TARTU ÜLIKOOL
ÕIGUSTEADUSKOND

Avaliku õiguse instituut

Eva Pära

ARVUTIKELMUSED JA NENDEGA SEONDUVAD VARAVASTASED SÜÜTEOD EESTI AKTUAALSES KOHTUPRAKTIKAS

Magistritöö

Juhendaja: õppeülesannete täitja mag. iur. Sten Lind

Tallinn
2013

SISUKORD

SISSEJUHATUS

Eestlastest kasutab internetti uuringute kohaselt keskeltläbi kolmandik, seejuures on arvuti hinnanguliselt 40 protsendil peredest. Meil on e-valitsus ja korraldame e-valimisi. Realiseerima on hakatud e-Eesti ideed, mille alusel käivituks rahvuslik infoühiskonna sihtprogramm. Majandus- ja kommunikatsiooniministeerium tegeleb interneti püsiühenduse projektiga, mille kohaselt kaetakse kogu riik internetiga.[1]

Uute kõrgtehnoloogiliste saavutuste kasutamine meie igapäevategevuses on tekitanud uue potentsiaali kelmustele. Suur osa informatsioonist telefonikõnede, lendude andmete ja internetikeskkonnas sooritatud ostude kohta on säilitatud digitaalsel kujul ja arvutivõrgud tagavad viljaka keskkonna arvutikelmuste tekkeks ning paljastavad tarbijad ja firmad ohtlikele finantsriskidele. Arvutikelmus hõlmab ükskõik millist arvutiga manipuleerimise tehnikat varalise kasu eesmärgil.[2]

Arvutikuritegevusega (sh ka arvutikelmustega) seonduv on käesoleval ajal väga aktuaalne. Sellist seisukohta kinnitab ka Eesti kuritegevuse statistika. Kui varavastaste süütegude arv nii üldiselt ja ka konkreetsete süütegude lõikes on enamasti olnud stabiilne või vähenenud, siis tõusutendentsi on näidanud just nimelt arvuti vahenduselt toime pandavad varavastased süüteod. Arvutikuritegudest on Justiitsministeeriumi andmetel näiteks 2012. aastal enim pandud toime arvutikelmusi, suurenenud on ka arvutisüsteemide ebaseaduslik kasutamine ehk kõnekeeles võõrasse arvutisse häkkimine. Üheks küberkuritegevuse kasvu põhjuseks võib pidada interneti laialdast levikut ja veebivõimaluste aktiivset kasutamist.[3] Arvutikelmuste kasvu näitavad ilmekalt alljärgnevad andmed. Kui aastal 2003 registreeriti 19 arvutikelmuse juhtumit (see moodustas üldse varavastastest süütegudest 0,044%) ja aastal 2007 oli neid 128 (0,464%), siis 2008 aastal registreeriti juba 367 arvutikelmust (1,299%). Seega kui 2003 aastal pandi üks arvutikelmus toime keskmiselt 19 päeva jooksul, siis aastal 2008 registreeriti

[1] A. Kukrus. Küberkuritegevuse tõkestamine infoühiskonnas. Arvutivõrgus: http://www.riigikogu.ee/rito/index.php?id=11319, 23. aprillil 2013.

[2] G. Stamatellos. Computer Ethics. Jones & Bartlett Publishers, 2007, p 14.

[3] Eesti Vabariigi 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 2013.

neid keskmiselt juba 1 päevas.[4] Aastal 2009 registreeriti 470 arvutikelmust, aastal 2010 oli neid 381 ja aastal 2011 kasvas arvutikelmuste arv 512-ni. 2011. aastal kasvas võrreldes 2010. aastaga kõige enam arvutikelmuste arv (+131). 2011. aastal suurenes põhiliselt interneti teel toime pandavate arvutikelmuste osakaal ning see trend on jätkunud ka 2012. aasta esimesel poolaastal.[5] 2012. aastal registreeriti aga 456 arvutikelmust. Teiste arvutikuritegude kohalt tasuks veel välja tuua, et kui aastal 2003 registreeriti 3 KarS §-s 178 sätestatud kuritegu (lapsporno valmistamine ja selle võimaldamine), siis aastal 2008 oli nende arv 52 ja aastal 2010 juba 76. Kui KarS § 206 järgi kvalifitseeritavaid kuritegusid (arvutiandmetesse sekkumine) registreeriti 2005. aastal 2 juhtumit, siis 2008. aastal oli neid juba 9 ja 2012. aastal 14. Statistikast nähtuvalt on populaarseks kuriteoks arvutisüsteemi ebaseaduslik kasutamine (KarS § 217). Selliseid kuritegusid pandi 2003. aastal toime 10, 2008. aastal 22 ja 2012. aastal juba 34.[6] Eeltoodud kuritegevuse statistika näitab ilmekalt, et arvutikuritegevus on aasta-aastalt suurenenud ja seetõttu tuleb ka sellele temaatikale suuremat tähelepanu pöörata.

Kuna arvutikuritegude sagenemine ja selle vastane võitlus on probleemiks paljudes riikides üle kogu maailma, siis siinkohal on oluline mainida, et ka Euroopa Liit on pidanud oluliseks arvutikuritegevusega seonduvat käsitleda ning on astunud küberkuritegevuse vastases võitluses jõulisi samme edasi. Näiteks alustas 11. jaanuaril 2013 tööd küberkuritegevuse vastase võitluse Euroopa keskus, mille eesmärk on kaitsta Euroopa kodanikke ja ettevõtteid küberkuritegevuse eest. Keskus asub Hollandis Haagis Euroopa Politseiameti (Europol) juures. Küberkuritegevuse vastase võitluse keskus aitab Euroopa Liidul tõhusamalt võidelda küberkuritegevusega ning kaitsta vaba, avatud ja turvalist internetti. Küberkurjategijad on nutikad ja kiired ning kasutavad uut tehnoloogiat kriminaalsetel eesmärkidel. Küberkuritegevuse vastase võitluse Euroopa keskus aitab meil olla neist osavamad ja kiiremad, et kuritegevust ära hoida ja selle vastu võidelda.[7] Keskusel peaks olema neli põhiülesannet: toimida küberkuritegevuse Euroopa teabekeskusena; Euroopa

[4] T. Reinthal. Küberkuritegevuse kohtupraktika Eestis, 2009. Arvutivõrgus: http://www.riigikohus.ee/vfs/899/Kyberkuritegevus%202009.pdf, 23. aprillil 2013.

[5] Justiitsministeerium, kriminaalpoliitika osakond. Kuritegevus Eestis 2011. aastal. Arvutivõrgus: http://www.just.ee/orb.aw/class=file/action=preview/id=56353/2011_statistika+kokkuv%F5te.pdf, 23. aprillil 2013.

[6] Justiitsministeerium, kriminaalpoliitika osakond. Registreeritud kuriteod Eestis 2003-2012. Arvutivõrgus: http://www.just.ee/57886, 23. aprillil 2013.

[7] Euroopa Komisjon. Pressiteade. 11. jaanuaril alustab tööd küberkuritegevuse vastase võitluse Euroopa keskus. Arvutivõrgus: http://europa.eu/rapid/press-release_IP-13-13_et.htm, 23. aprillil 2013.

küberkuritegevuse alaste eksperditeadmiste koondamine toetamaks liikmesriike suutlikkuse suurendamisel; abi liikmesriikidele küberkuritegude uurimisel; Euroopa küberkuritegude uurijate esindamine õiguskaitseorganite ja kohtuorganite tasandil.[8]

Lisaks eelnevale on Euroopa Liidul olemas ka küberkuritegevuse vastane tegevuskava. Selle raames on välja töötatud strateegiad, mille raames pannakse paika Euroopa Liidu ühine lähenemisviis digitaalvõrkude turbe, internetikuritegevuse tõkestamise ja tarbijakaitse küsimustes.[9]

Arvutikuritegevusega (sh arvutikelmused) võitlemine on ka tänapäeva Eesti üks suurimatest prioriteetidest, mida kinnitab asjaolu, et Eesti Vabariigi Riigikogu kiitis heaks kriminaalpoliitika arengusuunad aastani 2018. Nimetatud dokumendis tuuakse välja, et küberkuritegevuse vastane võitlus peab keskenduma alaealiste seksuaalse kuritarvitamise vastasele võitlusele, suurte arvutikelmuste tõkestamisele ning arvutiviiruste ja häkkimise leviku tõkestamisele. Küberkuritegevuse ennetamisel tuleb koostöös erasektoriga tegeleda haavatavate sihtrühmade (näiteks alaealised, eakad) teadlikkuse tõstmisega. Küberkuritegevuse paremaks piiramiseks tuleb tagada piisava hulga IT-spetsialistide olemasolu õiguskaitseasutustes.[10]

Käesolevas töös on kaks keskset küsimust:

1) Mis on arvutikelmus Eesti ja Euroopa Liidu õigusaktide järgi?
2) Kuidas sisustavad kohtud neid õigusaktides antud arvutikelmuse tunnuseid?

Et töö kesksetele küsimustele vastust leida, siis on käesolevas töös vajalik käsitleda ka alljärgnevaid küsimusi: kas Eesti seadusandlus on kooskõlas Euroopa Nõukogu poolt kehtestatud arvutikelmuse mõiste ja olemusega; millised on arvutikelmuse võimalikud toimepaneku vormid; millisel juhul tuleks kuritegu kvalifitseerida arvutikelmusena, millal arvutikelmustega seotud varavastaste süütegudena (kelmus, vargus, omastamine ja muud arvutikuriteod); kas Eesti kohtute praktika on arvutikelmuste kvalifitseerimise osas ühtne; kas ja kuidas on alama astme kohtute praktika arvutikelmuste osas kooskõlas Riigikohtu

[8] Komisjoni teatis nõukogule ja Euroopa Parlamendile. Võitlus kuritegevusega digiajastul: küberkuritegevuse vastase võitluse Euroopa keskuse loomine. Arvutivõrgus: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:ET:HTML, 23. aprillil 2013.

[9] Euroopa Komisjon. Küberkuritegevuse vastane ELi tegevuskava - 12/02/2013. Arvutivõrgus: http://ec.europa.eu/news/science/130212_et.htm, 23. aprillil 2013.

[10] Kriminaalpoliitika arengusuunad aastani 2018 heakskiitmine. – RT III 2010, 26, 51.

juhtnööride ja praktikaga. Käesoleva töö raames on oluline puudutada küberkuritegevusega seonduvat ka põhjusel, et arvutikelmuse mõiste sisustamiseks on vaja määratleda, mis üldse on arvutikuritegu.

Käesolev töö on jaotatud kolmeks peatükiks. Töö esimeses peatükis on kirjutatud arvutikuritegevusest (sh Euroopa Nõukogu küberkuritegevuse konventsioonist ja Eesti riiklikust küberjulgeoleku strateegiast) ning karistusseadustikus (edaspidi KarS) sätestatud arvutikuritegudest. Teine peatükk käsitleb arvutikelmuse mõistet, arvutikelmuse koosseisu kujunemist ning seda, kuidas eristada arvutikelmust teistest sarnastest arvutikuritegudest. Töö kolmas osa hõlmab arvutikelmuse sisustamist meie kohtupraktikas, alama astme ja riigikohtu praktikat ning viimasena nende kahe omavahelist analüüsi. Töö kolmas osa põhineb Eesti kohtute praktikal.

Käesolevas töös on kasutatud kombineeritud meetodit – kohtupraktika empiirilist analüüsi koos teoreetilises kirjanduses toodud käsitlusega.

Töö peamisteks allikateks on Euroopa Nõukogu koostatud materjalid, kus on sätestatud arvutikelmuse mõiste, mille analoog on Eestis kasutusele võetud arvutikelmuse mõiste. Lisaks sellele on osad töö dokumendid kättesaadavad arvutivõrgus, kuna Eestis on arvutikelmus alles viimasel ajal populaarsust kogunud kuriteotüüp. Kõige olulisema tähtsusega on aga Eesti erineva astme kohtute kohtulahendid ning erinevad artiklid arvutikelmuste ja arvutikuritegevuse kohta. Teoreetilised seisukohad põhinevad peamiselt karistusseadustiku kommenteeritud väljaandel ja J. Sootaki õpikul: Varavastased süüteod.

1. ARVUTIKURITEGEVUS

1.1 Arvutikuriteod

Viimaste aastakümnete jooksul on olnud maailmas elektrooniliste seadmete revolutsioon. Tehnoloogiad nagu mobiiltelefonid, piiparid, kodu-, süle- ja tahvelarvutid, internet ning veebileheküljed on lisanud kuritegevusele teise dimensiooni. Nimetatud dimensioon hõlmab endas võimalust sooritada teatud kuritegusid kauge maa tagant. Varavastased süüteod ei eelda enam seda, et kurjategija ja kannatanu kohtuvad näost näkku. Tänu tehnoloogia arengule võivad kurjategijad tänapäeval sooritada varavastaseid kuritegusid mugavalt iseenda kodus olles inimeste vastu, kes elavad kasvõi teisel pool maakera.

Interneti kasutamine illegaalsetel eesmärkidel ei tunnista sarnaselt paljude teiste kuriteoliikidega riigipiire ning selle läbi saadav tulu on võrreldav narkokaubandusega. Küberkurjategijad, ebaseadusliku sisuga serverid või veebileheküljed võivad ühel ajahetkel kuuluda küberruumi ühe jurisdiktsiooni alla ning järgmisel hetkel kolida juba üle järgmisesse ja nii edasi. See muudab küberkuritegevuse vastase võitluse eriti keeruliseks. Olukorras, kus on vajalik reaalajas toimuvate rünnete tõrjumine või kuritegude tõkestamine, omab kiire infovahetus ning kindlaksmääratud kontaktisikute võrgustik eriti suurt rolli. Rahvusvaheline koostöö on vajalik, et identifitseerida teistest riikidest pärit ründed ja kurjategijad ning võtta tarvitusele kaitsemeetmed. Lisaks sellele on edu võtmeks koostöö õiguskaitseasutuste ning erasektori vahel.[11]

Arvestades arvutikuritegevuse jõudsat kasvu ja selle kuriteoliigi spetsiifikat, siis 2001. aastal mõisteti, et arvutitega seotud kuriteod vajavad erilist regulatsiooni. Sellest ajendatuna kohtusid 26 riigi esindajad ning 2001. aasta 8. novembril võeti vastu Euroopa Nõukogu küberkuritegevuse konventsioon *(*Council of Europe Convention on Cybercrime). Tegemist on esimese rahvusvahelise lepinguga, mille objekt on interneti ja teiste arvutivõrkude vastu või abil sooritatud kuriteod. Konventsiooni eesmärk oli võtta vastu Euroopa Liidu tasandil asjakohane seadusandlus ja edendada rahvusvahelist koostööd arvutitega seotud kuritegevuse

[11] Eesti Vabariigi Siseministeerium. Küberkuritegevuse vastane võitlus. Arvutivõrgus: https://www.siseministeerium.ee/37266/, 23. aprillil 2013.

takistamiseks. Arvutikuritegevusvastase konventsiooni ratifitseerimise seaduse võttis Riigikogu vastu 12. veebruaril 2003 (RT II 2003, 9, 32). Konventsiooni ratifitseerinud riigid on kohustatud viima riigisisese õiguse vastavusse konventsiooniga. Õigusalane koostöö kriminaalasjades kuulub Euroopa Liidu (edaspidi EL) III samba ehk justiits- ja siseküsimuste alase koostöö valdkonda. III samba raames võib Euroopa Liit võtta vastu soovitusi, resolutsioone, ühisseisukohti, ühismeetmeid, raamotsuseid, konventsioone jms. Euroopa Liit avaldas konventsioonile otsest toetust Euroopa Liidu Nõukogu ühispositsiooni vastuvõtmise teel 27. mail 1999. Ühispositsiooni artikli 1 kohaselt toetavad Euroopa Liidu liikmesriigid konventsiooni eelnõu ning tagavad jurisdiktsiooni kehtestamise konventsioonis nimetatud rikkumiste üle. Arvutikuritegevusvastase konventsiooni preambula kohaselt on ühiskonna kaitseks küberkuritegevuse vastu esmatähtis ellu viia ühtset kriminaalpoliitikat, võttes vastu asjakohased õigusaktid ja edendades rahvusvahelist koostööd muul viisil.[12]

Euroopa Nõukogu küberkuritegevuse konventsiooni areng oli läbimurre rahvusvahelisel tasandil tehtavate juurdluste osas arvutikeskkonnas. Peale selle, et küberkuritegevuse konventsioon on seotud karistusõigusega, kohustab antud konventsioon osapooli kasutama erinevaid meetmeid arvutialastes juurdlustes. Need meetmed asuvad konventsiooni artiklites 14-22.[13]

Euroopa Nõukogu küberkuritegevuse konventsioon käsitleb nelja liiki arvutikuritegevusega seotud rikkumisi:

1) arvutiandmete ja -süsteemide konfidentsiaalsuse, puutumatuse ja kättesaadavuse vastu toimepandud süüteod;
2) arvutisüüteod;
3) lapspornoga seotud süüteod;
4) autoriõiguse ja autoriõigusega kaasnevate õiguste rikkumisega seotud süüteod.[14]

Esimese liigi alla (artiklid 2-6) on koondatud loata arvutisüsteemi või selle osasse sisenemine (nn häkkerlus), ebaseaduslik pealtkuulamine, arvutiandmete loata omastamine ja nendega manipuleerimine (nn Trooja hobuse tüüpi viiruste saatmine arvutisse), arvutisüsteemi

[12] A. Kukrus (viide 1).

[13] Council of Europe. Cyberterrorism – the Use of the Internet for Terrorist Purposes. Council of Europe Publishing, 2007, p 81.

[14] Council of Europe. Convention on Cybercrime. Budapest, 23.XI.2001. Arvutivõrgus: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm, 23. aprillil 2013.

toimimise tõsine takistamine, seadmete kuritarvitamine, s.t eelkõige küberkuritegude toimepanemiseks kavandatud ja kohandatud seadmete, k.a arvutiprogrammide (sh viirused) ja paroolide kättesaadavaks tegemine (s.o müük, kasutamiseks hankimine jms). Viimati nimetatud rikkumise (sätestatud artiklis 6) sanktsioneerimise eesmärk on häkkerite relvituks tegemine. Arvutisüüteod (artiklid 7-8) on arvutite abil tehtavad võltsingud (digitaalsete dokumentide võltsimine) ja pettused (kuulub majanduskuritegude valdkonda, sest peab olema sooritatud ärieesmärgil). Arvutikelmuse teel pannakse toime kõige rohkem pangapettusi ja rahapesukuritegusid. 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 ning lapsporno valdamine arvutisüsteemis või andmekandjal. Artikli 10 kahes esimeses lõikes on sätestatud konventsiooniosaliste kohustus kriminaliseerida tahtlikud arvutisüsteemi abil toimepandud autoriõiguse ja autoriõigusega kaasnevate õiguste rikkumised juhul, kui need pandi toime ärieesmärgil.[15]

Euroopa Nõukogu küberkuritegevuse konventsiooni käsitlemine on käesolevas töös oluline ka põhjusel, et just nimetatud konventsiooni artikkel 8 on pühendatud arvutikelmusele ja sealt pärineb arvutikelmuse mõiste Euroopa Liidu õiguses. Antud konventsiooni artikkel 8 sätestab järgmist: konventsiooniosaline võtab seadusandlikke ja muid meetmeid, et oma seaduses määratleda kuriteona teisele isikule varalise kahju tekitamine, kui selle eesmärk on kelmuse teel või muul ebaausal viisil ilma õigusliku aluseta saada endale või teisele isikule majanduslikku kasu ning kui tegu pannakse toime tahtlikult ja ilma õigusliku aluseta:
a) arvutiandmete sisestamise, muutmise või sulustamise teel või
b) arvutisüsteemi toimimisse sekkumise teel.[16]

Kuna arvutikuritegude toimepanemiste arv aasta-aastalt sageneb, arvutikuritegudes kasutatavad skeemid muutuvad aina keerulisemaks ja nimekirja lisandub uusi võimalusi arvutikuritegude toimepanemiseks, siis on tähtis astuda selle vastu võitlemiseks konkreetseid samme. Et inimestele arvutikuritegevuse eest kaitset pakkuda, on oluline, et iga riik võtaks vastu seadused, mille alusel on võimalik küberkurjategijaid vastutusele võtta. Samuti on

[15] A. Kukrus (viide 1).

[16] Arvutikuritegevusvastane konventsioon. – RT II 17.03.2003, 9, 32.

oluline arvutikuritegude piisavalt karm sanktsioneerimine, mis aitaks vältida arvutikuritegevuse edasist kiiret levikut.

Eesti karistusseadustikust võib leida kolmteist erinevat arvutiga seostatavat kuritegu. Nendeks on sõnumisaladuse rikkumine (KarS § 156), lapsporno valmistamine ja selle võimaldamine (KarS § 178), arvutiandmetesse sekkumine (KarS § 206), terminalseadmete identifitseerimisvahendi ebaseaduslik kõrvaldamine ja muutmine (KarS § 206^1) arvutisüsteemi toimimise takistamine (KarS § 207), nuhkvara, pahavara ja arvutiviiruse levitamine (KarS § 208), arvutikelmus (KarS § 213), arvutikuriteo ettevalmistamine (KarS § 216^1), arvutisüsteemi ebaseaduslik kasutamine (KarS § 217), ebaseaduslikult kõrvaldatud ja muudetud identifitseerimisvahendiga terminalseadme kasutamine (KarS § 217^1), ebaseaduslikult reprodutseeritud arvutiprogrammi valdamine (KarS § 222^1), terrorikuritegu (KarS § 237) ja kaitsekoodide üleandmine (KarS § 284). Karmim arvutikuritegudega seonduv sanktsioon on sätestatud KarS §-s 237, mis sätestab terrorikuriteo, sealhulgas ka arvutiterrorikuriteo eest võimalikuks maksimumkaristuseks eluaegse vangistuse. Kõikide nende kuritegude ühiseks jooneks on kuritegude toimepanemine arvutisüsteemi vahendusel.

1.2 Eesti riiklik küberjulgeoleku strateegia (mai 2008)

Kuigi Eestis on selgelt ja üheselt teadvustatud infosüsteemide kaitse vajadust arenevas infoühiskonnas, pole selleks võetud meetmed olnud alati piisavad. Terve riigi küberjulgeoleku tagamine nõuab kogu ühiskonna kaasamist. Peame teadvustama, et infosüsteemide kasutusega kaasnevate riskide ja infotehnoloogia laialdase kasutamise tasakaalustamine on väljakutse mitte ainult Eestis, vaid kogu maailmas.[17]

2007. aastal oli 51% Eesti leibkondadest varustatud kiiret interneti-ühendust võimaldava lairiba püsiühendusega. Kuna igas leibkonnas on mitu arvutikasutajat, on reaalne kodukasutajate suhtarv ligikaudu 70% kogu elanikkonnast.[18] Kuna enamik meist puutuvad kas vabal ajal või oma töös kokku arvutitega, siis võivad arvutikuriteod mõjutada paljusid meist, kuna internetikeskkonnas varitsevad ohud, millest ei olda tihtilugu vähese

[17] E. Pära. Arvutikelmused ja nendega seonduvad varavastased süüteod aktuaalses kohtupraktikas. Bakalaureusetöö. Tallinn, 2010, lk 12-13.

[18] Uuring „Avalike e-teenuste kasutamine". TNS Emor, oktoober 2007. Arvutivõrgus: http://www.riso.ee/et/files/avalike_e-teenuste_kasutamine_aruanne.pdf, 23. aprillil 2013.

informeerituse tõttu teadlikud. Seega on küberjulgeoleku strateegia oluline mitte ainult riigile, vaid meile kõigile. Suuremat tähelepanu tuleks pöörata tavakodanikele suunatud teavitustööle, et nad oleksid teadlikud, millised ohud neid küberruumis varitsevad ja kuidas end nende eest paremini kaitsta.

Arvutikuritegusid on tihtilugu väga raske tuvastada, sest arvuti taga on varjatud isik, kes võib oma tegevuse jälgi oskuslikult peita ja sellist isikut on raske tuvastada. Kuna Eesti koges laiaulatuslikke küberrünnakuid 2007. aasta kevadel, siis peale seda hakkas Eesti Vabariigi Valitsus koostama oma küberjulgeoleku strateegiat, mis valmis 2008. aasta mais. Muuhulgas defineerib antud strateegia nii riikliku tähtsusega küberkuritegevuse vastu võitlemise eesmärke kui ka tähtsustab koostööd erasektoriga.[19] Küberkaitse julgeoleku strateegia[20] mõte on iseenesest hea - inimesi tuleks tõesti küberruumis valitsevate ohtude eest teavitada, kuid kahjuks ei ole selles vallas laiahaardelist teavitustööd läbi viidud. Teavitustöö võiks olla suunatud just vanuritele, alaealistele või siis algajatele arvutikasutajatele, kuna nemad on isikud, kes ei oska end tavaliselt internetis peituvate ohtude eest kaitsta. Teavitustöö võiks olla laiaulatuslikum ja intensiivsem ning sellekohaseid artikleid ning kajastusi võiks aktiivsemalt massimeedias kajastada, kuna võib eeldada, et enamik meist küberkaitse strateegiat lugema ei satu ja iseseisvalt küberruumis valitsevate ohtude kohta informatsiooni ei otsi.

Inimesi tuleks teavitada sellest, et ei tasu oma isiklikke andmeid, krediitkaardi andmeid või pangakoode Internetis ühelgi leheküljel avalikult levitada. Lisaks sellele tuleks hoiatada, et tundmatult aadressilt tulnud kirjade avamine ja nendele vastamine võib olla seotud peidetud riskidega. Eriti tähtsaks peab autor alaealiste teavitamist, kuna viimasel ajal on meedia kajastanud väga palju juhtumeid, kus noored on saatnud endast arvuti teel kompromiteerivaid pilte või raha tundmatule isikule teisel pool arvutit, kes on siis pilte kuritarvitanud või rahaga lihtsalt kadunud ja hiljem tuleb välja, et tegu oli lihtsa pettusega.[21] Teavitustöö olulisust peaks tõestama ka järgnev fakt: umbes 85% arvutikelmustest ei teatata, kuna tuntakse piinlikkust, kardetakse avalikkuse halvustamist või vale isiku süüdistamist ja teatakse, et üleüldse on kellegi süüd raske tõestada.[22]

[19] Council of Europe. Cyberterrorism – the Use of the Internet for Terrorist Purposes. (viide 20), p 47.

[20] Küberjulgeoleku strateegia komisjon. Küberjulgeoleku strateegia 2008-2013. Kaitseministeerium, 2008. Arvutivõrgus: http://www.valitsus.ee/failid/kuberjulgeolek.pdf, 24. aprillil 2013.

[21] E. Pära (viide 17), lk 13-14.

[22] R. J. McMahon. Partial Handbook for Private Investigators. CRC Press, 2001, lk 114.

Eesti on kindlasti õigel teel küberkaitse tähtsuse teadvustamisega, kuid kahjuks üksnes sellest veel ei piisa, sest teoorias on küberkaitse strateegia hea, kuid nüüd tuleb seda rakendada ka praktikas: inimeste teadlikkust tuleb hakata tõstma läbi avalike kampaaniate ning teavitustöö. Lisaks sellele pakub töö autor välja, et võiks olla üks kindel aadress, kuhu arvutikuritegude (sh ka arvutikelmuste) ohvriks langenud isikud saaksid oma murest anonüümselt kirjutada, eeldusel, et neil on olemas kindlad tõendid, et oma seisukohti tõestada. Dokumentaalseteks tõenditeks kirjade näol võiksid olla näiteks petturliku oksjoni puhul ostule eelnev ning järgnev kirjavahetus müüjaga ning pangaülekande tõestus, et tellitud asja eest maksti, kuid pakk ei ole kunagi kohale jõudnud, mida saaks kindlaks teha läbi postiasutuste. Kuna eelnevalt sai juba mainitud, et paljud arvutikuritegude ohvriks langenud isikud tunnevad häbi või kardavad asjaolude avalikuks tulemist, siis võiks olla koht, kuhu oma murest anonüümselt kirjutata ja loomulikult peaks piisavate tõendite olemasolul asja uurima politsei.[23]

Eelneva idee sai teksti autor arvutialasest õiguskirjandusest: Internetikelmuste kaebuste keskus, mis on FBI üks allüksustest, teatab, et oksjonitega seotud kelmused on nüüd arvutikelmustest esikohal. Eelmine aasta logis antud internetilehekülgele 7193 kasutajat, kes teatasid oma arvutikelmuse ohvriks sattumisest ning nendest alla kümne protsendi esitasid kaebuse ka politseisse. Põhjus, miks see protsent nii väike on, seisneb selles, et ohvrid tunnevad tavaliselt end häbistatult ja nad ei tea, kuhu edasi pöörduda.[24]

Siinkohal ei saa jätta mainimata, et 21. märtsil 2013 kiitis Eesti Vabariigi Valitsus heaks ka „Küberjulgeoleku strateegia 2014–2017“ koostamise ettepaneku. Strateegia koostamise eesmärk on leppida kokku ja luua tingimused selleks, et kasutada infotehnoloogiast tulenevaid võimalusi tõhusalt ja turvaliselt. Koostatava strateegia eesmärgid peavad järgima põhimõtted, mille alusel:

- Strateegia sätestab infotehnoloogiaga seotud riskide tundmise, haldamise ning maandamise üldised riiklikud eesmärgid ning viisid ja vahendid nende eesmärkide saavutamiseks.
- Strateegia kohaselt peab ühiskond aktsepteerima infotehnoloogiaga seotud riskide olemasolu, olema nendest teadlik ning haldama ja maandama neid teadmuspõhiselt.

[23] E. Pära (viide 17), lk 14.

[24] W. Koletar. Fraud Exposed. John Wiley and Sons, 2003, lk 49.

- Strateegia seab üheks eesmärgiks Eesti rahvusvahelise konkurentsivõime tõstmise, efektiivse riigivalitsemise ja majandusliku arengu stimuleerimise just infotehnoloogiliste riskide parema tundmise kaudu.
- Tehnoloogia ja selle rakendamisega seotud riskide uurimine võimaldab riske tunda ja täpsemalt hallata ning vältida teadmiste puudumisest või eelarvamustest tingitud hirmu uute tehnoloogiate rakendamise ees. Selleks on aga hädavajalik kogu ühiskonna IKT alaste teadmiste tõstmine ning vastava hariduse ja teadustöö koordineeritud arendamine.[25]

[25] Lühikokkuvõte. „Küberjulgeoleku strateegia 2014-2017“ koostamise ettepanek Vabariigi Valitsusele. Arvutivõrgus: https://valitsus.ee/UserFiles/valitsus/et/valitsus/arengukavad/majandus-ja-kommunikatsiooniministeerium/K%C3%BCberjulgeoleku%20arengukava%20koostamise%20ettepanek_lyhikokkuvote.pdf, 23. aprillil 2013.

2. ARVUTIKELMUS JA SELLE MÕISTE KARISTUSSEADUSTIKUS

2.1 Arvutikelmus ja selle koosseisu kujunemine

Kelmus on üks olulisemaid varavastaste süütegude liike, mis on suunatud vara vastu kitsamas mõttes (KarS 13. Ptk 2. J). Võrreldes varasema, kriminaalkoodeksijärgse karistusõigusega ei ole seadusandja kehtivas õiguses piirdunud üksnes kelmuse üldkoosseisu (KarS § 209) nimetamisega, vaid on selle kõrvale konstrueerinud veel mitu kelmuse eriliiki (§ 210 soodustuskelmus, § 211 investeerimiskelmus, § 212 kindlustuskelmus ja § 213 arvutikelmus), mis on kelmuse üldkoosseisu suhtes erinormid ega moodusta seetõttu esimesega kogumit. Kelmuste toimepanemiseks loovad soodsa pinnase ka moodsa majandustegevuse mitmekesisus ja kõikvõimalikud nüüdisaegsed tehnoloogiad ja lahendused (nt interneti-pank), mis ühelt poolt on määratud lihtsustama inimeste igapäevaelu, kuid teiselt poolt moodustavad ka täiesti unikaalse keskkonna kuritegevuseks.

Et aru saada, miks meie karistusseadustikus eraldi arvutikelmuse koosseisu vaja läheb, siis selleks tuleb kõigepealt käsitleda kelmuse koosseisu. Kelmuse põhikoosseisu (KarS § 209) puhul viiakse isik pettuse teel eksitusse (luuakse reaalsetest asjaoludest ebaõige pilt), mille tulemusena isik loovutab vara vabatahtlikult. KarS § 209 annab kelmuse põhikoosseisu järgmises sõnastuses: varalise kasu saamise eest tegelikest asjaoludest teadvalt ebaõige ettekujutuse loomise teel.[26] KarS-s sätestatud kelmuse ja kelmuse alaliikide puhul on oluline teise isiku eksitusse viimine. Pettus tähendab teise isiku kujutluse ehk intellektuaalse arusaama mõjutamist, millega kutsutakse esile esimus, toetatakse olemasoleva eksimuse edasikestmist või tugevdatakse seda. Pettuslik tegu ehk petmistoiming ehk petmine on tõele mittevastava asjaolu esitamine.[27] Tsiviilõigus määratleb pettust kui isiku eksimusse viimist või eksimuses hoidmist temale ebaõigete asjaolude avaldamise teel (TsÜS § 94 I).[28] Kelmuse koosseisuelementideks loetakse ka varakäsutust ja varalist kahju[29], mida seaduses otsesõnu

[26] Karistusseadustik. – RT I, 17.04.2013, 8.

[27] J. Sootak. Varavastsed süüteod. Juura, 2003, lk 121.

[28] Tsiviilseadustiku üldosa seadus. – RT I, 06.12.2010, 12.

[29] RKKKo 01.03.2010, nr 3-1-1-2-10, p 6.

kirjas ei ole. See tähendab karistatavate tegude ringi kitsendamist seaduse kirjatähest tulenevaga võrreldes, nii et *nullum crimen sine lege* põhimõtet rikutud ei ole. Seega koosneb kelmuse objektiivne koosseis neljast elemendist. Need on: petmine, eksimus, varakäsutus, varaline kasu (kannatanu varalise kahju arvelt)[30]. Need neli elementi peavad olema põhjuslikus seoses. Petmine peab seega kannatanu eksitusse viima, eksimus peab olema kannatanu poolt oma varakäsutuse põhjuseks, mistõttu süüdlane saab varalist kasu kannatanu varalise kahju arvelt.[31] Subjektiivsest küljest eeldab kelmus tahtlust koosseisu kõigi asjaolude suhtes.[32]

Arvutikelmus sarnaneb kelmusega selle poolest, et nagu kelmusegi puhul, siis on ka arvutikelmuse koosseisuga kaitstav õigushüve vara.[33] Arvutikelmuse näol on koosseisutüübilt tegu materiaalse kuriteokoosseisuga – andmetöötlusprotsessi sekkumisega (tegu) peab süüdlane olema saanud varalist kasu (tagajärg).[34] Arvutikelmuse objektiivne koosseis on varalise kasu saamine lubamatu sekkumise teel andmetöötlusprotsessi. Koosseis annab nimetatud sekkumise vormide mitteammendava loetelu.[35] Andmetöötlusprotsessi sekkumiseks ei ole vaja, et andmetöötlusprotsess oleks juba toimunud. Ka andmetöötlusprotsessi lubamatul käivitamisel on andmetöötlusprotsessi sekkutud. Ei ole oluline, mil viisil andmetöötlusprotsessi sekkutakse, nõutav on, et sekkumise tagajärjel saab sekkuja varalist kasu.[36] Subjektiivsest küljest eeldab antud süütegu tahtlust koosseisu kõigi asjaolude suhtes. Koosseis on täidetud, kui isik tegutseb vähemalt kaudse tahtlusega.[37] Siinkohal tuleks täpsustuseks mainida, et arvutiandmed tähendavad käesolevas paragrahvis igasugust faktide, teabe või mõistete esitust infosüsteemi töötlemiseks sobivas vormis. Käesoleva paragrahvi mõistes ei hõlma andmed arvutiprogramme. Programm tähendab käesolevas paragrahvis süntaktilist üksust, mis vastab mingi programmikeele reeglitele ning koosneb teatava automatiseeritud andmetöötlusfunktsiooni täitmiseks vajalikest deklaratsioonidest ja lausetest või käskudest[38], mille kohaselt arvutisüsteem teostab

[30] RKKKo 10.11.2009, nr 3-1-1-87-09, p 12.

[31] K. Aas, N. Aas, M. Hirvoja, K. Siitam. Karistusõigus. Eriosa. Sisekaitse Akadeemia kirjastus, 2002, lk 55.

[32] Karistusseadustik. Komm vln § 209 komm 22.

[33] Karistusseadustik. Komm vln § 209 komm 1.

[34] Karistusseadustik. Komm vln § 213 komm 1.2.

[35] Karistusseadustik. Komm vln § 213 komm 2.1.

[36] Karistusseadustik. Komm vln § 213 komm 2.2.

[37] Karistusseadustik. Komm vln § 213 komm 3.

[38] Official Journal L 069, 16/03/2005 P.0067-0071. Arvutivõrgus: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:ET:HTML, 01. mail 2013.

automaatset andmetöötlust.[39] Muutmine tähendab, et olemasolevad andmed või programm asendatakse teiste andmete või programmiga. Kustutamine tähendab, et olemasolevad andmed või programm kõrvaldatakse arvutisüsteemist. Rikkumine tähendab, et andmetesse või programmi tehakse muudatus, mis teeb võimatuks andmete või programmi kasutamise nende esialgseks otstarbeks või raskendab seda. Sulustamine tähendab, et andmed ja programmid säilivad arvutisüsteemis, kuid arvutisüsteemi kasutaja ei saa neid kasutada, kuna juurdepääs nendeni on takistatud. Muutmine, kustutamine, rikkumine või sulustamine on lõpule viidud sõltumata sellest, et tehtud muudatust on informatsiooni valdamisel võimalik väga kiiresti kõrvaldada ja algset situatsiooni taastada. Andmete või programmi arvutisüsteemi sisestamine tähendab nende arvutisüsteemi kandmist andmetöötlusprotsessiks või säilitamiseks.[40]

Eeltoodust nähtub, et nii kelmuse kui ka arvutikelmuse koosseis eeldab konkreetse varalise kahju tekkimist. Erinevalt kelmuse koosseisust, arvutikelmuse koosseis petmistoimingut ja sellega inimese eksitusse viimist ei nõua. Tingimuseks on ainult pettusetaoliste manipulatsioonide tegemine arvutil.[41] Arvutikelmuse erinormi järele on vajadus just seetõttu, et arvutikelmuse puhul on raske leida isikut (see võib ka puududa), kelles luuakse ebaõige ettekujutus tegelikest asjaoludest, mis on vajalik kelmuse üldkoosseisu kui suhtesüüteo puhul.[42] Antud asjaolu viitab ilmselt ka sellele, miks ei ole arvutikelmuse koosseisu iseloomulikuks tunnuseks petmistoiming, olgugi, et koosseis sisaldab mõistet „-kelmus“ – nimelt on eestikeelses õiguskirjanduses lisaks järeldusele, et arvutikelmuse puhul on raske määratleda petetud isik, jõutud dogmaatiliselt õigele järeldusele, et petta ei saa ka süüteo toimepanemiseks kasutatavad vahendit.[43]

Riigikohtu kriminaalkolleegium puutus esmakordselt juba 1999. aastal kriminaalkoodeksi kehtimise ajal kokku kelmuse ja arvutikelmuse piiritlemise probleemidega. Riigikohtu lahendist nr 3-1-1-2-99 nähtub, et Tartu Linnakohus mõistis M. Leego ja E. Leego muuhulgas süüdi kelmuses selles, et E. Leego võttis Tartu linnas telefoni ja modemi teel Telehansa teenust ning AS Tapila identifitseerimistunnust ja paroole kasutades ühendust AS-ga

[39] Karistusseadustik. Komm vln § 206 komm 5.

[40] Karistusseadustik. Komm vln § 206 komm 6.

[41] Prof. dr. E. Samson. Kriminaalõiguse eriosa 2. osa. Abimaterjal kohtunike ja prokuröride järelkoolituse karistusõiguse õppegrupile, 2000, lk 27. Arvutivõrgus: http://www.just.ee/orb.aw/class=file/action=preview/id=10714/krimoiguse+eriosa+II.pdf, 24. aprillil 2013.

[42] Karistusseadustik. Komm vln § 213 komm 1.1.

[43] J. Sootak (viide 27), lk 165.

Hansapank ning andis korralduse kanda AS Tapila arveldusarvelt AS Voineki ja K. Ummeri arvetele kokku 467 506,35 krooni, millest M. Leego ja E. Leego võtsid suurema osa sularahana välja. Tartu Ringkonnakohus jättis Tartu Linnakohtu otsuse selles osas muutmata. Kassatsioonkaebuses vaidlustasid süüdistatavad karistuse kelmuse täideviimise eest ja palusid süüdistatavad kelmuses õigeks mõista põhjusel, et süüdistatavate tegu vastavat hoopis arvutikelmuse koosseisule. Probleem seisnes selles, et kuna kriminaalkoodeksit täiendati arvutikelmuse sättega (§ 268) alles 12. märtsil 1997 st. pärast süüdimõistetule inkrimineeritud kelmuse toimepanemist, siis kassatsioonkaebuses leiti, et süüdistatav tuleks kelmuses õigeks mõista, kuna tema tegu ei vastavat enam nn. puhta kelmuse faktilisele koosseisule, vaid arvutikelmusele, mille mõiste aga süüdimõistva otsuse tegemise hetkel kriminaalkoodeksist puudus. Kassatsioonkaebuses väideti, et eeltoodust tulenevalt ei olnud Eestis enne 12. märtsi 1997. a põhimõtteliselt võimalik arvutit kasutades panna toime kelmust - so KrK §-s 143 ettenähtud kuritegu. Riigikohus aga leidis, et kassatsioonikaebusel puudub alus, kuna ei saa põhjendatuks lugeda väidet, et enne 12. märtsi 1997 ei olnud põhimõtteliselt võimalik Eestis arvutit kasutades toime panna kelmust. Kriminaalkoodeksi eriosa täiendamine uute paragrahvidega ei pruugi mitte alati tähendada selliste tegude esmakordset kriminaliseerimist, mis varem ei olnud üldse kriminaalõiguslikult relevantsed. Seadusandja võib lülitada kriminaalkoodeksisse uusi paragrahve ka olemasolevaid paragrahve osadeks jagades, eesmärgiga diferentseerida kriminaalvastutust. Siinkohal oleks kohatu väita, et kuna eelnevalt oli kriminaalkoodeksis sätestatud vaid kelmus, siis arvuti vahendusel toime pandud kelmus ei ole karistatav hariliku kelmuse paragrahvi järgi. Antud hetkel ei ole oluline, et arvutikelmust paragrahv lisati alles hiljem kriminaalkoodeksisse. Arvutikelmuse kui kuriteo diferentseerumine kriminaalkoodeksi eriosa iseseisvasse paragrahvi ei välista kriminaalvastutust diferentseerumise eelselt arvuti vahendusel toimepandud kelmuse eest. Lisaks eelnevale pidas Riigikohus oluliseks rõhutada, et nimetatud kriminaalasja kontekstis ei seisnenud kohtuotsustega tõsikindlalt tuvastatu kohaselt süüaluste poolne kelmus mitte üksnes ebaseaduslikes arvutimanipulatsioonides. Ebaseaduslik arvutikorraldus raha ülekandmiseks teatud arveldusarvetele oli kohtuotsustega tuvastatu kohaselt vaid üks lüli süüdimõistetute kelmuslikus käitumises. Lisaks sellele hõlmas kõnealune kuritegelik käitumine ka väära identiteedi all arvete avamist pangas, samuti ebaseaduslike arvutimanipulatsioonide tulemina arvetele kantud sularaha väljavõtmist.[44]

[44] RKKKo 5.01.1999, nr 3-1-1-2-99, p 1.

Eeltoodud kohtuotsusest nähtub, et Riigikohtu hinnangul võis arvutikelmuse koosseisule vastav tegu enne arvutikelmuse koosseisu kehtestamist vastata kelmuse koosseisule ehk arvutikelmuse koosseisu kehtestamine ei tähenda seda, et sellele vastavad teod ei oleks enne olnud karistatavad. Siinkohal tuleb mainida, et nimetatud Riigikohtu otsus on tegelikult lakooniline ja üsnagi rünnatav, kuna Riigikohus ei näidanud ära, kuidas kelmuse koosseis täideti. Käesoleval juhul võis tõesti M. Leego ja E. Leego tegu olla käsitatav kelmusena põhjusel, et nad võtsid kannatanu identifitseerimistunnust ja paroole kasutades ühendust AS-ga Hansapank ja andsid korralduse kanda kannatanu arveldusarvelt kolmandate isikute arvetele raha. Nimetatud rahaülekanded tegi teisel pool telefonitoru inimene ehk praegusel juhul on meil olemas konkreetne isik, keda M. Leego ja E. Leego petsid. Kui nad oleksid aga sisestanud kannatanu identifitseerimistunnuse ja paroolid näiteks internetipanka ja oleksid sealt kolmandate isikute pangakontodele ülekandeid teinud, siis ei oleks võimalik nende tegu kelmusena käsitleda, kuna puudub isik, keda eksitatakse. Arvutit ei ole võimalik eksitada.

Eeldatavasti ajendas just arvutikelmuste sagenemine, selleliigilise kelmuse spetsiifika ning suurem ohtlikkus Eesti seadusandjat arvutikelmuse spetsiifiliseks, rangemat kriminaalvastutust ettenägevaks regulatsiooniks kriminaalkoodeksi (edaspidi KrK) § 268. Nagu nähtub ka eespooltoodud Riigikohtu lahendist, siis arvutikelmus kriminaliseeriti Eestis alles 12. märtsil 1997. Enne arvutikelmuse mõiste defineerimist kriminaalkoodeksis rakendusid arvutite vahendusel toime pandud kuritegude puhul tavalised varavastased koosseisud nagu kelmus või vargus. KrK § 268 kohaselt loeti arvutikelmuseks võõra vara, varalise eelise või muu kasu saamise eest arvutiprogrammide või andmete sisestamise, vahetamise, kustutamise või blokeerimise või muul viisil andmetöötlusprotsessi sekkumise teel, mis mõjutab andmete töötlemise tulemust ja põhjustab teise isiku omandile otsest varalist või muud kahju. Kriminaalkoodeksi kohaselt karistati arvutikelmuse toimepanijat rahatrahvi või arestiga või vabadusekaotusega ühest kuni kuue aastani.[45]

Enne 24.03.2008 nägi arvutikelmuse objektiivne koosseis KarS §-s 213 välja järgmine: varalise kasu saamise eest arvutiprogrammide või andmete ebaseadusliku sisestamise, vahetamise, kustutamise, sulustamise või muul viisil andmetöötlusprotsessi ebaseadusliku sekkumise teel, kui sellega on mõjutatud andmete töötlemise tulemust, – karistatakse rahalise karistuse või kuni viieaastase vangistusega,[46] kuid seda muudeti 24.03.2008 eelnõuga 166 SE

[45] Andmekogude seadus. – RT I 1997, 28, 423.

[46] Karistusseadustik. – RT I 2001, 61, 364

I. Eelnõu seletuskirja kohaselt oli karistusseadustiku muutmise seaduse eesmärk viia Eesti karistusseadustiku arvutikelmuse koosseis Euroopa Nõukogu arvutikuritegevusvastase konventsioonis (edaspidi konventsioon) oleva arvutikelmuse mõiste ja koosseisuga vastavusse. Samuti oli eesmärgiks täpsustada arvutisüsteemi vastu suunatud rünnetega seotud kuriteokoosseise ning korrigeerida kuritegude eest mõistetavaid karistusi.[47] Enne 24.03.2008 puudus KarS-s sätestatud arvutikuritegude puhul juriidilise isiku vastutus nii konventsioonis kui ka raamotsuses sätestatud kuritegude toimepanemise eest, lisaks ka konventsioonis sätestatud kohustus kriminaliseerida arvutikuritegude ettevalmistamine. Eelnõuga nähti ka ette rangemad sanktsioonid arvutikuritegude toimepanemise eest, kuna tegemist on raskesti avastatavate kuritegudega ning nende arv vaid kasvab.[48]

Kuna praegu on arvutikelmuse sõnastus KarS §-s 213 järgmine: arvutiprogrammi või andmete ebaseadusliku sisestamise, muutmise, kustutamise, rikkumise, sulustamise või muul viisil andmetöötlusprotsessi ebaseadusliku sekkumise teel. Lisaks eeldab subjektiivne koosseis varalise kasu saamise eesmärki,[49] siis sellest tulenevalt näeme, et peale 24.03.2008 tehti arvutikelmuse paragrahvi sõnastuses järgnevad muudatused – nimelt eemaldati lause fraas: „...kui sellega on mõjutatud andmete töötlemise tulemust.“ Samuti on lisatud säte selle kohta, et kui arvutikelmuse toimepanija on juriidiline isik, siis on ka teda võimalik arvutikelmuse toimepanemise eest vastutusele võtta ning teda karistatakse rahalise karistusega. Esimest muudatust saab põhjendada järgmiselt: andmetöötlusprotsessi sekkumiseks ei ole vaja, et andmetöötlusprotsess oleks juba toimunud. Ka andmetöötlusprotsessi lubamatul käivitamisel on andmetöötlusprotsessi sekkutud. Ei ole oluline, mis viisil andmetöötlusprotsessi sekkutakse, nõutav on, et sekkumise tagajärjel saab sekkuja varalist kasu.[50] Sõnastuse lihtsustamiseks ja mõttekordusest hoidumiseks eemaldati ebavajalik lause, kuna karistusseadustikus toodud arvutikelmuse (§ 213) sisu ja mõtet see tegelikult ei muutnud. Seega saab öelda, et kuivõrd esmapilgul võib tunduda, et tegu oli üksnes kosmeetilise muudatusega, siis tegelikult langes üks tõendamist vajav asjaolu (et andmete töötlemise tulemust oleks muudetud) ära. Juriidilise isiku vastutuse lisamine oli aga igati vajalik ja

[47] H. Loot. Karistusseadustiku muutmise seaduse eelnõu seletuskiri. Arvutivõrgus: http://www.riigikogu.ee/?op=emsplain&page=pub_file&file_id=85a4d8e5-2c8a-0faf-b0e9-3ff75214ffbf&, 01. mail 2013.

[48] *ibid.*

[49] Karistusseadustik. – RT I, 17.04.2013, 8.

[50] Karistusseadustik. Komm vln § 213 komm 2.2.

mõistlik, kuna ka nemad võivad arvutikelmusi toime panna ning peavad selle eest vastutama samamoodi nagu füüsilised isikud.

Kui võrrelda Euroopa Liidu tasandil eksisteerivat arvutikelmuse mõistet Eesti karistusseadustikus oleva arvutikelmuse mõistega, siis märkame, et KarS §-s 213 on päris sarnane konventsioonis oleva arvutikelmuse käsitlusega. Eesti KarS-s puudub otsesõnu varalise kahju tekitamine kellelegi, kuid on välja toodud arvutikelmuse toimepanija varalise kasu saamine. Ometigi on tegu põhimõtteliselt kokkulangeva mõttega, kuna sisuliselt kuulub kelmuse objektiivsesse koosseisu ka varalise kasu saamise pöördkülg – varalise kahju tekkimine kannatanul. Teine nn kirjutamata koosseisutunnus on kannatanu varakäsutus, mis seob eksimust ning varalise kahju tekkimist. Subjektiivsest küljest on kelmus tahtlik kuritegu.[51] Viimati muudeti siis karistusseadustiku arvutikelmuse sätet (§ 213) selliselt, et lisati juurde juriidilise isiku vastutus ning eemaldati arvutikelmuse olemusest tulenev mõttekordus. Kui võrrelda konventsioonis olevat arvutikelmuse koosseisu karistusseadustikus toodud arvutikelmuse koosseisuga, siis erinevad koosseisude sõnastused selle poolest, et karistusseadustikus ei ole KarS §-s 213 otsesõnu sätestatud subjektiivse koosseisu elementi ehk tahtluse olemasolu. Nimetatu on aga seletatav sellega, et karistusseadustiku üldosas ehk § 15 lg-s 1 märgitakse, et kuriteona on karistatav üksnes tahtlik tegu, kui käesolev seadustik ei sätesta karistust ettevaatamatu teo eest.[52] Seetõttu puudub vajadus, et arvutikelmuse koosseisus oleks tahtlus eraldi välja toodud.

2.2 Arvutikelmuse eristamine sarnastest arvutikuritegudest

Peale kelmuse põhikoosseisu leidub veel teisigi koosseise, mille puhul võib tekkida piiritlemisprobleeme. Sellest tulenevalt on siinkohal oluline lühidalt peatuda ka teistel arvutikuritegudel, milliste koosseisud võivad esmapilgul arvutikelmuse koosseisuga sarnased tunduda.

Esmapilgul võiks tekkida probleem arvutikelmuse (KarS § 213) ja arvutiandmetesse sekkumise (KarS § 206) piiritlemisega. Arvutiandmetesse sekkumise objektiivne koosseis on arvutisüsteemis olevate andmete või programmi ebaseaduslik muutmine, kustutamine, rikkumine või sulustamine; samuti arvutisüsteemi andmete või programmi ebaseaduslik

[51] J. Sootak (viide 27), lk 116-117.

[52] Karistusseadustik (viide 49).

sisestamine. Tagajärg ei ole lg 1 koosseisutunnus ning teo lõpuleviimiseks ei ole isegi vajalik, et arvutisüsteemi töö saaks reaalselt häiritud.[53] Lg 2 ehk raskendava koosseisu moodustab kuritegu elutähtsa valdkonna arvutisüsteemi vastu või kui sellega on tekitatud oluline kahju.[54] Arvutiandmetesse sekkumise poolt ohustatav õigushüve on arvutisüsteemi omaniku ja õiguspärase valdaja õigus vallata, kasutada ja käsutada arvutisüsteemi. Koosseisutüübilt on tegemist formaalse kuriteokoosseisuga.[55] KarS § 206 ja § 213 piiritlemisprobleem tekib põhjusel, et tegu on nende kahe koosseisu puhul sama, kuid erinevuse tingib see, et KarS § 213 näeb ette ka tagajärje ja on sellisena erinorm KarS § 206 suhtes. KarS § 206 ja KarS § 213 koosseisudega kaitstakse ka erinevaid õigushüvesid. Kui arvutiandmetesse sekkumise koosseisuga kaitstakse arvutisüsteemi omaniku ja õiguspärase valdaja arvutisüsteemiga seotud õiguseid, siis arvutikelmuse koosseisuga kaitstakse aga vara. Samuti on oluline mainida, et arvutiandmetesse sekkumise puhul ei ole oluline mingi tagajärje saabumine ega varalise kasu saamine (piisab sekkumisest), kuid arvutikelmuse puhul on oluline, et andmetöötlusprotsessi sekkumisega peab teo toimepanija saama varalist kasu. Riigikohus käsitles esmakordselt lahendis nr 3-1-1-114-12 KarS § 213 ja § 206 piiritlemist. Riigikohus leidis, et kuigi KarS § 213 kohaldamine on käesoleval juhul varalise kasu mittesaamise tõttu välistatud, siis tuleb tähelepanu pöörata asjaolule, et süüdistatav sisestas ettevõtte tuvastuskoodid 03.12.2009 internetipanka ebaseaduslikult. Kuriteona on karistatav ka üksnes andmete ebaseaduslik sisestamine arvutisüsteemi (KarS § 206 lg 1).[56] Kuigi arvutisüsteemis olevate andmete või programmi ebaseaduslik muutmine, kustutamine, rikkumine või sulustamine, samuti arvutisüsteemi andmete või programmi ebaseaduslik sisestamine on KarS § 206 lg 1 järgi karistatavad kuritegudena, tuleb selle sätte kohaldamisel silmas pidada asjaolu, et samaaegselt sätestab KarS § 218 lg 1 samade tegude toimepanemise eest väärteokaristuse. Kuna KarS § 206 lg 1 on formaalne delikt ja selle koosseisualternatiivid kattuvad KarS §-s 213 loetletud koosseisualternatiividega, võib tõusetuda küsimus veel KarS § 213 lg 1 katse ja KarS § 206 lg 1 (õigemini küll KarS § 218 lg 1) piiritlemise kohta. Abistavaks kriteeriumiks saab siin olla üksnes subjektiivne koosseis ehk kas isikul oli tahtlus varalist kasu saada. Olukorras, kus isikul on andmete ebaseadusliku sisestamise hetkel tahtlus sel teel varalist kasu saada, kuid see tagajärg jääb isiku tahtest sõltumatult saabumata, tuleb isik võtta vastutusele arvutikelmuse katse eest. Kuna andmete ebaseaduslik sisestamine (KarS § 206 lg 1) on varalise kasu saamise viisina KarS § 213 lg-s 1 nimetatud, kujutab KarS § 213

[53] Karistusseadustik. Komm vln § 206 komm 2.

[54] Karistusseadustik. Komm vln § 206 komm 8.1.

[55] Karistusseadustik. Komm vln § 206 komm 1.1.

[56] RKKKo 14.12.2012, nr 3-1-1-114-12, p 9.

lg 1 endast sisuliselt KarS § 206 lg 1 kvalifitseeritud koosseisu. KarS § 206 lg 1 tuleb kohaldada juhul, kui puudub nii KarS § 213 koosseisupärane tagajärg kui ka tahtlus varalist kasu saada.[57]

Järgmisena tuleks tähelepanu pöörata arvutisüsteemi toimimise takistamise koosseisule (KarS § 207). Arvutisüsteemi toimimise takistamise objektiivne koosseis on arvutisüsteemi toimimise ebaseaduslik häirimine või takistamine andmete sisestamise, edastamise, kustutamise, rikkumise, muutmise või sulustamise teel. Igasugused füüsiliste mõjutustega põhjustatud takistused, nagu sidekaablite arvutisüsteemide füüsiline rikkumine või hävitamine, § 207 alla ei lähe, vaid kvalifitseeritakse § 203 järgi.[58] Lg 2 ehk raskendava koosseisu moodustab elutähtsa valdkonna arvutisüsteemi töö või avalike teenuste osutamise takistamine või kui sellega on tekitatud oluline kahju.[59] Arvutisüsteemi toimimise häirimise all mõeldakse siinkohal arvutifunktsioonide täitmise halvendamist, eelkõige arvutisüsteemi poolt ülesannete täitmise aeglustamist. Arvutisüsteemi toimimise takistamiseks loetakse arvutisüsteemi funktsioonide täitmise vähemalt ajutise lakkamise põhjustamist.[60] Andmete edastamine on igasuguste infosüsteemis töötlemiseks sobivas vormis faktide, teabe või mõistete ühest punktist teise edastamine, tavaliselt telekommunikatsiooniühenduses.[61] KarS §-ga 207 kaitstavaks õigushüveks on arvutivõrkude ja arvutisüsteemide kasutajate õiguspärane ootus nende võrkude ja süsteemide takistamatuks kasutamiseks.[62] Koosseisutüübilt on tegemist formaalse kuriteokoosseisuga.[63] Eeltoodust nähtub, et taaskord on võimalik KarS § 207 koosseisu KarS § 213 koosseisust eristada kaitstava õigushüve järgi. Kui arvutisüsteemi toimimise takistamise puhul kaitstakse arvutisüsteemide õiguspäraste kasutajate õiguspärast ootust arvutisüsteemide takistamatuks kasutamiseks, siis arvutikelmuse puhul on kaitstavaks õigushüveks vara.

Viimaseks peab käesoleva töö autor veel vajalikuks tähelepanu pöörata arvutisüsteemi ebaseaduslikule kasutamise (KarS § 217) koosseisule ja selle eristamisele arvutikelmusest.

---

[57] 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.

[58] Karistusseadustik. Komm vln § 207 komm 2.1.

[59] Karistusseadustik (viide 49).

[60] Karistusseadustik. Komm vln § 207 komm 2.2.

[61] Karistusseadustik. Komm vln § 207 komm 2.5.

[62] RKKKo 25.02.2009, nr. 3-1-1-85-08, p 10.2.

[63] Karistusseadustik. Komm vln § 207 komm 1.2.

Arvutisüsteemi ebaseadusliku kasutamise objektiivse koosseisu moodustab arvutisüsteemile ebaseadusliku juurdepääsu saamine. Juurdepääs võib seisneda nt andmete või programmide edastamises, töötlemises või säilitamises antud arvutisüsteemis.[64] Lg 2 ehk raskendava koosseisu moodustab järgnev: kui on juurde pääsetud elutähtsa valdkonna arvutisüsteemile; kui on kasutatud riigisaladust, salastatud välisteavet või ainult ametialaseks kasutamiseks ettenähtud andmeid sisaldavat arvutisüsteemi; kui sellega on tekitatud oluline kahju.[65] Ebaseaduslik juurdepääs arvutisüsteemile on selline, milleks kasutajal ei ole luba.[66] Ebaseaduslik juurdepääs on käesoleva paragrahvi kohaselt karistatav vaid juhul, kui see toimub koodi, salasõna või muu kaitsevahendi kõrvaldamise või vältimise teel.[67] KarS §-ga 217 kaitstav õigushüve on arvutisüsteemi omaniku huvi selle takistamatuks kasutamiseks ja võimaluseks saada selle teiste isikute poolt kasutamise eest hüvitust.[68] Ka KarS § 217 ja KarS § 213 koosseisudel saab kõige lihtsamalt vahet teha kaitstava õigushüve põhjal. Nimetatud kuriteokoosseisude kvalifitseerimisel tuleb lähtuda sellest, kas teo toimepanija eesmärgiks oli saada varalist kasu.

[64] Karistusseadustik. Komm vln § 217 komm 2.

[65] Karistusseadustik (viide 49).

[66] Karistusseadustik. Komm vln § 217 komm 3.

[67] Karistusseadustik. Komm vln § 217 komm 4.1.

[68] Karistusseadustik. Komm vln § 217 komm 1.1.

3. ARVUTIKELMUSED EESTI KOHTUPRAKTIKAS

3.1 Arvutikelmuse sisustamine senises kohtupraktikas

Riigikohtu praktikast võime leida käesolevaks ajaks juba üsna mitu lahendit, kus on tegu KarS §-s 213 toodud arvutikelmuse mõiste sisustamisega ning lisaks veel mõned, kus on arvutikelmust põgusalt mainitud. Maa- ja ringkonnakohtute praktikast on võimalik leida arvutikelmuse lahendeid aasta-aastalt üha rohkem, mis on ka iseenesest mõistetav põhjusel, et arvutikelmuste toimepanemise arv ühe suureneb.

Maakohtu lahenditest ei ole üldjuhul kahjuks võimalik leida otsest arvutikelmuse koosseisu detailset analüüsi ning põhjendusi, miks just sellises olukorras määrati karistus KarS § 213 järgi. Ringkonnakohtu lahendeid analüüsides nähtub, et ringkonnakohtud on võtnud vaevaks oma lahendites juba üsna detailselt arvutikelmuse koosseisu analüüsida ja tuua välja põhjendused, mille alusel leiti, et süütegu tuleb just KarS § 213 järgi kvalifitseerida. Ringkonnakohtud on nii mõnelgi puhul maakohtu otsuseid tühistanud ja leidnud, et maakohtu poolt KarS § 213 järgi kvalifitseeritud tegu tuleb mõneks teiseks varavastaseks süüteoks ümber kvalifitseerida või ka vastupidi. Enne kohtupraktika juurde asumist tuleb ilmselt etteruttavalt märkida, et kahjuks on maakohtu lahendite näol dogmaatiliselt üsnagi primitiivsete KarS § 213 analüüsidega, kus koosseisuelemente sisuliselt ei analüüsita. Näitena võime tuua Viru Maakohtu Narva kohtumaja 09. aprilli 2008. a otsuse, kus peale kuriteo kirjeldust võetakse asi kokku järgmiselt: „Oma tahtliku tegevusega pani M. A. toime varalise kasu saamise arvutiprogrammide ebaseadusliku sisestamise andmetöötlusprotsessi ebaseadusliku sekkumise teel, kui sellega on mõjutanud andmete töötlemise tulemust, s.o arvutikelmus, mis on KarS § 213 järgi kvalifitseeritav süütegu.“[69] Seega puudub sisuliselt igasugune kuriteokoosseisu elementide detailne tuvastamine. Otsusest võib leida vaid arvutikelmuse toimepanemise fakti nentimist. Ometi peab mainima, et kui võrrelda 2008. või 2009. aasta maakohtu otsuseid näiteks 2012. või 2013. aasta otsustega, siis on näha, et ka maakohtu lahendite põhistused on muutunud põhjalikumas.

[69] Viru Maakohtu otsus 09.04.2008, nr 1-07-15253/7.

Alama astme kohtu otsustest tulenevalt on võimalik arvutikelmused liigitada nelja suuremasse kategooriasse. Kõige sagedamini esines kas internetipanga ülekannetega või pangakaardi ebaseadusliku kasutamisega seotud juhtumeid. Olulisel kohal on ka mobiiltelefonidega seotud juhtumid ja viimasel ajal on nendele lisandunud ka kütusekaardi ebaseadusliku kasutamisega seotud juhtumid. Samuti leiame alama astme kohtute praktikast veel juhtumeid, kus arvutikelmusena kvalifitseeriti krediitkaartidega seotud juhtumeid ja tuludeklaratsiooni esitamist. Otsustest nähtub, et suur osa kohtuotsuseid on tehtud kokkuleppemenetluses või siis lühimenetluses. Ilmselt ongi just see põhjuseks, miks arvutikelmus on ühelt poolt väga levinud kuritegu, kuid teiselt poolt on arvutikelmuse koosseisu käsitlev Riigikohtu praktika üsnagi tagasihoidlik. Alama astme kohtute praktika puuduseks saab välja tuua asjaolu, et otsustes tuuakse välja puudulikult asjaolud, millest tulenevalt ei ole isegi võimalik kontrollida, kas süüdistatava tegu kvalifitseeriti õigesti arvutikelmusena või oli tegu hoopis näiteks mõne muu varavastase süüteoga nagu vargus, omastamine või kelmus.

Kui võrrelda arvutikelmuse koosseisu kas varguse, omastamise või kelmuse koosseisudega, siis tundub esmapilgul üsna võimatu, et arvutikelmuse piiritlemisel eelnimetatud kuritegude koosseisudega võiks tekkida probleeme. Ometi ei ole aga arvutikelmuse eristamine nimetatud varavastaste süütegude koosseisudest kuigi lihtne. Just see on eeldatavalt üks põhjustest, miks Riigikohus on pidanud oma viimase aasta lahendites korduvalt vajalikuks peatuda just arvutikelmuse piiritlemise probleemidel. Et aru saada, kuidas arvutikelmust sellega seonduvatest varavastastest süütegudest eristada, siis tuleb selleks appi võtta erinevad kohtulahendid, kuna just nende pinnalt on võimalik analüüsida, millistel juhtudel tuleks kuriteod kvalifitseerida kas arvutikelmusena, omastamisena, vargusena või hariliku kelmusena. Kuna arvutikelmuseid on võimalik toime panna väga erinevatel viisidel ja erinevaid vahendeid kasutades, siis et asja lihtsustada ja luua kindel süsteem, on oluline paigutada kohtulahendid erinevate alapeatükkide alla.

3.2 Pangakontol oleva raha õiguslikku staatust käsitlevad lahendid

Kuna arvutikelmuseid pannakse tihti toime just pangakaarti ja pangaautomaati kasutades, siis on oluline kõigepealt peatuda sellel, kas pangakontol oleva raha näol on tegemist vallasasjaga või mitte. Nimetatud asjaolu omab eelkõige tähtsust just arvutikelmuse ja omastamise koosseisude piiritlemisel, mis on edasistes lahendites üheks keskseks teemaks.

Riigikohus jõudis pangakontol oleva raha õigusliku staatuse suhtes otsusele lahendis nr 3-1-1-83-07, mille kohaselt ei ole arvelduskontol olev raha vallasasi karistusseadustiku tähenduses, vaid tegemist on arvelduskonto omaniku varalise nõudega panga vastu arvelduskontol näidatud ulatuses. Kohus märkis, et nõue ei saa olla isiku valduses. Selline käsitlus on kooskõlas tsiviilõiguse põhimõtetega (otsuse p 14, vt ka Riigikohtu kriminaalkolleegiumi otsus asjas 3-1-1-130-04[70]). Sellega välistas kolleegium ülekannete tegemise suhtes omastamise esimese alternatiivi kohaldamise (s.o valduses oleva võõra vallasasja enda kasuks pööramine). Eeltoodust järeldub, et arvelduskontolt ülekande tegemine ei saa vastata ka varguse süüteokoosseisule, mis kaitseb omandiõigust vallasasjale. Otsuse punktis 15 kinnitab kolleegium, et põhimõtteliselt võib ülekannete tegemist teise isiku arvelduskontolt ilma kontoomaniku heakskiiduta käsitada omastamisena, kuid seda ainult tingimusel, et kontol olev vara (antud juhul raha) on süüdistatavale usaldatud.[71]

Riigikohus märkis, et: „1. septembrist 2002 kuni 23. märtsini 2008 kehtinud KarS § 213 redaktsioon nägi ette vastutuse varalise kasu saamise eest arvutiprogrammi või andmete ebaseadusliku sisestamise, muutmise, kustutamise, rikkumise, sulustamise või muul viisil andmetöötlusprotsessi ebaseadusliku rikkumise teel, kui sellega on mõjutatud andmete töötlemise tulemust. 24. märtsil 2008 jõustunud karistusseadustiku muutmise seadusega jäeti sättest välja tunnus „kui sellega on mõjutatud andmete töötlemise tulemust“ (vt RT I 2008, 13, 87, p 4). Arvuti all tuleb mõista arvutisüsteemi, mille definitsioon on antud arvutikuritegevusvastases konventsioonis (RT II 2003, 9, 32). Selle kohaselt on arvutisüsteem andmeid programmi järgi automaatselt töötlev seade (s.o programmeeritav seade). Kolleegium leidis, et andmete ebaseaduslik sisestamine hõlmab ka arvelduskontole juurdepääsu ja sellel oleva varaga toimingute tegemist võimaldavate andmete sisestamise, kui selleks puudub arvelduskonto omaniku nõusolek.“ Näitena viitas kolleegium siinkohal kontoomaniku nõusolekuta virtuaalsesse maksekeskkonda – internetipanka – sisenemisele ja korralduste tegemisele raha ülekandmiseks teise isiku arvelduskontole. „Andmete töötlemise tulemust mõjutatakse seejuures andmetöötlusprotsessi lubamatu käivitamise kaudu, kuna vastasel korral andmeid ei töödeldaks. Süütegu on lõpule viidud varalise kasu saamisega ehk raha laekumisega teo toimepanija või kolmanda isiku arvele. Kui isik võtab seejärel sularaha ka välja, on tegemist nn mittekaristatava järelteoga, mille ebaõigus neeldub enne toimepandud arvutikelmuses (sama põhimõte rakendub ka omastamise puhul).“ Ülekannete tegemist saab

[70] RKKKo 14.01.2005, nr 3-1-1-130-04, p 9.

[71] E. Elkind. Varavastane süütegu Interneti keskkonnas: selle piiritlemise probleemid Eesti karistusõiguses. Riigikohtu otsus 3-2-1-83-07. Juridica, 2008, nr 5, lk 334.

käsitada andmete ebaseadusliku sisestamisena. Süütegu on lõpule viidud varalise kasu saamisega ehk raha laekumisega teo toimepanija või kolmanda isiku kontole. Samuti leidis Riigikohus, et ülekannete tegemist saab käsitada andmete ebaseadusliku sisestamisena. Arvutit ei ole võimalik petta, kuna elektroonilise süsteemil puudub teadvus ja kujutlusvõime ning tänu sellele ei saa tekkida arvutil eksimust. Arvutikelmuse koosseisus asendab pettust arvutisüsteemi töö mõjutamine.[72]

Antud seisukohta on kinnitanud Riigikohus oma lahendis 3-1-1-60-04, mille kohaselt juhul, kui isiku tahte vastaselt hõivatakse raha pangaautomaadist, ei olnud tähendust asjaolul, kas pangakaart on leitud või varastatud. Kuigi pangakaardi valdus võib nii õiguspärase (leidmine) kui ka õigusvastase tegevuse tagajärjel üle minna kolmandale isikule, ei teki tal selle tulemusena mingeid õigusi pangakontol oleva rahasumma kasutamiseks. Iseenesestki mõista ei teki pangakaardi valduse üleminekuga automaatselt ka kontol oleva raha valduse üleminekut.[73]

3.3 Internetipangaga seotud juhtumid

Nagu nähtub alljärgnevatest kohtulahenditest, siis ebaseaduslike ülekannete tegemist internetipangas on võimalik kvalifitseerida tüüpjuhtumitel kas omastamisena või arvutikelmusena. Kahjuks aga ei ole internetipangaga seotud juhtumite kvalifitseerimine nii lihtne, kui pealtnäha paistab. Seetõttu peab käesoleva töö autor oluliseks välja tuua erinevaid internetipangaga seotud kohtulahendeid, kuna nende pinnalt on kõige lihtsam selgitada, millisel juhul ja miks tuleb osadel juhtumitel pealtnäha sarnaseid tegusid käsitleda ühel korral arvutikelmusena, teisel korral aga jälle omastamisena.

Ka käesoleva alapunkti all on oluline mainida Riigikohtu otsust asjas nr 3-1-1-83-07, kuna tegu oli esimese lahendiga, mille põhiliseks raskuspunktiks oli varguse, arvutikelmuse ja omastamise piiritlemine virtuaalpanganduse tingimustes. Nimetatud lahendist võib järeldada, et Riigikohus püüdis lahendis toodud selgituste näol anda alama astme kohtutele juhendi, kuidas edaspidi sisustada omastamise koosseisu elemente juhul, kus isik kasutas kuriteo toimepanemisel internetipanka või pangakaarti. Kolleegium selgitas, et internetipanga abil

[72] RKKKo 21.04.2008, nr 3-1-1-83-07 p 16.

[73] RKKKo 01.07.2004, nr 3-1-1-60-04 p 6.

rahaülekannete tegemine kannatanu arvelduskontolt süüdistatava või teise isiku kontole, kui selleks puudub kannatanu nõusolek, kahjustab kannatanu varalisi õiguseid. Vara kriminaalõiguslik kaitse laieneb ka olukorrale, kus süüdistatav kasutab arvelduskontole juurdepääsu võimaldavaid vahendeid varalise kasu saamiseks muul viisil, näiteks selleks, et osta internetikeskkonnas teenuseid ja kupu või kanda raha üle enda või teiste isikute arvele eesmärgita seda sularaha välja võtta. Kirjeldatud tegevusele õigusliku hinnangu andmine sõltub aga järgmisest.[74] Arvelduskontol oleva raha näol on tegemist arvelduskonto omaniku varalise nõudega panga vastu arvelduskontol näidatud ulatuses. Varaline nõue ei saa olla süüdistatava valduses, kuna valdus on tegelik võim asja üle (asjaõigusseaduse § 30). Seega ei toimu ülekannete tegemisel valduses oleva võõra vallasasja enda kasuks pööramist. Süüdistatav kasutab internetipangas arvelduskontole juurdepääsu võimaldavaid vahendeid võõra vallasvara käsutamiseks. Ülaltoodust tulenevalt on omastamise süüteokoosseisu esimene teoalternatiiv (valduses oleva võõra vallasasja ebaseaduslikult enda või kolmanda isiku kasuks pööramine) välistatud. Kannatanu arvelduskontol olev raha (vara) võib olla süüdistatavale usaldatud, s.o antud tema pädevusse, lepinguga või muul õiguslikul alusel. Vara usaldamise mõiste hõlmab juhtumeid, kus on olemas arvelduskonto omaniku nõusolek teise isiku juurdepääsuks arvelduskontole ja sellel oleva raha käsutamiseks.[75] Omastamisega on tegemist siis, kui isik teeb selliseid toiminguid (rahaülekandeid), milleks teda volitatud ei ole, pöörates vara enda või kolmanda isiku kasuks. Seejuures tuleb arvestada, et kuriteo täideviijaks võib olla vaid isik, kellele on vara usaldatud, teiste isikute puhul on võimalik kuriteost osavõtt.[76] Vara usaldamisega ei ole aga tegemist juhul, kui arvelduskontole juurdepääsu võimaldavad vahendid satuvad isiku valdusesse (või saavad talle teatavaks) arvelduskonto omaniku nõusolekuta, samuti kui neid antakse talle vaid hoiule või edasiandmiseks ilma konto kasutamise ja käsutamise õiguseta. Selles olukorras tuleb kõne alla arvutikelmuse koosseis (KarS § 213).[77]

Eelnimetatud lahendi järel on asjakohane mainida Riigikohtu otsuses nr 3-1-1-70-10 toodut. Nimetatud otsuses tunnistati süüdistatav KarS § 213 järgi süüdi selles, et olles saanud eelnevalt enda valdusesse kannatanule väljastatud internetipanga kasutajatunnise ja paroolid, kasutas ta neid kannatanu nõusolekuta internetipanka sisenemiseks ja kannatanu arvelduskontolt maksete tegemiseks kolmanda isiku arveldusarvele. Sellega mõjutas

[74] RKKKo 21.04.2008, nr 3-1-1-83-07 p 13.

[75] RKKKo 21.04.2008, nr 3-1-1-83-07 p 14.

[76] RKKKo 21.04.2008, nr 3-1-1-83-07, p 15.

[77] RKKKo 21.04.2008, nr 3-1-1-83-07, p 16.

süüdistatav arvutisüsteemis andmete töötlemise tulemust andmetöötlusprotsessi lubamatu käivitamise kaudu. Seejärel võttis kannatanu kolmanda isiku arveldusarvele kantud raha sularahaautomaadist välja, saades sellega varalist kasu.[78] Käesolevast lahendist nähtub, et praegusel juhul on põhirõhk suunatud sularaha väljavõtmisele ehk sellele, et just sularaha automaadist välja võttes saadi varalist kasu. Võrdluseks tuleks tähelepanu pöörata juba käesolevas töös osundatud Riigikohtu otsusele nr 3-1-1-83-07, milles kolleegium leidis, et raha väljavõtmine sularahaautomaadist ei olegi oluline, kuna varalist kasu saadi juba raha teisele kontole ülekandmisega.[79]

Riigikohus käsitleb oma 14. detsembri 2012 lahendis nr 3-1-1-114-12 olukorda, kus ajal, mis äriühing võttis laenu, oli süüdistatav äriühingu juhatuse liige. Kui saabus aeg laenu tagasimaksmiseks, süüdistatav enam äriühingusse ei kuulunud ja äriühing laenu tagasi ei maksnud. Süüdistatav, kelle kätte oldi varasemast ajast jäänud äriühingu internetipanga juurdepääsukoodid, tegi äriühingu arvelt võlausaldaja arvele osa laenusumma ulatuses ülekande. Maakohus tunnistas süüdistatava süüdi arvutikelmuses, kuid ringkonnakohus mõistis süüdistatava õigeks.[80] Nimetatud asjaolude pinnalt asus Riigikohus seisukohale, et kelmuse objektiivse koosseisu täitmiseks ei pea süüdlane vara vahetult endale võtma, vaid see võib üle minna ka kolmanda isiku vara hulka, kuid sellisel juhul peab kolmanda isiku varaline seis süüdlase teo tulemusel ka paranema. Kolmas isik sai äriühingult küll 45 000 krooni, kuid omas samal ajal äriühingu vastu realiseeritavat nõuet summas 52 000 krooni. Kuna kolmas isik ei saanud käesoleval hetkel süüdistatava poolt tehtud ülekande tagajärjel varalist kasu, siis koosseisupärase tagajärje puudumise tõttu on süüdistatava vastutusele võtmine arvutikelmuse järgi välistatud.[81] Süüdistatava poolt tehtud ülekannet ei saa kvalifitseerida ka omastamisena, kuna kaasuse tehioludest nähtuvalt ei olnud süüdistatav ülekande tegemise ajal enam äriühingu juhatuse liige ega omanud äriühingu internetipanka sisenemiseks ega arvelduskontol oleva raha käsutamiseks õiguslikku alust.

Internetipanga vahendusel on tänapäeval võimalik teha palju erinevaid toiminguid, sh teha ülekandeid ja sõlmida erinevaid lepinguid. Sellest tulenevalt on käesolev alapeatükk väga mahukas ja siia on koondunud väga erineva sisuga lahendeid. Eeltoodu näitab, et internetipanka kasutades on võimalik arvutikelmuseid toime panna väga erinevatel viisidel.

[78] RKKKo 15.11.2010, nr 3-1-1-70-10, p 1.2.

[79] RKKKo 05.02.2009, nr 3-1-1-83-07, p 13.

[80] RKKKo 14.12.2012, nr 3-1-1-114-12, p 1 ja p 3.

[81] RKKKo 14.12.2012, nr 3-1-1-114-12, p 7.

Riigikohtu otsuste valguses võib väita, et internetipangas ebaseaduslikku ülekande tegemist võib kvalifitseerida kas omastamisena või arvutikelmusena. Siinkohal tuleb kõige kuriteokoosseisu määramiseks välja selgitada, kuidas süüdistatav sai võõrale pangakontole ligipääsu. Riigikohtu lahendi nr 3-1-1-83-08 valguses tuleb mainida, et kuna arvelduskontol oleva raha näol ei ole tegemist vallasasjaga karistusseadustiku tähenduses, vaid tegemist on arvelduskonto omaniku varalise nõudega panga vastu arvelduskontol näidatud ulatuses, siis ei saa arvelduskontolt ülekande tegemine vastata varguse süüteokoosseisule, mis kaitseb omandiõigust vallasasjale.

Arvutikelmuses mõisteti süüdi näiteks isikud, kes Ungaris asuvate arvutite Trooja-viirusega nakatamise teel kogusid nakatatud arvutitest internetipankade juurdepääsukoode ja salasõnasid. Nimetatud andmete abil teostasid arvuteid nakatanud isikud Eesti Vabariigis erinevates pankades avatud erinevate isikute pangakontodele ebaseaduslikke, s.t. ilma Ungari pankade arvete kasutajate teadmata ja loata, ülekandeid st said varalist kasu. Süüalune aga aitas arvutikelmusele kaasa sellega, et ostis kolmanda isiku vahendusel erinevate isikute poolt pankades avatud arveid ja nende juurde välja antud pangadokumente, millised süüalune edastas kahele isikule. Seejärel kandsid need kaks isikut ebaseaduslikult avatud arvetele Ungari panga klientide arvelt erinevaid summasid. Maakohus leidis, et süüalune osutas seeläbi ka vaimset kaasabi, tugevdades kahe ülekandeid teinud isikute soovi ja tahet ebaseaduslikke ülekannete tegemiseks, sest oli loodud võimalus varjata ülekannet teinud isikut ja kontrollida eelpoolnimetatud arvetel olevat raha.[82]

Veel mitmekesisem ning samuti arvutiviiruse levitamisega seotud lahend on nr 1-07-5805, kus isikud mõisteti saadi arvutikelmuses, kuna nad said varalist kasu andmete ebaseadusliku sisestamisega, millega mõjutati andmete töötlemise tulemust. Süüdistatavad said ebaõige sisuga e-kirjade saatmise teel Itaalia Vabariigi elanike pangakontodelt 5 kuu jooksul ebaseaduslike rahaülekannete teostamise teel varalist kasu. Teatud ettevõtte koduleheküljelt ja e-maili teel levitati valekuulutusi Itaalia Vabariigi elanike seas, mille sisuks oli finantsmänedžeride otsimine, kelle ülesandeks oli oma pangaarvele laekunud raha edasitoimetamine vastavalt süüdistatavate poolt antud e-maili ja telefoni teel antud juhistele. Süüdistatavad korraldasid Itaalias elavate isikute arvutitesse arvutiviiruse programmi, mis sisaldas arvutiviirust Trooja, allalaadimise internetileheküljelt, kuhu oli märgitud, et tegemist on tarkvara uuendusega, kuid mis arvutis avatuna tegelikult kogus ning edastas internetipanga

[82] Harju Maakohtu otsus 19.10.2009, nr 1-09-1894/10.

klientide kasutajatunnuseid ja turvaparoole ühe süüdistatava serverisse. Olles selliselt juurde pääsenud Itaalia pankade internetipankade klientide arvetele, värbas üks süüalustest e-maili teel isikud, kelle arvele teostati ebaseaduslikult ülekanded. Seejärel andsid süüalused variisikuteks palgatutele e-maili ja telefoni teel korraldusi raha edasikandmiseks Western Unioni rahasiirdamisteenust kasutades Eestis oleva variisiku nimele.[83] Sama skeemi viisid süüalused läbi ka Kreekas, Prantsusmaal, Austrias ning Taanis. Kui tavaliselt on arvutikelmustega toime pandud kahju väike, siis antud juhtum on oluline seetõttu, et eelpoolnimetatud skeemi rakendamisel erinevates riikides tekitati kahju umbes kahe ja poole miljoni eesti krooni väärtuses.

Arvutikelmuse esinemist jaatatakse ka järgnevas arvutiviiruse levitamisega seotud otsuses nr 1-07-8428, kus süüalune korraldas Leedu Vabariigis elavate isikute arvutitesse e-posti kasutades arvutiprogrammi saatmise, mis salvestus turvaaugu olemasolul adressaadi arvutisse ja asus saatma teostatud internetipanga külastuste informatsiooni (sh paroolid ja kasutajanimed) tema enda hallatavasse FTP serverisse. Saanud sellisel viisil internetipanga paroolid ja kasutajanime, sisenes süüalune neid paroole kasutades Leedu panga internetipanga keskkonda ning teostas kontodelt konto omaniku teadmata ja volituseta ülekandeid kolmanda isiku kontole. Järgmisel päeval võttis süüalune raha kolmanda isiku kontolt sularahas välja. Selliselt, sekkudes ebaseaduslikult andmetöötlusprotsessi, sai süüalune varalist kasu, tekitades kannatanule kahju.[84]

Eelnevad otsused on kõik seotud arvutiviiruse levitamisega, mille kaudu inimesi peteti ja pettuse kaudu saadi varalist kasu. Kohtud ei analüüsinud, kuidas nad jõudsid järelduseni, et eelnimetatud teod tuleb kvalifitseerida just arvutikelmustena. Kuna maakohtu analüüs nimetatud kuritegude osas on puudulik, siis peab käesoleva töö autor vajalikuks eeltoodud kuritegude koosseisu pisut lähemalt analüüsida. Lahendi asjaolude pinnalt nähtub, et esmane toiming oli inimese eksitusse viimine ja selle kaudu paroolide saamine, mis oli varalise kasu saamisel edasiseks vahendiks. Antud viisi ebaseaduslikul teel paroolide hankimist nimetatakse *phishing'*uks.[85] Kui analüüsida mainitud kuritegude koosseisu, siis näeme, et kuriteo objektiks oli vara (raha), mida loodeti pettuse teel omale saada. Kannatanu jaoks toimus asjaolude moonutamine ehk käeoleval juhul e-kirjade saatmine ning kannatanul tekkis eksimus. Kannatanu tegi tahtmatu varakäsutuse, mis seisnes e-maili avamises, millega

[83] Harju Maakohtu otsus 12.06.2007, nr 1-07-5805/2.

[84] Harju Maakohtu otsus 18.09.2007, nr 1-07-8428/3.

[85] Danske Bank. Internetipank. Arvutivõrgus: http://www.danskebank.ee/et/13136.html, 02. mail 2013.

käivitas oma arvutis viiruse, mis püüdis internetipanga paroole. Kokkuvõttes sai süüdlane varalist kasu ja kannatanul tekkis varaline kahju. Lisaks sellele ei ole võimalik käesolevate kaasuste asjaolude pinnalt võimalik väita, et süüdistavatel ei oleks esinenud kuritegude toimepanemisel tahtlust eespoolmainitud tegusid teha, kuna kannatanutele saadeti e-kirjad just internetiparoolide püüdmise eesmärgil – seega on olemas ka tahtlus ehk subjektiivne koosseis on täidetud. Kui nüüd vaadata uuesti objektiivse koosseisu elemente, siis on võimalik järeldada, et tegelikult võiks nimetatud kuriteod liigitada pigem kelmuse alla, kuna reaalselt on olemas isik, keda petetakse.

Arvutikelmuse jaatamist näeme ka maakohtu otsuses nr 1-08-6581. Süüalune esitas 2006. a varalise kasu saamise eesmärgil kannatanu nimelt Maksu- ja Tolliametile tuludeklaratsiooni, kasutades kannatanu teadmata ja nõusolekuta viimase nimele välja antud Krediidipanga paroolikaarti ja püsiparooli ning märkis enammakstud tulumaksu tagastamiseks kannatanu Eesti Krediidipanga konto numbri, mida kannatanu ise ei kasutanud. Enammakstud tulumaks kanti Maksu- ja Tolliameti poolt kannatanu kontole, mille süüdistatav, kasutades kannatanu teadmata ja nõusolekuta viimasele väljastatud internetipanga paroolikaarti ja kasutajatunnust, kandis hiljem enda kontole ning sai sellega varalist kasu.[86] Siinkohal seab käesoleva töö autor jällegi kahtluse alla arvutikelmuse kohaldamise õiguspärasuse. Maakohus ei arvestanud asjaoluga, et tulumaksu ei tagastata automaatselt arvutiprogrammi poolt, vaid enne seda peab tulumaksu läbi vaatama maksuametnik, kes peab veenduma, et deklaratsioonis esitatud andmed vastavad tõele ja alles seejärel kinnitab maksuametnik deklaratsiooni. Arvestades, et nn teisel pool ekraani on olemas reaalne isik, keda peteti, siis sellest tulenevalt oleks kohus pidanud sellise teo kvalifitseerima arvutikelmuse asemel nn hariliku kelmusena.

Eelneva Maksu- ja Tolliameti juhtumiga saab kaudselt siduda ka otsuse nr 1-07-12666, mis on jällegi seotud internetipanga poolt pakutavate võimalustega. Arvutikelmuse toimepanemist jaatati olukorras, kus süüdistatav kasutas kannatanu internetikaarti ja sõlmis internetis pettuse teel kannatanu nimele Tele 2 iseteeninduse kaudu kolme mobiiltelefoni liitumislepingud ning järelemaksulepingud. Süüdistatav omastas telefonid ja hakkas lepingulisi teenuseid kasutama, tekitades sellega kannatanule varalist kahju. Süüdistatav kasutas sama skeemi ka teise kannatanu puhul. Maakohus leidis, et sel moel ülalnimetatud tegudega pani süüdistatav toime varalise kasu saamise arvuti programmi või andmete ebaseadusliku sisestamise ja muul viisil andmetöötlusprotsessi ebaseadusliku sekkumise teel, s.o KarS § 213 lg 1 järgi

[86] Pärnu Maakohtu otsus 18.09.2008, nr 1-08-6581/7.

kvalifitseeritava kuriteo.[87] Nimetatud lahendi puhul omab kuriteokoosseisu kvalifitseerimisel jällegi tähtsust asjaolu, kas ja kes aktsepteeris Tele 2 iseteeninduses mobiiltelefoni liitumis- ja järelemaksulepingud. Üldjuhul ei käi selliste lepingute sõlmimine automaatselt, vaid teisel pool on isik, kes analüüsib esitatud ja taotlust ja selle pinnalt tehakse otsus, kas esitatud taotlused rahuldatakse või mitte. Kui teisel pool on olemas reaalne isik, kes taotluseid analüüsib ja langetab nende suhtes otsuse, võiks kaaluda, kas tegemist ei olnud lihtsalt hariliku kelmusega.

Maakohus mõistis süüdistatava süüdi arvutikelmuses järgmistel asjaoludel: süüdistatav kasutas kolmandalt isikult saadud internetipanga koodikaarte ja paroole, et esitada laenutaotlusi erinevatele krediidiasutustele. Isik X andis süüdistatavale oma internetipanga koodikaardi ja paroolid, kuna süüdistatav palus seda. Süüdistatav väitis, et tema konto on arestitud, aga tal on vaja tingimata kanda raha üle. Selleks oli tal vaja isiku X internetipanga koodikaarti ja paroole. Kasutades isik X teadmata tema andmeid, esitas süüdistatav interneti kaudu laenutaotluseid erinevatele kiirlaenuandjatele. Pärast taotluste rahuldamist ja rahaülekandmist isiku X kontole, kandis süüdistatav kiirlaenuandjatelt isik X kontole laekunud raha üle enda pangaarvele. Süüdistataval puudus seejuures laenude taotlemiseks isik X luba. Kohus leidis, et süüdistatav sisestas ebaseaduslikult isik X andmeid kiirlaenuandjate andmebaasidesse, et saada varalist kasu. Ebaseaduslike andmete sisestamise teel sekkus süüdistatav ebaseaduslikult andmetöötlusprotsessidesse. Seega oma käitumisega pani süüdistatav toime arvutikelmuse.[88] Arvestades Riigikohtu lahendi nr 3-1-1-83-07 punktides 15 ja 16 toodud seisukohti, tuleb kontrollida, kas eelpoolnimetatud tegu saaks kvalifitseerida arvutikelmuse asemel hoopis omastamise II teoalternatiivina, mis näeb ette isikule usaldatud muu võõra vara ebaseaduslikult enda või kolmanda isiku kasuks pööramist. Käesoleval juhul andis kannatanu ise vabatahtlikult oma internetipanga paroolid süüdistatavale, et süüdistatav saaks kasutada tema kontot ülekannete tegemiseks, kuid süüdistatav kasutas isik X pangakontot selliste toimingute tegemiseks, milleks kannatanu teda ei volitanud. Seetõttu tuleks selline juhtum kvalifitseerida pigem omastamisena, mitte arvutikelmusena.

Sama kaasuse raames süüdistatakse süüdistatavat omastamises nimelt selles, et ta kasutas tema kätte sattunud isik Y andmeid, et taotleda laenu interneti teel. Sealjuures oli süüdistataval oli olemas isik Y nõusolek võtta viimase nimele laenu. Kuigi isikule Y öeldi, et

[87] Viru Maakohtu otsus 23.03.2009, nr 1-07-12666/8.

[88] Viru Maakohtu otsus 29.10.2012, nr 1-12-9838.

laene ei õnnestunud võtta, esitas süüdistatav laenutaotlused kahele kiirlaenupakkujale. Laenutaotlused rahuldati ja kanti üle isik Y arvele. Samal päeval kandis süüdistatav isik Y kontolt üle enda kontole kiirlaenupakkujatele esitatud taotluste alusel laekunud raha. Käesoleval juhul leiab töö autor, et kohus kvalifitseeris nimetatud teo juba eespooltoodud põhjenduste valguses õigesti omastamisena. Siin puudus pettus selles osas, et isik Y teadis, et ta annab oma internetiparoolid süüdistatavale selleks, et süüdistatav saaks tema nimel laene taotleda. Süüdistatava tegu vastab KarS § 201 II teoalternatiivi koosseisule. Tegemist ei ole arvutikelmusega, kuna arvelduskontole juurdepääsu võimaldavad vahendid usaldati süüdistatava kätte.

Kohus kohaldas lahendis nr 1-934/05 KarS § 213 olukorras, kus isik leidis 2004. a septembris kesklinnas Tallinna Kaubamaja lähedalt kannatanult varastatud internetipangakaardi ja kasutas häkkeriprogramme, et teada saada pangaarve numbrit, paroole ja PIN-koode ning sisestas ebaseaduslikult varem teada saadud andmed arvutisse ja tegi internetipangast ülekandeid.[89] Antud lahendi faktilisest koosseisust tulenevalt tekib kahtlus, kas tegu ei võiks olla hoopis omastamisega. Karistusõiguslikult saab omastamisest – antud juhul leiu omastamisest ehk enda kasuks pööramisest rääkida alles siis, kui leidja on asjaga teinud toiminguid, mis näitavad tema omastamistahet või manifesteerivad omastamist (leitud asja müümine, ümbertöötamine jms).[90] Käesoleval juhul saab kindlalt väita, et internetipangakaardi kasutamisega ja häkkerprogrammide kasutamisega paroolide teadasaamine näitavad süüaluse selget omastamistahet, kuna leidja pööras asja faktiliselt enda kasuks. Objektiivsetest tunnustest esineb antud juhtumis võõra vallasasja olemasolu (võõras internetipanga kaart), mis oli leitud. Eelneva analüüsi käigus on tuvastatud enda kasuks pööramine (omaniku kestev ilmajätmine, endale pidamine, omastamistahte manifesteerimine, enda kasuks pööramise ebaseaduslikkus). Subjektiivsest küljest oli süüalusel kindlasti olemas tahtlus. Seega on võimalik antud lahendit vaadelda ka KarS §-s 201 sätestatud omastamisena. Kui aga süüalune oleks antud internetipangakaardi varastanud, siis oleks tegu täiesti tavalise vargusega ning sellisel juhul oleks KarS § 213 kohaldamine olnud kaheldav.[91]

Kõige tüüpilisemad on juhtumid, mil võõralt pangakontolt kantakse enda pangakontole raha. Sellise näite leiame Harju Maakohtu 01. oktoobri 2012 otsusest nr 1-12-8271. Käesoleval juhul mõistis maakohus M. V. süüdi selles, et tema, kasutades teatud ajavahemikus ilma M. L.

[89] Tallinna Linnakohtu otsus 16.05.2005, nr 1-934/05.

[90] J. Sootak (viide 27), lk 103.

[91] E. Pära (viide 17), lk 24.

nõusolekuta ja teadmata M. L isikutunnistust ja vastavat PIN1 koodi, sisenes korduvalt M. L. arvelduskonto internetipanka ja tegi enda arvelduskontole korduvalt rahaülekandeid.[92] Võõralt pangakontolt oma kontole raha ülekandmine on arvutikelmus (§ 213), sularaha järgnev väljavõtmine on mittekaristatav järeltegu.[93] Järelteo neeldumine eel- ehk põhiteos on vaadeldav konsumeerimisena, sest tegemist on tüüpiliste järeltegude – tagamissüütegudega –, mis pannakse toime põhiteoga (eelkõige varavastase süüteoga) saadud kasu kindlustamiseks.[94]

Kohtuasi nr 1-190/03 on huvitav, kuna süüdistatav töötas panga kontoris tellerina, kelle ülesandeks oli muuhulgas teleteenuste lepingute sõlmimine. Süüdistatav võltsis teleteenuste lepingul kannatanu allkirja, vormistas fiktiivse lepingu kannatanu arvelduskontode kasutamiseks Interneti ja telepanga vaheldusel, saades selleks lepingu järgi endale kasutajatunnuse, püsiparooli, muutuvparoolid ja PIN-koodi. Süüalune kasutas ilma kannatanu nõusolekuta samas lepingus ette nähtud kasutajatunnust, püsiparooli ja turvaparooli, saades andmetöötlusprotsessi andmete sisestamise teel 21 480 krooni varalist kasu. Kohus kvalifitseeris süüaluse niisuguse tegevuse arvutikelmusena, s.o. KarS §-s 213 ette nähtud kuriteona.[95]

Antud lahendi puhul võiks tõstatada küsimuse, kas tegu on arvutikelmusega, tavalise kelmusega või hoopis KarS § 201 II alternatiiviga ehk isiku kätte usaldatud vara kuritarvitamisega. Antud juhul puudus süüdistataval kannatanu nõusolek kannatanu nimel teleteenuste lepingu sõlmimiseks. Süüdistatav võltsis kannatanu allkirja, identifitseerides ennast sellega konto omanikuna, mille tagajärjel tegi ta ise internetipangas toiminguid. Selle tulemusena võeti kannatanu kontolt tehingu katteks raha, millise summa väärtuses omastas süüalune raha. Seega leiame siit enamuse kelmusele vastavad nii objektiivsed kui ka subjektiivsed faktilised asjaolud, kuid ometi puudub isik, keda petetakse. Juhul, kui tegu oleks puhta kelmusega, siis peaks antud juhul petetama kas panka või masinat. Kuna autor on töös eelnevalt maininud, et panka ega masinat ei ole võimalik petta, siis on antud hetkel kelmuse koosseisu esinemine välistatud. Võimalik, et antud lahendit saaks käsitleda kui KarS § 201 II alternatiivi ehk isiku kätte usaldatud vara kuritarvitamist. Seadusandja on teinud KarS § 201

[92] Harju Maakohtu otsus 01.10.2012, nr 1-12-8271.

[93] RKKKo 21.04.2008, nr 3-1-1-83-07, p 16.

[94] J. Sootak. Seadusainsus. Kui isiku tegu vastab mitmele süüteokoosseisule, siis mitme järgi ja kuidas ta tegelikult vastutab? Juridica, 2010, nr 1, lk 20.

[95] Rapla Maakohtu otsus 18.11.2003, nr 1-190/03.

teise alternatiiviga otsustava sammu kõrvale senisest dogmaatikast, mille kohaselt sai KarS §-de 201 ja 199 ese olla vaid vallasasi. 15. märtsil 2007 jõustunud täiendusega on KarS § 201 esemeks muutunud vallasasjade kõrval muu võõras vara. Senise kohtupraktika paraadnäiteks võõra vara mõiste sisustamisel on saamas arveldusarvel olevad vahendid (RKKKo 3-1-1-83-07).[96] Nimelt kinnitas Riigikohus enne 15. märtsi 2007 kehtinud KarS § redaktsiooni (praegust esimest alternatiivi) tõlgendades, et asjana ei ole käsitatav pangakontol olev raha, sest sellel puuduvad kehalise eseme tunnused, küll aga näiteks sularaha.[97] Kuna KarS § 201 teine alternatiiv hakkas kehtima alates 15. märtsi 2007 jõustunud täiendusega, siis on arusaadav, miks kohtud seda kuriteokoosseisu siinkohal ei analüüsinud. Seega tõdeb töö autor, et antud lahendi puhul on ikkagi tegu arvutikelmusega.

Maakohus jaatas arvutikelmuse (KarS § 213) koosseisu esinemist olukorras, kus süüdistatav võttis kannatanu elukohas laua pealt kannatanu internetipanga paroolikaardi, püsiparooli ja kasutajatunnuse, kirjutas need endale paberi peale ja lasi kolmandal isikul teha toiminguid kannatanu nimel Hansapangas väites, et on kannatanu seaduslik hooldaja, mille tulemusena kolmas isik kannatanu nimel esinedes internetipanka andmeid sisestades ja sellega ebaseaduslikult Hansapanga andmetöötlusprotsessi sekkudes kandis kannatanu arvelduskontolt raha süüdistava arvelduskontole, kust süüdistatav omastas nimetatud summa.[98] Käesoleval juhul ei ole tegu omastamisega, kuna internetipanga paroolid ei olnud süüdistatavale usaldatud. Internetipangas ülekande tegemist ei ole võimalik käsitleda ka töös juba eespool mainitud põhjustel vargusena (olenemata sellest, et internetipanga paroolid saadi teada ebaseaduslikult). Kuna internetipanka siseneti läbi internetipanga keskkonna, kus sisestati ka raha ülekandmiseks vajalikud paroolid, siis puudus isik, keda peteti (arvutit ei saa petta), siis ei ole tegu ka hariliku kelmusega. Maakohus kvalifitseeris sellise teo õigesti arvutikelmusena, kuna esineb tegu ehk andmetöötlusprotsessi sekkumine selle käivitamise näol kui ka tagajärg – varalise kasu saamine. Siinkohal on oluline mainida, et kolmas isik, kes tegelikult ülekande tegi (koos süüdistatavaga), tema suhtes ei ole võimalik arvutikelmuse koosseisu jaatada, kuna tema küll sekkus andmetöötlusprotsessi selle käivitamise näol, kuid ei saanud ise selle tulemusena vara.

Lisaks eelnevatele lahenditele tuleks siinkohal ära märkida veel mõned eripalgelised internetipangaga seotud juhtumid, millised kvalifitseeriti arvutikelmustena. Nimelt leidis aset

[96] E. Pära (viide 17), lk 25.

[97] M. Kairjak. Varaliste huvide järgimise kohustus ja teisele isikule usaldatud vara. Juridica, 2010, nr 1, lk 24.

[98] Tartu Maakohtu otsus 15.09.2008, nr 1-08-9816/3.

juhtum, kus süüdistatav avastas pangakontoris, et isik, kes vahetult enne teda makseterminali kasutas, ei väljunud oma pangakonto teeninduskeskkonnast. Süüalune kasutas sellist olukorda enda huvide ära ja teostas internetipangas varalise kasu saamise eesmärgil enda kontole ülekandeid.[99] Samuti juhtum, kus süüdistatav sai oma valdusesse kannatanu internetipanga kasutajatunnuse, salasõna ja paroolikaardi ning kirjutas need endale üles. Üleskirjutatud andmeid kasutades laaditi kannatanu kontolt süüdistatavale ZEN kõneaega ja hiljem tegi süüdistatav ka ülekandeid enda kontole.[100]

Eelnevalt kajastatud olukorra kohta on õiguskirjanduses aga leitud, et kelmus peaks olema põhimõtteliselt välistatud, sest arvutiprogrammijärgse käitumise korral ei peteta panka. Veel vähem saab inimene eksimusse viia arvutit. Siiski on võimalik konstrueerida ahel, mille ühes otsas asub konto omanik, teises aga pank. Nende vahel on sõlmitud leping, mille mitmesugused tingimused on suunatud sellele, et konto omanik saab teatud alustel pangast võtta sularaha (kontorist või automaadist), teha ülekandeid (kontorist või internetipanga abil) jne. Sularahaautomaadis vale (võltsitud või õige, kuid talle mittekuuluva) kaardiga manipuleerides käivitab süüdlane ahela, mille tulemusena ta lõppkokkuvõttes petab panka. Selle pettuse tagajärjel teeb pank varakäsutuse. Erinevalt kontoris telleri poolt tehtavast toimub sularahaautomaadi kasutamise korral varakäsutus elektroonilise seadme abil. Kelmuse ehk panga petmisega on tegemist mitte ainult sularahaautomaadist raha võtmisel, vaid ka nende juhtudel, kui süüdlane saab teada kliendi kasutajanumbri, püsiparooli ning enda käsutusse päevakoodide tabeli ja kannab seejärel võõralt kontolt raha üle oma kontole, maksab oma arve jms.[101]

J. Sootak on leidnud, et olemuslikult ei saa kindlasti tegemist olla kelmusega § 209 tähenduses, samas aga on ta jätnud § 213 kohaldamise lahtiseks. Kohtud on aga antud olukorras just jaatanud § 213 olemasolu. Siinkohal ilmneb asjaolu, mis eristab arvutikelmust tavalisest kelmusest: arvutikelmus ei sisalda kelmusele omast kelmuslikku elementi. Kelmuse ehk § 209 rakendamiseks oli vajalik objektiivse koosseisu poole pealt nelja elemendi (petmine, eksimus, varakäsutus, varaline kasu (kannatanu varalise kahju arvelt)) olemasolu ning lisaks sellele peavad antud elemendid olema omavahel põhjuslikus seoses. Arvutikelmuse puhul aga eeldab koosseis samuti konkreetse varalise kahju tekkimist, lubamatut sekkumist ja sekkumine peab olema tehtud andmetöötlusprotsessi, kuid

[99] Harju Maakohtu otsus 08.04.2009, nr 1-09-2639/3.

[100] Tartu Maakohtu otsus 15.12.2009, nr 1-09-18141/11.

[101] J. Sootak (viide 27), lk 164.

petmistoimingut ja sellega inimese eksitusse viimist siiski ei nõuta. Tingimuseks on ainult pettusetaoliste manipulatsioonide tegemine arvutil. Sisuliselt puudub arvutikelmuse puhul otsene isik, keda petetakse. Sisuliselt on § 213 kohaldatud olukordades, kus õiguskirjandus on selgelt eitanud kellegi petmist.[102]

Eelpool toodud kaasuste pinnalt saab järeldada, et internetipangaga seotud juhtumite puhul on kõige keerulisem vahet teha selles, kas tegu on arvutikelmuse või omastamisega. Nimetatud kuriteokoosseisude piiritlemisel on oluline teha vahet, millisel viisil sattusid internetipanga kasutajatunnus ning paroolid süüdistatava kätte. Omastamisega on tegu siis, kui isik teeb selliseid toimingud (rahaülekandeid), milleks teda volitatud ei ole, pöörates vara enda või kolmanda isiku kasuks. Arvutikelmusega on tegemist aga juhul, kui arvelduskontole juurdepääsu võimaldavad vahendid satuvad isiku valdusesse või saavad talle teatavaks arvelduskonto omaniku nõusolekuta. Samuti on tegemist arvutikelmusega juhul, kui arvelduskontole juurdepääsu võimaldavad vahendid antakse isikule vaid hoiule või edasiandmiseks ilma konto kasutamise ja käsutamise õiguseta.

3.4 Pangakaartidega seotud juhtumid

Pangakaartidega seotud juhtumite puhul võivad kuriteod olla kvalifitseeritavad kas omastamisena, vargusena, kelmusena või arvutikelmusena. Kuritegude kvalifitseerimisel tuleb eelkõige tähele panna, kuidas pangakaart ja PIN-koodid süüdistatava valdusesse said ning kas pangakaarti kasutades petetakse kedagi või sisestatakse PIN-kood lihtsalt makseterminali. Et aru saada, kuidas täpselt tuleks pangakaartidega seonduvaid kuritegusid kvalifitseerida, siis tuleb selleks appi võtta kohtulahendid, mille pinnalt on võimalik erinevate kuriteokoosseisude esinemist analüüsida.

Riigikohtu otsusest nr 3-1-1-60-04 nähtub, et Riigikohus käsitleb pangakaardi ebaseaduslikku kasutamist vargusena. Kaasuse asjaolude kohaselt varastas süüdistatav grupis koos teiste isikutega kannatanu sõiduautost kannatanule väljastatud pangakaardi ja võttis PIN-koodi lehe kasutamise teel tema arveldusarvelt kolmel korral raha kogusummas 152 400 krooni. Nimetatud asjaolude valguses leidis Riigikohus, et juhul, kui isiku tahte vastaselt hõivatakse raha pangaautomaadist, ei olnud tähendust asjaolul, kas pangakaart on leitud või varastatud.

[102] E. Pära (viide 17), lk 26-27.

Olenemata sellest, millisel viisil pangakaardi valdus kolmandale isikule üle läheb, ei teki tal selle tulemusena mingeid õigusi pangakontol oleva rahasumma kasutamiseks. Pangakaardi valduse üleminekuga ei teki automaatselt ka kontol oleva raha valduse üleminekut. Selleks, et saada raha, mida oli pangalt õigustatud nõudma vaid kannatanu, pidi kohtualune teostama rea toiminguid, millised ei ole aga kuidagi käsitletavad raha leidmisena. Riigikohus leidis, et pangakaardi näol oli tegemist riistaga, millega kõrvaldatakse tõke võõra vara juurde pääsemiseks. Väljutamisavas olev rahasumma kuulub kannatanule, olenemata sellest, kes pangakaardi ja PIN-koodi sisestas. Selle rahasumma äravõtmise hetkel lõpeb valduse murdmine ja võõras raha võetakse ära, so. pannakse toime varavastane kuritegu, milleks käesoleval hetkel oli vargus.[103]

Riigikohtu 10. mai 2010 otsus nr 3-1-1-35-10 on oluline selle poolest, et Riigikohus selgitas iseloomult küllaltki sarnaste tegude (arvutikelmus ja nn harilik kelmus) kvalifitseerimise reegleid. Käesoleva kaasuse asjaolude kohaselt puudus süüdistataval kannatanu nõusolek viimasele kuuluva pangakaardi ja pangakontol oleva raha kasutamiseks. Süüdistatav esitas müüjale kannatanu pangakaardi ja valis maksmiseks kassa, kus puudus PIN-kalkulaator, identifitseeris süüdistatav end kaardi ja konto omanikuna, mille tagajärjel tegi müüja kassas toimingu. Nimetatud tehingu tulemusena võeti kannatanu kontolt raha, millise summa väärtuses omastasid toimepanijad kaupa. Riigikohus märkis, et eelnimetatud tegu vastab kolmnurkkelmuse teokoosseisule, kuna petetu ja isik, kelle arvel toimus varalise kasu saamine, ei langenud omavahel kokku.[104] Täpsustuse korras märkis Riigikohus täiendavalt, et teo kvalifitseerimisel tuleb eristada olukorda, kus võõrast pangakaarti ilma selle õiguspärase omaniku loata kasutav isik sisestab kaardi kasutamisel PIN-koodi ja olukorda, kus kaarti kasutatakse ilma PIN-koodi sisestamata. Esimesel juhul on tegu KarS § 213 ehk arvutikelmuse koosseisuga ja teisel juhul KarS § 209 koosseisuga ehk kelmuse koosseisuga. Eeltoodust tulenevalt saab järeldada, et kelmuse koosseis eeldab inimese olemasolu, sest teda on võimalik eksitusse viia. Kelmusega aga ei ole tegemist juhul, kui inimese asemel on arvuti ning tehakse täiendav toiming ehk andmete ebaseaduslik sisestamine, mille tulemusena käivitatakse lubamatult andmetöötlusprotsess ning saadakse varalist kasu. [105]

Käesoleva töö seisukohast on oluline ära märkida ka Riigikohtu lahend nr 3-1-1-105-10, kus süüdistatav mõisteti süüdi omastamises. Kaasuse tehiolude kohaselt oli kannatanu täisealine

[103] RKKKo 01.07.2004, nr 3-1-1-60-04, p 6.

[104] RKKKo 10.05.2010, nr 3-1-1-35-10, p 8.1

[105] RKKKo 10.05.2010, nr 3-1-1-35-10, p 8.2.

invaliid, kes ei ole vaimse puude tõttu muu hulgas võimeline iseseisvalt tegema pangatoiminguid, sh kasutama deebetkaarti ega internetipanka. Kannatanule ei olnud määratud eestkostjat. Kannatanu asus elama noortekodusse, kus talle osutati rehabilitatsiooni teenust, mis seisnes abi osutamises igapäevaeluga toimetulekul. Kõnealust teenust osutas kannatanule noortekodu sotsiaaltöötaja ehk süüdistatav, kelle käes olid ka kannatanu deebetkaart, PIN-koodid ja internetipanga juurdepääsukoodid. Ajal, mil deebetkaart ja PIN-koodid olid süüdistatava käes, võeti kannatanu deebetkaardiga sularaha automaatidest korduvalt välja sularaha. Samuti kanti kannatanu internetipanga koode kasutades kannatanu pangakontolt raha süüdistatava ja kolmanda isiku pangakontodele. Süüdistatav pööras vähemalt 79 750 krooni enda ja kolmanda isiku kasuks.[106] Riigikohus märkis, et käesoleval juhul hoidis süüdistatav kannatanu deebetkaarti ja PIN-koode ebaseaduslikult enda valduses. Õigus juurdepääsuks kannatanu pangakontole ja seega ka õigus vallata seda võimaldavat maksevahendit ja isikustatud turvaelemente võinuks kannatanu enda kõrval või asemel olla üksnes kannatanu eestkostjal. Käesoleval juhul aga ei olnud sotsiaaltöötaja näol tegu kannatanu eestkostjaga.[107] Riigikohus viitas lahendis ka kurvale tõsiasjale, et võõraste maksevahendite (nt pangakaartide) hoidmine selleks õigust mitteomavate isikute käes on Eesti hoolekandeasutustes levinud praktika. Eeltoodud asjaolusid arvesse võttes saab tõstatada küsimuse, kas eelkirjeldatud tegu oleks võimalik kvalifitseerida omastamise asemel ka arvutikelmusena? Sotsiaaltöötaja kasutas kannatanu kontole juurdepääsu saamiseks kannatanu pangakaarti ja arvelduskontot ebaseaduslikult, kuna sisestas PIN-koodid ebaseaduslikult ja temale usaldatud vara oli saadud ilma õigusliku aluseta (vt juba eelnevalt käesolevas töös viidatud Riigikohtu lahendi 3-1-1-83-07 seisukohti). Siinkohal tasuks tähelepanu pöörata juba käesolevas töös välja toodud Riigikohtu otsuse nr 3-1-1-114-12 seisukohale, et süüdistatava poolt tehtud ülekannet ei ole võimalik kvalifitseerida omastamisena, kuna süüdistatav ei omanud ülekande tegemise ajal (äriühingu) internetipanka sisenemiseks ega arvelduskontol oleva raha käsutamiseks õiguslikku alust. Kuna sotsiaaltöötajal puudus samuti õiguslik alus kannatanu deebetkaardi kasutamiseks, siis kas sotsiaaltöötaja tegu kvalifitseeriti õigesti omastamisena? Kuna arvelduskontol olev raha näol on tegemist arvelduskonto omaniku varalise nõudega panga vastu arvelduskontol näidatud ulatuses ja arvestades asjaõigusseaduse §-s 30 sätestatut, ei toimu ülekannete tegemisel valduses oleva võõra vallasasja enda kasuks pööramist. Seega on omastamise süüteokoosseisu esimene teoalternatiiv välistatud. Omastamise teine teoalternatiiv näeb ette isikule usaldatud muu võõra vara ebaseaduslikult

[106] RKKKo 23.02.2011, nr 3-1-1-105-10, p 9.1.

[107] RKKKo 23.02.2011, nr 3-1-1-105-10, p 15.

enda või kolmanda isiku kasuks pööramist. Vara usaldamisega ei ole tegemist juhul, kui arvelduskontole juurdepääsu võimaldavad vahendid satuvad isiku valdusesse arvelduskonto omaniku nõusolekuta, samuti kui need antakse talle vaid hoiule ilma konto kasutamise ja käsutamise õiguseta (vt Riigikohtu lahend nr 3-1-1-83-07 p-d 14, 15 ja 16). Käesoleva kaasuse tehiolusid arvestades, et sotsiaaltöötajale anti kannatanu internetipanga paroolid hoiule ja tal puudus õiguslik alus nende kasutamiseks (kuna sotsiaaltöötaja ei olnud kannatanu eestkostja), siis võiks nimetatud tegu kvalifitseerida ka arvutikelmusena.

Riigikohtu 17. jaanuari 2013 otsus asjas nr 3-1-1-128-12 annab juhiseid selle kohta, millal tuleks isik arvutikelmuses süüdi tunnistada. Siinkohal tuleks mainida, et tegu on olulise lahendiga, mille valguses tuleks seada nii mõnedki alama astme kohtute otsustes kvalifitseeritud süüteokoosseisud küsimärgi alla. Kaasuse asjaolude kohaselt mõistis maakohtu kahtlustatava süüdi arvutikelmuses selles, et süüdistatav võttis kannatanult röövitud pangakaartidega sularahaautomaadist kannatanu PIN-koodi kasutades omastamise eesmärgil välja korduvalt sularaha.[108] Maakohus mõistis A. R. muuhulgas süüdi ka arvutikelmuses KarS § 213 lg 1 järgi selles, et ta võttis kannatanult röövitud pangakaartidega sularahaautomaadist pannatanu PIN-koodi kasutades omastamise eesmärgil korduvalt sularaha. Tallinna Ringkonnakohus jättis maakohtu otsuse muutmata. Riigikohus aga mõistis A. R. arvutikelmuses õigeks ja märkis, et maakohus tuvastas A. R. käitumises nii KarS § 213 lg 1 objektiivse kui ka subjektiivse külje ja õigusvastasust ning süüd välistavate asjaolude mitteesinemist. Süüdistatavale ei saa KarS § 213 lg 1 sätestatud kuritegu omistades hinnata süüdistatava käitumist lahus sellele teole eelnevatest tegudest. A. R. on juba süüdi mõistetud röövimises ja mõrvas röövimise eesmärgil, mille käigus ta omastas kannatanute pangakaardid. Süüdistatavale heideti arvutikelmuse toimepanemises ette just nende samade röövitud pangakaartide ebaseaduslikku kasutamist. Riigikohus märkis, et süüdistatava eesmärgiks ei olnud plastikkaardi kui asja omastamine, vaid ligipääs nende abil kannatanu sularahale. „Vaadeldes süüdistatava käitumist ühtse tervikuna, saab sedastada, et pangakaartide ja PIN-koodide sisestamisega ning sularaha väljavõtmisega kannatanute pangakontolt jätkas A. R. alustatud röövimist, st võttis ära võõra vallasasja selle omastamise eesmärgil.“ Kohtud tunnistasid A. R. arvutikelmuses süüdi tegudes, mis on hõlmatud juba eelnevalt toime pandud tegude (röövimine ja röövmõrva) koosseisudes sisalduva ebaõigusega. Arvutikelmuse järgi subsumeeritud kuriteo näol oli tegemist sisuliselt röövimise ja röövmõrva jätkumise ning nendes koosseisudes neelduva järelteoga. Seetõttu mõistis Riigikohus süüdistatava

[108] RKKKo 17.01.2013, nr 3-1-1-128-12, p 2.4.

arvutikelmuse toimepanemises õigeks.[109] Olgu öeldud, et käesoleva lahendi olulisus seisneb just selles, et see annab kohtutele suunise, kuidas edaspidi kvalifitseerida näiteks varastatud pangakaardiga sularaha väljavõtmist, milliseid kaasuseid on meie alama astme kohtu praktikas küllaldaselt. Riigikohtu seisukohta võiks tõlgendada selliselt, et kuna käesoleval juhul tungis A. R. kannatanu koju just eesmärgiga röövida kannatanult vägivalla abil pangakaart koos selle PIN-koodiga ja sularaha, siis tuleb kannatanu süüdi mõista vaid röövimises ja röövmõrvas, mitte aga arvutikelmuses, kuna A. R. jätkas pangakaartide ja PIN-koodide sisestamisega ning sularaha väljavõtmisega kannatanute pangakontolt alustatud röövimist, st võttis ära võõra vallasasja selle omastamise eesmärgil. Kui A. R. oleks tunginud kannatanu elamisse eesmärgiga varastada televiisor ja selle käigus sattusid tema valdusesse ka kannatanu pangakaart ja PIN-koodid (mis lebasid televiisori kõrval) ja A. R oleks seejärel läinud nimetatud pangakaardiga kannatanu arvelt sularaha välja võtma, siis kuidas sellist kuritegu kvalifitseerida? Kas me saaks sellisel juhul endiselt öelda, et A. R. jätkas kannatanu pangakontolt sularaha välja võttes röövimist? Siinkohal leiab käesoleva töö autor, et eeltoodud näite puhu oleks A. R. tulnud süüdi mõista lisaks röövimisele ja röövmõrvale ka arvutikelmuses, sest tegu on täiesti iseseisva kuriteoga. Siinkohal tuleks eristada kahte erinevat olukorda: esimesel puhul sisenes A. R. kannatanu elamusse, et varastada just pangakaart ja PIN-koodid, eesmärgiga saada endale kannatanu pangakontol olev raha; teisel juhul sisenes A. R. kannatanu elamusse eesmärgiga röövida televiisor, kuid nähes televiisori kõrval olevat pangakaarti koos PIN-koodiga, võttes need kaasa ja võtta nendega kannatanu pangakontolt sularaha, otsustas ta lisaks röövimisele toime panna ka arvutikelmuse. Sellisel juhul ei ole võimalik enam rääkida röövimise jätkamisest ja A. R. tuleks süüdi mõista nii röövimises kui ka arvutikelmuses.

„Pangaautomaat on panga seade, mis võimaldab kliendil välja võtta sularaha ööpäevaringselt. Selleks antakse kliendile magnetilindiga kaart, millele on kodeeritud tema identifitseerimisnumber (PIN-kood). Pank ja klient sõlmivad kaardi kasutamise kohta vastava lepingu.“[110] „Sageli on pangakaardiga manipuleerimine võimalik üksnes andmetöötlusprotsessi sekkumisega, sest pangaautomaat on lülitatud arvutivõrku.[111] Kui keegi saab teada teise isiku PIN-koodid, siis on tal võimalk sularahaautomaadi kaudu kas makseid teostada või siis sularahaautomaadist raha välja võtta. Kuna Eestis ei ole sularahaautomaadi kaudu maksete tegemise võimalus just kuigi populaarne (selleks kasutatakse tavaliselt

[109] RKKKo 17.01.2013, nr 3-1-1-128-12, p 10.1.

[110] J. Sootak. Varavastsed süüteod. Juura, 2009, lk 204.

[111] Samas, lk 205.

internetipanga keskkonda), siis ei ole käesoleva töö autor suutnud tuvastada ühtegi kohtulahendit, mis puudutab sularahaautomaadi kaudu maksete tegemist. See-eest on aga deebetkaardi abil sularaha väljavõtmisega seotud juhtumeid ohtralt. Deebetkaarti saab lisaks eelnevale kasutada ka poes kaupade või teenuste eest tasumiseks. Kuna sularahaautomaati ja deebetkaarti kasutades on tehtavate tehingute arv ning võimalused piiratud, siis on ka antud lahendid suhteliselt ühetaolised. Täpsemalt võiks välja tuua kolme erinevat tüüpi juhtumeid: esimese puhul on süüdistatav deebetkaardi ja sinna juurde kuuluvad PIN-koodid kannatanult varastanud, teisel juhul on süüdistatav juba eelnevalt PIN-koodidest teadlik ning on vaja vaid kannatanu deebetkaart oma valdusesse saada ja kolmandal juhul on deebetkaart ja PIN-koodid süüdistatavale usaldatud.

Kohtulahendis nr 1-08-17233 kirjeldatakse juhtumit, kus süüdistavaid on mitu ja nad tegutsevad koos. Kaasuse asjaolude kohaselt rööviti kannatanult hilisõhtul poe juures elukaaslase pangakaart. Ta teatas süüdistatavale pangakaardi PIN-koodi, et vältida edasist peksmist. Väidetavalt võeti peksmise ajal kannatanu taskust pangakaart ja pärast PIN-koodide avalikustamist jooksid süüdistatavad minema. Hommikul ärgates märkas kannatanu, et tema elukaaslase pangakaart oli taas tema taskus, kuid hiljem selgus siiski, et kannatanu elukaaslase pangaarvelt võeti öösel neljal korral ühest ja samast pangaautomaadist välja sularaha kokku summas 7600 krooni. Pangakontori turvalintidelt nähtus, et just süüdistatavad omastasid kannatanu elukaaslase pangaarvelt ebaseaduslikult raha. Käesolevas asjas ei suudetud aga kindlaks teha asjaolu, kas kannatanut peksti või mitte, kuna süüdistatavad väitsid, et kannatanu magas bussipeatuses ja nemad varastasid pangakaardi koos PIN-koodidega kannatanu taskust. Eeltoodud asjaoludele tuginedes leidis kohus, et tegu oli arvutikelmusega KarS § 213 lg 1 järgi. Süüdistatavad panid teo toime ühiselt, ühtse ja otsese tahtlusega raha saamiseks. Andmete töötlemisprotsessi lülitumisega omaniku tahte vastaselt ning andmete lubamatu käivitamisega pangaautomaadis ja seda korduvalt eesmärgil omastada võõralt kontolt sularaha näitabki kuriteo objektiivse koosseisu täitmine süüdistatava X otsest tahtlust. Olulise teopanuse teo valmistamisel kuriteo lõpuleviimisel andis süüdistatav X, kuid teine süüdistatav, olles raha väljavõtmise ajal selle juures, pannes pangakaardi tagasi kannatanu taskusse, võttes endale osa rahast, tegutsedes ühiselt ja kooskõlastatult esimese süüdistatavaga, seega kaastäideviijana.[112] Riigikohus väljendas üheselt oma 14. juuni 2006.a. kohtuotsuses nr 3-1-1-43-06 seisukohta, et teovalitsemise teooriast tulenevalt pole nõutav, et kaastäideviijana käsitletav isik realiseeriks ise kas tervikuna või osaliselt süüteo objektiivse

[112] Harju Maakohtu otsus 18.02.2009, nr 1-08-17233/7.

koosseisu, on oluline, et iga kaastäideviija lisaks tagajärje saabumisse teoühtsust silmas pidades teopanuse. Kaastäideviimisel vastutab üks isik ka teise poolt faktiliselt tehtu eest nii, nagu ta oleks seda ise teinud.[113] Riigikohtu lahendis nr 3-1-1-128-12 toodud seisukohtade valguses peab käesoleva töö autor vajalikuks analüüsida, kas maakohus kvalifitseeris nimetatud teo õigesti just arvutikelmusena. Praegusel juhul nähtub maakohtu otsuses toodud asjaoludest, et kohus ei suutnud tuvastada, kas kannatanut peksti või mitte, kuna süüdistatavad väitsid, et kannatanu magas bussipeatuses ja nemad varastasid pangakaardi koos PIN-koodidega kannatanu taskust. Kuna pangakaardi röövimist et suudetud tuvastada, siis oleks kohus pidanud kaaluma, kas antud kuritegu ei ole tulnud kvalifitseerida hoopis vargusena ja arvutikelmuse näol oli tegu lihtsalt varguse jätkumisega ja vaguse koosseisus neelduva järelteoga. Süüdistatavad panid kaasuse asjaolude kohaselt toime varguse, mille käigus nad omastasid kannatanu elukaaslase pangakaardi. Selle sama varastatud pangakaardi ebaseaduslikku kasutamist heitiski maakohus süüdistatavatele ette. Ilmselgelt ei olnud süüdistatavate teo, s.o varguse eesmärgiks plastikkaardi kui asja omastamine, vaid ligipääs selle abil kannatanu (elukaaslase) sularahale. Vaadeldes ka siinkohal süüdistatavate käitumist ühtse tervikuna, saab sedastada, et pangakaardi ja PIN-koodi sisestamisega ja sularaha väljavõtmisega kannatanu (elukaaslase) pangakontolt jätkasid süüdistatavad vargust, st võttis ära võõra vallasasja selle omastamise eesmärgil. Maakohus tunnistas süüdistatavad süüdi KarS § 213 lg 1 järgi teos, mis on juba hõlmatud varguse koosseisus sisalduva ebaõigusega. Arvutikelmuse järgi subsumeeritud kuriteo näol oli tegemist sisuliselt varguse jätkumise ja varguse koosseisus neelduva järelteoga. Seetõttu oleks pidanud maakohus nimetatud teo kvalifitseerima hoopis vargusena, mitte arvutikelmusena.

J. R. süüdistati selles, et olles ajavahemikul 19.04.2004 kuni 07.06.2007 OÜ VC juhatuse liikmeks ning omades OÜ VC nii Hansapanga kui ka Sampo panga arveldusarvel olevate rahaliste vahendite käsutamisõigust, mh vallates juhatuse liikme kohustuste täitmiseks kõiki OÜ VC pangakaarte, pööras OÜ VC rahalisi vahendeid enda kasuks järgmiselt. J. R. võttis ajavahemikul 11.01.2005 kuni 04.10.2005 alusetult OÜ VC Hansapanga arvelduskontolt sularahas välja 127 625 ning Sampo panga arvelduskontolt 584 300 krooni. Samuti võttis ta alusetult pangakontorites Hansapanga arveldusarvelt sularahas välja 800 krooni ning Sampo panga arveldusarvelt 25 000 krooni.[114] Maakohus leidis õigesti, et käesolev kuritegu tuleb kvalifitseerida omastamisena KarS § 201 lg 2 p 2 järgi. Karistusseadustiku algredaktsioonis

[113] RKKKo 14.06.2006, nr 3-1-1-43-06, p 8.

[114] Harju Maakohtu otsus 19.07.2012, nr 1-10-6319.

nägi § 201 ette vastutuse üksnes valduses oleva võõra vallasasja enda kasuks pööramise eest, kuid pangakontol oleva raha näol ei ole tegu vallasasjaga. 17. detsembri 2003 seadusemuudatusega kõrvaldati see lünk ja nüüd hõlmab § 201 koosseis objektina ka isikule usaldatud muu võõra vara. Mõistagi on tegemist asja, mitte aga vara omastamisega, kui isik võtab oma volitusi kasutades firma või muult võõralt pangakontolt sularaha, mille pöörab enda kasuks.[115] Vara omastamine on seega toime pandud juhul, kui isik, kellele on vara usaldatud, teeb selliseid toiminguid (rahaülekandeid), milleks teda volitatud ei ole, pöörates vara enda või kolmanda isiku kasuks.[116]

Eelmise juhtumiga peaaegu analoogse juhtumi leiame ka Harju Maakohtu otsusest nr 1-13-792, kus süüdistatav oli samaaegselt kahe erineva ettevõtte juhatuse liige. Esimene ettevõte andis teisele ettevõttele laenu ja süüdistatav teise ettevõtte juhatuse liikmena tegi esimesele ettevõttele laenu katteks tagasimakseid oluliselt suuremas summas, kui ta laenu sai. Nimetatud teoga omastas süüdistatav tema valduses oleva esimese ettevõtte rahalisi vahendeid teise ettevõtte kasuks kogusummas 1 180 000 krooni. Samuti tema, olles teise ettevõtte juhatuse liige, pööras enda kasuks teise ettevõtte rahalisi vahendeid, võttes teise ettevõtte arvelduskontolt välja temale väljastatud teise ettevõtte deebetkaardiga kokku 1 069 000 krooni ning omastas selle. Maakohus kvalifitseeris sellised süüdistatava teod õigesti omastamisena. Samuti tema, olles teise ettevõtte juhatuse liikme kohalt tagasi kutsutud, jättis uuele juhatuse liikmele üle andmata äriühingu pangakaardi ja PIN-koodid, võttis teatud ajavahemikul ettevõtte arvelduskontolt deebetkaardiga välja 1 143 000 krooni Nimetatud teo kvalifitseeris maakohus arvutikelmusena. Samuti tema, olles juhatuse liikme kohalt tagasi kutsutud, kasutades ära olukorda, kus Äriregistris oli ettevõtte B-kaardil sellekohane kanne tegemata, võttis ta pangakontoris ettevõtte arvelduskontolt välja sularaha. Maakohus märkis õigesti, et viimaste tegude näol on tegemist kelmusega (KarS § 209), kuna süüdistatav lõi varalise kasu saamise eesmärgil SEB Panga töötajale ebaõige ettekujutuse, ta võttis pettuse teel välja ettevõtte pangakontolt pangakontorite sularaha ja omastas selle.[117] Nimetatud kaasus on väga hea näide selle kohta, et deebetkaardiga sularaha väljavõtmist on võimalik kvalifitseerida väga mitmeti. Et seda õigesti teha, siis tuleb tähelepanu pöörata just pisidetailidele.

[115] J. Sootak (viide 111), lk 121.

[116] E. Elkind (viide 72), lk 335.

[117] Harju Maakohtu otsus 15.02.2013, nr 1-13-792.

S. V. mõisteti KarS § 199 lg 2 p 9 järgi selles, et ta võttis Viru Keskuse WC ruumis võõra vallasasja ebaseadusliku omastamise eesmärgil kannatanu taskust rahakoti, milles olid muuhulgas ka Nordea panga deebet- ja krediitkaardid koos PIN-koodidega. Samuti mõisteti S. V. süüdi arvutikelmuse toimepanemises KarS § 213 lg 1 järgi selles, et tema varalise kasu saamise eest andmete ebaseadusliku sisestamisega pangaautomaati, et saada juurdepääs võõrale arvelduskontole ning omaniku nõusolekuta käivitada andmete töötlusprotsess kontol oleva varaga toimingute tegemiseks, saanud ligipääsu kannatanu pangakontole Nordea pangas, st sisestades ebaseaduslikul teel saadud ehk kannatanult varastatud Nordea panga pangakaardi koos PIN-koodiga, võttis kolm korda Nordea panga sularahaautomaadist sularaha kokku summas 1700.[118] Olgu öeldud, et töö autori arvamuse kohaselt tunnistas maakohus S. V. õigesti süüdi nii varguses kui ka arvutikelmuses. Sellisele arvamusele on võimalik jõuda Riigikohtu 17. jaanuari 2013 otsusese nr 3-1-1-128-12 seisukohti tõlgendades. Nimetatud otsuses leidis Riigikohus järgmist: „süüdistatavale KarS § 213 lg-s 1 sätestatud kuritegu omistades ei saa hinnata süüdistatava käitumist lahus sellele teole eelnevatest tegudest.“[119] Käesoleval juhul tunnistati S. V. süüdi õigesti KarS § 199 lg 2 p 9 järgi varguses, mille käigus omastas ta kannatanu rahakoti. Hiljem avastades, et kannatanu rahakotis olid ka kannatanu pangakaardid koos PIN-koodidega, otsustas ta neid kasutades pangaautomaadist kannatanu kontolt sularaha välja võtta. Käesoleva töö autor leiab, et maakohus kvalifitseeris siinkohal sularaha väljavõtmise õigesti arvutikelmusena. Süüdistuses KarS § 213 lg 1 järgi heidetakse kannatanule küll ette seda, et ta kasutas eelnevalt varastatud pangakaarti ebaseaduslikult, kuid rahakoti varguse eesmärgiks ei olnud pangakaardi ja PIN-koodi varastamine (kuna ta ei saanud teada, et need kannatanu rahakotis on), vaid rahakoti ja selle sees olnud sularaha varastamine. Alles hiljem selgus, et varastatud rahakotis oli ka pangakaart koos PIN-koodidega. Eeltoodust tulenevalt ei ole võimalik vaadelda süüdistatava käitumist ühtse tervikuna, millest tulenevalt ei ole võimalik ka sedastada, et pangakaardi ja PIN-koodi sisestamisega ning sularaha väljavõtmisega kannatanu pangakontolt jätkas süüdistatav alustatud vargust. Eeltoodust tulenevalt saab siinkohal väita, et maakohus mõistis süüdistatava õigesti süüdi nii varguses kui ka arvutikelmuses.

Deebetkaardiga raha väljavõtmist on võimalik kvalifitseerida ka omastamisena. Pärnu Maakohus mõistis T. K. süüdi omastamises KarS § 201 lg 2 p 1 järgi selles, et tema kasutas teatud ajavahemikus temale eelnevalt R. I. poolt koos PIN-koodiga usaldatud x panga

[118] Harju Maakohtu otsus 09.08.2012, nr 1-12-7420

[119] RKKKo 17.01.2013, nr 3-1-1-128-12, p 10.1.

deebetkaarti, millega sai juurdepääsu kannatanu arvelduskontole viisil, milleks R. I. teda ei volitanud, võttes panga sularahaautomaadist kaheksal järjestikulisel korral välja 100 eurot sularaha, millega pööras temale usaldatud võõra vara enda kasuks. Lisaks sellele kasutas T. K. talle eelnevalt R. I. Poolt koos PIN-koodiga usaldatud x panga deebetkaarti, millega sai juurdepääsu kannatanu arvelduskontole, viisil, milleks R. I. Teda ei volitanud, kastes kaupluses erinevate esemete eest, millega pööras temale usaldatud võõra vara enda kasuks.[120] Nimetatud juhul on õigustatud süüdistatava eeltoodud tegude kvalifitseerimine omastamisena (II teoalternatiiv). Käesoleval juhul andis R. I. Nõusoleku T. K.-le oma arvelduskontole ligipääsuks ja sellel oleva raha käsutamiseks. Kuna R. I. tegi selliseid toiminguid (võttis sularaha välja ja maksis poes erinevate kaupade eest), milleks teda ei olnud volitatud ja pööras vara enda kasuks, siis on omastamise koosseis täidetud.

Märkimist väärt juhtumi asjaolud nähtuvad Harju Maakohtu otsusest nr 1-12-5954. Vanemale naisterahvale pakkus abi noormees, kes saatis kannatanu bussiterminali. Sinna jõudes küsis mees, kas kannatanu sooviks koos temaga ehk toidupoodi minna. Koos mindi poodi ja kannatanu soovis kaupade eest maksta kassas kaardiga. Ta sisestas PIN-koodi, kuid kaardilugeja näitas viga. Süüdistatav pakkus oma abi ja kannatanu ütles meesterahvale oma PIN-koodi, mille viimane kaardilugejasse sisestas. Pärast ostu sooritamist pani kannatanu pangakaardi oma käekotti. Meesterahvas ütles, et saadab kannatanu koju. Kui kannatanu sellest keeldus, saatis meesterahvas kannatanut sellest hoolimata. Meesterahvas läks koos kannatanuga kannatanu koju ja viimane pakkus talle süüa. Pärast seda meesterahvas lahkus korterist. Hiljem avastas kannatanu, et esikus rippunud käekott oli avatud ja sealt oli varastatud tema deebetkaart, mida ta poes kasutas. Süüdistatav aga võttis kannatanult varastatud pangakaardiga sularahaautomaadist kannatanu pangakontolt välja sularaha. Maakohus kvalifitseeris sellise juhtumi arvutikelmusena.[121] Siinkohal võib korraks mõelda, kas tegemist ei olnud omastamisega, kuna kannatanu ütles süüdistatavale PIN-koodi vabatahtlikult, kuid selline seisukoht oleks ekslik. Kannatanu ei usaldanud süüdistatavale oma pangakaarti koos PIN-koodidega selleks, et süüdistatav saaks kannatanu arvelduskontole juurdepääsu ja saaks arvelduskontol tehinguid teha. Seega ei ole võimalik siinkohal omastamisest rääkida. Tuginedes Riigikohtu lahendis nr 3-1-1-128-12[122] toodud seisukohtadele, võiks kirjeldatud teo kvalifitseerida hoopis vargusena. KarS § 213 lg 1 järgi kvalifitseeritud tegu on juba hõlmatud varguse koosseisus sisalduva ebaõigusega.

[120] Pärnu Maakohtu otsus 26.02.2013, nr 1-13-856.

[121] Harju Maakohtu otsus 11.09.2012, nr 1-12-5954

[122] RKKKo 17.01.2013, nr 3-1-1-128-12.

Arvutikelmuse järgi subsumeeritud kuriteo näol oli tegemist sisuliselt varguse koosseisus neelduva järelteoga, kuna süüdistatav varastas vaid kannatanu deebetkaardi põhjusel, et saada selle abil ligipääs kannatanu pangakontol olevale sularahale. Käesolev juhtum on õpetlik just selle poolest, et oma pangakaardi PIN-koode ei ole arukas mitte kellelegi usaldada. Kui rahakotis ei ole PIN-koode, kuid seal on pangakaart ja isikule on PIN-kood juba eelnevalt teada, siis pangakaardi varastamine ei pruugi olla nii raske. Juhul kui kannatanu ei oleks praegusel juhul süüdistatavale oma PIN-koodi teatavaks teinud, ei oleks süüdistataval olnud võimalust ka kannatanu arvelduskontolt raha välja võtta.

Töö autor soovib juhtida veel tähelepanu sellele, et maakohtu otsustest nähtuvalt on võimalik analoogseid kuritegusid vähemalt kolmel erineval moel kvalifitseerida. Eeltoodu kinnituseks toon alljärgnevad näited.

Harju Maakohus tunnistas V. O. süüdi varguses KarS § 199 lg 2 p 4 järgi selles, et tema võttis võõra vallasasja ebaseadusliku omastamise eesmärgil Tallinnas, kannatanu korterist M. P.-le kuuluva pangakaardi ja teades kannatanu pangakaardi PIN-koodi, võttis M. P. tahte vastaselt ja ilma viimase nõusolekuta M. P. arvelduskontolt korduvalt välja sularaha. Sellise tegevusega pani V. O. Toime võõra vallasasja äravõtmise selle ebaseadusliku omastamise eesmärgil, so kuriteo, mis on kvalifitseeritav KarS § 199 lg 2 p 4 järgi.[123] Siinkohal nähtub, et maakohus järgis Riigikohtu otsuses nr 3-1-1-128-12 toodud juhendit selle kohta, et sellistel juhtudel, kui varastatakse vaid pangakaart ja isik mõistetakse juba varguses süüdi, siis on arvutikelmuse järgi subsumeeritud kuriteo näol tegemist sisuliselt varguse jätkumise ja varguse koosseisus neelduva järelteoga. Samuti leidis Riigikohus lahendis nr 3-1-1-60-04, et pangakaardi ja PIN-koodide kasutamise teel teise isiku arveldusarvelt sularaha väljavõtmise näol on tegu vargusega. Sellises olukorras kasutab süüdlane rahatähtede üle oma valduse kehtestamiseks pangakaarti kui kuriteovahendit ehk riista, millega kõrvaldatakse tõke võõra vara juurde pääsemiseks (antud kaasuses kannatanute arvelduskontol olev raha). Pangaautomaadi väljutamisavas olev rahasumma kuulub seejuures kannatanule, olenemata sellest, kes pangakaardi ja/või PIN-koodi sisestas. Selle rahasumma äravõtmise hetkel lõpeb valduse murdmine ja võõras raha võetakse ära, s.o pannakse toime varavastane kuritegu, mille kvalifikatsioon võib sõltuda sellest, milliste vahenditega on pangakaart ja PIN-kood süüdlase valdusesse läinud.[124] Kuna käesoleva kaasuse asjaolude kohaselt varastas süüdistatav

[123] Harju Maakohtu otsus 06.03.2013, nr 1-13-1706.

[124] RKKKo 01.07.2004, nr 3-1-1-60-04, p 6.

pangakaardi ja PIN-koodid, siis kvalifitseeris maakohus teo õigesti vargusena KarS § 199 järgi, mitte arvutikelmusena KarS § 213 lg 1 järgi.

Eelneva kaasusega sarnased asjaolud on välja toodud ka Pärnu Maakohtu otsuses nr 1-13-418, kuid käesoleval juhul mõistis kohus V. M. süüdi hoopis arvutikelmuse toimepanemises KarS § 213 lg 1 järgi. Süüdistatav, viibides teatud ajavahemikul külas R. S. elukohas, võttis elutoa laualt võõra vallasasja ebaseadusliku omastamise eesmärgil R. S. arvelduskonto kasutamiseks R. S. nimele välja antud deebetkaardi koos PIN-koodiga ning andmete ebaseadusliku sisestamise ja andmetöötlusprotsessi ebaseadusliku sekkumise teel varalise kasu saamise eesmärgil kontoomaniku nõusolekuta võttis sularahaautomaadist korduvalt välja sularaha, saades R. S. arvelduskontolt ebaseaduslikult kokku rahalisi vahendeid üldsummas 2980 eurot ja tekitas kahju teenustasude näol üldsummas 28,17 eurot.[125] Samuti Viru Maakohus mõistis N. V. süüdi arvutikelmuses KarS § 213 lg 1 järgi selles, et tema, varalise kasu saamise eesmärgil, teatud ajavahemikul varastas kannatanu pangakaardi, mille sisestas ebaseaduslikult pangaautomaati ja tegi andmetöötlusprotsessi ebaseadusliku sekkumise teel kannatanu arvelduskontolt viimase nõusolekuta ülekandeid, millega ta sai varalist kasu 27 500 krooni ja tekitas kannatanule sama summa eest varalist kahju. Oma nimetatud tegudega pani N. V. toime varalise kasu saamise andmete andmetöötlusprotsessi ebaseadusliku sisestamise teel, so KarS § 213 lg-s 1 ettenähtud kuriteo.[126] Kuigi käesolevas lõigus toodud kaasuste asjaolud on põhimõtteliselt analoogsed eelmises lõigus toodud Harju Maakohtu otsuses nr 1-13-1706 välja toodud asjaoludega, siis käesoleval juhul kvalifitseerisid kohtud süüdistatavate teod ekslikult arvutikelmustena. Töö autor on juba eelnevalt selgitanud, millest tulenevalt oleks tulnud sellised teod kvalifitseerida vargustena ja seetõttu ei ole otstarbekas sellekohast analüüsi siia uuesti lisada.

Viru Maakohus mõistis A. S. süüdi varguses KarS § 199 lg 2 p 8, 9 järgi selles, et süüdistatav tungis kannatanu korterisse ja varastas sealt erinevaid esemeid, mille hulgas oli ka krediitkaart kannatanu nimele. Samuti süüdistatav, kasutades korterist varastatud krediitkaarti M. R. nimele koos PIN-koodiga, pani toime sularahaautomaadist M. R.-le kuuluvalt arvelt kolmel korral sularaha varguse. Oma tegevusega pani A. S. toime võõra vallasasja äravõtmise selle ebaseadusliku omastamise eesmärgil, sissetungimisega, süstemaatiliselt, st. KarS § 199 lg 2 p 8, 9 ettenähtud kuriteo.[127] Nimetatud kaasuse asjaoludest näeme, et süüdistatav tungis

[125] Pärnu Maakohtu otsus 23.01.2013, nr 1-13-418.

[126] Viru Maakohtu otsus 01.11.2012, nr 1-12-9554.

[127] Viru Maakohtu otsus 12.09.2012, nr 1-12-6741.

kannatanu korterisse ja varastas sealt erinevaid esemeid (sh ka pangakaardi koos PIN-koodidega) ja kasutas hiljem varastatud pangakaarti sularaha väljavõtmiseks. Maakohus otsustas teo kvalifitseerida vaid vargusena ega pidanud vajalikuks analüüsida, kas varastatud pangakaardiga sularaha väljavõtmisel on täidetud ka arvutikelmuse koosseis ning kui jah, siis kas süüdistatav vastutab vaid varguse või ka arvutikelmuse eest. Kohtulahendis puudub igasugune analüüs, miks maakohus süüdistatava teo just vargusena kvalifitseeris. Käesoleva töö autor leiab, et maakohus oleks pidanud A. S. süüdi mõistma nii varguses kui ka arvutikelmuses.

Harju Maakohus mõistis S. K. süüdi KarS § 199 lg 2 p 9 ja KarS § 213 lg 1 järgi selles, et tema tungis teatud ajavahemikus ukse avamise teel kannatanu korterisse ning võttis korterist võõra vallasasja ebaseadusliku omastamise eesmärgil ära erinevaid asju, sh AS SEB Pank ja Swedbank AS deebetkaardid, Swedbank AS hanzaneti ja AS SEB Pank u-neti internetipanga koodikaardid. Seega S. K. võõra vallasasja äravõtmisega selle ebaseadusliku omastamise eesmärgil sissetungimisega ja süstemaatiliselt pani toime KarS § 199 lg 2 p 8, 9 järgi kvalifitseeritava kuriteo. Samuti tema, varalise kasu eest andmete ebaseadusliku sisestamisega pangaautomaati, et saada juurdepääs võõrale arvelduskontole ning omaniku nõusolekuta käivitada andmete töötlusprotsess kontol oleva varaga toimingute tegemiseks, saanud ligipääsu kannatanu pangakontole, st sisestades ebaseaduslikul teel saadud ehk kannatanult varastatud Swedbank AS deebetkaardi PIN-koodi, mille tulemusena sai süüdistatav võtta Swedbank AS pangaautomaadist sularaha kokku summas 630 eurot. Seega S. K. pani toime varalise kasu saamise eesmärgil andmete ebaseadusliku sisestamise andmetöötlusprotsessi ebaseadusliku sekkumise teel, so KarS § 213 lg 1 järgi kvalifitseeritava kuriteo.[128] Samuti Tartu Maakohus mõistis A. L. süüdi selles, et tema teatud ajavahemikus võttis muuhulgas ebaseadusliku omastamise eesmärgil Tartu Kõrgemast Kunstikoolist K. L.-le kuuluva rahakoti, milles oli K. L. nimele väljastatud AS Hansapank pangakaart ja PIN-koodid. Sellega A. L. pani toime KarS § 199 lg 2 p 8, 9 järgi kvalifitseeritava kuriteo, so võõra vallasasja äravõtmise selle ebaseadusliku omastamise eesmärgil, kui see on toime pandud sissetungimisega ja süstemaatiliselt. A. L. kahtlustatakse veel selles, et tema kasutas Tartu Kõrgemast Kunstikoolist varastatud K. L. nimele välja antud AS Hansapank pangakaarti ja PIN-koodi varalise kasu saamise eesmärgil ja võttis PIN-koodi ebaseadusliku sisestamise teel Hansapanga sularahaautomaadist K. L.-i arvelduskontolt välja sularaha kogusummas 10 000 krooni. Seega A. L. pani toime KarS § 213 lg 1 järgi kvalifitseeritava kuriteo, so varalise kasu

[128] Harju Maakohtu otsus 26.07.2012, nr 1-12-6231.

saamise muul viisil andmetöötlusprotsessi ebaseadusliku sekkumise teel.[129] Süüdistatavad mõisteti õigesti süüdi nii varguses kui ka arvutikelmuses, kuna arvutikelmust ei ole võimalik sellistel juhtumitel vaadelda varguse jätkumisena. Kuna töö autor on oma sellekohaseid seisukohti juba eelnevalt põhjendanud, siis ei ole vajalik siinkohal neid taas korrata.

Eeltoodud näidete pinnal saab varastatud pangakaardiga sularaha väljavõtmist kvalifitseerida vähemalt kolmel erineval moel. Asjaolu, et me võime Eesti aktuaalsest kohtupraktikast selliseid vastuolulisi näiteid tuua, viitab üheselt sellele, et arvutikelmuse piiritlemine on väga oluline ja problemaatiline teema. Loodetavasti annab Riigikohus tulevikus veelgi selgemaid ja sirgjoonelisemaid juhiseid selle kohta, kuidas eristada arvutikelmust teistest varavastastest süütegudest ja kuidas neid täpselt kvalifitseerida.

3.5 Mobiiltelefonidega ja SIM-kaartidega seotud juhtumid

Mobiiltelefonidega seotud juhtumid võib liigitada kahte suurde rühma: esimesel juhul kasutatakse kannatanu mobiiltelefoni ja seal olnud SIM-kaarti tema teadmata eritariifsetele numbritele helistamiseks (mobiiltelefoni kasutatakse ajutiselt, seda varastamata või omastamata), teisel juhul aga mobiiltelefon ja selles olnud SIM-kaart kas varastatakse, omastatakse või see leitakse, misjärel kasutatakse telefoni ja selles olnud SIM-kaarti eritariifsetele numbritele helistamiseks. Käesoleval juhul tuleb tähelepanu pöörata sellele, et SIM-kaardi ebaseadusliku kasutamise puhul tuleb vahet teha SIM-kaardi kasutamisel ning mobiiltelefoni kasutamisel. Kui isik kasutab võõrast mobiiltelefoni, pannes sinna enda SIM-kaardi, ei ole tegemist arvutikelmusega. Andmetöötlusprotsessi käivitamiseks tuleb SIM-kaarti kasutada mobiiltelefonis, seejuures ei ole oluline, kas mobiiltelefon ise on võõras või mitte.[130] Et aru saada, kuidas tuleb mobiiltelefonidega ja SIM-kaartidega seotud kuritegusid kvalifitseerida, on vajalik alljärgnev kohtuotsuste analüüs.

Esimese juhtumi näitena saab tuua Viru Maakohtu lahendi nr 1-09-15620, kus kohus mõistis süüdistatava süüdi arvutikelmuses selles, et ta helistas raamatukogu lauatelefonilt kümme korda www.rate.ee tasulisele numbrile ja iga kõnega sai ta teada kuuekohalise koodi, millega laadis samal õhtul oma www.rate.ee kontole ja sai koodide eest kokku tuhande krooni eest

[129] Tartu Maakohtu otsus 13.11.2012, nr 1-11-12853.

[130] K. Masing. Arvutikelmuse piiritlemisprobleemid. Magistritöö. Tartu, 2012.

rate-raha SOL-e, mille eest on võimalik nimetatud internetikeskkonnast tellida erinevaid teenuseid.[131] Sellise juhtumi puhul puudub kahtlus, et tegu tuleb kvalifitseerida arvutikelmusena. Nimetatut kinnitab ka Tartu Maakohtu otsuses nr 1-10-8347 toodud seisukoht, et: „arvutikelmus on materiaalne kuriteokoosseis, mis seisneb andmetöötlusprotsessi sekkumises ja mille tulemusena peab süüdlane olema saanud varalist kasu. Kohus on seisukohal, et andmetöötlusprotsessina arvutisüsteemi kaudu tuleb käsitleda ka mobiiltelefoni kaasabil andmete töötlust. Ka mobiiltelefoni saab ja tuleb vaadelda seadmena, mis võimaldab täita automaatset andmetöötlus funktsiooni“.[132]

Teise tüüpjuhtumi näiteid on alama astme kohtu praktikas mitmeid. Ometi tasub siinkohal tähele panna seda, milles maakohus süüdistatavad süüdi mõistsid. Viru Maakohus mõistis A. A. süüdi KarS § 266 lg 1 (omavoliline sissetung) alusel selles, et A. A. tungis omaniku tahte vastaselt kannatanu saunamajja ja varastas sealt mobiiltelefoni koos selles olnud SIM-kaardiga. KarS § 213 lg 1 järgi mõisteti A. A. süüdi selles, et tema kasutas eelnevalt varastatud mobiiltelefonis olnud kõnekaarti ja teostas teatud ajavahemikul kõnesid, millega tekitas kõnekaardi kasutajale ehk kannatanule varalise kahju summas 1222,33 eurot.[133] Viru Maakohus mõistis J. A süüdi omastamises selles, et võttis enda valdusesse ja pööras enda kasuks parkimisplatsilt leitud kannatanule kuuluva mobiiltelefoni koos selles olnud lepingulise kõnekaardiga. Samuti mõisteti J. A. süüdi selles, et tema, kasutades varem tema poolt ebaseaduslikult omastatud mobiiltelefonis olnud kannatanu kõnekaarti ja selle PIN-koodi, teostas kõnekaarti kasutades kõnesid tasulisele lühinumbrile, millega laadis X keskkonnas samal kuupäeval varem registreeritud kontole X ning millega tekitas kannatanule varalist kahju summas 65,124 eurot.[134] T. P. süüdistati selles, et tema teatud ajavahemikul sisestas leitud ja kannatanule kuuluva mobiiltelefoni SIM kaardi oma mobiiltelefoni ja teostas erinevaid tehinguid: tegi erinevatele numbritele kõnesid, kasutas GPRS teenust, saatis SMS-e ja kasutas internetti. Kohus mõistis T. P. eeltoodud asjaoludel süüdi arvutikelmuses.[135]

Eeltoodud kaasused on analoogsed selle poolest, et süüdistatav sai kannatanu telefoni oma kasutusse (kas siis sissemurdmise, varguse, omastamise või leidmise teel) ning kasutas seejärel telefonis olnud SIM kaarti selleks, et kasutada selle poolt pakutavaid erinevaid

[131] Viru Maakohtu otsus 06.10.2009, nr 1-09-15620/6.

[132] Tartu Maakohtu otsus 03.03.2011, nr 1-10-8347.

[133] Viru Maakohtu otsus 03.09.2012, nr 1-12-8295.

[134] Viru Maakohtu otsus 31.10.2012, nr 1-12-10483.

[135] Viru Maakohtu otsus 05.12.2012, nr 1-12-11686.

võimalusi kas siis helistamiseks, sõnumite saatmiseks vms. Viidatud kaasustest nähtub, et esimeses kahes kohtuotsuses mõisteti süüdistatav süüdi nii selles teos, kuidas ta telefoni ja selles olnud SIM-kaardi sai kui ka eraldi arvutikelmuses, kuna süüdistatav kasutas telefonis olnud SIM kaarti. Kolmanda juhtumis puhul näeme, et kohus ei pidanud vajalikuks karistada T. P.-d selle eest, kuidas kannatanu telefon tema kätte sattus. Siinkohal näeme, et maakohtu praktika ei ole selle koha pealt ühtne. Erinevatest kohtulahenditest nähtub, et praegune maakohtu praktika on enamus juhtudel siiski sellel meelel, et kui telefon varastatakse ja selles oleva SIM kaardiga tehakse erinevatele numbritele kõnesid või kasutatakse muid teenuseid, siis mõistetakse isik süüdi nii selles varavastases kuriteos, mille alusel ta telefoni sai kui ka arvutikelmuses. Sellise väite kinnitusena saab tuua lisaks eeltoodud näidetele veel ka Pärnu Maakohtu otsuse nr 1-09-3680/6 [136] ja Tartu Maakohtu otsuse nr 1-12-9130.[137]

KarS § 213 lg 1 järgi mõisteti A. V. süüdi selles, et tema varalise kasu saamise eesmärgil, kasutades tuvastamata asjaoludel M. T. valdusest välja läinud A. T.-le kuuluvat mobiiltelefoni, sekkus ebaseaduslikult andmetöötlusprotsessi andmete ebaseadusliku sisestamisega ja mõjutas andmete töötlemise tulemust, teostades omaniku nõusolekuta telefonis olnud MTSIN-kaardilt erinevaid kõnesid eritariifsetele numbritele.[138]

V. K. süüdistati KarS § 213 lg 1 järgi arvutikelmuse toimepanemises selles, et tema varalise kasu saamiseks sekkus ebaseaduslikult andmetöötlusprotsessi, kasutades teatud ajavahemikul H. L. SIM-kaarti, mille viimane oli ekslikult prügikasti visanud, sest seda ei kasutatud. V. K. tegi seda SIM-kaarti kasutades kõnesid erinevatele numbritele, saatis sõnumeid ja tellis tasulisi teenuseid ilma H. L. teadmata ja tema loata, millega tekitas viimasele varalist kahju. Harju Maakohus mõistis V. K. süüdistuses KarS § 213 lg 1 järgi õigeks põhjusel, et KarS § 213 objektiivse teokoosseisu tunnuseks on andmete ebaseaduslik sisestamine mille tõttu sekkutakse andmetöötlusprotsessi ebaseaduslikult. Ainuüksi andmete (numbri, tähe vms) sisestamine seadmesse ei moodusta teokoosseisu. Tavapärane telefonil helistamine, SMS-i saatmine või isikukoodi sisestamine sõidupileti ostmiseks ei ole andmetöötlusprotsessi ebaseaduslik sisenemine KarS § 213 tähenduses. Prokurör esitas maakohtu otsuse peale apellatsiooni ja märkis, et maakohus mõistis V. K. põhjendamatult KarS § 213 lg 1 järgi õigeks. Tallinna Ringkonnakohus leidis kokkuvõtvalt seda, et: „V. K. sisestas oma mobiiltelefoni temale võõra SIM kaardi, seejärel leitud PIN koodi, identifitseeris ennast

[136] Pärnu Maakohtu otsus 21.04.2009, nr 1-09-3680/6.

[137] Tartu Maakohtu otsus 05.02.2013, nr 1-12-9130.

[138] Harju Maakohtu otsus 11.02.2013, nr 1-12-12235.

kaardi seadusliku valdajana, mis omakorda tagas talle mobiilsideteenuse kasutamise võimaluse. Selleks tal luba puudus, kuna V. K. ei olnud liitunud side teenuse osutajaga ja abonendinumber mille ta aktiviseeris, talle ei kuulunud. V. K., kasutades leitud kaarti, omandas varalise väärtusega võimaluse. Tagajärjena on kannatanu saanud ka varalist kahju, kuna teenuse kasutamise eest oli esitatud talle arve, mis kuulus tasumisele."[139] Ringkonnakohus leidis, et mobiiltelefoni kaardi leidmisel ei tekkinud V. K.-l automaatselt õigust seda kasutada ja ta sai aru või vähemalt pidas võimalikuks, et tema poolt tasulise teenuse kasutamise eest peab keegi teine maksma, et ta tekitab kellelegi varalist kahju. V. K. poolt kaardi ja koodi sisestamata jätmisel poleks andmetöötlusprotsess üldse käivitunud. Eeltoodud põhjendustel mõistis Tallinna Ringkonnakohus V. K. süüdi KarS § 213 lg 1 järgi arvutikelmuses.

Siinkohal tuleb märkida, et SIM-kaardi kasutamisega seotud kuriteod on valdavas osas toime pandud just alaealiste või siis äsja 18-aastaseks saanud isikute poolt. Suurem osa mobiiltelefonidega seotud juhtumitest olid seotud portaaliga www.rate.ee ja kujutasid endast sõnumite saatmist antud internetileheküljele virtuaalse raha ehk SOL-ide saamiseks. Harvematel juhtudel on kasutatud kannatanu mobiiltelefonis olevat SIM-kaarti selleks, et teha kõnesid muudele eritariifsetele numbritele.

3.6 Kütusekaartide ja tankimisega seotud juhtumid

Kütusekaartide ja tankimisega seotud juhtumite puhul tekivad taas piiritlemisprobleemid varguse, omastamise, kelmuse ja arvutikelmuse vahel. Kütusekaartidega maksmise puhul saame paralleele tõmmata pangakaartidega maksmise vahel. Kuidas täpselt aru saada, millise varavastase süüteo alla tuleks kütusekaartide ja tankimisega seotud juhtumid liigitada, siis tuleb selleks taas kord appi võtta erinevate kohtute lahendid.

Oluliseks ja huvitavaks Riigikohtu lahendiks võib pidada ka otsust nr 3-1-1-78-06, kus süüdistatav võttis Neste ettemaksukaardiga Neste Eesti AS automaattanklast kaardisüsteemi tarkvara rikkudes välja 17 357,76 krooni väärtuses kütust. Nimetatud ettemaksukaardil olid seejuures rahalised vahendid kütuse omandamiseks ainult 50.- krooni väärtuses. Kuna antud lahendis ei saadud menetluses antud ütlustele tuginedes tõendada kütuseautomaadiga

[139] Tallinna Ringkonnakohtu otsus 10.10.2012, nr 1-12-4215.

manipuleerimist, siis Riigikohus leidis, et süüaluse tegu on kvalifitseeritav vargusena, kuna võõras valdus asjale (bensiinile) lõpetati ja selle suhtes kehtestati uus valdus. Kuna isik kasutas teadlikult ära kaardisüsteemis olevat viga, siis kasutas isik automaadi defektsust enda huvides ära. Seega oli antud hetkel tegu valdusest loobumise vabatahtlikkuse näilisusega ja see ei vasta automaadi kasutamisettepaneku peamisele nõudele, milleks on pakkuja ja kliendi kahepoolne sooritus. Riigikohus leidis, et süüdistatav eiras seega teadlikult talle tankla poolt seatud kaardi kasutamistingimusi ja kehtestades omastamise eesmärgil valduse võõrale asjale, realiseeris KarS § 199 lg 2 p 4 koosseisu.[140] Kui käesolevas kaasuses oleks suudetud tõestada, et kütus saadi kütuseautomaadiga manipuleerimise teel, siis oleks võinud Riigikohus kõigi eelduste kohaselt kaaluda hoopis arvutikelmuse koosseisu realiseerimist.

P. S. süüdistatakse omastamises KarS § 201 lg 2 p 1 ja 3 järgi selles, et tema, olles määratud Lõuna Kaitseringkonna staabi- ja tagalakeskuse ülema ametikohale ja olles seega karistusseadusliku tähenduses ametiisikuks, omastas teatud ajavahemikul korduvalt Kaitseväele väljastatud kütusekaarti, kasutades Kaitseväele kuuluvat diislikütust isiklikuks otstarbeks, tankides selle isiklikku sõidukisse. Eeltoodud teoga põhjuseks P. S. Kaitseväele varalist kahju kogusummas vähemalt 669,16 eurot.[141] Kütusekaardiga seotud juhtumite puhul on oluline tuvastada, kuidas isik kütusekaardi enda kätte sai. Maakohus kvalifitseeris eelpoolmainitud teo õigesti omastamisena, kuna käesoleval juhul oli kütusekaart P. S.-le usaldatud tööülesannete täitmiseks. Seega oli temal õigus kütusekaarti kasutada, kuid ta ületas temale antud volituse piire ja kasutas kütusekaarti isiklikku autosse kütuse tankimiseks. Kui isik oleks saanud kütusekaardi näiteks varguse teel, siis tuleks selline tegu kvalifitseerida kas vargusena (vt Riigikohtu lahend nr 3-1-1-128-12) või arvutikelmusena.

Tartu Maakohus tunnistas E. K. süüdi KarS § 209 lg 2 p 1, 3 järgi kelmuses. E. K. süüdistati muuhulgas selles, et tema grupis koos K. K.-ga, lõi AS Sektoron kütusetanklas varalise kasu saamise eesmärgil tegelikest asjaoludest teadvalt ebaõige ettekujutuse AS Sektoron juhatuse liikmele X sellega, et E. K. sõlmis OÜ Lindemal juhatuse liikmena AS-ga Sektoron ostu müügilepingu nr 5, millega sai kütust osta krediidivõimalusega, kohustusega arved tasuda 14 päeva jooksul peale arve saamist, ettekavatsusega jätta raha maksmata. Peale lepingu sõlmimist tankis K. K. tanklast korduvalt kütet. Kelmusega põhjustas E. K. AS-le Sektoron

[140] RKKKo 6.10.2006, nr 3-1-1-78-06, p 14.

[141] Tartu Maakohtu otsus 18.10.2012, nr 1-12-9283.

varalist kahju kokku 141 221,60 krooni.[142] Maakohus kvalifitseeris sellise teo õigustatult kelmusena, kuna käesoleval juhul sai E. K. varalist kasu tegelikest asjaoludest teadvalt ebaõige ettekujutuse loomisega. Käesoleva juhtumi puhul omab tähtusust asjaolu, et olemas on reaalne isik ehk AS Sektoron juhatuse liige, keda peteti.

S. H. Laenas oma endisest töökohast Flow Service OÜ kaubiku Ford Transit, mille seest leidis Flow Service OÜ-le kuuluva kütusekaardi. Samal päeval ostis ta võõra vallasasja ebaseadusliku omastamise eesmärgil ja nimetatud kaarti kasutades ilma Flow Service OÜ nõusolekuta mitmel korral kütust. Ostetud kütuse valas S. H. kanistritesse ja müüs maha. Vargusega tekitas S. H. Flow Service OÜ-le varalist kahju kokku 9865,98 krooni. Maakohus leidis, et eeltoodud teoga pani S. H. toime KarS § 199 lg 1 järgi kvalifitseeritava kuriteo, so võõra vallasasja äravõtmise selle ebaseadusliku omastamise eesmärgil.[143] Kuna kaasuse asjaoludest nähtub lisaks eelnevale, et kaubikus olid lisaks kütusekaardile ka selle paroolid, ja ta pidi kütuse saamiseks automaati PIN-koodi sisestama, siis tuleks käesoleval hetkel kaaluda ehk hoopis arvutikelmuse koosseisu realiseerumist. Samas kui arvestada Riigikohtu lahendis nr 3-1-1-128-12 toodud seisukohti, siis kvalifitseeris maakohus nimetatud teo õigesti vargusena. Juhul kui tegu oleks olnud selvetanklaga ja tankimisel ei oleks vaja läinud PIN-koode, siis oleks tulnud sama tegu kvalifitseerida kelmusena, kuna olemas on reaalne isik, keda petetakse. Kui S. H. oleks kütuse tankimise ajal olnud endiselt Flow Service OÜ töötaja ja kütusekaart oleks olnud temale usaldatud tööauto tankimiseks, siis oleks kaasuse asjaolusid arvesse võttes kõne alla tulnud kütuse omastamine.

Et asju veelgi segasemaks ajada, siis toon järgmise näitena Tallinna Ringkonnakohtu otsuse, milles V. R. ja A. K. tunnistati süüdi KarS § 213 lg 1 järgi selles, et V. R. ühiselt ja kooskõlastatult koos A. K.-ga tankis teatud ajavahemikul korduvalt erinevates tanklates diiselkütust enda kasutuses olevasse kaubikusse kokku 34 951,30 liitrit maksumusega kokku 443 329,69 krooni, kasutades selleks A. K. valduses olevat AS-le X väljastatud kütusekaarti ilma seadusliku valdaja nõusolekuta. 31.10.2008 toimunud kütuse tankimisel esitas V. R. ise ja ülejäänud kordadel A. K. kokkuleppel A. R.-ga tankla klienditeenindajale AS Lukoil Eesti poolt AS-le X väljastatud kütusekaardi, sisestades A. K.-le töösuhte tõttu teatavaks saanud kütusekaardi PIN koodi makseterminali, käivitades selliselt kaardi seadusliku valdaja nõusolekuta andmete ebaseadusliku sisestamisega andmetöötlusprotsessi, mille tulemusena

[142] Tartu Maakohtu otsus 30.08.2012, nr 1-11-4399.

[143] Harju Maakohtu otsus 12.09.2012, nr 1-12-7258.

sai V. R. koos A. K-ga varalist kasu tangitud kütuse näol, tekitades AS-le X 443 329,69 krooni suuruses summas varalist kahju. Selline käitumine vastab KarS § 213 lg 1 tunnustele, kuna kütusekaardiga maksmiseks oli vaja täiendav toiming – andmete ebaseaduslik sisestamine, mille tulemusena käivitati lubamatult andmetöötlusprotsess. V. R. mõisteti arvutikelmuses süüdi põhjusel, et ta oli teadlik, et kütuse eest maksmisel kasutatakse võõrast kütusekaarti omaniku loata. Kuna V. R.-il oli samuti kütuse tankimise ja selle realiseerimise juures täita oluline roll, siis mõlema isiku panus süüteokoosseisu kui terviku realiseerumisse oli oluline. A. K., kes sisestas süsteemi PIN-koodi, ei pane tegu toime üksiktäideviijana olukorras, kus isikute tegu tervikuna on alust käsitleda kaastäideviijana.[144] Seega nähtub, et kohtupraktikas puudub ühtsus. käesolevas kaasuses tunnistas ringkonnakohus isikud süüdi arvutikelmuses, kuid eelmises otsuses tunnistas maakohus isikud üldjoontes analoogse teo eest süüdi varguses.

3.7 Krediitkaartidega seotud juhtumid

Varastatud, pettuse teel saadud või isikule usaldatud krediitkaardi andmete kasutamine kaardikasutaja nimele kaupade ostmiseks või teenuste kasutamiseks on käsitatav arvutikelmusena. Nimetatud alapeatükis on võimalik arvutikelmuste ja nendega seotud varavastaste süütegude piiritlemisel leida sarnaseid jooni nii internetipangaga seotud juhtumitega kui ka pangakaartidega seotud juhtumitega.

Harju Maakohtus mõistis L. M. arvutikelmuses süüdi selles, et ta kasutas teatud ajavahemikul kaardiomanike teadmise ja nõusolekuta temale mittekuuluvate krediitkaartide andmeid internetis tehingute tegemisel erinevatel veebilehtedel, tehes nimetatud kaartidega korduvalt makseid lennupiletite ja hotelliteenuste eest.[145] Kuna nimetatud otsuse asjaoludest ei selgu, millisel viisil L. M. krediitkaardi andmed enda kätte sai, siis ei ole võimalik maakohtu otsuses välja toodud asjaolude pinnalt analüüsida, kas maakohus kvalifitseeris nimetatud teo õigesti arvutikelmusena või mitte.

Kohtuasjas nr 1-139-05 on tegu krediitkaardi andmete ebaseadusliku kogumisega ja kasutamisega. Süüalune kopeeris internetist aadressilt irc.sbotirc.com 2004. a oma kasutuses

[144] Tallinna Ringkonnakohtu otsus 15.09.2011, nr 1-10-13009/36.

[145] Harju Maakohtu otsus 02.05.2011, nr 1-11-4870.

olevasse arvutisse UK ja USA kodanike isikuandmeid, krediitkaardi numbreid ja nende kasutamiseks vajalikke turvanumbreid. Süüalune, kasutades oma emaili aadressi, tasus 02.11.2004. a. kannatanu isiku-, krediitkaardi- ja turvanumbrit kasutades interneti poes tellitud kauba eest 187,41 USA dollarit, märkides interneti poes postiteel kättetoimetatava tellimuse vormistamisel kauba saaja aadressiks iseenda aadressi. Kokku tuvastati 27 käesoleva juhtumiga analoogset episoodi. Maakohus kvalifitseeris süüaluse tegevuse KarS § 213 järgi arvutikelmusena varalise kasu korduva saamisena ning saamise katsetena arvutiprogrammide ja andmete ebaseadusliku sisestamisena ja vahetamisena andmetöötlusprotsessi ebaseadusliku sekkumise teel, millega mõjutati andmete töötlemise tulemust.[146]

Siinkohal tuleb mainida, et kohus loetles otsuses sisuliselt üles kuriteo koosseisu asjaolud ja elemendid ning seejärel langetas koheselt otsuse, et tegemist oli arvutikelmusega. Kohus ei võtnud vaevaks analüüsida, kas nimetatud teo kvalifitseerimine KarS § 213 järgi on õigustatud või mitte. Maakohus lihtsalt jaatas, et tegemist oli arvutikelmusega. Kuna maakohus ei põhjendanud oma seisukohti, siis on oluline seda kontrollida. Süüalune säästis interneti vahendusel tellitud kauba maksmisel teiste isikute krediitkaardi andmeid kasutades 187,41 USA dollarit, millest tulenevalt sai süüalune varaliust kasu (arvutikelmuse objektiivsesse koosseisu element). Teiseks ja kolmandaks objektiivse koosseisu elementideks on lubamatu sekkumise ja kolmandaks, et see sekkumine on tehtud andmetöötlusprotsessi. Asjaolusid vaadates näeme, et süüalune kopeeris oma arvutisse teiste isikute isikuandmed, krediitkaardi numbrid ja nende kasutamiseks vajalikud turvanumbrid. Kopeerimist siinkohal ei saa iseenesest lugeda kuriteoks, kuna andmed pidid olema avalikud, et tavakasutaja neile ligi pääseks ja siinkohal oli teatud süü ka kannatanutel. Ometi ei loe kannatanute ettevaatamatus siin midagi, kuna süüdlane kopeeris nende andmed oma arvutisse eesmärgiga neid ebaseaduslikult kasutada. Antud juhul pani süüalune toime kuriteo siis, kui ta sisestas kauba eest tasumiseks programmi võõrad krediitkaardiandmed. Vaatleme ka kuriteo subjektiivset koosseisu, milleks on tahtlus. Subjektiivsest küljest on kelmus tahtlik kuritegu. Siinkohal võime ka vaadelda süüaluse tegusid, milleks oli teiste isikute andmete otsimine Internetist ja seejärel nende kasutamine. Seega võime antud kohal väita, et süüalune pani teo toime tahtlusega ning seega on ka arvutikelmuse subjektiivne koosseis täidetud.[147]

[146] Viljandi Maakohtu otsus 02.05.2005, nr 1-139-05.

[147] E. Pära (viide 17), lk 30-31.

Eeltoodud maakohtu otsuse näol on tegemist näitega sellest, kuidas maakohtu lahendites puudub piisav selgitus kuriteo objektiivsete ja subjektiivsete koosseisu elementide kohta, mis võiks olla elementaarne, kuna kohtuotsust lugev suvaline isik ei tea eeldatavalt arvutikelmuse koosseisu elemente ja seega võib juhtuda, et lahendus jääb temale arusaamatuks osas, mis puudutab süüteo aluseks oleva paragrahvi valikut ja seega ka karistuse raskusastme määramist.

Kohtuasi nr. 1-806/2003 on seotud automaattankla kütuseautomaadi manipuleerimisega. J. S. mõisteti süüdi arvutikelmuses selles, et tema omandas kahe päeva jooksul AS-le Flexar kuuluvast automaattanklast 404,90 liitrit diiselkütust väärtusega 3038,75 krooni, makstes kütuse eest ainult 175 krooni. Selleks sekkus ta automaattankla andmetöötlusprotsessi, liigutades tankuri püstolit edasi-tagasi, kuni õnnestus saada diiselkütust selle eest tasumata. Seega sai J. S. andmete töötlemise tulemust mõjutades varalist kasu 2863,75 krooni. Sellega Jüri Sisask pani toime KarS § 213 järgi kvalifitseeritava teo, s.o. varalise kasu saamise andmetöötlusprotsessi sekkumise teel, millega on mõjutatud andmete töötlemise tulemust.[148] Käesoleval juhul on tegu kindlasti arvutikelmusega. Süüalune säästis tankimisel 2863,75 krooni, millest tulenevalt sai süüalune varalist kasu. Süüalune sekkus lubamatult andmetöötlusprotsessi sellega, et manipuleeris kütuseautomaadiga. Käesoleval juhul puudub kahtlus, et J. S. pani sellise teo toime tahtlikult.

Kui tegu oleks olnud mitte automaattanklaga, vaid selvetanklaga, siis oleks pidanud arvestama ka sellega, kas personal jälgis tankimist, kas süüalusel tekkis mõte lahkuda bensiini eest maksmata alles tankimise ajal või oli tal juba tankima tulles kavatsus maksmata lahkuda. Antud juhul eelnev jutt aga automaattanklatele ei laiene, kuna põhimõtteliselt ei ole vahet, kas automaadist saadakse raha või muid asju, nt bensiini, koolat vms. Seega tuleb asja (antud juhul bensiini) saamisele anda hinnang pangaautomaatide juhtude alusel.[149]

3.8 Muud juhtumid

Nagu juba käesolevast tööst nähtub, siis arvutikelmusi on võimalik toime panna väga erinevaid oskusi ja vahendeid kasutades. Kuna kõik Eesti kohtupraktikas aset leidnud

[148] Tartu Maakohtu otsus 22.09.2003, nr 1-806/2003.

[149] J. Sootak (viide 27), lk 166.

arvutikelmuse juhtumeid ei ole võimalik eelnevatesse alapeatükkidesse paigutada, siis ongi vajalik ka alapeatükk „Muud juhtumid“. Siin on kajastatud mõned arvutikelmuse juhtumid, mis on kindlasti mainimist väärt.

Kindlasti tasub ära märkida järgmine humoorikas juhtum, mis leidis aset tänu inimeste kergeusklikkusele. Maakohus tuvastas, et alaealine süüdistatav sai andmetöötlusprotsessi lubamatu käivitamise teel varalist kasu enda elukohas viibides ja kodust arvutit kasutades järgmiselt: süüdistatav esines internetikeskkonnas tütarlapsena ja pettis kannatanult välja raha, lubades veebikaamera vahendusel kannatanule MSN-Messengeris tasulist striptiisišõud, mille vaatamiseks kandis kannatanu süüdistatava kontole raha. Süüdistatav aga lubatud šõud ei näidanud, vaid valetas, et tema kontole ei ole raha laekunud ja küsis rahasumma ülekandmise kontrollimise ettekäändel kannatanu internetipanga paroolid. Kannatanu edastas süüdistatavale eeltoodud põhjusel oma interneti paroolid. Seejärel, väljapetetud internetipanga paroole kasutades, sisenes süüdistatav arvuti vahendusel kontoomaniku nõusolekuta virtuaalsesse maksekeskkonda ja andis virtuaalses maksekeskkonnas korralduse raha ülekandmiseks enda arvelduskontole, saades sel viisil ebaseaduslikult arvutisüsteemi andmeid sisestades kannatanu arvelduskontolt kontoomaniku nõusolekuta raha (varalist kasu).[150] Olgu mainitud, et süüdistatav tütarlaps kasutas sama skeemi kahe erineva kannatanu peal ja mõlemal juhul toimis see edukalt.

Antud näide on ilmekas juhtum sellest, et siin oleks võimalus antud kuritegu liigitada ka tavalise kelmusena. Täidetud on kõik kelmuse nii objektiivsed kui ka subjektiivne tunnus. On olemas reaalne isik, keda petetakse asjaolude moonutamise teel ning kannatanul eksimuse tekkimine. Objektiks on vara ehk raha, kannatanu teeb varakäsutuse, kannatanu saab kahju ja süüdlane tahtlikult varalist kasu. Selliste juhtumite puhul, mille alusel saab kindlaks teha erinevad süüteod, peaks kohus oma otsust põhjendama, miks antud juhul süüdistatav just arvutikelmuses süüdi mõisteti, kui esineb ka reaalne võimalus kelmuses süüdimõistmiseks.[151]

Ametikoha kuritarvitamisega seotud juhtumi asjaolud leiame järgnevast Tartu Maakohtu otsusest. Süüdistatav töötas Lõuna Politseiprefektuuris infosüsteemi Polis administraatorina ja tema teenistusülesandeks oli infosüsteemidesse andmete sisestamine ning kontrollimine, sealhulgas väärteoasjades karistuseks mõistetud rahatrahvide osas järelvalve teostamine nende

[150] Pärnu Maakohtu otsus 16.04.2009, nr 1-09-5395/3.

[151] E. Pära (viide 17), lk 33.

õigsuse seisukohast. Süüdistatav sisestas infosüsteemi Polis teadlikult vale kande selle kohta, et tema abikaasa on tasunud väärteoasjas temale karistuseks mõistetud üheksa tuhande krooni suurusest rahatrahvist kokku seitse tuhat krooni, kuigi tegelikkuses oli selleks ajaks tasutud vaid tuhat krooni. Sellise käitumisega pani süüdistatav toime KarS § 213 järgi kvalifitseeritava kuriteo.[152]

Süüdistatav tunnistati süüdi arvutikelmuses selles, et ta ühendas AS X sidekaablikappides erinevate klientide numbritele juhtmetega järgi oma telefoni ja helistas kannatanute nimelt mitmeid kordi tasulistele numbritele. Lisaks sellele helistas süüdistatav ka teenusnumbrile, mille kaudu sai www.rate.ee koodid ja omakorda rate-raha, mille müüs hiljem interneti kaudu rate-kontole maha, saades vastu Eesti kroone.[153]

Arvutikelmuse koosseisu jaatatakse ka järgmises otsuses. Süüdistatavad sekkusid andmetöötlusprotsessi sellega, et süüdistatav kinnitas internetikeskkonnas X AS-le S ülekandva rahalise summa. Selle tagajärjel internetikeskkond X suunas teda automaatselt SEB Ühispanga internetpanga terminali, kus olid juba sisestatud internetikeskkonna X poolt maksekorraldusele makse sooritamiseks vajalikud rekvisiidid ja süüdistatava poolt internetikeskkonnas X eelnevalt sisestatud ülekantav summa. Seejärel avas süüdistatav internetikeskkonnas eraldi SEB Ühispanga internetikeskkonna ja registreerus SEB Ühispanka makse sooritamiseks teatud veebileheküljel olevale kontole, sisestades eelnevalt internetikeskkonnast X makse sooritamiseks andmed - saadud vajalikud rekvisiidid ning väiksema ülekantava summa kui esialgselt internetikeskkonnas X kinnitatud summa ja sooritas makse. Selle tagajärjel laekus AS-le S. mitte süüdistatava poolt internetikeskkonnas X sisestatud summa, vaid hiljem süüdistatava poolt SEB Ühispanga internetipanga terminalis vähendatud summa. Ringkonnakohus leidis, et süüdistatavad käitusid küll neile loodud tehnilise võimaluse raames, kuid tegemist oli programmi puuduse teadliku ärakasutamisega, mille eesmärgiks oli teise osapoole varaliste huvide kahjustamine. Kui isik on eelnevalt juba teadlik programmi defektsusest ja ta soovib programmi rakendamisel kasutada seda defekti ära enda varalistes huvides, on tegemist kuriteoga. Käesoleval juhul oli tegu andmete ebaseadusliku vahetamisega (muutmisega) KarS § 213 objektiivse koosseisu tähenduses, millega sekkuti ebaseaduslikult andmetöötlusprotsessi ja mõjutati vahetult andmete töötlemise tulemust. Süüdistatavad käitusid tahtlikult (subjektiivse koosseisu element).[154] Selline on ühe

[152] Tartu Maakohtu otsus 30.10.2006, nr 1-06-11375/2.

[153] Pärnu Maakohtu otsus 27.05.2008, nr 1-08-5241/3.

[154] Tallinna Ringkonnakohtu otsus 14.09.2010, nr 1-09-9855.

korraliku otsuse musternäidis st. otsuses on analüüsitud kuriteo koosseisu elementide esinemist ja seda, mille alusel kohus leidis, et käesolev tegu tuleb kvalifitseerida just arvutikelmusena. Kui kõik kohtuotsused oleksid nii hästi põhistatud, et tekiks arvutikelmuste piiritlemisel probleeme ja kohtupraktika oleks selles osas kindlasti ühtsem.

Viimase näitena ei saa jätta märkimata juhtumit, kus isik mõisteti arvutikelmuses süüdi selles, et töötades teatud ajavahemikul apteegis abitöötaja ametikohal, muutis teatud ajavahemikul süüdistatavebaseaduslikult apteegi müügiprogrammis kassatšekkidel müüdud toodete andmeid sellega, et avas kliendi teenindamisel kassas müügiprogrammis varasema kliendi sularahas tasutud ja lõpetatud tšeki, muutis tšeki olekut, kustutas tšekilt varem sisestatud ja müüdud tooted, sisestas uued tooted ja lõpetas müügi ning andis toodete eest tasumisel tooted kliendile üle. Süüdistatava tegevuse tulemusena taastus tšekilt kustutatud toodete saldo programmis, tekkis toodete puudujääk müügisaalis ja sularaha ülejääk kassas. Süüdistatav eemaldas kassast sularaha ülejäägi ja jättis endale, tekitades ettevõttele varalist kahju kokku summas 27 426,96 eurot.[155]

3.9 Arvutikelmuse seotus rahapesuga

Riigikohus käsitles oma 3-1-1-21-11 lahendis rahapesu ja arvutikelmusega seonduvat. Rahapesu on kuritegeliku tegevuse tulemusel saadud vara või selle asemel saadud vara tõelise olemuse, päritolu, asukoha, käsutamisviisi, ümberpaigutamise, omandiõiguse või varaga seotud muude õiguste varjamine või saladuses hoidmine; või muundamine, ülekandmine, omandamine, valdamine või kasutamine eesmärgiga varjata või hoida saladuses vara ebaseaduslikku päritolu või abistada kuritegelikus tegevuses osalenud isikut, et ta saaks hoiduda oma tegude õiguslikest tagajärgedest.[156] Isik mõisteti süüdi kelmuses selles, et ta pettis teatud ajavahemikul 17 korral internetikeskkonnas ja 1 korral kannatanuga vahetult suheldes erinevatelt isikutelt välja raha. Samuti mõisteti ta süüdi arvutikelmuses selles, et ta sisenes teatud ajavahemikul erinevatelt isikutelt välja petetud internetipanga paroole kasutades 36 korral arvuti vahendusel internetipangas nende isikute arvelduskontole ja tegi kontoomaniku nõusolekuta virtuaalses maksekeskkonnas korralduse raha ülekandmiseks enda või kolmandate isikute pangakontodele. Lisaks eelnevalt süüdistati nimetatud isikut ka lisaks

[155] Pärnu Maakohtu otsus 17.12.2012, nr 1-12-10520.

[156] Rahapesu ja terrorismi rahastamise tõkestamise seadus. – RT I, 08.05.2012, 5.

rahapesus selles, et kandis eelpool mainitud raha üle teiste isikute arveldusarvetele ja lasi neil seejärel selle raha pangaautomaadist sularahana välja võtta.[157] Riigikohus aga leidis, et: „süüdistatav ei pannud kelmuste ja arvutikelmustega saadud rahaga toime rahapesu. Kandes kannatanute raha kolmandate isikute arvetele või lastes kannatanutel endil raha kolmandate isikute arvetele kanda, ei ole eelkuritegu, s.t kelmus või arvutikelmus rahapesu süüdistusest eristatav. Süüdistatava käitumise ebaõigussisu nendes süüdistustes ammendub varavastases kuriteos - pettuslikul teel kannatanu varakäsutuse saavutamises või arvutisüsteemi ebaseadusliku kasutamise tulemusel talle varalise kahju tekitamises. Rahapesuna käsitletud käitumine - enda, kui varavastast kuritegu sooritava isiku identiteedi varjamiseks raha kolmandate isikute arvetele kanda laskmine või ise sinna ülekande tegemine on hinnatav kelmusliku teo loomuliku osana, milles ei väljendu legaalse majandus- või rahakäibe kahjustamine sinna kuritegelike vahendite suunamisega.“[158] Samuti märkis Riigikohus, et: „rahapesu koosseisu realiseerimiseks peab kuritegelikul teel saadud varaga tehtavates õigustoimingutes olema keskne osa vara ebaseadusliku päritolu ja selle tegeliku omaniku varjamisel. Rahapesust ei saa rääkida juhul kui vara ebaseadusliku päritolu ja tegeliku omaniku varjamine on varaga tehtavates toimingutes üksnes kõrvaleesmärk või selle tagajärg.“[159] Nimetatud lahendist saab järeldada, et eelkuritegu, s.t kelmus või arvutikelmus ei ole rahapesu süüdistusest eristatav. Seetõttu ei ole võimalik isikut süüdi mõista ühel ajal nii kelmuse kui ka rahapesu või arvutikelmuse ja rahapesu sätete alusel. Süüdistatava käitumine ammendub kas siis kelmuses või arvutikelmuses, kuna teo eesmärgiks oli siiski saada pettuse teel raha. Raha päritolu varjamine on juba kelmusliku teo loomulik osa, milles ei väljendu legaalse majandus- või rahakäibe kahjustamine sinna kuritegelike vahendite suunamisega.

3.10 Arvutikuritegu kui sõltuvuskuritegu

Vaadates Riigikohtu määrust nr 3-1-1-108-09, kus vaidlustati Tartu Ringkonnakohtu 05. oktoobri 2009.a määrus kriminaalasjas nr 1-09-14298, leiame sündmustiku, kus sisuliselt vaidlustatakse KarS § 213 järgi arvutikelmuse toimepanijale määratud vahistamine. Pärnu Maakohus vabastas süüdistatava karistusest tingimisi katseajaga 18 kuud. Süüdistatav aga jätkas kuritegude toimepanemist ka pärast tema suhtes tehtud süüdimõistva kohtuotsuse

[157] RKKKo 03.05.2011, nr 3-1-1-21-11, p-d 2.2 ja 2.3 ja 2.4.

[158] RKKKo 03.05.2011, nr 3-1-1-21-11, p 13.

[159] RKKKo 03.05.2011, nr 3-1-1-21-11 p 14.

jõustumist, mida kinnitas tõsiasi, et kahtlustatava pangaarvele laekus pärast kohtuotsuse tegemist erinevatelt isikutelt väljapetetud summasid. Tartu Ringkonnakohus tühistas aga maakohtu määruse ja süüdistatav vahistati põhjendusega, et kahtlustatav võib jätkuvalt toime panna kuritegusid, s.o esineb vahistamisalus. Riigikohus märkis, et juba Riigikohtu varasemast praktikast nähtub, et kuritegude jätkuva toimepanemise oht on suur eeskätt nn sõltuvuskuritegude puhul. Sellisteks kuritegudeks on näiteks seksuaal- ja narkokuriteod; teatud juhtudel ka vargused ja arvutikuriteod. Kuna sedalaadi kuritegude toimepanemine on olulisel määral tingitud teatud isikulistest asjaoludest, siis võib põhimõtteliselt ka ühe sedalaadi kuriteo toimepanemine kahtluse pinnalt prognoosida selliste kuritegude jätkamise ohtu.[160] Eeltoodud Riigikohtu seisukoht on käesoleva töö kontekstis oluline just seetõttu, et liigitab arvutikuriteo võimalikuks sõltuvuskuriteoks. Käesoleva töö autor peab riigikohtu määruses toodud seisukohaga nõustuma põhjusel, et ka käesolevas töös on kirjeldatud juhtumeid, kus süüdistatavad petavad mitmetelt kannatanutelt välja kas krediitkaardiandmeid või internetikoode, et siis saadud andmeid varalise kasu saamise eesmärgil ära kasutada. Samuti on maakohtu otsustes ära toodud isikute varasemad karistused ja seal torkab silma, et isikuid, keda süüdistatakse arvutikelmuste toimepanemises, on tihti juba ka eelnevalt arvutikelmuste toimepanemises süüdi mõistetud. Samuti võime siin tuua näitena ka käesolevas töö käsitletud lahendi, kus süüdistatav tegeles krediitkaardi andmete ebaseadusliku kogumisega ja kasutamisega ning ta mõisteti süüdi 28 erinevas kuriteoepisoodis. Eeltoodust nähtub, et arvutikuritegude näol võib tõesti olla tegu sõltuvuskuritegudega.

3.11 Alama astme kohtu praktika võrdlus Riigikohtu praktikaga

Riigikohtu praktikas on arvutikelmuse ja selle eelduste üle kõige paremini analüüsitud lahendis nr. 3-1-1-83-07, millele on autor oma töös juba eelnevalt viidanud. Samuti tuleb väga oluliseks lahendiks pidada ka üsna värsket Riigikohtu otsust nr 3-1-1-128-12, mis annab samuti juhiseid selle kohta, millal tuleks isik arvutikelmuses süüdi tunnistada. Kui vaadata Riigikohtu lahendites arvutikelmuste kohta sätestatut ja võrrelda seda alama astme kohtu lahendites tooduga, siis on võimalik tõdeda, et enamus maakohtu lahenditest on järginud Riigikohtu poolt antud juhtnööre ning alama astme kohtu lahendid on vastavuses Riigikohtu seisukohtadega. Samas torkas silma asjaolu, et maakohtud mõistavad inimesed tihtilugu liiga kergekäeliselt süüdi just arvutikelmuses, arvestamata, kas tegu võiks tegelikult olla hoopis

[160] RKKKm 08.12.2009, nr 3-1-1-108-09, 10.1.

kelmusega (juhul kui on olemas petetav), omastamisega või vargusega. Kõige suuremaid vastuolusid võib leida Riigikohtu lahendite ja maakohtu lahendite vahel just internetipangaga ja deebetkaartidega seotud lahendite puhul. Kui süüdistatav varastab kannatanult üksnes pangakaardi ja selle PIN-koodid ning võtab neid kasutades pangaautomaadist raha välja, siis väga tihti kvalifitseeris maakohus sellise teo arvutikelmusena. Riigikohtu lahendi nr 3-1-1-128-12 valguses tuleks aga hoopis kaaluda varguse koosseisu. Internetipangaga seotud juhtumite puhul torkas silma asjaolu, et juhul kui süüdistatav on saanud enda kätte kannatanu internetipanga ligipääsu koodid ja sõlmib läbi internetipanga kannatanu nimel näiteks kiirlaenu lepinguid, siis kvalifitseeritakse selline tegu peaaegu alati arvutikelmusena. Ometi tuleks siinkohal mõelda, kas tegu ei võiks olla hoopis kelmusega, kuna teisel pool ekraani on suure tõenäosusega reaalne isik, kes laenutaotleja andmeid analüüsib ja otsustab, kas nimetatud laenu väljastada või mitte.

Enamikel juhtudel on maakohus küll süüdistatava tegusid õigesti kvalifitseerinud, aga maakohtu otsuste probleem seisneb pigem selles, et puudub igasugune loogiline arutluskäik, mille tulemusena maakohus otsustas isiku teo kvalifitseerida just näiteks arvutikelmusena, vargusena vms. Maakohtu otsuste näol on tihtilugu tegu väga primitiivsete otsustega, kus maakohus kirjeldab kahel või kolmel real asjaolusid, nimetab paragrahvi, mille alusel süüdistatav tuleks süüdi mõista ja määrab seejärel kohe karistuse. Käesoleva töö autor luges magistritöö kirjutamise raames läbi mitusada maakohtu otsust, kuid vaid mõnes üksikus otsuses oli olemas jälgitav mõttekäik, mille alusel kohus otsustas just teatud kuriteokoosseisu kasuks. Olenemata sellest, et tegemist on esimese astme kohtu otsustega, siis ka neid tuleks põhjalikult motiveerida. Maakohtu otsustest peaks nähtuma asjaolud ja analüüs, et miks just täpselt antud lahendi puhul oli tegu arvutikelmusega, millised kuriteo koosseisu elemendid olid seal kajastatud ja miks just täpselt selline karistus määrati. Eeltoodust tulenevalt on suhteliselt raske ka maakohtu lahendeid Riigikohtu lahendite valguses analüüsida, kuna maakohtu poolt määratud kuriteo kvalifikatsiooni ja asjaolusid vaadates tuleb tihtilugu ise välja mõelda, millised võisid need põhjused olla, miks maakohus süüteo otsustas seekord just näiteks arvutikelmusena kvalifitseerida. Maakohtu otsuseid analüüsides torkas pigem just silma see, et maakohtute praktika ei ole ühtlane. Näiteks juhtum, kus süüdistatav varastab kannatanu rahakoti, milles on nii pangakaart kui ka PIN-koodid ja süüdistatav võtab hiljem nende abil pangaautomaadist kannatanu arvelduskontolt raha välja, siis samade asjaolude pinnalt võime leida lahendeid, kus selline süütegu on kvalifitseeritud esimeses maakohtu otsuses vargusena, teises arvutikelmusena ja kolmandas nii varguse kui arvutikelmusena. Õnneks saab väita, et Riigikohus on viimase aasta jooksul käsitlenud arvutikelmustega

seonduvat väga mitmetes lahendites ning selle valguses jääb käesoleva töö autoril üle vaid loota, et ühel päeval on ka maakohtu praktika ühtne ja on kooskõlas Riigikohtu lahenditega.

Huvitav tähelepanek tekkis Riigikohtu lahendi nr. 3-1-1-78-06 ja alama astme kohtu lahendi nr. 1-806/2003 analüüsil, kus mõlemal juhul oli tegu automaattanklast kütuse võtmisega. Esimesel juhtumil oli tegu automaattanklast ettemaksukaardiga, millel oli 50 krooni välja üle 17 000 krooni väärtuses kütust. Oli mainitud, et tegu võis olla kütuseautomaadi manipuleerimisega, kuid kuna see ei leidnud tõendust, siis määrati antud isik süüdi KarS § 199 lg 2 p 4 ehk varguse alusel. Kui aga eelnev asjaolu oleks leidnud tõestust, siis oleks Riigikohus võinud selle teo lugeda arvutikelmuseks nagu seda on tehtud alama astme kohtu poolt kohtuasjas nr. 1-806/2003, kus oli samuti tegu automaattankla kütuseautomaadi manipuleerimisega. Antud juhul oli see aga tõestatud, kuna süüdistatav sekkus automaattanklas andmetöötlusprotsessi liigutades tankuri püstolit edasi-tagasi kuni õnnestus saada diiselkütust selle eest tasumata. Seega sai Jüri Sisask mõjutades andmete töötlemise tulemust varalist kasu 2863,75 krooni. Tema tegu süütegu kvalifitseeriti seega arvutikelmusena.[161]

Lisaks eelnevale on ka töös eespool mainitud, et just maakohtu otsuste puhul leidis käesoleva töö autor mitmeid juhtumeid, mille puhul oleks võinud arvutikelmuse koosseisu asemel kaaluda hoopis teiste varavastaste süütegude (vargus, omastamine, kelmus) koosseisude esinemist. Kuriteod, mille puhul on võimalik jaatada mitme erineva kuriteokoosseisu esinemist, nõuaks maakohtute poolt otsuste paremat põhistamist. Kui tegu vastab näiteks nii varguse kui ka arvutikelmuse koosseisudele, kuid kohus otsustab kuriteo toimepanija süüdi mõista ainult arvutikelmuses, siis peaks kohus oma sellist otsust ka põhistama.

Käesoleva töö kolmandas peatükis toodust on võimalik järeldada, et arvutikelmuste osas puudub käesoleval ajal ühtne kohtupraktika. Riigikohtu otsused on põhjalikud ning argumenteeritud, kuid maakohtud ei ole võtnud vaevaks arvutikelmuse koosseisu sisustamisega eriti vaeva näha. Käesoleva töö pinnalt ei ole võimalik väita, et maakohtu lahendid oleksid otseselt Riigikohtu seisukohtadega vastuolus, kuna nagu eespool juba mainitud, siis maakohtud ei ole oma otsuseid põhjendanud.

[161] E. Pära (viide 17), lk 34-35.

KOKKUVÕTE

Arvutikuritegude ja sealhulgas ka arvutikelmuste arv on tõusuteel ja seetõttu tuleb antud valdkonnale ka suuremat tähelepanu pöörata. Euroopa Liidu tasandil võeti 2001. aasta 8. novembril vastu Euroopa Nõukogu küberkuritegevuse konventsioon, mis on oluline selle poolest, et tegemist on esimese rahvusvahelise lepinguga, mille objekt on interneti ja teiste arvutivõrkude vastu või abil sooritatud kuriteod. Konventsiooni eesmärk oli võtta vastu Euroopa Liidu tasandil asjakohane seadusandlus ja edendada rahvusvahelist koostööd arvutitega seotud kuritegevuse takistamiseks. Kuna Eesti ratifitseeris arvutikuritegevusvastase konventsiooni 12. veebruaril 2003, siis pidi Eesti oma seadusandluse nimetatud konventsiooniga kooskõlla viima. Sellest tulenevalt tegi Eesti 24.03.2008 oma karistusseadustikus arvutikelmuse mõiste osas olulisi muudatusi ning täpsustas sinnamaani üsna ebaselget arvutikelmuse regulatsiooni, kuhu lisati muuhulgas ka juriidilise isiku vastutus. Käesolevaks ajaks võib öelda, et konventsiooni ja karistusseadustiku sõnastus ei kattu täielikult. Kui konventsioonis on arvutikelmuse sõnastuses välja toodud subjektiivse koosseisu element ehk tahtluse olemasolu, siis karistusseadustikus eeldatakse arvutikelmuse paragrahvis (KarS § 213) tahtluse olemasolu vaikimisi.

Eestis võeti 2008. aastal vastu ka küberjulgeoleku strateegia, mis käsitleb arvutikuritegevusega seotud eesmärke, mida Eesti soovib 2013. aastaks saavutada. Tundub, et nimetatud strateegia oli edukas, kuna 21. märtsil 2013 kiitis Eesti Vabariigi Valitsus heaks ka „Küberjulgeoleku strateegia 2014–2017“ koostamise ettepaneku, mille eesmärk on leppida kokku ja luua tingimused selleks, et kasutada infotehnoloogiast tulenevaid võimalusi tõhusalt ja turvaliselt. On oluline ja tänuväärne, et Eesti on pidanud oluliseks arvutikuritegevusele suuremat rõhku panna, kuna arvutikuritegevus on tänapäeva ühiskonnas pigem tõusuteel. Sellist väidet kinnitab ka Eesti kuritegevuse statistika, millest nähtuvalt suureneb pea iga aasta arvuti vahendusel toime pandud kuritegude arv.

Kui veel 6 või 7 aastat tagasi oleks võinud väita, et arvutikelmustega seotud kuriteod moodustavad nii väikse osa Eestis toime pandud kuritegudest, et sellele ei ole mõtet tähelepanu pöörata, siis nüüdseks on arvutikelmused Eesti kohtupraktikas juba arvestatava osakaaluga kuriteoliik. Kui võrrelda 2005. või 2006. aastast pärinevaid kohtuotsuseid näiteks 2011. ja 2012. aasta kohtuotsustega, siis näeme, et arvutite vahendusel toimepandud kuriteod

on muutunud keerukamateks ja kurjategijad osavamateks, mistõttu on tihtilugu raske tuvastada, kes arvutikelmuse toime pani. Arvutikelmuste puhul tuleks arvestada, et kohtutesse jõuab arvatavasti suhteliselt väike osa toimepandud kuritegudest, kuna osad kuriteod jäävad avastamata põhjusel, et ohvrid ei julge oma pettasaamisest teatada, kuna neil on häbi ja nad kardavad avalikku hukkamõistu. Ometi on võimalik alama astme kohtu praktikat analüüsides väita, et paljud arvutikelmuste juhtumid jõuavad kohtutesse ja süüdistatavad saavad ka oma teenitud karistuse. Ka Riigikohtu lahendeid vaadates saame väita, et arvutikelmustega seonduv on muutunud meie kohtupraktikas väga oluliseks, kuna Riigikohus on teinud viimastel aastatel mitmeid erinevaid lahendeid, kus on muuhulgas peetud vajalikuks selgitada ka seda, mille alusel eristada arvutikelmuse koosseisu temaga seotud varavastaste süütegude koosseisudest. Nagu nähtub ka alama astme kohtuotsuste analüüsist, siis puudub alama astme kohtute praktikas ühtne seisukoht, kuidas täpselt ja mille alusel tuleb süütegu kvalifitseerida just arvutikelmusena. Riigikohus on küll püüdnud oma lahendites alama astme kohtutele sellesisulisi juhtnööre anda, kuid tundub, et Riigikohtul tuleb enne veel nii mõnigi selgitav lahend teha, kui maakohtute praktika arvutikelmuste kvalifitseerimise osas ühtseks muutub.

Erinevalt Riigikohtu praktikast võime alama astme kohtu praktikas arvutikelmuse koosseisu kohata juba väga tihti. Maakohtu lahenditest nähtub, et suurem osa arvutikelmuse juhtumitest on seotud just pangakaartidega ja internetipangaga. Maakohtu otsuseid on küll palju, kuid kahjuks on need enamus primitiivsed ja arvutikelmuse koosseisuelemente sisuliselt ei analüüsita. Enamustes lahendites on maakohtud pidanud vajalikuks välja tuua vaid kuriteo kirjelduse ja seejärel nenditakse, et tegu on arvutikelmusega ja isikule mõistetakse KarS § 213 alusel karistus. Maakohtu otsuste probleem seisneb selles, et otsustes puudub arvutikelmuse koosseisuelementide analüüs ja seetõttu on võimalik leida päris mitmeid maakohtu lahendeid, kus võib väita, et kohtud on ekslikult jaatanud arvutikelmuse koosseisu olemasolu seal, kus tegelikult vastas süüdistatava käitumine hoopis mõne muu varavastase süüteo koosseisule. Eriti hoolikalt on vaja argumenteerida paragrahvi valikut sellisel juhul, kui kuritegu võib vastata mitme erineva varavastase süüteo koosseisule, kuid kohus otsustab mingil põhjusel kohaldada neist vaid ühte. Käesoleva töö tulemusena võib väita, et arvutikelmuse koosseisu piiritlemine varguse, omastamise või kelmuse koosseisust ei ole just väga lihtne, kuna maakohtu otsused on selle koha pealt väga vastuolulised. Käesoleva töö autorile tundub, et tihtilugu lähevad maakohtud lihtsama vastupanu teed ja mõistavad isiku süüdi arvutikelmuses, kuna tema tegu vastab ka arvutikelmuse süüteokoosseisule, kuid kohtud ei pea vajalikuks hinnata süüdistatava arvutikelmuse toimepanemisele eelnenud tegusid. Kui siinkohal välja tuua konkreetne näide, siis juhul, kui süüdistatav varastab kannatanult ainult

pangakaardi koos PIN-koodidega eesmärgil, et sellega pangaautomaadist raha välja võtta, siis olenemata sellest, et käesoleval juhul esinevad süüdistatava käitumises nii varguse kui ka arvutikelmuse kuriteo koosseisud, siis tuleks selline tegu Riigikohtu lahendi nr 3-1-1-128-12 valguses kvalifitseerida ikkagi vargusena, mitte arvutikelmusena või varguse ja arvutikelmusena. Nimetatud näite puhul ei olnud süüdistatava tahe suunatud pangakaardi kui sellise vargusele, vaid ta soovis selle abil saada juurdepääsu kannatanu kontol olevale rahale. Seega jätkas süüdistatav varastatud pangakaardiga pangaautomaadist kannatanu arvelt raha välja võttes vargust ja seetõttu tuleks selline tegu kvalifitseerida just vargusena.

Analüüsides Riigikohtu ja alama astme kohtute praktikat, siis Riigikohus on võtnud vaevaks iga kord arvutikelmuste osas oma seisukohta põhjendada ja argumenteerida, kuid alama astme kohtud ei ole seda siiani veel vajalikuks pidanud või siis suutnud seda teha. Suurimaks probleemiks võib välja tuua selle, et maakohtu lahendid on vastuolulised ja primitiivsed. Kuna maakohtu otsustes puudub analüüs, siis ei ole tihtilugu võimalik väita, et kas alama astme kohtu otsus on Riigikohtu seisukohtadega vastuolus või kooskõlas.

COMPUTER FRAUD AND RELATED PROPERTY OFFENCE IN ESTONIAN ACTUAL COURT CASES

Résumé

Today more and more people are using computers and internet. The increase of the activity in computer usage has been accompanied by the increase in computer crimes all over the world. Computer crimes are difficult to detect and the biggest problem is that computer crimes do not recognise the country boarders. This is the reason why it is important to pay more attention to the national co-operation and legislation when it comes to computer crimes. The author is glad to say that 26 European Union (hereinafter the EU) member countries convened in Budapest 08.11.2001 and signed Convention of Cybercrime to create a common policy aimed at the protection of countries and people against cybercrime, *inter alia*, by adopting appropriate legislation and fostering international co-operation. It is important to mention that Estonia was one of those 26 countries that ratified the Convention. The Convention contains a clause that the members who ratified the Convention, must bring their domestic law into line with the convention. This is one of the main reasons why Estonian legislator made 24.03.2008 a change in the section of computer-related fraud (§ 213) in the Estonia Penal Code (hereinafter the Penal Code). As said before, the purpose of the change was to coordinate the Penal Code § 213 with the EU law. The author may say that the last change was successful, because it improved computer-related fraud paragraph (§ 213) in Penal Code significantly and now we may say that our Penal Code is accordance with the EU law.

At this point it is also important to mention that Estonia has also turned attention to computer-related crimes and is doing its best to try to prevent computer-related crimes from spreading. Estonia experienced large-scale cyber attacks in spring 2007 and after that, in 2008, Estonian government began to draw up Estonia's own Strategy of Cybersecurity (hereinafter the Strategy). Among other things, the Strategy gives instructions, how to counter cyber-attacks against government institutions and defines critical infrastructures, which need to be protected.

Five years ago we could have said that the computer-related crimes form such a small part of other crimes that it is not necessary to pay attention to this but today computer-related crimes are an important part of our everyday court cases. The second part of this thesis is based on

the Estonian court rulings. The thesis provides an overview of the computer-related fraud decisions made by the Supreme Court of Estonia (hereinafter the Supreme Court) and also the decisions made by lower Court instances. The purpose of the second part of the thesis is to observe the quality and quantity of the decisions made by lower Court instances and also to see if the lower Court decisions are in accordance with the Supreme Court viewpoints. It is important to mention that the Supreme Court has also understood that computer-related fraud cases are becoming more complex and has given guidelines to lower Court instances, how to delimit computer-related fraud from other related property offences as theft, embezzlement and fraudulence.

The Supreme Court has analyzed thoroughly the purpose and the different elements of the computer-related frauds in its decisions. This fact gives the author the courage to declare that the Supreme Court viewpoints and decisions are competent and well substantiated. The quantity of the Supreme Court rulings is low, but what is more important, the quality is good. Unlike the Supreme Court decisions, the lower Court decisions are primitive and the analysis is basically missing. Lower Court decisions just note the fact that the defendant is guilty of a computer-related fraud but they do not bother to explain, why they decided to convict the defendant on this specific crime. Consequently, the quantity of decisions made by lower Court instances is high but quality is low. In addition to low-quality decisions the author could find many cases where it would have been necessary to justify the ruling under § 213, because in some cases the author proved with an analysis that the defendants could also have been condemned under other sections of the Penal Code (fraud, theft, embezzlement). After analysing the Supreme Court and lower Court decisions, the biggest problem is that author may say that there is a lack of unified law cases.

Tallinn, 06.05.2013

KASUTATUD MATERJALIDE LOETELU

Kasutatud kirjandus

1. A. Kukrus. Küberkuritegevuse tõkestamine infoühiskonnas. Arvutivõrgus: http://www.riigikogu.ee/rito/index.php?id=11319, 23. aprillil 2013.

2. Council of Europe. Convention on Cybercrime. Budapest, 23.XI.2001. Arvutivõrgus: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm, 23. aprillil 2013.

3. Council of Europe. Cyberterrorism – the Use of the Internet for Terrorist Purposes. Council of Europe Publishing, 2007.

4. Danske Bank. Internetipank. Arvutivõrgus: http://www.danskebank.ee/et/13136.html, 02. mail 2013.

5. E. Elkind. Varavastane süütegu Interneti keskkonnas: selle piiritlemise probleemid Eesti karistusõiguses. Riigikohtu otsus 3-2-1-83-07. Juridica, 2008, nr 5.

6. Eesti Vabariigi Siseministeerium. Küberkuritegevuse vastane võitlus. Arvutivõrgus: https://www.siseministeerium.ee/37266/, 23. aprillil 2013.

7. Eesti Vabariigi 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 2013.

8. E. Pära. Arvutikelmused ja nendega seonduvad varavastased süüteod aktuaalses kohtupraktikas. Bakalaureusetöö. Tallinn, 2010.

9. Euroopa Komisjon. Küberkuritegevuse vastane Euroopa Liidu tegevuskava - 12/02/2013. Arvutivõrgus: http://ec.europa.eu/news/science/130212_et.htm, 23. aprillil 2013.

10. Euroopa Komisjon. Pressiteade. 11. Jaanuaril alustab tööd küberkuritegevuse vastase võitluse Euroopa keskus. Arvutivõrgus: http://europa.eu/rapid/press-release_IP-13-13_et.htm, 23. aprillil 2013.

11. H. Loot. Karistusseadustiku muutmise seaduse eelnõu seletuskiri. Arvutivõrgus: http://www.riigikogu.ee/?op=emsplain&page=pub_file&file_id=85a4d8e5-2c8a-0faf-b0e9-3ff75214ffbf&, 01. mail 2013.

12. G. Stamatellos. Computer Ethics. Jones & Bartlett Publishers, 2007.

13. J. Sootak, P. Pikamäe. Karistusseadustik. Kommenteeritud väljaanne. Juura, 2003.

14. J. Sootak, P. Pikamäe. Karistusseadustik. Kommenteeritud väljaanne. Juura, 2009.
15. J. Sootak. Seadusainsus. Kui isiku tegu vastab mitmele süüteokoosseisule, siis mitme järgi ja kuidas ta tegelikult vastutab? Juridica, 2010, nr 1.
16. J. Sootak. Varavastsed süüteod. Juura, 2003.
17. J. Sootak. Varavastsed süüteod. Juura, 2009.
18. Justiitsministeerium, kriminaalpoliitika osakond. Kuritegevus Eestis 2011. aastal. Arvutivõrgus: http://www.just.ee/orb.aw/class=file/action=preview/id=56353/2011_statistika+kokkuv%F5te.pdf, 23. aprillil 2013.
19. Justiitsministeerium, kriminaalpoliitika osakond. Registreeritud kuriteod Eestis 2003-2012. Arvutivõrgus: http://www.just.ee/57886, 23. aprillil 2013.
20. K. Aas, N. Aas, M. Hirvoja, K. Siitam. Karistusõigus. Eriosa. Sisekaitse Akadeemia kirjastus, 2002.
21. K. Domaškina. Ebaseaduslik sekkumine arvutiandmetesse ja sel teel varalise kasu saamine. Riigikohtu kriminaalkolleegiumi otsus 3-1-1-114-12. Juridica, 2013, nr 2.
22. K. Masing. Arvutikelmuse piiritlemisprobleemid. Magistritöö. Tartu, 2012.
23. Komisjoni teatis nõukogule ja Euroopa Parlamendile. Võitlus kuritegevusega digiajastul: küberkuritegevuse vastase võitluse Euroopa keskuse loomine. Arvutivõrgus: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:ET:HTML, 23. aprillil 2013.
24. Küberjulgeoleku strateegia komisjon. Küberjulgeoleku strateegia 2008-2013. Kaitseministeerium, 2008. Arvutivõrgus: http://www.valitsus.ee/failid/kuberjulgeolek.pdf, 24. aprillil 2013.
25. Lühikokkuvõte. „Küberjulgeoleku strateegia 2014-2017“ koostamise ettepanek Vabariigi Valitsusele. Arvutivõrgus: https://valitsus.ee/UserFiles/valitsus/et/valitsus/arengukavad/majandus-ja-kommunikatsiooniministeerium/K%C3%BCberjulgeoleku%20arengukava%20koostamise%20ettepanek_lyhikokkuvote.pdf, 23. aprillil 2013.
26. M. Kairjak. Varaliste huvide järgimise kohustus ja teisele isikule usaldatud vara. Juridica, 2010, nr 1.
27. Official Journal L 069, 16/03/2005 P.0067-0071. Arvutivõrgus: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:ET:HTML, 01. mail 2013.
28. Prof. dr. E. Samson. Kriminaalõiguse eriosa 2. osa. Abimaterjal kohtunike ja prokuröride järelkoolituse karistusõiguse õppegrupile, 2000, lk 27. Arvutivõrgus:

http://www.just.ee/orb.aw/class=file/action=preview/id=10714/krimoiguse+eriosa+II.pdf, 24. aprillil 2013.
29. R. J. McMahon. Partial Handbook for Private Investigators. CRC Press, 2001.
30. T. Reinthal. Küberkuritegevuse kohtupraktika Eestis, 2009. Arvutivõrgus: http://www.riigikohus.ee/vfs/899/Kyberkuritegevus%202009.pdf, 23. aprillil 2013.
31. 14. Uuring „Avalike e-teenuste kasutamine". TNS Emor, oktoober 2007. Arvutivõrgus: http://www.riso.ee/et/files/avalike_e-teenuste_kasutamine_aruanne.pdf, 23. aprillil 2013.
32. W. Koletar. Fraud Exposed. John Wiley and Sons, 2003.

Kasutatud normatiivmaterjalid

33. Andmekogude seadus. – RT I 1997, 28, 423.
34. Arvutikuritegevusvastane konventsioon. – RT II 17.03.2003, 9, 32.
35. Karistusseadustik. – RT I, 17.04.2013, 8.
36. Kriminaalpoliitika arengusuunad aastani 2018 heakskiitmine. – RT III 2010, 26, 51.
37. Rahapesu ja terrorismi rahastamise tõkestamise seadus. – RT I, 08.05.2012, 5.

Kasutatud kohtupraktika

38. Riigikohtu Kriminaalkolleegiumi otsus 17. jaanuarist 2013, nr 3-1-1-128-12.
39. Riigikohtu Kriminaalkolleegiumi otsus 14. detsembrist 2012, nr 3-1-1-114-12.
40. Riigikohtu Kriminaalkolleegiumi otsus 03. maist 2011, nr 3-1-1-21-11.
41. Riigikohtu Kriminaalkolleegiumi otsus 23. veebruarist 2011, nr 3-1-1-105-10.
42. Riigikohtu Kriminaalkolleegiumi otsus 15. novembrist 2010, nr 3-1-1-70-10.
43. Riigikohtu Kriminaalkolleegiumi otsus 10. märtsist 2010, nr 3-1-1-35-10.
44. Riigikohtu Kriminaalkolleegiumi otsus 01. märtsist 2010, nr 3-1-1-2-10.
45. Riigikohtu Kriminaalkolleegiumi määrus 08. detsembrist 2009, nr 3-1-1-108-09.
46. Riigikohtu Kriminaalkolleegiumi otsus 10. novembrist 2009, nr 3-1-1-87-09.
47. Riigikohtu Kriminaalkolleegiumi otsus 25. veebruarist 2009, nr. 3-1-1-85-08.
48. Riigikohtu Kriminaalkolleegiumi otsus 21. aprillist 2008, nr 3-1-1-83-07.
49. Riigikohtu Kriminaalkolleegiumi otsus 06. oktoobrist 2006, nr 3-1-1-78-06.
50. Riigikohtu Kriminaalkolleegiumi otsus 14. juunist 2006, nr 3-1-1-43-06.

51. Riigikohtu Kriminaalkolleegiumi otsus 14. jaanuarist 2005, nr 3-1-1-130-04.
52. Riigikohtu Kriminaalkolleegiumi otsus 01. juulist 2004, nr 3-1-1-60-04.
53. Riigikohtu Kriminaalkolleegiumi otsus 05. jaanuarist 1999, nr 3-1-1-2-99.

54. Tallinna Ringkonnakohtu otsus 10. oktoobrist 2012, nr 1-12-4215.
55. Tallinna Ringkonnakohtu otsus 15. septembrist 2011, nr 1-10-13009/36.
56. Tallinna Ringkonnakohtu otsus 14. septembrist 2010, nr 1-09-9855.
57. Harju Maakohtu otsus 06. märtsist 2013, nr 1-13-1706.
58. Pärnu Maakohtu otsus 26. veebruarist 2013, nr 1-13-856.
59. Harju Maakohtu otsus 15. veebruarist 2013, nr 1-13-792.
60. Harju Maakohtu otsus 11. veebruarist 2013, nr 1-12-12235.
61. Tartu Maakohtu otsus 05. veebruarist 2013, nr 1-12-9130.
62. Pärnu Maakohtu otsus 23. jaanuarist 2013, nr 1-13-418.
63. Pärnu Maakohtu otsus 17. detsembrist 2012, nr 1-12-10520.
64. Viru Maakohtu otsus 05. detsembrist 2012, nr 1-12-11686.
65. Viru Maakohtu otsus 01. novembrist 2012, nr 1-12-9554.
66. Viru Maakohtu otsus 31. oktoobrist 2012, nr 1-12-10483.
67. Viru Maakohtu otsus 29. oktoobrist 2012, nr 1-12-9838.
68. Tartu Maakohtu otsus 18. oktoobrist 2012, nr 1-12-9283.
69. Harju Maakohtu otsus 01. oktoobrist 2012, nr 1-12-8271.
70. Viru Maakohtu otsus 12. septembrist 2012, nr 1-12-6741.
71. Harju Maakohtu otsus 12. septembrist 2012, nr 1-12-7258.
72. Viru Maakohtu otsus 03. septembrist 2012, nr 1-12-8295.
73. Tartu Maakohtu otsus 30. augustist 2012, nr 1-11-4399.
74. Harju Maakohtu otsus 09. augustist 2012, nr 1-12-7420.
75. Harju Maakohtu otsus 11. septembrist 2012, nr 1-12-5954.
76. Harju Maakohtu otsus 26. juulist 2012, nr 1-12-6231.
77. Harju Maakohtu otsus 19. juulist 2012, nr 1-10-6319.
78. Harju Maakohtu otsus 02. maist 2011, nr 1-11-4870.
79. Tartu Maakohtu otsus 03. märtsist 2011, nr 1-10-8347.
80. Tartu Maakohtu otsus 15. detsembrist 2009, nr 1-09-18141/11.
81. Harju Maakohtu otsus 19. oktoobrist 2009, nr 1-09-1894/10.
82. Viru Maakohtu otsus 06. oktoobrist 2009, nr 1-09-15620/6.
83. Pärnu Maakohtu otsus 21. aprillist 2009, nr 1-09-3680/6.
84. Pärnu Maakohtu otsus 16. aprillist 2009, nr 1-09-5395/3.

85. Harju Maakohtu otsus 08. aprillist 2009, nr 1-09-2639/3.
86. Viru Maakohtu otsus 23. märtsist 2009, nr 1-07-12666/8.
87. Harju Maakohtu otsus 18. veebruarist 2009, nr 1-08-17233/7.
88. Pärnu Maakohtu otsus 18. septembrist 2008, nr 1-08-6581/7.
89. Tartu Maakohtu otsus 15. septembrist 2008, nr 1-08-9816/3.
90. Pärnu Maakohtu otsus 27. maist 2008, nr 1-08-5241/3.
91. Viru Maakohtu otsus 09. aprillist 2008, nr 1-07-15253/7.
92. Harju Maakohtu otsus 18. septembrist 2007, nr 1-07-8428/3.
93. Harju Maakohtu otsus 12. juunist 2007, nr 1-07-5805/2.
94. Tartu Maakohtu otsus 30. oktoobrist 2006, nr 1-06-11375/2.
95. Tallinna Linnakohtu otsus 16. maist 2005, nr 1-934/05.
96. Viljandi Maakohtu otsus 02. maist 2005, nr 1-139-05.
97. Rapla Maakohtu otsus 18. novembrist 2003, nr 1-190/03.
98. Tartu Maakohtu otsus 22. septembrist 2003, nr 1-806/2003.

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, Eva Pära (27.08.1987), annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose: „Arvutikelmused ja nendega seonduvad varavastased süüteod Eesti aktuaalses kohtupraktikas“, mille juhendaja on õppeülesannete täitja mag. iur. Sten Lind,

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.

Tallinnas, 06.05.2013