Küberturvalisuse seadusest

Laura Kask[1]
Tartu Ülikooli doktorant

1. Sissejuhatus

Eesti küberturvalisust ohustab eelkõige riigi, majanduse ja elanikkonna sõltuvus info- ja kommunikatsioonitehnoloogiast (IKT) ja e-teenustest. IKT sektori kiire areng ning piiriülene mõju koos globaliseeruva ühiskonnaga avaldavad mõju nii igapäevaelule kui ka majanduse ning riigi toimimisele tervikuna. Asjade internet suurendab andmesidevõrkudesse ühendatud seadmete hulka, samuti suurenevad andmemahud ja nende teenuste hulk, mida on võimalik uuenenud keskkonnas pakkuda. Ühest küljest toob selline paradigmamuutus kaasa teenuste parema kättesaadavuse ja kasutusmugavuse, teisalt kaasneb tehnoloogiasõltuvusega ühiskonna, majanduse ja riigi sõltuvus harjumuspärastest e-lahendustest ning ühiskonnas kinnistub ootus tehnoloogia tõrgeteta toimimise järele.

Selle aasta 9. mail võttis Riigikogu kolmandal lugemisel vastu küberturvalisuse seaduse[2]. Küberturvalisuse seadus[3] (KüTS) jõustus 23. mail ning selle eesmärk on tugevdada ühiskonna jaoks olulise tähtsusega teenuste osutamisel ning riigi ja kohaliku omavalitsuse üksuste töös kasutatavate võrgu- ja infosüsteemide turvalisust ning kaitset. Kuigi 2018. a maikuus mõjutab andmekaitset ja infoturvet põhiliselt isikuandmete kaitse üldmäärus[4] (edaspidi *GDPR*), siis ei saa alahinnata ka Euroopa Parlamendi ja nõukogu direktiivi (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus[5] (edaspidi *NIS direktiiv*) ülevõtmist liikmesriikide riigisisesesse õigusesse. NIS direktiivi eesmärk on kehtestada ühiskonna ja majanduse jaoks määrava tähtsusega teenustele miinimumstandardid võrgu- ja infosüsteemide kaitseks ning saavutada siseturul ühtlaselt kõrge tase. Eesti õigusesse võetakse NIS direktiiv üle KüTS-ga.

Teadlik küberkäitumine on osa kogu ühiskonna turvalisemast toimimisest. Eesti õigusteadlane Mario Rosentau on öelnud, et „infoühiskonna optimistlikuks tulevikuväljavaateks on kübersümbiootiline ühiskond, kus inimene valitseb ja kasutab arukalt tehnoloogiat üldiselt väärtusliku ja meeldiva elu elamiseks ja seda ohustavate riskide haldamiseks.“[6] Siiski ei muuda ainuüksi Riigi Teatajas avaldatud seadus küberkeskkonda turvalisemaks, küll aga peaks

[1] Artikli autor oli üks väljatöötamiskavatsuse ning seaduseelnõu ja seletuskirja koostajatest.
[2] Küberturvalisuse seadus 597 SE. https://www.riigikogu.ee/tegevus/eelnoud/eelnou/61815f7a-1025-4aea-9b0e-d9cf97337e59/. Vaadatud 21.05.2018.
[3] RT I, 22.05.2018, 1.
[4] Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 04.05.2016, lk 1–88.)
[5] Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus (ELT L 194, 19.07.2016, lk 1–30).
[6] **M. Rosentau**. *E-tempora, e-mores.* – Juridica 2015, nr 2, lk 151.

tugevnema ühiskonna jaoks määrava tähtsusega võrgu- ja infosüsteemide kaitse. Seega on artiklis käsitletav seadus kindlasti üks „kübersümbiootilise ühiskonna“ väljendusvorme ning kujundab küberkeskkonna edasist arengut. Artikli eesmärk on kirjeldada seaduse eesmärki, kohaldamisala ning anda ülevaade kohaldamisala subjektide uutest õiguslikest kohustustest. Artiklis ei keskenduta järelevalve küsimustele.

2. Küberturvalisuse seaduse eesmärgid ning kohaldamisala

Alljärgnevates alapeatükkides on käsitletud küberturvalisuse terminid ning seaduse reguleerimisala, samuti NIS direktiivi eesmärki.

2.1. Küberturvalisus ning seaduse reguleerimis- ja kohaldamisala

Küberturvalisuse seaduse väljatöötamisprotsessis sai üsna pea selgeks, et termin või eesliide *küber* tekitab IT-teadmistega spetsialistidele sama palju küsimusi ja seisukohti kui *õiguse* defineerimine. Eesti 2014.–2017. a küberjulgeoleku strateegia[7] defineerib eesliidet *küber*- terminina, mis on seotud omavahel suhtlevate infotöötlusvahenditega. Teisisõnu peaks seaduse jõustumisel muutuma turvalisemaks võrgu- ja infosüsteemide toimimine ning häirete vältimine või lahendamine. Ka küberõiguse ekspert Eneken Tikk-Ringas on leidnud, et eesliidet *küber* sisaldavad terminid on lõpuni määratlemata ning pidevas arengus mõisted, mis igal kasutamisjuhul vajavad konkretiseerimist.[8] Liiati on tegemist moesõnaga, mis leiab laialdast kasutust ja kajastust, samas mõistavad seda nii poliitikakujundajad, IT-inimesed kui ka juristid erinevalt.

Kui KüTS peaks *küberi* grammatilisel tõlgendamisel reguleerima küberruumi ning selle turvalisust, peaks esmalt vaatama, mis on küberruum. Andmekaitse ja infoturbe leksikoni[9] kohaselt on küberruumi käibetähendus inimeste, tarkvara ja teenuste interaktsiooniga tekitatav virtuaalne keskkond (peamiselt) internetis, sageli interneti sünonüüm. Samas julgeoleku kontekstis on tegemist infokeskkonna globaalse piirkonnaga, mille moodustab infosüsteemide üksteisest sõltuvate taristute võrk, millesse kuuluvad Internet, sidevõrgud, arvutisüsteemid ning sisseehitatud protsessorid ja kontrollerid. KüTS ei defineeri ei küberruumi ega ka küberturvalisust ning seda ilmselt taotluslikult.[10] Eelnõu seletuskirjast nähtub, et kuigi *küberturvalisus* jääb eelnõus määratlemata õigusmõisteks, saab seda avada ja mõista kui ühiskonna seisundit, mida iseloomustab võrgu- ja infosüsteemi kaudu avalikku korda, isikute tervist, vara ja keskkonda mõjutavate ohtude realiseerumise madal tõenäosus, võimekus ohtudele reageerida ja leevendada ohtude realiseerumisel tekitatud kahjulikku mõju ning mis tagatakse füüsiliste, organisatsiooniliste ja infotehniliste abinõude rakendamisega.[11] Samas on tegemist terminiga, mis on Eesti õiguses

[7] **Majandus- ja Kommunikatsiooniministeerium**, 2014. Küberjulgeoleku strateegia 2014–2017. https://www.mkm.ee/sites/default/files/kuberjulgeoleku_strateegia_2014-2017.pdf. Vaadatud 05.03.2018.
[8] **E. Tikk-Ringas**. Küberjulgeoleku õiguslik raamistik. – Juridica 2012, nr 4, lk 274–275.
[9] Andmekaitse ja infoturbe leksikon. https://akit.cyber.ee/term/568-kuberruum. Vaadatud 24.05.2018.
[10] Termineid ei defineeri ka Eesti õigekeelsussõnaraamat. Eesti õigekeelsussõnaraamat 2013. Tallinn: Eesti Keele Sihtasutus, 2013. https://www.eki.ee/dict/qs/index.cgi?Q=k%C3%BCber&F=M. Vaadatud 24.05.2018.
[11] Küberturvalisuse seaduse seletuskiri (viide 2), lk 4.

juba ka varasemalt kasutuses ning praktikas juurdunud. Terminit kasutatakse Kaitseliidu seaduses,[12] riigisaladuse ja salastatud välisteabe seaduses[13] (RSVS) ning ka madalama tasemega õigusaktides,[14] kuid üheski õigusaktis pole terminit defineeritud.

Eelnõu seletuskirja järgi kaaluti eelnõu pealkirjana ka „Võrgu- ja infosüsteemide turvalisuse seadust", kuid sellest loobuti, kuna võrreldes küberturvalisuse määratlusega on esimene olemuselt ja sisult kitsam, viidates eeskätt riist- ja tarkvarale.[15] Samas on seaduse reguleerimisala KüTS § 1 lõike 1 kohaselt ühiskonna toimimise seisukohast oluliste ning riigi ja kohaliku omavalitsuse üksuse võrgu- ja infosüsteemide pidamise nõuded, vastutus ja järelevalve ning küberintsidentide ennetamise ja lahendamise alused. Seega kitsendab KüTS § 1 lõige 1 seaduse reguleerimisala ning samamoodi NIS direktiiviga reguleeritakse ühiskonna toimimiseks olulisi teenusepakkujaid, kes kasutavad teenuse osutamiseks võrgu- ja infosüsteeme.

On selge, et turvalist elektroonilist ja digilahendustele orienteeritud virtuaalset keskkonda ei ole võimalik saavutada mitte üksnes võrgu- ja infosüsteemide turbe, vaid ka organisatsioonilise ning teadliku käitumise kaudu. Sellest lähtuvalt võib jõuda järeldusele, et seadus reguleeribki võrgu- ja infosüsteemide turvalisust laiemalt, kaasates sellesse horisontaalselt kõiki sektoreid. Kuigi õigusakt saab kohalduda üksnes kohaldamisala subjektidele, siis üldiste küberturvalisuse tagamise põhimõtete (KüTS § 6) sätestamisega annab seadus tegelikult kaudseid käitumissuuniseid ja juhiseid ka neile, kes seaduse kohaldamisala subjektideks ei ole.

KüTS ei kohaldata § 1 lõike 2 kohaselt riigisaladuse ja salastatud välisteabe töötlemisele ning sellise teabe töötlussüsteemide pidamisele. Kuigi sellised süsteemid on kahtlemata osa küberturvalisuse tagamisest, on elektroonilise teabeturbe korraldamine ja nõuete täitmise kontrollimine selliste süsteemide pidamisel reguleeritud RSVS-ga ning Välisluureameti pädevuses.

Kokkuvõtvalt on KüTS eesmärk tugevdada ühiskonna jaoks määrava tähtsusega teenuste ning riigi ja kohaliku omavalitsuse üksuste töö toimimiseks kasutatavate võrgu- ja infosüsteemide kaitset ning kuigi seaduse pealkiri võib hea õigusloome ja normitehnika eeskirja[16] § 21 lõikes 1 sätestatud suunisest erineda ning olla laiem kui reguleerimisala, annab see edasi üldisema suunise edaspidiseks õigusloomeks ja poliitikakujundamiseks ning on kindlasti märgilise tähtsusega ka e-riigi üldisemas riigisiseses ja piiriüleses silmapaistvuses. Kuna *küber-* ja *küberturvalisus* on käibefraasid, on praegune pealkiri kindlasti kõrvaltvaatajale arusaadavam kui võrgu- ja infosüsteemide turvalisus.

[12] RT I, 20.04.2018, 6.
[13] RT I, 05.05.2017, 5.
[14] Nt majandus- ja kommunikatsiooniministri 25. aprilli 2011. a määrus nr 28 „Riigi Infosüsteemi Ameti põhimäärus". RT I, 21.02.2018, 2.
[15] Küberturvalisuse seaduse seletuskiri (viide 2), lk 4.
[16] RT I, 29.12.2011, 228.

2.2. NIS direktiivi eesmärk

KüTS-ga võetakse muu hulgas Eesti õigusruumi üle NIS direktiiv. NIS direktiivi artikli 1 järgi on selle peamine eesmärk siseturu toimimise parandamine ehk tegemist on majandusliku arengu soodustamise direktiiviga. Direktiivi eesmärgid võib tinglikult jagada kolmeks.

Esiteks on need tegevused, mis peaksid arendama piiriülest koostööd ning ühtlast taset liikmesriikides. Selleks sätestatakse kõigile liikmesriikidele kohustus võtta vastu riiklik võrgu- ja infosüsteemide turvalisuse strateegia, luuakse koostöörühm, mille eesmärk on toetada ja hõlbustada strateegilist koostööd ja teabevahetust ning luua usaldust ja kindlustunnet liikmesriikide vahel, samuti luuakse küberturbe intsidentide lahendamise üksuste võrgustik, et aidata luua liikmesriikide vahel usaldust ja kindlustunnet ning edendada kiiret ja tõhusat operatiivkoostööd (NIS direktiivi artikli 2 lõike 1 punktid a–c). Seda osa NIS direktiivist ei ole KüTS üle võetud, kuna tegemist ei ole riigisisese õiguse reguleerimisesemega. Samas ei saa nende tegevuste tähtsust alahinnata direktiivi üldise eesmärgi täitmisel – tegemist on olulise edasiminekuga valdkondlikus koostöös Euroopa Liidu tasandil.

Kui eespool mainitud tegevused on soovitused, siis digitaalse teenuse osutajatele kohaldatavad nõuded võrgu- ja infosüsteemide turvalisuse tagamiseks ning küberintsidentidest teavitamiseks tuleb üle võtta, st liikmesriigid ei tohi ette näha karmimaid või leebemaid nõudeid, kui direktiivi V peatükk sätestab.

Kolmas eesmärk on kehtestada olulise teenuse operaatoritele kohaldatavad nõuded, et tagada võrgu- ja infosüsteemide turvalisus ning teavitada küberintsidentidest. Siinkohal on liikmesriikidel teatav diskretsioonotsus, kuna NIS direktiiv defineerib teenuse operaatori NIS direktiivi lisas II kehtestatud teenuste loetelu kaudu, mis võib liikmesriigiti olla erinev. Näiteks direktiivi lisas II on loetletud teenusena tuumaelektrijaama pidamine, mida Eestis praegu ei osutata ning mida KüTS ei reguleeri. Samuti ei ole mõnede liikmesriikide jaoks oluline näiteks veetransport. Seega tekib NIS direktiivi jõustumisel Eesti õiguskorda uus termin *olulise teenuse operaator* (*olulise teenuse osutaja*), mis on defineeritud KüTS § 3 lõikes 1. Oluline on märkida, et olulise teenuse osutaja definitsioon ei ole võrdväärne elutähtsa teenuse osutaja definitsiooniga, vaid on laiem ning hõlmab ka teisi teenusepakkujaid, kelle teenused on ühiskonna ja majanduse toimimise seisukohast olulised.

Nii oluliste teenuste operaatorite kui ka digitaalse teenuse osutajate puhul on nõuete täitmise kontrollimiseks oluline sätestada ka järelevalvepädevus, mistõttu kohustab direktiiv sätestama riiklikud pädevad asutused, ühtsed kontaktpunktid ja küberturbe intsidentide lahendamise üksuse, mille ülesanded on seotud võrgu- ja infosüsteemide turvalisusega.

Direktiivi rakendamisega tugevneb võrgu- ja infosüsteemide turvalisus ning ühtlustuvad nõuded selle tagamisele, samuti paraneb küberturbealane koostöö liikmesriikide vahel. Eesti jaoks on valdkonnas oluline, et riigis jagataks rohkem kogemusi, oskusi, tehnoloogiaid ja teavet riiklikus küberruumis toimuva kohta, kuna see võimaldab samalaadseid olukordi paremini ennetada ja lahendada.

3. Küberturvalisuse seaduse subjektid

Eelnõu kohaldamisala subjektid võib jagada kolme kategooriasse. Küberturvalisuse tagamiseks peavad meetmeid kasutama nii ühiskonna toimimise seisukohast oluliste teenuste (sealhulgas elutähtsa teenuse osutajad, olulised infrastruktuuri ettevõtted) kui ka digitaalse teenuse osutajad (pakuvad internetipõhise kauplemiskoha teenust, otsimootori teenust või pilveandmetöötlusteenust). Lisaks sellele peavad võrgu- ja infosüsteemide turvalisuse tagamisel meetmeid rakendama ka riigiasutused ja kohaliku omavalitsuse üksused, kes võrreldes NIS direktiivi kohaldamisala subjektide ringiga on KüTS lisandunud, kuigi nõudeid neile on rakendatud juba ka varem. Võrgu- ja infosüsteemide usaldusväärsus ja turvalisus peavad majanduse ja ühiskondlike vajaduste jätkusuutlikuks rahuldamiseks olema tagatud valdkondade üleselt. Siinkohal analüüsib autor kõiki kohaldamisala subjektide kategooriaid eraldi, kuna ka nõuded võrgu- ja infosüsteemide turvalisusele ning kohati ka järelevalvepädevus on subjektide puhul erinev.

3.1. Olulise teenuse operaatorid ehk teenuse osutajad

Olulise teenuse operaatorid ehk teenuse osutajad, kes Eesti kontekstis peaksid rakendama võrgu- ja infosüsteemide turvalisuse tagamiseks nõudeid ning kuuluvad kohaldamisala subjektide alla, on sellised teenuseosutajad, kellest sõltub riigi ja ühiskonna toimimine. Eestis on hädaolukorra seaduse[17] (HOS) § 2 lõike 4 kohaselt elutähtsad teenused sellised teenused, millel on ülekaalukas mõju ühiskonna toimimisele ja mille katkemine ohustab vahetult inimeste elu või tervist või teise elutähtsa teenuse või üldhuviteenuse toimimist. Elutähtsat teenust käsitatakse tervikuna koos selle toimimiseks vältimatult vajaliku ehitise, seadme, personali, varu ja muu sellisega. Seega on selliste teenuste olulisus ühiskonna jaoks juba enne KüTS jõustumist määratud ning uut mõisteaparaati või hinnangut ei olnud vaja. Siiski on KüTS teenuse osutajate kohaldamisalas teenuse osutajaid, kellele varem ei ole nõudeid rakendatud, kuid kelle puhul nii seadusandja kui ka Riigi Infosüsteemi Amet (RIA) on leidnud, et nad on riigi ja ühiskonna toimimise seisukohast küberturvalisuse kontekstis olulised. Seega kasutab KüTS teenuse osutaja terminit ning viide direktiivi olulise teenuse operaatori terminile on KüTS § 3 lõikes 2, mis loob justkui silla direktiivi terminite ja riigisisese õiguse terminite vahel.

KüTS § 3 lõike 1 punkti 1 kohaselt on teenuseosutaja, kellele seadus kohaldub, isik, kes kasutab võrgu- ja infosüsteeme elutähtsa teenuse osutamisel. HOS § 36 kohaselt on elutähtsate teenuste loetelus elektriga varustamine, maagaasiga varustamine, vedelkütusega varustamine, riigitee

[17] RT I, 22.05.2018, 4.

sõidetavuse tagamine, telefoniteenus, mobiiltelefoniteenus, andmesideteenus, elektrooniline isikutuvastamine ja digitaalne allkirjastamine, vältimatu abi toimepidevus, makseteenus, sularaharinglus, kaugküttega varustamine, kohaliku tee sõidetavuse tagamine ning veega varustamine ja kanalisatsoon. Oluline on, et nõuded ei ole tervikuna uued, vaid Eestis on ka enne KüTS jõustumist elutähtsa teenuse osutajatel olnud kohustus elektroonilise turvalisuse nõudeid (ehk võrgu- ja infosüsteemide turvalisuse nõudeid) järgida.[18]

Elutähtsate teenuste nimekirjas tehti 1. juulil 2017. a suurem muudatus, mistõttu vähenes elutähtsate teenuste hulk. Küll aga rakendusid elektroonilise turvalisuse nõuded ka pärast 1. juuli 2017. a redaktsiooni jõustumist laiemale hulgale teenuse osutajatele. KüTS jõustumisega ei ole nende teenuseosutajate nõuded reguleeritud enam HOS-s ja selle alusel kehtestatud määrustes, vaid kohaldamisala subjektideks on ka enne 1. juulit 2017. a jõustunud HOS redaktsioonis olnud teenuseosutajad, kes sõltuvad võrgu- ja infosüsteemidest suurel määral ning kes osutavad ühiskonna toimimise seisukohast olulisi teenuseid. Seaduse tõlgendamisel on oluline, et nõudeid ei kohaldata kõikidele kohaldamisala subjekti võrgu- ja infosüsteemidele, vaid ainult nendele süsteemidele, mis on seotud olulise teenuse osutamisega. Sellised teenuse osutajad ja nende tegevusega seotud võrgu- ja infosüsteemid on loetletud allpool.

1. Suuremad transporditaristu ettevõtted:
   1.1. raudteeseaduses sätestatud raudtee-ettevõtja, kes majandab avalikku raudteeinfrastruktuuri või kelle kaubaveo või reisijateveo turuosa on vähemalt 20 protsenti kaubaveo või reisijateveo turuosast võrgu- ja infosüsteemidele, mida kasutatakse avaliku raudtee toimimise ning raudteeveo ja avaliku reisijateveo toimimise teenuse osutamisel (KüTS § 3 lg 1 p 2);
   1.2. lennundusseaduses sätestatud lennuvälja käitaja, kelle käitatav lennuväli on avatud rahvusvaheliseks regulaarseks lennuliikluseks, samuti Tallinna lennuinfopiirkonnas lennuliikluse teenindamist tagav aeronavigatsiooniteenuse osutaja võrgu- ja infosüsteemidele, mida kasutatakse lennuvälja toimimise ja aeronavigatsiooni toimimise teenuse osutamisel (KüTS § 3 lg 1 p 3);
   1.3. sadamateenuse osutaja, kellele kuulub sadamaseaduses sätestatud sadam, mis teenindab rahvusvahelises meresõidus sõitvaid reisilaevu või 500-se ja enama kogumahutavusega laevu, ning sadam, mis teenindab meresõiduohutuse seaduse kohaselt määratletud kohalikus rannasõidus sõitvaid I kategooria laevu või A-klassi reisilaevu võrgu- ja infosüsteemidele, mida kasutatakse sadama toimimise teenuse osutamisel (KüTS § 3 lg 1 p 4).

2. Sideteenuse pakkujad:
   2.1. elektroonilise side seaduses sätestatud sideettevõtja, kes osutab kaabelleviteenust, mida tarbib vähemalt 10 000 lõppkasutajat, ja ringhäälinguvõrgu teenuse osutaja võrgu- ja infosüsteemidele, mida kasutatakse kaabelleviteenuse või ringhäälinguvõrgu teenuse osutamisel (KüTS § 3 lg 1 p 5);

[18] Vt lähemalt HOS § 41.

2.2. kriitilise tähtsusega side-, mereraadioside ja operatiivraadiosidevõrgu teenuse osutaja elektroonilise side seaduse tähenduses ning nõuded kohalduvad võrgu- ja infosüsteemidele, mida kasutatakse nende teenuste osutamisel (KüTS § 3 lg 1 p 9).

3. Tervishoiuteenuse pakkujad:
   3.1. tervishoiuteenuste korraldamise seaduses sätestatud haiglavõrku kuuluvate piirkondliku haigla ja keskhaigla pidaja võrgu- ja infosüsteemidele, mida kasutatakse statsionaarse eriarstiabi osutamisel, ja kiirabibrigaadi pidaja võrgu- ja infosüsteemidele, mida kasutatakse kiirabi osutamisel (KüTS § 3 lg 1 p 6);
   3.2. tervishoiuteenuste korraldamise seaduses sätestatud perearsti võrgu- ja infosüsteemidele, mida kasutatakse üldarstiabi osutamisel (KüTS § 3 lg 1 p 7).

4. Eesti Interneti Sihtasutus (KüTS § 3 lg 1 p 8) ja Eesti Rahvusringhääling (KüTS § 3 lg 1 p 10).

Perearstid, kes peavad hakkama rakendama turvanõudeid võrgu- ja infosüsteemidele, mida kasutatakse üldarstiabi osutamisel, on eelnõu kohaldamisalas uue subjektina. KüTS eelnõu teise lugemise seletuskirja kohaselt[19] on perearstide puhul vaja ühtlustada nende kasutatavate infosüsteemide turvanõudeid, et vältida näiteks isikuandmete lekkeid või andmete krüpteerimist lunavara rünnakute käigus. Paljudel perearstidel on nimistus sadu, kui mitte tuhandeid inimesi ning võimalus sellises mahus isikuandmete lekkimiseks küberrünnaku käigus on tänapäeval üsna tõenäoline. Kuigi isikuandmete kaitseks turvameetmete rakendamine tuleneb nii isikuandmete kaitse seadusest[20] kui ka selle aasta maikuus jõustunud GDPR-ist, on siiski tegemist valdkonnaga, kus peamine ülesanne on inimeste ravimine. Samas on seadmete keerukus järjest enam tekitanud sõltuvust võrgu- ja infosüsteemidest. RIA 2018. a raamatus on keskendutud eraldi ka küberriskidele tervishoiusektoris ning toodud välja, et 2017. a mõjutasid haiglate ja tervishoiuasutuste tööd retseptikeskuse, kindlustusregistri ja haigekassa teenuste katkestused, samuti langes teadaolevalt kaks Eesti perearstikeskust möödunud aastal lunavara ohvriks.[21] Sellised ohud näitavad, et tervishoiusektoris on järjest suurenevad riskid, mistõttu on oluline pöörata tähelepanu nende riskide hindamisele ja infoturbe süsteemi üldisele korraldusele organisatsioonis. Oluline aspekt on aga kindlasti seaduse täitmisega seotud keerukus. Terviseameti andmetel on Eestis 795 perearstinimistut.[22] RIA aastaraamatus on nenditud, et kuigi seaduste järgi on ka perearstidel kohustus tagada andmete kaitse ja turvalisus, ei hooma paljud perearstid, millised on andmetega seotud riskid.[23] Seega on seaduse rakendamisel ja tegeliku eesmärgi saavutamisel kindlasti RIA-l, Sotsiaalministeeriumil, Andmekaitse Inspektsioonil ja Eesti Haigekassal oluline roll aidata ja luua süsteeme, mis kindlustaksid kübeturvalisuse ka

[19] Küberturvalisuse seaduse teise lugemise seletuskiri (viide 2), lk 1–2.
[20] RT I, 06.01.2016, 10.
[21] Vt **Riigi Infosüsteemi Amet**. Küberturvalisus 2018. https://www.ria.ee/public/Kuberturvalisus/RIA-kuberturvalisus-2018.pdf. Vaadatud 24.05.2018.
[22] Terviseameti koduleht. http://www.terviseamet.ee/peremeditsiin/perearstide-nimistud.html. Vaadatud 24.05.2018.
[23] **Riigi Infosüsteemi Amet** (viide 21).

tervishoiusektoris ning seda laiemalt, kui seni kehtinud õigusaktides sätestatud kohustused on olnud.

Eesti Interneti Sihtasutuse ja Eesti Rahvusringhäälingu (ERR) puhul on tegemist on kahe isikuga, kes on seaduses väga täpselt defineeritud ning kellele võrgu- ja infosüsteemide turvanõudeid ei ole varem rakendatud. Seaduse kohaldamisala subjektiks on KüTS § 3 lõike 1 punkti 8 kohaselt Eesti maatunnusega seotud tipptaseme domeeninimede registri haldaja (ehk Eesti Interneti SA) registri pidamiseks kasutatava võrgu- ja infosüsteemi ja tipptaseme nimeserveri teenuse osas. Oluline on märkida, et Eesti Interneti SA osutatava teenusega seonduv pole reguleeritud üheski seaduses, kuid kuna tegemist on teenusega, mille sujuv toimimine on kriitilise tähtsusega Eesti internetikeskkonna küberturvalisuse tagamisel, on teenuse hõlmamine kohaldamisala subjektide hulka kindlasti otstarbekas.

Lisaks sellele on kohaldamisala subjektiks ka ERR. Eesti Rahvusringhäälingu seaduse[24] § 5 järgi on ERR-il sätestatud hulk ülesandeid ning lõike 1 punktis 10 on sätestatud, et ERR tagab adekvaatse informatsiooni operatiivse edastamise elanikkonda või riiklust ohustavates olukordades. Selle ülesande täitmiseks kasutatavate võrgu- ja infosüsteemide puhul on oluline küberturvalisuse nõuete järgmine. ERR on koos perearstidega subjektiks, kelle hõlmamine kohaldamisala subjektide all oli küll juba kooskõlastusele saadetud versioonides, kuid lõplikult otsustati see alles Riigikogus eelnõu teisel lugemisel. Arvestades, et info elanikkonna teavitamisel kriisidest või tähtsatest ühiskonda puudutavatest sündmustest on äärmiselt oluline, tuleb tagada rahvusringhäälingu toimimise järjepidevus ja katkematus. Selle tagamiseks peavad olema ka rahvusringhäälingu infosüsteemid kaitstud ning seda on võimalik saavutada piisavate turvanõuete täitmise kaudu.[25]

Seega on KüTS kohaldamisala subjektide hulgas peamiselt teenuseosutajad, kellele elektroonilise turvalisuse tagamise nõuded on HOS erinevate redaktsioonide alusel kehtinud ka varem, uute teenuseosutajatena on lisandunud perearstid üldarstiabi teenuse osutamisel, Eesti Interneti SA ning ERR.

3.3. Digitaalse teenuse osutajad

Digitaalse teenuse osutaja regulatsioon on NIS direktiivi osa, mille puhul on tegemist selliste subjektidega, kellele küberturvalisuse tagamise nõudeid varem ei kohaldatud. Digitaalse teenuse osutaja on infoühiskonna teenuse osutaja infoühiskonna teenuse seaduse[26] § 2 punkti 1 tähenduses, kes pakub internetipõhist kauplemiskohta (ehk e-poed), internetipõhist otsimootorit või pilvandmetöötlusteenust.

[24] RT I, 13.03.2014, 20.
[25] Küberturvalisuse seaduse teise lugemise seletuskiri (viide 2), lk 2.
[26] RT I, 12.07.2014, 48.

Teenuseosutaja ja digitaalse teenuse osutaja terminid KüTS-s ei ole samatähenduslikud ning kohalduvad nõuded on samuti erinevad. Samas ei saa praktikas välistada, et olulise teenuse osutaja osutab samal ajal ka digitaalseid teenuseid, mistõttu võib olla vaja kohaldada mõlemat tüüpi subjekti kohta käivat regulatsiooni. Lisaks sellele võib digitaalse teenuse osutaja olla ka riigi või kohaliku omavalitsuse üksus juhul, kui ta pakub internetipõhist kauplemiskohta või muud digitaalset teenust. Ühe näitena on eelnõu seletuskirjas nimetatud Draamateatri Piletimaailm.[27]

Kuigi digitaalse teenuse osutaja teenuse osutamine põhinebki võrgu- ja infosüsteemidel ning eelduslikult on teenuse osutamiseks süsteemide turvalisus oluline, on tegemist uute teenusepakkujatega. Siiski ei kohaldu nõuded kõikidele digitaalse teenuse osutajatele. KüTS § 1 lõike 3 kohaselt ei kohaldata seadust digitaalse teenuse osutajale, kellel on majandusaasta jooksul keskmiselt alla 50 töötaja ja kelle aasta bilansimaht või aastakäive ei ületa 10 miljonit eurot, arvestades mikro- ja väikeste ettevõtjate määratlusi Euroopa Komisjoni soovituses 2003/361/EÜ mikro-, väikeste ja keskmise suurusega ettevõtjate määratlemise kohta.[28] Kuna tegemist on siseturu ühtsete reeglitega, on nende määratluste kohaselt ettevõtjad Eesti kontekstis üsna suured. Samas on digitaalse teenuse osutaja ärimudel enamasti piiriülene, mistõttu on korrektne järelevalvemetoodika digitaalse teenuse osutajate üle kindlasti vajalik. Liiatigi on tegemist *ex post* järelevalvega, mis Eesti õigusruumis on pigem tavapäratu.

3.4. Riigi või kohaliku omavalitsuse üksus

Eelnõu kohaldamisala subjektide hulgas on ka riigi või kohaliku omavalitsuse üksus. Kui teenuse osutaja ning digitaalse teenuse osutaja regulatsioon on seotud NIS direktiivi ülevõtmisega, siis riigi ja kohaliku omavalitsuse üksuse lisandumine kohaldamisala subjektide hulka aitab lahendada avaliku teabe seaduse[29] praktilisi tõlgendamisprobleeme. Avaliku sektori asutustele on nõuded varem kehtestatud AvTS § 43⁹ lõike 1 punkti 4 alusel Vabariigi Valitsuse 20. detsembri 2007. a määrusega nr 252 „Infosüsteemide turvameetmete süsteem“. Määruse kohaselt on avaliku sektori asutustel kohustus järgida infosüsteemide kolmeastmelise etalonturbe süsteemi (nn infoturbestandard ISKE).

AvTS tõlgendamise praktilised probleemid tulenevad sellest, et AvTS-s sätestatud kohustus rakendada turvameetmeid laieneb üksnes seesugustele infosüsteemidele, mis on AvTS tähenduses andmekogud. AvTS § 43[1] lõike 1 kohaselt on andmekogu riigi, kohaliku omavalitsuse või muu avalik-õigusliku isiku või avalikke ülesandeid täitva eraõigusliku isiku infosüsteemis töödeldavate korrastatud andmete kogum, mis asutatakse ja mida kasutatakse seaduses, selle alusel kehtestud õigusaktis või rahvusvahelises lepingus sätestatud ülesannete täitmiseks. Praktikas on sagedad olukorrad, kus asutused infosüsteemide turvalisuse tagamise kohustuse vältimiseks infosüsteeme

[27] Küberturvalisuse seaduse seletuskiri (viide 2), lk 9.
[28] Euroopa Komisjoni soovitus 2003/361/EÜ, mis käsitleb mikroettevõtete ning väikeste ja keskmise suurusega ettevõtete määratlust (ELT L 124, 20.05.2003), lk 36.
[29] RT I, 4.07.2017, 11.

andmekogudena ei käsitata.[30] Andmekogu ja infosüsteemi terminite tõlgendamisprobleeme on põhjalikult analüüsinud Liis Getter Silberg oma magistritöös „Andmekogu või andmete kogumine“ ning jõudnud samuti järeldusele, et andmekogu tähendus AvTS-s on liiga kitsas.[31]

Infosüsteemideks, mida ei saa mahutada andmekogu mõiste alla ning mis pole käsitatavad andmekoguga seotud infovarana, on näiteks nimeserverid, ajaserverid, meiliserverid, virtualiseerimisplatvormid, kataloogiteenus, failiserverid, testserverid, testkeskkonnad, pääsusüsteemid, monitoorimissüsteemid, kettamassiivid, ruuterid, võrgu infrastruktuuri arenduskeskkonnad ja asutuse arvutivõrku ühendatud tööjaamad.[32] Kuigi riigi ja kohaliku omavalitsuse üksuse andmekogudele on turvanõuded kehtinud juba alates 2008. a ning infosüsteemide terviklik turvalisuse tagamine peab olema osa IT-süsteemide arendusest ja haldusest, on KüTS jõustumisel lahendatud pikaaegne praktiline probleem avaliku sektori võrgu- ja infosüsteemide turvalisuse tagamisel.

4. Kohustused võrgu- ja infosüsteemide turvalisuse tagamisel ning RIA roll järelevalveasutusena

Eelnevast peatükist lähtuvalt võib KüTS kohaldamisala subjektid jagada kolme suuremasse kategooriasse ning KüTS-s sätestatud kohustused võrgu- ja infosüsteemide turvalisuse tagamisel erinevad samuti. Käesolevas peatükis keskendutakse pigem kohustuste ülevaatele ning võrdlusele seni kehtivas õiguses sätestatud kohustustega, praktilisi lahendamisprobleeme ja võimalikke kohustuste dubleerimist erinevate seaduste alusel pikemalt ei puudutata.

4.1. Teenuse osutaja kohustused võrgu- ja infosüsteemide turvalisuse tagamisel

Teenuse osutajad ehk KÜTS § 3 lõikes 1 nimetatud teenuseosutajad peavad rakendama turvameetmeid küberintsidendi ennetamiseks ja lahendamiseks nii enda kui ka teiste sõltuvate teenuste võrgu- ja infosüsteemidele avaldava mõju leevendamiseks lähtuvalt KüTS §-st 7. KüTS § 7 lõike 2 kohaselt on kohustus koostada süsteemi riskianalüüs (§ 7 lg 2 p 1), tagada dokumenteeritud süsteemi riskianalüüsi, turvaeeskirjade ja turvameetmete rakendamise kirjelduse olemasolu ja ajakohasus (§ 7 lg 2 p 2), seirata ennetavalt süsteeme intsidentide vältimiseks ja edastada ohtude kohta teavat RIA-le (§ 7 lg 2 p 3), teenuse osutaja peab võtma kasutusele abinõusid küberintsidendi mõju ja leviku vähendamiseks ning vajaduse korral piirama süsteemi kasutamist või juurdepääsu sellele (§ 7 lg 2 p 4), kontrollima rakendamise piisavust, dokumenteerima kontrolli tulemused ja neid säilitama (§ 7 lg 2 p-d 5–6).

Lisaks sellele on teenuse osutajal kohustus 24 tunni jooksul teavitada RIA-t olulise mõjuga küberintsidendist ja ta peab saatma intsidendi lahendamisel RIA-le raporti toimunu, tehtu ja mõju kohta (KüTS § 8). Intsidendid, mida loetakse olulise mõjuga küberintsidentideks, on loetletud

[30] Küberturvalisuse seaduse seletuskiri (viide 2), lk 19

[31] **L. G. Silberg**. Andmekogu või andmete kogumine. Magistritöö, 2017. http://dspace.ut.ee/bitstream/handle/10062/57144/silberg_ma_2017.pdf. Vaadatud 26.05.2018.

[32] Küberturvalisuse seaduse seletuskiri (viide 2), lk 19.

KüTS § 8 lõikes 2. Oluline on teavitamiskohustuse täitmine ning soovituslikult on RIA küberturbe intsidentide lahendamise üksusele võimalik teatada ka intsidentidest, mille puhul ei ole oluline mõju tuvastatud.

Enamik kohustusi on elutähtsate teenuste osutajatel (HOS redaktsioonide alusel) rakendunud juba enne KüTS jõustumist. Uue kohustusena on lisandunud võrgu- ja infosüsteemide seire kohustus, et ennetada ja tuvastada küberintsidente juba enne kahju tekkimist. Seireseade monitoorib liiklust, kuid ei kogu isikuandmeid. Lisaks sellele täpsustatakse KüTS-s küberintsidentidest teavitamise korda. NIS direktiivi kohaselt on meetmete eesmärk parandada nii valmisolekut tulla toime küberintsidentidega kui ka Euroopa Liidu ülest ohuteadlikkust ja piiriülestele küberintsidentidele reageerimise võimet.

4.2. Digitaalse teenuse osutaja kohustused võrgu- ja infosüsteemide turvalisuse tagamisel

Digitaalse teenuse osutajate poolt turvameetmete rakendamise nõuded on reguleeritud mõneti paindlikumalt kui punktis 4.1 nimetatud teenuseosutajatele kohalduvad nõuded. Regulatsioon on üle Euroopa Liidu ühtne ning siseturu toimimise toetamiseks peavad nõuded liidusiseselt olema ühtsed. Üldjoontes on kohustused aga samad. Digitaalse teenuse osutajatel on KüTS § 10 kohaselt kohustus teha kindlaks riskid, analüüsida neid ning rakendada korralduslikke ja tehnilisi meetmeid. Samuti on kohustus teavitada olulise mõjuga intsidentidest, kuid teavitamisel lähtutakse NIS direktiivi artikli 16 lõike 8 alusel kehtestatud rakendusmääruses sätestatud kriteeriumitest, mis on loodud ühtset Euroopa turgu arvestades. Eesti ettevõtete puhul on kriteeriumid aga mahtusid ning klientide arvu arvestades pigem leebed. Ka digitaalse teenuse osutajal on soovituslikult võimalik RIA küberturbe intsidentide lahendamise üksust teavitada intsidentidest, mille puhul oluline mõju ei ole tuvastatud.

Digitaalse teenuse osutajatele kohalduvad nõuded on seaduse tasandil küll uued, kuid ka eelnõu seletuskirjas selgitatakse, et kuna infoturbega arvestamine on iga digitaalse teenuse osutaja teenuse pakkumisel juba enesestmõistetav, on raske eristada, millised infoturbega seotud tegevused on teenuse osutaja poolt omaalgatuslikult planeeritud või on mõne tegevuse motivatsiooniks olnud KüTS.[33] Sellegipoolest võib öelda, et nõuded on pigem üldised ning lähtuvad digitaalse teenuse osutamise praktilistest vajadustest ning valdkonna üldisest heast tavast.

4.3. Riigi ja kohaliku omavalitsuse üksuse kohustused võrgu- ja infosüsteemide turvalisuse tagamisel

Riigi ja kohaliku omavalitsuse üksuse turvameetmed on sätestatud KüTS §-s 9, mille kohaselt kohaldatakse KüTS § 7 lõigetes 1–3 sätestatud kohustusi. See tähendab, et nõuded on samad, mis teenuseosutaja puhul. Riigi- ja kohaliku omavalitsuse üksuse asutustel ei ole täiendavat turvastandardit vaja kasutusele võtta ning AvTS alusel jäävad avaliku teabe töötlemiseks peetava ja AvTS tähenduses andmekogu pidamise nõuded kehtima ning KüTS-s sätestatud kohustusi

[33] Küberturvalisuse seaduse seletuskiri (viide 1), lk 37–38.

täpsustab riigi ja kohaliku omavalitsuse üksuste jaoks AvTS § 43^9 lõike 1 punkti 4 alusel kehtestatud Vabariigi Valitsuse määrus.

4.4. RIA roll riikliku koordineerija ning järelevalveasutusena

Seaduse jõustumisel sai RIA riikliku koordinatsiooni ülesande küberturbe alal, lisaks täpsustuvad asutuse volitused ja käitumisreeglid küberintsidentide lahendamisel. Artikli mahtu arvestades ei ole RIA järelevalverolli ning selle pädevuse muutust võrreldes KüTS jõustumisega eraldi analüüsitud ning piirdutakse üksnes RIA üldiste ülesannete loetlemisega, kuid seni seadustes reguleeritud riiklikud kohustused küberturvalisuse korraldamisel on KüTS-s terviklikult sätestatud.

RIA ülesanne on teostada küberintsidentide ennetamiseks üldist seiret ning analüüsida süsteemide turvalisust ohustavaid riske ja nende mõju, edastada küberintsidentide ennetamiseks ja lahendamiseks ohuteateid (KüTS § 12 ja 13). RIA on NIS direktiivi tähenduses ühtne kontaktpunkt ning edastab vajaduse korral informatsiooni EL vastavatele pädevatele asutustele (KüTS § 5). Lisaks sellele on RIA KüTS ja selle alusel kehtestatud õigusaktide üle riikliku ja haldusjärelevalve teostaja. Lisaks korrakaitseseaduse erimeetmetele on KüTS §-des 16 ja 17 sätestatud riikliku ja haldusjärelevalve erisused, millest lähtuvalt on RIA-l õigus küberintsidendi puhul kõrgendatud ohu korral selle tõrjumiseks piirata süsteemi kasutamist või juurdepääsu sellele, kuid seda vaid juhul, kui intsident võib ohustada teisi süsteeme, süsteemi haldaja ei saa ise ohtu tõrjuda ning meetme kasutamine on proportsionaalne (sh ei tekitata liigset kahju).

Avalikku korda rikkuvate küberintsidentide tõhusamaks lahendamiseks antakse RIA-le elektroonilise side seaduse[34] § 114^3 alusel ka õigus küsida sideettevõtjatelt isikustamata andmeid võrguvoo kohta, mis aitaks tuvastada pahavara jagava seadme ja teha kindlaks ka ründeobjektid. Tegemist ei ole isikuandmete, vaid süsteeme puudutavate metaandmetega, mis on vajalikud küberintsidendi lahendamiseks. Sellele vaatamata võib GDPR ning Euroopa Kohtu otsuste valguses[35] sideandmete säilitamine ning kättesaamine ka KüTS kontekstis muutuda.

5. Kokkuvõte

Teadlik küberkäitumine on osa kogu ühiskonna turvalisemast toimimisest. On selge, et ükski Riigi Teatajas avaldatud seadus ei muuda küberkeskkonda turvalisemaks ning olulisem on seaduse tegelik rakendumine ja kujunev praktika. 23. mail 2018. a jõustunud KüTS eesmärk on korrastada Eesti senist praktikat küberturvalisuse tagamisel ning ühtlasi võtta Eesti õigusesse üle NIS direktiiv, mille tulemusel peaks ühtlustuma ka küberturbealane koostöö liikmesriikide vahel.

Turvaline elektrooniline ja digilahendustele orienteeritud virtuaalne keskkond ei ole saavutatav mitte üksnes võrgu- ja infosüsteemide turbe, vaid ka organisatsioonilise ning teadliku käitumise

[34] RT I, 22.05.2018, 3.
[35] Euroopa Kohtu 21.12.2016 otsus C-203/15 Tele 2 Sverige. Vaadatud 26.05.2018.

kaudu. Seadus reguleeribki võrgu- ja infosüsteemide turvalisust laiemalt, kaasates sellesse horisontaalselt kõiki sektoreid.

Eelnõu kohaldamisala subjektid võib jagada kolme kategooriasse. Küberturvalisuse tagamiseks peavad meetmeid kasutama nii ühiskonna toimimise seisukohast olulised teenused (sealhulgas elutähtsa teenuse osutajad, olulised infrastruktuuri ettevõtted) kui ka digitaalse teenuse osutajad (pakuvad internetipõhise kauplemiskoha teenust, otsimootori teenust või pilveandmetöötlus teenust). Lisaks sellele peavad võrgu- ja infosüsteemide turvalisuse tagamisel meetmeid rakendama ka riigiasutused ja kohaliku omavalitsuse üksused. Võrgu- ja infosüsteemide usaldusväärsus ja turvalisus peavad majanduse ja ühiskondlike vajaduste jätkusuutlikuks rahuldamiseks olema tagatud valdkondade üleselt.

Seaduse kohaldamisalas olevad asutused ja ettevõtted peavad rakendama turvameetmeid küberintsidendi ennetamiseks ja lahendamiseks. Näiteks tuleb analüüsida riske, seirata oma süsteeme ohustavat tegevust, rünnete korral piirama süsteemi kasutamist ning teavitama RIA-t, kui juhtunud on intsident, mis mõjutab oluliselt teenust või teisi teenusepakkujaid. Järelevalvet seaduse täitmise üle teostab RIA.

Eesti senine küberkaitse mudel põhineb valdkonnaülesel lähenemisel. KüTS jõustumisega jätkub kindlasti senine praktika. Eesti e-riigi kui ökosüsteemi turvalisus sõltub meist kõigist. Turvalisust ei saa võtta iseenesestmõistetavana ning küberruumi turvalisuse tagamiseks on oluline nii riigi, ettevõtete kui ka akadeemia koostöö. KüTS annab selleks terviklikuma ja raamistatud aluse.