SORAINEN
EESTI LÄTI LEEDU VALGEVENE

Pärnu mnt 15, 10141 Tallinn, Eesti
tel +372 6 400 900
estonia@sorainen.com
reg nr 10876331

Läti
Kr. Valdemāra iela 21, LV-1010 Riia
tel +371 67 365 000, latvia@sorainen.com

Leedu
Jogailos 4, LT-01116 Vilnius
tel +370 52 685 040, lithuania@sorainen.com

Valgevene
ul Internatsionalnaya 36-1, 220030 Minsk
tel +375 17 306 2102, belarus@sorainen.com

ISO 9001 sertifikaat
www.sorainen.com

RIIGI INFOSÜSTEEMI AMETI JÄRELEVALVE MEETMED HALDUSJÄRELEVALVEMENETLUSTES NING HÄDA- JA ERIOLUKORRAS

ÕIGUSANALÜÜS

2017

SISSEJUHATUS

Käesoleva analüüsi eesmärgiks on anda õiguslik hinnang küsimustele, milliseid riikliku ja haldusjärelevalve meetmeid on Riigi Infosüsteemi Ametil (edaspidi RIA) kehtiva õiguse alusel küberkaitsevaldkonnas ohtude tõrjumiseks võimalik võtta ning millised õigused peaksid RIA-l täiendavalt olema, et küberintsidentidest tulenevaid ohte efektiivselt ennetada ning tõrjuda.

Püstitatud küsimustele vastamiseks anname kõigepealt ülevaate RIA ülesannetest ning tegutsemise õiguslikust raamistikust küberkaitsevaldkonnas. Sealjuures pööratakse erilist tähelepanu põhiseaduslikele väärtustele ning põhimõtetele, mis on aluseks RIA tegevusele. Seejärel analüüsitakse, milliseid riikliku ja haldusjärelevalve meetmeid on RIA-l kehtiva õiguse alusel võimalik ohtude tõrjumiseks võtta, mille raames hinnatakse sealjuures, kas nendel meetmetel on olemas piisav seaduslik alus PS § 3 mõistes.

Analüüsi viimases osas käsitletakse erinevaid näiteid küberintsidentide juhtumitest, mis on praktikas Eestis või mujal maailmas toimunud, ning analüüsitakse olemasolevate meetmete piisavust nende ohtude ennetamisel ja tõrjumisel. Analüüsi tulemusel tehakse ettepanekud RIA volitusi puudutava regulatsiooni täiendamiseks.

KOKKUVÕTE

Käesoleva analüüsi eesmärgiks oli anda õiguslik hinnang küsimustele, milliseid riikliku ja haldusjärelevalve meetmeid on RIA-l kehtiva õiguse alusel küberkaitsevaldkonnas ohtude tõrjumiseks võimalik võtta ning millised õigused peaksid RIA-l täiendavalt olema, et küberintsidentidest tulenevaid ohte efektiivselt ennetada ning tõrjuda.

Selleks anti kõigepealt ülevaade RIA ülesannetest ning tegutsemise õiguslikust raamistikust küberkaitsevaldkonnas. RIA kohustus tegutseda ning tõrjuda ohte tuleneb muuhulgas põhiseaduse preambulist, mis näeb riigi esmase ülesandena ette sisemise ja välise rahu ning julgeoleku kaitsmise ühiskonnas. Lisaks tuleneb põhiseaduse §-dest 13 ja 14 isiku õigus riigi ja seaduse kaitsele. Küberintsident võib seada ohtu olulise või elutähtsa teenuse toimimise, mis võib omakorda seada ohtu inimese elu, tervise, vara ja keskkonna. Kuivõrd RIA on ainus asutus, mis tegeleb küberintsidentide lahendamise ja ennetamisega, on RIA-l põhiseaduslik kohustus tõrjuda küberintsidentidest tulenevaid ohte isiku elu, tervise ja vara ning keskkonna kaitseks.

Selleks, et RIA saaks seadusest ja põhiseadusest tulenevaid kohustusi täita, peavad RIA-l olema piisavad õigused ja volitused. See hõlmab ka riikliku ja haldusjärelevalve meetmeid, mis on vajalikud ohtude tõrjumiseks. Need meetmed on reeglina suunatud teistele riigiasutustele, avalik-õiguslik ja eraõiguslikele juriidilistele isikutele ning mõnikord ka füüsilistele isikutele. Kuivõrd küberintsidentide lahendamine ja ennetamine toob kaasa vajaduse piirata põhiõigusi (õigus omandi puutumatusele, eraelu kaitsele jne), peab see põhiseaduse §-de 3 ja 11 alusel põhinema seaduslikul alusel. See tähendab, et põhiõigusi piiravaid meetmeid on riigiasutustel lubatud kasutusele võtta üksnes siis, kui seadus näeb ette nende meetmete kasutamise. Ilma vastava volituseta on riigiasutusel tegutsemine keelatud.

Lisaks sellele, et vastav alus meetme rakendamiseks peab olema sätestatud seaduses, peab see õigusselguse põhimõttest (põhiseaduse § 13 lg 2) tulenevalt olema sõnastatud selliselt, et nii meetme rakendajale kui ka meetme adressaadile oleks selge ja ettenähtav, et meetme rakendajal on volitus selliseid meetmeid võtta. Juhul kui riigiasutuse volitus meetme rakendamiseks tuletatakse liialt avara tõlgendamisega, võib see tuua kaasa olukorra, kus riigiasutus ületab talle seadusega antud volitusi, tegutsedes tegelikult ilma õigusliku aluseta. Selline olukord on vastuolus põhiseadusega ja rikub isikute põhiõigusi. Teisisõnu, et RIA saaks täita oma kohustust tõrjuda ohtusid ja teha seda seaduslikult, peaks RIA-l olema piisavad seaduse tasemel sätestatud õigused riikliku ja haldusjärelevalve meetmete rakendamiseks.

Vastamaks küsimusele, milliseid riikliku ja haldusjärelevalve meetmeid on RIA-l ohtude tõrjumiseks küberkaitsevaldkonnas vaja võtta, analüüsiti erinevaid küberintsidentide olukordi, mis on praktikas ette tulnud ning hinnati KorS-s, HOS-s, ESS-s, LennS-s, RdtS-s, SadS-s ja AvTS-s sätestatud riikliku ja haldusjärelevalve meetmete sobivust nendes olukordades. Sealjuures analüüsiti, kas vajaminevatel meetmetel on olemas piisav seaduslik alus PS § 3 ja 11 mõistes ja kas need vastavad õigusselguse põhimõttele PS § 13 lg 2 mõistes.

Analüüsi tulemusel selgus, et kuigi praegu on üldised õiguslikud alused RIA põhimääruse, KorS, HOS, ESS, LennS, RdtS, SadS ja AvTS alusel justkui olemas, siis põhiseadusega nõutavat seadusliku aluse olemasolu need RIA-le ei paku. Analüüsis jõuti järeldusele, et RIA-l puuduvad turvaintsidentide (küberrünnakute) käsitlemiseks, hoiatuste andmiseks turvaintsidentide ennetamiseks ja küberturve seire teostamiseks vajalikud seadusest tulenevad volitused.

Täpsemalt puuduvad Eesti õiguses vajalikud riikliku ja haldusjärelevalve meetmed, mis võimaldaks küberintsidente efektiivselt ennetada ning tõrjuda. Kuivõrd avalik võim on õigustatud tegutsema üksnes siis, kui seadus annab selleks volituse, tuleb eelnimetatud ülesannete täitmiseks RIA volitused seaduse tasemel sätestada. Näiteks puudub RIA-l volitus

siseneda võrgu- ja infosüsteemi, kontrollida süsteemis andmete töötlemist ja rakendada meetmeid intsidendi ära hoidmiseks, kõrvaldamiseks või selle edasise leviku tõkestamiseks. Samuti puudub RIA-l selge volitus nõuda erinevate teenuste (nt mobiilside teenuse, veebikeskkondade jne) sulgemist võrgu- ja infosüsteemide turvalisuse tagamiseks. Kolmandaks puudub RIA-l õigus paigaldada tehnilisi seireseadmeid ohu tuvastamiseks, ohu olemuse ja ulatuse ning ohu tekitanud isiku kindlaks tegemiseks.

Eelnevalt nimetatud meetmete kasutamisest sõltub otseselt RIA tegevuse tõhusus ohtude ennetamisel ja tõrjumisel. Seetõttu ei ole isikute elu, tervis, vara ja keskkond kaitstud, kui RIA-le ei ole antud seaduse tasandil küberintsidentidega tegelemiseks ja meetmete võtmiseks volitusi. Seetõttu tuleks RIA ülesanded ning vajalikud riikliku ja haldusjärelevalve meetmed sätestada seaduse tasemel.

1. RIA TEGEVUSE ÕIGUSLIK RAAMISTIK

1.1. RIA ülesanded

1. RIA on Majandus- ja Kommunikatsiooniministeeriumi valitsemisalasse kuuluv valitsusasutus, kes on Eestis ainuke küberintsidentidega tegelev ametiasutus[1]. Kuigi RIA roll järelevalveasutusena tuleneb erinevatest seadustest, siis võrgu- ja infosüsteemide turvalisuse ennetus- ja planeerimisalased ülesanded, sh küberintsidentide käsitlemine, tulenevad peamiselt RIA põhimäärusest[2].

2. RIA põhimääruse kohaselt täidab RIA mitmeid avalikke ülesandeid küberturvalisuse ja kriitilise informatsiooni infrastruktuuri kaitse valdkonnas (§ 7). Sealjuures on RIA põhiülesanneteks:

1) haldus- ja riikliku järelevalve teostamine ameti tegevusvaldkondi reguleerivate õigusaktide nõuete täitmise üle ja nende nõuete rikkumise korral riikliku sunni rakendamine;
2) riigi infosüsteemi kindlustavate süsteemide arendamise ja haldamise korraldamine;
3) riigi infosüsteemi arendamise projektide koordineerimine;
4) elektroonilise identiteedi tarkvara ning usaldusteenuste infrastruktuuri arendamise ja haldamise korraldamine;
5) riigi infosüsteemi ja Eesti kriitilise informatsiooni infrastruktuuri infoturbega seotud tegevuste korraldamine;
6) baasinfrastruktuuri ja andmeside korraldamine;
7) riigi infotehnoloogilise arhitektuuri terviklik haldamine;
8) osalemine oma tegevusvaldkonda reguleerivate õigusaktide väljatöötamisel ning nende õigusaktide muutmiseks ettepanekute esitamine;
9) osalemine oma tegevusvaldkonnaga seotud poliitikate, strateegiate ja arengukavade väljatöötamisel (RIA põhimääruse § 8).

3. Nende ülesannete täitmiseks teeb RIA muuhulgas järgmist:

1) korraldab kriitilise informatsiooni infrastruktuuri kaitset ning tegeleb sealhulgas riskianalüüside koostamise ja kriitilise informatsiooni infrastruktuuri kaitseks vajalike turvameetmete arendamisega;
2) koordineerib infoturbe standardite (sh infosüsteemide kolmeastmelise etalonturbe süsteemi) rakendamist riigi ja kohaliku omavalitsuse asutustes ja avalikke ülesandeid täitvate eraõiguslike isikute juures ning töötab nende rakendamiseks välja infoturbe alaseid soovitusi;
3) käsitleb Eesti arvutivõrkudes toimuvaid ja ametile raporteerituid turvaintsidente, annab hoiatusi turvaintsidentide ennetamiseks ning tegeleb kasutajate turvateadlikkuse tõstmisega ja koostab raporteid Eesti arvutivõrkudes toimunud intsidentidest ja kahjurvara levikust;
4) arendab küberturbega seotud strateegiaid ja poliitikaid;
5) teostab küberturbe seiret, hinnates perioodiliselt küberkeskkonna turvalisust ja sellega seotud riske ning nende mõju Eesti riigile ja elutähtsatele teenustele, sealhulgas teostab

[1] 2016. a. advokaadibüroo LEXTAL teostatud "Kübervaldkonna õigusanalüüs" raames läbi viidud intervjuudest selgus, et kokkuleppeliselt peetakse Riigi Infosüsteemi Ametit (edaspidi RIA) kübervaldkonna eest vastutavaks asutuseks. Kättesaadav: https://www.ria.ee/public/Kuberturvalisus/Kubervaldkonna-oigusanaluus-Lextal-2016.pdf

[2] RT I, 29.12.2016, 14.

riigiasutuste vahelise andmeside turvaseiret ning koordineerib riigi infosüsteemi teiste komponentide turvaseire teostamist;

6) teostab järelevalvet elutähtsa teenuse osutamiseks kasutatavate infosüsteemide ning nendega seotud infovarade turvameetmete alalise rakendamise üle;
7) töötab välja ja avaldab juhiseid elutähtsate teenuste infosüsteemide turvalisust tagavate meetmete ja nende rakendamise kohta;
8) teostab järelevalvet infosüsteemide turvameetmete süsteemi rakendamise ja infosüsteemide andmevahetuskihiga liitumise üle;
9) teostab järelevalvet sidevõrkude ja -teenuste turvalisuse ja terviklikkuse tagamise üle;
10) viib läbi väärtegude kohtuvälist menetlemist oma pädevuse piires jne (RIA põhimääruse § 9).

4. Eelmises punktis loetletud tegevused on üksnes osa RIA tegevustest. Kokkuvõtlikult on RIA üheks põhiülesandeks sisuliselt kõikide riigi ja ühiskonna toimimiseks oluliste võrgu- ja infosüsteemide turvalisuse tagamine, mille raames peab RIA käsitlema Eesti arvutivõrkudes toimuvaid turvaintsidente ning andma hoiatusi turvaintsidentide ennetamiseks.

5. Seaduse tasemel on RIA ülesanded küberturvalisuse ja kriitilise informatsiooni infrastruktuuri kaitse valdkonnas reguleeritud avaliku teabe seaduses (AvTS)[3], elektroonilise side seaduses (ESS)[4], hädaolukorra seaduses (HOS)[5], lennundusseaduses (LennS)[6], raudteeseaduses (RdtS)[7] ja sadamaseaduses (SadS)[8].

6. AvTS § 53[1] lg 1 alusel teostab RIA haldus[9]- ja riiklikku järelevalvet[10] infosüsteemide turvameetmete süsteemi rakendamise ning infosüsteemide andmevahetuskihiga liitumise üle. Sisuliselt on RIA ülesandeks kontrollida riigi- ja kohaliku omavalitsuse asutuse, avalik-õiguslik juriidilise isiku, eraõigusliku juriidilise isiku ja füüsilise isiku, kes täidab avalikke ülesandeid, hallatavate andmekogude turvalisust.

7. HOS § 45 lg 1 p 4 alusel teostab RIA haldus- või riiklikku järelevalvet elutähtsa teenuse osutamiseks kasutatavate infosüsteemide ja nendega seotud infovara turvameetmete rakendamise üle. Lisaks HOSis määratletud elutähtsatele teenustele, teostab RIA riiklikku järelevalvet infosüsteemide ja nendega seotud infovara turvameetmete täitmise üle järgmiste teenuse osutajate poolt:

1) lennuvälja käitaja ja aeronavigatsiooniteenuse osutaja (LennS § 60[1] lg 5 alusel);
2) raudtee-ettevõtja, kes majandab avalikku raudteeinfrastruktuuri või kelle kaubaveo või reisijateveo turuosa on vähemalt 20 protsenti kaubaveo või reisijateveo turuosast (RdtS § 71 lg 7[1]);

---

[3] RT I, 06.01.2016, 7.
[4] RT I, 23.03.2017, 6.
[5] 01.07.2017 jõustuv hädaolukorra seadus (RT I, 03.03.2017, 1).
[6] RT I, 03.03.2017, 16 (01.07.2017 jõustuvad muudatused).
[7] RT I, 16.05.2017, 3 (01.07.2017 jõustuvad muudatused).
[8] RT I, 03.03.2017, 24 (01.07.2017 jõustuvad muudatused).
[9] Haldusjärelevalve on haldusesisese (internse) järelevalve liik, mille korral kontrollib üks haldusekandja (juriidiline või füüsiline isik, kes täidab avaliku halduse ülesannet) teise haldusekandja poolt haldusülesande täitmist, samuti sama haldusekandja organite vahel väljaspool alluvusvahekorda toimuv seaduslikkuse ja otstarbekuse kontroll. See hõlmab nii ohtude tõrjumist ja rikkumise kõrvaldamist kui ka ülesannete täitmise otstarbekuse hindamist. Korrakaitse seaduse eelnõu, lk 14 kättesaadav: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/8a9c2286-06fc-65d2-957b-bd9e11a940c4
[10] Riiklik järelevalve on korrakaitseorgani tegevus eesmärgiga ennetada ohtu, selgitada see välja ja tõrjuda või kõrvaldada korrarikkumine. (KorS § 2 lg 4). Riiklikku järelevalvet teostatakse halduse väliste isikute üle, see on suunatud haldusevälistе ohtude väljaselgitamisele ja tõrjumisele.

3) sadam, mis teenindab rahvusvahelises meresõidus sõitvaid reisilaevu või 500-se ja enama kogumahutavusega laevu ning mis teenindavad meresõiduohutuse seaduse kohaselt määratletud kohalikus rannasõidus sõitvaid I kategooria laevu või A-klassi reisilaevu (SadS § 42 lg 5).

8. ESS § 133 lg 5 alusel on RIA-l õigus teostada riiklikku ja haldusjärelevalvet:

1) sideettevõtjate üle sidevõrkude ja -teenuste turvalisuse ja terviklikkuse tagamise osas ning

2) kriitilise tähtsusega side, mereraadioside ja operatiivraadiosidevõrgu teenuse osutajate üle infosüsteemide ja nendega seotud infovara turvameetmete täitmise osas.

9. **Kokkuvõttes on seaduse tasemel RIA ülesannetest reguleeritud järelevalvefunktsioon teatud valdkondade võrgu- ja infosüsteemide turvalisuse üle, st kas ettevõtjad ja asutused järgivad nendes valdkondades sätestatud turvameetmeid. Samal ajal on jäetud seaduse tasandil reguleerimata ohtu ennetavad ja tõrjuvad tegevused, nagu turvaintsidentide (küberrünnakute) käsitlemine, hoiatuste andmine turvaintsidentide ennetamiseks ning küberturve seire teostamine.** Sellele puudujäägile RIA tegevust puudutavas regulatsioonis ning vajadusele sätestada RIA ülesanded seaduse tasemel, on viidatud ka varasemates õigusanalüüsides.[11] Probleem seisneb selles, et vastavalt PS §-le 3 lõikele 1 teostatakse riigivõimu üksnes põhiseaduse ja sellega kooskõlas olevate seaduste alusel ning kui seadusandja soovib RIA-le panna info- ja võrgusüsteemide turvalisuse tagamisel ülesandeid, mille abil võib RIA kitsendada kolmandate isikute õigusi, siis tuleb RIA vastavad ülesanded loetleda seaduse tasemel (vt ka järgmine alapeatükk).[12]

10. Kuivõrd seaduse tasemel on RIA ülesannete õiguslikud alused puudulikud, on vajalik vastava õigusliku raamistiku loomine. Selle loomisel tuleb muuhulgas juhinduda põhiseaduslikest väärtustest ning põhimõtetest. Järgnevalt käsitletaksegi neid põhiseaduslikke väärtuseid ning põhimõtteid, mis on aluseks RIA tegevusele ning millega tuleb õigusliku raamistiku loomisel arvestada.

1.2. Põhiseadusest tulenevad aluspõhimõtted, millest RIA peab oma tegevuses lähtuma

1.2.1. Kohustus tagada sisemine ja välimine rahu (PS preambula)

11. Põhiseaduse preambula 4. lõik sätestab *expressis verbis*, et riigi esmane ülesanne on sisemise ja välise rahu ning julgeoleku kaitsmine ühiskonnas. Sisemise rahu puhul ähvardab riiki ja ühiskonda oht seestpoolt, nt kuritegevus, nakkushaigused, loodusõnnetused ja inimesed, kes eiravad õiguslikke ning muid ühiselureegleid ega täida oma kohustusi.[13] Sealjuures mõeldakse sisemise rahu all eelkõige sisepoliitilist stabiilsust, avalikku korda ehk *ordré public*'i, ilma milleta ei ole võimalik teostada täiel määral muid riikluse eesmärke (nt vabadus, õiglus, õigus, rahu jne). Välimise rahu ja julgeoleku kaitsmise puhul ähvardab ühiskonda väljastpoolt tulenev oht, nt võõrriigi agressioon.

---

[11] 2016. a. advokaadibüroo LEXTAL teostatud "Kübervaldkonna õigusanalüüs". Kättesaadav: https://www.ria.ee/public/Kuberturvalisus/Kubervaldkonna-oigusanaluus-Lextal-2016.pdf; 2013. a advokaadibüroo SORAINEN AS teostatud „Kriisireguleerimise valdkonna juriidiline analüüs" Kättesaadav: https://www.siseministeerium.ee/sites/default/files/dokumendid/kriisireguleerimise_valdkonna_juriidiline_analuus.pdf

[12] Vt ka 2016. a. advokaadibüroo LEXTAL teostatud "Kübervaldkonna õigusanalüüs". Kättesaadav: https://www.ria.ee/public/Kuberturvalisus/Kubervaldkonna-oigusanaluus-Lextal-2016.pdf

[13] R. Narits, H. Schneider. Kommentaar preambulale – Justiitsministeerium, Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. Kolmas täiendatud väljaanne. Tallinn 2012, preambula, komm 14.

12. Kohustusest tagada sisemine ja välimine rahu tuleneb otseselt riigi ametiasutuste ülesanne kaitsta riigi sisemist korda ja julgeolekut ning moodustada selleks ka vajalikke institutsioone, kes ei ole kohustatud mitte üksnes tegelema õigusrikkumistega, vaid peavad looma ka tingimused nende vältimiseks.[14] Turvaintsident (küberintsident) võib seada ohtu olulise või elutähtsa teenuse toimimise, mis võib omakorda seada ohtu inimese elu, tervise, vara ja keskkonna ning riigi julgeoleku. Sealjuures ei ole küberturvalisuse puhul tegemist üksnes sisemise rahu küsimusega, vaid oma rahvusvahelise leviku ja mõõtmete tõttu on tegemist välise rahu ja julgeoleku küsimusega. **Turvaintsident võib seega mõjutada nii sisemist kui ka välimist rahu. Seetõttu on riigi põhifunktsiooniks muuhulgas küberintsidentidega tegelemine, sest riik on selleks PS preambula alusel kohustatud.**

1.2.2. Õigus korraldusele ja menetlusele (PS § 13 lg 1 ja PS § 14)

13. Põhiseaduse §-st 13 tulenevalt on igaühel õigus riigi ja seaduse kaitsele. Põhiseaduse § 14 järgi on õiguste ja vabaduste tagamine seadusandliku, täidesaatva ja kohtuvõimu ning kohalike omavalitsuste kohustus. Nendest põhiseaduse sätetest tuleneb igaühe õigus riigi või kohaliku omavalitsuse korraldusele ja menetlusele.[15] See sisaldab endas õigust nii riigi normatiivsele kui ka faktilisele tegevusele, et isik saaks end kaitsta ja turvaliselt tunda.[16]

14. Normatiivselt on riigil põhiseaduse § 14 järgi kohustus luua põhiõiguste kaitseks kohased menetlused[17]. Faktiliselt on isikul kaitseõigusest tulenevalt õigus nõuda riigi aktiivset sekkumist ja riigil on kohustus võtta tarvitusele vastavad abinõud kolmanda isiku suhtes. Sealjuures on isikul õigus nõuda riigilt seda, et riik looks vastavad asutused ning annaksid neile asutustele piisavad volitused, et nendel asutustel oleks võimalik faktiliselt isiku põhiõiguseid kaitsta.

15. Kuivõrd küberintsidentide toimumine võib ohustada nii riigi sisemist kui välimist rahu, on seadusandjal PS §-dest 13 ja 14 tulenevalt kohustus kehtestada regulatsioon, mis tagaks efektiivse küberintsidentide lahendamise ja ennetamise. **Vastasel juhul ei täidaks riik oma ülesannet tagada sisemist ja välist rahu.**

16. Teisisõnu on seadusandjal kohustus luua vastav asutus, kes tegeleks küberintsidentide lahendamise ja ennetamisega ning kellele tuleb anda piisavad volitused oma ülesannete täitmiseks. RIA on loodud VVS § 42 lõike 1 alusel ning kokkuleppeliselt peetakse RIA-t kübervaldkonna ja küberintsidentide eest vastutavaks asutuseks. Samas ei saa RIA volitusi pidada piisavaks, mida selgitatakse järgnevates punktides.

1.2.3. Seaduslikkuse ja seadusliku aluse põhimõte (PS § 3 lg 1)

17. PS § 3 lõike 1 esimese lause kohaselt teostatakse riigivõimu üksnes põhiseaduse ja sellega kooskõlas olevate seaduste alusel. Sellest tuleneb täitevvõimu põhiseaduslik seotus seaduse ja õigusega, mis on üks vabadusliku õigusriigi möödapääsmatutest tingimustest[18]. Seda järgmisel põhjusel. *Seaduslikkuse kui (rahvusvahelise) õiguse üldtunnustatud põhimõtte ning Eesti Vabariigi Põhiseaduse §-s 3 sätestatud printsiibi kohaselt võib põhiõigusi ja vabadusi piirata üksnes seaduse alusel. Seadusega kindlaksmääratud ja avalikustatud õiguste ja vabaduste piiramise kord ning avalikkus võimaldab valikuvabaduse ning tagab võimaluse vältida võimu kuritarvitust. Põhjaliku seadusandliku regulatsiooni puudumine ja varjatus jätab aga isiku ilma*

[14] R. Narits, H. Schneider. Kommentaar preambulale – Justiitsministeerium, Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. Kolmas täiendatud väljaanne. Tallinn 2012, preambula, komm 14.
[15] RKÜKo 3-4-1-5-02, p 30; 3-1-1-86-0,7 p 23.
[16] RKÜKo 3-1-1-86-07, p 23.
[17] RKPJKo 3-4-1-4-03, p 16.
[18] Fr. Schoch. Üldklausli vältimatus nüüdisaegses ohutõrjeõiguses. – Juridica 2010/8, lk 541.

õigusest informatsioonilisele enesemääratlusele, valida käitumisjoont ja end kaitsta.[19] Seetõttu peab sellised küsimused, millega piiratakse isikute põhiõigusi, otsustama seadusandja ning seadusandja ei saa seda edasi delegeerida täitevvõimule.[20]

18. PS § 3 lg 1 esimene lause sisaldab seega olulisuse põhimõtet ja seadusliku aluse nõuet, mis tähendab, et igal põhiõiguse riivel peab olema seaduslik alus ning seadusandja ei saa aluse kehtestamist delegeerida täitevvõimule. Põhiõiguste seisukohalt võib oluline olla (ja seega kuuluda seaduse reguleerimisesemesse) nii õiguste piiramise üksikasjalik kord kui ka pädeva organi määramine.[21] Riigikohus[22] on oma praktikas leidnud, et riigiasutuse õigus teha ettekirjutusi ei saa tuleneda põhimäärusest, vaid avalik võim on õigustatud tegutsema üksnes siis, kui seadus annab selleks volituse. See tähendab, et ametiasutus ei või tungida kodaniku õigusteringi, kui seadus seda võimalust ette ei näe.[23] Teisisõnu on avalik võim õigustatud tegutsema üksnes siis, kui seadus annab selleks volituse[24], mistõttu eeldab põhiõiguste piiramine seadusandjast alamalseisva organi poolt seadusandja volitust[25].

19. Eelnevast tulenevalt peab ametiasutuse tegevus, sh volitused meetmete rakendamiseks või korralduste andmiseks olema loodud seaduse tasandil ning kooskõlas põhiseadusega. Seetõttu peaksid RIA volitused küberintsidentide käsitlemiseks, hoiatuste andmiseks ning küberturve seire teostamiseks, sh vastavate riikliku ja haldusjärelevalve meetmete kohaldamiseks selle raames, olema sätestatud seaduse tasemel.

1.2.4. Õigusselguse põhimõte (PS § 13 lg 2)

20. PS § 13 lõikest 2 tuleneva õigusselguse põhimõtte kohaselt peavad õigusaktid olema piisavalt selged ja arusaadavad, et isikutel oleks mõistlik võimalus riigi tegevust ette näha ja kohandada oma tegevust sellele vastavalt.[26] Nõutav normi määratletuse ehk õigusselguse aste ei ole kõikide normide puhul sama. Riigikohus on selgitanud, et põhiseadusega nõutava normi määratletuse ehk õigusselguse nõude kohaselt peavad olema selgemad ja täpsemad need õigusnormid, mis võimaldavad isiku õigusi piirata[27].

21. Põhiseaduslike printsiipide järgimiseks ning igaühe põhiõiguste ja vabaduste kaitseks peavad legislatiiv- ja haldusfunktsioonid olema eristatud ja täpselt määratletud ning nende funktsioonide täitmine peab toimuma kooskõlas PS-ga ja õigusteoorias tunnustatud põhimõtetega. Pädevuse umbmäärasus, samuti pädevuse ületamine kahjustab üldist õiguskindlust ning loob ohu põhiseaduslikele printsiipidele ning igaühe õiguste ja vabaduste kahjustamiseks.[28] Õigusselguse põhimõte keelab riigivõimu omavoli, teisisõnu tagab selle, et üksikisikul on võimalik riigiorganite käitumist teatava tõenäosusega ette näha ja sellega arvestada[29].

22. **Eelnevast tulenevalt peavad RIA volitused oma ülesannete täitmisel, mis puudutavad ka teisi isikuid (eraõiguslikke isikuid, avalik-õiguslikke isikuid kui ka teisi riigiasutusi), olema piisavalt määratletud ehk kooskõlas õigusselguse põhimõttega.**

---

[19] RKPJKo III-4/A-1/94.
[20] RKPJKo III-4/A-1/94.
[21] M. Ernits. Põhiõigused, demokraatia, õigusriik. Tartu Ülikooli Kirjastus 2011, lk 264. vt ka RKHKm 3-3-11-77-03, p 24.
[22] RKHKo 3-3-1-41-00, p 4.
[23] J. Kaiv, J. Klesment. Eesti Vabariigi põhiseadus, § 3.
[24] RKHKo 3-3-1-41-00, p 4.
[25] RKPJKo 3-4-1-5-05, p 9; 3-4-1-14-09, p 34
[26] RKÜKo 3-4-1-33-09, p 47.
[27] RKPJKo 3-4-1-16-05, p 21.
[28] RKPJKo 3-4-1-3-96, p I.
[29] M. Ernits. Kommentaarid §-le 10. – Justiitsministeerium, Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. Kolmas täiendatud väljaanne. Tallinn 2012, § 10, komm 3.4.3.1.

1.2.5. Proportsionaalsuse põhimõte (PS § 11 lg 1)

23. PS § 11 lg 1 alusel tohib õigusi ja vabadusi piirata ainult kooskõlas põhiseadusega ning need piirangud peavad olema demokraatlikus ühiskonnas vajalikud ega tohi moonutada piiratavate õiguste ja vabaduste olemust. Seadus on demokraatlikus ühiskonnas vajalik siis, kui see on püstitatud eesmärgi saavutamiseks sobiv (kohane), vajalik kitsamas tähenduses (tarvilik) ja proportsionaalne kitsamas tähenduses (mõõdukas).[30]

24. Proportsionaalsuse põhimõte ehk ülemäärasuse keeld seob kogu riigivõimu, nii õiguse kohaldaja kui ka seadusandja.[31] See on õigusriigi keskseks põhimõtteks ja selle aluseks on idee, et riik tohib isiku vabadussfääri üldistes huvides piirata üksnes niivõrd, kuivõrd see on möödapääsmatu.[32]

25. **Eelnevast tulenevalt peavad seaduse tasandil sätestatud meetmed, millega sekkutakse isiku põhiõigustesse või –vabadustesse, järgima proportsionaalsuse printsiipi. Seega peavad ka RIA rakendatavad riikliku ja haldusjärelevalvemeetmed, millega riivatakse põhiõigusi või -vabadusi, vastama proportsionaalsuse põhimõttele.**

1.3. RIA kasutuses olevad haldus- ja riikliku järelevalvemenetluse meetmed

26. Põhiseaduslike põhimõtete kõrval reguleerivad RIA tegevust AvTS, HOS, ESS, LennS, RdtS ning SadS, mis sätestavad muuhulgas RIA õigused (meetmed) haldus- ja riikliku järelevalvemenetluse raames. Järgnevalt käsitletaksegi seda, milliseid haldus- ja riikliku järelevalvemenetluse meetmeid võib RIA kehtiva õiguse alusel oma ülesannete täitmiseks kasutada.

1.3.1. Haldusjärelevalvemenetlus

27. Haldusjärelevalve on haldusesisese (internse) järelevalve liik, mille korral kontrollib üks haldusekandja (juriidiline või füüsiline isik, kes täidab avaliku halduse ülesannet) teise haldusekandja poolt haldusülesande täitmist.[33] Samuti on haldusjärelevalveks sama haldusekandja organite vahel väljaspool alluvusvahekorda toimuv seaduslikkuse ja otstarbekuse kontroll. Seega hõlmab haldusjärelevalve eelkõige selle kontrollimist, kas haldusekandja on täitnud oma seadusest tulenevaid kohustusi. Küberintsidenti toimumisel ei ole põhiküsimus haldusekandja tegevuse seaduslikkusest ega otstarbekusest, vaid ohu tõrjumisest. Haldusekandja võib teha kõik vastavalt seadusele, kuid sellegi poolest võib küberintsident halvata haldusekandja tegevuse. Samas selgitatakse korrakaitse seaduse eelnõu seletuskirjas, et haldusjärelevalve hõlmab nii ohtude tõrjumist ja rikkumise kõrvaldamist kui ka ülesannete täitmise otstarbekuse hindamist.[34] Eelnevast tulenevalt ei ole üheselt selge, kas haldusjärelevalve võib põhimõtteliselt hõlmata ohtude ennetamist ning tõrjumist.

28. Haldusjärelevalve pädevus on RIA-le antud RIA põhimääruse, AvTS, HOS ning ESS alusel. LennS, RdtS ning SadS alusel on RIA-le antud üksnes riikliku järelevalve pädevus.

29. Haldusjärelevalve meetmed on sätestatud Vabariigi Valitsuse seaduse (VVS) §-s 75^1. VVS § 75^1 lg 3 kohaselt võib RIA haldusjärelevalve raames riigi haldusorgani suhtes puuduse

---

[30] M. Ernits. Kommentaarid §-le 11. – Justiitsministeerium, Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. Kolmas täiendatud väljaanne. Tallinn 2012, § 11, komm 3.
[31] RKPJKo 3-4-1-6-00, p 13; 3-4-1-2-01, p 16; 3-4-1-6-01, p 17; RKÜKo 3-4-1-7-01, p 21.
[32] M. Ernits. Kommentaarid §-le 11. – Justiitsministeerium, Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. Kolmas täiendatud väljaanne. Tallinn 2012, § 11, komm 3.
[33] Korrakaitse seaduse eelnõu, lk 14 kättesaadav: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/8a9c2286-06fc-65d2-957b-bd9e11a940c4
[34] Korrakaitse seaduse eelnõu, lk 14 kättesaadav: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/8a9c2286-06fc-65d2-957b-bd9e11a940c4

korral teha ettekirjutuse (lg 3). Teiste haldusekandjate suhtes on RIA-l õigus kohaldada lisaks ettekirjutusele selle täitmata jätmise korral sunniraha, mille ülemmäär 9600 eurot (VVS § 75^1 lg 4). RIA-l on VVS § 75^2 alusel lisaks õigus võtta järgmiseid meetmeid:

1) nõuda järelevalvatavalt seletusi ja dokumentide esitamist;
2) peatada järelevalvatava asjakohane ametnik või töötaja ning teda küsitleda;
3) kontrollida meeleliselt või tehnilise vahendi abil järelevalvatava valduses olevat vallasasja, sealhulgas avada uksi ja kõrvaldada muid takistusi;
4) võtta järelevalvatava valduses olev vallasasi hoiule ning vajaduse korral hoiulevõetud vallasasi müüa või hävitada;
5) siseneda järelevalvatava territooriumile, piiratud või tähistatud kinnisasjale, ehitisse ja ruumi, sealhulgas avada uksi ja väravaid ning kõrvaldada muid takistusi;
6) jäädvustada olukord, võtta proove ja näidiseid, samuti teostada mõõtmisi ning teha ekspertiisi;
7) rakendada seaduses sätestatud muid haldusjärelevalve meetmeid.

30. Nii VVS kui ka asendustäitmise ja sunniraha seaduse (ATSS) § 5 lg 1 kohaselt ei ole sunnivahendit võimalik rakendata riigiasutuse suhtes. Seega on RIA-l võimalik sunniraha määrata ettekirjutuse täitmata jätmisel üksnes kohalikule omavalitsusele ning avalik- ja eraõiguslikule isikule, kes täidab AvTS alusel avalik- õiguslikku funktsiooni ja on AvTS tähenduses teabevaldajaks või kes on HOS ja ESS alusel haldusekandjateks.

1.3.2. Riiklik järelevalvemenetlus

31. Nagu eelnevalt selgitatud on riikliku järelevalve pädevus antud RIA-le nii RIA põhimääruse, AvTS, HOS, ESS, LennS, RdtS kui ka SadS alusel. Riiklik järelevalve on korrakaitseorgani[35] tegevus eesmärgiga ennetada ohtu, selgitada see välja ja tõrjuda või kõrvaldada korrarikkumine, mida teostatakse halduse väliste isikute üle (KorS § 2 lg 4). KorS § 1 lõige 7 kohaselt ei kohaldata KorS-i ühe haldusorgani poolt teise haldusorgani tegevuse õiguspärasuse ja otstarbekuse üle järelevalve teostamisel ega ühe haldusekandja poolt teise haldusekandja haldusülesande täitmise õiguspärasuse ja otstarbekuse üle järelevalve teostamisel.

32. Riigikohus on Andmekaitse Inspektsiooni ja Riigikogu Kantselei vahelises vaidluses selgitanud, et kehtiv õigus ei näe otsesõnu ette riiklikku järelevalvet riigiasutuste üle.[36] Sellest tulenevalt on riikliku ja haldusjärelevalve kohaldamise ulatust peetud ebaselgeks[37] (vt ka punkt 27). Eelnevast tulenevalt ei ole võimalik üheselt öelda, kas KorS-is sätestatud järelevalvemeetmeid ja sunnivahendeid ohtude ennetamiseks ja tõrjumiseks on võimalik kasutada teiste haldusorganite või riigiasutuste vastu.

33. Korrakaitseasutusena on RIA-l õigus kasutada KorS-s sätestatud riikliku järelevalve üldmeetmeid:

1) teavitamist (KorS § 26);
2) ohukahtluse korral kohaldada seaduses ettenähtud meetmeid ohu olemasolu väljaselgitamiseks (KorS § 27);
3) kohaldada ettekirjutust ja haldussunnivahendit (KorS § 28);

---

[35] Korrakaitseorgan on seaduse või määrusega riikliku järelevalve ülesannet täitma volitatud asutus, kogu või isik (KorS § 6 lg 1).
[36] 3-3-1-90-14, p 14.
[37] http://www.aki.ee/et/andmekaitse-inspektsiooni-peadirektori-erakorraline-ettekanne-avaliku-teabe-seaduse-jarelevalve

4) kasutada vahetut sundi (KorS § 28 lg 3);
5) tõrjuda ise ohtu või kõrvaldada korrarikkumine (KorS § 29).

34. Ettekirjutust, haldussunnivahendit ning vahetut sundi on võimalik kohaldada ainult siis kui vastava ohu tõrjumine on RIA pädevuses. Nimelt selgitatakse KorS seaduseelnõu seletuskirjas, et *vastava ohu tõrjumine peab olema korrakaitseorgani pädevuses, s.t õigusakt peab sätestama selle ohu tõrjumise korrakaitseorgani ülesandena. Volitus vastava ohu tõrjumiseks sekkuda isikute põhiõigustesse või muudesse subjektiivsetesse õigustesse ei tohi tuleneda ühestki muust alusest (erimeetmed) ning oht peab nõudma korrakaitselist sekkumist kaalutlusõiguse alusel*.[38] Kuivõrd RIA põhimäärus sätestab RIA ülesannetena turvaintsidentide (küberrünnakute) käsitlemise, hoiatuste andmise turvaintsidentide ennetamiseks ning küberturve seire teostamise, on RIA KorS mõistes pädev asutus ning seega korrakaitseasutus.

35. Lisaks üldmeetmetele võib RIA kasutada riikliku järelevalvemeetmeid seaduses sätestatud juhul, ehk teisisõnu juhul siis kui eriseadus annab selleks RIA-le erivolituse.[39] Erivolitused on RIA-le antud AvTS § 53^1 lg 2, ESS § 133^1, HOS § 46, SadS § 43, RdtS § 72 ning LennS § 60 lg 1^2 alusel, mille alusel on RIA-l volitus kohaldada järgmiseid korrakaitseseaduse sätestatud erimeetmeid korrakaitseseaduses sätestatud alusel ja korras:

1) küsitleda ja nõuda dokumente (KorS § 30);
2) kutsuda isikut ametiruumi, kui on alust arvata, et isikul on andmeid, mis on vajalikud ohu ennetamiseks, väljaselgitamiseks või tõrjumiseks või korrarikkumise kõrvaldamiseks, ning selle ohu ennetamine, väljaselgitamine, tõrjumine või korrarikkumise kõrvaldamine on kutse esitanud korrakaitseorgani pädevuses (KorS § 31);
3) tuvastada isikusamasust (KorS § 32);
4) viia läbi vallasasja vaatlust (KorS § 49);
5) siseneda valdusesse (ilma valdaja nõusolekuta) (KorS § 50);
6) läbi vaadata valdust (Kors § 51);
7) võtta vallasasi hoiule (KorS § 52).

36. Erinevalt AvTS-st on kõikides ülejäänutes seadustes lubatud lisaks eelnevalt nimetatule kasutada erimeetmena hoiule võetud vallasasi müüa või hävitada (KorS § 53).

37. Nii korrakaitse üldmeetmete kui ka erimeetmete rakendamisel on RIA-l sunniraha määramise õigus tulenevalt KorS § 23 lg-st 4. ATSS § 5 lg 1 kohaselt ei ole samas sunnivahendit võimalik rakendata riigiasutuse suhtes.

38. Lisaks KorS-le, sätestavad eriseadused mõned täiendavad erisused. Nimelt sätestab ESS § 87^2 lg 5, et RIA-l on õigus nõuda, et sideettevõtja esitaks oma sideteenuse ja -võrgu turvalisuse ja terviklikkuse hindamiseks vajaliku teabe, sealhulgas turvaeeskirjad ning telliks pädeva sõltumatu asutuse või pädeva riigiasutuse läbi viidava turvaauditi ning teeks selle tulemused RIA-le kättesaadavaks. Sisuliselt on teabe küsimise õigus RIA-l ka KorS § 30 alusel.

39. Lisaks on LennS § 60^2 lg 2 alusel RIA-l õigus:

1) keelata või peatada lennukõlblikkuse või keskkonnakõlblikkuse nõuetele mittevastava õhusõiduki, samuti lennuvälja või kopteriväljaku või mis tahes muu lennundustegevusega seotud objekti, sealhulgas ehitise ja seadme käitamine, kui ei ole tagatud käitamise ohutus, lennu- ja keskkonnaohutus või turvalisus;
2) kõrvaldada lennundustegevusega seotud ülesannete täitmiselt isik, kui kontrolli tulemusel ilmneb, et tema pädevus ei vasta kehtestatud nõuetele, või kui isiku tegevuse

[38] Korrakaitseseaduse eelnõu seletuskiri, lk 52.
[39] Üldmeetme ja erimeetme kohta vt korrakaitse seaduse eelnõu seletuskiri, lk 47.

või tegevusetuse tulemusel ei ole tagatud käitamise ohutus, lennu- ja keskkonnaohutus või turvalisus.

40. Kokkuvõttes on RIA-l haldus- ja riikliku järelevalvemenetluses võimalik kasutada tavapäraseid sellistes menetlustes kasutatavaid meetmed, mida kasutavad analoogsetes menetlustes ka teised riigiasutused. Tähelepanu tuleb juhtida siiski sellele, et haldusjärelevalve meetmete ja riikliku järelevalve erimeetmete kasutamise õigus on antud RIA-le üksnes tegemaks järelevalvet selle üle, kas ettevõtjad ja asutused järgivad seadusega sätestatud turvameetmeid.

41. Muude ülesannete täitmisel, eelkõige ohtu ennetavatel ja tõrjuvatel tegevustel nagu turvaintsidentide (küberrünnakute) käsitlemine, hoiatuste andmine turvaintsidentide ennetamiseks ja küberturve seire teostamine, on RIA tegevus reguleeritud üksnes RIA põhimääruse ja KorS üldmeetmete tasemel. Seetõttu ei ole nende ülesannete täitmiseks seaduse tasemel RIA volitusi täpsustatud, nt pole täpsustatud riikliku järelevalve erimeetmete kasutamist küberintsidentide käsitlemisel. VVS § 70 lg 1 alusel teostavad ametid kui valitsusasutused riiklikku järelevalvet ning kohaldavad riiklikku sundi seaduses ettenähtud alustel ja ulatuses. Seetõttu on kaheldav, kas põhimääruse tasemel RIA järelevalveülesannete sätestamine on piisavad ohtude tõrjumiseks. Nagu alapeatükis 1.2.3. eelnevalt selgitatud, peaksid RIA volitused selliste ülesannete täitmiseks olema sätestatud seaduse tasemel.

42. Isegi kui eeldada, et RIA-le põhimääruse alusel antud ülesanded ja volitused on piisavaks õiguslikuks aluseks eelnevalt kirjeldatud ohtude ennetamisele ja tõrjumisele, on küsitav VVS-s ja KorS-s sätestatud haldus- ja riikliku järelevalvemeetmete rakendatavus küberkaitsevaldkonnas, mis oma sisu poolest erinevad oluliselt klassikalises mõttes korrakaitsetegevusest politsei poolt. Järgnevalt käsitletakse erinevaid näiteid küberintsidentidest ning analüüsitakse olemasolevate järelevalvemeetmete rakendamise võimalusi selliste ohtude ennetamiseks ja tõrjumiseks.

2. OHU TÕRJUMISEKS JA ENNETAMISEKS VAJALIKUD MEETMED

2.1. *Näide nr 1*: *RIA saab teiste riikide väliskolleegidelt informatsiooni, et Eesti arvutivõrgus asuv arvuti või seade on nakatunud ohtliku kahjurvaraga, mis võib ohustada Eestis asuvaid elutähtsa teenuse osutajaid.*

43. Ohu kõrvaldamiseks peab RIA tuvastama kahjurvara jagava serveri, tegema kindlaks kahjurvara serveri käsujagaja ning ka ründeobjektid (sh nakatunud IP-aadressi, arvuti või seadme omanikud). Sealjuures on RIA-l vaja välja saata hoiatusteated sideettevõtjale, et nende võrgus on teatud IP-aadresside puhul tuvastatud kahjurvara. Sideettevõtjad peaksid seejärel omakorda ohu ise kõrvaldama või andma oma teenuse kasutajatele kahjurvaraga nakatumisest teada.

44. Ohu tõrjumiseks eelnevalt kirjeldatud viisil on RIA-l vaja võrguliikluse protokolle ja logisid ehk teisisõnu elektroonilise side logiandmeid ESS § 111[1] lg 3 tähenduses[40] (mis

[40] Need andmed on: 1) sideettevõtja poolt eraldatud kasutajatunnused;
2) telefoni- või mobiiltelefonivõrku siseneva side kasutajatunnus ja telefoninumber;
3) kliendi nimi ja aadress, kelle nimele Interneti-protokolli aadress, kasutajatunnus või number olid side toimumise ajal eraldatud;
4) Interneti-telefoni kõne kavandatud vastuvõtja kasutajatunnus või number;
5) kavandatud vastuvõtva kliendi nimi, aadress ja kasutajatunnus elektronposti ning Interneti-telefoni teenuse korral;

IP-aadressil oht asub, mis arvuti või programm on selle IP-aadressiga seotud). Pärast IP-aadressi tuvastamist on vaja lisaks analüüsida interneti kasutamise ajalugu, et tuvastada probleemi allikas – kuidas sattus seadmesse või programmi kahjurvara. Riikliku järelevalve teostamise käigus on RIA-l tulenevalt ESS §-st 87² lõikest 5 õigus teenusepakkujalt nõuda, et teenusepakkuja esitaks RIA-le sideteenuse ja -võrgu turvalisuse ja hindamiseks vajaliku teabe. Samas reguleerib see säte olukordi, kus RIA kontrollib, kas on sideettevõtja on järginud sideteenuse ja -võrgu turvalisuse nõudeid, mitte olukordi, kus oht on tekkinud sideteenuse ja -võrgu teenuse kasutaja tegevusest (on külastanud veebilehti, mille tulemusel on temale kuuluv seade nakatunud kahjurvaraga).

45. Teiseks on RIA-l õigus nõuda riikliku järelevalve käigus dokumentide esitamist KorS § 30 alusel. Isegi kui võrguliikluse protokolle ja logisid võiks mööndustega pidada dokumentideks (ÕS järgi on dokument *ametlik paber, kiritõend*, kuid võrguliikluse protokollide puhul tegemist on andmetega, mis ei ole dokumendi kujul), võivad võrguliikluse protokollid ja logid sisaldada endast isikuandmeid, mistõttu ei tohi sideettevõtjad ja teised asutused ja eraisikud neid andmeid kolmandale osapoolele avaldada. Selliste andmete avaldamine on lubatud üksnes kliendi nõusolekul või seaduse alusel. Riikliku järelevalve erimeetmena näeb KorS § 35 sellise võimaluse ette, kuid üksnes juhul, kui seadus näeb sellise võimaluse RIA-le ette. Need asutused, kellele sideettevõtja tohib sideandmeid, sh IP-aadresse, edastada, on määratletud ESS §-s 111[1]. RIA-t nende asutuste loetelus, kes nendele andmetele ligipääsu saavad nõuda, nimetatud ei ole.

46. Eelnevast tulenevalt ei anna ESS, KorS ega ka muu seadus RIA-le õigust küsida sideettevõtjatelt võrguliikluse protokolle ja logisid, sh IP aadresside kohta käivat informatsiooni. Isegi kui sellised päringud ei sisalda otseselt isikuandmeid – teada on üksnes IP-aadress, aga mitte isikud nende IP-aadresside taga, on vaieldav, et tegemist on dokumentidega KorS mõistes. Õigusselguse põhimõttest tulenevalt peaks seaduse tasemel olema selgelt sätestatud, et RIA-l on õigus selliseid päringuid esitada.

47. Eelnevast tulenevalt teeme ettepaneku kaaluda ESS täiendamist selliselt, et ESS § 111[1] lõikes 11 teabe saamiseks õigustatud isikute loetelu lisatakse RIA. Samas tuleb andmetele ligipääsu reguleerimisel arvestada Euroopa Kohtu kohtupraktikaga, eelkõige kohtuotsusega *Tele2 Sverige*[41], mille kohaselt on elektroonilise side andmetele ligipääsu andmine õigustatud üksnes tõsiste kuritegude avastamise, tõkestamise ja lahendamise eesmärgil, ning mille puhul tuleb kehtestada piisavad tagatised põhiõiguste kaitseks (nt eelnev kohtulik kontroll jne).

48. Vastava regulatsiooni kehtestamisel tuleks kaaluda kaheastmelise ligipääsu seadmist andmetele. Esiteks, ohu põhjustaja ja mõjutatud (ohustatud) isikute väljaselgitamine võiks esmalt toimuda isikustamata andmete põhjal – RIA-l pääseb küll võrguliikluse andmetele ligi, kuid ei tea, kellele IP-aadress, kasutajatunnus või number kuuluvad (nn isikustamata andmed). Selle põhjal saab RIA vajadusel välja saata hoiatusteated sideettevõtjatele, et nende võrgus on teatud IP-aadresside puhul tuvastatud kahjurvara ning paluda neil IP-aadressi kasutajat teavitada.

---

6) Interneti-seansi alguse ja lõpu kuupäev ning kellaaeg konkreetse ajavööndi järgi koos Interneti-protokolli aadressiga, mille on kasutajale eraldanud Interneti-teenuse osutaja, ja kasutajatunnusega;
7) elektronposti või Interneti-telefoni teenuse kasutamise alguse (log-in) ja lõpu (log-off) kuupäev ning kellaaeg konkreetse ajavööndi järgi;
8) kasutatud Interneti-teenus elektronposti ja Interneti-telefoni teenuse korral;
9) helistaja number sissehelistamisega Interneti-ühenduse korral;
10) digitaalne kliendiliin (Digital Subscriber Line – DSL) või mõni muu tunnus side algataja kohta.

[41] EKo 21.12.2016, liidetud kohtuasjad C-203/15 ja C-698/15, Tele2 Sverige AB vs. Post- och telestyrelsen ja Secretary of State for the Home Department vs. Tom Watson jt.

49. Juhul kui tegemist on tõsisema kahjurvarast tuleneva ohuga ning on kahtlus, et tegemist on KarS §-s 206 lg 2 punktis 3 nimetatud kuriteoga ning on reaalne oht elule ja tervisele või julgeolekule, võiks RIA-l olla õigus küsida ka andmeid rünnatavate objektide kohta.

2.2. Näide nr 2: RIA avastab, et Eesti arvutivõrgus asuv populaarne veebikeskkond on nakatunud ohtliku kahjurvaraga ning mille külastajad võivad kahjurvara levitades ohustada Eestis asuvaid elutähtsa teenuse osutajaid.

50. Tekkinud ohu tõrjumiseks peab RIA-l olema võimalik teha ettekirjutus infosüsteemi (veebilehe) omanikule või haldajale infosüsteemis oleva kahjurvara likvideerimiseks ning kui oht on tõsine, siis teha ettekirjutus veebikeskkonna ajutiseks sulgemiseks, näiteks keelates sellele siseneda Eesti IP-aadressidelt.

51. KorS § 28 lg 1 alusel saab korrakaitseorgan panna avaliku korra eest vastutavale isikule ettekirjutusega ohu tõrjumise või korrarikkumise kõrvaldamise kohustuse. Samuti saab samaaegselt hoiata teda haldussunnivahendi kohaldamisest.

52. KorS § 15 lg 1 alusel on avaliku korra eest vastutav isik see isik, kes on põhjustanud ohukahtluse või ohu, rikub avalikku korda või on põhjustanud sellise olukorra tekkimise võimaluse, mille realiseerumisel tekib oht või ohukahtlus. Juhul kui infosüsteem (veebiserver, ruuter jmt) on nakatunud kahjurvaraga ning see ei ole juhtunud infosüsteemi omaniku või haldaja tahtliku tegevuse tõttu, ei saa see isik olla põhjustanud ohtu. Samuti on vaieldav, kas isik on põhjustanud sellise olukorra tekkimise võimaluse, kui on võtnud kasutusele vajalikud turvameetmed (isegi kui pole selleks kohustatud), kuid infosüsteem on siiski kahjurvaraga nakatunud.[42] KorS seletuskirja kohaselt ei saa tegevusetust (nt turvameetmete rakendamisel) lugeda ohu tekitamiseks, kui isik pole selleks seaduse alusel kohustatud.[43] Käesoleva näite puhul on tegemist sellise teenuse osutajaga, kes pole kohustatud järgima õigusaktides sätestatud turvalisuse nõudeid. Seetõttu võib käesoleva näite puhul jõuda järeldusele, et infosüsteemi omanik või haldaja ei ole alati avaliku korra eest vastutav isik.

53. Problemaatiline on vastutuse rakendamine ka asjast lähtuva ohu puhul. KorS seletuskiri viitab, et *asja ja omandi mõistete määratlemisel võib lähtuda neile tsiviilõiguses antud sisust (TsÜS § 49, AÕS § 68 lg 1)*. Veebikeskkonnale (infosüsteemile) muu kui TsÜSis ja tavakeeles kasutuses oleva tähenduse andmine laiendaks aga lubamatult KorSis sätestatud ning läheks vastuollu seadusliku aluse ja õigusselguse põhimõttega. Seda põhjusel, et veebikeskkonna puhul ei ole tegemist asjaga TsÜS mõistes. TsÜS § 49 lg 1 lause kohaselt on asi kehaline ese, kuid veebikeskkonda (veebilehte) selleks pidada ei saa. Veebikeskkonna või veebilehe puhul on tegemist dokumendi või teabeallikaga, mis sisaldab andmetekogumit, kuid mis ei ole kehalise eseme kujul.

54. Muu isiku kui avaliku korra eest vastutava isiku võib kohustada ohtu tõrjuma või korrarikkumist kõrvaldama KorS § 16 ning 28 lg 2 alusel asendustäitmise korras.[44] Seda võib

---

[42] Täiendavalt selgitus KorS seletuskirjast põhireeglid vastutuse määramiseks: *1) Oht tuleb lugeda omistatavaks isikule, kes on oma käitumisega selle vahetu põhjustaja. Seos ohu tekkimise ja isiku käitumise vahel ei saa olla kaudne (**vahetu põhjustamine**). Tegevus, mis iseenesest veel ohtu ei tekita, vaid on selle eelastmeks, ei ole korrakaitse seisukohalt käsitatav ohu või korrarikkumise tekitamisena. 2) Isiku tegevus, mis iseenesest veel ohtu ei põhjusta, võib siiski olla vaadeldav korrakaitselise põhjustamisena, kui isik loob teadlikult tingimused, milles teised isikud ei saa praktiliselt käituda muul moel kui ohtu või korrarikkumist vahetult põhjustades, või kui isik kallutab teisi isikuid tahtlikult ohu vahetule tekitamisele või korrarikkumisele (**nn eesmärgiga põhjustamine**).*

[43] KorS seletuskiri: *Tuleks asuda seisukohale, et tegevusetus võib olla korrakaitselise vastutuse aluseks siiski ainult juhul, kui ohutõrjetegevuse kohustus tuleneb õigusaktist*. Lk 37.

[44] Vt ka KorS § 28 lg 4, ATSS § 11 ja 12.

nõuda juhul, kui isik on võimeline ohtu tõrjuma või korrarikkumist kõrvaldama või kui tema valduses on ohu tõrjumiseks või korrarikkumise kõrvaldamiseks vajalik ese ja kui:

1) tegemist on vahetu kõrgendatud ohuga;
2) avaliku korra eest vastutavat isikut ei ole või vastutaval isikul ei ole võimalik ohtu õigel ajal tõrjuda või korrarikkumist kõrvaldada või see ei anna piisavat tulemust;
3) korrakaitseorgan ei saa ise või vabatahtlikult kaasatud isiku abil õigel ajal või piisavalt tulemuslikult ohtu tõrjuda või korrarikkumist kõrvaldada ja
4) kaasamine ei tekita ebaproportsionaalselt suurt ohtu kaasatavale isikule või tema varale ega ole vastuolus kaasatava isiku muude seadusest tulenevate kohustustega (KorS § 16 lg 1).

55. KorS § 16 ja § 28 alusel on seega võimalik, et infosüsteemi (veebikeskkonna) omanik või haldaja võtaks kasutusele meetmeid kahjurvara hävitamiseks. Samad sätted annavad sisuliselt ka aluse RIA-le õiguse nõuda teistsuguste meetmete kasutusele võtmist, näiteks veebikeskkonna sulgemist või teatud IP-aadressidelt sisenemise keelu seadmist, sest selle eesmärgiks on samuti ohu tõrjumine. Milliseid meetmeid on RIA-l konkreetsel juhul õigus kasutusele võtta, sõltub vastava meetme proportsionaalsuse hindamisest. Juhul kui oht on kaalukas ning isik ei suuda kiiresti kahjurvara oma süsteemist kõrvalda, oleks tõhusam vahend keskkonnale ligipääsu piiramine. Samas võib see kaasa tulla olulise kahju ettevõtjale (nt saamata jäänud tulu näol).

56. Kuigi üldine õiguslik alus RIA-l ligipääsu keelamiseks on olemas, siis võttes arvesse õigusselguse põhimõtet, ei pruugi KorS §-dest 16 ja 28 tulenev õigus keelata sisenemine keskkonda või veebilehele, olla isikule piisavalt ettenähtav. Sel põhjusel tuleks kaaluda eraldi vastava õiguse sätestamist seaduse tasemel. Alternatiivselt tuleks kaaluda KorS § 15 lg 4 täpsustamist selliselt, et avaliku korra eest vastutavaks isikuks ning teatud viisil käituma kohustatud isikuks loetakse ka infosüsteemi või serveri haldajat.

2.3. Näide nr 3: Riigiasutuse dokumendihaldussüsteem satub kahjurvaralise ründe alla, mistõttu lekivad riigiasutuse dokumendihaldussüsteemist avalikkusesse asutusesiseseks kasutamiseks mõeldud e-kirjad ja dokumendid.

57. Tekkinud ohu tõrjumiseks peab RIA andma riigiasutustele korraldusi teenuste ja/või nende osutamise mahtude piiramiseks või siis teenuste peatamiseks. VVS § 75^1 lg 3 alusel on RIA-l õigus teha riigiasutusele puuduse kõrvaldamiseks ettekirjutusi. VVS § 75^1 lg 3 alusel hõlmab haldusjärelevalve teise haldusorgani tegevuse õiguspärasuse ning seaduses sätestatud juhul otstarbekuse kontrollimist.

58. AvTS alusel on RIA-l haldusjärelevalveõigus riigiasutuste infosüsteemide turvameetmete süsteemi rakendamise ja infosüsteemi andmevahetuskihiga liitumise üle. Teisisõnu peaks RIA haldusjärelevalve AvTS hõlmama selle kontrollimist, kas riigiasutuse tegevus on õiguspärane, st kas on järgitud seadusega sätestatud turvameetmeid. Ka RIA põhimääruse kohaselt teostab ROA haldusjärelevalve ameti tegevusvaldkondi reguleerivate õigusaktide nõuete täitmise üle. Võimalik ettekirjutus peaks olema samas suunatud sellele, et riigiasutus kasutaks seadusega nõutud ning vajalikke turvameetmeid.

59. Tekkinud vahetu oht võib aga tekkida sõltumata sellest, kas riigiasutus on siiani järginud vajalikke turvalisuse nõudeid, st kas on tegutsenud õiguspäraselt. Seetõttu võivad RIA korraldused teenuste ja/või nende osutamise mahtude piiramiseks või peatamiseks väljuda RIA-le antud haldusjärelevalve pädevusest. Nagu eespool selgitatud, ei saaks RIA tõenäoliselt ohu tõrjumiseks tegutseda ka KorS üldsätete alusel riikliku järelevalve raames, sest KorS-i ei ole tõenäoliselt võimalik kohaldada ühe haldusorgani poolt teise haldusorgani või riigiasutuse suhtes (või vähemasti ei ole see üheselt selge).

60. Lisaks oleks RIA-l vaja anda korraldusi erakorraliste infoturbe meetmete rakendamiseks kõikidele mõjutatud asutustele ja isikutele, kellel on probleemid ilmnenud või kellel on vahetu oht sarnaste probleemide tekkimiseks (ennetavaks tegevuseks). Ka sellise õiguse olemasolu on haldusjärelevalve raames on vaieldav.

61. Eelnevast tulenevalt puudub RIA-l selge alus anda ettekirjutusega korraldusi teenuse ja/või nende osutamise mahtude piiramiseks või peatamiseks. Samuti puudub RIA-l õigus anda korraldusi erakorraliste infoturbe meetmete rakendamiseks kõikidele mõjutatud asutustele ja isikutele, kellel on probleemid ilmnenud või kellel on vahetu oht sarnaste probleemide tekkimiseks.

62. Isegi kui sellised volitused oleksid RIA-l olemas, puuduksid haldussunni võimalused. Nii VVS kui ka ATSS § 5 lg 1 kohaselt ei ole sunnivahendit võimalik rakendata riigiasutuse suhtes. Seega, kui riigiasutus keelduks RIA ettekirjutuse täitmisest, ei saaks RIA kohaldada sunniraha.

63. **Seetõttu tuleks kaaluda kehtiva regulatsiooni täpsustamist selliselt, et RIA-l oleks õigus teha riigiasutusele või teisele haldusekandjale ettekirjutus teenuste osutamise mahtude piiramiseks või peatamiseks küberintsidentide korral ka juhul, kui riigiasutuse või teise haldusekandja senine tegevus on õiguspärane**.

2.4. Näide nr 4: Eesti riigi- ja eraõiguslike asutuste andmesidevõrkusid rünnatakse massiliste hajusate teenustõkestusrünnakutega (DDOS) välisriikides asuvate serverite poolt, mille tõttu on tekkinud häired või teenuste katkemine

64. Nii DDOS kui ka teiste keeruliste kahjurvaraliste rünnete puhul võib teatud juhtudel olla ainuke lahendus isoleerida andmesidevõrk välistest ühendustest. Selle tagajärjel jääks võrk isoleeritult toimima võrgus olevate kohalike klientide vahel, kuid väliste ühenduste ja teenuste osutamine oleks piiratud või katkestatud.

65. Sellise lahenduse kasutamine tähendaks seda, et RIA peaks andma korralduse andmesidevõrgu operaatoritele (st sideettevõtjatele) Eesti nö välismaailmast lahtiühendamiseks (mis tähendaks teenuste osalist katkestamist), et tagada riigisisene teenuste parem toimimine. Samuti võib osutuda vajalikuks katkestada koheselt ka riigi andmesidevõrgu välised ühendused ohu ilmnemisel.

66. Sideettevõtjaid ei saa sellises olukorras pidada avaliku korra eest vastutavateks isikuteks KorS mõistes, kellele saaks panna kohustuse ohu tõrjumiseks (vt eespool alapeatükk 2.2.). Samas on võimalik sideettevõtjaid kaasata korrakaitsesse KorS § 16 ja § 28 lg 2 alusel. Sideettevõtja võib kaasata juhul, kui isik on võimeline ohtu tõrjuma või korrarikkumist kõrvaldama või kui tema valduses on ohu tõrjumiseks või korrarikkumise kõrvaldamiseks vajalik ese ja kui:

1) tegemist on vahetu kõrgendatud ohuga;
2) avaliku korra eest vastutavat isikut ei ole või vastutaval isikul ei ole võimalik ohtu õigel ajal tõrjuda või korrarikkumist kõrvaldada või see ei anna piisavat tulemust;
3) korrakaitseorgan ei saa ise või vabatahtlikult kaasatud isiku abil õigel ajal või piisavalt tulemuslikult ohtu tõrjuda või korrarikkumist kõrvaldada ja
4) kaasamine ei tekita ebaproportsionaalselt suurt ohtu kaasatavale isikule või tema varale ega ole vastuolus kaasatava isiku muude seadusest tulenevate kohustustega (KorS § 16 lg 1).

67. Samas sätestab ESS § 66 alused, millal sideettevõtja võib piirata juurdepääsu sidevõrgule. Muuhulgas võib piirata juurdepääsu sidevõrgule, kui tekib oht sidevõrgu terviklikule toimimisele (ESS § 66 lg 1 p 5), see on vajalik eriolukorra, erakorralise seisukorra või sõjaseisukorra tõttu (p 7), või see tuleneb õigusaktist (p 8). Olukorras, kus tegemist on

tavaolukorra või hädaolukorraga (HOS § 2 lg 1 mõistes), kehtiv õigus sidevõrgu lahtiühendamiseks muust maailmast ei luba. Samas võib piirata juurdepääsu sidevõrgule, kui tekib oht võrgu terviklikule toimimisele. Samas kerkib küsimus, kas olukorras, kus teenuste pakkumises on üksnes osalised häired, on tegemist proportsionaalse meetmega võrreldes kaasneva mõjuga ettevõtja varale (majanduslikule seisule). Seetõttu ei pruugi KorS § 16 lg 1 punktis 4 sätestatud tingimused olla selgelt ja üheselt täidetud, mis võib takistada kiiret ohu tõrjumist. Samuti ei pruugi selline olukord olla piisavalt ettenähtav sideettevõtjale. **Eelnevast tulenevalt ei ole käesoleval hetkel RIA-l selget ja piisavalt ettenähtavat volitust nõuda sideettevõtjatelt andmesidevõrgu isoleerimist (st teenuste osutamise ajutist peatamist). Samasugune õigus puudub RIA-l ka riigiandmeside osas (vt eespool alapeatükk 2.3.).**

68. Eelnevast tulenevalt tuleks täiendada ESS § 66 võimalusega piirata juurdepääsu sidevõrgule seoses küberintsidendiga. Õigusselguse ja piisava ettenähtavuse tagamiseks tuleks kaaluda sellise meetme kohaldamiseks volituse sätestamist vastavas eriseaduses (nt kas ESS-s või eraldi küberturvalisuse seaduses).

2.5. Näide nr 5: Raudtee infosüsteemi vastu toimub kahjurvara rünne, mis väljendub algselt infotabloode häiretes. Selle põhjal tekib kahtlus, et kahjurvara on ühtlasi sattunud raudtee juhtimissüsteemi ning võib häirida märgi- ja foorisüsteemi tööd, kujutada ohtu raudtee pöörangutele nende välise kontrollimise kaudu ning mille tagajärjel võib sattuda ohtu inimeste elu ja tervis.

69. Sellise ohukahtluse[45] korral tuleks viivitamata peatada infosüsteemi töö, tuvastada probleem ja vajadusel süsteemid kahjurvarast puhastada. Selleks peaks RIA esiteks nõudma süsteemi töö peatamist, et kontrollida tegeliku ohu olemasolu (kontrollida ohukahtlust).

70. KorS § 27 alusel on korrakaitseorganil ohukahtluse korral õigus kohaldada seaduses ettenähtud meetmeid ohu olemasolu väljaselgitamiseks. Seetõttu võib RIA ohu väljaselgitamiseks kasutada üksnes neid meetmeid, mis on KorSis ette nähtud ohukahtluse korral (nt KorS § 30, § 31, §-d 49-51). Seetõttu ei ole võimalik RIA-l ohukahtluse korral teha ettekirjutust infosüsteemi töö peatamiseks KorS § 28 alusel.

71. Juhul kui tegemist ei ole ohukahtlusega, vaid ohuga[46], siis KorS § 16 võimaldab kaasata infosüsteemi teenuse osutajat korrakaitsesse (vt eespool alapeatükk 2.2.). Nimelt, raudtee infosüsteemi teenuse osutajat ei saa pidada tõenäoliselt avaliku korra eest vastutavaks isikuks KorS mõistes, kellele saaks panna kohustuse ohu tõrjumiseks (vt eespool alapeatükk 2.2.). Seda eelkõige juhul kui see teenuse osutaja järgis kõiki seaduses sätestatud turvalisuse tagamise nõudeid. Juhul, kui ta seda ei teinud, siis on infosüsteemi teenuse osutaja põhjustanud ise sellise olukorra tekkimise võimaluse. Kuidas selline olukord tekkis, on võimalik välja selgitada alles pärast uurimise läbiviimist, mistõttu ei ole võimalik algselt öelda, kas infosüsteemi teenuse osutaja on avaliku korra eest vastutav isik või mitte ning kas infosüsteemi teenuse osutaja on kohustatud tegutsema või mitte.

72. Juhul kui infosüsteemi teenuse osutaja on muu isik kui avaliku korra eest vastutav isik, võib teenuse peatamise ajal tekitada ebaproportsionaalne äriline kahju, so ohu varale (KorS § 16 lg 1 p 4). Sellisel juhul peab RIA hakkama kaaluma, kas tõenäosus, et juhtub õnnetus, kaalub üles võimalikud majanduslikud kahjud infosüsteemi peatamisega seoses.

---

[45] KorS § 5 lg 6: Ohukahtlus on olukord, kus ilmnenud asjaoludele antava objektiivse hinnangu põhjal ei saa tõenäosust, et korrarikkumine aset leiab, pidada piisavaks, kuid mille puhul on alust arvata, et korrarikkumine ei ole välistatud.

[46] KorS § 5 lg 2: Oht on olukord, kus ilmnenud asjaoludele antava objektiivse hinnangu põhjal võib pidada piisavalt tõenäoliseks, et lähitulevikus leiab aset korrarikkumine.

73. Juhul kui infosüsteemi teenuse osutaja ei suuda probleemi allikat tuvastada või kõrvaldada või ei suuda seda teha piisavalt kiiresti, peaks RIA ohu tõrjumiseks ise kontrollima süsteemi tööd ning vajadusel kahjurvara kõrvaldama. KorS § 29 sätestab üldnormi, mille kohaselt võib pädev korrakaitseorgan ise kohaldada meetmeid ohu tõrjumiseks või korrarikkumise kõrvaldamiseks. Seda üldnormi täpsustavad KorS § 49 (vallasasja läbivaatus) ning KorS § 50 (valdusesse sisenemine), kuid nende erimeetmete kasutamine eeldab erivolituse olemasolu. Kuivõrd küberintsidentide lahendamiseks sellist volitust ette pole nähtud, ei ole RIA-l seda meedet ohu tõrjumiseks võimalik kasutada. Kuivõrd infosüsteemi sisenemine võib seada ohtu ärisaladuse või isikuandmetekaitse, peab selleks RIA-l olema erivolitus.

74. Isegi, kui RIA-l oleks volitus kasutada nimetatud erimeetmeid, siis ei ole need sätted kohaldatavad infosüsteemi suhtes. Nimelt selgitatakse KorS seletuskirjas, et *asja ja omandi mõistete määratlemisel võib lähtuda neile tsiviilõiguses antud sisust (TsÜS § 49, AÕS § 68 lg 1)*. Võrgu ja infosüsteemi näol pole tegemist vallasasjaga TsÜS § 50 lg 2^{47} ja § 49 lg 1^{48} alusel. Tsiviilseadustiku üldosa seadus kommentaaride kohaselt ei ole nt arvutiprogrammid asjad, vaid mõttetegevuse tagajärjel tekkinud immateriaalne hüve.[49] Kuigi konkreetse seadme (nt arvuti) puhul võib olla tegemist vallasasjaga, ei saa selles sisalduvad programmid ja info olla vallasasjad, mistõttu ei ole võimalik nende läbivaatus KorS § 49 alusel.

75. Samal põhjusel ei ole võimalik infosüsteemi sisenemist käsitleda valdusesse sisenemisena. AÕS § 32 sisustab valdust tegeliku võimuna asja üle. Samuti viidatakse KorS § 50 lõikes 1 sisenemisele *piiratud või tähistatud kinnisasjale, ehitisse, eluruumi või ruumi, sealhulgas avada uksi, väravaid ja kõrvaldada muid takistusi*. Kuigi infosüsteemis on võimalik samuti „uksi avada“, viidatakse §-s 50 selgelt kinnisasjale sisenemisele. Infosüsteem seda aga selgelt pole.

76. Infosüsteemi sisenemine võib seada ohtu ärisaladuse või isikuandmetekaitse. Kuivõrd sellisel juhul on tegemist tõsise põhiõiguste riivega, peab selleks olema selge seadusandja volitus selliseks sekkumiseks. Seega, kuigi KorS § 29 alusel on RIA-l õigus võtta meetmeid ohu tõrjumiseks, puudub RIA-l seaduslikkuse ning õigusselguse põhimõttest tulenevalt õigus siseneda võrgu- ja infosüsteemi, kontrollida ohu olemasolu ja süsteemi toimimist ning kõrvaldada kahjurvara. Kuivõrd HOS ei näe raudteeveo ja muude teiste oluliste teenuste toimimist elutähtsa teenusena, siis käesoleva näite puhul ei ole võimalik vastavat volitust sätestada HOS-s. Seetõttu tuleks vastav volitus sätestada küberturvalisuse seaduse tasemel.

2.6. Näide nr 6: Andmesideteenuse osutaja tuumikvõrgu seadmetega on pahatahtlikult manipuleeritud ning kahtlustatakse keerulise kahjurvara sattumist süsteemidesse. Selle tulemusel katkeb suurele osale Eesti klientidest andmesideteenuse osutamine.

77. Antud olukorras ohu tõrjumiseks on RIA rolliks suunata küberintsidendi lahendamist ning pakkuda sideettevõtjatele vajadusel tuge. Samuti peab RIA tagama, et andmesideteenus toimiks riigi seisukohalt kõige kriitilisematele klientidele.

78. Selleks, et RIA saaks probleemide korral efektiivsemalt suunata (tõsiste) intsidentide lahendamist, peab RIA olema kursis reaalsetest ohtudest ja riikliku toe andmise võimalustest. Selleks on RIA-l vaja saada eelnevalt sideettevõtetelt andmeid võrkude ülesehitusest ja paiknemisest. Sealjuures on vaja RIA-l teada, milliseid seadmeid või tarkvara vastav andmesideteenuse osutaja kasutab. RIA-l on ESS § 87^2 lg 5 alusel õigus nõuda, et sideettevõtja esitaks oma sideteenuse ja -võrgu turvalisuse ja terviklikkuse hindamiseks vajaliku teabe. Ka

[47] Asi, mis ei ole kinnisasi, on vallasasi.
[48] Asi on kehaline ese.
[49] § 49, p.3.1.3.

KorS § 30 alusel on RIA-l võimalik isikuid küsitleda ja nõuda dokumente (sh küsida selgitusi kirjalikus vormis). Kuivõrd teabe küsimine ei pruugi olla kõige kiirem ja efektiivsem lahendus, võib osutuda vajalikuks ka tehniliste seireseadmete paigaldamine sideettevõtjate juurde, et tuvastada võimalikud ründed, selle olemus ja ulatus ning teha kindlaks rünnaku allikas.

79. Samas võib selline seireseadmete paigaldamine anda ligipääsu isikuandmetele (sh hõlmab andmete kogumist võrguliikluse kohta). Seetõttu peaks selline võimalus olema üksnes erandjuhtudel, olemas peaksid olema tagatised isikuandmete kaitseks (andmed nt krüpteeritud kujul) ning selle meetme kasutamiseks peaks olema selgelt seadusest tulenev volitusnorm. Hetkel sellist volitusnormi KorS ega ESS alusel sätestatud ei ole, mistõttu tuleks kaaluda vastava normi lisamist ESS-i.

2.7. Näide nr 7: RIA saab teiste riikide väliskolleegidelt informatsiooni, et teatavates elutähtsa teenuse osutajate kasutatavates programmides uuendusi tegemata jättes, on need avatud ohtlike kahjurvarade rünnakutele ning tõsiseks turvalisuse riskiks.

80. Juhul kui on võimalik, et elutähtsa teenuse osutajad Eestis võivad kasutada selliseid seadmeid või programme, mida pole uuendatud ning mis võivad osutuda tõsiseks turvaauguks, on RIA-l vaja sellised teenuse osutajad üles leida. Kuivõrd praktikas ei ole lihtsalt teenuse osutajalt informatsiooni küsimine, kas nad kasutavad vastavaid seadmeid või programme, või üldiste teavituste väljasaatmine (palun uuendage tarkvara), efektiivseks osutunud, on alternatiivseks tõhusaks võimaluseks kogu Eesti võrgu skaneerimine, otsides sisuliselt haavatavaid seadmeid ja programme.

81. Skaneerimist on võimalik teha avalikult kasutatava tarkvaraga ning see on kättesaadav igaühele, mitte üksnes riigiasutustele. **Kuigi sellise tegevusega ei kaasne isikuandmete ega privaatsuse riivet, peaks vastav volitusnorm olema siiski sätestatud seaduse tasemel. Tulenevalt seaduslikkuse põhimõttest, peab riigiasutuse tegevusel olema seaduslik alus. Seetõttu tuleks see volitus sätestada seaduse alusel (nt HOS-is) ning koos sellega näha ette võimalus kohustada teenuse osutajaid täiendavate meetmete võtmiseks turvalisuse suurendamiseks.**