioonivõrgu riist- ja tarkvara kasutusele võtmist peab telekommunikatsiooniettevõtja esitama TTJale kooskõlastamiseks sidevõrgu riist- ja tarkvara tehnilise dokumentatsiooni.
- b. TTJA edastab vastava teabe julgeolekuasutustele ning Riigi Infosüsteemi Ametile. Kõnealused asutused annavad oma arvamuse, kas sidevõrgu riist- ja tarkvara kasutusele võtmine vastab riigi julgeoleku huvidele, 30 tööpäeva jooksul arvamuse küsimisest arvates.
- c. Vajaduse korral küsib TTJA Vabariigi Valitsuse julgeolekukomisjoni küberjulgeoleku nõukogu põhjendatud ettepanekut. Kõnealune nõukogu esitab oma põhjendatud ettepaneku 60 tööpäeva jooksul ettepaneku küsimisest arvates.
- d. Punktis b kirjeldatud julgeolekuasutuse või punktis c kirjeldatud nõukogu arvamuse saamisel otsustab TTJA seadmete kasutamiseks vajaliku kooskõlastuse andmise 30 tööpäeva jooksul.

(12) Olenevalt sellest, kas TTJA edastab esialgse taotluse julgeolekuasutustele või Riigi Infosüsteemi Ametile või küberjulgeoleku nõukogule, võib eespool kirjeldatud menetlus aega võtta rohkem kui 120 tööpäeva ehk teisisõnu ligikaudu 6 kuud. See menetlus takistab telekommunikatsiooniettevõtjatel oma hädaolukorra seadusest tulenevate kohustuste täitmist⁸. Hädaolukorra seaduse § 38 lõike 2 punkti 3 järgi on elutähtsat teenust osutav telekommunikatsiooniettevõtja kohustatud hädaolukorra või muu sarnase olukorra ajal tagama enda osutatava teenuse järjepideva toimimise ja kiire taastamise võime. Määruseelnõu takistab eeltoodu tegemist, kuna mis tahes riist- või tarkvara asendamiseks tuleks telekommunikatsiooniettevõtjal läbida Määruseelnõuga kavandatav kooskõlastusmenetlus. Arvestades elutähtsa teenuse toimepidevuse otsest seost riigi julgeolekuga, on selge, et määruseelnõul on riigi julgeolekule negatiivne mõju.

(13) Samuti soovime rõhutada, et Eesti oleks ainus Euroopa Liidu liikmesriik, kus sellist äärmiselt koormavat üleregulatsiooni rakendatakse fikseeritud lairibavõrkude osas.

(14) Lisaks, seletuskirja kohaselt on määruse eesmärk kehtestada meetmed üldkasutatava elektroonilise side võrgu turvalisuse tagamiseks ning ühtlasi tagada, et võrk on kaitstud küberohtude eest. ELis asutatud äriühinguna suhtub Huawei küberturvalisusesse suure tõsidusega.

(15) Esiteks, tõhusa küberturbe tagamine nõuab pidevat seiret. Turvaauku avastamisel peavad ettevõtjad riskide kõrvaldamisel kiiresti tegutsema. Kui kehtivad õigusaktid seda ei võimalda, jääb võrk haavatavaks vajaliku lahenduse kooskõlastamise ja kasutusele võtmiseni. Valitsuse kehtestatud eelneva kooskõlastuse saamise nõue tähendab, et võimalikke turvaauke ei saa võimalikult kiiresti kõrvaldada, mis omakorda vähendab võrkude turvalisust.

(16) Teiseks, telekommunikatsiooniettevõtjad kui Eestis elutähtsa teenuse osutajad on kohustatud järgima küberturvalisuse seaduse §-des 7 ja 8 sätestatud nõudeid⁹. Küberturvalisuse seaduse eesmärk on kehtestada ühiskonna toimimise seisukohast oluliste ning riigi ja kohaliku omavalitsuse üksuse võrgu- ja infosüsteemide pidamise nõuded, vastutuse ja järelevalve ning küberintsidentide ennetamise ja lahendamise alused (küberturvalisuse seaduse § 1). Seega, küberturvalisuse seaduse §-d 7 ja 8 sätestavad teenuse osutajatele (ehk telekommunikatsiooniettevõtjatele) nõuded, millega soovitakse tagada, et teenuse osutajate organisatsioonistruktuurid töötavad pidevalt küberintsidentidest tulenevate riskide ennetamise,

⁸ Hädaolukorra seadus, RT I, 22.05.2018, 5. Arvutivõrgus: <https://www.riigiteataja.ee/akt/103032017001?leiaKehtiv>

⁹ Küberturvalisuse seadus, RT I, 22.05.2018, 1. Arvutivõrgus: <https://www.riigiteataja.ee/akt/122052018001>

lahendamise ja leevendamise nimel. Eeltoodust tulenevalt on selge, et telekommunikatsioonivõrgu turvalisuse tagamisel pole kasutatavatele telekommunikatsiooniseadmetele ja -tarkvarale valitsuse eelneva kooskõlastuse taotlemine piisav, sest tegema peab pidevat seiret, mida telekommunikatsiooniettevõtjad juba praegusel hetkel ka teevad. Kuna Määruseelnõu keskendub peamiselt riist- ja tarkvara nime ning nende tootja tuvastamisele, on ebaselge, kuidas kõnealune teave võiks panustada riigi julgeoleku ja küberturvalisuse tagamisse.

(17) Viimaseks, hinnangut pole antud olukordadele, kus teatud telekommunikatsiooniseadmed on ühes ELi liikmesriigis turvaliseks tunnistatud, teises aga mitte. Telekommunikatsioon on oma olemuselt piiriülene ning teiste ELi liikmesriikide tegevusi arvestamata pole võimalik, et Määruseelnõuga kavandatud nähtavalt riigi julgeolekut suurendaks.

(18) Eeltoodust järeldub, et Määruseelnõu ei võimalda valitsusel hinnata, kas teatud telekommunikatsiooni riist- või tarkvara kasutamine oleks riigi julgeoleku huvides. Seega ei ole Määruseelnõu sobiv riigi julgeoleku suurendamiseks.

3. Vähem koormavate ja mõõdukamate meetmete olemasolu

(19) ESS § 87 lõike 2 punkt 4 annab valitsusele volituse võtta vastu määrusi, et kehtestada tehnilised nõuded, mis on vajalikud ESS § 87 lõikes 2 sätestatud eesmärkide saavutamiseks, sh riigi julgeoleku tagamiseks. Kõnealuste tehniliste nõuete kehtestamisele peab eelnema nõuete vajalikkuse kontroll vastavalt § 87 lõike 2 punktile 4.

(20) Määruseelnõust ja selle seletuskirjast ei nähtu, et eespool mainitud vajalikkust oleks kontrollitud. Eelkõige selleks, et tagada riigikaitset ja küberturvalisust puudutavate huvide kaitse, sätestavad hädaolukorra seadus ning küberturvalisuse seadus telekommunikatsiooniteenuse pakkujate suhtes mitu riigikaitse huvidest lähtuvat kohustust. Eeltoodust tuleneb, et telekommunikatsioonivõrke ja riigikaitset puudutavad meetmed on juba kasutusel ning on ebaselge, miks kohaldatavates õigusaktides sätestatud ebapiisavaks ja täiendavate normide loomist vajalikuks peetakse. Vajalikkuse kontrolliks on miinimumina vajalik hinnata, et millised riigi julgeoleku ja küberturvalisuse aspektid pole hetkel kehtivate õigusaktidega hõlmatud ja piisavalt kaitstud.

(21) Samuti ei sisalda Määruseelnõu ning seletuskiri hetkel teavet selle kohta, kas kavandatud meetmed üldse läbiksid eespool mainitud kontrolli ning kuidas need tagavad riigi julgeolekut, väldivad konkurentsi piiramist ja tagavad sideteenuse kvaliteedi, mille nõue tuleneb volitavast õigusaktist ehk ESS § 87 lõike 1 punktides 7 ja 11. Ühtlasi pole selge, kas valitsus on kaalunud olemuselt vähem koormavate ja mõõdukamate alternatiivsete meetmete kasutamist.

4. ELi tasandi küberturvalisuse ja õiguslike arengute kõrvalejätmine

(22) Määruseelnõu ei arvesta ELi hõlmavate meetmetega, täpsemini NIS direktiivi¹⁰, ELi küberturvalisuse määruse¹¹, ELi telekommunikatsioonisektori õigusliku raamistiku, sh

¹⁰ EUROOPA PARLAMENDI JA NÕUKOGU DIREKTIIV (EL) 2016/1148, 6. juuli 2016, meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus. Arvutivõrgus: <https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32016L1148&from=ET>.

¹¹ Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta määrus (EL) 2019/881, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (küberturvalisuse määrus), EMPs kohaldatav tekst. Arvutivõrgus: <https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32019R0881&from=EN>.

loadirektiivi¹² ja Euroopa elektroonilise side seadustiku¹³, meetmetega, mis on telekommunikatsioonisektori digitaalse vastupidavuse suurendamiseks juba kasutusele võetud. Muu hulgas on eespool mainitud direktiivide eesmärk tagada telekommunikatsioonivõrkude kui oluliste teenuste vastupidavus ja turvalisus ehk sätestatud eesmärk kattub Määruseelnõu seletuskirjas toodud põhjendustega.

- (23) Elkoige on Määruseelnõu vastuolus kohaldatavast ELi õigusest tulenevate riigisestte reeglite kehtestamise piirangutega. ELi tasandil kohaldatakse telekommunikatsiooniteenuste osutamisele hetkel loadirektiivi (direktiiv 2002/20/EÜ), mille asendab Euroopa elektroonilise side seadustiku (edaspidi: **EESS**) kehtestanud direktiiv (direktiiv 2018/1972).
- (24) Loadirektiiv ja EESS direktiiv loovad aluse elektroonilise side võrkude toimimiseks kasutatava tehnoloogia suhtes riigisestte piirangute kohaldamiseks. Need piirangud peavad olema: i) läbipaistvad, mõõdukad (proportsionaalsed), mittediskrimineerivad, konkurentsi soodustavad ning põhinema objektiivsetel kriteeriumitel, et tagada raadiospektri tõhus ja tulemuslik kasutamine; ii) vastavuses tehnoloogianeutraalsuse põhimõttega; ja iii) vajalikud kõnealuse piirangu üldhuvi eesmärgi saavutamiseks. EESS täpsususte kohaselt peavad kriteeriumid ühtlasi olema: v) prognoositavad, selged ja järjepidevad, et tagada õiguskindlus ja edendada pikaajalisi investeeringuid; vi) toetavad kõige vähem koormavat loasüsteemi. Kuna Määruseelnõud ei esita selgeid objektiivseid kriteeriume, mille alusel haldusmenetluses kaalutlusõigust kasutatakse, tuleb järeldada, et eeltoodud tingimused käesoleval juhul täidetud ei ole.
- (25) Selguse mõttes tuleb märkida seda, et hoolimata asjaolust, et Eestil tuleb EESS direktiiv riigisestte õigusesse üle võtta alles 21.12.2020, on Euroopa Liidu Kohus üheselt selgitanud, et liikmesriigid peavad enne riigisestte õigusesse ülevõtmise tähtpäeva saabumist hoiduma selliste meetmete kasutusele võtmisest, mis võiksid direktiiviga ette nähtud tulemuse saavutamist kahjustada (vaata nt 18. detsembri 1997. aasta otsus kohtuasjas C-129/96: *Inter-Environnement Wallonie*, ECLU:EU:C:1997:628, punkt 45¹⁴).
- (26) Lisaks ei ole Määruseelnõus arvestatud ELi küberturvalisuse määruse (määrus (EL) 2019/881) mõjuga, mis otseselt käsitleb info- ja kommunikatsioonitehnoloogia vastupidavusvõimet, täpsemini võimalust sertifitseerida info- ja kommunikatsioonitehnoloogia tooteid ja teenuseid, et tagada nende kasutamise turvalisus ja ohutus.
- (27) Kuna ELi küberturvalisuse määrus ja asjakohased sertifikaadid puudutavad telekommunikatsioonisüsteemide turvalisust ELi ühtsel turul, sh Eestis, peab Määruseelnõus arvestama olemasolevate ELi tasandi õigusinstrumentidega ning nende mõjuga Määruseelnõule.

5. Ebapiisav üleminekuperiood

- (28) Määruseelnõu jõustub 6-kuulise üleminekuperioodi möödumisel. Telekommunikatsioonivõrgu olemusest tulenevalt põhjustaks eeltoodu olulisi häireid telekommunikatsiooniturul, millel võivad olla erakordselt kahjulikud tagajärjed.

¹² Euroopa Parlamendi ja nõukogu 7. märtsi 2002. aasta direktiiv 2002/20/EÜ elektrooniliste sidevõrkude ja -teenustega seotud lubade andmise kohta (loadirektiiv). Arvutivõrgus: <https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32002L0020>

¹³ Euroopa Parlamendi ja nõukogu 11. detsembri 2018. aasta direktiiv (EL) 2018/1972, millega kehtestatakse Euroopa elektroonilise side seadustik (uuesti sõnastatud), EMPs kohaldatav tekst. Arvutivõrgus: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2018.321.01.0036.01.ENG

¹⁴ 18. detsembri 1997. aasta otsus kohtuasjas C-129/96: *Inter-Environnement Wallonie*, ECLI:EU:C:1997:628, punkt 45. Arvutivõrgus: <http://curia.europa.eu/juris/liste.jsf?language=en&num=C-129/96>

(29) Näiteks 5G võrgud on ehitatud olemasolevatele 4G võrkudele, mis tähendab, et 5G võrke ettevalmistavate investeeringutega on juba alustatud ning see on kestnud mitmeid aastaid. Määruseelnõu jõustumisel tuleks telekommunikatsiooniettevõtjatel maha kanda ligikaudu viimase kümnendi jooksul olemasolevatesse telekommunikatsioonivõrkudesse tehtud investeeringud. Huawei olemasolevate seadmete väljavahetamise kulu oleks juba 150 miljonit eurot. See 150 miljonit eurot ei sisalda teisi negatiivseid tagajärgi. 6-kuuline üleminekuperiood ei ole piisav, et turg saaks teha vajaminevad muudatused. Kõnealune õigusakt oleks vastuolus ettevõtlusvabaduse põhimõttega, mis on sätestatud nii Eesti põhiseaduses kui ka Euroopa Liidu põhiõiguste hartas.

(30) Ühtlasi võimaldaks piisava tähtajaga üleminekuperiood valitsusel jälgida ELi tasandi arenguid („EU Toolbox“).

6. Mõjuanalüüsi puudumine

(31) Määruseelnõu seletuskirjas on väidetud, et „eelnõul ei ole puutumust Euroopa Liidu õigusega“. See väide pole tõene.

(32) Esiteks, seletuskirjas endas on mitmel korral viidatud erinevatele ELi tasandil toimuvatele tegevustele. Teiseks, telekommunikatsioonivõrgud ja -tooted moodustavad digitaalse ühtse turu saavutamise nurgakivi ja seega on iga telekommunikatsioonivõrke ja -tooteid puudutav piirang ELi kohaldamisalas ja pädevuses.¹⁵ Kolmandaks, iga õigusakt, mis võib piirata liikmesriikide vahelist kaubandust, on vastuolus Euroopa Liidu toimimise lepingus vaba liikumise kohta sätestatuga. Olenemata sellest, et valitsus võib eespool mainitud sätetest kõrvale kalduda avaliku julgeoleku huvidest lähtuvalt, on Euroopa Liidu Kohus sedastanud, et kuivõrd kõnealused erandid on lubatud ELi õigusega, peab Euroopa Liidu õiguse rakendamata jätmisel arvestada ELi õiguse üldpõhimõtetega olukorras, kus liikmesriik tugineb piiranguid kehtestades ülekaalukale avalikule huvile või avalikust julgeolekust lähtuvatele põhjendustele (vaata nt 30. aprilli 2014. aasta otsus kohtuasjas C-390/12: Pfleger jt, ECLU:EU:C:2014:281, punkt 35¹⁶). Sama kohalduks ka juhul, kui ELi tasandil vastavad õigusaktid puuduvad, mis aga hetkel nii ei ole (vt ülalpool punkti 4). Eeltoodu põhjal saab järeldada, et Määruseelnõul on puutumus ELi õigusega ning seega tuleb läbi viia vastav analüüs kooskõlas „Mõjude hindamise metoodika“¹⁷ punktiga 2.1.3, mis on koostatud teiste hulgas Justiitsministeeriumi poolt.

(33) Samuti ei arvestata Määruseelnõu seletuskirjas turuosalistele tekkivaid kulusid, mis lõppkasutajatele üle kanduvad. Kuigi seletuskirjas väidetakse, et telekommunikatsiooni ettevõtjatele tekkida võivate „teatud kulude“ ette ennustamine pole võimalik, on selge, et kõnealused kulud on märkimisväärsed ning sellel on olulised tagajärjed.

(34) Näiteks 5G võrgud on ehitatud olemasolevatele 4G võrkudele, mis tähendab, et 5G võrke ettevalmistavate investeeringutega on juba alustatud ning see on kestnud mitmeid aastaid. Eksisteerib kahte tüüpi 5G arhitektuure – eraldiseisev 5G (edaspidi: „5G SA“ – *standalone*) ja mitte-eraldiseisev 5G (edaspidi: „5G NSA“ – *non-standalone*). Neist kahest arhitektuurist on 5G NSA kõige küpsem valik, mis on saadaval äriliseks kasutamiseks. NSA arhitektuur vajab 5G kinnituspunktina (n-ö ankruna) 4G võrku. Kooskäitamisprobleemide vältimiseks peaksid levialas olevad 5G ja 4G raadioseadmed pärinema ühelt tarnijalt.

¹⁵ Vaata nt määrus (EL) 2019/881, põhjendus 2.

¹⁶ 30. aprilli 2014. aasta otsus kohtuasjas C-390/12: Pfleger jt, ECLU:EU:C:2014:281, punkt 35. Arvutivõrgus: <http://curia.europa.eu/juris/liste.jsf?&num=C-390/12>.

¹⁷ *Mõjude hindamise metoodika*, Justiitsministeerium ja Riigikantselei, 2012. Arvutivõrgus: https://www.just.ee/sites/www.just.ee/files/elfinder/article_files/mojude_hindamise_metoodika.pdf

- (35) 5G NSA arhitektuuri puhul peab 5G seade saama esmalt juurdepääsu 4G võrku. 4G võrk juhendab seda 5G seadet, saamaks juurdepääsu 5G võrku. 5G võrk võimaldab 5G seadmel kasutada 10-20 korda kiiremat kiirust ja muid 5G eeliseid. 5G ühenduse ajal viib kõik juhtimistoimingud läbi 4G võrk. Seetõttu valivad operaatorid iga leviala jaoks sama tarnija 5G ja 4G võrgu.
- (36) 5G seadmete soetamine muult tarnijalt kui olemasoleva 4G seadmete tootjalt tähendaks märkimisväärselt kulude suurenemist, sest kõik eksisteerivad 4G seadmed tuleks välja vahetada. Juhul kui operaator kasutab mitme tarnija strateegiat, on tema võrguseadmete levialad eristatud. Operaator kasutab ühe ja sama tarnija 4G ja 5G seadmeid ühe leviala piires. 5G NSA jääb pikaajaliseks arhitektuuriks, vaatamata lähiaastatel eesootavatest 5G SA arengutest. Isegi tuleviku 5G SA arhitektuuri puhul on vajalik 4G ja 5G sageduste spektri agregeerimine, mistõttu oleks sama tarnija 4G ja 5G seadmete sama tarnija käest hankimine operaatorite jaoks parim valik.
- (37) Kui Huawei tõrjutakse turult, võib see tähendada, et kõik Huawei telekommunikatsiooniseadmed, mille telekommunikatsiooniettevõtjad on juba kasutusele võtnud, tuleb välja vahetada. Huawei hinnangul oleks selle üldine majanduslik tagajärg peaaegu 300 miljonit eurot. Ettevõtjatel tuleks teha lisakulutusi summas 150 miljonit eurot, et olemasolevad süsteemid välja vahetada, ning neil jääks väljavahetamise käigus saamata umbes 100 miljonit eurot müügitulu. Kogu majanduses jääks 5G võrkude ökosüsteemi arendamises tekkinud viivituste tõttu lisaks tekkimata käive, mille summa on vähemalt 50 miljonit eurot. Järgnevatel aastatel tekkivad telekommunikatsiooni ülereguleerimisest tulenevad majanduslikud tagajärjed oleks veel suuremad. Mitmed Euroopa Liidu liikmesriigid, näiteks Soome, on juba 5G-võrke äriliseks kasutamiseks juba välja arendamas. Eestil võib tekkida 5G väljaarendamisel märkimisväärne viivitus, kui üks seadmete müüja turult välja jäetakse. Seetõttu võivad Eesti digiettevõtted kaotada oma konkurentsieelise võrreldes naaberriikidega.
- (38) Kuna kõnealused olemasoleva infrastruktuuri väljavahetamise kulud tekiksid otseselt Määruseelnõust tulenevate kohustuste täitmisest, ei saa välistada, et valitsusel tuleks need kulud võrguettevõtjatele hüvitada.
- (39) Halduskoormuse kohta on seletuskirjas mainitud, et ministeeriumi hinnangul tekib vajadus ühe lisatöötaja järele, kelle ülesandeks on telekommunikatsiooniettevõtjate taotluste läbivaatamine. Arvestades seletuskirjas otseselt välja toodud asjaolu, et telekommunikatsioonisektor on keeruline, pole ühele ametnikule jõukohane potentsiaalselt tuhandeid lehekülgi teavet läbi töötada ja riigi julgeoleku huvidest lähtuvad vajalikud analüüsid teha, tagades sealjuures, et telekommunikatsiooniettevõtjate taotluste läbivaatamine on olnud korrektne, õigeaegne ja seadmetes kasutatud riist- ja tarkvara on tõepoolest kooskõlas riigi julgeoleku huvidega.
- (40) Sellest saab järeldada, et Määruseelnõu koostamisel pole tegelikkust arvestavat mõjuanalüüsi tehtud.

7. Vastutuse piiritlemine

- (41) Turvaintsidentide esinemisel pole selge telekommunikatsiooniettevõtjate ja seadmete tootjate vastutus valitsuse kooskõlastustega tark- või riistvara puudutavas. Määruseelnõus on esitatud TTJA „tehnilise dokumentatsiooni kooskõlastamise“ mudel. See mudel hägustab vastutuse tegelikku jaotumist sidusrühmade vahel, täpsemini järelevalveorgani ja ettevõtjate vahel, aga ka erinevate ametiasutuste vahel (näiteks TTJA ja Riigi Infosüsteemi Ameti vahel).
- (42) Jääb ebaselgeks, millist mõju peaks kogu telekommunikatsioonivõrkudes kasutatava riist- ja tarkvara valitsusega kooskõlastamine omama telekommunikatsiooniettevõtjate küberohtude pideva seire, ennetamise ja leevendamise kohustustele. Kui valitsusega kooskõlastamisel puuduks igasugune mõju telekommunikatsiooniettevõtjate praegustele kohustustele, on

võimalik järeldada, et valitsusega kooskõlastamisest kasu ei teki. Sellisel juhul rikuks kooskõlastusmenetlus ettevõtlusvabadust, loomata sealjuures riigi julgeoleku suurendamiseks sobivaid vahendeid.

- (43)Erinevate sidusrühmade vastutuse selgeks piiritlemiseks on vajalik kindlaks määrata kõiki sidusrühmi hõlmav vastutuse ja kooskõlastamise mehhanism.

8. Kaubanduse ja konkurentsi moonutamine

- (44)ELi liikmesriigina on Eestil kohustus tagada ELi siseturu toimimine. ELi õigusest tulenevalt on liikmesriikide vahel keelatud koguselised impordipiirangud ja kõik samaväärse toimega meetmed. Kuigi liikmesriigid võivad avaliku korra ja avaliku julgeoleku kaalutlustest lähtuvalt kasutusel võtta meetmeid, mis seavad piiranguid kaubandusele ELi siseturul, peavad kõnealused piirangud olema saavutatava eesmärgi suhtes mõõdukad.

- (45)Määruseelnõus ei selgitata millised asjaolud on olulised hindamaks seda, kas teatud telekommunikatsiooniseadmete tootja toodetud tarkvara või tooted on riigi huvidega kooskõlas. Kuigi tegemist ei ole ametlike seisukohtadega, on avalikult antud intervjuude põhjal turu arusaamaks kujunenud see, et Määruseelnõu hakkab eelkõige mõjutama Huawei. Praktikas kujuneks Määruseelnõu tagajärjeks olukord, kus Määruseelnõuga kavandatava kohaldamine mõjutab Huawei rohkem kui teisi konkureerivaid tootjaid, olenemata sellest, et Huawei kontserni Soome tütarfirma on asutatud Soomes ja seega kohaldatakse selle suhtes ELi õigust. Asjakohaseid kohtulahendeid arvestades tähendab see omakorda, et Määruseelnõu jõustumine piiraks Huawei seadmete ja tarkvara kaubavoogusid, mis tulevad Eestisse teistest ELi liikmesriikidest. See tähendab, et Määruseelnõu mõju oleks samaväärne liikmesriikidevahelise koguselise kaubanduspiiranguga, mis on Euroopa Liidu Toimumise Lepingu artikli 34 alusel keelatud.

- (46)Samuti mõjutab Huawei väljajätmine oluliselt konkurentsi. Telekommunikatsiooni turgu iseloomustab väike arv toodete müüjaid ning Huawei väljajätmine vähendaks oluliselt konkurentsi ülejäänud müüjate vahel. Seda mõju võimendaks veelgi seadmete ja tarkvaratootjate vahetamisele kuluv 6-kuuline kooskõlastusperiood, mille tulemusel suureneksid sideettevõtjate seadmete väljavahetamisele tehtavad kulutused. Mida suuremaid kulutusi telekommunikatsiooniettevõtjad väljavahetamisele tegema peaksid, seda väiksem on tõenäosus, et nad seadmed välja vahetavad, ja seda haavatavamad nad oleks telekommunikatsiooniseadmete tootjate hinnatõusudele. Arvestades 5G lubade saamiseks vajalikke nõudeid täitvate telekommunikatsiooniettevõtjate väikest arvu, on tõenäoliseks tulemuseks turu jagamine, mis jätkaks turult välja Huawei, kuid välja jääksid ka kõik uued turule siseneda või naasta soovivad ettevõtjad.

- (47)Lisaks, kuna Määruseelnõus esitatud valitsuse kooskõlastusmenetluses nähakse ette valikulise 60-tööpäevase kestusega sammu sätestamine, siis juhul, kui seda sammu kohaldatakse praktikas üksnes Huawei seadmete suhtes, on see juba iseenesest piisav, et muuta klientide käitumist ja seega moonutada EL siseturul konkurentsi.¹⁸ Eeltoodust võib järeldada, et Määruseelnõu on vastuolus ELi õigusega. Võttes arvesse, et ELi õigusega vastuolus olevad riigisisesed õigusaktid tuleb ELi õiguse ülimuslikkuse tõttu kohaldamata jätta, ei saaks Määruseelnõuga kavandatavat praktikas kohaldada.

- (48)Konkurentsi moonutamisest hoidumiseks tuleks mittetehnilisi ja standarditel mittepõhinevaid „tehnilisi nõudeid“ vältida.

¹⁸ Sellega seoses vt. Euroopa Liidu Kohtu 19 oktoobri 2016 aasta otsust asjas C-148/15, *Deutsche Parkinson Vereinigung*, ECLI:EU:C:2016:776, punkt 27.

Viimase 30 aasta jooksul on Huawei teenindanud kolme miljardit inimest enam kui 170 riigis ja piirkonnas ning on küberjulgeoleku valdkonnas saavutanud kindla kogemuse. Huawei jääb Eesti operaatoritele usaldusväärseks tehnoloogiapartneriks ja loodab panustada veelgi Eesti digitaalsesse ühiskonda. Oleme alati valmis lahendama kõiki valitsuse küberjulgeolekuga seotud probleeme.

Huawei Technologies Oy (Finland) Co. Ltd nimel Tuomas Latola



Principal legal counsel, Huawei

20.12.2019, Helsinki, Finland