TARTU ÜLIKOOL

ÕIGUSTEADUSKOND

AVALIKU ÕIGUSE INSTITUUT

KRIMINAALÕIGUSE, KRIMINOLOOGIA JA KOGNITIIVSE PSÜHHOLOOGIA ÕPPETOOL

Evelin Elken

ARVUTIKURITEGUSID KÄSITLEVAD SÄTTED KARISTUSSEADUSTIKUS JA NENDE MUUTMISE VAJADUS

Magistritöö

Juhendaja: *dr iur* Erkki Hirsnik

Kaasjuhendaja: *dr iur* Mario Rosentau

TARTU

2014

SISUKORD

SISSEJUHATUS

Reaalmaailma kõrval muutub üha enam kuriteo toimepanemise kohaks virtuaalmaailm, kuna tänapäeva ühiskonnas mõjutab inimeste elukorraldust olulisel määral infotehnoloogia, mille revolutsioon on kaasa toonud selle, et suur osa inimeste loodud väärtusi on kätketud teabesse, mida hoitakse, teisendatakse ja edastatakse universaalsel digitaalsel kujul.[1]

Uute kõrgtasemeliste info- ja kommunikatsiooni-tehnoloogiliste saavutuste kasutamisega avanevad kahjuks ka uued võimalused arvutikuritegude toimepanemiseks. Suur osa informatsioonist, näiteks telefonikõned, lendude andmed ja Interneti-keskkonnas sooritatud ostud, säilitatakse digitaalsel kujul, mistõttu tagavad arvutivõrgud viljaka keskkonna küberkuritegudele.[2]

Arvutikuritegevus kasvab kiiresti kogu maailmas, sest arvutid on üha suuremas hulgas riikides olemas peaaegu igas majapidamises ja järjest enam toiminguid viiakse läbi Interneti vahendusel, mistõttu kasvab ka antud keskkonnas toimepandavate rikkumiste arv. [3] Kuritegude toimepanemiseks kasutatakse üsna sageli arvutit, mis saab olla kuriteo toimepanemise:

- vahend – sellisel juhul sooritatakse erinevaid kuritegusid arvuti vahendusel. Siia alla kuuluvad näiteks erinevad pettused, viiruste levitamised, intellektuaalse omandi õiguste rikkumised, lapsporno jt;
- infokandja – sellisel juhul kogutakse informatsiooni erinevatest võrkudest, mis on süsteemidesse talletatud digitaalselt.
- sihtmärk – selle tulemusena võidakse häirida arvutisüsteemi toimimist või sekkuda selles sisalduvatesse andmetesse.[4]

Kuna umbes 98% pangatoimingutest teostatakse Eestis Interneti vahendusel, siis on üsna selge, et ka kuritegevus püüab kolida sinna, kus liigub raha.[5] Kui varavastaste tavasüütegude arv on olnud enamasti stabiilne ja aastate jooksul isegi vähenenud, siis küberkuritegevuse

[1] V. Praust. Infoühiskond ja selle teetähised. IT haldusjuhtimises. MKM aastaraamat, 1998. Arvutivõrgus: http://www.riso.ee/aastaraamatud/et/pub/1998it/12.htm, 23. aprillil 2014.
[2] G. Stamatellos. Computer Ethics. Jones & Bartlett Publishers, 2007, p 14.
[3] Siseministeerium. Turvalisuspoliitika 2010. Kokkuvõte „Eesti turvalisuspoliitika põhisuunad aastani 2015“ täitumisest. Arvutivõrgus: https://www.siseministeerium.ee/public/Turvalisuspoliitika_2010.pdf, 23. aprillil 2014.
[4] R. W. Downing. Shoring Up the Weakest Link. – Columbia Journal of Transnational Law. Vol 43, No 3, 2005, p 711-713.
[5] Siseministeerium (viide 3).

kasv on jätkunud, sest tõusutententsi on näidanud just arvuti vahendusel toime pandavad varavastased süüteod.[6]

Registreeritud kuritegude statistikast aastatel 2003-2011 nähtub, et KarS § 213 järgi kvalifitseeritavate süütegude arv on pidevalt kasvanud. Kui 2003. aastal registreeriti arvutikelmusi 19-l korral, siis 2008. aastal oli see arv juba 367 ning 2011. aastal 512. Arvutiandmetesse sekkumist KarS § 206 järgi teostati 2003. aastal kolmel korral, 2008. aastal ja 2011. aastal üheksal korral. Arvutisüsteemi ebaseaduslikku kasutamist KarS § 217 järgi registreeriti 2003. aastal kümnel korral, 2008. aastal tõusis see näitaja 22ni ja 2011. aastal juba 40ni.[7]

Samade paragrahvide alusel registreeritud kuritegude statistika aastatel 2011-2013 näitab, et arvutikelmuste arv oli 2012. aastal 456 ning 2013. aastal 470. Arvutiandmetesse sekkumist registreeriti 2012. aastal 14-l ning 2013. aastal 12-l korral. Arvutisüsteemi ebaseaduslikku kasutamist registreeriti aga 2012. aastal 34-l ja 2013. aastal 31-l korral.[8]

Ehkki viimasel paaril aastal on arvutikelmuse ja arvutisüsteemi ebaseadusliku kasutamise juhtumite arv küll minimaalsel määral vähenenud (võrreldes 2011. aastaga), on pikaajaline tendents siiski tõusu suunas. Ka arvutiandmetesse sekkumiste arv viimaste aastatega suurenenud ja seega ei saa lühiajalise statistika põhjal teha põhjapanevaid järeldusi kuritegude vähenemise kohta.

Arvutikuriteod on moodsa ühiskonna arenguga kaasnev nähtus. Erinevad tehnoloogilised lahendused küll lihtsustavad inimeste elu, ent nendega kaasnevad mitmed uuele ja ainulaadsele keskkonnale iseloomulikud ohud. Väljatoodud statistika näitab selgelt, et tegemist on problemaatilise valdkonnaga ja antud kuritegevusliik võib kiirelt kasvada. Küberkurjategijad arendavad pidevalt oma oskusi arvutikuritegude toimepanemiseks, muutudes tegude toimepanemises üha professionaalsemaks. Samuti loovad kurjategijad võrgustikke küberkuritegude toimepanemiseks, põhjustades seeläbi kahju nii üksikisikutele

[6] Siseministeerium. „Turvalisuspoliitika põhisuunad aastani 2015“ täitmise tegevusaruanne 2012. aasta kohta. Arvutivõrgus: https://valitsus.ee/UserFiles/valitsus/et/valitsus/arengukavad/siseministeerium/TPPS%20aruanne%202012.%20aasta%20kohta%20.pdf, 23. aprillil 2014.

[7] J. Salla. Registreeritud kuriteod 2003-2013. Justiitsministeerium. Arvutivõrgus: http://www.just.ee/orb.aw/class=file/action=preview/id=59296/Kuritegevuse+andmed+2003-2013.xlsx, 23. aprillil 2014.

[8] Justiitsministeerium. Kuritegevus Eestis 2010. Kriminaalpoliitika uuringud 15. Arvutivõrgus: http://www.just.ee/orb.aw/class=file/action=preview/id=54700/KuritegevusEestis2010_web.pdf, 23. aprillil 2014.

kui ka organisatsioonidele.[9]

Selleks, et arvutikuritegevust piirata, tuleb antud probleemiga tegeleda nii siseriiklikult kui ka rahvusvaheliselt. Seadusandja passiivsus võib viia olukorrani, kus tehnoloogia kiire arengu tõttu pole võimalik teatud karistust väärivaid tegusid nn ajale jalgu jäänud sätete alla subsumeerida. Kui riigid lähtuvad sarnastest õiguspõhimõtetest oma regulatsioonides, siis võimaldab see kiirema kurjategijate tabamise, hoiab kokku ressursse ning muudab efektiivsemaks riikidevahelise koostöö. Kõik riigid peaksid seadma endale eesmärgiks võimalikult sarnase arvutikuritegudega seonduva regulatsiooni sätestamise.

Juba 2001. aasta Eesti Vabariigi julgeolekupoliitika alustes on tõdetud, et „üha kiirenev elektrooniliste infosüsteemide kasutuselevõtt Eestis ning nende seotus globaalsete infosüsteemidega suurendab arvutikuritegevuse ohtu ja riigi infosüsteemide haavavust. Uued julgeolekuriskid nõuavad riiklike institutsioonide koordineeritud tegevust ja laialdast rahvusvahelist koostööd.“[10]

Eesti langes 2007. aasta kevadel „pronksööl“ laialdaste küberrünnakute ohvriks, mille järel hakkas Eesti Vabariigi Valitsus koostama küberjulgeoleku strateegiat, mis sai valmis 2008. aasta mais.[11] Selle strateegia üks eesmärk on inimeste teavitamine küberkeskkonnas valitsevatest ohtudest. Arvutikuritegude kasvav hulk viitab, et ilmselt ei ole see teavitustöö olnud piisav. Haavatavateks sihtrühmadeks võivad olla eelkõige lapsed ja vanurid, kes ei pruugi olulisel määral olla informeeritud ega teadlikud neid Internetikeskkonnas valitsevatest ohtudest. Kuigi pidevalt rõhutatakse, et oma isiklikke andmeid (krediitkaardiandmeid, pangaparoole jms) ei tohiks ühelgi lehel avaldada või avada tundmatult aadressilt tulnud kirju, tehakse seda ikkagi, põhjustades seeläbi mitmeid negatiivseid tagajärgi. Arvutikuriteo ohvriks langenud inimesed ei teavita tihtipeale õiguskaitseorganeid kuriteost, sest tuntakse piinlikust, neile tekitatud kahju on väike, nad ei oska nimetada konkreetset süüdlast või arvavad, et teo toimepanemist on raske tõendada ning kurjategija pääseb niikuinii karistusest.

Kuna arvutikuritegude toimepanemiste arv aasta-aastalt suureneb, on väga oluline, et riigis oleks piisav kompetents ja ressurss, et veebikeskkonnas toimepandud kuritegusid ennetada või siis juba toime pandud kuritegude sooritajad välja selgitada ning koguda kvaliteetseid

[9] K. M. Finklea, C.A. Theohary. Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement. CRS Report for Congress, 2012. Arvutivõrgus: http://www.law.umaryland.edu/marshall/crsreports/crsdocuments/R42547_07202012.pdf, 23. aprillil 2014.
[10] Julgeolekupoliitika alused. – RT 1 2001, 24,134.
[11] Kaitseministeerium. Küberjulgeoleku strateegia 2008-2013. Arvutivõrgus: http://valitsus.ee/UserFiles/valitsus/et/valitsus/arengukavad/kaitseministeerium/kuberjulgeolek.pdf, 23. aprillil 2014.

tõendeid nende süüdimõistmiseks.[12]

Eestis reguleerib arvutikuritegusid karistusseadustik (edaspidi KarS)[13], millesse laialdasemad muudatused viidi sisse 2008. aasta redaktsiooniga. Muudatuste eesmärgiks oli täiendada materiaalõigust selliselt, et see oleks kooskõlas nõuetega, mis on sätestatud Euroopa Nõukogu arvutikuritegevusvastases konventsioonis[14] (edaspidi konventsioon) ning Euroopa Nõukogu 2005. aasta raamotsuses 2005/222/JSK[15] (edaspidi raamotsus). 2013. aasta augustis võeti vastu Euroopa Parlamendi ja Nõukogu direktiiv 2013/40/EL[16] (edaspidi direktiiv), mis asendab varasemat raamotsust ja mille tulemusena tuleb karistusseadustikku sisse viia teatavad muudatused arvutikuritegevust reguleerivates sätetes. Muudatuste teostamise vajalikkus tuleneb lisaks direktiivile ka karistusõiguse revisjonist e kodifitseerimisprojektist, mille eesmärgiks on karistusõiguse süsteemi korrastamine, kattuvate kuriteo- ja väärteokoosseisude kõrvaldamine ning karistavate tegude koosseisu kirjelduste täpsustamine.[17] Arvutikuritegevust reguleerivatest sätetest on plaanis muuta KarS § 206, 207, 208 (kehtetuks tunnistatav), 217 ja 216[1],

Käesolevas magistritöös analüüsitakse arvutikuritegusid reguleerivaid sätteid nii karistusseadustikus kui ka rahvusvahelistes õigusaktides (konventsioon, raamotsus, direktiiv). Lähtutakse materiaalset küberkuritegevust puudutavatest sätetest, jättes välja jurisdiktsiooni ja koostööd puudutavad normid.

Töö eesmärgiks on leida vastused küsimustele:

- millised on arvutikuritegevust puudutavate sätete kitsaskohad karistusseadustiku kehtivas redaktsioonis; millised probleemid võivad seetõttu tekkida, mis tuleks karistusõiguse revisjoniga likvideerida;
- kas Eesti siseriikliku õiguse arvutikuritegevust reguleerivad sätted on kooskõlas rahvusvaheliste õigusaktide põhimõtetega ning missuguste muudatuste sisseviimist sätetesse nõuab 2013. aasta augustis kehtima hakanud direktiiv.

Magistritöö jaguneb kaheks peatükiks, millest esimeses käsitletakse arvutikuritegevust

[12] Siseministeerium (viide 3).
[13] Karistusseadustik. – RT I 2001, 61, 364.
[14] Euroopa Nõukogu Arvutikuritegevusvastane konventsioon. 01.07.2004 − ELS nr 185.
[15] Euroopa Nõukogu raamotsus. 24.02.2005 – 2005/222/JSK.
[16] Euroopa Parlamendi ja Nõukogu direktiiv. 14.08.2013 – 2013/40/EL.
[17] Justiitsministeerium. Karistusõiguse revisjon. Arvutivõrgus: http://www.just.ee/Protsess, 23. aprillil 2014.

üldisemalt, selle mõistet, Eesti arvutikuritegevuse regulatsiooni ajalugu ning rahvusvahelisi õigusakte, mis küberkuritegevust reguleerivad. Teine peatükk keskendub arvutikuritegevust reguleerivate sätete koosseisuelementide analüüsile: vaadeldakse nii neid elemente, mida on karistusõiguse revisjoni käigus plaanis muuta kui ka neid, mis jäävad muutmata.

Käesoleva magistritöö kirjutamisel on primaarsete allikatena kasutatud rahvusvahelistest õigusaktidest Euroopa Nõukogu arvutikuritegevusvastast konventsiooni, Euroopa Nõukogu raamotsust ja Euroopa Parlamendi ja Nõukogu direktiivi. Koosseisuelementide analüüsimisel on tuginetud eeskätt J. Sootaki ja P. Pikamäe „Karistusseadustiku kommenteeritud väljaandele“, Eesti kohtupraktikale, E. Hirsniku „Arvutikuritegevuse koolitus“ (avaldamata ettekande materjal) ning inglisekeelsele arvutikuritegevusvastase konventsiooni seletuskirjale. Kuna eestikeelsed erialaartiklid ja teosed antud valdkonnas praktiliselt puuduvad (on vaid mõned artiklid Juridicas ja seadusemuudatuste eelnõude seletuskirjad), siis on töö kirjutamisel tuginetud ka erinevatele inglisekeelsetele artiklitele ja erialakirjandusele, mis arvutikuritegevust käsitlevad. Välismaa autoritest on kasutatud peamiselt A. Bequai, S. Schjolbergi, S. L. Hopkinsi, K. M. Finklea ja C.A. Theohary poolt avaldatud materjale. Töö kirjutamisel on kasutatud analüüsiv-võrdlevat meetodit.

1. ARVUTIKURITEGEVUS: MÕISTE, AJALUGU JA RAHVUSVAHELISED REGULATSIOONID

1.1 Arvutikuriteo mõiste

Tänapäeva ühiskond on infoühiskond, kus väga paljude valdkondade korraldus sõltub tehnoloogiast. Paljud protsessid meie ümber on mõjutatud infotehnoloogiast, alustades näiteks pangatehingutest ja mobiilsest parkimisest ning lõpetades lennu- ja rongiliikluse korraldamisega läbi erinevate kanalite. Digimaailmas on lihtne kuritegusid toime panna: tehnoloogia abil sooritatakse näiteks identiteedirikkumisi ja krediitkaardipettusi, aga ka intellektuaalse omandi vastaseid rikkumisi. Lisaks üksikisikutele võivad küberkuriteod põhjustada negatiivseid tagajärgi ka riigi majandusele, rahvatervisele ja riiklikule julgeolekule.[18]

Globaliseeruvas maailmas tuleb meil arvestada erinevate probleemidega, mis kõrge internetiseeritusega kaasnevad. Üha enam on sagenenud olukorrad, kus kiirelt arenevat tehnoloogiat kasutatakse erinevate kuritegude toimepanemiseks. Seega tuleb tõdeda, et Interneti plahvatuslik areng on endaga kaasa toonud arvutikuritegevuse kasvu. Enamik era- ja äritehingutest teostatakse infotehnoloogia vahendusel, mistõttu on järsult kasvanud sel teel toime pandud pettuste arv.[19]

Arvutikuritegevuse tõusule on kaasa aidanud Interneti spetsiifiline iseloom:

- globaalsus – Interneti kaudu on omavahel ühenduses väga palju riike ning inimesi;
- interaktiivne iseloom – Interneti jututubadele ja serveritele on võimalik eriliste raskusteta juurde pääseda, tekitades kasutajates võltsi vabadustunde, mistõttu ei kontrollita oma esitatud avaldusi ja väiteid piisavalt;
- kerge juurdepääs – ligipääs Internetile on suhteliselt lihtne ning seetõttu on seal kerge levitada tõele mittevastavaid andmeid;
- kasutajate anonüümsus – selle tagab infotehnoloogiline keskkond.[20]

[18] K. M. Finklea, C.A. Theohary (viide 9).
[19] A. Kukrus. Küberkuritegevuse tõkestamine infoühiskonnas. Arvutivõrgus: http://www.riigikogu.ee/rito/index.php?id=11319, 23. aprillil 2014.
[20] S. Luide. The legal status and liability of Internet service providers. – Juridica Abstract, 2001, nr 5, p 329.

Kui võrrelda tavakuritegusid arvutikuritegudega, tekib küsimus, mis neid üksteisest eristab. Üks võimalus on vaadelda küberkuritegusid kui digitaalseid versioone tavalistest kuritegudest.[21] Küberkuritegusid eristab tavakuritegudest just see, et lisatud on virtuaalne element. Näiteks teise isiku identiteedi ebaseaduslikku kasutamist saab toime panna nii nn reaalmaailmas kui ka kübermaailmas. Arvutikuriteod muutuvad üha ulatuslikumaks, mille tingib eeskätt nende komplekssus ja rahvusvahelisus. Geograafiline kaugus kuriteo toimepanemiskoha ning teo tagajärgede vahel võib olla suur – see eristabki arvutikuritegusid paljudest teistest kuriteoliikidest.[22]

Küberkuritegevuse rahvusvahelise iseloomu tõttu seisavad menetlejad selle kuriteoliigiga võitlemisel mitmete väljakutsete ees. Kui riigis A elav kurjategija sooritab teo läbi riigis B asuva arvutisüsteemi, tagajärg saabub aga hoopiski riigis C, on teo toimepanija vastutuselevõtmine keerulisem kui olukorras, kus kurjategija paneb teo toime samas riigis, kus asub teo toimepanemisel kasutatud arvutisüsteem ja kus saabub ka tagajärg. Viimati nimetatud juhul on õiguskaitseorganitel kurjategijat lihtsam tabada ja kehtiva siseriikliku õiguse järgi karistada, sest kui kurjategija sooritab teo rahvusvahelisel tasandil, võib muutuda tema karistamine keeruliseks. Sellisel juhul võivad küsimused tekkida seoses kohtualluvusega, aga ka näiteks kohaldatava õigusega ning seesuguse olukorra tagajärg võib olla see, et arvutikurjategija pääseb karistusest sootuks.[23] Karistamise keerukus rahvusvahelise mõõtme tõttu kerkis esile ka kuulsa arvutiviiruse *Love Letter* uurimise puhul. Nimetatud viirus hävitas faile ja hankis paroole erinevatest arvutitest ja arvutivõrkudest, ilmnedes esmakordselt 11. mail 2000. aastal. Viirus levis kiiresti üle maailma ning nakatas ka NASA (*National Aeronautics and Space Administration*) ja CIA (*Central Intelligence Agency*) arvuteid, põhjustades ulatuslikku kahju. Eksperdid jõudsid viiruse allika otsimisel Filipiinidele ning kindlaks suudeti teha viiruse loomises ja levitamises kahtlustatavad isikud. Uurimine takerdus aga ootamatult, sest Filipiinidel ei olnud sel ajal ühtegi seadust, mis kriminaliseerinuks arvutiviiruste loomist ja levitamist. Samuti esinesid menetluslikud probleemid, sest kohus ei tahtnud anda uurijatele luba kahtlustatava korteri läbiotsmiseks. Tuvastati, et nimetatud arvutiviiruse looja oli Onel de Guzman, kes mõisteti varguse ja krediitkaardipettuste süüdistuses õigeks. Samuti puudus väljaandmislepingutes tingimuseks seatud teo mõlema riigi poolne karistatavus ning seetõttu ei olnud võimalik ka

[21] K. M. Finklea, C.A. Theohary (viide 9).
[22] Euroopa Ühenduste Komisjon. Küberkuritegevuse vastase võitluse üldise poliitika kujundamine. Brüssel, 2007. Arvutivõrgus: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:ET:HTML, 23. aprillil 2014.
[23] E. Elken. Arvutikuritegude menetlemise rahvusvahelised aspektid. Bakalaureusetöö. Tartu, 2009, lk 24.

arvutikurjategija väljaandmine Ameerika Ühendriikidele.[24]

Selliste olukordade vältimiseks tuleb arenenud riikidel avaldada survet ka nendele riikidele, kus vastavad kuriteod on jäänud sanktsioneerimata, sest muidu võib juhtuda nii, nagu eeltoodud näites, kus põhjalikult reguleerimata seadusandlus viis selleni, et kurjategija pääses vastutusest, kuigi tema toimepandud tegu põhjustas suurt kahju mitmekümnetes riikides.[25]

Kindlasti oleme kõik puutunud kokku arvutikuritegevuse mõistega, ent küsima peaks, kuidas võiks seda mõistet lihtsalt ja arusaadavalt defineerida lugejale, kes igapäevaselt infotehnoloogia ning õigusvaldkonnaga kokku ei puutu. Arvutikuriteo või küberkuriteo mõistet on püütud defineerida erinevalt ning on proovitud jõuda ka ühe kindla definitsioonini, kuid hetkel ei ole veel ülemaailmset aktsepteeritavat terminit, mida kõik kasutada saaksid.[26]

Näiteks on erialakirjanduses välja pakutud järgnevaid definitsioone:

- arvutikuritegu on kuritegu, mis on toime pandud arvutiga illegaalse tegevuse tulemusena, mõjutades sellega arvuteid või teisi tehnoloogiaseadmeid.[27]
- riistvara, tarkvara või andmete kasutamise, muutmise või hävitamisega sooritatud kuritegu.[28]
- kuritegu, mis on teostatud arvutite või Interneti vahendusel.[29]
- kriminaalne tegevus, kus kuritöö allikaks, sihtmärgiks ja/või toimumiskohaks on arvuti või arvutivõrk.[30]
- kuriteod, mis on toime pandud elektrooniliste sidevõrkude ja infosüsteemide abil või selliste võrkude või süsteemide vastu.[31]

Eelnevad näited ilmestavad selgelt, et arvutikuritegude määratluses esineb probleeme. Läbisegi kasutatakse mõisteid „küberkuritegevus", „arvutikuriteod" või „arvutitega seotud kuritegu".[32] Seetõttu on arusaadav, miks Euroopa Komisjon antud valdkonda puudutavates

[24] S. W. Brenner, Mark D. Goodman. Cybercrime: The Need to Harmonize National Penal and Procedural Law. Arvutivõrgus: http://www.isrcl.org/Papers/Brenner.pdf, 23. aprillil 2014.
[25] E. Elken (viide 23), lk 25.
[26] Samas.
[27] Web Strategist & Project Manager. Computer Crime Definition. Arvutivõrgus: http://www.mariosalexandrou.com/definition/computer-crime, 23. aprillil 2014.
[28] Eesti Rahvusraamatukogu. Raamatukogusõnastik. Arvutivõrgus: http://www.nlib.ee/termin/public_term/termin/view/4664, 23. aprillil 2014.
[29] Oxford Dictionaries. Arvutivõrgus: http://www.oxforddictionaries.com/definition/english/cybercrime, 23. aprillil 2014.
[30] H. Vallaste. Arvutivõrgus: http://wordties.cst.dk/wordties-estwn/w/full/354951-arvutikuritegevus, 23. aprillil 2014.
[31] T. Rosenfeldt. IT turvalisus. Arvutivõrgus: http://www.e-uni.ee/e-kursused/itturvalisus/112_kberkuritegevuse_termin.html, 23. aprillil 2014.
[32] I. Metusa. Telekommunikatsioonialased õigusrikkumised Informatsioonivabaduse loomulikust piirist. – Juridica, 2002, nr 5, lk 314.

küsimustes terminoloogiad ja põhimõtted ühtlustada soovib.[33]

Kui võrrelda omavahel mõisteid „küber“ ja „arvuti“, siis nõustub töö autor E. Tikk-Ringase tähelepanekuga, et „küber“ on erineva ulatuse ja tähendusega ning pidevas arengus olev mõiste, mille kasutus on tihti ebajärjekindel.[34] Küberkuriteo kontekstis antakse sõnale „küber“ arvuti või arvutivõrgu tähendus, samas kannab see mõnikord ka informatsiooni tähendust.[35] Sõna „arvuti“ kasutamine võib olla küll konkreetsem, ent on liiga piiratud, jättes mulje, et sellised kuriteod peavad kindlasti olema seotud arvutiga klassikalises mõttes, mitte mõne teise infotehnoloogilise vahendiga.

Kuna arvutikuritegevuse määratluses ei ole kokku lepitud ja erinevaid mõisteid kasutatakse tihti sünonüümidena, kasutab ka käesoleva töö autor sama nähtuse tähistamiseks erinevaid termineid ning peab arvutikuriteo ehk küberkuritegevuse mõiste selgitamiseks kõige paremini viimasena eelnevas loetelus välja pakutud definitsiooni (kuriteod, mis on pandud toime elektrooniliste sidevõrkude ja infosüsteemide abil või selliste võrkude või süsteemide vastu), sest kirjeldab antud kuriteo liiki kõige ülevaatlikumalt.

[33] Euroopa Ühenduste Komisjon (viide 22).
[34] E. Tikk-Ringas. Küberjuleoleku õiguslik raamistik. – Juridica, 2012, nr 4, lk 274.
[35] Samas.

1.2 Arvutikuritegevuse regulatsiooni ajalugu

Kui maailmas hakati arvutikuritegevusega kokku puutuma esmalt 1970. aastate lõpul ja tihedamalt 1980. aastatel[36], siis Eesti esimene teadaolev arvutikuritegu pandi toime 1997. aastal, mil vennad M. ja E. Leego tegid Laeva Meieri arveldusarvelt ebaseaduslikke ülekandeid 467 000 krooni ulatuses, mis hiljem võõra nime all esinedes Tallinnas Hansapangast välja võeti. Süüdi mõisteti vennad Leegod siiski kelmuses, sest arvutikelmuse mõiste lisati kriminaalkoodeksisse[37] (edaspidi KrK) alles 12. märtsil 1997. aastal vastuvõetud andmekogude seadusega [38] , millega täiendati kriminaalkoodeksit §-ga 268; nimetatud muudatuse tegemise ajaks oli kohtuotsus Leegode kriminaalasjas juba jõustunud.[39]

Arvutikuritegusid tunneb Eesti karistusõigus seega 1997. aastast. Karistusseadustiku jõustumisega 1. septembril 2002. aastal kaasnesid aga mitmesugused muudatused arvutikuritegevuse regulatsioonis.[40] Kui kriminaalkoodeksis oli eraldi peatükk arvuti- ja andmetöötusalaste kuritegude kohta (14. peatükk), siis karistusseadustiku nii 2002. aasta kui ka hilisemates redaktsioonides paiknevad enamik arvutikuritegusid reguleerivad paragrahve varavastaste süütegude alajaotuses.

Kui vaadelda, millised olid arvutikuritegusid reguleerivad sätted kriminaalkoodeksis ja hilisemates karistusseadustiku redaktsioonides, siis näeme, et muudatused paragrahvide sisus on ulatuslikud. Kriminaalkoodeksis olid arvutikuritegudest välja toodud järgnevad: arvutikelmus (§ 268); arvutis olevate andmete või programmide hävitamine (§ 269); arvutisabotaaž (§ 270); arvuti, arvutisüsteemi või arvutivõrgu ebaseaduslik kasutamine (§ 271); arvutivõrgu ühenduse ebaseaduslik rikkumine või tõkestamine (§ 272); arvutiviiruse teadlik levitamine (§ 273); kaitsekoodide üleandmine (§ 274).[41]

Karistusseadustiku 2002. aasta redaktsioonis olid arvutikuriteod: arvutikahjurlus (§ 206); arvutivõrgu ühenduse kahjustamine (§ 207); arvutiviiruse levitamine (§ 208); arvutikelmus (§ 213); arvuti, arvutisüsteemi ja arvutivõrgu ebaseaduslik kasutamine (§ 217); kaitsekoodide üleandmine (§ 284). Ka 2008. aastal kehtima hakanud redaktsioonis on põhijaotus jäänud samaks: enamus arvutikuritegude liike paigutub 13. peatüki varavastaste süütegude alla ja

[36] S. Schjolberg. The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva, 2008. Arvutivõrgus: http://www.cybercrimelaw.net/documents/cybercrime_history.pdf, 23. aprillil 2014.
[37] Kriminaalkoodeks. − RT 1992, 20, 287 ja 288.
[38] Andmekogude seadus. – RT I 1997, 28, 423.
[39] V. Päärt. Kohus mõistis Laeva Meieri petturid vangi. Arvutivõrgus: http://www.postimees.ee/print/2542947/kohus-moistis-laeva-meierei-petturid-vangi, 23. aprillil 2014.
[40] J. Sootak, P. Pikamäe. Karistusseadustik. Kommenteeritud väljaanne. Tallinn: Juura 2004, lk 24.
[41] E. Elken (viide 23), lk 9.

kaitsekoodide üleandmine on endiselt 16. avaliku rahu vastaste süütegude peatükis, nagu 2002. aasta redaktsioonis. Peatükkide liigituse kohaselt tuleks välja tuua ka see, et lisandunud on säte riigivastaste süütegude kohta, mis paikneb 15. peatükis.[42]

Kuigi paragrahvide paiknemine seaduses on jäänud suuresti samaks, viidi 2008. aastal sisse mitmeid muudatusi, mille eesmärgiks oli tagada karistusseadustiku kooskõla rahvusvahelisest õigusest tulenevate nõuetega. 2008. aasta redaktsioonis on lähtutud Euroopa Nõukogu arvutikuritegevusvastasest konventsioonist ning Euroopa Liidu Nõukogu raamotsusest. Kui konventsiooniga sooviti ühtlustada arvutikuritegude regulatsiooni sellega liitunud riikide seadustes, siis raamotsusega täpsustati arvutisüsteemi vastu suunatud rünnete koosseise ja korrigeeriti nende eest mõistetavaid karistusi.[43] Kui konventsiooni puhul on riigi liitumine sellega vabatahtlik, siis raamotsusest tulenevaid nõudeid peavad täitma kõik Euroopa Liidu liikmesriigid.

Nii Eestis kui ka kogu maailmas on erinevate arvutikuritegude toimepanemine pidevalt suurenenud ning riigi järjest suurema internetiseerituse ning elanikkonna poolt elektrooniliste kanalite kasutamise tulemusena muutuvad need kuriteod järjest ohtlikumaks. Seetõttu nähakse ette ka rangemad sanktsioonid selliste kuritegude toimepanemise eest kui varasemalt. Osaliselt oli sanktsioonimäärade muutmine seotud ka jälitustoimingutega. Kriminaalmenetluse seadustiku [44] (edaspidi KrMS) eelmise redaktsiooni kohaselt sai jälitustoiminguid teostada, kui kuriteo eest nähti ette vähemalt kolmeaastane vangistus. Praegu sisaldab kriminaalmenetlusseadustik aga nende kuritegude kataloogi, mille uurimisel tohib jälitustoiminguid kasutada. Kuna tegemist on raskesti avastatavate kuritegudega, on sellisel juhul vajalik jälitustoimingutega tõendite kogumine, mida varasemad redaktsioonid ei võimaldanud.[45]

Karistusseadustiku 2008. aasta redaktsioonis on arvutikuritegusid reguleeriva sätted: arvutiandmetesse sekkumine (§ 206); arvutisüsteemi toimimise takistamine (§ 207); nuhkvara, pahavara ja arvutiviiruse levitamine (§ 208); arvutikelmus (§ 213); arvutikuriteo ettevalmistamine (§ 216[1]); arvutisüsteemi ebaseaduslik kasutamine (§ 217). Riigivastastest süütegudest tuleb välja tuua terrorikuritegu (§ 237), mille mõistet 2008. aasta seadusemuudatusega täiendati loeteluga kuritegudest, mille toimepanemist KarS §-s 237

[42] E. Elken (viide 23), lk 9.
[43] Justiitsministeerium. Karistusseadustiku muutmise seaduse eelnõu seletuskiri. Arvutivõrgus: http://www.riigikogu.ee/?op=emsplain&page=pub_file&file_id=85a4d8e5-2c8a-0faf-b0e9-3ff75214ffbf&, 23. aprillil 2014.
[44] Kriminaalmenetluse seadustik. – RT I 2003, 27, 116.
[45] Justiitsministeerium (viide 43).

sätestatud terroristlikul eesmärgil loetakse terrorikuriteoks. Seega on nimetatud kuriteoks ka andmetesse sekkumine, arvutivõrgu toimimise takistamine, samuti selliste tegude toimepanemisega ähvardamine, kui see on toime pandud eesmärgiga sundida riiki või rahvusvahelist organisatsiooni midagi tegema või tegemata jätma või tõsiselt häirida riigi poliitilist, põhiseaduslikku, majanduslikku või ühiskondlikku korraldust või see hävitada või tõsiselt häirida rahvusvahelise organisatsiooni tegevust või see hävitada või tõsiselt hirmutada elanikkonda.[46] Varasemalt see säte nii põhjalikult reguleeritud ei olnud. 16. peatükist, mis on suunatud avaliku rahu vastastele süütegudele, on arvutikuritegude käsitlemise korral oluline säte kaitsekoodide üleandmise (§ 284) kohta.[47]

2013. aasta augustis võeti vastu direktiiv 2013/40/EL, mis asendab varasemat raamotsust ja mille tulemusena tuleb karistusseadustikku sisse viia teatavad muudatused arvutikuritegusid reguleerivates sätetes. Eelkõige puudutavad muudatused KarS-i § 217, 216¹, 206, 207, 208 (kehtetuks tunnistatav) ning mida põhjalikumalt analüüsitakse käesoleva töö teises peatükis. Strukturaalsetel põhjustel teostatakse arvutikuritegusid reguleerivate sätete analüüsi järgnevas järjestuses: KarS § 206, 207, 208, 217, 216¹).

[46] Justiitsministeerium (viide 43).
[47] E. Elken (viide 23), lk 12.

1.3 Rahvusvahelised sammud arvutikuritegevuse vastu

1.3.1 Euroopa Nõukogu arvutikuritegevusvastane konventsioon

Üha rohkem arvutikuritegusid pannakse toime mitte üksnes organisatsioonide või eraisikute vastu, aga ka riikide vastu. Olukorda on süvendanud tehnoloogiate põimumine ja infosüsteemide omavaheline kiire ühendatus, muutes rünnatavad objektid senisest veelgi haavatamateks. Selle vastu võitlemiseks on vaja võtta nii riikide kui ka Euroopa tasandil kiiresti meetmed mistahes kuriteoliikide vastu, mis kujutavad endast järjest suuremat ohtu kriitilistele infrastruktuuridele, ühiskonnale, ettevõtlusele ja kodanikele.[48]

Enamikes Euroopa riikides on arvutialased kuriteod kriminaalkorras karistatavad, kuid peamine probleem ja ühtlasi ka põhjus, miks on vaja rahvusvahelist regulatsiooni, peitub asjaolus, et kuritegude koosseisud ja karistusmäärad on riigiti väga erinevad. Nagu me teame võivad ühe kuriteo tagajärjed ilmneda üheaegselt mitmes riigis ja ebaselgus jurisdiktsiooni ning kohaldatava õiguse osas muudab süüdlase karistamise raskeks või lausa võimatuks. Keeruliseks muutuvad probleemid pädeva kohtuga, kohaldatava õigusega, piiriülese õiguskaitse või elektroonilise tõendusmaterjali tunnustamise ja kasutamisega.[49]

Üheks esimeseks olulisemaks rahvusvaheliseks sammuks arvutikuritegude vastases võitluses saab pidada Euroopa Nõukogu „Soovitust nr (89) 9“[50], milles nõutakse, et liikmesriigid vaataksid üle vanad õigusaktid ning jõustaksid uusi, sest küberkuriteod on üha kasvav nähtus kogu maailmas.[51] See sisaldab endas miinimum nimekirja süütegudest, millele oleks vaja rakendada ühtset poliitikat õigusaktides, et arvutikuritegevust sarnaselt reguleerida.[52]

Nimetatud soovitusele järgnes Euroopa Nõukogu „Soovitus nr (95) 13“[53], mis kehtestas protseduurid „Soovituse nr (89) 9“ kohaldamiseks, sest võitlus rünnete vastu ei olnud piisavalt koordineeritud – need olid aeglased ega vastanud nõutavale tasemele. Väga paljud

[48]K. Archick. CRS Report for Congress. Cybercrime: The Council of Europe Convention. Arvutivõrgus: http://fpc.state.gov/documents/organization/74909.pdf, 23. aprillil 2014.
[49] E. Elken (viide 23), lk 17.
[50] Council of Europe. Recommendation No. Recommendation No. R (89) 9. Committee of Ministers, 1989. Arvutivõrgus: https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=610660&SecMode=1&DocId=702280&Usage=2, 23.aprillil 2014.
[51] S. L. Hopkins. Cybercrime Convention: A Positive Beginning to a Long Road Ahead. – Journal of High Technology Law, 2003, p 106.
[52] S. Schjolberg (viide 36).
[53]Council of Europe. Recommendation No. R (95) 13. Committee of Ministers, 1995. Arvutivõrgus: https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=1900870&SecMode=1&DocId=528034&Usage=2, 23. aprillil 2014.

riigid jõudsid järeldusele, et nende õigussüsteemid on tehnoloogia arengu tõttu ajale jalgu jäänud ning vajaks uuendusi, et küberkuritegevuse vastu tõhusamalt võidelda. [54] Küberkuritegevuse vastu võitlemisel jooksevad õigusloojad ajaga võidu, et selle kuriteoliigi erinevaid muutuvaid vorme regulatsiooniga katta. Olulisel kohal küberkuritegevusvastases võitluses on ka riikidevaheline koostöö, sest omavaheline kogemuste jagamine, vigade vältimine aitab regulatsiooni ajakohasena hoida.[55]

Kuna eelnevad soovitused ja sammud ei olnud piisavad arvutikuritegevuses võitluses, siis moodustati Euroopa Nõukogu poolt ekspertide kommitee, mille tulemusena võeti 8. novebmbril 2001. aastal vastu arvutikuritegevusvastane konventsioon, millele Eesti kirjutas alla sama aasta 23. novembril. See on põhimõtteliselt esimene rahvusvaheline leping, mis kriminaliseerib arvutisüsteemide kaudu toime pandud õigusrikkumised.[56]

Konventsiooni koostajatel oli kaks peamist eesmärki. Esiteks sooviti tagada kuritegude loetelude nimetamisel piisavalt paindlik määratlus, mis arvestaks ka tehnoloogia kiiret arengut ning teiseks sooviti, et konventsioon säilitaks osaliste riikide õigusrežiimid, sest inimõiguste valdkonnas on riikidel erinevad moraalsed ja kultuurilised väärtused.[57] Siinkohal tuleb lisada, et teine eesmärk on seotud pigem menetlusõigusliku poolega, sest erinevatel riikidel on erinev arusaam sellest, kui palju ning kuna riik kuritegude avastamiseks võib menetluslikult sekkuda, näiteks millal tohib teostada jälitustegevust, millal läbiotsimisi, millal võib arvuteid konfiskeerida jne).

Konventsiooni ratifitseerinud riigid on kohustatud viima riigisisese õiguse vastavusse konventsiooniga. Hetkel on lisaks EL-i (Euroopa Liidu) liikmesriikidele liitunud konventsiooniga ka näiteks USA, Jaapan ning Austraalia jt. Et konventsiooniga on liitunud mitmeid riike, on kõigiti positiivne, sest aitab ühtlustada erinevate riikide seadusi ja samme arvutikuritegevusevastases võitluses. Esialgselt oldi skeptilised, kas konventsiooni abil ikkagi suudetakse vähendada arvutikuritegevust ja võidelda selle vastu. Sealhulgas suhtus konventsiooni kriitiliselt ka nt Tiigrihüppe Sihtasutuse asutaja Linnar Viik, sest arvas, et konventsiooniga liitumine ei too endaga kaasa olukorra paranemist; samas tõdes L. Viik siiski, et antud protsess ei saagi edu saavutada mõne aasta möödudes, vaid teeb seda pikemas

[54] S. L. Hopkins (viide 51), p 107.
[55] M. Gercke. Europe's legal approaches to cybercrime. – ERA Forum, 2009, Vol 10, Iss 3, p 409-410. Arvutivõrgus: http://link.springer.com/article/10.1007%2Fs12027-009-0132-5, 23. aprillil 2014.
[56] Arvutikuritegevusvastase konventsooni lisaprotokoll. − RTL 2003,14, 192.
[57] S. L. Hopkins (viide 51), p 105.

perspektiivis.[58]

Euroopa Nõukogu poolset arvutikuritegevusvastast konventsiooni saab pidada läbimurdeks rahvusvahelisel tasandil veebikeskkonnas aset leidvate kuritegude reguleerimiseks. Lisaks sellele, et arvutikuritegevusvastane konventsioon on seotud materiaalõigusega, kohustatakse konventsiooni osapooli kasutama ka erinevaid meetmeid arvutialastes juurdlustes.

Konventsiooni preambula kohaselt on ühiskonna kaitseks küberkuritegevuse vastu esmatähtis ellu viia ühtest kriminaalpoliitikat, võttes vastu asjakohased õigusaktid ja edendades rahvusvahelist koostööd muul viisil. Konventsiooni sõnastuses on peetud silmas tehnoloogia kiiret arengut ning seetõttu on normid sätestatud küllaltki paindlikult, et vältida nn jalgujäämist uuele tehnoloogiale. Kuigi konventsioon nimetab ära rikkumised, mille korral kriminaalvastutust kohaldatakse, ent aktiga ei täpsustata seda, milliseid õiguslikke samme kuritegude menetlemiseks peab riik kohaldama. Ka „tahtluse“, subjektiivse koosseisuelemendi, määratlemine on jäetud konventsiooniosaliste riikide otsustada.[59]

Konventsioon koosneb 48st artiklist ja hõlmab nelja peatükki: mõistete kasutamine, riigi tasandil võetavad meetmed, rahvusvaheline koostöö ja lõppsätted. Konventsiooni esimeses peatükis on välja toodud erinevad mõisted ning nende seletused. Teises peatükis on sätted kriminaalmateriaalõiguse, menetlusõiguse ja jurisdiktsiooni kohta. Kolmas peatükk sätestab rahvusvahelise koostöö üldpõhimõtted ning neljandas peatükis on välja toodud üldsätted konventsiooni kehtivuse, territoriaalsuse kohta ning reservatsioonid, muudatused ja vaidluste lahendamise põhimõtted.

Arvutikuritegevusvastane konventsioon käsitleb nelja liiki rikkumisi:

1. arvutiandmete ja -süsteemide konfidentsiaalsuse, puutumatuse ja kättesaadavuse vastu toimepandud süüteod;
2. arvutisüüteod;
3. lapspornoga seotud süüteod;
4. autoriõiguste ja autoriõigustega kaasnevate õiguste rikkumisega seotud süüteod.[60]

Esimese liigi alla on koondatud loata arvutisüsteemi või selle osasse sisenemine (nn häkkerlus), ebaseaduslik pealtkuulamine, arvutiandmete loata omastamine ja nendega

[58]L. Viik. Küberrünnak suveräänse riigi vastu oli maailmas esmakordne. Arvutivõrgus: http://www.postimees.ee/250507/esileht/siseuudised/261227.php, 23. aprillil 2014.
[59] Euroopa Nõukogu Arvutikuritegevusvastane konventsioon (viide 14).
[60] Samas.

manipuleerimine (siia kuulub ka nn Trooja hobuse tüüpi pahavara saatmine arvutisse), arvutisüsteemi toimimise tõsine takistamine, seadmete kuritarvitamine, st eelkõige küberkuritegude toimepanemiseks kavandatud ja kohandatud seadmete, ka arvutiprogrammide (sealhulgas viirused) ja paroolide kättesaadavaks tegemine (müük, kasutamiseks hankimine jms). Vastavad põhimõtted on välja toodud konventsiooni artiklites 2–6, kusjuures viimati nimetatud rikkumise (artiklis 6 sätestatud ettevalmistuskuriteo) sanktsioneerimise eesmärk on häkkerite relvituks tegemine.[61] Siinkohal on oluline tähelepanu pöörata sellele, et konventsiooni koostamise käigus vaieldi selle üle, kuidas otsustada, millised tehnilised vahendid, programmid vms on loodud just kuritegude sooritamiseks. Lõpuks sõnastati artikkel nii, et artikli kohaldamisalasse jäävad need seadmed ja programmid, mis on kavandatud või kohandatud eelkõige konventsiooni artiklites 2–5 ettenähtud tegude toimepanemiseks.[62]

Arvutisüüteod (artiklid 7–8) on arvutite abil tehtavad võltsingud (digitaalsete dokumentide võltsimine) ja pettused (viimane kuulub majanduskuritegude valdkonda, sest peab olema sooritatud ärieesmärgil). Arvutikelmusi on ka Eestis kuritegude statistika kohaselt arvutikuritegudest kõige enam toime pandud; arvutikelmused kujutavad endast tihti pangapettusi ja nendega kaasnevad rahapesukuriteod.[63]

Lapspornoga seotud süütegude alla (artikkel 9) kuuluvad lapspornograafia valmistamine selle levitamiseks arvutisüsteemi kaudu, lapsporno pakkumine või kättesaadavaks tegemine arvutisüsteemi kaudu, lapsporno edastamine või muul viisil levitamine arvutisüsteemi kaudu, lapsporno hankimine endale või teisele isikule arvutisüsteemi kaudu ja lapsporno valdamine arvutisüsteemis või andmekandjal. Alaealisena käsitletakse alla 18-aastast isikut. Konventsiooni osalisel on siiski õigus kehtestada ka madalam vanusepiir, mis on 16 aastat. Konventsiooni koostamise käigus plaaniti lisada lapspornoga seotud süütegude alla ka rassismi käsitlevad sätted, kuid seda ei tehtud peamiselt USA vastuseisu tõttu, kes pidas seda võimalikuks sõnavabaduse piiramiseks. Vastuolude vältimiseks on rassismi käsitlevad sätted koondatud esimesse lisaprotokolli.[64]

Artikli 10 kahes esimeses lõikes on sätestatud konventsiooniosaliste kohtustus kriminaliseerida tahtlikud arvutisüsteemi abil toimepandud autoriõiguse ja autoriõigusega kaasnevate rikkumiste juhud, kui need pandi toime ärieesmärgil. Siinkohal on arvutikuritegevusvastase konventsiooni sõnastusest tulenevalt autoriõiguse ja autoriõigusega

[61] A. Kukrus (viide 18).
[62] A. Kukrus. Virtuaalmaailm ja küberkuriteod. – A&A, nr 3, 2002, lk 41.
[63] A. Kukrus (viide 18).
[64] Samas.

kaasnevate õiguste rikkumise defineerimine liikmesriikide pädevuses, kes peaksid nende mõistete sisu avamisel lähtuma nimetatud rahvusvahelistest lepingutest, mille sätted on konventsiooniosalistele siduvad üksnes juhul, kui nad on nimetatud konventsioonidega ühinenud, ning selles ulatuses, mida nad pole reservatsioonidega piiranud. Nimetatud konventsioonidest on kriminaalkaristuste kohaldamise kohustus Maailma Kaubandusorganisatsiooni lisas 1C Intellektuaalomandi õiguste kaubandusaspektide leping" ehk TRIPS-i lepingus (*Agreement on Trade-Related Aspects of Intellectual Property Rights*), mille artikkel 61 sätestab liikmete kohustuse näha ette kriminaalmenetluse ja –karistuste kohaldamist vähemalt juhtudel, kui on võltsitud kaubamärki või rikutud autoriõigusi kommertseesmärkidel ning tegemist on tahtliku rikkumisega.[65]

Teise peatüki teine jagu keskendub menetlusõigusele (artiklid 14–21) ning sellega kaasnevale problemaatikale. Siin on reguleeritud konventsiooniosaliste kohustus tagada meetmed, mis võimaldavad jälgida andmete liikumist, arvutiandmete kogumist, arestimist, otsimist jne. Sellega võimaldatakse niiöelda jälgede säilitamine küberkuriteo puhul. Teise peatüki kolmas jagu keskendub jurisdiktsioonile, et anda ülevaade, kuidas peaksid liikmesriigid arvutikuritegude puhul seadusi kohaldama. Probleeme tekitab just see, et Internet ei tunnista riiklikke piire ning Internetis olevaid andmeid on kerge muuta ja eemaldada. Kõige suurem miinus ongi see, et sellisel juhul esineb risk, et kui isegi politsei avastab need kuriteod, siis ei ole järele jäänud tõendusmaterjali, mille alusel saaks arvutikurjategijaid karistada.[66]

Kolmas peatükk (artiklid 23–35) sätestab rahvusvahelise koostöö üldpõhimõtted, jagunedes kaheks jaoks, millest esimesed on välja toodud üldsätted näiteks kuidas leiab aset kurjategija väljaandmine ja kuidas peaks toimuma vastastikuse abi osutamine. Teine jagu keskendub erisätetele, kus selgitatakse, kuidas peab toimuma säilitatavate liiklusandmete (arvutisidesüsteemi ühe osana toimiva süsteemi andmed, mis käsitlevad edastatud teabe päritolu; teabe edastamise eesmärki, marsruuti ja kuupäeva; teabe mahtu ja teabe edastamise kestust ning asjaomase teenuse liiki [67]) kiiravalikustamine, vastastikune abi seoses juurdepääsuga salvestatud arvutiandmetele ning kuidas peab olema organiseeritud ööpäevane koostöö.[68]

Neljas peatükk (artiklid 36–48) keskendub lõppsätetele, kus on välja toodud erinevad tingimused konventsiooni kehtivuse kohta, territoriaalsuse kohta, reservatsioonid, muudatused ja vaidluste lahendamine.

[65] A. Kukrus (viide 18).
[66] D. Cangemi. Procedural Law Provisions of the Council of Europe Convention on Cybercrime. International review of law computers and technology, 2003, p 166-171.
[67] Euroopa Nõukogu Arvutikuritegevusvastane konventsioon (viide 14).
[68] A. Kukrus (viide 18).

Euroopa Nõukogu arvutikuritegevuse vastase konventsiooni põhjalikum käsitlus leiab aset käesoleva töö teises peatükis, kus analüüsitakse karistusseadustiku arvutikuritegusid reguleerivate sätete koosseisuelemente.

1.3.2 Euroopa Parlamendi ja Nõukogu direktiiv 2013/40/EL

Kui varasemalt tuli Eestil arvestada arvutikuritegude regulatsioonis lisaks konventsioonile ka Euroopa Nõukogu raamotsusega 2005/222/JSK, siis käesoleval hetkel on endine raamotsus asendunud Euroopa Liidu Parlamendi ja Nõukogu direktiiviga 2013/40/EL. Eesti Euroopa Liidu liikmesriigina peab järgima Euroopa Liidu õigusakte, mistõttu on vastavad muudatused vaja sisse viia ka siseriiklikku regulatsiooni. Nimelt on raamotsust asendava direktiivi eesmärgiks muuta ja laiendada infosüsteemide vastu suunatud rünnete sätteid. Kuna tehtavad muudatused on arvukad ja sisulised, siis otsustati raamotsus selguse huvides asendada uue regulatsiooni ehk direktiiviga.[69]

Direktiivi eesmärkideks on ühtlustada liikmesriikide kriminaalõigust infosüsteemide vastu suunatud rünnete valdkonnas, kehtestada miinimumeeskirjad kuritegude määratlemise ja asjakohaste sanktsioonide kohta ning tõhustada koostööd pädevate asutuste, sealhulgas liikmesriikide politsei- ja muude spetsialiseeritud õiguskaitseasutuste ning liidu pädevate spetsialiseeritud asutuste ja organite vahel.[70]

Direktiivi kohaselt tuleb tagada ühine lähenemisviis kuriteokoosseisude suhtes, kriminaliseerides selleks kõikjal liidus ebaseadusliku infosüsteemi, sisenemise, ebaseadusliku süsteemi häirimise, andmetesse sekkumise, teabe ebaseaduslikult pealtkuulamise. Samuti soovitakse näha arvutikuritegude toimepanemise eest ette senisest karmimad sanktsioonid.[71]

Arvutikuritegevust puudutava mõisteaparaadiga seoses tuleb juhtida tähelepanu asjaolule, et kui varasem raamotsus käsitles mõningaid mõisteid konventsioonist erinevalt, tugineb antud direktiiv konventsiooni terminoloogiale.[72]

Direktiivi artikkel 2 toob välja erinevad mõisted, mida selles õigusaktis kasutatakse. Arvutikuriteod on üles loetletud artiklites 3–6: ebaseaduslik sisenemine infosüsteemi, ebaseaduslik süsteemi häirimine, ebaseaduslik andmetesse sekkumine ja teabe ebaseaduslik

[69] Euroopa Parlamendi ja Nõukogu direktiiv (viide 16).
[70] Samas.
[71] Samas.
[72] Samas.

pealtkuulamine. Kuriteo toimepanemisel kasutatavate vahenditega seotud ettevalmistustegusid käsitletakse artiklis 7. Artikkel 9 toob välja nõude näha ette tõhusad, proportsionaalsed ja hoiatavad kriminaalkaristused füüsilistele isikutele ja artiklis 11 reguleeritakse juriidilise isiku suhtes kohaldatavate sanktsioonidega seonduvat. Direktiivi järgmistes artiklites on käsitletud jurisdiktsiooni, teabevahetust, järelevalvet ja statistikat ning põhimõtteid, millest liikmesriigil tuleb oma seadusandluses lähtuda.[73]

Käesoleva töö autor keskendub arvutikuritegude regulatsiooni analüüsis pigem direktiivi mõisteid, arvutikuritegusid ja sanktsioone käsitlevatele artiklitele, materiaalsele küberkuritegevusele, jättes välja jurisdiktsiooni ja koostööd puudutavad sätted, mis antud töös on teemavälised.

[73] Euroopa Parlamendi ja Nõukogu direktiiv (viide 16).

2. ARVUTIKURITEGUDE KOOSSEISUDE ANALÜÜS

2.1 Arvutiandmetesse sekkumine

2.1.1 Sissejuhatavad märkused

Kui enne 2008. aastat käsitles KarS § 206 arvutikahjurlust, mis reguleeris nii arvutis olevatesse andmetesse sekkumist kui ka arvuti- või telekommunikatsioonitöö takistamist, siis 2008. aasta seadusemuudatuse järel jäi antud säte reguleerima vaid arvutiandmetesse sekkumist, sest karistuse arvutivõrgu ühenduse kahjustamise eest nägi ette KarS § 207. Enne 2008. aasta seadusemuudatust reguleeris arvuti- või telekommunikatsiooni töö takistamist ka KarS § 206 lg 2, mistõttu tõi selline paragrahvide sisuline kattuvus kaasa segadust seaduse tõlgendamisel. Kuna ründeid arvutisüsteemis olevate andmete ja ründeid arvutisüsteemi enda vastu eristati konventsioonis, siis leiti, et sellest põhimõttest tuleb lähtuda ka karistusseadustiku regulatsioonis.[74] 2008. a seadusemuudatusega täpsustati KarS § 206 sõnastust ning sätestati kuriteona arvutiandmetesse sekkumine. Normi lõikega 2 nähti ette andmetesse sekkumise kvalifitseeritud koosseis, mille puhul rangem karistus sama teo eest kohaldub siis, kui kuritegu on toime pandud elutähtsa valdkonna arvutisüsteemi vastu või kui sellega on tekitatud oluline kahju. Lõikega 3 lisati sättesse juriidilise isiku vastutus.[75]

Arvutiandmetesse sekkumise paragrahv kujutab endast n-ö virtuaalset asja kahjustamist. Tänapäeva inimesed sõltuvad väga palju infotehnoloogiast, kus erinevaid protsesse teostatakse arvutite vahendusel. Sellega on kaasnenud olukord, kus lisaks füüsiliste esemete hävitamise ja kahjustamise kaitsele reaalmaailmas, tuleb tagada füüsiliste esemete virtuaalsete ekvivalentide e arvutiandmete kaitse kübermaailmas. Sellisele järeldusele on jõudnud Euroopa Nõukogu juba oma „Soovituses nr (89) 9“, sest rikkumisi võidakse toime panna ka arvutiandmete ja -programmide vastu. Soovitusega peeti vajalikuks kriminaliseerida arvutiandmete või -programmide kustutamine, kahjustamine, rikkumine või sulustamine, kui see on toime pandud õigusliku aluseta.[76]

Iga kuriteokoosseis peab kaitsma mõnda õigushüve. Õigushüve on eluline hüve, mis on inimeste sotsiaalseks kooseluks vajalik sotsiaalne väärtus, mille kaitsmisel on oluline

[74] Justiitsministeerium (viide 43).
[75] Samas.
[76] A. Bequai. Computer-related crime. Recommendation No. R (89) 9 on computer-related crime and final report of the European Committee on Crime Problems. Strasbourg 1990, p 45.

rakendada riigi karistusvõimu. See võib olla individuaalne (elu, tervis, kehaline puutumatus) või kollektiivne (riik, avalik rahu vms).[77] Tegemist on õigustatud isiku huviga oma andmete segamatu kasutamise osas. Karistusseadustiku kommentaaride (2009. aasta väljaande) kohaselt on paragrahviga 206 ohustatavaks õigushüveks arvutisüsteemi omaniku ja õiguspärase valdaja õigus vallata, kasutada ja käsutada arvutisüsteemi[78], ent see tõlgendus on vastuoluline, sest arvutisüsteemiga seonduvate õiguste kaitse tagatakse KarS §-ga 207. Koosseisutüübilt on tegemist formaalse kuriteokoosseisuga.[79]

§ 206. Arvutiandmetesse sekkumine
(1) Arvutisüsteemis olevate andmete või programmi ebaseadusliku muutmise, kustutamise, rikkumise või sulustamise, samuti arvutisüsteemi andmete või programmi ebaseadusliku sisestamise eest – karistatakse rahalise karistuse või kuni kolmeaastase vangistusega.
(2) Sama teo eest, kui see on toime pandud elutähtsa valdkonna arvutisüsteemi vastu või kui sellega on tekitatud oluline kahju, – karistatakse rahalise karistuse või kuni viieaastase vangistusega.
(3) Käesoleva paragrahvi lõikes 1 või 2 sätestatud teo eest, kui selle on toime pannud juriidiline isik, – karistatakse rahalise karistusega.[80]

2.1.2 Teoobjekt

KarS § 206 lg-s 1 sätestatud teoobjekt on arvutisüsteemis olevad arvutiandmed ja programmid. Enne 2008. aasta seadusemuudatust olid antud paragrahvis teoobjektina välja toodud arvutis olevad andmed või programmid. Järgnevalt analüüsitakse, mida on silmas peetud arvutis ehk arvutisüsteemis olevate andmete all.

Arvutiandmed karistusseadustiku kommentaaride kohaselt tähistavad igasugust faktide, teabe või mõistete esitust infosüsteemis töötlemiseks sobivas vormis. KarS §-s 206 käsitletakse eraldi ka programmi mõistet, mille all peetakse silmas süntaktilist üksust, mis vastab mingi programmikeele reeglitele ning koosneb teatava automatiseeritud andmetöötlusfunktsiooni täitmiseks vajalikest deklaratsioonidest, lausetest või käskudest ning mille kohaselt arvutisüsteem teostab automaatset andmetöötlust.[81]

Konventsioonis on arvutiandmete all silmas peetud teavet või programmi, mis on töötlemiseks sobivas vormis esitatud ning mille abil arvutisüsteem toimib.[82] Konventsiooni

[77] J. Sootak. Karistusõigus. Üldosa. Tallinn, 2010, lk 34.
[78] Karistusseadustik. Komm vln § 206 komm 1.1.
[79] Samas.
[80] Karistusseadustik (viide 13).
[81] Karistusseadustik. Komm vln § 206 komm 4 ja 5.
[82] Euroopa Nõukogu Arvutikuritegevusvastane konventsioon (viide 14).

seletuskirja kohaselt peavad need andmed olema sellises vormis, et neid oleks võimalik arvutisüsteemis töödelda, sest sihtmärgiks on elektrooniliselt töödeldavad andmed, mida materiaalsel kujul ei eksisteeri. Arvutiandmete mõistet on selgitanud ka raamotsus ja direktiiv – nende kohaselt on arvutiandmete puhul tegemist faktide, teabe või mõistete esitamisega infosüsteemis töötlemiseks sobivas vormis, mille abil saab infosüsteemi panna ülesannet täitma.[83] Seega nii konventsioonis, raamotsuses kui direktiivis on arvutiandmete all silmas peetud ka programme. Seega ei ole arusaadav, miks Eesti normilooja on koormanud sätet eraldi „programmi“ mõistega. Programmi puhul on tegemist ühe arvutiandmete liigiga, mistõttu piisab andmetest kõnelemisest. Seega on igati põhjendatud karistusõiguse revisjoni käigus tehtud ettepanek „programmi“ mõiste eemaldamiseks KarS §-st 206.[84]

Arvutisüsteemi mõistet on Eesti seadusandja soovinud sisustada konventsiooni abil: seade või omavahel ühendatud seadmete grupp, millest vähemalt üks täidab automaatse andmetöötluse funktsiooni.[85] Konventsiooni seletuskirja kohaselt on arvutisüsteemi puhul tegemist riist- ja tarkvarast koosneva seadmega, mis töötleb automaatselt digitaalseid andmeid. Inimene otseselt protsessi ei sekku: andmete töötlemine toimub automaatselt; andmete haldajaks on arvutisüsteemis olev programm või mitu programmi. Kuna arvutisüsteem koosneb erinevatest seadmetest, siis on oluline eristada, millal on tegemist protsessori või keskseadmega ning millal välisseadmega – viimast käesoleva töö autori arvates arvutisüsteemi osaks pidada ei saa, sest välisseade ei ole arvutisüsteemi lahutamatu osa. Välisseade on iseseisev seade, mis täidab teatud funktsioone koostoimel keskseadmega (printer, skänner, CD-lugeja/kirjutaja vms mäluseade).[86]

Erinevalt konventsioonist, kasutab raamotsus ja direktiiv „infosüsteemi“ mõistet, millega tähistatakse seadet või omavahel ühendatud või seotud seadmete rühma, mille hulgast üks või mitu seadet töötlevad vastavalt programmile automaatselt arvutiandmeid. Samuti aga nimetatud seadme või seadmete rühma salvestatud, töödeldud, välja võetud või edastatud arvutiandmeid, mis on vajalikud kõnealuse seadme või seadmete rühma toimimiseks, kasutamiseks, kaitseks ja hoolduseks.[87]

Konventsiooni, raamotsuse ning direktiivi artiklites kõneletakse arvutisüsteemi puhul, „andmete automaattöötlusest“. Järgnevalt uuritakse, mida selline protsess endast kujutab.

[83] Euroopa Nõukogu raamotsus (viide 15).
[84] Justiitsministeerium. Seletuskiri karistusseadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu juurde, lk 59.
[85] Karistusseadustik. Komm vln § 206 komm 3.
[86] Council of Europe. Explanatory Report to the Convention on Cybercrime. Arvurivõrgus. Kättesaadav: http://conventions.coe.int/Treaty/en/Reports/Html/185.htm, 23. aprillil 2014.
[87] Euroopa Parlamendi ja Nõukogu direktiiv (viide 16).

Arvutisüsteemi määratlemisel tuleb lähtuda *IPO*-printsiibist (*input, processing, output*; sisestamine, töötlemine, väljastamine). Selleks, et tegemist oleks arvutisüsteemiga, peab olema täidetud kolm tingimust. Esiteks peab olema võimalik sellesse andmeid sisestada, teiseks peab seade suutma neid andmeid töödelda (neist aru saama ja nendega midagi peale hakkama) ning kolmandaks olema võimeline neid väljastama.[88] Andmeid on võimalik arvutisüsteemi sisestada väga erineval moel, näiteks klaviatuuri, hiire või skänneri abil. Andmete töötlemisprotsess leiab aset binaarsüsteemis e kahendsüsteemis, kus arvutisüsteemid saavad aru ainult „ühtedest“ ja „nullidest“ ning kus arvutisüsteem võtab iga sisestatud teabe tohutuks hulgaks osadeks. Selles protsessis leiab aset andmete töötlemine, mille järel saab neid andmeid vastava programmiga väljastada – väljendudes monitoriekraanil ilmuva teabena, printeri poolt trükitud teabena või kõlari poolt edastatud akustilise teabena.[89]

Kui raamotsuse art 4 paneb EL-i liikmetele kohustuse kriminaliseerida teod infosüsteemis asuvate arvutiandmete vastu, mida teeb ka direktiivi art 5, siis konventsiooni art 4 on laialdasemalt mõistetav, sest sätestab kohustuse määratleda kuriteona teod kõigi arvutiandmete vastu; ei ole tähtsust sellel, kas arvutiandmed on arvutisüsteemis või mitte. Seega ei hõlma EL-i õigusaktid arvutisüsteemist väljaspool asuval andmekandjal (mälupulk, kõvaketas vms) paiknevaid andmeid või andmeid, mis liiguvad ülekandmise teel ühest serverist teise (nt meilid). Konventsioon on seega sõnastatud laiemalt kui EL raamotsus ning direktiiv, mistõttu EL-i aktide kohaselt on vaja tagada kaitse vähematele objektidele kui konventsioonis. Et KarS § 206 kõneleb otsesõnu „arvutisüsteemis olevatest“ objektidest, on selle sätte järgi kuriteona karistatavad need teod, mis on suunatud arvutisüsteemis olevate andmete ja programmide vastu, mitte aga nende andmete vastu, mis asuvad andmekandjal või mida parajasti edastatakse ühest arvutisüsteemist teise.[90] Seega tuleb tõdeda, et Eesti seadus ei vasta selles osas konventsiooni nõuetele.

KarS § 206 lg-ga 2 kriminaliseeritakse arvutiandmetesse sekkumine elutähtsa valdkonna arvutisüsteemi vastu. Elutähtsa valdkonna arvutisüsteemi mõistet karistusseadustik enne 2008. aasta seadusemuudatust ei tundnud. Varasemalt olid tuntud elutähtsa süsteemi ja elutähtsa rajatise mõiste, mida kasutavad KarS §-d 406 (elutähtsa süsteemi häirimine ja kahjustamine) ja 407 (elutähtsa rajatise kahjustamine). Nende all peetakse karistusseadustiku kommentaaride kohaselt silmas süsteeme ja rajatisi, mille toimimisest sõltub inimeste elu ja tervis, riigi

[88] E. Hirsnik. Arvutikuritegevuse koolitus, lk 3.
[89] E. Hirsnik (viide 88), lk 3.
[90] E. Hirsnik (viide 88), lk 20.

julgeolek ning majandussüsteem.[91]

Elutähtsad valdkonnad on ära nimetatud hädaolukorraks valmisoleku seaduse[92] § 7 lg-s 2, mille järgi on elutähtsa valdkonna arvutisüsteemiks selline süsteem, mis tagab erinevate valdkondade tegevuse, millest inimesed oma igapäevases elus sõltuvad. Näiteks kuuluvad siia sellised süsteemid, mis reguleerivad tervishoiuteenuse osutamist, tulekustutus- ja päästetööd, elektri- ja gaasisüsteemi toimimist, rahandussüsteemi, aga ka postisidet ning transporti.[93] Siinkohal ei ole tegemist ammendava loeteluga, vaid välja on toodud töö autori arvates kõige olulisemad elutähtsad valdkonnad.

Konventsioonis ja raamotsuses elutähtsa valdkonna arvutisüsteemi mõistet ei käsitleta, kuid direktiivis on kõneldud elutähtsast infrastruktuurist, mille sisu avab direktiivi 4. selgituspunkt. Selle kohaselt saab elutähtsa infrastruktuurina käsitleda liikmesriikides asuvat vara, süsteemi või selle osa (näiteks elektrijaamad, transpordivõrgud ja valitsusvõrgud), mis on hädavajalikud eluliselt tähtsate ühiskondlike toimingute, rahvatervise, turvalisuse, julgeoleku, majanduse ja sotsiaalse heaolu toimimiseks ning mille kahjustada saamine või hävimine mõjutaks nimetatud funktsioonide häirimise tulemusena oluliselt liikmesriiki.[94]

Kui analüüsida KarS § 206 lõike 1 ja 2 sisu, siis tuleb tõdeda, et tegemist on ilmselge vasturääkivusega. Kui esimese lõike järgi on teoobjekt arvutiandmed, siis teine lõige ei kõnele mitte arvutiandmete, vaid arvutisüsteemi vastu suunatud teo toimepanemisest. Seetõttu on karistusõiguse revisjoniga vajalik muuta KarS § 206 lg 2 sõnastust. Tegemist on põhimõttelise erinevusega, mida normis eksisteerida ei tohi. Alates 1989. aastast, mil Euroopa Nõukogu koostas „Soovituse nr (89) 9“, tehakse selget vahet arvutisüsteemi ja -andmete vastu toimepandud rünnetel. Sellest tulenevalt on tehtud ettepanek asendada „arvutisüsteem“ sõnadega „arvutisüsteemis olevate andmete“ või siis kvalifikatsioon kustutada, sest praegusel kujul olev sõnastus võib tekitada segadust normi mõistmisel.[95]

Karistusseadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse seletuskirja kohaselt on tehtud ettepanek KarS § 206 muutmiseks. Selle kohaselt lisatakse KarS § 206 lg-sse 2 p 1, mis sätestab vastutuse arvutiandmetesse sekkumisega toime pandud teo paljudes arvutisüsteemides olevate andmete vastu ja selle toimepanemisel kasutati KarS §-s 216[1] nimetatud seadet või arvutiprogrammi. Seadusemuudatuse eelnõu koostajad on direktiivist tulenevalt soovinud KarS §-ga 206 reguleerida ka robotvõrgu e *botnet* abil teostatavaid

[91] Justiitsministeerium (viide 43).
[92] Hädaolukorraks valmisoleku seadus. – RT I 2000, 95, 613.
[93] Karistusseadustik. Komm vln §206 komm 8.1.
[94] Euroopa Parlamendi ja Nõukogu direktiiv (viide 16).
[95] Justiitsministeerium (viide 84), lk 60.

ründeid, mille tulemusena võidakse sekkuda paljudes arvutisüsteemides olevatesse andmetesse.[96] Robotvõrk kujutab endast arvutitest koosnevat arvutivõrku, mis on vastavate programmide abil allutatud kurjategijale, kelle eesmärgiks on laiamastaabiliste rünnete teostamine. Need võivad olla suunatud nii arvutisüsteemi kui ka selles olevate andmete vastu. Robotvõrguga luuakse kaugkontroll arvutite üle sel teel, et nakatatakse eesmärgipäraste küberrünnakute abil kõnealused arvutid kurivaraga. Hiljem on võimalik nakatunud arvutitevõrk aktiveerida arvutikasutaja teadmata ning panna selle vahendusel toime suuremahuline rikkumine.[97] Selliste rünnete reguleerimine on õigustatud ja vajalik, kuid kuidas suhtuda määratlusse „paljudes arvutisüsteemides olevatesse andmetesse“, mis seadusemuudatuse tulemusena KarS § 206 lg 2 p-i 1 lisatakse.[98]

Käesoleva töö autori arvates on määratluse „paljudes arvutisüsteemis olevate andmete vastu“ sättesse lisamine küsitav, sest keeruline on anda hinnangut selle, kui suur hulk andmeid on „paljudes arvutisüsteemides olevad andmed“. Kas neid peab olema kümneid või piisab juba mõnest üksikust arvutisüsteemist, kus andmed asuvad? Vastuse sellele küsimusele saab anda tulevane kohtupraktika. Karistusseadustik näeb mitmes paragrahvis ette tunnuse „paljud“, mille all mõeldakse reeglina seda, et oht põhjustatakse paljude inimese elule või tervisele (KarS §-d 111, 112, 372 jt). Reeglina mõeldakse seda, et oht põhjustatakse konkreetselt määratlemata inimeste hulgale.[99] Kui näiteks robotvõrgu kasutamise korral võetakse „sihikule“ vaid mõnes üksikus arvutisüsteemis paiknevad andmed, võib ikkagi kõneleda „paljudest arvutisüsteemis olevatest andmetest“, sest andmete hulk, mida süsteem sisaldab on erinev. Ilmselt on selle punkti lisamise eesmärgiks reguleerida ründeid, mida pannakse toime KarS §-s 216[1] nimetatud seadme või programmi abil, mis ulatuslikemaid ründeid võimaldavad teostada, mida määratlus „paljudes arvutisüsteemis olevate andmete vastu“ näitab, ent nagu varasemalt kirjeldatud, võib seesuguse määratluse lisamine tuua kaasa probleeme sätte tõlgendamisel.

Karistusseadustiku seadusemuudatuse tulemusena sätestatakse vastutus KarS § 206 lg 2 p-ga 2 grupi poolt toime pandud arvutiandmetesse sekkumise eest. Selle lisamine on seotud direktiivi art 9 lg 4 p-ga a, sest teoobjekti vastaseid ründeid võivad teostada ka grupid e kuritegelikud ühendused. Varasemalt on karistusseadustik kasutanud kuritegeliku ühenduse mõistet, mis karistusõiguse revisjoni tulemusena asendatakse grupi mõistega. Punkti eesmärgiks on kriminaliseerida organiseeritud kurjategijate tegevus, kes võivad andmete

[96] Euroopa Parlamendi ja Nõukogu direktiiv (viide 16).
[97] Justiitsministeerium (viide 84), lk 60.
[98] Samas.
[99] Samas.

vastaseid ründeid teostada näiteks robotvõrkude vms loomise abil.[100] Sellest tulenevalt on põhjendatud ka kuni 5-aastane karistusmäär, sest grupi poolt teostatavad ründed võivad olla laiaulatuslikumad, kui seda on üksikute isikute poolt teostatavad ründed.

2.1.3 Koosseisutegu

KarS §-s 206 on koosseisupäraste tegudena välja toodud: ebaseaduslik muutmine, kustutamine, rikkumine või sulustamine ning arvutisüsteemi andmete või programmi ebaseaduslik sisestamine. Järgnevalt vaadeldakse, mida need teod endast kujutavad.

Koosseisutunnusena ei ole oluline, et tagajärg saabuks ning teo lõpuleviimiseks ei ole vajalik, et arvutisüsteemi töö saaks reaalselt häiritud, koosseisu realiseerumiseks piisab andmetesse sekkumisest[101] ning tahtlust koosseisu kõikide asjaolude suhtes ning see on täidetud, kui isik tegutseb vähemalt kaudse tahtlusega.[102]

Karistusseadustiku kommenteeritud väljaande kohaselt tähendab muutmine seda, et olemasolevad andmed või programm asendatakse teiste andmete või programmidega.[103] Käesoleva töö autori arvates on tegemist muutmisega siis, kui varasemaid andmeid on muudetud olulisel määral. Muutmisega ei ole tegemist siis, kui tekstidokumendis muudetakse üks või kaks tähte, vaid näiteks juhul, kui muudetakse faili struktuuri. Andmete muutmist saab pidada oluliseks, kui see kahjustab õigustatud isiku huve. Ka programmis olevate andmete muutmise korral saab kõneleda andmete muutmisest ja kohaldada isiku vastutuselevõtmiseks KarS §-i 206.

Kustutamise tulemusena kõrvaldatakse olemasolevad andmed või programm arvutisüsteemist.[104] Seega ei ole võimalik neid arvutisüsteemis olevaid andmeid või programme enam kasutada, kuigi arvutisüsteem ise võib selle tulemusena olla töökorras. Euroopa Nõukogu „Soovituses nr (89) 9“ leiti, et andmete kustutamine infosüsteemis on samaväärne kehalise eseme hävitamisega ning selline tegevus peab olema karistatav, sest kustutamise tulemusena ei pruugi andmed olla enam kättesaadavad.[105]

[100] Euroopa Parlamendi ja Nõukogu direktiiv (viide 16).
[101] Karistusseadustik. Komm vln § 206 komm 2.
[102] Karistusseadustik. Komm vln § 206 komm 7.
[103] Karistusseadustik. Komm vln § 206 komm 6.
[104] Samas.
[105] A. Bequai (viide 76), p 45.

Rikkumine tähendab, et andmetesse või programmi tehakse muudatus, mis teeb võimatuks andmete või programmi kasutamise nende esialgseks otstarbeks või raskendab seda.[106] Selle sekkumise tulemusena tekib negatiivne muutus arvutisüsteemi andmetes ja programmides, mistõttu on neid andmeid esialgsel eesmärgil raskem kasutada.[107] Sulustamine tähendab, et andmed ja programmid säilivad arvutisüsteemis, kuid arvutisüsteemi kasutaja ei saa neid kasutada, kuna juurdepääs nendeni on takistatud.[108] Õigustatud isiku seisukohast ei ole oluline, kas need andmed on sulustatud või kustutatud, sest mõlemal juhul ei ole tal võimalik neid kasutada.

Nimetatud koosseisuteod arvutisüsteemis olevate andmete vastu peavad olema toime pandud ebeseaduslikult. Samuti näevad KarS § 207 ja KarS § 217 objektiivse koosseisuelemendina ette „ebaseaduslikkust". Kui KarS § 206 ja KarS § 217 tundsid „ebaseaduslikkuse" koosseisuelementi juba varem, siis KarS § 207 kvalifikatsiooni lisati see 2008. aasta seadusemuudatusega.

Konventsioon, raamotsus ja direktiiv kasutavad oma artiklite pealkirjades mõistet „ebaseaduslik", kuid artiklites kõneletakse „õigusliku aluseta" toimepandud teost. Mõiste „ebaseaduslik" ja „õigusliku aluseta" on sünonüümid, sest mõlemad tähistavad seadusevastast tegevust, milleks on teo toimepanijal puudunud õigus. Karistusseadustiku kommentaarid ei defineeri mõiste „ebaseaduslik" sisu ega konventsioon mõiste „õigusliku aluseta" sisu. Nende all peetakse silmas manipulatsioone, mille teostamiseks ei ole isikutel õigust. Raamotsus ja direktiiv selgitavad „õigusliku aluseta" sisu ning nende kohaselt on tegemist toiminguga, mis ei ole lubatud süsteemi või selle osa omaniku või selle suhtes muu õiguse valdaja poolt, või millega rikutakse riiklikke õigusakte.[109] Ebaseaduslik arvutiandmetesse sekkumine, arvutisüsteemi toimimise takistamine või arvutisüsteemi kasutamine ei pea olema toime pandud isiku poolt, kellel puudub arvutile juurdepääs, vaid silmas on peetud ka sellist olukorda, kus töötajatele on tööülesannete täitmiseks antud volitus kasutada teatud osa arvutisüsteemist (nt kasutajakontot), ent juurdepääs hangitakse toimingute tegemiseks ka teisele kontole (nt adminkontole), milleks ei ole luba. Kui näiteks ettevõtte töötaja teostab uuendusi arvutisüsteemis, mille tõttu on süsteemi töö häiritud, ei ole tema tegevuse puhul tegemist arvutikuriteoga, sest volitused süsteemi toimimise takistamiseks on tal olemas. Kriminaliseeritud peab süsteemi toimimise takistamine olema ka juhul, kui selle teostamiseks

[106] Karistusseadustik. Komm vln § 206 komm 6.
[107] A. Bequai (viide 76), p 45.
[108] Karistusseadustik. Komm vln § 206 komm 6.
[109] Euroopa Parlamendi ja Nõukogu direktiiv (viide 16).

ületatakse volituste piire.[110] Samast põhimõttest lähtutakse andmetesse sekkumise puhul KarS §-s 206 ning arvutisüsteemi ebaseadusliku kasutamist reguleerivas KarS §-s 217.

Antud paragrahvis väljatoodud koosseisupäraste tegude määratlemise juures võib tekkida teatavaid probleeme, mida järgnevad näited kirjeldavad. Kui tegemist on olukorraga, kus üks isik kustutab teise inimese arvutist käsklusega „*delete*“ faili, siis kas sellisel juhul on tegemist kustutamisega või sulustamisega? Arvutisüsteemis olevate andmete kustutamise tagajärjel ei ole nende kasutamine enam võimalik. Käsklus „*delete*“ asetab faili ühest asukohast teise (paberkorvi) ning seega ei ole tegemist kustutamisega, vaid sulustamisega.[111] Faili saab sellisel juhul kerge vaevaga endisesse asukohta asetada ja seega võib sulustamise järgi isikule karistuse määramine kaasa tuua ülekriminaliseerimise, sest antud näite põhjal jäävad andmed algsel kujul alles. Seega, kui teoeelse olukorra saab kergesti ja kiiresti taastada, siis ei ole õige koosseisupärasest teost rääkida. Siinkohal tuleb koosseisu realiseerumise puhul vaadelda ka seda, kas isik, kelle fail paberkorvi asetati, oskaks endist olukorda taastada. Kui ta oskab seda, siis ei ole tegemist koosseisupärase teoga, kui aga mitte ja sellest teo sooritaja teadis, siis võib tegemist olla koosseisupärase teoga.[112]

Piiritlemisprobleemi sulustamise ja kustutamise vahel ei teki aga siis, kui isik kasutab faili kustutamiseks arvutis käsklust „*Shift*“ + „*Delete*“. Sellisel juhul on tegemist sulustamisega, sest endise olukorra taastamine on keeruline. Olukord on taastatav spetsiaalsete programmidega siis, kui süsteemi ei ole salvestatud uusi andmeid, kui seda on tehtud siis on andmed pöördumatult kadunud ning endise olukorra taastamine ei ole võimalik.[113]

Seejuures on vajalik hinnata olukorra tõsidust, sest minimaalset arvutiandmetesse sekkumist ei ole põhjendatud arvutikuriteona käsitleda. Sellisel juhul tuleks vaadata, millistesse andmetesse on sekkutud, kas nende andmetega on aset leidnud mõni muutus, mis nende omanikule kahju võib põhjustada.

KarS § 206 käsitleb koosseisupärase teona ka andmete või programmi arvutisüsteemi sisestamist, mis tähendab nende arvutisüsteemi kandmist andmetöötlusprotsessiks või säilitamiseks.[114] Mida normilooja on sisestamise alternatiivi all silmas pidanud ning mis eristab sisestamist edastamisest, sest KarS §-s 207 on teoalternatiividena nimetatud mõlemaid? Mõisteid eristatakse ka konventsiooni art-s 5, raamotsuse art-s 3 ja direktiivi art-s 4, ent defineeritud neid ole. Sisestamine on andmete vahetu lisamine süsteemi (nt hiire, klaviatuuri,

[110] R. W. Downing (viide 4), p 727.
[111] E. Hirsnik (viide 88), lk 21.
[112] Samas.
[113] Samas.
[114] Karistusseadustik. Komm vln § 206 komm 6.

USB-pulga abil), edastamine on aga andmete lisamine läbi teise arvutisüsteemi (nt meilide vahetamine).[115] KarS §-s 206 seisneb probleem selles, et sisestamise mõistet kasutatakse liiga laialt, sest Eesti kohtud (sh Riigikohus) lähtuvad sisestamise all ka edastamise mõttest, kuigi koosseisuteod on erinevad – andmete lisamist ühest arvutisüsteemist teise arvutisüsteemi ei saa pidada sisestamiseks.[116]

Karistusseadustiku muutmise seaduse eelnõus on jõutud järeldusele, et sisestamise formuleering tuleb KarS §-st 206 eemaldada, sest esiteks ei tunne seda konventsiooni art 4, raamotsuse art 4 ega ka direktiivi art 5 ning selle formuleeringuga võib kaasneda ülekriminaliseerimise oht. Rahvusvaheliste normiloojate eesmärgiks on olnud kaitsta õigustatud isikute selliseid huve, mis seonduvad juba olemasolevate andmetega, mitte nendega, mida saab süsteemi juurde lisada – sellest põhimõttest peaksid lähtuma ka siseriiklikud normiloojad.[117] Kui lähtuda sellest, et hoolimata KarS §-st 207 on KarS §-s 206 hõlmatud igasugune andmete lisamine, tooks see kaasa ülekriminaliseerimise. Andmete lisamist (sisestamist) andmesüsteemi kujutaks seega ka meili või SMS-i saatmine. Kui näiteks saatja möönab, et adressaat meili või SMS-i ei soovi, siis tuleks teda hetkel kehtiva seaduse kohaselt karistada.[118]

2.1.4 Muud aspektid

Karistuse määramisel võib tekkida küsimus, milline säte teatud teo puhul kohaldub. Millistel juhtudel on õige kohaldada KarS § 206 asemel KarS § 207, millal KarS § 206 asemel KarS § 213? KarS § 206 ja KarS § 213 eristab see, et kuigi tegu nende kahe koosseisu puhul on andmetesse sekkumise korral sama, peab KarS § 213 kohaselt saabuma teole ka tagajärg. Kui arvutiandmetesse sekkumise koosseisuga kaitstakse arvutisüsteemi omaniku ja õigusliku valdaja arvutisüsteemiga seotud õigusi, siis arvutikelmuse koosseisuga on kaitstavaks õigushüveks vara. Arvutiandmetesse sekkumise puhul ei ole oluline, et sellest varalist kasu saadakse, koosseisu realiseerumiseks piisab asjaolust, et tegu on toime pandud. KarS § 206 ja KarS § 213 piiritlemist on käsitlenud Riigikohus oma lahendis 3-1-1-114-12. Riigikohus leidis, et kuigi KarS § 213 kohaldamine kõne alla ei tule, sest varalist kasu ei saadud, tuleks tähelepanu pöörata sellele, et süüdistatav sisestas ettevõtte tuvastuskoodid Internetipanka ebaseaduslikult. Andmete ebaseaduslik sisestamine arvutisüsteemi on kuriteona karistatav

[115] E. Hirsnik (viide 88), lk 23.
[116] Samas.
[117] Justiitsministeerium (viide 84), lk 59.
[118] E. Hirsnik (viide 88), lk 24.

KarS § 206 lg 1 järgi, sest andmete ebaseaduslik sisestamine hõlmab arvelduskontole juurdepääsu ja sellel oleva varaga toimingute tegemist võimaldavate andmete sisestamist, kui selleks puudub arvelduskonto omaniku nõusolek.[119] Kuna andmete ebaseaduslik sisestamine (KarS § 206 lg 1) on varalise kasu saamise viisina KarS § 213 lg-s 1 nimetatud, kujutab KarS § 213 lg 1 endast sisuliselt KarS § 206 lg 1 kvalifitseeritud koosseisu. KarS § 206 lg 1 tuleb kohaldada juhul, kui puudub nii KarS § 213 koosseisupärane tagajärg ning tahtlus varalist kasu saada.[120] Kui aga saadakse ka varalist kasu, võib tegemist olla ideaalkogumiga.

KarS §-l 206 esineb piiritlemisprobleeme ka KarS §-ga 207, mida analüüsitakse arvutisüsteemi toimimise takistamise alapeatükis.

[119] RKKKo 14.12.2012, nr 3-1-1-114-12, p 9.
[120] K. Domaškina. Ebaseaduslik sekkumine arvutiandmetesse ja sel teel varalise kasu saamine. Riigikohtu kriminaalkolleegiumi otsus 3-1-1-114-12. – Juridica, 2013, nr 2, lk 145.

2.2 Arvutisüsteemi toimimise takistamine

2.2.1 Sissejuhatavad märkused

Seoses 2008. aasta seadusemuudatusega täpsustati KarS §-s 207 arvutisüsteemi toimimise takistamise süüteokoosseisu objektiivset külge, sest varasem redaktsioon käsitles üksnes ühenduse rikkumist või tõkestamist. Muudatustega asendati ühenduse häirimine ja tõkestamine arvutisüsteemi toimimise takistamisega ning normi lisati kirjeldus, mil viisil see peab toimuma (sisestamise, edastamise, kustutamise, rikkumise, muutmise või sulustamise teel). Peamine põhjus, miks need teokirjeldused sättesse lisati, seisnes selles, et uue sõnastusega välistada igasugused otsese füüsilise mõjutusega takistused, mis antud paragrahvi all ei kvalifitseeru. Nende all peetakse silmas sidekaablite, arvutisüsteemide füüsilist hävitamist ning lõhkumist, aga ka füüsilist elektri väljalülitamist.[121] Lõikega 2 lisati vastutus elutähtsa valdkonna arvutisüsteemi toimimise takistamise eest ning samuti juhul, kui selle tulemusena häiritakse avaliku võimu toimimist või avalike teenuste osutamist. Lõikega 3 lisati juriidilise isiku vastutus, mida varasem redaktsioon ette ei näinud.[122]

Euroopa Nõukogu „Soovitusega nr (89) 9“ leiti, et arvutikuritegevust reguleerivate sätetega on vajalik kriminaliseerida ka arvutisabotaaži e arvuti- või telekommunikatsioonisüsteemi toimimise takistamist, kui see on aset leidnud arvutiandmete või programmide sisestamise, muutmise, kustutamise või sulustamise teel.[123]

Kuigi KarS § 207 asub karistusseadustiku varavastaste süütegude peatükis, ei ole normiga kaitstavaks õigushüveks vara, vaid arvutisüsteemide õiguspäraste kasutajate õiguspärane ootus arvutisüsteemide takistamatuks kasutamiseks.[124]

§ 207. Arvutisüsteemi toimimise takistamine
(1) Arvutisüsteemi toimimise ebaseadusliku häirimise või takistamise eest andmete sisestamise, edastamise, kustutamise, rikkumise, muutmise või sulustamise teel – karistatakse rahalise karistuse või kuni kolmeaastase vangistusega.
(2) Sama teo eest, kui sellega on tekitatud oluline kahju või kui sellega takistatakse elutähtsa valdkonna arvutisüsteemi tööd või avalike teenuste osutamist, – karistatakse rahalise karistuse või kuni viieaastase vangistusega.
(3) Käesoleva paragrahvi lõikes 1 või 2 sätestatud teo eest, kui selle on toime pannud juriidiline isik, – karistatakse rahalise karistusega.[125]

[121] Justiitsministeerium (viide 43).
[122] Samas.
[123] A. Bequai (viide 76), p 47.
[124] Karistusseadustik. Komm vln § 207 komm 1.1.
[125] Karistusseadustik (viide 13).

Arvutisüsteemi toimimise takistamist reguleerivad rahvusvahelistes õigusaktides konventsiooni art 5, raamotsuse art 3 ja direktiivi art 4. Konventsiooni art 5 kohaselt peab konventsiooniosaline võtma seadusandlikke ja muid meetmeid, et oma seaduses määratleda kuriteona arvutisüsteemi toimimise oluline takistamine, mis pannakse toime tahtlikult ja ilma õigusliku aluseta arvutiandmeid sisestades, edastades, kustutades, rikkudes, muutes või sulustades.[126] Ebaseadusliku süsteemi sekkumise sätestab ka raamotsuse art 3, mille kohaselt tuleb riigil võtta vajalikud meetmed, et infosüsteemi töö tahtlik takistamine või katkestamine arvutiandmete sisestamise, edastamise, kahjustamise, kustutamise, rikkumise, muutmise, sulustamise või ligipääsmatuks muutmise teel on kriminaalkorras karistatav.[127] Sama sõnastust on kasutanud ka direktiiv ebaseadusliku süsteemi häirimise sätestamiseks oma art-s 4.[128] Uue direktiiviga, mis asendab varasemat raamotsust, kaitstakse infosüsteemide terviklikkust, mille tõttu saab infosüsteemi sekkumine olla ebaoluline ainult juhul, kui see on vähese tähtsusega või kui infosüsteemi terviklikkust on kahjustatud vähesel määral.[129]

2.2.2 Teoobjekt

Kui KarS § 206 reguleerib arvutisüsteemis olevatesse andmetesse sekkumist, siis KarS § 207 reguleerib arvutisüsteemi kui terviku toimimise takistamist. Teoobjektiks on antud sättes arvutisüsteem, mida erinevate rünnete eest kaitstakse. Arvutisüsteemi mõistet ja sisu käsitleti juba KarS § 206 analüüsis, nagu ka elutähtsa valdkonna arvutisüsteemi. Järgnevalt uuritakse, mida tähendab KarS § 207 lg-s 2 väljatoodud „avalike teenuste osutamise takistamine“. Karistusseadustiku kommentaarid ei sätesta, mida KarS § 207 lg-s 2 esitatud „avalike teenuste osutamise“ all on peetakse silmas on peetud, kuid ilmselt on tegemist selliste arvutisüsteemide toimimise takistamisega, mis inimeste elu igapäevaselt mõjutavad. Selliseid avalikke teenuseid osutavad näiteks Maksu-ja Tolliamet, riigiportaal *e*-riik, mis pakub usaldusväärset infot, kontaktandmeid ning avalikke *e*-teenuseid, aga ka sotsiaalvõrgustik *Facebook*, meiliserverid jt.

Konventsiooni art 5 ega konventsiooni seletuskiri ei nimeta neid avalike teenuste osutamise arvutisüsteeme, mille töö ründe tulemusena peab häiritud saama – need konkreetsed arvutisüsteemid, mis inimeste elu igapäevaselt mõjutavad, on jäetud konventsiooniosaliste määrata. „Avalike teenuste“ sisu ei ava raamotsuse art 3 ega ka direktiivi art 4, jättes samuti

[126] Euroopa Nõukogu Arvutikuritegevusvastane konventsioon (viide 14).
[127] Euroopa Parlamendi ja Nõukogu direktiiv (viide 16).
[128] Samas.
[129] Euroopa Nõukogu raamotsus (viide 15).

nende süsteemide määratlemise liikmesriikidele.

Kehtivas regulatsioonis esineb normi sõnastuses paar süstemaatilist viga, milles esimene puudutab KarS § 207 lg-s 2 kasutatav sõna „tööd“. Kui võrrelda sätte esimest ja teist lõiget, siis näeme, et esimeses lõikes kõneletakse toimimisest, teises lõikes aga tööst.[130] Siinkohal võib tekkida küsimus, kas toimimise ja töö all mõeldakse erinevaid protsesse või kasutatakse neid mõisteid normis sünonüümidena. Normilooja eesmärgiks peab olema siiski võimalikult selgete, konkreetsete ja arusaadavate sätete koostamine, et vältida segadust sätete tõlgendamisel. Karistusõiguse revisjoniga on tehtud ettepanek asendada normi teises lõikes olev sõna „tööd“ sõnaga „toimimist“ või kvalifikatsioon kustutada.[131] Käesoleva töö autor pooldab sõna asendamist, sest see aitab normis süstemaatilise vea kõrvaldada ning muudab normi sisu lugejale üheselt mõistetavaks.

Direktiivist tulenevalt lisatakse KarS § 207 lg-sse 2 p 1, mis reguleerib arvutisüsteemi toimimise ebaseaduslikku häirimist ja takistamist, kui see on toime pandud paljude arvutisüsteemide vastu ning selle toimepanemisel on kasutatud KarS §-s 216[1] nimetatud seadet või arvutiprogrammi. Direktiivi kohaselt on liikmesriigi kohustuseks võtta vajalikud meetmed tagamaks, et artiklites 4 ja 5 osutatud kuritegude tahtliku toimepanemise eest määratakse karistus, mille maksimummäär on vähemalt kolmeaastane vangistus, kui arvestatavat hulka infosüsteeme on mõjutatud sellise artiklis 7 osutatud vahendi kasutamise teel, mis on loodud või kohandatud eelkõige kuriteo toimepanemiseks. Samadel alustel on lisatud KarS § 206 lg-sse 2 p 1, kuid erinevus nende kahte sätte vahel seisneb selles, et KarS § 207 puhul ei ole ründeobjekt mitte arvutiandmed, vaid arvutisüsteem ning sellest tulenevalt tuleb kasutada KarS § 207 lg 2 p-s 1 sõnastust „paljude arvutisüsteemide vastu“.[132]

Karistusseadustiku seadusemuudatusega tuleb KarS § 207 lg-sse 2 lisada kvalifitseeriva tunnusena grupilisus, kohustuse selle lisamiseks sätestab direktiivi art 9 lg 4 p a.

2.2.3 Koosseisutegu

Koosseisupärased teod on käesolevas sättes andmete sisestamine, edastamine, kustutamine, rikkumine, muutmine ja sulustamine, mille tulemusena võidakse arvutisüsteemi toimimist häirida või takistada. Karistusseadustiku kommentaaride kohaselt ei subsumeerita füüsiliste

[130] Justiitsminiseertium. Arvamuste tabel karistusseadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu seletuskirja juurde, lk 27.
[131] Samas.
[132] Justiitsministeerium (viide 84), lk 60.

mõjutustega põhjustatud takistused, nagu sidekaablite, arvutisüsteemide füüsiline rikkumine mitte KarS § 207, vaid KarS § 203 järgi.[133] Selle väite tõepärasus on küsitav, sest kui näiteks mobiiltelefoni maha viskamisega põhjustatakse telefonis olevate andmete kustutamine, pöördumatu mittetöödeldavateks tegemine, siis saab kõneleda nii andmete kustutamisest KarS § 206 kohaselt kui ka arvutisüsteemi toimimise takistamisest KarS § 207 järgi. Hävinenud ei ole seetõttu ainult õigustatud isiku füüsiline ese – telefon, vaid ka selles sisalduvad andmed, mille kaitse tuleb samuti normidega tagada.

Koosseisutunnusena on oluline, et saabuks tagajärg ning arvutisüsteemi tööd reaalselt häiritaks või takistataks. KarS § 207 puhul on tegemist KarS § 206 kvalifikatsiooniga, sest kui viimase puhul piisab pelgalt andmete kustutamisest, rikkumisest, muutmisest, sulustamisest või sisestamisest, nõuab KarS § 207 neile lisaks tagajärge – süsteemi toimimise häirimist või takistamist. Kuna KarS § 207 on KarS § 206 kvalifikatsioon, neeldub arvutiandmetesse sekkumine arvutisüsteemi toimimise takistamises ning karistus toimepandud teo eest järgneb viimase järgi. Neid sätteid eristab aga see, et KarS § 206 puhul peab andmetesse sekkumine olema ebaseaduslik, kuid KarS § 207 puhul võib andmetesse sekkumine olla seaduslik, kui sellega vähemalt kaudse tahtlusega häiritakse või takistatakse arvutisüsteemi toimimist.[134]

Subjektiivsest küljest eeldatakse antud süüteo puhul tahtlust kõigi asjaolude suhtes, va olulise kahju tekkimist (KarS § 207 lg 2) ning koosseis on täidetud, kui isik tegutseb vähemalt kaudse tahtlusega.[135]

Andmete sisestamist, kustutamist, rikkumist, muutmist ja sulustamist analüüsiti juba töö eelnevas peatükis ning seetõttu analüüsitakse käesolevas edastamist ning uuritakse, milline peab olema koosseisupärane häirimine ja takistamine.

KarS § 207 on osaliselt enamat kui pelgalt KarS § 206 kvalifikatsioon, sest viimase puhul on koosseisupärane tegu ka „andmete edastamine“ (rahvusvahelistes õigusaktides ka „sisestamine“). Nimetatud teokirjelduse lisasid rahvusvahelised normiloojad selliste olukordade reguleerimiseks, kus süsteemi tööd häiritakse seoses uute andmete lisamisega, sest alati ei ole ründed suunatud arvutisüsteemi nn vanade andmete vastu. Selline uute andmete lisamine võib aset leida näiteks robotvõrgu vahendusel, mida võidakse kasutada ministeeriumite arvutisüsteemi toimimise takistamiseks, et piirata nii töötajate kui tavakasutajate koduleheküljele pääsemist. Robotvõrgu abil võivad selles võrgus olevad arvutid hakata iseseisvalt sisenema korduvalt ministeeriumi kodulehele, põhjustades rünnaku,

[133] Karistusseadustik. Komm vln § 207 komm 2.1.
[134] Karistusseadustik. Komm vln § 207 komm 5.
[135] Karistusseadustik. Komm vln § 207 komm 4.

millega võib kaasneda oluline kahju.[136] Süsteem võib robotvõrgu kasutamise tulemusena saada uusi andmeid ning antud näite põhjal järeldub, et alati ei pea olema midagi tehtud vanade andmete vastu, sest ka uute andmete edastamine võib kaasa tuua arvutisüsteemi toimimise takistamise.

KarS § 207 kohaldub, kui koosseisupärase teoga häiritakse või takistatakse arvutisüsteemi tavapärast toimimist. Karistusseadustiku kommentaaride kohaselt on arvutisüsteemi toimimise häirimine arvutisüsteemi funktsioonide täitmise halvendamine, eelõige arvutisüsteemi poolt ülesannete täitmise aeglustamine.[137] Seejuures on oluline lähtuda konkreetsest situatsioonist, sest igasugune arvutisüsteemi toimimise häirimine ei pruugi kaasa tuua selliseid tagajärgi, et oleks vajalik ning põhjendatud kriminaalkaristust kohaldada. Häirimisega on tegemist siis, kui näiteks ettevõtte endine töötaja saadab sisutühje meile tööandja serverisse, et viimase aega kulutada nende kustutamisele. Kui tööandja meiliserveri töö selle tulemusena ei aeglustu või ei lakka, siis ei saa rääkida endise töötaja vastutusele võtmisest KarS § 207 alusel, sest õigushüve, mida antud paragrahviga kaitstakse, kahjustada ei saa. Ka ajakulu nende sisutühjade meilide likvideerimiseks ei ole piisav argument kriminaalvastutuse kohaldamiseks. Teistsugune oleks olukord siis, kui töötaja teostaks *DoS*-ehk teenusetõkestusründeid tööandja meiliserveri töö takistamiseks. Kui arvutisüsteemi ei saa enam tavapäraselt kasutada ning tekib infosulg, on vastutuse kohaldamine õigustatud.

Arvutisüsteemi toimimise takistamine on arvutisüsteemi funktsioonide täitmise vähemalt ajutise lakkamise põhjustamine.[138] Takistamise puhul on tegemist tagajärjega, mis toimepandud teole järgneb, ent koosseisuteo alapunktis käsitletakse seda strukturaalsetel põhjustel. Tavaliselt teostatakse selliseid ründeid erinevate programmide abil, et blokeerida mõne inimese, asutuse või riigi arvutisüsteemi tööd.[139] Konventsiooni seletuskirja kohaselt peab karistuse kohaldamiseks tegemist olema tõsise takistamisega, ent see, millisel juhul on tegemist tõsise takistamisega, jäetakse konventsiooniosaliste otsustada.[140] Häirimise mõistet, mida kasutab Eesti normilooja, konventsioon ei kasuta ning sellest tulenevalt tekib küsimus, kas konventsiooni art-ga 5 saab reguleerida ka rämpsposti saatmist, arvutiviiruse levitamist, sest need tegevused võivad samuti arvutisüsteemide tööd oluliselt takistada. Konventsiooni seletuskirja kohaselt võib art-ga 5 reguleerida kirjade masspostitust ning arvutiviiruse levitamist, sest nende tegevuste tulemusena võib aeglustuda või katkeda arvutisüsteemi töö

[136] Euroopa Parlamendi ja Nõukogu direktiiv (viide 16).
[137] Karistusseadustik. Komm vln § 207 komm 2.2.
[138] Samas.
[139] Council of Europe (viide 86), p 67.
[140] Samas.

või võrguosutaja teenus.[141]

Kirjade masspostitus kujutab endast kindla intervalliga elektronkirjade saatmist teatud meiliaadressile, eesmärgiga halvata süsteemi tööd. Saaja poolelt vaadates on rämpspost selline post, mida saaja ei vaja või ei soovi saada ning mis risustab tema postkasti.[142] Sellist elektronkirjade masspostitust käsitleb riigikohtu lahend 3-1-1-85-08, kus J. K saatis maavalitsuse elektronposti aadressile suure arvu mittevajalikke elektronkirju, millele olid lisatud ka manused ning mille tulemusena ummistusid töötajate kirjakastid ning selle tulemusena takistati ka meilide vahetamist, saatmist ning vastuvõtmist. [143] Antud kohtulahendis määrati J.K-le karistus KarS § 207 järgi, sest juba siis leiti, et KarS §-de 207 ja 208 koosseisulised tunnused erinevad oluliselt üksteisest. Arvutiviiruse levitamine leiab aset ainult viiruse kui iseleviva ja isetoimiva kahjuliku arvutiprogrammi olemasolul ning seejuures ei ole ühendus arvutivõrguga vajalik, kuna viirust saab levitada ka andmekandja vahendusel. Seega ei ole arvutivõrgu olemasolu KarS § 208 koosseisuliseks tunnuseks. KarS §-s 207 sätestatud arvutivõrgu või -süsteemi ühenduse kahjustamise puhul on aga esmase tähendusega arvutivõrgu või -süsteemi olemasolu ja nende ühenduse rikkumine või tõkestamine, mida käesoleval juhul kirjade masspostitusega teostati.[144]

Konventsiooniosalise riigi otsustada jäetakse aga see, kas arvutisüsteemi toimimise takistamine peab karistuse kohaldamiseks olema aset leidnud osaliselt või täielikult, ajutiselt või alaliselt. [145] Arvutisüsteemi toimimise takistamine on arvuti süsteemi funktsioonide täitmise vähemalt ajutise lakkamise põhjustamine – käesolevaga näeme, et Eesti normilooja lähtub mõistest „ajutine“.

Siinjuures võib tekkida küsimus, miks on EL-i normiloojad eraldi välja toonud kahjustamise ning ligipääsmatuks muutmise teoalternatiivid raamotsuse art-s 3 ja direktiivi art-s 4. Eesti normilooja ei ole neid KarS §-s 207 välja toonud, vaid on lähtunud konventsiooni art 5 sõnastusest. See on igati põhjendatud, sest ilmselt on Eesti normilooja katnud kahjustamise mõiste juba andmete rikkumise elemendi väljatoomisega ning ligipääsmatuks muutmist reguleerib sättes juba sulustamise element. Käesoleva töö autori arvates saab neid mõisteid kasutada sünonüümidena ning seetõttu ei ole topeltviitamine samasugustele koosseisuelementidele normis vajalik.

[141] Council of Europe (viide 86), p 69.
[142] H. Vallaste. e-Teatmik: IT ja sidetehnika seletav sõnaraamat. Arvutivõrgus. Kättesaadav: http://vallaste.ee/index.htm?Type=UserId&otsing=2330, 23. aprillil 2014.
[143] RKKKo 25.02.2008, nr 3-1-1-85-08.
[144] Samas.
[145] Council of Europe (viide 86), p 69.

KarS § 207 analüüsi käigus on selgunud veel üks süstemaatiline viga. KarS § 207 lg-s 1 tehakse vahet häirimisel ja takistamisel, kuid sama sätte lõikes 2 kõneletakse vaid takistamisest, ent seesugust eristust normilooja põhjendanud ei ole.[146] Töö autor nõustub väitega, et seesugune eristamine normi selguse huvides on korrektne ning igati õigustatud on revisjoni käigus tehtud ettepanek lisada normi sõnade „sellega“ ja „takistatakse“ vahele sõnad „või häiritakse“ või kvalifikatsioon kustutada, sest vastasel korral ei reguleeriks normi lõige 2 häirimist koosseisuteona üldse.[147] Tekib küsimus, miks on Eesti normilooja sättesse lisanud häirimise mõiste, sest konventsioon, raamotsus ja direktiiv häirimise mõistet arvutisüsteemi toimimise takistamise sätetes ei kasuta. Ilmselt soovitakse normiga reguleerida ka neid olukordi, mille tagajärjeks ei ole arvutisüsteemi funktsioonide täitmise lakkamine, vaid aeglustumine.

Järgnevalt vaadeldakse erinevaid ründeid, mis KarS § 207 alla kvalifitseeruvad. Nendeks on: elektronkirjade masspostitus, arvutiviiruse levitamine, *DoS*-ründed ning robotvõrkude vahendusel teostatud ründed – nimetatud tegevustega võidakse olulisel määral takistada arvutisüsteemi tavapärast toimimist. Käesolevas töös on eelnevalt käsitletud elektronkirjade masspostitust, mistõttu vaadeldakse järgnevalt, mida kujutavad endast *DoS*-ründed ja robotvõrgu ründed, millega arvutisüsteemi toimimist saab takistada. Arvutiviiruse levitamist käesolevas peatükis ei käsitleta, sest selle analüüs leiab aset käesoleva töö alapunktis 2.3.

DoS-rünne e teenusetõkestusründe (*Denial of Service*) puhul on tegemist arvutisüsteemi vastase ründega, milles süsteemile esitatakse sedavõrd palju päringuid, et ta ei suuda nendega toime tulla, neid hallata, muutudes töökõlbmatuks. Sellise ründe korral koormatakse võrk tarbetu liiklusega üle. Ründed võivad olla suunatud mistahes võrguseadme vastu (sh marsruuterid, veebi- ja meiliserverid). Praktikas on tavapärane, et arvutisüsteemile esitatavad päringud seadistakse *DoS*-rünnete puhul keerulisemalt, kui tavapäringud, mistõttu on need serveri jaoks koormavamad ning süsteem võib selle tulemusena lakata tööst.[148]

Selliste rünnetega tuli Eestis laialdaselt kokku puutuda 2007. aasta aprillirahutuste ajal, mil neid erinevate pankade, ministeeriumite ning teiste riiklikele arvutisüsteemide vastu teostati, et häirida ja takistada nende tööd. Sellega seoses tulid välja karistusseadustiku kitsaskohad, mille tõttu võivad arvutikurjategijad karistusest pääseda. 2008. aastal muudeti KarS § 207 kvalifikatsiooni ja asendati ühenduse häirimine ja tõkestamine arvutisüsteemi toimimise takistamisega ning lisati kirjeldus, mil viisil see peab aset leidma. Varasem KarS § 207

[146] Justiitsministeerium (viide 130), lk 27.
[147] Samas.
[148] H. Vallaste. e-Teatmik: IT ja sidetehnika seletav sõnaraamat. Arvutivõrgus. Kättesaadav: http://vallaste.ee/index.htm?Type=UserId&otsing=2330, 223. aprillil 2014.

kvalifikatsioon *DoS*-ründeid ei reguleerinud.[149]

Arvutisüsteemi toimimise takistamist võidakse teostada ka robotvõrke kasutades. Nende võrkude abil saab toime panna nii varasemalt mainitud *DoS*-ründeid, elektronkirjade masspostitust kui ka levitada pahavara, nuhkida kasutajate järel ning ummistada veebiliiklust.[150] Inimene, kelle võrku kuritegude toimepanemiseks kasutatakse, ei pruugi seda märgata. Samal ajal kui tema teeb tavapäraseid toiminguid arvutis, võib süsteem teostada kuritegelikke ründeid, olles robotvõrgu lüli. Robotvõrku võib kuuluda miljoneid arvuteid, ent viimasel ajal on arvutikurjategijate seas domineeriv arusaam, et kõige optimaalsem ja ohutum on pidada väikesi, paarikümnest arvutist koosnevaid robotvõrke, millest ulatusliku rünnaku teostamiseks piisab. Sellest hoolimata võib mõnda robotvõrku kuuluda iga neljas 600 miljonist Internetti ühendatud arvutist.[151] Samuti võivad ühed kurjategijad üürida neid võrke teistele nii anonüümsuse eesmärgil kui ka seetõttu, et suurema hulga arvutitega on arvutiandmete või süsteemi kahjustamine ulatuslikum. Robotvõrgu puhul on tegemist väga spetsiifilise süsteemiga, mille avastamisel korral tuleb see oskuslikult süsteemist eemaldada, sest vastasel korral saab kurjategija seda edasi kasutada. Huvitavat lähenemisviisi selle eemaldamiseks on kasutanud Holland oma „Bredolabi“ juhtumis, millest annab ülevaate E. Tikk-Ringase „Juridicas“ ilmunud artikkel, mis nimetatud robotvõrgu avastamist ja likvideerimist käsitleb. Nimelt olid paljud Hollandi arvutisüsteemid selle juhtumi puhul seotud robotvõrguga, mille abil arvutikurjategijad ründeid teostasid. Kuriteo avastamise järel ei suutnud Hollandi politsei tuvastada kõiki võrgus olevaid arvuteid, mis selle robotvõrguga seotud olid. Seetõttu otsustati kasutada kahjustunud arvutivõrkude puhastamiseks robotvõrgu enda infrastruktuuri. Kui politsei oli kontrollinfrastruktuuri üle võtnud, kasutati olemasolevaid robotvõrke, millega ründeid teostati selleks, et anda nakatunud arvutitele korraldus teavitada omanikke ja kasutajaid asjaolust, et nende arvutis sisaldub pahavara, ning lisati informatsioon sellest vabanemiseks.[152] Selline robotvõrgu kasutamine olukorra likvideerimiseks võib olla õiguslikult küsitav. Kuna eraldi robotvõrkude mahavõtmist käsitlevaid norme Hollandi õiguses polnud, siis tuletas politsei oma tegevuse põhialuse sealse politseiseaduse sätetest.[153] Juristid hindasid selle meetme vastavaks nii seaduslikkuse kui ka isikuandmete töötlemise minimaalsuse põhimõttele ning asusid seisukohale, et robotvõrku kasutades ei pane politsei toime arvutitesse ebaseaduslikku sisenemist, kuigi robotvõrku haldav tarkavara installeeriti

[149] Justiitsministeerium (viide 43).
[150] E. Tikk-Ringas (viide 34), lk 282.
[151] Arvutikaitse. Arvutivõrgus. Kättesaadav: http://www.arvutikaitse.ee/arvutikaitse-algtoed/botnet/, 23. aprillil 2014.
[152] E. Tikk-Ringas (viide 34), lk 282.
[153] Samas.

ning käivitati. Selle õigustuseks kõneleb fakt, et nakatunud olid miljonid arvutid ning nende arvutite omanike väljaselgitamine oleks võtnud kaua aega ning olnuks isikute eraelule koormavam kui anonüümsete teadete saatmine.[154] Kirjeldatud näide ilmestab hästi seda, et robotvõrgu puhul on tegemist väga mõjuvõimsa vahendiga, mille abil on võimalik erinevaid ründeid arvutisüsteemi ja -andmete vastu teostada ning mille kahjutuks tegemine võib osutuda keeruliseks.[155]

Karistusõiguse revisjonis on leitud, et esineb teatav vastuolu KarS §-s 206 ja KarS §-s 207 väljatoodud sanktsiooni vahel, mis seadusemuudatuse tulemusena võiks paremini reguleeritud olla. Hetkel ei ole normiloojal KarS § 206 ja KarS § 207 omavaheline suhestumine läbi mõeldud, sest mõlemad sätted näevad karistusena ette lõikes 1 toimepandud teo eest rahalise karistuse või kuni 3-aastase vangistuse. Siinkohal tekib küsimus, kuidas saavad sanktsioonid nendes sätetes olla ühesugused, kui toimepandavad teod on erineva raskusega. KarS § 207 on suuresti KarS § 206 kvalifikatsioon. Suures osas on nendes paragrahvides sätestatud teod kattuvad. Käesolev redaktsioon on ebaloogiline, sest kui kurjategija põhjustab arvutiandmete kustutamisega arvutisüsteemi toimimise takistamise, siis hetkel kehtiva redaktsiooni kohaselt ei ole kohtul vaja tõendada, et süsteemi tööd on reaalselt häiritud või takistatud. Karistuse määramiseks piisab andmetesse sekkumise tõendamisest, sest nii KarS § 206 lg-s 1 kui ka KarS § 207 lg-s 1 kohaldatav sanktsioon on ühesugune. On küsitav, kas seadusandja on üldse normide loomisel teostanud nende süvaanalüüsi. Seetõttu on tehtud ettepanek sanktsiooni langetamiseks KarS § 206 lg-s 1 või tõstmiseks KarS § 207 lg-s 1. Töö autori arvates on see igati põhjendatud ning käesolevas lõigus oleva näite korral rakenduks kustutamisega toime pandud kuriteo eest kuni 2-aastane vangistus ning juhul, kui nende andmete kustutamisega on takistatud arvutisüsteemi tööd, kohalduks kuni 4-aastane vangistus. Ebaloogilisuse lahendaks seaduses see, kui KarS § 206 lg-s 1 väljatoodud sanktsiooni langetataks kuni 2-aastase vangistusele. Selle muudatuse tulemusena vastuolulisus seaduses kaoks ning sanktsiooni KarS § 207 lg-s 1 muuta ei oleks vaja.[156]

[154] E. Tikk-Ringas (viide 34), lk 282.
[155] Samas.
[156] Justiitsministeerium (viide 130), lk 27.

2.3 Nuhkvara, pahavara ja arvutiviiruse levitamine

2.3.1 Sissejuhatavad märkused

Kui enne 2008. aasta seadusemuudatust oli KarS § 208 eesmärgiks reguleerida arvutiviiruse levitamist, siis seadusemuudatuse järel lisati vastutus ka nuhkvara (*spyware*) või pahavara (*malware*) levitamise eest. Lisaks koosseisu laiendamisele karmistati KarS § 208 sanktsioone. Selle tulemusena sätestati normi lõikega 1 maksimumkaristusena kuni 3-aastane vangistus, kvalifitseeritud koosseisu korral lõikega 2 kuni 5-aastane vangistus. Seadusemuudatuse tulemusena kehtestati juriidilise isiku vastutus ning süüteo toimepanemise vahetuks objektiks olnud andmete konfiskeerimine. Arvutikuritegude toimepanemiseks loodud tarkvara ja programmid on sellised objektid, mille eesmärgiks on koguda, salvestada varjatult isiku arvutisüsteemis olevaid andmeid, mistõttu on normilooja pidanud vajalikuks reguleerida sättega ka nende andmete konfiskeerimist.[157]

Paragrahviga kaitstav õigushüve on seaduslike arvutikasutajate õiguspärane ootus arvutite takistamatuks kasutamiseks.[158]

§ 208. Nuhkvara, pahavara ja arvutiviiruse levitamine
(1) Nuhkvara, pahavara või arvutiviiruse levitamise eest – karistatakse rahalise karistuse või kuni kolmeaastase vangistusega.
(2) Sama teo eest, kui see on toime pandud:
1) vähemalt teist korda või
2) kui sellega on tekitatud oluline kahju, – karistatakse rahalise karistuse või kuni viieaastase vangistusega.
(3) Käesoleva paragrahvi lõikes 1 või 2 sätestatud teo eest, kui selle on toime pannud juriidiline isik, – karistatakse rahalise karistusega.
(4) Kohus võib kohaldada käesolevas paragrahvis sätestatud süüteo toimepanemise vahetuks objektiks olnud eseme konfiskeerimist vastavalt käesoleva seadustiku §-s 83 sätestatule.[159]

2.3.2 Teoobjekt ja koosseisutegu

Käesolevas paragrahvis on teoobjektiks nii arvutiandmed kui arvutisüsteem, mida nuhkvara, pahavara või arvutiviiruse levitamisega soovitakse kahjustada. Arvutiandmete ja arvutisüsteemi mõiste sisu on käesolevas töös juba analüüsitud, kuid mida kujutavad endast nuhkvara, pahavara ja arvutiviirus, mille levitamise tulemusena võivad arvutiandmed või

[157] Justiitsministeerium (viide 43).
[158] Karistusseadustik. Komm vln § 208 komm 1.1.
[159] Karistusseadustik (viide 13).

-süsteem kahjustada saada.

Nuhkvara all peetakse silmas programmi, mis kasutaja teadmata kogub arvutisüsteemist mitmesugust informatsiooni. Selline kuritegeliku eesmärgiga loodud tarkvara võib koguda informatsiooni isikute arvutisüsteemides olevate programmide ja failide kohta, jälgida teostatud toiminguid, salvestada infot külastatud veebilehtede kohta. Lisaks sellele võib nuhkvara automaatselt paigaldada uusi programme või nende lisasid ja muuta olemasolevate programmide seadistusi või suunata ümber veebilehti. Samuti on võimalik, et kogutud andmed edastatakse programmis määratud aadressile, mille tulemusena võivad need kättesaadavaks saada kolmandatele isikutele.[160]

Pahavaraks on programm, mis arvutikasutaja teadmata muudab arvutisüsteemi tarkvaras seadistusi või kahjustab muul viisil arvutisüsteemi. Siia alla kuuluvad ka programmid, mis koguvad arvutisüsteemist informatsiooni klaviatuurivajutuste kohta. Samuti on pahavaraks programmid, mille abil saab kolmas isik kontrolli arvutisüsteemi üle nii, et kasutajal endal puudub selle kohta teave. [161] Pahavara laiemas ja tavakasutuses hõlmab endas ka arvutiviiruseid ja nuhkvara.[162]

Arvutiviirus on kahjulik arvutiprogramm, mis on võimeline end oma algsel või modifitseeritud kujul ise või teiste arvutiprogrammide abil arvutivõrgu kaudu edasi levitama ning häirima arvutite kasutamist (muu hulgas muutes või kustutades arvutis olevaid andmeid või programme, kasutades ära arvuti ressursse andmete säilitamiseks, edastamiseks, töötlemiseks jne).[163]

Konventsioon, raamotsus ning direktiiv nuhkvara, pahavara ja arvutiviiruse levitamist eraldi artiklina välja ei toogi, sest sellise tegevuse kriminaliseerimise näevad ette juba teised artiklid. Näiteks reguleerivad konventsiooni art-d 4, 5, 6 arvutiviiruse levitamist, mida pannakse toime arvutiandmetesse sekkumise, süsteemi sekkumise või seadmete kuritarvitamise eesmärgil. Arvutiviirus on suunatud arvutiandmete või -süsteemi vastu, mille vastased teod on kriminaliseeritud raamotsuse art-ga 2, 3, 4 ning selle asemel kehtima hakanud direktiivi art-ga 3, 4, 5.

Koosseisupärane tegu käesolevas sättes on levitamine ning koosseis realiseerub, kui eelpool nimetatud programm on edastatud vähemalt ühte arvutisse, mille valdaja ei ole selleks

[160] Justiitsministeerium (viide 43).
[161] Samas.
[162] Karistusseadustik. Komm vln § 208 komm 2.4.
[163] Karistusseadustik. Komm vln § 208 komm 2.3.

nõusolekut andnud.[164] Levitamine käesolevas sättes tähendab edastamist, mille tõttu võidakse näiteks pahavara abil kahjustada teise isiku arvutiandmeid või arvutisüsteemi. Levitamine kujutab endast ka vastavate programmide müümist, mille tõttu võimaldatakse kolmandatel isikutel teostada seadusevastaseid ründeid. Selliste programmide müümise korral võib esile kerkida küsimus vastutuse kohaldamiseks arvutikuriteo ettevalmistamist reguleeriva sätte järgi. Levitamise korral on probleemiks vastutuse küsimus, sest kes on vastutavaks siis, kui arvutisüsteem ise levitab arvutiomaniku teadmata viirust, pahavara või nuhkvara.

Kui näiteks KarS § 206 eeldab aktiivset sekkumist arvutiandmetesse, siis KarS § 208 eripära seisneb selles, et nuhkvara, pahavara või arvutiviiruse levitamise puhul ei ole tegemist aktiivse sekkumisega andmetesse, sest toimepanija ei muuda ise teises arvutisüsteemis andmeid ega paigalda sinna uut programmi, vaid seda teeb tarkvara ise, mis ennast iseeneslikult paljundab ja levitab.[165] Seejuures ei ole välistatud, et arvutisüsteemi seaduslik kasutaja võib selle ise pahaaimamatult installeerida.[166]

On küsitav, miks on Eesti normilooja pidanud vajalikuks luua eraldi paragrahv nuhkvara, pahavara ja arvutiviiruse levitamise reguleerimiseks, sest koosseisupärane tegu on käesoleva redaktsiooni kohaselt juba teiste normidega kriminaliseeritud. Seda enam, et KarS § 208 puhul ei ole selge, kas norm kriminaliseerib aktiveerimata pahavara levitamise, et programmi saanud isik selle hiljem käiku saaks lasta (isik, kellele tarkvara levitatakse, soovib seda) või kriminaliseeritakse sellega teiste arvutite nakatamine (isik, kellele tarkvara levitatakse, ei tea sellest midagi ega soovi seda).[167] Käesoleva sättes on seega kaks võimalikku grammatilist tõlgendusviisi, mis sätte ebavajalikkust põhjendavad. Kui silmas on peetud ettevalmistamist, siis ei ole KarS § 208 vaja, sest ettevalmistamist reguleerib KarS § 216[1]. Kui silmas on peetud hilisemaid arvutikuritegusid, siis nende puhul määratakse sanktsioon KarS §-de 206, 207 või 217 alusel. Seejuures ei ole oluline, et viirusega arvutiandmeid hävitav inimene ei tea, kelle arvutiandmeid ta hävitab, sest näiteks KarS § 206 kohaldumiseks piisab sellest, et teo toimepanija vähemalt kaudse tahtlusega möönab, et mingisugused arvutiandmed tema tegevuse tulemusena võivad hävida. Samuti ei ole oluline koht, kus need andmed hävivad, kas Eestis, Saksamaal või mujal.[168]

Sellest tulenevalt on karistusõiguse revisjoniga plaanis KarS § 208 seadusest kustutada, sest õigushüve, mida käesoleva paragrahviga kaitsta soovitakse, on juba kaitstud teiste

[164] Karistusseadustik. Komm vln § 208 komm 2.5.
[165] Karistusseadustik. Komm vln § 208 komm 4.
[166] Samas.
[167] Justiitsministeerium (viide 84), lk 61.
[168] Samas.

arvutikuritegusid reguleerivate sätetega. Regulatsiooni ei ole vaja eraldi sätet, mis kõneleks üksnes ühest kahjustamismoodusest (nt pahavara abil). Sätete eesmärk on reguleerida kindlaid olukordi, mille toimepanemisele peaks järgnema vastutus, mitte nimetata viise, kuidas seda on võimalik teostada.

Antud sättes on problemaatiline ka selle tagurlik sõnastus. Seadusandja on sättes välja toonud kindla loetelu kahjustamisviisidest, mille levitamise korral sanktsioon järgneb, ent ammendava loetelu kasutamise korral võib tekkida olukord, kus ühiskonna kiire tehnoloogilise arengu tõttu jääb norm „ajale jalgu“, mistõttu võib kurjategija karistusest sootuks pääseda. Normides tuleb kasutada neutraalset sõnavara, mida pooldab ka konventsiooni seletuskiri.[169] Sätete sõnavara peab olema piisavalt paindlik, et arvestada ka tulevasi ründeid, mida paragrahv reguleeriks.[170] KarS § 208 oma konkreetselt väljatoodud mõiste loeteluga sellest põhimõttest lähtunud ei ole.

KarS § 208 sooviti karistusseadustikust kustutada juba 2008. aasta seadusemuudatusega, kuid Riigiprokuratuuri põhjendatud märkus normi tühistamiseks lükati tagasi, sest leiti, et „KarS §-s 208 sätestatud käitumine erineb oluliselt §-des 206, 207 ja 216¹ sätestatud tegevusest. Kui viimaste puhul on isiku tahe suunatud konkreetse arvutisüsteemi töö või konkreetses arvutisüsteemis sisalduvate andmete kahjustamisele, siis arvutiviiruse levitamise puhul ei pruugi olla kuriteo objektiks konkreetne arvutisüsteem. Arvutiviiruse puhul käivitab selle ning põhjustab tahtmatult tagajärje kolmas isik. Levitades arvutiviirust, mis ennast ise reprodutseerib, puudub isikul kontroll selle edasiste tegevuste üle“.[171] On arusaamatu, miks seadusandja viitab vaid KarS §-dele 206 ja 207 – § 216¹, mitte aga §-le 217 ning mida tähendab väide, et „arvutiviiruse levitamise puhul ei pruugi olla kuriteo objektiks konkreetne arvutisüsteem“. Kui kurjategija möönab, et tema poolt lahti lastud programm hävitab kellegi arvutis andmeid (§ 206), takistab kellegi arvutisüsteemi toimimist (§ 207) või võimaldab juurdepääsu kellegi arvutisüsteemile (§ 217) on täidetud nii §-de 206, 207 ja 217 kui ka § 208 koosseis. Riigiprokuratuuri põhjendatud märkuse tagasilükkamine ei ole õigustatud, sest teiste arvutikuritegusid reguleerivate sätetega oli arvutiviiruse levitamine kaetud juba siis, mistõttu tulnuks säte seadusest kustutada 2008. aasta seadusemuudatusega.

[169] Council of Europe (viide 86), p 36.
[170] R. W. Downing (viide 4), p 730.
[171] Justiitsministeerium (viide 130), lk 30.

2.4 Arvutisüsteemi ebaseaduslik kasutamine

2.4.1 Sissejuhatavad märkused

Karistusseadustiku 2008. aasta redaktsiooniga muudeti KarS §-i 217, mis käsitleb arvutisüsteemi ebaseaduslikku kasutamist. Selle tulemusena asendati „kasutamine“ normis sõnadega „juurdepääsemine“. Seadusemuudatuse tulemusena lisati kuriteo kvalifitseeritud koosseisulise tunnusena paragrahvi lõikesse 2 punkt 3, mis sätestab elutähtsa valdkonna arvutisüsteemi ebaseadusliku kasutamise. Juriidilise isiku vastutus lisati lõikega 3.[172]

Euroopa Nõukogu „Soovitusega nr (89) 9“ leiti, et riikidel tuleks lisaks turvameetmete tõhustamisele kriminaliseerida ebaseaduslik juurdepääs arvutisüsteemile või võrgule, sest kardeti, et selliste kuritegude toimepanemiste arv võib tulevikus tõusta.[173]

Käesoleva paragrahviga kaitstav õigushüve on arvutisüsteemi omaniku huvi selle takistamatuks kasutamiseks[174] ning arvutisüsteemis olevate andmete salajas hoidmine.[175] Koosseisutüübilt on tegemist formaalse ja spetsiifilise teokirjeldusega kuriteokoosseisuga.[176] Kood, salasõna või muu kaitsevahend paigaldatakse oma vara kaitsmiseks.

§ 217. Arvutisüsteemi ebaseaduslik kasutamine
(1) Arvutisüsteemile ebaseadusliku juurdepääsu eest koodi, salasõna või muu kaitsevahendi kõrvaldamise või vältimise teel – karistatakse rahalise karistuse või kuni kolmeaastase vangistusega.
(2) Sama teo eest:
1) kui sellega on tekitatud oluline kahju või
2) kui on kasutatud riigisaladust, salastatud välisteavet või ainult ametialaseks kasutamiseks ettenähtud andmeid sisaldavat arvutisüsteemi või
3) kui on juurde pääsetud elutähtsa valdkonna arvutisüsteemile, – karistatakse rahalise karistuse või kuni viieaastase vangistusega.
(3) Käesoleva paragrahvi lõikes 1 või 2 sätestatud teo eest, kui selle on toime pannud juriidiline isik, – karistatakse rahalise karistusega.[177]

Konventsioonis reguleerib ebaseaduslikku süsteemi või selle osasse sisenemist artikkel 2, mille kohaselt võtab konventsiooniosaline seadusandlikke ja muid meetmeid, et oma seaduses

[172] Justiitsministeerium (viide 43).
[173] A. Bequai (viide 76), p 50.
[174] Karistusseadustik. Komm vln § 217 komm 1.1.
[175] E. Hirsnik (viide 88), lk 28.
[176] Karistusseadustik. Komm vln § 217 komm 1.2.
[177] Karistusseadustik (viide 13).

määratleda kuriteona sisenemine arvutisüsteemi või selle osasse, mis pannakse toime tahtlikult ja õigusliku aluseta.[178] Ebaseadusliku sissetungimise tulemusena võidakse saada juurdepääs konfidentsiaalsetele andmetele, mis võivad olla kättesaadavad ka juhul, kui juurdepääs saadakse vaid mingile süsteemi osale.[179]

Raamotsuses reguleerib ebaseaduslikku sisenemist infosüsteemi art 2 ning seda asendavas direktiivis art 3, mille kohaselt võtab liikmesriik vajalikud meetmed, et kriminaliseerida vähemalt raskemate juhtumite puhul tahtlikult ja õigusliku aluseta sisenemine infosüsteemi või selle osasse, kui sisenemisega rikutakse mõnda turvameedet.[180]

2.4.2 Teoobjekt

Käesolevas paragrahvis on teoobjektiks arvutisüsteem, millele ebaseaduslikku juurdepääsu ja kasutamist normiga kaitstakse. Arvutisüsteemi mõistet ja sisu on käesolevas töös juba käsitletud. Järgnevalt uuritakse, mida kujutavad endast kood, salasõna või muu kaitsevahend, mille kõrvaldamise või vältimise teel saab arvutisüsteemi ebaseaduslikult kasutada.

Kood ja salasõna tähistavad käesolevas paragrahvis andmeid, mida on vaja kasutaja kasutusõiguse tuvastamiseks, seega andmeid, mida peaks teadma ainult kasutusõigusega isik.[181] Kood või salasõna on tõke, mille isik peab kõrvaldama, et saada ligipääs kas arvutile, arvutisüsteemile või -võrgule.[182] Karistusseadustiku kommentaaride kohaselt on vaieldav, kas karistatav on ainult koodiga (salasõnaga) kaitstud arvutisse, arvutisüsteemi või -võrku sisenemine juhul, kui selline kood (salasõna) on murtud selleks kasutatava programmi abil, või on karistatav ka selline arvutisüsteemi kasutamine koodi (salasõna) sattumise tõttu isiku kätte, kellele seda õiguspäraselt ei ole antud.[183] Selline lähenemine ei ole õige, sest kuidas saab väita, et karistatav on vaid salasõna „lahtihäkkimise“ abil sisemine. Oluline ei ole, mil viisil salasõna kõrvaldatakse või välditakse, sest ka „väljanuhitud“ salasõna sisestamise abil arvutisüsteemile juurdepääsu hankimine on karistatav.

Muu kaitsevahend võib olla igasugune muu tark- ja riistvaraline lahendus, mis on kasutatav kasutusõiguse tuvastamiseks (nt sõrmejälje, hääle või silma võrkkesta järgi isiku tuvastamine). Kaitsevahendite alla saab liigitada ka erinevad tarkvaralised vahendid, nagu

[178] Euroopa Nõukogu Arvutikuritegevusvastane konventsioon (viide 14).
[179] Council of Europe (viide 86), p 44.
[180] Euroopa Parlamendi ja Nõukogu direktiiv (viide 16).
[181] Karistusseadustik. Komm vln § 217 komm 4.2.
[182] T. Ploom. Arvutikuritegude kvalifitseerimine. – Juridica, 2003, nr 8, lk 577.
[183] Karistusseadustik. Komm vln § 217 komm 4.2.

näiteks tulemüür e *firewall*. See on programm, mille eesmärgiks on ära hoida seda, et võrgu kaudu ei siseneks arvutisüsteemi keegi teine. Kaitsevahendiks on ka nuhkvaratõrje ning viirusetõrje.

Formuleeringut „koodi, salasõna või muu kaitsevahendi“ ei saa normis pidada kuigi õnnestunuks, sest ei selgu, mis eristab „koodi“ „salasõnast“ – tegemist on sünonüümidega. Seesugune näitlikustav loetelu võib olla eksitav, sest jääb mulje, nagu peaks kaitsevahend olema tingimata tarkvaraline. Isik võib kaitsta oma arvutisüsteemi ka füüsiliselt (seifi sulgedes, ukse lukustades). [184] Konventsiooni seletuskirjas on normiloojatele seatud eesmärgiks kasutada neutraalset sõnavara, mitte tuua normides välja kindlaid loetelusid. Karistusseadustiku seadusemuudatusega soovitakse asendada formuleering „koodi, salasõna või muu kaitsevahendi“ sõnaga „kaitsevahendi“. See on õigustatud, sest kood ja salasõna ongi kaitsevahendid ning nende eraldi väljatoomine normis ei ole vajalik.

Eesti kohtupraktika on tõkke või lukustuse kõrvaldamist tõlgendanud laialt ning lugenud ka lukustamata sahtlist võtme võtmist tõkke kõrvaldamiseks [185] ning seega on käesolevas paragrahvis koosseisutunnuseks oleva kaitsevahendi kõrvaldamise küllaltki lai tõlgendamine.[186] Käesoleva töö autori arvates ei saa laia tõlgendamist pidada põhjendatuks, sest õigustatu peab ise midagi ette võtma, järgima vähemalt minimaalseid hoolsusstandardeid, et tema vara oleks karistusõiguslikult kaitstud. Näiteks peab ta lukustama töölt lahkudes ukse või panema kasutatavale arvutile salasõna, et selles olev informatsioon ei oleks kättesaadav kolmandatele isikutele. Väga lai tõlgendamine võib tuua kaasa ülekriminaliseerimise, sest arvutisüsteemi ebaseaduslik kasutamine ehk sellele juurdepääsu hankimine peab aset leidma kaitsevahendi kõrvaldamise teel.

Analüüsides KarS §-s 217 väljatoodud vahendeid juurdepääsu tõkestamiseks, jääb arusaamatuks, kas selle sätte all on silmas peetud ka füüsilisi kaitsevahendeid. Ilmselt küll, sest Riigikohus on tõkke kõrvaldamist tõlgendanud laialt, pidades selle all silmas ka füüsilisi kaitsevahendeid, milleks võivad olla suletud ruumid, kapid, riistvarale vahetult paigaldatud plommid, biomeetrilised kaitsevahendid jne.[187]

Sellisel juhul võib esile kerkida kaitsevahendi kvaliteedi küsimus, sest mõlemad äärmused tuleb välistada. Ei saa nõuda, et isik kasutaks kaitsevahendit, mis igasuguse juurdepääsu välistab, sest 100% turvalist vahendit ei ole olemas. Samas ei saa väita, et kaitsevahendiks on

[184] Justiitsministeerium (viide 130), lk 26.
[185] Karistusseadustik. Komm vln § 266 komm 3.7.1
[186] Karistusseadustik. Komm vln § 217 komm 4.3.
[187] E. Hirsnik (viide 88), lk 8.

täiesti marginaalset kaitset pakkuv või üksnes keelufunktsiooni kandev vahend. Kaitsevahendiks ei ole hoiatussilt, et arvutit ei tohi kasutada või suletud uks, mis ei ole lukustatud jne.[188] Vahendi kvaliteedi hindamisel on küsitav, kas iga suvaline parool on kaitsevahend või liiga lihtsad paroolid seda ei ole. Töö autori arvates ei saa liiga kerge kombinatsioon salasõna näol olla kaitsevahend, sest kui parooliks pannakse enda nimi või numbrikombinatsioon „1,2,3,4,5,6“, siis tuleb tõdeda, et neid on kerge ära arvata ning kaitsmise eesmärki sellise parooliga tagada ei saa. Tegemist on igakordse hindamise küsimusega. Lähtuma peaks sellest, et kaitsevahend on selline meetod, mis on objektiivselt sobiv ja subjektiivselt õigustatud isiku tahte kohaselt seatud selleks, et vältida teiste isikute poolset juurdepääsu hankimist arvutisüsteemile või seda vähemalt raskendada.[189]

Käesoleva sättega kriminaliseeritakse lisaks elutähtsa valdkonna arvutisüsteemi ebaseadusliku kasutamisele ka riigisaladust, salastatud välisteavet või ainult ametialaseks kasutamiseks ettenähtud andmeid sisaldava arvutisüsteemi kasutamist. Elutähtsa valdkonna arvutisüsteemi on käesolevas töös eelnevalt käsitletud. Riigisaladus on aga riigisaladuse ja salastatud välisteabe seaduse[190] (edaspidi RSVS) § 3 p 1 kohaselt Eesti Vabariigi julgeoleku või välissuhtlemise tagamise huvides avalikuks tuleku eest kaitset vajav üksnes käesolevas seaduses ja selle alusel antud õigusaktides sätestatud tunnustele vastav teave. Salastatud teave on RSVS § 3 p 2 kohaselt välisriigi, EL-I, NATO (*North Atlantic Treaty Organisation*) või mõne muu rahvusvahelise organisatsiooni või rahvusvahelise kokkuleppega loodud institutsiooni poolt salastatud ja Eestile avaldatud teave ning Eesti Vabariigi poolt välislepingu täitmiseks loodud teave, mis tuleb salastada välislepingu kohaselt. „Ametialaseks kasutamiseks ettenähtud andmed on avaliku teabe seaduse[191] §-de 34 ja 35 alusel asutusesiseseks kasutamiseks mõeldud teabeks tunnistatud andmed“.[192]

KarS § 217 kohaselt on karistatav arvutisüsteemi ebaseaduslik kasutamine, aga normiga on jäetud reguleerimata arvutisüsteemi osa ebaseaduslik kasutamine, nagu see on sätestatud konventsiooni art-s 2 ja direktiivi art-s 3. Teoobjektiks ei pea olema kogu arvutisüsteem, vaid selleks võib olla ka arvutisüsteemi osa. Rahvusvahelised normiloojad on soovinud kriminaliseerida ka olukorda, kus arvutisüsteemi õiguspärane kasutaja hangib endale juurdepääsu arvutisüsteemi sellistesse osadesse, milleks tal puudub luba.[193] KarS §-ga 217 ei ole reguleeritud olukorrad, kus näiteks töötaja ületab oma volituste piire ning kasutab või

[188] E. Hirsnik (viide 88), lk 9.
[189] Samas.
[190] Riigisaladuse ja salatatud välisteabe seadus. – RT I 2007, 16, 77.
[191] Avaliku teabe seadus. – RT I 2000, 92, 597.
[192] Karistusseadustik. Komm vln §217 komm 6.
[193] Justiitsministeerium (viide 130), lk 26.

hangib juurdepääsu arvutisüsteemi osale. Kuna norm arvutisüsteemi osale ebaseaduslikku juurdepääsu hankimist, ei reguleeri, siis KarS § 217 lg 1 käesoleva redaktsiooni kohaselt kriminaalvastutus sellisele toimepandud teole ei järgne. Arvutikuritegevuse alased uuringud USA-s (*United States of America)* on näidanud, et ligi 65% avastatud rikkumistest on sellised, kus ebaseaduslik juurdepääs arvutisüsteemile on saadud tööülesannete täitmiseks ettenähtud volituspiire ületades. Regulatsioon peaks tagama õigusliku kaitse ka nendes olukordades, kus ebaseaduslik juurdepääs hangitakse süsteemi osale.[194]

2.4.3 Koosseisutegu

KarS § 217 alusel on karistatav arvutisüsteemi ebaseaduslik kasutamine koodi, salasõna või muu kaitsevahendi kõrvaldamise teel.[195] Koosseis on täidetud, kui isik saab endale koodi teadmisega, et sellega pääseb ta võõrasse arvutisse ning mõistab, et selline tegevus rikub teise isiku õigusi, kuna kood või salasõna paigaldati omaniku poolt selleks, et kaitsta oma vara ja takistada teiste isikute juurdepääsu varale.[196] Objektiivne koosseis on arvutisüsteemile ebaseadusliku juurdepääsu saamine, mis võib seisneda andmete või programmide edastamises, töötlemises või säilitamises antud arvutisüsteemis.[197] Lõpule on tegu viidud hetkest, kui sissetungija saab pärast kaitsevahendi kõrvaldamist või selle vältimist esimesed andmed sissemurtud arvutisüsteemist, sisestab sinna uusi andmeid või käivitab selles mõne programmi.[198]

Subjektiivsest küljest eeldatakse tahtlust koosseisu kõikide asjaolude suhtes ning koosseis on realiseeritud, kui isik on tegutsenud vähemalt kaudse tahtlusega.[199]

Koosseisupärane tegu on juurdepääsu hankimine, mis on saadud koodi, salasõna või muu kaitsevahendi kõrvaldamise või vältimise teel, kuigi sätte peakiri viitab arvutisüsteemi ebaseaduslikule kasutamisele. Juurdepääsu hankimine kujutab endast olukorra loomist, kus isikul on võimalik arvutisüsteemi selle sihipärasel moel rakendada/kasutada kas aktiivselt, ise andmetöötlust teostades, või passiivselt, kasutades selleks juba teostatud andmetöötluse tulemusi.[200] Tegemist peab olema sellise juurdepääsuga, mis on ebaseaduslik ehk milleks puudub kasutajal luba. Luba võib olla kirjalik, suuline või konkludentne. Kõiki arvutivõrku

[194] R. W. Downing (viide 4), p 721-722.
[195] T. Ploom (viide 182), lk 577.
[196] Samas.
[197] Karistusseadustik. Komm vln § 217 komm 2.
[198] Karistusseadustik. Komm vln § 217 komm 4.1.
[199] Karistusseadustik. Komm vln § 217 komm 5.
[200] E. Hirsnik (viide 88), lk 6.

ühendatud arvutisüsteeme loetakse selle võrgu õiguspärastele kasutajatele kasutamiseks lubatuks, kui ei ilmne kasutamispiiranguid, mille seadmine võib avalduda salasõnade või mõne muu kaitsevahendi rakendamises, aga ka selgelt väljendatud kasutamise keelus.[201] KarS § 217 kohaldub seega siis, kui juurdepääs on saadud koodi, salasõna või muu kaitsevahendi kõrvaldamise või vältimise teel.

Mitmetes riikides oli varasemalt karistatav ainult arvutisüsteemi ebaseaduslik kasutamine, mitte sellele ebaseadusliku juurdepääsu hankimine. Kuna häkkerid hakkasid ründed arvutisüsteemi vastu teostama rahateenimise eesmärgil, süsteemi testimise kõrval, siis leidsid konventsiooni ja raamotsuse koostajad, et karistuslävi tuleb tuua ettepoole ning kriminaliseerida ka ebaseaduslik juurdepääsu hankimine.[202] Vastav muudatus sooviti normi sisse viia karistusseadustiku 2008. aasta seadusemuudatusega, ent seda ei tehtud kuigi korrektselt. Sättes esineb probleem sõnaga „kasutama“ – seda nii normi pealkirjas kui lõike 2 punktis 2. Pealkirja eesmärgiks on anda edasi paragrahvi sisu, mistõttu oleks õigem kasutada „arvutisüsteemile ebaseadusliku juurdepääsu hankimine“. „Juurdepääsu hankimist“ ja „kasutamist“ ei saa omavahel samastada, sest KarS § 217 lg 2 p-s 2 tähistab sõna „kasutama“ endast selget teokirjeldust, kuid juurdepääsu hankimine ei saa olla kasutamine, sest viimane eeldab mingi andmetöötlusprotsessi algatamist.[203] KarS § 217 lg 2 p 2 puhul ei ole tegemist KarS § 217 lg 1 kvalifikatsiooniga, sest kui sätte lõige 1 näeb ette karistuse „juurdepääsu hankimise eest“, siis sätte lõike 2 punkt 2 kõneleb „kasutamisest“, mistõttu on seesugune normitehniline ja õigusdogmaatiline ebatäpsus normis taunitav. Teokirjeldus lõikes 2 ei või erineda lõikes 1 sätestatust. Lahendus oleks see, kui asendada sõnad „on kasutatud“ sõnadega „juurdepääs on hangitud“ või kustutada punkt 2 sättest.[204]

KarS § 217 lg 2 p-ga 1 on sätestatud koosseisupärase teoga põhjustatud olulise kahju tekkimine. Käesolev punkt tuleks seadusest kustutada, sest tegemist on ülimalt harva rakendatava sättega, mille eemaldamise poolt kõneleb ka asjaolu, et arvutikuritegevus ei ole alati suunatud ainult vara vastu. Arvutikuritegudest kõneledes mainitakse tihti suuri kahjusid, mis erinevate toimepandud tegudega võivad kaasneda, kuid nende kahjude tõendamise tõenäosus on küsitav. Käesoleva sätte kohaldumiseks peab kahju olema tekkinud juba juurdepääsu hankimisega ning seetõttu on selle kvalifikatsiooni vajalikkus normis küsitav.[205]

Karistusseadustiku seadusemuudatusega muudetakse KarS § 217 lg 2 p 3, mida põhjendatakse

[201] Karistusseadustik. Komm vln §217 komm 3.
[202] A. Bequai (viide 76), p 50.
[203] E. Hirsnik (viide 88), lk 5-6.
[204] Justiitsministeerium (viide 130), lk 26.
[205] Samas.

sellega, et norm peab lähtuma ühtsest keelekasutusest. Kui eelnevalt räägitakse „juurdepääsu hankimisest“, ei ole põhjust kõneleda KarS § 217 lg 2 p-s 3 „juurde pääsemisest“.[206]

[206] Justiitsministeerium (viide 84) , lk 65.

2.5 Arvutikuriteo ettevalmistamine

2.5.1 Sissejuhatavad märkused

KarS § 216¹, mis reguleerib arvutikuriteo ettevalmistamist, lisati karistusseadustikku 2008. aasta seadusemuudatusega. Arvutikuritegudega võidakse põhjustada olulist kahju, mistõttu peeti vajalikuks kriminaliseerida selliste tegude ettevalmistamine, mida varasemalt reguleeritud ei olnud. Arvutikuriteo ettevalmistamise staadiumis võib isik koguda andmeid või valmistada programme, et neid hiljem kuritegude toimepanemiseks kasutada. [207] Lisandunud sätte eesmärk on kriminaliseerida ettevalmistavaid tegusid, mis on sätestatud KarS §-s 206 (arvutiandmetesse sekkumine), KarS §-s 207 (arvutisüsteemi toimimise takistamine), KarS §-s 208 (arvutiviiruse levitamine), KarS §-s 213 (arvutikelmus), KarS §-s 217 (arvutisüsteemi ebaseaduslik kasutamine).[208] Käesoleva paragrahvi lõikega 2 nähti ette juriidilise isiku vastutus ning lõikega 3 sätestati võimalus süüteo toimepanemise vahetuks objektiks olnud eseme konfiskeerimine.

Rahvusvahelised normiloojad on leidnud, et arvutikuritegevus on selline valdkond, mille puhul on põhjendatud ettevalmistustegevuse kriminaliseerimine, sest Interneti laialdased võimalused aitavad kergesti hankida erinevaid programme ning koode, millega arvutikuritegusid sooritada. Tulenevalt konventsioonist peeti vajalikuks lisada arvutikuritegude ettevalmistamist reguleeriv säte ka karistusseadustikku.

Antud sättega kaitstakse arvutisüsteemi omaniku või õiguspärase kasutaja huvi arvutiandmete või arvutisüsteemi takistamatuks kasutamiseks. Sättega kaitstakse samasid hüvesid, mida kaitsevad kahjustusdeliktid (KarS §-d 206, 207, 208, 213, 217). Käesoleva töö autor ei nõustu karistusseadustiku kommentaarides väljatoodud mõttega, et „kaitstava õigushüve rikkumise korral on arvutisüsteemi omanikul võimalus saada nende objektide teiste isikute poolt kasutamise eest hüvitust[209]“, sest sättega ei kaitsta vaid varalisi õigusi, vaid ka teisi õigusi, mida arvutikuritegude toimepanemisega võidakse rikkuda. Koosseisutüübilt on tegemist formaalse deliktiga.[210]

[207] Justiitsministeerium (viide 43).
[208] Samas.
[209] Karistusseadustik. Komm vln § 216¹ komm 1.1.
[210] Karistusseadustik. Komm vln § 216¹ komm 1.2.

§ 216[1]. Arvutikuriteo ettevalmistamine
(1) Käesoleva seadustiku §-s 206, 207, 208, 213 või 217 sätestatud kuritegude toimepanemise eesmärgil selleks vastavalt kavandatud või kohandatud seadme, programmi, ka salasõna, kaitsekoodi või muude arvutisüsteemile juurdepääsuks vajalike andmete valmistamise, valdamise, levitamise või muul viisil kättesaadavaks tegemise eest, samuti muude käesolevas paragrahvis nimetatud kuritegude toimepanemiseks vajalike andmete kasutamise, levitamise või muul viisil kättesaadavaks tegemise eest – karistatakse rahalise karistuse või kuni kolmeaastase vangistusega.
(2) Sama teo eest, kui selle on toime pannud juriidiline isik, – karistatakse rahalise karistusega.
(3) Kohus võib kohaldada käesolevas paragrahvis sätestatud süüteo toimepanemise vahetuks objektiks olnud eseme konfiskeerimist vastavalt käesoleva seadustiku §-s 83 sätestatule.[211]

2.5.2 Teoobjekt

KarS §-s 216¹ on kahte liiki teoobjekte: esiteks on nendeks seadmed või arvutiprogramm, mis on loodud või kohandatud KarS §-de 206, 207, 208, 217 sätestatud kuritegude toimepanemiseks; teiseks kaitsevahendid, mille abil on võimalik juurdepääs arvutisüsteemile hankida. [212] Seadme kuritarvitamist reguleerib konventsiooni art 6, milles tuuakse teoobjektidena välja vastavalt kavandatud ja kohandatud seade või arvutiprogramm, aga ka arvutiparool või juurdepääsukood või samalaadi andmed, mille abil on võimalik juurde pääseda kogu arvutisüsteemile või selle osale, et kasutada seda artiklites 2-5 nimetatud tegude toimepanemiseks. [213] Direktiivi art-s 7 on teoobjektiks arvutiprogramm, mis peab olema loodud või kohandatud eelkõige artiklites 3-6 osutatud kuritegude toimepanemiseks. Sarnaselt konventsiooniga on ka direktiivis teoobjektiks arvuti salasõna, juurdepääsukood või samalaadsed andmed, mille abil on võimalik siseneda infosüsteemi või selle osasse.[214]

Konventsiooni seletuskirja kohaselt vaidlesid normiloojad tuliselt selle üle, millised arvutiprogrammid peaksid olema kohased teoobjektid arvutikuritegude ettevalmistamise korral. [215] Normiloojad ei soovinud seda, et teoobjektideks loetaks kõikvõimalikud IT-spetsialistide igapäevased töövahendid, ent kardeti ka liiga kitsast reguleerimist, mille kohaselt oleks teoobjektiks üksnes arvutikuritegude toimepanemiseks valmistatud programm. Jõuti järeldusele, et kohaseks teoobjektiks on seesugune programm, mis peab olema loodud või kohandatud eelkõige arvutikuritegude toimepanemiseks (viirused, pahavara jms). Näiteks ei ole turvaanalüüsi teostamiseks loodud tarkvara kohane teoobjekt, kui seda kasutatakse

[211] Karistusseadustik (viide 13).
[212] Justiitsministeerium (viide 84), lk 63.
[213] Euroopa Nõukogu Arvutikuritegevusvastane konventsioon (viide 14).
[214] Euroopa Parlamendi ja Nõukogu direktiiv (viide 16).
[215] Council of Europe (viide 86), p 73.

eesmärgipäraselt, sest niisugune tarkvara võimaldab ka arvutikuritegude toimepanemist.

KarS §-s 216¹ on teoobjektina välja toodud seade, mis karistusseadustiku kommentaaride kohaselt võib olla arvutisüsteem, kuid ei pruugi.[216] Konventsiooni seletuskirja kohaselt võib seadme all silmas pidada ka füüsilisi esemeid ning seejuures ei ole vajalik, et nad paikneksid vaid arvutisüsteemis. Seega nii konventsiooni art 6 kui KarS § 216¹ kohaselt võib seadme puhul tegemist olla kehalise esemega e asjaga. Sellised vastavalt kavandatud või kohandatud füüsilised esemed on näiteks „koorimisseadmed" e *skimmer´*id, mida kasutatakse pangakaardi andmete kopeerimisel.[217] Andmete kättesaamiseks kasutatakse seadet, mis meenutab pangaautomaadi klahvistikku ning selle asetamisel õige klahvistiku peale saab salvestada PIN-koodi, mida kaardikasutaja automaati sisestab.[218] Informatsiooni kättesaamiseks võidakse kasutada väga väikest kaamerat, mis kõik klahvivajutused salvestab ning kasutatakse ka selliseid seadmeid, mis meenutavad pangaautomaadi kaardisisestuspilu, mis kinnitatakse õige pilu peale, et kaardiandmeid kopeerida.[219] Kui informatsioon on kätte saadud, kirjutatakse saadud andmed tühjale kaarditoorikule, millega hiljem raha automaadist välja võetakse. Teatud juhtudel võidakse kopeerimisseade asetada pangauksele, kujutades seda ukseavamisseadmena, kuid näiteks Euroopas ja Eestis on sellise kasutamine muutunud keeruliseks, sest puhtaid magnetribaga kaarte on alles jäänud vähe ning populaarsemad on *smartcard´*d, millel on protsessorina toimiv kiip ning seetõttu on andmete kopeerimine raskendatud.[220]

Teokohasteks programmideks on kõikvõimalikud häkkimisriistad (*hacking tools*), aga ka näiteks nuhkavara, pahavara, arvutiviirused, mida kasutatakse rünnete toimepanemiseks nii arvutisüsteemi kui selles olevate andmete vastu.[221] Konventsiooni kohaselt on „arvutiprogramm" üks „seadme" alaliik, mistõttu on küsitav selle mõiste väljatoomise vajalikkus KarS §-s 216¹.[222]

Arvutikuriteo ettevalmistamist reguleerivas normis on sätestatud ka salasõna ning kaitsekoodide levitamine ning teistele teistele isikutele kättesaadavaks tegemine, ent neid teoobjekte on juba käesoleva töös (alapunktis 2.4) käsitletud.

KarS §-s 216¹ on sätestatud ka muude nimetatud kuritegude toimepanemiseks vajalike

[216] Karistusseadustik. Komm vln § 216¹ komm 2.2.
[217] Justiitsministeerium (viide 84), lk 63.
[218] E. Hirsnik (viide 88), lk 31-32.
[219] Samas.
[220] Samas.
[221] Karistusseadustik. Komm vln § 216¹ komm 2.3.
[222] Council of Europe (viide 86), p 67.

andmete kasutamine, levitamine või muul viisil kättesaadavaks tegemine. [223] Karistusseadustiku kommentaaride kohaselt on muude andmete all mõeldud selliseid andmeid, mida läheb vaja KarS § 213 (arvutikelmuse) toimepanemiseks. Nende hulka kuuluvad näiteks teiste isikute krediitkaardiandmed või Internetipanga juurdepääsukoodid, mis võidakse andmesubjektilt kätte saada pettuse või arvutisüsteemis sisalduvatele andmetele ebaseadusliku juurdepääsu teel. [224] Ei ole mõistetav, miks ei saa Internetipanga juurdepääsukoode subsumeerida „salasõna" või „kaitsekoodi" mõiste alla või miks ei ole krediitkaardi andmed „muud arvutisüsteemile juurdepääsuks vajalikud andmed". Kommentaarides olevat viidet arvutikelmusele ei saa pidada tõeseks, sest normist nii kitsas tõlgendus välja ei tule.[225]

Seoses karistusseadustiku seadusemuudatusega soovitakse KarS § 216¹ sõnastada kitsamalt. Alus selleks tuleb nii konventsiooni art-st 6 kui ka raamotsust asendava direktiivi art-st 7 – Eesti karistusseadustik peab olema kooskõlas nendest tulenevate nõuetega. Kui vaadata konventsiooni ja direktiivi artikleid, mis arvutikuriteo ettevalmistamist reguleerivad, siis selgub, et kumbki sätetest ei tunne KarS §216¹ lg-s 1 kasutatud formuleeringut „muude käesolevas paragrahvis nimetatud kuritegude toimepanemiseks vajalike andmete kasutamise, levitamise või muul viisil kättesaadavaks tegemise eest".[226] Nimetatud alternatiiv muudab rahvusvaheliste normiloojate poolt ette võetud eesmärgid normi kitsendamiseks asjatuks, sest kui teatud objekt ei mahu esimese viie nimetatud alternatiivi alla, on tegemist „muude arvutikuritegude toimepanemiseks vajalike andmetega".[227]

KarS § 216¹ lg-s 1 olevat formuleeringut saab grammatiliselt kasutada väga laialt ning sellega võib kaasneda olukord, kus pelgalt operatsioonisüsteemi *Windows* kasutamine on karistatav, sest nimetatud süsteemi abil saab toime panna arvutikuritegusid.[228] Normi sõnastuse järgi on võimalik neid nimetatud programme pidada arvutiandmete liigiks, mille kasutamine või levitamine on kuriteona karistatav. Normilooja eesmärgiks ei ole olnud kriminaliseerida arvutisüsteemi tavaprogrammide kasutamist, mistõttu on vajalik muuta normi sõnastust, et see ei tooks kaasa ülekriminaliseerimist. Need sättes nimetatud muud vajalikud andmed võivad olla ka neutraalsed kirjeldused arvutisüsteemide, Interneti toimimise kohta, kuivõrd ilma sellise teabeta ei ole võimalik arvutikuritegusid toime panna.[229] KarS § 216¹ lg-s 1 tõusetub esile selle põhiseadusele mittevastavus, mitte üksnes määratletuspõhimõtte rikkumise tõttu,

[223] Justiitsministeerium (viide 43).
[224] Karistusseadustik. Komm vln § 216¹ komm 2.4.
[225] Justiitsministeerium (viide 130), lk 28-29.
[226] Justiitsministeerium (viide 84), lk 63.
[227] Justiitsministeerium (viide 130), lk 29.
[228] Justiitsministeerium (viide 84), lk 63.
[229] E. Hirsnik (viide 88), lk 32.

vaid ka muudel alustel. Seetõttu on tehtud ettepanek normi dispositsiooni teine osa kustutada.[230]

Käesolevat sätet analüüsides tekib küsimus, millele vastavalt peavad teoobjektid kavandatud olema – see küsimus oli ka rahvusvaheliselt kõige vaieldavam[231], sest KarS § 216¹ sõnastusest see ei selgu. Kui konventsiooni art 6 puhul räägitakse kavandamisest ja kohandamisest üksnes seoses seadmete ja arvutiprogrammidega, siis Eesti normilooja on sätte sõnastanud grammatiliselt nii, nagu „vastavalt kavandatud" peavad olema mitte üksnes „seade" ja „programm", aga ka „salasõna", „kaitsekood" ja „muud arvutisüsteemile juurdepääsuks vajalikud andmed". Seega tekitab probleemi sättes sõna "ka" kasutamine, mis sõna „salasõna" ees ei oma Eesti keeles sellist tähendust, et tal oleks loetelu „kaheks jagav funktsioon". Olukorra lahendaks see, kui norm sõnastataks ümber nii, et tegemist oleks kahe erineva koosseisupäraste objektide grupiga – ühelt poolt „vastavalt kavandatud" seadmed ja programmid, teisalt igasugused salasõnad jne.[232] Sellisel juhul oleks norm konventsiooniga kooskõlas ning ka üheselt mõistetavam.

2.5.3 Koosseisutegu

Antud sätte objektiivse külje moodustab vastavalt kavandatud või kohandatud andmete, programmide, seadmete valmistamine, kasutamine, levitamine või muul viisil kättesaadavaks tegemine, mille eesmärgiks on või mille tööpõhimõte on rünnete toimepanemine arvutisüsteemide vastu, sh ründed andmete ja arvutisüsteemi toimimise vastu.[233]

Subjektiivsest küljest eeldab antud süütegu tahtlust kõigi koosseisu asjaolude suhtes ning koosseisu realiseerumiseks peab isik olema tegutsenud vähemalt kaudse tahtlusega.[234]

Teokirjeldus on antud sättes lai, sest sisuliselt on selles hõlmatud igasugused objekti enda valdusse saamise ja teistele isikutele edastamise viisid. Regulatsiooni kohaselt on karistatav kaitsevahendi hankimine näiteks nn *phising´*ut kasutades; nt võidakse salasõna teada saada pettusliku meili teel. Kaitsevahendi hankimiseks võidakse kasutada ka nn *social emergineerig'*ut, mille puhul saadakse salasõna teada seeläbi, et helistatakse firma töötajale,

[230] Justiitsministeerium (viide 130), lk 29.
[231] Justiitsministeerium (viide 84), lk 63.
[232] Justiitsministeerium (viide 130), lk 28.
[233] Justiitsministeerium (viide 43).
[234] Karistusseadustik. Komm vln § 216¹ komm 3.

esinedes IT-eksperdina, kes „kontrollib salasõnade kvaliteeti“.[235] Käesoleva töö autor on veebikeskkonnas oleva *PayPal* maksesüsteemi aktiivne kasutaja, mistõttu on pettusliku meili saamine tuttav. Nimelt proovisid arvutikurjategijad *phising´*uga hankida *PayPal* kasutajate salasõnu, et saadud andmete abil sooritada oste veebipoodides või kanda virtuaalset raha ühelt kontolt teisele. Selleks saatsid arvutikurjategijad inimestele meile, paludes muuta oma *PayPal* süsteemis olevat salasõna. Kirjale oli lisatud link, millele abil seda „hõlpsam“ teostada oleks. Tegelikult suunati isikud selle lingi abil spetsiaalsele petuleheküljele, mis oma kujunduselt ei erinenud ametlikust koduleheküljest. *PayPal* meeskonnani jõudis info levivast petuskeemist ning seetõttu teavitati kõiki kasutajaid, et *PayPal* ei saada kunagi parooli muutmiseks kasutajale meili ega lisa linki, mis lehele pääsemist lihtsustaks. *PayPal* maksesüsteemil on käesoleva töö autori arvates väga suur miinus, mistõttu võivad ka arvutikurjategijad leida, et hangitava info abil on võimalik kuritegusid toime panna. Maksmine läbi selle süsteemi leiab aset nii, et kasutaja lisab vastavas keskkonnas kauba tasumiseks esmalt oma *PayPal* kasutajanime, milleks on isiku meiliaadress ning parooli, misjärel süsteem broneerib vajaliku summa kasutaja krediitkaardilt. Kui arvutikurjategija teab sisselogimiseks kasutatavat meiliaadressi, siis võib ta parooli teadasaamiseks kasutajale kirjutada. Need meiliaadressid on nähtavad kõikidele müüjatele, kellele kauba eest tasutakse.

Levitamine koosseisupärase teona võib kujutada endast vastavalt kavandatud või kohandatud seadmete, programmide, salasõnade jms müüki, mida hiljem arvutikuritegude toimepanemise eesmärgil saab kasutada. Kui näiteks loodud programm müüakse kolmandale isikule, kes ostetud tarkvaraga kuritegu toime panna soovib, siis kohaldub vastutus antud sätte alusel müüjale, kes programmi levitas ning ostjale, kes programmi ostmisega sai selle valdajaks. KarS § 216¹ kohaldub ka vastavalt kavandatud või kohandatud programmi valmistajale, kui ta on loonud selle kuritegude toimepanemise eesmärgil.

Kehtiva redaktsiooni kohaselt on KarS § 208 erinorm KarS § 216¹ suhtes, sest kui on tuvastatud nuhkvara, pahavara või arvutiviiruse levitamine, siis subsumeeritakse tegu erinormi järgi. Kui tarkvara ei ole veel jõutud levitada, kuid tegemist on tarkvara loomisega selle levitamise eesmärgil, siis kuulub tegevus subsumeerimisele KarS § 216¹ järgi. Samuti kohaldub KarS § 216¹, kui on tegemist tarkvara levitamisega, mida erinormis ei ole ära nimetatud ning samuti muude andmetega, mida kasutatakse arvutikuriteo toimepanemiseks.[236] Seadusemuudatuse tulemusena ei ole KarS § 208 enam erinorm KarS § 216¹ suhtes, sest nuhkvara, pahavara ja arvutiviiruse levitamist sätestav norm on plaanis kehtetuks tunnistada.

[235] Justiitsministeerium (viide 84), lk 63.
[236] Samas.

Käesolev säte toob koosseisupärase teona välja „kasutamise“, mis tekitab normis segadust, sest sätte eesmärk on reguleerida arvutikuritegevuse ettevalmistamist, kuid see teokirjeldus märgib reaalse kuriteo toimepanemist. Grammatiliselt on norm sõnastatud nii, et kuritegu on toime pandud juba arvutikuritegevuse toimepanemiseks vajalike andmete kasutamisega ning teo toimepanijal ei ole vaja, et tal oleks eesmärk selle toimepanemiseks.[237] Kurjategijad võivad juurdepääsu hankida e häkkida arvutisüsteemidesse ka vaid selleks, et koguda informatsiooni mõne teise kuriteo toimepanemiseks. Nii võidakse hankida näiteks krediitkaartide numbreid, et nende abil sooritada oste netipoodides või kanda raha soovitud kontole. Käesoleva sättega reguleeritakse aga arvutikuriteo ettevalmistamist, mistõttu vastutuse kohaldamiseks piisab andmete kogumise faktist, ei ole vaja, et neid andmeid oleks hakatud kasutama. Kui seda tehakse, siis järgneb vastutus toimepandud teo eest mõne teise sätte alusel, mis sooritatud tegu kriminaliseerib.[238] Seega ei ole mõistetav, miks on käesolevas sättes „kasutamine“ teokirjeldusena välja toodud.

KarS §-s 216¹ ei kattu normi subjektiivne koosseis objektiivse koosseisuga. Karistatav on ainult selline tegu, millega soovitakse panna hiljem ise või võimaldada näiteks kolmandal isikul panna toime KarS §-s 206, 207, 208 või 217 sätestatud kuritegu. Kui näiteks firma IT-spetsialist soovib teatava programmi allalaadimise abil testida arvutisüsteemi turvalisust, siis arvutikuritegu ta sooritanud ei ole, sest tööülesannete iseloomu tõttu ongi vajalik süsteemi testimine ning kasutamine sellisel juhul koosseisupärane tegu ei ole. Süsteemi turvalisuse testimiseks võib IT-spetsialist kasutada näiteks „trooja hobust“, mis on kasuliku programmi või andmete sisse manustatud kahjulik programmiosa, mis täidab tegelikult mingit varjatud ülesannet, näiteks muudab teatud tingimustel andmeid, rikub kõvakettal failipaigutustabeli või teeb muud kurja.[239] IT-spetsialisti eesmärgiks ei ole programmi abil kuritegude sooritamine, vaid süsteemi vigade leidmine. Olukord oleks teine, kui ta laeks „trooja hobuse“ Internetti üles, et võimaldada ka teistel spetsialistidel arvutisüsteemi testida. Sellisel juhul võib tegemist olla arvutikuriteo ettevalmistamisega KarS § 216¹ mõttes, sest programmi üleslaadimisega veebikeskkonda peab ta möönma, et selle võib alla laadida tubli süsteemiadministraatori kõrval ka kuritegelike kavatsustega isik. Siinjuures ei ole vaja, et tal oleks kavatsus kuritegu toime panna, sest vastutuse kohaldamiseks piisab juba kaudsest tahtlusest.[240]

[237] Justiitsministeerium (viide 130), lk 29.
[238] R. W. Downing (viide 4), p 725.
[239] H. Vallaste. e-Teatmik: IT ja sidetehnika seletav sõnaraamat. Arvutivõrgus. Kättesaadav: http://www.vallaste.ee/index.htm?Type=UserId&otsing=1265, 23. aprillil 2014.
[240] E. Hirsnik (viide 88), lk 30.

KarS § 216¹ kohaldub ka juhul, kui on tegemist programmide valmistamise ning müümisega, mille abil on võimalik arvutikuritegusid toime panna. Koosseisu realiseerumiseks vajalik, et need loodud programmid oleksid üle antud kolmandatele isikutele. Vastutuse kohaldamiseks piisab asjaolust, et programmi koostaja on selle veebikeskkonda üles laadinud, millega võimaldatakse kolmandal isikul selle allalaadimisega toime panna arvutikuritegu. Interneti kasutamine on tänapäeval laialdane, mistõttu on sellises keskkonnas liikvel ka küberkurjategijad. Vastutuse kohaldamiseks ei ole seega vajalik, et programmi valmistajal endal oleks soovi arvutikuriteo toimepanemiseks, selle võib sooritada ka keegi teine.

Tuleb tõdeda, et Eesti seadusandjal ei ole kuigivõrd hästi õnnestunud konventsiooni art 6 mõtte lisamine KarS § 216¹. Tegemist on ebaõnnestunud ja keeruliselt sõnastatud sättega, mis võib oma ebaselguse tõttu rikkuda karistusõiguslikku määratletuspõhimõtet.[241] KarS § 216¹ tuleneb konventsiooni art-st 6, mis paneb konventsiooniosalistele kohustuse kriminaliseerida arvutikuritegude ettevalmistamine. Säte võiks olla liigendatud sarnaselt konventsiooni artikliga, sest hetkel on norm süsteemitu ning üheselt mitte mõistetav. Seadusandja on normi lühiduse huvides loobunud konventsiooni art-s 6 sisalduvast topeltviitest teatud kuritegudele, mistõttu on see ebaselge. Konventsiooni art-s 6 olev esimene viide art-tele 2-5 tähendab, et teoobjektid on vaid kuritegude tarvis kavandatud seadmed ja programmid. Teine viide on seotud hilisema teoga (nt müümine või muul viisil kättesaadavaks tegemine) ja sätestab, et karistatav on vaid see tegu, mis pannakse toime sooviga teostada objektiga arvutikuritegu.[242]

Keeruliselt on sõnastatud ka eestikeelse konventsiooni art 6, mistõttu võib tekkida olukord, kus arvutikuritegude ohvriks langevate isikute õiguslik kaitse on väiksem, kui see on inglisekeelse konventsiooni art-ga 6.[243] Normiga reguleerimata on olukord näiteks siis, kui poejärjekorras seisev kuritegelike kavatsustega isik soovib teada saada teiste inimeste pangakaartide PIN-koode. Selleks seisab ta järjekorras olevatel inimestel väga lähedal, et kaardiga tasumise puhul märgata isikute PIN-koode, sooviga varastada rahakott ning võtta kaardi abil raha automaadist välja. Kui koodide teadasaamine sel viisil on õnnestunud, siis on kurjategija hankinud endale „arvutiparooli või juurdepääsukoodi või sama laadi andmeid, mille abil võib juurde pääseda kogu arvutisüsteemile või selle osale“ (kolmas teokirjeldus art 6 lg 1 p-s a). Koode soovib ta teada saada ju selleks, et kasutada neid art-s 2 nimetatud teo toimepanemiseks.[244] Kui vaadata konventsiooni eestikeelset tõlget, siis tuleb tõdeda, et antud situatsiooni reguleerimiseks on eestikeelse tõlke järgi hõlmatud vähem olukordi kui

[241] Justiitsministeerium (viide 130), lk 28.
[242] Samas.
[243] E. Hirsnik (viide 88), lk 28.
[244] Samas.

inglisekeelse tõlke puhul. Seega, kui näites toodud isik sooviks neid kaartide salasõnasid kellelegi edasi müüa, tekib olukord, kus isikut ei saa karistada, kuna eestikeelse tõlke versiooniga sellised juhtumid reguleeritud ei ole. Inglisekeelne versioon on umbisikuliselt sõnastatud, eestikeelne aga mitte. Sellised möödalaskmised ja vead õigusaktides võivad tuua kaasa isikute väiksema kaitse toimepandavate rikkumiste eest.[245] Seetõttu on oluline pöörata tähelepanu ka tõlkele, et rahvusvahelise normilooja mõte ei läheks kaduma.

Probleemne on ka normis olev sanktsioon, sest kui kahjustusdelikti eest näevad muudatustejärgses KarS-s §-d 207, 213, 217 ette kuni 3-aastase vangistuse, siis ei ole aktsepteeritav, et ettevalmistustegu karistataks sama rangelt. Sanktsioon, mis karistusõigusdogmaatika aluspõhimõtteid eirab, kehtestati paragrahvis varasemalt seetõttu, et saaks teostada jälitustegevust, sest omal ajal sai jälitustegevust teostada vaid juhul, kui karistusnorm nägi ette vähemalt kolmeaastase sanktsiooni. Käesoleval hetkel ei ole jälitustegevuse läbiviimine sanktsiooniraamiga enam seotud, mistõttu saab karistuse määra langetada.[246] Kui määrata sanktsiooniks kuni 2-aastane vangistus, jääks ebaloogilisus normi püsima, sest muudatustejärgses karistusseadustikus näeksid nii KarS § 206 lg 1 kui KarS § 216[1] lg 1 ette kuni 2-aastase vangistuse. Normiloojad on teinud ettepaneku sanktsiooni maksimummääraks kehtestada kuni 1-aastane vangistus.[247] Kuna sellisel juhul tekiks vastuolu direktiivi art 9 lg-ga 2, mis sätestab, et maksimummääraks peab raskemate juhtumite puhul olema 2-aastane vangistus, ei ole võimalik leebemat karistust sätestada kui vähemalt 2-aastane vangistus.

[245] E. Hirsnik (viide 88), lk 28.
[246] Justiitsministeerium (viide 43).
[247] Samas.

2.6 Ebaseaduslik pealtkuulamine

Euroopa Nõukogu „Soovitusega nr (89) 9“ on leitud, et andmeside pealtkuulamise puhul on tegemist sama tõsise privaatsuse rikkumisega, kui seda on näiteks suulise kõne või telefonivestluse pealtkuulamine. Infotehnoloogiline areng on tinginud selle, et väga palju infot on liikvel arvutisüsteemides ja -võrkudes, mille tõttu on sagenenud juhtumid, kus informatsiooni soovitakse omaniku teadmata kopeerida, lindistada vms. Omanik ei pruugi sellest midagi teada, kuna tema arvutisüsteemis olevad andmed jäävad muutumatul kujul alles. Euroopa Nõukogu poolt väljatöötatud „Soovitusega (89) 9“ seati eesmärgiks kriminaliseerida ebaseaduslik pealtkuulamine, mille tõttu võib kolmas isik saada informatsiooni arvutisüsteemis ja -võrgus edastatud suhtlusandmetest, milleks tal õigus puudub.[248]

Kriminaliseeritud ei tohiks olla vaid ebaseaduslik arvutisüsteemis ja -võrgus olevate andmete jälgimine, vaid ka selline pealtkuulamine, mis on teostatud näiteks tööülesandeid täites. Sellisel juhul ei pruugi süsteemile juurdepääs ebaseaduslik olla, ent pealtkuulamist võidakse siiski teostada. Seadusandja ei tohiks kriminaliseerida vaid ebaseaduslikku juurdepääsu arvutisüsteemis ja -võrgus olevate andmete jälgimiseks, karistatav peaks olema ka selline pealtkuulamine, mida ei teostata ebaseadusliku juurdepääsu teel. Selline olukord võib tekkida siis, kui süsteemiadministraator kirjaserveri testimise kõrval loeb ka selles sisalduvaid meile, milles on näiteks informatsiooni ettevõtte ärisaladusest ning mille teatavakssaamine konkurendile tooks kaasa olulist kahju. Süsteemiadministraatoril võib tekkida soov info müümiseks, mistõttu on vajalik, et regulatsioon kaitseks füüsilisi isikuid ja ettevõtteid ka selliste toimepandud tegude eest.[249]

Konventsiooni art 3 ja direktiivi art 6 sätestavad ebaseadusliku pealtkuulamise. Varasem raamotsus oma artiklitega ebaseaduslikku pealtkuulamist ei reguleeri. Eesti on teatanud, et on konventsiooni ilma reservatsioonideta ratifitseerinud ja Eesti esindajad on avaldanud arvamust, et ebaseadusliku pealtkuulamise kriminaliseerimine on kaetud KarS §-ga 137 (ebaseaduslik jälitustegevus) ning KarS §-ga 156 (sõnumisaladuse rikkumine), kuid on küsitav, kas nendes sätetes avaldub konventsiooni art 3 ja direktiivi art 6 mõte.

[248] A. Bequai (viide 76), p 53-54.
[249] R. W. Downing (viide 4), p 731.

§ 137. Eraviisiline jälitustegevus
(1) Jälitustegevuseks seadusliku õiguseta isiku poolt teise inimese jälgimise eest tema kohta ndmete kogumise eesmärgil – karistatakse rahalise karistuse või kuni kolmeaastase vangistusega.
(2) Sama teo eest, kui selle on toime pannud juriidiline isik, – karistatakse rahalise karistusega.[250]

§ 156. Sõnumisaladuse rikkumine
(1) Kirjavahetuse ja sidevahendi abil edastatud sõnumi saladuse rikkumise eest – karistatakse rahalise karistusega.
(2) Sama teo eest isiku poolt, kes pääses sõnumi juurde oma tööülesannete tõttu, – karistatakse rahalise karistuse või kuni üheaastase vangistusega.[251]

Direktiivi art 6 sätestab, et liikmesriik võtab vajalikud meetmed, et infosüsteemi, sellest infosüsteemist või selle infosüsteemi piires, sh infosüsteemi elektromagnetkiirguse abil mitteavalikult edastavate arvutiandmete tahtlik ja õigusliku aluseta pealtkuulamine tehniliste vahendite abil on vähemalt raskemate juhtumite puhul kriminaalkorras karistatav. Pealtkuulamine hõlmab endas teabe sisu kuulamist, jälgimist või seiret ning andmete sisu hankimist kas vahetult (infosüsteemidesse sisenemise ja nende kasutamise teel) või kaudselt (tehniliste vahendite abil elektrooniliste pealtkuulamisseadmete kasutamise teel), ent ei pea tingimata eelpool väljatooduga piirduma, loetelu jäetakse lahtiseks.[252] Konventsiooni art 3 sätestab, et konventsiooniosaline võtab vastu seaduslikke ja muid meetmeid, et määratleda kuriteona arvutiandmete ja neid sisaldavast arvutisüsteemist pärineva elektromagnetkiirguse pealtkuulamine tehnikavahenditega ajal, kui andmeid konfidentsiaalselt edastatakse arvutisüsteemi, -süsteemis või -süsteemist, kui tegu pannakse toime tahtlikult ja ilma õigusliku aluseta.[253] Konventsiooni seletuskirja kohaselt ei ole sellisteks pealtkuulamisandmeteks praktikas nn „küpsised“ e *cookies*, mida kaubanduspoliitikas kasutatakse inimeste ostuharjumuste väljaselgitamiseks, sest nende puhul ei ole tegemist õigusliku aluseta teostatud pealtkuulamisega.[254] „Küpsis“ on tekstikujuline andmeblokk kliendi veebilehitsejas, mida saadetakse määratud aadressile e *domeenile* iga kord, kui klient teeb sinna päringu. Nii saab server tuvastada kliendi päringu teiste omadest ja pakkuda talle isikupärastatud andmeid. „Küpsiseid“ võib kasutada veebilehtedele sisse logimiseks, eelistuste salvestamiseks aga ka ostukäru sisemuse meelespidamiseks.[255] Konventsiooni art 3

[250] Karistusseadustik (viide 13).
[251] Samas.
[252] Euroopa Parlamendi ja Nõukogu direktiiv (viide 16).
[253] Euroopa Nõukogu Arvutikuritegevusvastane konventsioon (viide 14).
[254] Council of Europe (viide 86), p 58.
[255] H. Vallaste. e-Teatmik: IT ja sidetehnika seletav sõnaraamat. Arvutivõrgus. Kättesaadav: http://vallaste.ee/index.htm, 23. aprillil 2014.

ei reguleeri juhtumeid, kus isik seisab info saamiseks teise selja taga (füüsiliselt) ja loeb näiteks arvutis saadetavat meili. Artiklisse on lisatud märge tehnilise vahendi kasutamise kohta, mille abil pealtkuulamist teostatakse, mistõttu füüsilist juuresolekut väljatoodud näites ei saa käsitleda pealtkuulamisena. Kui nimetatud olukorrad oleksid normiga reguleeritud, tekiks isikute ülekriminaliseerimise oht.[256]

Võimalik, et ebaseaduslik pealtkuulamine on Eestis juba karistatav KarS §-ga 137 ja KarS §-ga 156. Nimelt on KarS §-ga 137 kaitstav õigushüve eneseteostusvabadus ja enesemääramisõigus – need õigused tulenevad otseselt põhiseaduse[257] §-st 19.[258] Normi koosseisuga kaitstakse kõiki sh elulisi ja tööalaseid andmeid.[259] Objektiivne koosseis sisaldab teona teise inimese jälgimist.[260]

KarS §-ga 156 kaitstav õigushüve on igaühe põhiõigus määrata, kes võib sõnumiga tutvuda (põhiseaduse § 43, Euroopa inimõiguste konventsiooni art 8). Kaitstav õigushüve ei ole käesoleva paragrahvi mõttes sõnumi saatmise fakti saladus või kirjavahetuse õigus.[261] Antud süüteokoosseisu objektiivne koosseis seisneb sellise sõnumisaladuse rikkumises, mis on edastatud kirjavahetuse või sidevahendi abil.[262]

KarS § 137 ja KarS § 156, mis väidetavalt käesolevas regulatsioonis ebaseadusliku pealtkuulamise juhtumeid reguleerivad, on oma koosseisult liiga üldised ega sisalda endas rahvusvahelistes õigusaktides sisalduvaid põhimõtteid ebaseaduslikku pealtkuulamise reguleerimiseks. KarS §-s 137 on koosseisupärase teona välja toodud teise isiku jälgimine tema kohta andmete kogumiseks, ent mida tähendab teise inimese jälgimine, on määratlemata. Normi sisust ei selgu, kas tegemist peab olema visuaalse vaatamisega või kujutab seesugune jälgimine endast ka midagi muud.[263] Norm on sõnastatud liiga kitsalt ning ei ole õige väita, et sellega saab reguleerida ka arvutisüsteemis olevate andmete ebaseaduslikku jälgimist.

Samuti ei saa ebaseaduslikku pealtkuulamist reguleerida KarS §-ga 156, sest see säte ei ole konkreetselt määratletud. Norm kaitseb sisuliselt „sõnumi saladuse rikkumise eest“, ent selline karistusnormi formuleerimine ei ole õige. Karistusnormi teoobjekt peab olema reaalne välismaailma objekt, mis on kas käega katsutav või „virtuaalne tegelikult olemasolev objekt“. Ka „rikkumine“ teokirjelduse kasutamist normis ei saa pidada õigeks, sest teokirjeldus ei ole

[256] R. W. Downing (viide 4), p 732.
[257] Eesti Vabariigi Põhiseadus. – RT 1992, 26, 349.
[258] Karistusseadustik. Komm vln § 137 komm 1.
[259] Samas.
[260] Karistusseadustik. Komm vln § 137 komm 3.1
[261] Karistusseadustik. Komm vln § 156 komm 1.
[262] Karistusseadustik. Komm vln §156 komm 2.
[263] E. Hirsnik (viide 88), lk 18.

mingi abstraktne õigushüve rikkumine, vaid mingi rohkem või vähem konkretiseeritud tegevus.[264] KarS § 156 ei saa kasutada ebaseadusliku pealtkuulamise reguleerimiseks ka seetõttu, et konventsioon nõuab vähemalt 2-aastast karistusmaksimumi, ent KarS § 156 lg 1 näeb ette vaid rahalise karistuse, lisaks ei ole ette nähtud vastutust juriidilistele isikutele.[265] Seega ei vasta Eesti seadus konventsioonile ega ka raamotsust asendavale direktiivile.

Olukorra aitaks käesoleva töö autori arvates lahendada erinormi lisamine ebaseadusliku pealtkuulamise reguleerimiseks, sest hetkel on siseriiklik õigus konventsiooni art-ga 3 ja direktiivi art-ga 6 vastuolus. Lisaks inimeste andmete ebaseaduslikule jälgimisele on vajalik lisada vastutus juriidilise isiku andmete ebaseadusliku pealtkuulamine eest, mida nõuab ka konventsiooni art 12 ja direktiivi art 11. Karistusõiguse revisjonis on tehtud ettepanek ebaseadusliku pealtkuulamise normi lisamiseks seadustikku, kuid kahjuks ei ole seda arvesse võetud, sest on leitud, et eelpool nimetatud normid karistusseadustiku regulatsioonis reguleerivadki ebaseaduslikku pealtkuulamist.[266]

[264] E. Hirsnik (viide 88), lk 19.
[265] Samas.
[266] Justiitsministeerium (viide 130), lk 31.

KOKKUVÕTE

Arvutikuriteod on moodsa ühiskonna arenguga kaasnev nähtus, kus erinevad tehnoloogilised lahendused küll lihtsustavad inimeste elu, ent nendega kaasnevad mitmed uuele ja ainulaadsele keskkonnale iseloomulikud ohud. Kõrge infotehnoloogiline areng on tinginud arvutikuritegude kasvu nii Eestis kui ka mujal, mistõttu muutub reaalmaailma kõrval üha enam kuriteo toimepanemise kohaks ka virtuaalmaailm.

Selleks, et arvutikuritegevust piirata, tuleb antud probleemiga tegeleda nii siseriiklikult kui ka rahvusvaheliselt, kus riikide eesmärgiks peaks olema võimalikult sarnase regulatsiooni sätestamine. Eestis reguleerib arvutikuritegusid karistusseadustik, millesse laialdasemad muudatused viidi sisse 2008. aastal, eesmärgiks täiendada materiaalõigust, et see oleks kooskõlas nõuetega, mis on sätestatud Euroopa Nõukogu arvutikuritegevusvastases konventsioonis ning Euroopa Nõukogu 2005. aasta raamotsuses 2005/222/JSK. 2013. aasta augustis võeti vastu Euroopa Parlamendi ja Nõukogu direktiiv 2013/40/EL, mis varasema raamotsuse asendas.

Käesoleva magistritöö eesmärgiks oli analüüsida karistusseadustiku arvutikuritegusid reguleerivaid sätteid (KarS § 206, 207, 208, 217, 216[1]) ning nende muutmise vajalikkust. Selleks esitas autor mitmeid küsimusi: missugused kitsaskohad esinevad karistusseadustiku arvutikuritegusid reguleerivates sätete ning millised neist tuleks karistusõiguse revisjoniga likvideerida. Töös analüüsiti, kas hetkel kehtiv regulatsioon on kooskõlas rahvusvahelistes õigusaktides kehtestatud põhimõtetega ning vaadeldi, missuguste muudatuste sisseviimist sätetesse nõuab 2013. aasta augustis kehtima hakanud direktiiv.

Tõstatatud küsimuste põhjal jõudis töö autor järgmistele põhilistele järeldustele.

Käesolevas magistritöös teostatud karistusseadustiku arvutikuritegusid reguleerivate sätete analüüsi tulemusena selgus, et teataval määral on arvutikuritegusid kriminaliseerivate normide kaitseala rahvusvahelise õiguse normidest kitsam. Kohati on normid sõnastatud grammatiliselt ebakorrektselt ning normilooja ei ole kasutanud ühtset keelekasutust, mistõttu on sätete sisu keeruline mõista. Kuna koosseisude kirjeldused ei ole täpselt formuleeritud ning läbimõeldud, võib kehtiva redaktsiooniga kaasneda ülekriminaliseerimise oht. Ebaproportsionaalselt on kehtestatud ka sanktsioonid.

KarS §-s 206, mis arvutiandmetesse sekkumist reguleerib, on problemaatiline “sisestamise” teokirjeldus, mida rahvusvahelised õigusaktid andmetesse sekkumise artiklites ei nimeta.

Eestis käsitletakse “sisestamise” mõistet laialt, mis võib endaga kaasa tuua isikute tegude ülekriminaliseerimine. Seega nõustub autor karistusõiguse revisjonis tehtud ettepanekuga formuleeringu kustutamiseks normist. Sättes on vajalik muuta ka sõnastust, sest kehtivas regulatsioonis kõneletakse normi lõikes 1 arvutiandmetest, lõikes 2 aga arvutisüsteemist, mis normi lugemisel võib segadust tekitada, sest KarS § 206 reguleerib arvutiandmetesse sekkumist.

Seoses direktiiviga lisatakse sättesse vastutus grupi poolt toime pandud eest ning paljudes arvutisüsteemides olevate andmete vastu teostatud rünnete eest, mille toimepanemiseks kasutati KarS §-s 216¹ nimetatud seadet või programmi. Autor asus seisukohale, et määratluse “paljudes arvutisüsteemides olevate andmete ” lisamine sättesse ei ole põhjendatud, sest kuigi robotvõrkude rünnetega võidakse kahjustada suurel hulgal arvutiandmeid, võib selle määratlemine osutuda keeruliseks. Normilooja on soovinud reguleerida ilmselt ka selliseid olukordi, kus ründeid andmete vastu teostatakse näiteks robotvõrkude abil, kuna rahvusvaheline normilooja on möönnud, et selle käigus võivad paljud andmed kahjustatud saada, kuid ei ole määratletud, kui palju neid peab olema.

KarS §-s 207, mis arvutisüsteemi toimimise takistamist reguleerib, on peamine probleem sanktsiooni vastuolulisuses KarS §-ga 206. KarS § 207 on raskem arvutikuriteo avaldumisvorm, mistõttu ei ole kohane, et nii andmetesse sekkumise kui ka arvutisüsteemi toimimise takistamise eest nähakse ette ühesugune karistusmäär. Kehtiv regulatsioon on ebaloogiline, sest kui kurjategija põhjustab andmetesse sekkumisega arvutisüsteemi toimimise takistamise, siis kehtiva õiguse järgi ei olegi kohtul vaja tõendada, et süsteemi tööd on reaalselt häiritud. Sanktsioonimäär on ühesugune, mistõttu vastutuse kohaldamiseks piisab andmetesse sekkumise asjaolu tõendamisest.

Töö autor nõustub karistusõiguse revisjonis tehtud ettepanekuga KarS § 207 sõnastuse muutmiseks, kuna normi esimeses lõikes kõneletakse „toimimisest”, teises lõikes aga „tööst”. Lõigetes kasutatavad formuleeringud peaksid olema aga ühesugused. Lahenduseks oleks see, kui mõlemates lõigetes kasutataks sõna „toimimist“. Sättes esineb veel üks analoogne viga, nimelt kasutatakse lõikes 1 koosseisuteona „ häirimist ja takistamist“, lõikes 2 kõneletakse vaid „takistamisest“, kuigi ka seal peaks olema koosseisuteona välja toodud „häirimine“.

Direktiivist tulenevalt lisatakse vastutus paljude arvutisüsteemide toimimise takistamise kohta ja selle toimepanemisel kasutati KarS §-s 216¹ nimetatud seadet või arvutiprogrammi. Samuti lisatakse vastutus grupi poolt toime pandud teo poolt.

KarS § 208, mis reguleerib nuhkvara, pahavara ja arvutiviiruse levitamist analüüsi tulemusel selgus, et sättega reguleeritav tegu on kaetud juba teiste arvutikuritegusid reguleerivate sätetega, millest tulenevalt on seadusemuudatusega tehtud ettepanek normi kustutamiseks. Seda enam, et rahvusvahelised õigusaktid ei reguleeri eraldi nuhkvara, pahavara ja arvutiviiruse levitamist, sest nimetatud õigusvastane tegu on kaetud teiste artiklitega. Normile heidetakse ette ka tagurlikku sõnastust, sest esiteks ei ole kindla loeelu lisamise korral võimalik reguleerida sellega teistsuguseid ründeid, mida sättega kvalifitseerida saaks.

KarS §-s 217, mis reguleerib arvutisüsteemi ebaseaduslikku kasutamist, on problemaatiline asjaolu, et normiga reguleeritakse arvutisüsteemi kasutamist, ent normiga ei ole kaetud arvutisüsteemi osa ebaseaduslik kasutamine, kuigi rahvusvahelistes õigusaktidega on kriminaliseeritud ka süsteemi osale ebaseadusliku juurdepääsu hankimine. Selles osas on karistusseadustiku säte vastuolus rahvusvaheliste õigusaktidega, mis toob kaasa õigustatud isikute väiksema kaitse.

Analüüsi tulemusena selgus, et formuleeringu „koodi, salasõna ja muu kaitsevahendi“ kastutamine sättes võib tekitada segadust, sest ei selgu, mis neid omavahel eristab. Kehtivas regulatsioonis kasutatava sõnastusega tekitatakse arusaam, nagu peab kaitsevahend olema tarkvaraline. Seega on õigustatud ettepanek kasutada vaid formuleeringut „kaitsevahendi“.

KarS § 217 puhul on vastuoluline ka see, et nii normi pealkirjas kui sätte lõike teises punktis on teokirjeldusena märgitud „kasutamist“, kuid normi pealkirja eesmärgiks peaks olema normi sisu edasi andmine, mistõttu on korrektsem kasutada teokirjeldusena „juurdepääsu hankimist“. Hetkel on säte normitehniliselt ja õigusdogmaatiliselt ebatäpne.

KarS §-s 216¹, mis reguleerib arvutikuriteo ettevalmistamist, on probleemne sõnastusest tulenev liiga lai sätte tõlgendamisvõimalus ning seetõttu on seadusemuudatusega peetud vajalikuks normi kitsam sõnastamine, milleks tuleneb alus ka konventsioonist ning direktiivist. Kehtiva regulatsiooni sõnastus võimaldab seega vastusele võtta isiku juba *Windows* operatsioonisüsteemi kasutamise eest, ka selle abil on võimalik arvutikuritegusid toime panna. KarS § 216¹ toob koosseisupärase teona välja „kasutamise“, mis tegelikult märgib reaalse kuriteo toimepanemist, sätte eesmärk on reguleerida ettevalmistamist.

Normi analüüsimisel ei selgu ka, millele peavad teoobjektid vastavalt kavandatud ja kohandatud olema. Grammatiliselt on säte sõnastatud kehtivas regulatsioonis nii, nagu peaksid ka salasõna, kaitsekood ja muud arvutisüsteemile juurdepääsuks vajalikud andmed

olema vastavalt kavandatud ja kohandatud, kuigi rahvusvaheliste õigusaktide järgi peaksid seda olema vaid seadmed ja arvutiprogrammid.

KarS §-s 216¹ on vastuoluline ka sanktsioon, sest ettevalmistegu ei saa olla karistatav sama rangelt, kui kahjustusdelikt, mistõttu on vajalik ettevalmistusteo sanktsiooni vähendada.

Käesolevas töös analüüsiti lisaks seda, kas siseriikliku õigusega on reguleeritud ka arvutisüsteemis ja -võrgus olevate andmete ebaseaduslik pealtkuulamine, mille kriminaliseerimise näeb ette nii konventsioon kui direktiiv. Tuleb tõdeda, et Eesti normiloojad on leidnud, et KarS §-ga 137 ja KarS §-ga 156 on ebaseaduslik pealtkuulamine reguleeritud, ent see on vaieldav. Karistusõiguse revisjoniga tehti ettepanek erinormi lisamiseks, kuid sellega ei arvestatud, mistõttu tekib käesoleva autori arvates sellest tulenevalt vastuolu konventsiooni ja direktiiviga.

Analüüsist järeldub, et karistusseadustiku arvutikuritegusid reguleerivatesse sätetesse on vajalik sisse viia muudatusi, mis tulenevad peamiselt kahest alusest: esiteks sellest, et normid ei ole korrektselt sõnastatud, mistõttu ei ole need üheselt mõistetavad ning sellega võib kaasneda ka ülekriminaliseerimise oht. Teiseks tuleb muudatused sisse viia seetõttu, et karistusseadustiku arvutikuritegusid käsitlevad sätted oleks täielikult kooskõlas nii arvutikuritegevusvastase konventsiooniga kui ka uue raamotsust asendava direktiiviga.

Arvutikuritegusid kvalifitseerivate koosseisudega saab isikute õiguste kaitse olla tõhusamalt tagatud siis, kui neid kuritegusid reguleerivad normid on sõnastatud grammatiliselt korrektselt, lähtudes ühtsest keelekasutusest ning nende sisu on rahvusvahelistest õigusaktidest tulenevate nõuetega kooskõlas.

RÉSUMÉ

Computer crimes in the Penal Code and the provisions governing the need for amendment

Computer crime is a phenomenon associated with the development of modern society, where different technological solutions while facilitating the lives of people, are accompanied by a number of threats characteristic to the new environment. High development in information technology has led to the growth of computer crime in Estonia and other countries, because Internet is an anonymous environment for committing computer crimes.

The research in Estonian recorded crime statistics for the period 2003-2013, has seen an upward trend in computer crimes. High Internet use and the development of technology has led to the growth of computer crime in the entire world. In order to limit computer crime the problem must be attended both nationally and internationally. Countries should aim to regulating computer crime by the same token.

Computer crimes were firstly regulated in Estonia in 1997 when Estonian Criminal Code was in force. The problem with the regulation was that not all computer crimes were sanctioned with it. For thet reason the legislator made several changes in acts and structure – consummated Penal Code came into force on 1st September 2002.

Since developing the information society has made the development of computer possible, it has been necessary to amend the Penal Code. The renewed Penal Code came into force in 2008. The purpose was to upgrade the substantive law in a way that would be consistent with the requirements set out in the Council of Europe Convention on Cybercrime and Council Framework Decision 2005/222/JHA on attacks against information systems. In August 2013 The European Parliament and Council Directive 2013/40/EL came into force, which replaced the previous Framework Decision.

The purpose of this thesis was to analyze computer crimes in the Penal Code provisions (Penal Code § 206, 207, 208, 217, 216 ¹) and the need for the amendment. Cyber criminals are continuously developing their skills and are becoming more and more professional in committing computer crimes. They also create networks of cyber criminals in order to perpetrate computer crimes, causing harm to both individuals and organizations.

For making the survey the author presented a number of questions for analysing: what bottlenecks are present in Penal Code provisions governing computer crimes, which should be removed. The author examined whether the regulation currently in force is in accordance with the principles established in international law acts and looked at what kind of amendments to the provisions does the Directive, which came into force in August 2013, need.

The master thesis is divided into two chapters. The first chapter gives an overview of the following: the definition of computer crime in general, the concept of Estonian history of computer crime regulations, the concept of international legislation governing cyber crimes. The second chapter focuses on computer crime provisions governing the composition of the elements in the analysis; regarded as those that are planned to change with amendment to the act and those that remain unchanged.

In writing the author has used analyze-comparative method. As primary sources the author has used Council of Europe Convention on Cybercrime, the Council Framework Decision of the European Parliament and Council Directive. Theoretical views are mainly based on commented edition of Penal Code and J. Sootak's and P. Pikamäe´s, the Estonian court practise, E. Hirsnik´s „Computer Crime Training" (unpublished material) and Explanatory Report to the Convention on Cybercrime. In current thesis articles and literature published by A. Bequai, S. Schjolberg, S.L. Hopkins, K.M Finklea and C.A. Theohary have been used.

Based on the issues raised, the author reached to the following conclusions.

The analysis of the Penal Code provisions governing the review of the results showed that a certain degree of computer crimes in the Penal Code criminalization reserve narrower norms than in international law. The rules are at times formulated grammatically incorrect and the author of the norms has not used a particular language, therefore it is difficult to understand the content of the provisions. Computer crime sanctions imposed are disproportionate. Since the configurations of the descriptions are not precisely crafted and carefully considered, the current version entails a risk for over-criminalisation, on account of which it is necessary to amend the provisions of criminal law.

The analysis shows that it is necessary to carry out changes, which come primarily from two bases. Firstly the fact that the norms are not worded correctly and are therefore ambiguous. In some cases this may also lead to the threat of over-criminalisation. Secondly, the amendments should be introduced in order the Penal Code provisions governing computer crimes to be

consistent with both the Cybercrime Convention and the European Parliament and Council Directive.

Governing the composition of computer crime can be effectively guaranteed to protect the rights of people when it is governed by rules formulated grammatically correct, based on a particular language useage and their content is in accordance with international legal requirements – it assures to ensure the amendment of the Penal Code Act.

Tartu, 05.05.2014

KASUTATUD MATERJALIDE LOETELU

Kasutatud kirjandus

1. A. Bequai. Computer-Related Crime. European Committee on Crime Problems. Strasbourg, 1990, p 7-115.
2. A. Kukrus. Küberkuritegevuse tõkestamine infoühiskonnas. Arvutivõrgus: http://www.riigikogu.ee/rito/index.php?id=11319, 23. aprillil 2014.
3. A. Kukrus. Virtuaalmaailm ja küberkuriteod. A&A, 2002, nr 3, lk 39-45.
4. Arvamuste tabel karistusseadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu seletuskirja juurde. Justiitsministeerium, lk 26-31.
5. Arvutikaitse. Arvutivõrgus: http://www.arvutikaitse.ee/arvutikaitse-algtoed/botnet/, 23. aprillil 2014.
6. Council of Europe. Cyberterrorism – the Use of the Internet for Terrorist Purposes. Council of Europe Publishing, 2007. Arvutivõrgus: http://www.remep.mpg.de/files/publication_entries/sieber-ulrich_02/Sieber_-_Cyberterrorism_Council_of_Europe.pdf, 23. aprillil 2014.
7. Council of Europe. Explanatory Report to the Convention on Cybercrime. Arvutivõrgus: http://conventions.coe.int/Treaty/EN/Reports/html/185.htm, 23. aprillil 2014.
8. Council of Europe. Recommendation No. Recommendation No. R (89) 9. Committee of Ministers, 1989. Arvutivõrgus: https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=610660&SecMode=1&DocId=702280&Usage=2, 23.aprillil 2014.
9. Council of Europe. Recommendation No. R (95) 13. Committee of Ministers, 1995. Arvutivõrgus: https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=1900870&SecMode=1&DocId=528034&Usage=2, 23. aprillil 2014.
10. D. Cangemi. Procedural Law Provisions of the Council of Europe Convention on Cybercrime. – International Review of Law Computers and Technology, 2004, Vol 18, No 2. Arvutivõrgus: http://www.tandfonline.com/doi/pdf/10.1080/1360086042000223472, 23. aprillil 2014.
11. E. Elken. Arvutikuritegude menetlemise rahvusvahelised aspektid. Bakalaureusetöö. Tartu, 2009.
12. E. Hirsnik. Arvutikuritegevuse koolitus (avaldamata ettekande materjal), 2013.

13. E. Tikk-Ringas. Küberjuleoleku õiguslik raamistik. – Juridica, 2012, nr 4, lk 274-283.
14. Eesti Rahvusraamatukogu. Raamatukogusõnastik. Arvutivõrgus: http://www.nlib.ee/termin/public_term/termin/view/4664, 23. aprillil 2014.
15. Euroopa Ühenduste Komisjon. Küberkuritegevuse vastase võitluse üldise poliitika kujundamine. Brüssel, 2007. Arvutivõrgus: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:ET:HTML, 23. aprillil 2014.
16. G. Stamatellos. Computer Ethics. Jones & Bartlett Publishers, 2007.
17. H. Vallaste. e-Teatmik: IT ja sidetehnika seletav sõnaraamat. Arvutivõrgus: http://vallaste.ee/index.htm, 23. aprillil 2014.
18. H. Vallaste. Arvutivõrgus: http://wordties.cst.dk/wordties-estwn/w/full/354951-arvutikuritegevus, 23. aprillil 2014.
19. I. Metusa. Telekommunikatsioonialased õigusrikkumised Informatsioonivabaduse loomulikust piirist. – Juridica, 2002, nr 5, lk 312-320.
20. J. Salla. Registreeritud kuriteod 2003-2013. Arvutivõrgus: http://www.just.ee/orb.aw/class=file/action=preview/id=59296/Kuritegevuse+andmed+2003-2013.xlsx, 23. aprillil 2014.
21. J. Sootak, P. Pikamäe. Karistusseadustik. Kommenteeritud väljaanne. Tallinn: Juura 2009.
22. J. Sootak. Karistusõigus. Üldosa. Tallinn: Juura 2010.
23. K. Archick. Cybercrime: The Council of Europe Convention. CRS Report for Congress, 2006. Arvutivõrgus: http://fpc.state.gov/documents/organization/74909.pdf, 23. aprillil 2014.
24. K. Domaškina. Ebaseaduslik sekkumine arvutiandmetesse ja sel teel varalise kasu saamine. Riigikohtu kriminaalkolleegiumi otsus 3-1-1-114-12. – Juridica, 2013, nr 2, lk 144-145.
25. K. M. Finklea, C.A. Theohary. Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement. CRS Report for Congress, 2012. Arvutivõrgus: http://www.law.umaryland.edu/marshall/crsreports/crsdocuments/R42547_07202012.pdf, 23. aprillil 2014.
26. Karistusõiguse revisjon. Justiitsministeerium. Arvutivõrgus: http://www.just.ee/Protsess, 23. aprillil 2014.
27. Karistusseadustiku muutmise seaduse eelnõu seletuskiri (167). Arvutivõrgus: http://www.riigikogu.ee/?op=emsplain&page=pub_file&file_id=85a4d8e5-2c8a-0faf-b0e9-3ff75214ffbf&, 23. aprillil 2014.

28. Kuritegevus Eestis 2010. Kriminaalpoliitika uuringud 15. Justiitsministeerium. Arvutivõrgus: http://www.just.ee/orb.aw/class=file/action=preview/id=54700/KuritegevusEestis2010_web.pdf, 23. aprillil 2014.
29. Küberjulgeoleku strateegia 2008-2013. Kaitseministeerium. Arvutivõrgus: http://valitsus.ee/UserFiles/valitsus/et/valitsus/arengukavad/kaitseministeerium/kuberjulgeolek.pdf, 23. aprillil 2014.
30. L. Viik. Küberrünnak suveräänse riigi vastu oli maailmas esmakordne. Arvutivõrgus: http://www.postimees.ee/250507/esileht/siseuudised/261227.php, 23. aprillil 2014.
31. M. Gercke. Europe's legal approaches to cybercrime. ERA Forum, 2009, Vol 10, Iss 3. Arvutivõrgus: http://link.springer.com/article/10.1007%2Fs12027-009-0132-5, 23. aprillil 2014.
32. Oxford Dictionaries. Arvutivõrgus: http://www.oxforddictionaries.com/definition/english/cybercrime, 23. aprillil 2014.
33. R. W. Downing. Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime. – Columbia Journal of Transnational Law, 2005, Vol 43, No 3, p 707-761.
34. S. W. Brenner, M. D. Goodman. Cybercrime: The Need to Harmonize National Penal and Procedural Law. International Society for the Reform of Criminal Law 16th Annual Conference, 2002. Arvutivõrgus: http://www.isrcl.org/Papers/Brenner.pdf, 23. aprillil 2014.
35. S. L. Hopkins. Cybercrime Convention: A Positive Beginning to a Long Road Ahead. Journal of High Technology Law, 2003, p 101-122.
36. S. Schjolberg. The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva. Arvutivõrgus: http://www.cybercrimelaw.net/documents/cybercrime_history.pdf, 23. aprillil 2014.
37. S. Luide. The legal status and liability of Internet service providers. – Juridica Abstract, 2001, nr 5, p 329-336.
38. Seletuskiri karistusseadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu juurde (554 SE). Arvutivõrgus: http://www.riigikogu.ee/?op=ems&page=eelnou&eid=78433b29-8b2f-4281-a582-0efb9631e2ad&, 23. aprillil 2014.
39. T. Ploom. Arvutikuritegude kvalifitseerimine. – Juridica, 2003, nr 8, lk 576-578.
40. T. Rosenfeldt. IT turvalisus. Arvutivõrgus: http://www.e-uni.ee/e-kursused/itturvalisus/112_kberkuritegevuse_termin.html, 23. aprillil 2014.

41. Turvalisuspoliitika 2010. Kokkuvõte „Eesti turvalisuspoliitika põhisuunad aastani 2015“ täitumisest. Siseministeerium. Arvutivõrgus: https://www.siseministeerium.ee/public/Turvalisuspoliitika_2010.pdf, 23. aprillil 2014.
42. „Turvalisuspoliitika põhisuunad aastani 2015“ täitmise tegevusaruanne 2012. aasta kohta. Siseministeerium. Arvutivõrgus: https://valitsus.ee/UserFiles/valitsus/et/valitsus/arengukavad/siseministeerium/TPPS%20aruanne%202012.%20aasta%20kohta%20.pdf, 23. aprillil 2014.
43. V. Praust. Infoühiskond ja selle teetähised. IT haldusjuhtimises. MKM aastaraamat, 1998. Arvutivõrgus: http://www.riso.ee/aastaraamatud/et/pub/1998it/12.htm, 23.aprillil 2014.
44. V. Päärt. Kohus mõistis Laeva Meieri petturid vangi. Arvutivõrgus: http://www.postimees.ee/print/2542947/kohus-moistis-laeva-meierei-petturid-vangi, 23. aprillil 2014.
45. Web Strategist & Project Manager. Computer Crime Definition. Arvutivõrgus: http://www.mariosalexandrou.com/definition/computer-crime, 23. aprillil 2014.

Kasutatud normatiivmaterjalid

1. Andmekogude seadus. – RT I 1997, 28, 423.
2. Arvutikuritegevusvastase konventsooni lisaprotokoll. − RTL 2003,14, 192.
3. Arvutikuritegevusvastase konventsiooni ratifitseerimise seadus. – RT II 2003, 9, 32.
4. Avaliku teabe seadus. – RT I 2000, 92, 597; RT I, 19.12.2012, 5.
5. Eesti julgeolekupoliitika alused. – RT I 2010, 22, 110.
6. Euroopa Nõukogu Arvutikuritegevusvastane konventsioon. 01.07.2004 − ELS nr 185.
7. Euroopa Nõukogu raamotsus. 24.02.2005 – 2005/222/JSK.
8. Euroopa Parlamendi ja Nõukogu direktiiv. 14.08.2013 – 2013/40/EL.
9. Hädaolukorraks valmisoleku seadus. – RT I 2000, 95, 613.
10. Intellektuaalomandi õiguste kaubandusaspektide leping – RT II 1999, 22, 123.
11. Karistusseadustik. – RT I 2001, 61, 364; RT I, 26.02.2014, 6.
12. Karistusseadustiku rakendamise seadus. – RT I 2002, 56, 350; RT I, 05.07.2013, 12.
13. Kriminaalkoodeks. − RT 1992, 20, 287 ja 288.
14. Kriminaalmenetluse seadustik. – RT I 2003, 27, 116; RT I, 26.02.2014, 8.
15. Põhiseadus. – RT 1992, 26, 349; RT I, 27.04.2011, 2.

16. Riigisaladuse ja salatatud välisteabe seadus. – RT I 2007, 16, 77; RT I, 22.12.2011, 24.

Kasutatud kohtupraktika

1. RKKKo 14.12.2012, nr 3-1-1-114-12.
2. RKKKo 12.06.2012, nr 3-1-1-52-12.
3. RKKKo 25.02.2008, nr 3-1-1-85-08.
4. RKKKo 08.01.2007, nr 3-1-1-61-06.
5. RKKKo 05.05.2005, nr 3-1-1-43-03.
6. RKKKo 07.12.2000, nr 3-1-1-100-00.
7. HMKo 13.12.2007, nr 1-07-15185.

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, Evelin Elken,

(sünnikuupäev: 24.12.1986)

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose,

ARVUTIKURITEGUSID KÄSITLEVAD SÄTTED KARISTUSSEADUSTIKUS JA NENDE MUUTMISE VAJADUS

mille juhendajad on Erkki Hirsnik, Mario Rosentau

1.1. reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace-is lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;

1.2. üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace´i kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

2. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.

3. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tartus, 05.05.2014