TARTU ÜLIKOOL

ÕIGUSTEADUSKOND

KRIMINOLOOGIA JA KOGNITIIVSE PSÜHHOLOOGIA ÕPPETOOL

KRISTEL MASING

ARVUTIKELMUSE PIIRITLEMISPROBLEEMID

Magistritöö

Juhendaja: prof. J. Ginter

TARTU

2012

Sisukord

Sissejuhatus

Käesolev töö käsitleb arvutikelmuste kvalifitseerimisel tekkivaid probleeme. Kuna arvutikuritegevus, sh arvutikelmuste toimepanemine üha kasvab, on oluline, et menetlejatelnii uurijatel, prokuröridel kui ka kohtunikel, oleks ühtne seisukoht, millal on tegemist arvutikelmusega ja millal mitte. Nagu töös näha, on teema aktuaalne, kuna sarnast kuritegelikku käitumist kvalifitseeritakse erinevate paragrahvidega. Kui isik apellatsiooni või kassatsiooni ei esita, siis näib, et probleemi ei ole, kuid sellisel juhul ei ole meil üldse vaja Karistusseadustikku ning kõik kuriteod võiks subsumeerida ühe paragrahvi alla. Seega on teema käsitlus oluline seaduse ühetaolise kohaldamise seisukohast.

Töö eesmärgiks on välja selgitada, millised on peamised probleemid arvutikelmuste kvalifitseerimisel; millal tuleks kvalifitseerida kuritegu arvutikelmusena, millal omastamise, varguse, kelmuse või muu arvutikuriteona.
Eesmärgi saavutamiseks on püstitatud järgmised ülesanded:

- arvutikelmuste kvalifitseerimiseks nõutavate tunnuste väljaselgitamine;
- arvutikelmuste ja teiste kuritegude piiritlemise reeglite väljaselgitamine

Töö on jaotatud kolmeks peatükiks. Töö esimene peatükk käsitleb arvutikuritegevust üldiseltmillised arvutikuriteod on sätestatud karistusseadustikus ning töös käsitletavad peamised mõisted.
Töö teises osas käsitletakse arvutikelmuse koosseise Eestis, USA-s ja Saksamaal. Saksamaa on valitud seetõttu, et meie seaduste loomisel on just sealt kõige rohkem eeskuju võetud ning USA seetõttu, et võrrelda Kontinentaal-Euroopa lähenemisviise Anglo-Ameerika omadega, samuti seetõttu, et USA-s on arvutikuritegevuse uurimise ja selle vastu võitlemisega kõige suuremas mahus tegutsetud.
Töö kolmandas osas käsitletakse arvutikelmuse erinevaid liike ja millised on piiritlemisprobleemid; arvutikelmuse seotust rahapesuga ning arvutikelmuste eristamist arvutiandmetesse sekkumise, arvutisüsteemi toimimise takistamise ning arvutisüsteemi ebaseadusliku kasutamise koosseisust.
Töös on kasutatud kombineeritud meetodit - kohtupraktika empiirilist analüüsi koos teoreetilises kirjanduses toodud käsitlustega.

Töös kasutatud materjalideks on peamiselt Eesti, Saksamaa ja USA kohtulahendid; erinevad artiklid arvutikelmuste ning arvutikuritegevuse kohta; Eesti, Saksamaa ja USA seadused.

Teoreetilised seisukohad põhinevad peamiselt karistusseadustiku kommenteeritud väljaandel ning J.Sootaki õpikul: Varavastased süüteod.

1.Arvutikuriteod

Arvutikuritegevus kasvab kogu maailmas. Põhjusteks võib pidada asjaolu, et arvuteid on peaaegu igas majapidamises, enamus tehingud tehakse arvuti vahendusel ning ka seda, et arvutimaailmas tuntakse end anonüümsena ning levinud on arvamus, et keegi ei saa jälile.

Arvutikuritegevus on ka Eestis tõusuteel. Kui 2003.a registreeriti 19 arvutikelmuse juhtumit, siis 2011.a-l 512, võrreldes 2010.a-ga 131 kuritegu rohkem, 2009.a-l 470. Arvutisüsteemi ebaseadusliku kasutamise juhtumeid registreeriti 2009.a-l 20, 2010.a-l 36 ning 2011.a-l 40. Arvutiandmetesse sekkuti 2011.a-l 9 korral, 2010.a-l 6 korral, 2009.a-l 3 korda. Arvutisüsteemi toimimist takistati 2011.a-l 5 korda, 2010.a-l 1 kord, 2009.a-l 4 korda.[1]

Arvuti või arvutisüsteem võib kuriteos olla pettuse vahendiks, varguse objektiks või häkkimise sihtmärgiks. Küberkuritegude koosseisud on seotud arvutiga kui vahendiga tavalistes kuritegudes; digitaalkujul sisuga (andmetega, teostega sh piraatkoopiate või keelatud sisuga); IT-ga seotud ründavate tegevustega (sh viirused ja pahavara, millega rünnatakse arvutite ja sidevõrkude puutumatust, turvalisust, usaldusväärsust, kasutatavust).[2]
Küberkuriteod võib jagada ka kolmeks:
1) arvutisüsteemi vastu suunatud kuriteod (häkkimine, näotustamine);
2) arvutisüsteemi vahendusel toime pandud kuriteod (arvutikelmus, identiteedivargus, Interneti vahendusel vaenu õhutamine jne);
3) autoriõiguste vastu suunatud kuriteod.[3]

Eesti karistusseadustikus on kaheksa arvutitega otseselt seotud koosseisu: arvutiandmetesse sekkumine (§ 206), terminalseadme identifitseerimisvahendi ebaseaduslik kõrvaldamine ja muutmine (§ 206^1), arvutisüsteemi toimimise takistamine (§ 207); nuhkvara, pahavara ja arvutiviiruse levitamine (§ 208), arvutikelmus (§ 213), arvutikuriteo ettevalmistamine (§ 216^1), arvutisüsteemi ebaseaduslik kasutamine (§ 217), ebaseaduslikult kõrvaldatud ja muudetud identifitseerimisvahendiga terminalseadme kasutamine (§ 217^1). Lisaks on ka mitmeid koosseise, mis on kaudselt seotud arvutitega, nt intellektuaalse omandi vastased süüteod (14.peatükk), kaitsekoodide üleandmine (§ 284).[4]

[1] J.Salla. Registreeritud kuriteod 2003-2011. Justiitsministeerium. 2012
[2] M.Rosentau. Loengumaterjalid IT-õigusest, 2011
[3] Küberjulgeoleku strateegia 2008–2013, Kaitseministeerium, Tallinn 2008
[4] Karistusseadustik

Arvutikuritegevusvastane konventsioon kohustab konventsiooniosalist võtma „seadusandlikke ja muid meetmeid, et oma seaduses määratleda kuriteona teiste arvutikuritegude kõrval ka 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 arvutiandmete sisestamise, muutmise või sulustamise teel või arvutisüsteemi toimimisse sekkumise teel“.[5]

Arvutikelmused on seotud moodsa ühiskonna arenguga. Moodne majandustegevus ning mitmesugused nüüdisaegsed tehnoloogilised lahendused (internetipank, e-teenused jmt), teevad küll inimeste igapäevaelu lihtsamaks, kuid teisest küljest moodustavad täiesti uue ja unikaalse keskkonna kuritegevuseks. Seetõttu on karistusseadustikus peale põhikelmuse (KarS § 209) erikoosseisud (KarS § 210-213).[6]
„Automaatide ja andmesüsteemide ebasoovitav manipuleerimine on võimalik seetõttu, et sageli puudub neil piisav tehniline kaitse“. See, et automaatidega on võimalik manipuleerida täiusliku tehnilise taseme puudumise tõttu, provotseerib suure hulga süütegusid. Teisest küljest on automaatide kasutamine kulude kokkuhoid mehhaniseeritud tööjõu näol.[7]

Tänapäeval on meie raha ainult bitid arvutis, number ekraanil ja tint panga arveldusarvel. Meie palgatšekid hoiustatakse elektrooniliselt, meie arved makstakse elektrooniliselt. Seetõttu ei ole ka imestada, et suured pettused toimuvad samuti elektroonilisel teel. Pangad on sageli suur ahvatlus kurjategijatele.[8]

1.1 Olulisemad mõisted

Järgnevalt on toodud peamised käesolevat tööd puudutavad mõisted.

- Internet - mitut tüüpi sideteenuseid (nt isikutevaheline sõnumiside, raalkonverentsid, failiedastus ja dokumente sisaldavate failide vaatamine) andva globaalvõrgu nimi.[9] Internet ühendab kümneid tuhandeid iseseisvaid võrke hiiglaslikuks ülemaailmseks internetiks ning see on tõenäoliselt suurim WAN (Wide Area Network ehk laivõrk) maailmas.[10]

[5] Arvutikuritegevusvastane konventsioon, artikkel 8
[6] P.Pikamäe. Mõningad kelmuse üldkoosseisu sisustamisprobleemid kohtupraktikas. Juridica II, 2011, lk 129
[7] J.Sootak. Varavastased süüteod, lk 204
[8] D.Icove; K.Seger. Computer Crime. A Crimefighter´s Handbook. 1995 lk 11
[9] Keeleveebi IT terministandardi sõnastik.
[10] M.Enzer. Glossary of Internet Terms.

- internet- kaks või enam omavahel ühendatud võrku.[11]
- Arvutisüsteem - "andmeid programmi järgi töötlev seade või omavahel ühendatud seadmed".[12]
- Infosüsteem - andmeid töötlev, salvestav või edastav tehniline süsteem koos selle talituseks vajalike vahendite, ressursside ja protsessidega.[13]
- Arvutiandmed - töötlemiseks sobivas vormis esitatud teave või programm, mille abil arvutisüsteem toimib.[14] Informatsioon, teadmised, faktid, mõisted, juhised või esitus, mille eesmärgiks on arvuti või arvutisüsteemi töötlemine. Andmed võivad asuda erinevatel andmekandjatel- mikrofilmil, mikrokaardil, magnetandmekaardil jmt.[15]
- Phishing - tuleneb sõnast fishing ehk eesti keeles kalastamine. See on tegevus, mille käigus saadetakse e-mail näiliselt seaduslikult ettevõttelt (nt pank, Best Buy, PayPal jne), milles palutakse turvalisuse, andmete kontrolli vmt ettekäändel võltsitud veebilehele sisestada oma nimi, elukoht, pangakonto andmed, krediitkaardi andmed, paroolid, salasõnad vmt andmed. Sellise tegevuse eesmärgiks on kuritegelikul eesmärgil kasutada infot, nt avada petetu nimel arvelduskonto, teha ülekandeid pangakontolt, osta kaupu jne.[16]
- IP - (Internet Protocol) interneti protokoll. Reeglistik, mida järgitakse andmepakettide saatmisel ühelt võrguseadmelt teisele. Sellel põhineb Interneti andmevahetus.[17]
- IP aadress - arvuti või muu võrku ühendatud seadme aadress, mida kasutatakse seadmete identifitseerimiseks ja sidepidamiseks IP ja muude protokollide poolt.[18] IP võrku ühendatud arvuti või muu seadme indikaator. Sõnumite marsruutimine toimub vastavalt sihtkoha IP aadressile. Isoleeritud võrgus võib seadmetele omistada suvalisi IP aadresse, peaasi, et need ei korduks, kuid Internetiga ühendatud võrkude puhul tuleb kasutada registreeritud aadresse. InterNIC Registration Service (domeeninimesid ja IP aadresse registreeriv ja Interneti kohta teavitav konsortsium[19]) registreerib internetiaadresse neljast klassist: A kuni D. A klass on mõeldud suurtele võrkudele ja toetab 16 miljonit hosti; B klass on mõeldud keskmise suurusega võrkudele ja toetab 65000 hosti; C klass on mõeldud väikestele võrkudele, kus on alla 256 hosti; D klass on mõeldud multiedastusvõrkudele. IP aadresse väljendatakse harilikult nelja

[11] M.Enzer. Glossary of Internet Terms.
[12] Arvutikuritegevusvastane konventsioon, art 1
[13] Küberjulgeoleku strateegia 2008–2013, Kaitseministeerium, Tallinn 2008
[14] Arvutikuritegevusvastane konventsioon
[15] C.Palo; The Defense of a Computer Crime Case. 70 Am. Jur Trials 435
[16] K.Menninger .Identity Theft and Other Misuses of Credit and Debit Cards
[17] et.wikipedia.org
[18] Küberjulgeoleku strateegia 2008–2013, Kaitseministeerium, Tallinn 2008
[19] V.Hanson; A.Tavast. Arvutikasutaja sõnastik.

omavahel punktidega eraldatud kümnendarvuga, kus iga arv esindab kaheksat bitti. Nt A-klassi puhul on „võrk.kohalik.kohalik.kohalik“.[20]

- Autentimine (identifitseerimine) - isiku või protsessi identsuse kontrollimine.[21]
- Autoriseerimine - pääsuõigustel põhineva juurdepääsu andmine.[22]
- Pahavara - üldnimetus programmide kohta, mis on kirjutatud spetsiaalselt selleks, et arvutit kahjustada või kuritarvitada ja häirida või kontrollida arvutisüsteemide tööd. Pahavara jaguneb paljudesse liikidesse, näiteks viirused, ussid, troojalased jpt.[23]KarS § 208 tähenduses on pahavaraks kõik muud kahjulikud õiguspärase arvutikasutaja teadmata arvuti kahjustamiseks või kuritarvitamiseks kasutatavad programmid, mis ei ole nuhkvara ega arvutiviirus. Näiteks programmid, mis end levitavad, kasutamata selleks teiste programmide muutmist, troojalasi, käomune.[24]
- Viirus ehk arvutiviirus - programm, mis levitab end teisi programme muutes, lisades neisse enda koopia, ning mis täidetakse nakatunud programmi aktiveerimisel.[25] KarS 208 tähenduses on arvutiviirus kahjulik arvutiprogramm, mis on võimeline end oma algsel või modifitseeritud kujul ise või teiste arvutiprogrammide abil arvutivõrgu kaudu edasi levitama ning häirima arvutite kasutamist.[26]
- Ussid - iseseisevad programmid, mis võivad end levitada andmetöötlussüsteemide või arvutivõrkude kaudu.[27] Ussid täidavad tavaliselt ettemääratud funktsiooni, näiteks: ligipääs süsteemile, andmete modifitseerimine jne. On võimalik luua ussi programmi, mis jälgib kasutaja parooli pangasüsteemis ning saadab selle loojale. Ühe tuntud ussi programmi kirjutas Cornell´i ülikooli tudeng Robert Morris 1988. aastal, mis suutis juurduda ligi 6000-sse arvutisse viie tunni jooksul. Praegused viirused oskavad palju rohkem.[28]
- Trooja hobune - programm, mis on näiliselt kahjutu, kuid tegelikult kogub, võltsib või hävitab volitamatult andmeid,[29] rikub kõvakettal failipaigutustabeli või teeb arvutis muud kurja.[30] Oma nime on saanud Trooja hobuse müüdi järgi. Peale oma funktsiooni täitmist võib programm ennast ise hävitada või takistada viiruste jmt leidmist.[31]

[20] http://www.vallaste.ee/
[21] L.Liikane, M.Kesa. Arvutisõnastik
[22] Liikane, L; Kesa, M.Arvutisõnastik
[23] Küberjulgeoleku strateegia 2008–2013, Kaitseministeerium, Tallinn 2008
[24] Karistusseadustik. Komm vln § 208 komm 2.4
[25] IT terministandardi projekti sõnastik
[26] Karistusseadustik. Komm vln § 208 komm 2.3
[27] IT terministandardi projekti sõnastik
[28] J.Audal, Q.Lu, P.Roman. Computer Crimes. American Criminal Law Review Spring, 2008
[29] IT terministandardi projekti sõnastik
[30] L.Liikane, M.Kesa. Arvutisõnastik
[31] J.Audal, Q.Lu, P.Roman. Computer Crimes. American Criminal Law Review Spring, 2008

- Nuhkvara - tarkvara, mis paigaldatakse arvutisse ilma selle kasutaja teadmata ning on mõeldud tema tegevuste ja isikuandmete jälgimiseks ning arvuti kontrollimiseks.[32] Arvutiprogramm, mis kogub arvutikasutaja kohta informatsiooni ilma tema teadmata ning edastab seda nuhkvara paigaldajale või kolmandale isikule.[33] Paigaldatakse näiteks reklaami eesmärgil ning võivad kaasa tulla tasuta tarkvaraga või jaosvaraga.[34]
- ATM (ingl.k Automated Teller Machine) - pangaautomaat; rahaautomaat; rahaterminal. Masin, mis võimaldab panga klientidel võtta välja sularaha, teha makseid ja muid tehinguid ilma telleri abita.[35]
- PIN (ingl.k Personal Identification Number) - isikunumber, personaalne identifitseerimisnumber. Tähtedest ja/või numbritest koosnev kood, mida kasutatakse isiku identifitseerimiseks krediitkaardi, deebetkaardi, mobiiltelefoni jmt kasutamiseks.[36]

[32] Küberjulgeoleku strateegia 2008–2013, Kaitseministeerium, Tallinn 2008
[33] Karistusseadustik. Komm vln § 208 komm 2.2
[34] L.Liikane;M.Kesa. Arvutisõnastik
[35] L.Liikane; M.Kesa. Arvutisõnastik
[36] L.Liikane;M.Kesa. Arvutisõnastik

2.Arvutikelmuse koosseis erinevate riikide seadusandluses

Arvutikuritegevusvastane konventsioon kohustab konventsiooniosalist võtma 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: arvutiandmete sisestamise, muutmise või sulustamise teel või arvutisüsteemi toimimisse sekkumise teel.[37] Konventsiooniga kooskõlas muudeti karistusseadustikus § 213 lg 1 sõnastust ning jäeti koosseisust välja sõnad: „kui sellega on muudetud andmete töötlemise tulemust“.[38]

2.1 Arvutikelmuse koosseis Eestis

Karistusseadustiku § 213 sätestab arvutikelmuse koosseisuna varalise kasu saamise arvutiprogrammi või andmete ebaseadusliku sisestamise, muutmise, kustutamise, rikkumise, sulustamise või muul viisil andmetöötlusprotsessi ebaseadusliku sekkumise teel. Karistada saab nii füüsilist kui juriidilist isikut. [39]

Kaitstavaks õigushüveks on vara.[40] Vara mõistet määratletakse vara õiguslikust, vara majanduslikust või vara isikulisest küljest. Eelistatakse vara majanduslik-õiguslikku käsitlust ehk ühendteooriat- st kaitstakse kõiki majandusliku väärtusega varaühikuid, kuid jäetakse välja nt kuritegelikul teel saadud vara.[41]

Objektiivne koosseis on varalise kasu saamine lubamatu sekkumise teel andmetöötlusprotsessi.[42]

Varaline kasu saadakse siis, kui süüdlase varaline seis muutub positiivses suunas. Muudatuse kindlaks tegemiseks võrreldakse uut varalist seisu enne tegu olnud varalise seisuga ehk kasutatakse nn saldopõhimõtet. Varalise seisu paranemine võib seisneda ka ajutises varalise kahju või varalise seisundi üldise halvenemise ärahoidmises, samuti õiguse saamine, mis oleks tulevikus pidanud tekkima hoopis kannatanul.[43]

Andmeteks arvutikelmuse koosseisu tähenduses on igasugune faktide, teabe või mõistete esitus infosüsteemis töötlemiseks sobivas vormis.[44]

[37] Arvutikuritegevusvastane konventsioon
[38] Karistusseadustiku muutmise seletuskiri.
[39] Karistusseadustik
[40] Karistusseadustik. Komm vln § 213 komm 1.1
[41] Karistusseadustik. Komm vln § 209 komm 2-5
[42] Karistusseadustik. Komm vln § 213 komm 2.1
[43] Karistusseadustik. Komm vln § 209 komm 17
[44] Karistusseadustik. Komm vln § 206 komm 4

Programm on süntaktiline üksus, mis vastab mingi programmikeele reeglitele ning koosneb teatava automatiseeritud andmetöötlusfunktsiooni täitmiseks vajalikest deklaratsioonidest ja lausetest või käskudest, mille kohaselt arvutisüsteem teostab automaatset andmetöötlust.[45]
„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“.[46]

Koosseisutüübilt on tegemist materiaalse kuriteokoosseisuga- andmetöötlusprotsessi sekkumisega peab süüdlane saama varalist kasu.[47]
Andmetöötlusprotsessi sekkumiseks ei ole vaja, et andmetöötlusprotsess oleks juba toimunud. Ka andmetöötlusprotsessi lubamatul käivitamisel on andmetöötlusprotsessi sekkutud. Sekkumise tagajärjel peab sekkuja saama varalist kasu, oluline ei ole, mil viisil andmetöötlusprotsessi sekkutakse.[48] Eelkõige on nõutav, et sekkumise tagajärjel töötlemise tulemust mõjutatakse, st andmete töötluse tulemus oleks sekkumise puudumise korral olnud teistsugune.[49]
Subjektiivsest küljest eeldab süütegu tahtlust kõigi asjaolude suhtes. Koosseis on täidetud, kui isik tegutseb vähemalt kaudse tahtlusega.[50]

2.2 Arvutikelmuse koosseis Saksamaal

Arvutikelmuse koosseis on toodud Saksa kriminaalkoodeksi paragrahvis 263a lg 1- andmetöötlusprotsessi tulemuste mõjutamine: läbi ebaõige programmi muutmise, ebaõigete või ebatäielike või autoriseerimata andmete kasutamise või muu autoriseerimata protsessi

[45] Karistusseadustik. Komm vln § 206 komm 5
[46] Karistusseadustik. Komm vln § 206 komm 6
[47] Karistusseadustik. Komm vln § 213 komm 1.2
[48] Karistusseadustik. Komm vln § 213 komm 2.2
[49] 1-06-14599
[50] Karistusseadustik. Komm vln § 213 komm 3

käigu mõjutamise, millega kahjustatakse teise isiku vara, tahtlusega saada kas endale või kellelegi teisele ebaseaduslikult varalist kasu.[51]

2.3 Arvutikelmuse koosseis USA-s

U.S. Code Title 18 §-s 1030 on toodud arvutitega seonduvad kelmused ja muud kelmusega seonduvad teod, mille lg 4 sätestab- autoriseerimata sisenemine kaitstud arvutisse või autoriseeritud juurdepääsu ulatuse ületamine tahtlikult ja eesmärgiga petta ning sellise käitumisega aidatakse kaasa kavatsetud pettusele ja saadakse midagi rahalise väärtusega, välja arvatud kui pettuse objekt või asi, mis saadakse, sisaldab ainult arvuti kasutamist ja sellise kasutamise väärtus ei ületa üheaastase perioodi jooksul 5000 dollarit.[52]

Lisaks on mitmed paragrahvid, mis ei ole küll otseselt arvutikelmused, kuid seonduvad arvutikuritegevusega.

U.S. Code Title 18 § 1029 kohaselt on kuritegudeks teod, mis on tehtud teadlikult, pettuse kavatsusega ja kui see mõjutab osariikidevahelist või väliskaubandust:

- võltsitud juurdepääsuseadmete tootmine, kasutamine või nendega kauplemine;
- ühe või mitme volitamata juurdepääsuseadmega kauplemine või selle kasutamine üheaastase perioodi jooksul ning saades sellisest tegevusest kasu 1000 dollarit või rohkem;
- 15 või rohkem võltsitud või volitamata juurdepääsuseadme valdamine;
- seadme valmistamise varustuse tootmine, kontrolli omamine, valdamine või sellega kauplemine;
- tehingute mõjutamine; ühe või rohkema juurdepääsuseadme üle andmine teisele isikule, saades selle eest tasu või midagi muud väärtuslikku üheaastase perioodi jooksul kokku 1000 dollarit või rohkem;
- juurdepääsuseadme väljaandja volituseta teadlikult ja pettuse eesmärgil pakutakse müüa juurdepääsuseadet või informatsiooni juurdepääsuseadme kohta või avaldadatakse soovi omandada juurdepääsuseade.
- teadvalt ning pettuse eesmärgil kasutatakse, toodetakse, kaubeldakse, omatakse kontrolli või vallatakse telekommunikatsiooni seadet, mida on muudetud selleks, et saavutada volitamata ligipääs telekommunikatsiooni teenustele.

[51] Saksa kriminaalkoodeks
[52] U.S.Code Title 18 § 1030

- teadvalt ja pettuse eesmärgil kasutatakse, toodetakse, kaubeldakse, omatakse kontrolli või vallatakse skaneerimise vastuvõtjat.
- teadvalt kasutatakse, toodetakse, kaubeldakse, omatakse kontrolli või vallatakse tark- või riistvara, teades, et see on seadistatud sisestama või muutma telekommunikatsiooni seadmete tuvastamist võimaldavaid andmeid ja selliseid seadmeid saab kasutada autoriseerimata juurdepääsu saamiseks telekommunikatsiooni teenustele.
- krediitkaardi süsteemi liikme või agendi volituseta, teadlikult ning pettuse eesmärgil põhjustatakse või korraldatakse teine isik esitama liikmele või agendile vähemalt ühe tõendi või kinnituse tehingu tegemise kohta krediitkaardi või muu juurdepääsuseadmega [53]

Juurdepääsuseade defineeritakse kui igasugune kaart, kood, arve number või mingi muu vahend, millega saadakse juurdepääs kontole, iseseisvalt või koos mõne teise juurdepääsuseadmega, et saada raha, kaupu, teenuseid või midagi muud väärtuslikku või mida saab kasutada rahaülekande teostamiseks.[54]
Termin „volitamata juurdepääsuseade“ tähendab igasugust juurdepääsuseadet, mis on kaotatud, varastatud, aegunud, kehtetuks tunnistatud, tühistatud või saadud pettuse eesmärgil.[55]

U.S. Code Title 18 § 1343 sätestab ühenduse pettused, millega kaitstakse pettusi vara või raha saamisel läbi juhtme, raadio või TV-ülekande. Selle paragrahviga kaitstakse ka elektrooniliste ülekannete pettusi, kui ühendus mõjutab osariikide vahelist või väliskaubandust.[56]

U.S. Code Title 18 § 1344 sätestab panga pettused, kaitstes petuskeemi kasutamise eest kindlustatud panka. Karistatakse isikut, kes teadlikult viib ellu plaani või üritab ellu viia plaani: et petta finantsasutust või selleks, et saada finantsasutuselt raha, krediiti, vara vmt, kasutades pettust, valeesindust või valelubadusi.[57]

U.S. Code Title 15 § 1644 kohaselt on kriminaalkorras karistatavad järgmised teod:

- võltsitud, fiktiivse, muudetud, kaotatud, varastatud või välja petetud krediitkaardi kasutamine või kasutamise katse, eesmärgiga saada raha, kaupu, teenuseid või midagi

[53] U.S. Code Title 18 § 1029
[54] U.S Code Title 18 § 1029
[55] U.S. Code Title 18 § 1029
[56] U.S. Code Title 18. § 1343
[57] U.S. Code Title 18 § 1344

muud, mille väärtus ületab 1000 dollarit üheaastase perioodi jooksul ning mis mõjutab osariikidevahelist või väliskaubandust;

- võltsitud, fiktiivse, muudetud, kaotatud, varastatud või välja petetud krediitkaardi transportimine või transportimise katse osariikidevahelisse või väliskaubandusse, teades, et kaart on võltsitud, fiktiivne, muudetud, kaotatud, varastatud või välja petetud;
- kasutades osariikidevahelist või väliskaubandust vahendina, et müüa või transportida võltsitud, fiktiivset, muudetud, kaotatud, varastatud või väljapetetud krediitkaarti, teades, et kaart on võltsitud, fiktiivne, muudetud, kaotatud, varastatud või välja petetud;
- võltsitud, fiktiivse, muudetud, kaotatud, varastatud või välja petetud krediitkaardiga saadud raha, kauba, teenuse või muu väärtusliku asja, mille koguväärtus ületab aastase perioodi jooksul 1000 dollarit ja mis on liikunud osariikidevahelisse või väliskaubandusse, teadlik vastuvõtmine, varjamine, kasutamine või transportimine;
- võltsitud, fiktiivse, muudetud, kaotatud, varastatud või välja petetud krediitkaardiga saadud osariikidevaheliste või välisriikidesse sõitmise piletite, mille koguväärtus aastase perioodi jooksul ületab 500 dollarit, teadlik vastuvõtmine, varjamine, kasutamine või transportimine osariikidevahelisse või väliskaubandusse;
- raha, kaupade, teenuste või millegi muu väärtusliku hankimine tehinguga, mis mõjutab osariikidevahelist või väliskaubandust, mille koguväärtus aastase perioodi jooksul ületab 1000 dollarit, kasutades võltsitud, fiktiivset, muudetud, kaotatud, varastatud või välja petetud krediitkaarti, teades, et see on võltsitud, fiktiivne, muudetud, kaotatud, varastatud või välja petetud.[58]

Kui võrrelda Eesti ja USA seadusi, siis Eestis, samuti ka Saksamaal, saab subsumeerida arvutikelmuse koosseisu alla erinevaid arvutikelmuse liike- internetipangas ülekande tegemine, pangakaardi ja krediitkaardi ebaseaduslik kasutamine, telefoni SIM-kaardi ebaseaduslik kasutamine jmt. Samas USA seaduste järgi on need kuriteod paigutatavad erinevate paragrahvide alla.

[58] U.S. Code Title 15 § 1644

3. Arvutikelmuse liigid ja piiritlemisprobleemid

Arvutikelmusena kvalifitseeritakse järgmised ebaseaduslikud tegevused: internetipangas ülekande tegemine; pangakaardi, krediitkaardi, kütusekaardi, kinkekaardi kasutamine; mobiiltelefoni SIM-kaardi kasutamine; taksofoni kasutamine; tuludeklaratsiooni esitamine.

3.1 Internetipangas ülekande tegemine

Internetipangas ebaseaduslikku ülekande tegemist saab kvalifitseerida arvutikelmuse või omastamisena. Piiritlemisel tuleb selgitada, kuidas sai süüdistatav ligipääsu võõrale pangakontole.

Käesoleval ajal on kõige olulisemaks arvutikelmust käsitletavaks Riigikohtu lahendiks 3-1-1-83-07. Antud kaasuses teostasid A.L ja A.K seitsmel korral ülekandeid M.I arvelduskontolt U.E ja M.D arvelduskontodele, pöörates ebaseaduslikult enda kasuks nimetatud arvelduskontol oleva raha. „Teo toimepanemisel kasutasid süüdistatavad ära asjaolu, et nende valduses olid Harku vangla kinnipeetava N.I. poolt sõlmitud internetipanga lepingu kohaselt M.I. Hansapanga arvelduskontole juurdepääsu võimaldavad paroolid, mistõttu oli neil juurdepääs sellele kontole.“ U.E ja M.D arvelduskontodele kantud rahasummad võtsid kontoomanikud sularahaautomaadist välja ning andsid üle A.K-le. Kohtu alla anti isikud omastamise süüdistuses, maa- ja ringkonnakohus leidsid, et tegemist on vargusega.[59]
Riigikohus leidis, et kohtud väljusid süüdistuse piiridest, kuna süüdistusest ei nähtu, et isikuid oleks süüdistatud sularaha väljavõtmises tunnistajate kontodelt, kuid teo raskuspunkt oli asetatud just sularaha väljavõtmisele ning süüteo objektiks oli pangaautomaadist väljavõetud sularaha kui vallasasi varguse süüteokoosseisu tähenduses. „Süüdistuse kohaselt oli lõpuleviidud omastamisega tegemist juba raha ülekandmisel kannatanu pangakontolt tunnistajate kontodele“.[60]

Riigikohtu hinnangul kahjustab kannatanu nõusolekuta internetipangas rahaülekande tegemine kellegi teise kontole kannatanu varalisi õigusi. Varalisi õigusi kahjustatakse ka siis, kui süüdistatav ei võta sularaha kontolt välja, vaid ostab näiteks internetikeskkonnas teenuseid.[61]

[59] 3-1-1-83-07 p 1
[60] 3-1-1-83-07 p 10.4
[61] 3-1-1-83-07 p 13

Pangaülekannete tegemisel ei toimu valduses oleva võõra vallasasja enda kasuks pööramist, kuna panga arvelduskontol olev raha on arvelduskonto omaniku varaline nõue panga vastu arvelduskontol näidatud ulatuses. Kuna valdus on tegelik võim asja üle, siis ei saa varaline nõue olla ka süüdistatava valduses. Arvelduskontole juurdepääsemiseks on vajalik kasutada vahendeid võõra vara käsutamiseks, nt panga väljastatud kasutajatunnust, salasõna ja koodikaarti või PIN-kalkulaatori koode või digitaalset tuvastamist ja allkirjastamist võimaldavat sertifikaati vm isiku identifitseerimisvahendit.[62]
Pangakontol ülekannete tegemist võib kvalifitseerida omastamisena, kui pööratakse ebaseaduslikult enda või kolmanda isiku kasuks isikule usaldatud muu võõras vara. Siia alla kuulub ka volitus internetipanka sisenemiseks ja arvelduskontol oleva raha käsutamiseks vastuolus pangaga sõlmitud lepinguga ning kui arvelduskonto omanik palub kellelgi teha tema eest ülekandeid, kuid isik teeb selliseid toiminguid, milleks teda volitatud ei ole.[63]

Arvutikelmusega on tegemist juhtudel, kui internetipanga paroolid „satuvad isiku valdusesse (või saavad talle teatavaks) arvelduskonto omaniku nõusolekuta, samuti kui need antakse talle hoiule või edasiandmiseks ilma konto kasutamise ja käsutamise õiguseta. Andmete ebaseaduslik sisestamine hõlmab ka arvelduskontole juurdepääsu ja sellel oleva varaga toimingute tegemist võimaldavate andmete sisestamise, kui selleks puudub arvelduskonto omaniku nõusolek. 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“.[64]
Arvutikelmusega on tegemist ka juhtumitel, kui isik suudab sisse murda internetipanka, muukida lahti vastavad kaitsekoodid.[65]

Riigikohus lahendas ka kaasust, milles T.P mõisteti süüdi arvutikelmuses, kuna ta sisenes ajavahemikus 30.märtsist 2008 kuni 2.septembrini 2009 erinevatelt isikutelt välja petetud internetipanga paroole kasutades 36 korral arvuti vahendusel internetipangas nende isikute arvelduskontodele ning tegi kontoomanike nõusolekuta virtuaalses maksekeskkonnas korralduse raha ülekandmiseks enda või kolmandate isikute arvelduskontodele.[66]

[62] 3-1-1-83-07 p 14
[63] 3-1-1-83-07 p 15
[64] 3-1-1-83-07 p 16
[65] J.Sootak. Varavastased süüteod, lk 204-205. Tln 2009
[66] 3-1-1-21-11

Sama isiku kohta on tehtud mitu maakohtu otsust. T.P esines internetikeskkonnas tütarlapsena ning lubas erinevatele isikutele veebikaamera vahendusel strpitiisišõud 100 kuni 250 krooni eest. Peale küsitud summa ülekandmist T.P või kolmandate isikute kontole, lubatud šõud ei järgnenud, kuna T.P valetas, et raha ei ole kontole laekunud. T.P küsis rahasumma ülekandmise kontrollimise ettekäändel kannatanutelt internetipanga paroolid, mille kannatanud T.P-le ka edastasid. T.P sisenes väljapetetud paroole kasutades kannatanute arvelduskontodele ning kandis kontoomanike nõusolekuta nende arvelduskontodelt enda või kolmandate isikute arvelduskontodele üle 1500 kuni 1700 krooni. Sellise tegevusega pani T.P toime arvutikelmuse.[67]

Kuna toodud juhtumitel andsid kannatanud ise vabatahtlikult oma internetipanga paroolid T.P-le, et viimane saaks kontrollida ülekannete laekumist, siis tuginedes Riigikohtu otsusele nr 3-1-1-83-07 võib pangakontol ülekannete tegemist kvalifitseerida omastamisena, kui oli olemas arvelduskonto omaniku nõusolek teise isiku juurdepääsuks arvelduskontole ja sellel oleva raha käsutamiseks ning isik teeb sellised toiminguid, milleks teda volitatud ei ole, pöörates vara enda või kolmanda isiku kasuks. Samas oli nõusolek ainult teostatud ülekannete vaatamiseks, mitte kontol oleva raha käsutamiseks, seega tegemist arvutikelmusega.

Arvutikelmusega on tegemist juhul, kui isik, olles saanud eelnevalt enda valdusesse kannatanule väljastatud internetipanga kasutajatunnuse ja paroolid, kasutab neid kannatanu nõusolekuta internetipanka sisenemiseks ja kannatanu arvelduskontolt maksete tegemiseks kolmanda isiku arveldusarvele. Sellega mõjutab süüdistatav arvutisüsteemis andmete töötlemise tulemust andmetöötlusprotsessi lubamatu käivitamise kaudu. Seejärel võttis süüdistatav kolmanda isiku arveldusarvele kantud raha sularahaautomaatidest välja, saades sellega varalist kasu.[68] Antud kaasuse puhul on põhirõhk asetatud sularaha väljavõtmisele, st et varalist kasu saadi just raha sularahaautomaadist välja võttes, samas on Riigikohus oma varasemas lahendis (RK 3-1-1-83-07) leidnud, et varalist kasu saadi juba raha teisele kontole ülekandmisega ning raha väljavõtmine sularahaautomaadist ei olegi oluline.

Arvutikelmuse toimepanemises süüdistati L.S-i, kelle kohta saabus Berliini prokuratuurist Eestisse Euroopa vahistamismäärus. L.S avas kolm pangaarvet ning võimaldas neile juurdepääsu eeluurimisel tuvastamata kaasosalistel, kuhu nad teostasid kannatanute pangakontodelt rahaülekandeid kokku 40100 euro väärtuses. Tundmatud kaasosalised installeerisid kannatanute arvutitesse nuhkvaraprogrammid, mille abil koguti informatsiooni

[67] 1-09-5395
[68] 3-1-1-70-10

kannatanute pangakontodele ligipääsemiseks. „Selline tegevus on kvalifitseeritav Saksa Kriminaalkoodeksi § 263 lg 3 nr 1, 263 a lõike 1,2, 25 lõige 2, 53 järgi arvutikelmusena“.[69] Selline tegevus on kvalifitseeritav ka Eesti seaduse järgi arvutikelmusena.

Tartu Maakohus mõistis R.S-i süüdi arvutikelmuse toimepanemises, kuna tema sisestas varalise kasu saamise eesmärgil ebaseaduslikult A.J internetipanga kasutajanime, salasõna ja koodi ning sisenes A.J internetipanka, kus mõjutas andmete töötlemise tulemust selliselt, et kandis A.J arvelt raha enda arveldusarvele ning peale raha laekumist võttis R.S raha välja.[70]

Harju Maakohus lahendas kaasust, milles I.B, vastavalt seni tuvastamata isikult suhtlusprogrammis ICQ saadud ülesandele, veenis AS-i, et see lubaks teha enda arvelduskontole ülekande ning annaks selleks oma arveldusarve numbri. I.B edastas A.S-lt saadud konto numbri arvuti vahendusel seni tuvastamata isikule, kes sekkus internetipanga keskkonnas P.J poolt alustatud andmetöötlusprotsessi ning teostas tema kontolt konto omaniku teadmata ja volituseta 2100 krooni suuruse ülekande A.S-i kontole ning T.N poolt alustatud andmetöötlusprotsessi ning teostas tema kontolt konto omaniku teadmata ja volituseta 6000 krooni suuruse ülekande A.S-i kontole. Rahaülekannete järel informeeris seni tuvastamata isik sellest koheselt suhtlusprogrammi MSN vahendusel I.B-d, et viimane A.S-i arvel oleva raha sularahaautomaadist välja võtaks. I.B leppis raha väljavõtmise koheselt kokku A.S-ga, kuid raha väljavõtmine ning ülekande tegemine A.S-i kontolt ebaõnnestus, sest pank oli A.S-i konto kasutamise blokeerinud. I.B mõisteti süüdi arvutikelmusele kaasaaitamises.[71]

Arvutikelmusega on tegemist ka sellisel juhul, kui isik muudab maksekorraldusel olevaid andmeid, saades sellega varalist kasu. J.S-i süüdistati arvutikelmuse toimepanemises, mis seisnes selles, et ta „sisenes AS-i Spordiennustus internetikeskkonnas www.fortuuna.ee olevatele kontodele nr 106570 ning nr 127346 ja alustas seal kasu saamise eesmärgil andmetöötlusprotsessi sellega, et kinnitas internetikeskkonnas www.fortuuna.ee AS-le Spordiennustus ülekantavat rahalist summat. Selle tagajärjel internetikeskkond www.fortuuna.ee suunas ta automaatselt SEB Ühispanga internetipanga terminali, kus oli juba sisestatud internetikeskkonna www.fortuuna.ee poolt maksekorraldusele makse sooritamiseks vajalikud rekvisiidid ja J.S poolt internetikeskkonnas www.fortuuna.ee

[69] 1-06-12976
[70] 1-09-5360
[71] 1-09-8563

eelnevalt sisestatud ülekantav summa. Seejärel avas J.S internetikeskkonnas eraldi SEB Ühispanga internetikeskkonna ning registreerus SEB Ühispanka makse sooritamiseks www.fortuuna.ee olevale kontole, sisestades eelnevalt internetikeskkonnast www.fortuuna.ee makse sooritamiseks saadud vajalikud rekvisiidid ning väiksema ülekantava summa kui esialgselt internetikeskkonnas www.fortuuna.ee kinnitatud summa ning sooritas makse. Selle tagajärjel laekus AS-le Spordiennustus mitte J.S poolt internetikeskkonnas www.fortuuna.ee sisestatud summa, vaid hiljem J.S poolt SEB Ühispanga internetipanga terminalis vähendatud summa. J.S, olles enne internetikeskkonnas www.fortuuna.ee raha ülekandmise alustamist teadlik, et AS-i Spordiennustus arvutisüsteem kannab isiku kontole internetikeskkonnas www.fortuuna.ee summa, mille isik algselt sisestab internetikeskkonnas www.fortuuna.ee, jättes tegelikult ülekantava summa kontrollimata. Ülekantavate summade vähendamine SEB Ühispanga internetipanga maksekorraldusel, kui oli eelnevalt internetikeskkonnas www.fortuuna.ee sisestatud suurem summa, võimaldas J.S-l saada suuremat krediiti internetikeskkonnas www.fortuuna.ee võrreldes sellega, mida isik pidi tegelikult saama. Kui J.S-i internetikeskkonnas www.fortuuna.ee olevale kontole laekus tema poolt eelnevalt internetikeskkonnas www.fortuuna.ee sisestatud summa, mitte aga tegelikult ülekantud summa, võttis J.S raha internetikeskkonnast www.fortuuna.ee välja“. Näiteks sisestas ta sel viisil ülekandmisele kuuluvaks summaks 100 krooni, kuid muutis internetipanga maksekorraldusel oleva summa 10 krooniks. Kokku sai J.S sellisel viisil varalist kasu 64 899,98 krooni. Sama otsusega mõisteti taolistes kuritegudes süüdi ka R.P ja M.V.

Süüdistatavad esitasid apellatsiooni, kuna nad ei nõustunud süütegude kvalifitseerimisega arvutikelmusena, põhjendusel, et nad tegutsesid programmiga loodud tehnilise võimaluse raames ning kasutasid üksnes võimalust muuta maksekorralduses olevaid andmeid.

Ringkonnakohus jättis süüdimõistva otsuse jõusse põhjendades seda järgnevalt: arvutikelmuse koosseis külgneb esmajoones kelmuse põhikoosseisuga. Arvuti kaudu või abil toime pandud süütegudes ei peteta inimest nagu seda nõuab kelmuse koosseis. Olemuslikult on aga kelmus ja arvutikelmus võrreldavad. Kelmusega on näiteks tegemist tsiviilõiguslike lepingute sõlmimisel, kui ühel osapoolel ei ole algusest peale kavatsust lepingut täita, kuigi väliselt on selline käitumine täiesti seaduslik. Ringkonnakohus leidis, et sarnaselt võib seda väita ka antud juhtumi puhul - „süüdistatavad käitusid küll neile loodud tehnilise võimaluse raames, kuid tegemist oli programmi puuduse teadliku ärakasutamisega, mille eesmärgiks oli teise osapoole varaliste huvide kahjustamine“. Süüdistatavate käitumise näol on tegemist andmete ebaseadusliku muutmisega, mida nõuab arvutikelmuse objektiivne koosseis ning sellise

tegevusega sekkuti ebaseaduslikult andmetöötlusprotsessi ning mõjutati vahetult andmete töötlemise tulemust.[72]

Selliste põhjendustega Ringkonnakohtu poolt tuleb nõustuda – maksekorralduse andmete muutmine on andmete ebaseaduslik muutmine ning sellise tegevusega sekkutakse andmetöötlusprotsessi, saades varalist kasu.

Viru Maakohtus mõisteti A.K ja R.P arvutikelmuse toimepanemises süüdi, kuna A.K kasutas varem R.P-lt saadud V.B pangakontot puudutavaid dokumente, mis sisaldasid internetipanka ligipääsu võimaldavat püsiparooli, kasutajatunnust ja internetipanga paroole ning varem V.B arvelduskontole sõlmitud telefonipanga teenust ning teostas telefoninumbrite abil V.B arvelduskontolt maksed L.K pangakontole, sekkudes sel moel ebaseaduslikult andmetöötlusprotsessi selle lubamatu käivitamise kaudu.

V.B sõnul pöördus tema poole tundmatu isik, kes palus tema pangaarve andmeid, kuna tal läksid dokumendid kaotsi, kuid ta vajas pangaarvet, et sinna saaks raha üle kanda. V.B andis 300-kroonise tasu eest tundmatule isikule oma pangakaardi koos paroolidega. Kui V.B-l saabus pensionipäev, avastas ta, et tema pangakontolt on tehtud ülekanne pensionisumma ulatuses ilma tema nõusolekuta L.K pangakontole.[73]

Kuna antud juhtumil oli V.B nõusolek oma konto kasutamiseks olemas, kuid A.K tegi toiminguid, milleks V.B teda ei volitanud, tuleks selline juhtum kvalifitseerida omastamisena, mitte arvutikelmusena.

Arvutikelmusele kaasaaitamisega on tegemist, kui abistatakse isikut kontoga (k.a enda kontoga), kuhu ebaseaduslik ülekanne teostada.

M.M mõisteti süüdi arvutikelmusele kaasaaitamises andmetöötlusprotsessi ebaseadusliku sekkumise teel Saksamaa Liitvabariigis elava isiku AR'i LBAG pangas oleva pangakonto arvelt. M.M andis Sergei-nimelisele isikule, keda ta tundis vähe, oma pangakonto andmed-pangakonto numbri, internetipanga kasutajatunnuse ja paroolid, teades, et sellele kontole laekub välisriigist raha. Kriminaalmenetlusega tuvastamata isik kandis Saksamaa Liitvabariigis elava isiku AR'i LBAG pangas asuvalt kontolt ebaseaduslikult, ilma kontomaniku loa ja teadmiseta 5819 eurot üle M.M-le kuuluvale kontole. M.M võttis sellest rahast 90725 krooni välja sularahaautomaadi kaudu ja andis üle Sergei-nimelisele isikule ning sai selle eest 1000 krooni. "Luues tundmatule isikule juurdepääsu enda pangakontole ja võimaluse kanda sellel välisriigist kuriteo toimepanemisega saadud raha ning võttes selle raha

[72] 1-09-9855
[73] 1-09-9735

sularahas välja ja andes üle, aitas M.M kaasa sellele, et kuriteo toimepanija sai enda isikut paljastamata summas 5819 eurot varalist kasu andmetöötlusprotsessi ebaseadusliku sekkumise teel“.[74] Lähtudes Riigikohtu praktikast ei peaks sularaha väljavõtmine ning üleandmine olema oluline, piisab konto kasutamise võimaldamisest.

Harju Maakohtus mõisteti isikud süüdi arvutikelmuses, kuna nad said varalist kasu andmete ebaseadusliku sisestamisega, millega mõjutati andmete töötlemise tulemust. I.K grupis koos D.T ja M.Z-ga ning eeluurimisel tuvastamata isikuga korraldas ebaseaduslike rahaülekannete teostamisi Itaalia, Kreeka, Prantsusmaa, Austria ja Taani elanike pangakontodelt, levitades nimetatud riikide elanike seas valetöökuulutusi, mille sisuks oli finantsmänedžeride otsimine, kelle ülesandeks oli oma pangaarvele laekunud raha edasitoimetamine vastavalt süüdistatavate poolt e-maili ja telefoni teel antud juhistele. Süüdistatavad korraldasid koos eeluurimisel tuvastamata isikuga välisriikides elavate isikute arvutitesse arvutiviiruse programmi paigaldamise, mis sisaldas arvutiviirust Trooja. Kannatanud pidid internetilehelt alla laadima nö tarkvara uuenduse, kuid tegelikult kogus ja edastas see arvutis avatuna internetipanga klientide kasutajatunnuseid ja turvaparoole ning saatis need eeluurimisel tuvastamata isiku poolt määratud serverisse. Seejärel värbasid süüdistatavad isikud, kelle pangakontodele ülekanded laekusid ning eeluurimisega tuvastamata isik teostas sinna ebaseaduslikud ülekanded. Variisikuteks palgatud isikud kandsid raha Western Unioni rahasiirdamisteenust kasutades Eestis oleva variisiku M.P nimele.[75]

A.M ja K.K isikute grupis aitasid kaasa aktiivse füüsilise ja ainelise kaasabi osutamisega kohtueelse menetluse käigus tuvastamata isiku poolt toime pandud varalise kasu saamisel muul viisil andmetöötlusprotsessi ebaseadusliku sekkumisega. Tuvastamata isik sai ebaseaduslikult juurdepääsu Saksamaa ja Ungari erinevate pankade klientide arvelduskontodele ning teostas ebaseaduslikud maksed Eesti Vabariigi pankades avatud kolmandate isikute arveldusarvetele. Arvelduskontode andmed edastas K.K kuriteo toimepanijale ning A.M tegeles nimetatud arvelduskontodega seotud andmete, s.o pangadokumentide, pangakaartide, arvenumbrite ja parooliümbrikute muretsemise ning edasitoimetamisega K.K kätte. Üheskoos organiseeriti arvutikelmuse toimepanemise tulemusena saadud rahaliste vahendite väljavõtmine pangaautomaatidest ja selle jagamine

[74] 1-11-8706
[75] 1-07-5805

kuriteo toimepanijate vahel. Tuvastamata isik teostas kokku 58 ülekannet koguväärtuses 133105,46 eurot.[76]

Tartu Linnavalitsuse haridusosakonna raamatupidamisteenistuse vanemraamatupidaja mõisteti süüdi selles, et tema tekitas andmete ebaseadusliku sisestamise ja muutmise ning andmetöötlusprotsessi ebaseadusliku sekkumise teel Tartu linnale varalist kahju ja endale varalist kasu selliselt, et koostas korduvalt Tartu Linnavalitsuse haridusosakonna raamatupidamisteenistuse kasutuses olevas raamatupidamise programmis Axapta töölehe, kuhu lisas lisaks reaalsetest töövõtulepingutest tulenevatest tasudest väljamakse oma nimele. Sellise tasu saamiseks ei olnud tal õigust. Seejärel valmistas ta antud töölehe alusel ette koondmaksekorralduse, mille pearaamatupidaja aktsepteeris ning süüdistatava arvele laekus Tartu Linnavalituse haridusosakonna arvelduskontolt rahasumma. Peale ülekande saabumist enda kontole, kustutas süüdistatav eelnevalt ettevalmistatud ebaõigete andmetega töölehelt rea oma nime ja väljamaksele kuuluva summaga ning tulenevalt Tartu Linnavalitsuse haridusosakonna raamatupidamise sise-eeskirjast printis välja muudetud töölehe selle säilitamiseks koos töötasude andmetega. Et oma ebaseaduslikku tegevust varjata, sisestas ta raamatupidamise programmi haridusosakonna kontole „Muud õppevahendite ja koolituse kulud" fiktiivse kande, justkui oleks Tartu Kutsehariduskeskusel kulunud vastav rahasumma õppevahendite ja koolituste tarbeks, omamata kande aluseks alusdokumenti, millega viis kooskõlla haridusosakonna arvelduskonto raha jäägi raamatupidamise programmi andmetega. Raamatupidaja põhjustas sellise tegevusega Tartu linnale varalist kahju kokku 61730,95 krooni.[77]

Antud kaasuse puhul tekib piiritlemisprobleem omastamise koosseisuga. Raamatupidajal oli tööülesannete tõttu juurdepääs Tartu Linnavalitsuse haridusosakonna arveldusarvele ning rahaülekannete teostamisega ületas ta oma pädevuse piire. Kuigi raha omastamiseks kasutas raamatupidaja keerukat skeemi, sisestas ja muutis ebaseaduslikult andmed arvutisüsteemis, ei anna see eeldusi kuritegu kvalifitseerida arvutikelmusena.

Arvutikelmusena on kvalifitseeritav ka internetipangast raha ülekandmine mobiiltelefonile, nt kõneaja laadimiseks. J.J mõisteti süüdi varalise kasu saamises ilma teise isiku volituseta toimingute tegemises, kuna ta sisestas ebaseaduslikult andmeid süsteemi, mille tulemusena sai juurdepääsu J.H arvelduskontole ja võimaluse kontol oleva varaga toimingute tegemiseks.[78]

[76] 1-11-7211
[77] 1-10-17197
[78] 1-11-14453

Kohtuotsusest ei nähtu kannatanu ja süüdistatava omavahelised suhted, kas nad tundsid üksteist ning kuidas sai võimalikuks ülekande tegemine, st kuidas J.J sai juurdpääsu J.H arvelduskontole. Varalist kasu võib saada ka internetikeskkonnas mingit teenust ostes, sh mobiiltelefonile kõneaega laadides.

Tartu Maakohus aga ei kinnitanud kokkulepet, kus naine sisestas ebaseaduslikult abikaasa internetipanga kasutajanime, salasõna ja koodi, mille hankis salaja, mehe teadmata ning millega mõjutas andmete töötlemise tulemust selliselt, et kandis mehe arvelt 8000 krooni enda arvele, kulutades raha enda tarbeks, põhjendusega, et tegemist on abikaasadega, abikaasade lahusvara suhtes andmed puuduvad ning sellisel juhul on lähtuvalt perekonnaseadusest abielu kestel omandatud vara ühisvara ning abikaasadel on võrdne õigus seda vallata, kasutada ja käsutada.[79]

Harju Maakohtus mõisteti isikud süüdi arvutikelmuses. K.K veenis koos F.S-ga K.O-d, et viimane annaks neile oma kontonumbri, deebetkaardi ja selle PIN-koodi, lubades konto kasutamise eest maksta raha. Saades K.O-lt kontonumbri, deebetkaardi ja PIN-koodi, andis K.K need üle F.S-le, kes edastas need D.S-le, kes omakorda edastas need A.V-le. „Seejärel sekkus eeluurimisel tuvastamata isik täpselt tuvastamata viisil internetipanga keskkonnas V.K poolt alustatud andmetöötlusprotsessi ning teostas OÜ A kontolt volitatud kasutaja teadmata ja volituseta 50000-kroonise ülekande K.O kontole“. Tuvastamata isik kandis K.O kontolt 9750 krooni S.P kontole ning 10000 krooni O.M kontole. „Sellise tegevusega osutas K.K ainelist kaasabi andmetöötlusprotsessi ebaseadusliku sekkumise teel varalise kasu saamisele, millega mõjutati andmete töötlemise tulemust“ ning isikud mõisteti süüdi arvutikelmuses.[80]
Sama otsusega mõisteti K.K ja F.S süüdi ka omastamises, kuna S.P andis neile kasutada oma pangaarve numbri, internetipanga juurdepääsu koodid ja salasõna, kuna uskus süüdistatavate põhjendust, et nad saavad automüügist suurema summa raha, kuid nende enda pangaarve on võlgade pärast blokeeritud. Saades S.P pangakonto koos kontol olnud rahaliste vahenditega enda valdusesse, võtsid nad tema kontolt mitmel korral sularaha välja, tasusid teenuste eest, tegid ülekandeid kolmandate isikute kontodele ning laadisid kõneaega. Sellise tegevusega pöörasid nad ebaseaduslikult enda ja kolmanda isiku kasuks neile usaldatud muu võõra vara.[81]

[79] 1-08-4059
[80] 1-10-16007
[81] 1-10-16007

Arvutikelmusena kvalifitseeritakse ka püsikorralduse sõlmimine teise isiku nimele. K.K käis külas T.T tütrel ning teadis T.T ning ka tema isa A.T pangaparoolide asukohta. K.K sisestas internetikohvikus A.T internetipanga kasutajatunnuse, salasõna ja paroolid ning sisenes A.T pangakontole, kus lisaks ülekannete tegemisele enda arvele, sõlmis varalise kasu saamiseks püsikorralduse, mille kohaselt oleks A.T pangakontolt iga kuu 19.kuupäeval laekunud K.K kontole 3000 krooni. Kuritegu jäi lõpule viimata, kuna A.T avastas korralduse ning tühistas selle.[82] Kui esimese kuu rahasumma oleks K.K pangakontole laekunud, oleks tegemist lõpuleviidud arvutikelmusega.

Rhodes mõisteti Ida-Kentucky piirkonnakohtu poolt süüdi pangapettuses U.S.Code Title 18 § 1344 alusel. Rhodes, olles vastutav kolme firma rahaasjadega tegelemises, omastas 3,5 aasta jooksul firmade raha kokku 380000 dollarit, peamiselt tehes ülekandeid firma arvetelt enda isiklikule arvele. Apellatsioonikohus oli nõus otsusega, mis puudutas pangapettust, kuid ei olnud nõus Rhodesele mõistetud 30 kuu pikkuse karistusega, leides, et see on ebaproportsionaalne, võttes arvesse tema vaimset seisundit, seda, et ta enam kuritegusid toime ei pane ning et ta peab üleval pidama oma tütart.[83]
Eesti kohtud kvalifitseeriksid sellise kuriteo ilmselt omastamisena, kuna juurdepääs firmade arvelduskontodele oli Rhodesel seoses tööülesannetega, seega olid arvelduskontod ning sellel olev raha muu isikule usaldatud vara omastamise koosseisu teise teoalternatiivi tähenduses.

Pangakontode ebaseadusliku kasutamise kuritegude puhul tekivad kõige sagedamini piiritlemisprobleemid arvutikelmuse ja omastamise koosseisude vahel. Piiritlemisel on oluline teha vahet, kuidas internetipanga paroolid sattusid süüdistatava kätte- kas ta kasutas selleks mingit programmi, sai paroolid muul moel ebaseaduslikult enda kätte või usaldas talle need kannatanu mingite toimingute tegemiseks, kuid tema tegi toiminguid, milleks teda ei volitatud. Arvutikelmusena kvalifitseeritakse kuriteod, kui süüdistatav sai paroolid kannatanu tahtest sõltumata (varastas, leidis, kasutas mingit programmi) või kui paroolid anti küll vabatahtlikult, kuid mitte tehingute tegemiseks; omastamisena kvalifitseeritakse kuriteod, kui kannatanu vabatahtlikult andis kahtlustatavale paroolid, kuid süüdistatav ületas volituse piire, samuti tööülesannete tõttu saadud ligipääsu kuritarvitamine.
Ebaseaduslikeks pangaülekanneteks on ülekanne ühelt kontolt teisele, olenemata sellest, kas võetakse rahasumma sularaautomaadist välja või mitte; ülekanne kaupade või teenuste ostmiseks (sh mobiiltelefonile kõneaja laadimine).

[82] 1-10-15796
[83] U.S. v. Rhodes 410 Fed.Appx. 856 C.A.6 (Ky.),2010

3.2 Pangakaardi ebaseaduslik kasutamine

Arvutikelmusena kvalifitseeritakse nii õige pangakaardi kasutamine kui selleks puudus pangakaardi omaniku luba kui ka võltsitud pangakaardi kasutamine- nii sularahaautomaadist raha väljavõtmine kui ka kaardiga kaupluses tasumine.

„Pangaautomaat on panga seade, mis võimaldab kliendil välja võtta sularaha ööpäevaringselt. Selleks antakse kliendile magnetlindiga kaart, millele on kodeeritud tema identifitseerimisnumber ehk PIN-kood. Pank ja klient sõlmivad kaardi kasutamise kohta vastava lepingu“.[84] Praegusel ajal võib magnetlinti asendada ka kiip.

Eestis on kasutusel kahesugused pangakaardid:

„deebetkaart, mis võimaldab kliendil välja võtta teatud limiidi piires raha oma arvelt;

krediitkaart, kus raha tuleb panga arvelt ning klient peab hiljem vastava summa pangale tagasi maksma“.[85]

Käesoleval ajal on nt Swedbangas kasutusel Deebetkaart Pluss, millega saab maksta nagu krediitkaardiga, kuid ainult kliendi pangaarvel oleva summa ulatuses.[86]

„Pangakaardiga manipuleerimine on võimalik üksnes andmetöötlusprotsessi sekkumisega, sest pangaautomaat on lülitatud arvutivõrku. See kehtib nii sularahaautomaadi kui ka internetipanga kohta. Selline tegu on subsumeeritav § 213 järgi arvutikelmusena.“[87]

Riigikohtu otsuses käsitletakse pangakaardi ebaseaduslikku kasutamist vargusena. F.B varastas A.L sõiduautost A.L-le väljastatud pangakaardi ning võttis PIN-koodi lehe kasutamise teel tema arvelduskontolt kolmel korral raha kogusummas 152 400 krooni. Riigikohus leidis, et: „süüdlane kasutas teisele isikule kuuluva nõudeõiguse, s.o rahatähtede üle oma valduse kehtestamiseks pangakaarti kui riista, 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 ehk vargus“.[88]

Pigem on pangakaardi ning PIN-koodi sisestamine sularahaautomaati andmete ebaseaduslik sisestamine arvutiprogrammi ehk sularahaautomaati, mitte pangakaart kui riist tõkke kõrvaldamiseks.

[84] J.Sootak. Varavastased süüteod, lk 204-205. Tln, 2009
[85] J.Sootak. Varavastased süüteod, lk 204-205. Tln, 2009
[86] www.swedbank.ee
[87] J.Sootak. Varavastased süüteod, lk 204-205. Tln, 2009
[88] 3-1-1-60-04 p 6

Kui varastatakse ainult pangakaart näiteks koos rahakotiga ning hiljem sularaha väljavõtmisel ei kasutata, võiks kvalifitseerida vargusena kas KarS § 199 või § 218 alusel, olenevalt rahakoti ning selles olnud esemete väärtusest.

J.V mõisteti süüdi arvutikelmuses, kuna tema võttis ebaseaduslikult ära A.K pangakaardi ning, kasutades PIN-koodi, võttis kannatanu arvelt kaheteistkümnel korral sularahaautomaatidest välja sularaha, kokku 91250 krooni.[89]

L.H mõisteti Harju Maakohtus süüdi arvutikelmuses, mis seisnes selles, et ta kasutas varalise kasu saamise eesmärgil tema valdusesse sattunud E.P arveldusarve juurde väljastatud deebetkaarti ning arveldusarvele ligipääsu võimaldavat PIN-koodi, sisestades PIN-koodi pangaautomaati. Sellise tegevusega käivitas L.H lubamatult andmetöötlusprotsessi ning võttis erinevatest sularahaautomaatidest E.P arveldusarvelt välja kokku üle 3800 euro.[90] Kohtuotsusest ei nähtu, kuidas süüdistatava valdusesse „sattus“ kannatanu pangakaart ja PIN-kood, seetõttu ei saa ka välistada, et tegemist võib olla hoopis omastamisega.

Sarnaselt mõisteti arvutikelmuses süüdi V.S, kes sisestas varalise kasu saamise eesmärgil andmed (ehk PIN-koodi) ebaseaduslikult pangaautomaati, et saada juurdepääs võõrale arvelduskontole ning käivitas omaniku nõusolekuta andmete töötlusprotsessi kontol oleva varaga toimingute tegemiseks ja võttis välja sularaha.[91]

Harju Maakohtus mõisteti S.T, I.G, E.T, R.T ja M.J süüdi arvutikelmuses ning sellele kaasaaitamises, samuti pangakaartide võltsimises ning võltsimisele kaasaaitamises. S.T, saades ebaseadusliku ligipääsu kaudu RBS Worldpay arvutisüsteemidele Palm Desert National Bank’i erinevate deebetkaartide andmed, edastas ta need I.G-le, kes võltsis saadud andmete alusel pangakaardid, millega E.T, R.T ja M.J võtsid erinevatest sularahaautomaatidest erinevate isikute pangaarvetelt sularaha välja kokku 3 550 000 krooni, „sekkudes seega ebaseaduslikult arvutiandmetesse, kasutades võltsitud pangakaarte ning pangaautomaatide arvutisüsteemi sisenemiseks pangakaardi seadusliku kasutaja ebaseaduslikult saadud identifitseerivaid andmeid PIN-koodide sisestamise näol“.[92]

[89] 3-1-1-42-11 p 1
[90] 1-11-7639
[91] 1-11-13084
[92] 1-09-16675

Viru Maakohus on leidnud, et kui isik varastab koos rahakotiga pangakaardi ning seejärel võtab sellega pangakontolt kannatanu raha, siis sellises teos puuduvad varguse koosseisu objektiivsed tunnused ning kuritegu tuleb kvalifitseerida arvutikelmusena. Algselt esitati D.K-le süüdistus varguses, mis seisnes selles, et D.K varastas Y.M-le kuuluva mobiiltelefoni ja rahakoti koos ID-kaardi ja pangakaardiga ning võttis samal päeval Y.M-i pangakontolt välja sularaha 2050 krooni. Prokurör kvalifitseeris pangakaardiga sularaha väljavõtmise ümber arvutikelmuseks ning kohus oli sellega nõus, põhjendades, et varguse koosseis nõuab võõra vallasasja ehk kehalise eseme äravõtmist omaniku valdusest. Pangakonto puhul on aga tegemist varalise nõudega panga vastu ning see ei saa olla isiku valduses.[93]

Samale seisukohale jõudis Pärnu Maakohus, mõistes arvutikelmuses süüdi A.T, kes peale isiklikul pinnal tekkinud tüli ning kehalist väärkohtlemist oma elukaaslasega, varastas nende korterist elukaaslase pangakaardi ning seejärel, teades PIN-koodi, sisestas varalise kasu saamise eesmärgil sularahaautomaati pangakaardi ning PIN-koodi ja võttis välja sularaha kokku 250 eurot. Seega pani ta toime arvutikelmuse.[94]
Kui eespool toodud kaasuses leidis kohus, et abikaasade ühisvara kulutamine ei ole kuritegu, siis antud juhul on õigustatud A.T teo kvalifitseerimine arvutikelmusena, kuna perekonnaseadus kaitseb abikaasasid, mitte vabaabielus olevaid isikuid.

Harju Maakohus on kvalifitseerinud süstemaatilise vargusena juhtumi, kus A.F isikuna, kes on süstemaatiliselt toime pannud vargusi, võttis ära I.D-le kuuluva pangakaardi ning kasutas seda sularahaautomaadis ning ebaseadusliku omastamise eesmärgil võttis I.D arveldusarvelt 250 eurot, tekitades sellega I.D-le varalist kahju.[95] Selline tegevus tuleks samuti kvalifitseerida arvutikelmusena, kuna pangakontol olev raha ei olnud I.D valduses.

Arvutikelmuses mõisteti süüdi J.N, kuna ta sisestas varalise kasu saamise eesmärgil erinevate kaupluste makseterminali ebaseaduslikult ostude eest tasumisel A.P pangakaardi ja PIN-koodi, mille ta oli A.P-lt teada saanud. Samuti võttis mitmel korral sularahaautomaadist välja sularaha, sisestades PIN-koodi ebaseaduslikult pangaautomaadi terminali, eesmärgiks varalise kasu saamine, pannes seega toime arvutikelmuse.[96]

[93] 1-11-4895
[94] 1-11-12863
[95] 1-11-13549
[96] 1-11-13432

Arvutikelmuses mõisteti süüdi ka H.T kuna ta sekkus varalise kasu saamiseks ebaseaduslikult andmetöötlusprotsessi, kasutades oma tuttava T.T-le kuuluvat pangakaarti ning teadaolevat PIN-koodi, ilma T.T teadmiseta ja loata, makstes tema pangakaardiga erinevates ettevõtetes. Seega pani H.T oma tahtliku tegevusega toime varalise kasu saamise andmetöötlusprotsessi ebaseadusliku sekkumise teel. Sama otsusega on H.T mõistetud süüdi ka varguses, kuna ta kasutas T.T-le kuuluvat pangakaarti sularahaautomaadist raha väljavõtmiseks.[97]
Nii pangakaardiga sularahaväljavõtmisel kui ka kaupluses ostude eest tasumisel sekkutakse ühtemoodi lubamatult andmetöötlusprotsessi, kui sisestatakse ebaseaduslikult PIN-kood. Selline vahetegu kvalifitseerimisel, seda enam, et ühes otsuses- ühel juhul vargus, teisel juhul arvutikelmus, on arusaamatu. Kaaluda võiks siin hoopis mõlema kuriteo kvalifitseerimist omastamisena. Kannatanu on H.T tuttav ning H.T hoolitses tema eest kahe nädala jooksul kannatanu haiguse ajal, käies tema eest poes ning selleks oli tal kannatanu luba kasutada tema pangakaarti, kuid H.T ei tagastanud T.T-le pangakaarti. Üheselt ei ole selge, kas H.T kasutas T.T pangakaarti sellel ajal enda tarbeks, kui tal oli T.T luba sellega poes käia või kasutas seda siis, kui ta T.T juurest lahkunud oli ning seega ebaseaduslikult kaasa võtnud T.T pangakaardi. Viimase küsimuse lahendamisel saaks otsustada, kas kvalifitseerida H.T kuriteod arvutikelmusena või omastamisena.

A.L mõisteti süüdi arvutikelmuses, kuna tema, eelnevalt põhjustades ettevaatamatusest M.S-i surma, võttis enda kätte M.S-i pangakaardi, mille PIN-koodi teadis ta varasemast ajast, ning võttis sellega sularahaautomaadist välja M.S-le kuuluva sularaha, ehk pani toime andmete ebaseadusliku sisestamise, mille tulemusena käivitas M.S-i nõusolekuta andmetöötlusprotsessi, eesmärgiga saada juurdepääs võõrale arvelduskontole, et seal oleva varaga toiminguid teha ehk sularaha välja võtta.[98]

Gail Marie Hakley töötas koduabilisena Eleanor Belseri juures. Hakley sai teada Ms Belseri PIN-koodi ning kasutas seda numbrit, võttes Ms Belseri kontolt ebaseaduslikult välja sularaha, kokku 7746,72 dollarit. Lisaks sai Hakley teada Ms Belseri sotsiaalkindlustuse numbri ning kasutas seda mitme krediitkaardi tegemiseks. Krediitkaarte kasutas süüdistatav erinevates kauplustes, näiteks tegi ta sisseoste Victoria Secret´is 1000 dollari eest. Selline tegu kvalifitseeriti USA 6.piirkonna Apellatsioonikohtu poolt kui identiteedivargus U.S Code Title 18 § 1028(a)(7) alusel.[99]

[97] 1-11-10596
[98] 1-11-11863
[99] U.S. v. Hakley 101 Fed.Appx. 122 C.A.6

Eesti kohtutes saaks Hakley tõenäoliselt karistada arvutikelmuse eest, kuna ta sisestas PIN-koodi (ehk andmed) ebaseaduslikult sularahaautomaadi terminali (ehk arvutiprogrammi). Krediitkaardiga kaupluses maksmine tuleks kvalifitseerida arvutikelmusena (kui kaupluses tuleb sisestada kuskile kaardi andmed või PIN-kood) või kelmusena, kui ostu sooritamisel luuakse ebaõige ettekujutus kaupluse müüjale (Hakley esineb Ms Belserina).

Saksamaa Apellatsioonikohus tühistas isiku süüdimõistmise varguses, leides, et tegemist on arvutikelmusega.[100]

Süüdistatav, töötades pangas, kasutas seadmeid, mis olid seotud sularahaautomaatidega ning mida ta oskas käsitleda tööülesannete tõttu, kogudes ja hoides kontode kohta ulatuslikke andmeid ning salajasi numbreid, mis olid kodeeritud sularaha väljavõtmise kaartidele. Kasutades kodeerimisaparaati, kandis ta andmed tühjadele kaartidele. Ta kasutas neid koopiaid sularahaautomaatides ning võttis teiste inimeste kontodelt sularaha välja kokku 140000 saksa marka. Selline sularaha väljavõtmine oli võimalik seetõttu, et automaatides, mida süüdistatav kasutas, ei kasutatud spetsiaalset võltsitud kaartide kasutamise ennetamise turvasüsteemi või oli tegemist süsteemi defektiga, kuid automaat jätkas siiski tööd.[101]

Eesmärgiga saada ebaseaduslikult varalist kasu, põhjustas süüdistatav kontoomanikele (või pangale, kes pidi kontoomanikele hüvitama varalise kahju) varalist kahju, mõjutades ebaseaduslikult andmete töötlemise tulemust.[102]

Kohus leidis, et juhtumit, kus süüdistatav kasutab ilma panga volituseta arvutiandmeid, et võltsida pangakaarte ning võtta nendega sularahaautomaatidest raha välja, ei kvalifitseerita vargusena, kuna ta ei saa raha kätte kellegi valdust murdes ning ta ei võtnud raha ära sularahaautomaatide operaatoritelt, vaid raha anti talle automaatide vahendusel.[103]

Raha valduse ülekandmise tegu- kui kasutatakse sularahaautomaati, erineb seetõttu raha üleandmisest pangatöötaja poolt, et inimese asemel kontrollib kasutaja õigust raha välja võtta automaat, mis on arvutiprogrammi poolt kontrollitud, kooskõlas kriteeriumitega, mis sisalduvad spetsiaalses programmis. Samuti ei ole tegemist vargusega, kui sularahaautomaati kasutatakse lähtuvalt selle otstarbest, st kaart on väljastatud panga poolt, kuid seda kasutatakse kontoomaniku nõusolekuta.[104]

Kasutades sularahaautomaati lähtudes selle otstarbest, ei ole tegemist vargusega juhtudel, kui kaart on välja antud panga poolt ning kaarti kasutatakse ilma kolmanda poole nõusolekuta.

[100] Forged Cash Card, Re (2 StR 376/91) [1993] E.C.C. 91 Bundesgerichtshof (Germany)
[101] Forged Cash Card, Re (2 StR 376/91) [1993] E.C.C. 91 Bundesgerichtshof (Germany)
[102] Forged Cash Card, Re (2 StR 376/91) [1993] E.C.C. 91 Bundesgerichtshof (Germany)
[103] Forged Cash Card, Re (2 StR 376/91) [1993] E.C.C. 91 Bundesgerichtshof (Germany)
[104] Forged Cash Card, Re (2 StR 376/91) [1993] E.C.C. 91 Bundesgerichtshof (Germany)

Tõsiasi, et antud juhtumi puhul ei olnud tegemist panga poolt välja antud kaartidega (nö tõeliste kaartidega), vaid kasutati võltsitud kaarte, ei muuda fakti, et siin kasutati samuti sularahaautomaati kooskõlas selle otstarbega. Süüdistatav ei sekkunud automaati, pigem juurdepääsu vahenditesse, mille oli paigaldanud pank. Kasutades võltsitud kaarte, lõi ta automaadile vale ettekujutuse selleks, et pank väljastaks rahatähed. Määrav tegur raha väljastamisel oli õigete andmete talletamine kodeeritud ribale, oluline ei ole, kas see on tehtud panga või kellegi teise poolt.[105]

Müügiautomaadi ebaseadusliku kasutamise juhtumeid (nt müügiautomaati sisestatakse võltsitud mündid ning müügiautomaat väljastab selle tagajärjel kauba), mis kvalifitseeritakse vargusena, ei saa laiendada sularahautomaadi ebaseadusliku kasutamise juhtumitele, kuna müügiautomaatide tööpõhimõtted põhinevad lihtsatel vahenditel ning töötavad mehhaaniliselt, ilma spetsiaalse eelprogrammeerimiseta, sularahaautomaadid on aga ühendatud arvutisüsteemidega.[106] Võimalik, et praegusel ajal on ka müügiautomaadid arvutil baseeruvad ning sellisel juhul tuleks ka nende ebaseaduslik kasutamine kvalifitseerida arvutikelmusena.

Kehtestades kriminaalkoodeksi §-i 263a, oli seadusandja üheks eesmärgiks hõlmata sularahaautomaatides pangakaardi ebaseaduslik kasutamine, eelkõige teise isiku PIN-koodi ebaseaduslik kasutamine sularaha väljavõtmise eesmärgil.[107]

Meie seaduste kohaselt oleks selline kuritegu samuti kvalifitseeritud arvutikelmusena (lisaks ka pangakaartide võltsimine) ning seda kaasust võib võrrelda Harju Maakohtu otsusega nr 1-09-16675.

Saksamaa kohtus mõisteti isik arvutikelmuses õigeks. Süüdistatav elas ajutiselt koos kannatanuga ning neil oli ühine majapidamine. Süüdistataval ei olnud endal arvelduskontot, seetõttu kanti tema tööturaha kannatanu kontole. Pangakaardi PIN-koodi teadis süüdistatav varasemalt, kuna nad käisid kannatanuga koos poes. Süüdistatav ütles kannatanule, et ta annaks oma pangakaardi, kuna ta tahab konto väjavõtet vaadata, et näha, kas tema tööturaha on juba laekunud. Kannatanu andis talle pangakaardi, tööturaha ei olnud kontole veel laekunud, kuid süüdistatav võttis ikkagi tööturaha summa ulatuses ehk 650 eurot kannatanule kuuluvat raha välja. Sellega lõi ta kannatanule ettekujutuse, et ainult vaatab kontojääki, kuigi kavatses juba algusest peale ka raha välja võtta, isegi juhul, kui tööturaha ei ole veel tulnud. Kohus leidis, et tegemist ei ole arvutikelmusega, kuna süüdistataval oli pangakaardi PIN-kood teada. Ka ei ole kelmus, kuna tal oli kannatanu luba konto kasutamiseks, st ta ei kasutanud

[105] Forged Cash Card, Re (2 StR 376/91) [1993] E.C.C. 91 Bundesgerichtshof (Germany)
[106] Forged Cash Card, Re (2 StR 376/91) [1993] E.C.C. 91 Bundesgerichtshof (Germany)
[107] Forged Cash Card, Re (2 StR 376/91) [1993] E.C.C. 91 Bundesgerichtshof (Germany)

kontot ilma loata. Kokkuvõtteks leidis kohus, et tegemist ei ole üldse kuriteoga, kuna tööturaha tuli hiljem nagunii kannatanu kontole ning kannatanu varalist kahju ei saanud.[108]
Ka Eestis ei kvalifitseeritaks sellist tegu arvatavasti arvutikelmusena, kuna isikul oli konto kasutamise nõusolek olemas, samuti oli teada PIN-kood. Seisukohaga, et selline tegu ei ole üldse kuritegu, on raske nõustuda. Võrdluseks võib tuua töösuhte- näiteks makstakse töötajatele palka sularahas sellest summast, mis kuu jooksul kassasse laekub. Töötaja teab, et tal on kahe päeva pärast palgapäev ning tema palgaraha laekub nagunii samasse kassasse ja ta võtab ise tööandja käest palga ette ära. Kuigi tööandja ei saaks sellise tegevusega varalist kahju, võiks tegemist olla omastamisega.

Pangakaardi ja sularahaautomaadi ebaseadusliku kasutamise korral tekivad piiritlemisprobleemid arvutikelmuse, omastamise, varguse ja kelmusega.
Kelmuse ja arvutikelmuse piiritlemisprobleemid tekivad sellisel juhul, kui võõra pangakaardiga tasutakse kaupluses ostude eest. Sellistel juhtumitel tuleb vaadata, kas pangakaarti kasutades sisestatakse PIN-kood makseterminali või esinetakse kaardi omanikuna klienditeenindajale, st allkirjastatakse ostutšekk kaardi omanikuna.
Kui isik kasutab võõrast pangakaarti kaupluses ostude eest tasumiseks, esitab selle müüjale kassas, kus puudub PIN-kalkulaator, esineb ta kaardi ning konto omanikuna, luues sellega teadvalt ebaõige ettekujutuse ning sellise tegevuse tagajärjel teeb müüja kassas toimingu, mille tagajärjel võetakse kannatanu kontolt tehingu katteks raha.[109]
Kelmusena aga ei kvalifitseerita selliseid juhtumeid, kus teisele isikule kuuluva pangakaardiga makstakse kaupluse kassas, kus on vajalik sisestada PIN-kood ning sellise tegevuse tagajärjel tehakse kannatanu arvelduskontol varakäsutus ning süüdlane saab varalist kasu. Selline tegevus kvalifitseeritakse arvutikelmusena, kuna makse sooritamiseks tuleb sisestada andmed (ehk PIN-kood) ning sellega käivitatakse lubamatult andmetöötlusprotsess.[110]
Kaupluses võõra kaardiga tasumist võib kvalifitseerida ka omastamisena, kui pangakaart ning PIN-kood on antud isikule konto- ja kaardiomaniku poolt vabatahtlikult, kuid näiteks ostude valikul ületatakse volituse piire ja ostetakse midagi enda tarbeks. Või palub kannatanu, et isik võtaks tema arvelt välja 100 eurot, kuid süüdistatav võtab sularahaautomaadist välja 200 eurot, millest 100 eurot viib kannatanule, 100 eurot jätab endale.

[108] OLG Jena: Beschluss vom 20.09.2006 - 1 Ss 226/06 BeckRS, 2007, 05394
[109] 3-1-1-35-10 p 8.1
[110] 3-1-1-35-10 p 8.2

Sularahaautomaadist raha välja võtmisel tekivad probleemid varguse, omastamise ja arvutikelmuse piiritlemisel. Kuna pangakontol olevale rahale ei saa kehtestada kontoomaniku poolt valdust, siis ei saa tegemist olla ka valduse murdmise ehk vargusega. Lisaks sellele töötab pangaautomaat arvutiprogammi põhiselt ning sularaha väljavõtmiseks tuleb sisestada PIN-kood, mis käivitab andmetöötlusprotsessi ja kui selline tegevus on ebaseaduslik ning sellega saadakse varalist kasu, on täidetud kõik arvutikelmuse koosseisuks vajalikud tunnused ning tegu tuleb kvalifitseerida arvutikelmusena. Kuna vargus on pigem üldkoosseisuks ning arvutikelmus erikoosseisuks, siis erinormi olemasolul rakendadakse alati viimast.

Samas on kvalifitseeritud sularaha väljavõtmist pangaautomaadist omastamisena, kui süüdistatavale on kannatanu poolt juurdepääs võimaldatud, kuid kontot on kasutatud muuks otstarbeks (näiteks on võetud rohkem raha välja, kui kannatanu palus). Aga omastamise koosseis eeldab samuti, et asi (seega sularaha) oleks isiku valduses, kuid pangakontol olevale rahale ei saa kehtestada kontoomaniku poolt valdust. Sellisest loogikast lähtudes tuleks kõik sularahaautomaadist ebaseaduslikult sularaha väljavõtmised kvalifitseerida arvutikelmusena. Pangakontol olevat raha aga saab defineerida kui isikule usaldatud muud vara ning seega on võimalik kvalifitseerida ka omastamisena.

Palju on juhtumeid, kus sotsiaaltöötajate valdusesse on usaldatud hoolealuste pangakaarte ning internetipanga ligipääsu koode. Sotsiaaltöötajad on omastanud pangakontodelt raha, maksnud hoolealuste pangakaardiga, võtnud sularaha automaadist välja.
Riigikohus on seisukohal, et paljudes hoolekandeasutustes hoitakse hoolealuste maksevahendeid ning pangaandmeid, sh PIN-koode ebaseaduslikult töötajate valduses. Õigus selliseks juurdepääsuks on piiratud teovõimega isiku eestkostjal, milleks sageli ei ole määratud hoolekandeasutuse töötaja.[111]
Sellisest seisukohast lähtudes ei tuleks taolisi kaasuseid, kus isik kasutab oma tööülesannete tõttu võõrale kontole juurdepääsu saamise tõttu ebaseaduslikult hoolealuse pangakaarti ning arvelduskontot, kvalifitseerida omastamisena, vaid arvutikelmusena, kuna juurdepääsu koodid sisestatakse ebaseaduslikult ning talle usaldatud vara oli saadud ilma õigusliku aluseta.

3.3 Krediitkaardi pettused

Arvutikelmuste ühe osa moodustavad krediitkaardi pettused. See tähendab varastatud krediitkaardi andmete kasutamist, näiteks ostes kaupu või teenuseid kaardikasutaja nimele. Mõnel juhul võltsitakse uus pangakaart, kasutades teadaolevaid andmeid. Kaart varastatakse

[111] 3-1-1-105-10, p 15

või andmed saadakse failidest, mis ei ole korralikult kaitstud. Samuti ostetakse krediitkaardi andmed inimestelt, kellel on taolisele informatsioonile juurdepääs. Krediitkaardi pettused paigutatakse osades riikides identiteedivarguse alla.[112]

Arvutikelmuste toimepanemises mõisteti süüdi V.T, kuna tema sai koos eeluurimisel kindlaks tegemata M-nimelise isikuga varalist kasu andmete ebaseadusliku sisestamisega andmetöötlusprotsessi sekkumisega. V.T lasi S.J-l ja eeluurimisega kindlaks tegemata isikul vormistada panga arveldusarvete ja internetipanga kasutamiseks R.M, V.A, A.l, M.E ja V.K nimele arveldusarved, deebetkaardid, internetipanga liitumislepingud ning paroolikaardid. Seejärel vormistas V.T kontoomanike nimel virtuaalsed pangakaardid, edastas andmed M–nimelisele isikule, kes sisestas need elektroonilisel teel ebaseaduslikult mitmel korral USA internetikauplustega seotud kaardimaksesüsteemi ning selle tulemusel krediteeris pank kannatanute arvelduskontodelt tegelikkuses mittetoimunud tehingute eest raha. Sellise tegevusega said V.T ja M-nimeline isik varalist kasu kokku 1 351 966,40 krooni.[113]
Samuti vormistas V.T nii enda kui ka teise isiku nimele krediitkaardi, sisestas elektroonilisel teel ebaseaduslikult USA internetikauplustega seotud kaardimaksesüsteemi andmed krediitkaartide kohta ning nende krediitkaartidega internetikauplustes teostatud krediittehingute kohta, mille tulemusena sai pank informatsiooni arvelduskonto krediteerimiseks tegelikkuses mittetoimunud tehingute kohta. Pangatöötaja sekkumise tõttu jäi aga kuritegu lõpule viimata.[114] Kuritegu oleks lõpule viidud kui pank oleks jõudnud krediteerida tehingud. Katse algab krediitkaardi andmete sisestamisega kaardimaksesüsteemi.
Nimetatud otsuses leidis Ringkonnakohus ka, et arvutikelmuse toimepanemise kohaks tuleb lugeda kohta, kus süüdlane sai varalist kasu ehk kus reaalselt raha välja võeti.[115]
Arvutikelmuste puhul tekib tihti küsimus, milline prefektuur/prokuratuur/kohus (või siis ka riik) kuritegu menetlema peab, kuna kuriteoga võib olla seotud mitu kohta- juurdepääsu koodid saadakse ühes kohas, ülekanne tehakse teises kohas, raha võetakse välja kolmandas kohas ning see ei pruugi kokku langeda kohaga, kus kurjategija tegelikult varalist kasu saab. Praktikas on välja kujunenud, et menetleb see asutus, mille territooriumil raha pangakontolt välja võetakse (ehk kus süüdlane reaalselt varalist kasu saab) ning sellist lähenemist toetab ka nimetatud Ringkonnakohtu otsus. Kui kuriteo toimepanemise kohaks loetaks nii kohta, kus tehti ülekanne, kui ka kohta, kus kuritegu lõpule viidi ehk raha pangakontolt välja võeti, võib

[112] P.Gottschalk. Categories of financial crime. Journal of Financial Crime. 2010, 17(4).
[113] 1-06-14599
[114] 1-06-14599
[115] 1-06-14599

tekkida probleem, kes menetleb. Et sellist probleemi vältida, on igati põhjendatud, et kuriteo toimepanemise kohaks peab olema ainult üks riik.
Samas ei lange alati kokku varalise kasu saamise koht ja raha väljavõtmise koht. Paljudel juhtudel kasutatakse kuriteo toimepanemisel nö tankiste, kes raha välja võtavad ühes kohas, kuid saadavad selle hoopis teise riiki, kus kurjategija saab reaalselt varalist kasu. Tankistid võivad seda teha paarikümne euro või pudeli õlle eest ning ei saaks öelda, et sellisel juhul langevad raha väljavõtmise koht ning varalise kasu saamise koht kokku.

Arvutikelmusele kaasaaitamisega on tegemist järgneval juhul. Kriminaalmenetlusega tuvastamata isik tasus andmete ebaseadusliku sisestamise teel internetileheküljel www.supermagnete.de kauba eest, kasutades selleks A.P krediitkaardi andmeid ilma kaardiomaniku teadmise ja loata. V.P esitas postkontoris oma passi ja kriminaalmenetlusega tuvastamata isikult saadud volikirja saadetise vastuvõtmiseks ning võttis välja A.P nimele saadetud postipaki ja andis üle tuvastamata isikule, millega viimane sai varalist kasu. V.P sai töö eest (st saadetise väljavõtmise ja üleandmise eest) tuvastamata isikult 10-20 eurot. V.P mõisteti süüdi arvutikelmusele kaasaaitamises.[116] Selline nö tankistide kasutamine arvutikelmuste toimepanemisel on üsna levinud. Tegelik kurjategija jääb sageli tabamata ning karistada saab isik, kes oma teoga märkimisväärset varalist kasu ei saanudki.

I.D pani toime tahtliku kuriteo- kaasaaitamise varalise kasu saamisele andmete ebaseadusliku sisestamise teel ja mis seisnes selles, et tema aitas tahtlikult kaasa sellele, et kriminaalmenetluses tuvastamata isik teostas Interneti teel ilma krediitkaardi konto omaniku teadmise ja loata A.T arvelt rahaülekandeid neljal korral, kogusummas 1685,70 eurot, kasutades selleks ebaseaduslikult A.T krediitkaardi andmeid. Rahasummad kanti A.T konto arvelt üle Internetis finantstehinguid vahendava portaali Neteller.com kontole, mille omanik on I.D. Netelleri konto, millele A.T kontolt raha kanti, oli I.D loonud spetsiaalselt ülekande tegemise korraldanud isiku palvel ja just nende ebaseaduslike ülekannetega saadava raha väljavõtmiseks. A.T kontolt laekunud raha kandis I.D postkontoris Western Unioni vahendusel edasi Venemaale, V.S nimelisele isikule. Selle eest sai I.D raha laekumist ja edasi kandmist korraldanud isikult 2000 krooni.
Kuigi süüdistatava kaitsja väitel puudus süüdistataval tahtlus kuritegu toime panna, leidis kohus, et I.D pani talle inkrimineeritud kuriteo toime otsese tahtlusega. I.D vormistas oma nimele krediitkaardi ja isiklikult vormistas raha ülekandeblanketi, millest nähtuvalt ta kannab raha üle V.S-ile. Selle pangaülekande õigsust kinnitab ta oma allkirjaga. Selle tehingu eest

[116] 1-11-13820

edastas tema sõber talle 2000 krooni. Kohtuistungil väitis ta, et pangakaardi arestimise tõttu ja sõbra palvel tegi ta uue krediitkaardi. Kohtuistungil väidetu kohaselt ta teadis, et tema kaart on blokeeritud ja seega uue kaardi vormistamisega ei ole sellel kaardil rahasummat. Ta pidi aru saama ja ette nägema, et tema uuele krediitkaardile laekunud summa ei ole temale kuuluv ja ta oleks pidanud oma sõbralt küsima, kust on laekunud tema arvele raha, mille ta kandis üle VS-ile. Ta oli teadlik, et raha ülekandega teostab süüteokoosseisule vastava asjaolu ja tahab või möönab selle tagajärje saabumist. Ta oli teadlik, et selle tehingu eest saab ta 2000 krooni omanikuks ja selle summa saamist kinnitas ta ka kohtuistungil.[117]

L.M mõisteti süüdi arvutikelmuses, kuna tema sai varalist kasu sellega, et ta kasutas kaardiomanike K.U ja K.N teadmise ja nõusolekuta nende krediitkaartide andmeid internetis tehingute tegemisel erinevatel veebilehtedel, tehes nimetatud kaartidega makseid lennupiletite ja hotelliteenuste eest Türgi Vabariigi linnas, tasudes seal nii enda kui ka oma tuttavate hotelliteenuste eest.[118] Otsusest ei selgu, kuidas K.U ja K.N kaardiandmed L.M-i kätte sattusid.

USA Apellatsioonikohus jättis jõusse süüdistuse American Express´i töötaja Tamika Lawson´i suhtes, kes hankis Jennifer Augustele American Expressi kliendi D.K Shellmani konto numbri. Auguste lisas end Shellmani konto lisakasutajaks ning muutis arve aadressi nii, et talle saadeti krediitkaart koju. Auguste tegi Shellmani arvele kokku 16 ostu. Lisaks sellele pääses Lawson sisse veel viiele American Express kontole ning kõigil juhtudel lisas Auguste end kaardi lisakasutajaks. Auguste mõisteti süüdi ühe konto krediitkaardi pettuse katses ning ühe konto krediitkaardi pettuses U.S.Code Title 18 § 1029 (b)(2) ja § 1029(a) (2) alusel (6.tase).[119]

USA Virgiinia osariigi territooriumil asuv föderaalkohus mõistis süüdi David S. Lee kuues kuriteos, mis olid seotud varastatud krediitkaardi tehingutega. Lee töötas juveelipoes ning aktsepteeris ostude tegemisel krediitkaarte, mille kohta ta teadis, et need on varastatud, aktsepteerides maksmisel ka võltsitud konto väljavõtteid. Lee mõisteti süüdi U.S.Code Title 18 § 1029(b)2 ja 1029(a)(1) alusel volitamata juurdepääsuseadme kasutamises osalemises, kuna ta tegi seda teadlikult ja pettuse eesmärgil. Samuti mõisteti ta süüdi volitamata juurdepääsuseadme kasutamise katses ning krediitkaardist jäljendite tegemise seadme

[117] 1-11-7609
[118] 1-11-4870
[119] U.S. v. Auguste 392 F.3d 1266

omamise eest pettuse eesmärgil U.S. Code Title 18 § 1029(a)(4) alusel ning kahes episoodis siseriiklike telefonikõnede tegemises panga esindajana krediitkaardi autoriseerimiskeskusesse, et saada autoriseering järgnevateks pettuse tehinguteks U.S.Code Title 18 § 1343 alusel.[120]
Lee kaebas otsuse edasi, kuna leidis, et terminit „juurdepääsuseade" käsitletakse liiga ebamääraselt ja laialt ning et see on põhiseadusvastane. Apellatsioonikohus leidis, et terminit „juurdepääsuseade" käsitletakse laialt, et kaitsta uusi ja nõrku arveldussüsteeme (Lee puhul varastatud krediitkaardi kasutamine või võltsitud krediitkaardi väljavõtte kasutamine ebaseaduslike maksete tegemisel) ning seadus, mis keelab võltsitud ja ebaseaduslikku juurdepääsu võimaldavate seadmete kasutamise, ei ole põhiseadusevastaselt ebamäärane ega liiga avaralt käsitletud.[121]
Eestis oleks sellise juhtumi puhul tegemist arvatavasti arvutikelmusele kaasaaitamisega (juhul, kui klient sisestab ise PIN-koodi) või oleks Lee arvutikelmuse täideviija (juhul, kui Lee sisestab ise PIN-koodi).

Krediitkaarte saab ebaseaduslikult kasutada kahel viisil- kas varastatakse teise isiku andmed või kasutatakse võltsitud kaarti. Krediitkaardi ebaseaduslikku kasutamist võib kvalifitseerida samuti kui deebetkaardi ebaseaduslikku kasutamist- arvutikelmusena, omastamisena või kelmusena, koosseisudel tuleks vahet teha samadel põhjendustel, mis deebetkaardi kasutamise puhul. Osades riikides kvalifitseeritakse ka identiteedivargusena (juhul, kui isik taotleb pettusega pangalt uue krediitkaardi väljaandmist, mis on seotud teise isiku pangakontoga), mis võiks mõnel juhul kaalumisele tulla ka meil.

3.4 Kütusekaardi ebaseaduslik kasutamine

Riigikohus on käsitlenud vargusena järgnevat juhtumit. R.P-d süüdistati varguses, mis seisnes selles, et tema võttis Neste ettemaksukaardiga Neste Eesti AS automaattanklast kaardisüsteemi tarkvara rikkudes välja 17357,76 krooni väärtuses kütust. Nimetatud ettemaksukaardil olid seejuures rahalised vahendid ainult 50 krooni väärtuses kütuse omandamiseks. Riigikohus leidis, et kuna menetluse käigus ei tõendatud piisavalt kütuseautomaadiga manipuleerimist, siis tuleb süüdistatava tegevus kvalifitseerida vargusena, kuna kriminaalasjas on vastuvaidlematult tõendatud, et võõras valdus asjale ehk bensiinile lõpetati ja selle suhtes kehtestati uus valdus. Kuna uue valduse kehtestaja ei olnud algusest peale ei maksmisvõimeline ega maksmisvalmis ja tegutses seega algusest peale ebaausate

[120] U.S. v. Lee 815 F.2d 971 C.A.4
[121] U.S. v. Lee 815 F.2d 971 C.A.4

kavatsustega, on tegemist vara hõivamisega senise valduse murdmise näol ja seega vargusega.[122]

Siin võiks paralleele tõmmata nö külma arve tegemisega, mis kvalifitseeritakse kelmusena. Klient tellib söögikohas toitu, luues ettekandjale ettekujutuse endast kui maksejõulisest kliendist, kuid tegelikkuses tal raha ei ole ning ta lahkub, jättes arve tasumata. Kütuse tankimise puhul oli klient teadlik, et tema ettemaksukaardil on vaid 50 krooni, kuid tema tankis kütust tunduvalt suurema summa eest. Kuna aga tanklaautomaat ei ole inimene ning automaati petta ei saa, tuleks automaattankla kaardisüsteemi siiski käsitleda kui arvutiprogrammi. Samuti pidi R.P olema teadlik kaardisüsteemi rikkest, sest 50 krooni eest saadav bensiinikogus ei ole võrreldav kogusega, mida saab 17357,76 krooni eest. Teadlikkust näitab ka bensiini korduv tankimine. Vargusena võiks kvalifitseerida bensiini tankimise inimtööjõuga tanklates, kus tangitakse bensiini sõidukisse või kanistrisse ning seejärel lahkutakse maksmata, sellisel juhul ei sisestata kuskile mingeid andmeid ega kasutata kaardimaksesüsteemi (kütus voolab mehhaaniliselt kanistrisse või kütusepaaki). Automaattankla puhul tuleb maksta aga makseterminali ehk arvutiprogrammi vahendusel ning kui sinna sisestatakse ebaõiged andmed, võib tegemist olla arvutikelmusega. Kuigi ei leidnud piisavat tõendamist, et R.P kütuseautomaadiga manipuleeris ehk ise süsteemi rikkus või ebaõigeid andmeid sisestas, oli ta siiski teadlik, et ta saab ettemaksukaardil olevast summast rohkem kütust, kuna ta tankis kütust viieteistkümnel korral. R.P tunnistas ka ise, et muretses ettemaksukaardi just seetõttu, et oli teadlik, et sellega saab nö tasuta kütust. Seega on tsiviilõiguslik vahekord välistatud.

Sarnases asjas mõistis Saksamaa Apellatsioonikohus arvutikelmuse süüdistusega õigeks isiku, kes tankis 33 korral automaattanklas kütust, makstes pangakaardiga. Automaadil oli rike, mis seisnes selles, et kui kütus läks maksma üle 70 euro, siis automaat võttis vaid 70 eurot. Isik tankis summas 71-80 eurot ning selle kütuse, mis läks maksma üle 70 euro, sai ta tasuta. Isik teadis, et selline viga oli ning ta sai sellise tegevusega varalist kasu ning tankla varalist kahju. Kohus leidis, et ta kasutas ära tankimisautomaadi süsteemiriket, kuid ta ei sisestanud kuskile valesid andmeid ning ei sekkunud seega lubamatult andmetöötlusprotsessi ning tegemist ei ole kuriteoga.[123]

Kui lähtuda sellisest kohtu seisukohast, tuleks R.P mõista õigeks ning tankla võiks pöörduda hagiga tsiviilkohtusse. Saksamaa kohtu seisukohast tuleks selline tegevus kvalifitseerida arvutikelmusena, kui isik oleks sisestanud valesid andmeid ning sekkunud lubamatult

[122] 3-1-1-78-06
[123] OLG Braunschweig, Urteil vom 12. 10. 2007 - Ss 64/07, NStZ 2008, 402

andmetöötlusprotsessi, kuid kuna ta seda ei teinud, siis kuritegu on üldse välistatud. Tankimiskordade arv ning isiku teadlikkus rikkest ei ole määrav.

Arvutikelmuse toimepanemises mõisteti süüdi A.K ja V.R. A.K töötas AS-s H bussijuht-klienditeenindajana ning sai enda käsutusse tööülesannete täitmiseks bussi ning AS-ile H väljastatud kütusekaardi. Pärast töösuhte lõppu jättis A.K kütusekaardi tagastamata ning kasutas seda ebaseaduslikult AS H nõusolekuta peaaegu kolme kuu jooksul, tankides enda ja kohtueelse uurimisega tuvastamata isiku kasutuses olevasse sõidukisse ning koos V.R-ga viimase kasutuses olevasse sõidukisse diiselkütust. Tankimiseks esitas A.K tanklates klienditeenindajale kütusekaardi ning sisestas töösuhte tõttu teatavaks saanud PIN-koodi makseterminali, käivitades andmete ebaseadusliku sisestamisega andmetöötlusprotsessi ilma kaardi seadusliku valdaja nõusolekuta, saades varalist kasu tangitud kütuse näol kokku 40469,88 krooni. A.K tankis lisaks ühiselt ja kooskõlastatult koos V.R-ga V.R-i kasutuses olevasse kaubikusse kokku 443329,69 krooni väärtuses kütust. Ühel korral esitas V.R, ülejäänud kordadel A.K kokkuleppel A.R-ga (kes A.R on, otsusest ei selgu*)* tankla klienditeenindajale kütusekaardi, sisestades kütusekaardi PIN-koodi makseterminali, käivitades andmete ebaseadusliku sisestamisega andmetöötlusprotsessi ilma kaardi seadusliku valdaja nõusolekuta, mille tulemusena said A.K koos V.R-ga varalist kasu tangitud kütuse näol. Seega vastab selline käitumine KarS § 213 lg 1 objektiivsetele tunnustele, kuna kütusekaardiga maksmiseks oli vajalik täiendav toiming- andmete ebaseaduslik sisestamine, mille tulemusena käivitati lubamatult andmetöötlusprotsess. Ringkonnakohus leidis, et mõlemad isikud panid toime arvutikelmuse (maakohtus mõisteti V.R süüdi KarS § 201 ja § 202 alusel). V.R oli teadlik, et kütuse eest maksmisel kasutatakse võõrast kütusekaarti omaniku loata. Tema rolliks oli kütuse tankimine, ostjate leidmine, kütuse realiseerimine, raha saamine ning selle jagamine A.K-ga. Mõlema isiku panus süüteokoosseisu kui terviku realiseerumisse oli oluline. A.K, sisestades kaardi PIN-koodi, ei pane tegu toime üksiktäideviijana olukorras, kus isikute tegu tervikuna on alust käsitleda kaastäideviimisena.[124]

Saksamaal esitas ettevõte kaebuse oma töötaja kohta, kuna töötajale oli tööülesannete täitmiseks väljastatud kütusekaart, kuid töötaja lubas ettevõtte kütusekaardiga tankida ettevõttega mitteseotud isikutel. Töötaja esitas tööandjale kütusetšekid, mis klappisid kütusekaardilt maha läinud summadega, kuid kütust ei tangitud ettevõtte autosse. Kohus leidis, et tanklaautomaati ei kasutatud ebaseaduslikult ning sellist tegevust ei kvalifitseerita ka

[124] 1-10-13009

kaardipettusena, kuna tankmiskaart ei ole krediitkaart. Tankimiskaart on mõeldud kasutamiseks selleks otstarbeks, milleks see kokkulepitud on, ehk kütuse tankimiseks. Antud juhtumil oli tegemist kahe-partneri-süsteemiga ehk kaart oli mõeldud kasutamiseks tankla ja ettevõtte vahel ning ei olnud mõeldud kasutamiseks kolmandatele isikutele. Kohus leidis, et selline tegevus tuleks kvalifitseerida tsiviilpettusena StGB § 263 alusel, kuid süüdimõistmiseks ei ole piisavalt tõendeid.[125]

Eestis tuleks kaalumisele (muidugi, kui oleks piisavalt tõendeid) kas arvutikelmus või omastamine. Kütusekaarte kasutatakse tavaliselt automaattanklates ning nende juurde kuulub PIN-kood. Kui PIN-kood ja kütusekaart satuks töötaja kätte ebaseaduslikult ning ta kasutaks seda kütuse tankimiseks enda isiklikku või kellegi teise sõidukisse, oleks tegemist arvutikelmusega. Kui töötaja aga sai kaardi ja PIN-koodi seoses oma tööülesannetega ehk need on tema valduses (nagu ka Saksamaa kaasuse puhul), oleks tegemist omastamisega, kui ta pöörab kütusekaardi abiga kütuse enda või kolmanda isiku kasuks. Ettevõttega mitteseotud isikud saaksid aga karistada KarS § 202 alusel, kui nad teadlikult omandavad süüteoga saadud vara.

Kütusekaardi ebaseadusliku kasutamise puhul tekivad piiritlemisprobleemid arvutikelmuse, varguse, kelmuse ja omastamise koosseisude vahel.

Automaattankla kaardimakse süsteemi võib võrrelda pangaautomaadiga. Mõlemad töötavad arvutiprogrammi põhiselt. Selleks, et raha või kütust kätte saada, tuleb sisestada andmed- PIN kood, mis käivitab andmetöötlusprotsessi ning selle tagajärjel väljastatakse vastavalt kas raha või kütus. Kui see on toimunud ebaseaduslikult, siis on selline tegevus kvalifitseeritav arvutikelmusena. Kui automaat on rikkis ning väljastab ise suurema koguse raha või kütust ning ei ole tõendatud, et isik ise sisestas valesid andmeid või süsteemi rikkus, ei ole tegemist arvutikelmusega. Sellisel juhul tuleb kindlaks teha, kas on tegemist muu kuriteoga või tsiviilvahekorraga (alusetu rikastumine).

Arvutikelmuse ja omastamise koosseisude piiritlemisel tuleb selgitada, kuidas isik kütusekaardi sai. Kui talle anti kütusekaart tööülesannete täitmiseks, kuid ta kasutab kaarti endale kütuse tankimiseks, tuleks selline tegevus kvalifitseerida omastamisena. Tal oli õigus kasutada kütusekaarti, kuid mitte enda tarbeks. Kui isik saab tööülesannete täitmiseks kütusekaardi, kuid töölt lahkudes ei tagasta seda, vaid kasutab kütuse tankimiseks enda või kellegi teise tarbeks, tuleb selline tegevus kvalifitseerida arvutikelmusena. Arvutikelmusena tuleks kvalifitseerida ka juhtum, kus isik leiab kütusekaardi koos PIN-koodiga ning tangib sellega kütust enda kasuks.

[125] OLG Celle: Beschluss vom 05.11.2010 - 1 Ws 277/10 BeckRS 2010, 28415

Kelmuse koosseisuga piiritlemisprobleem võib tekkida juhul, kui tegemist ei ole automaattanklaga, vaid mehhaniseeritud tööjõuga tanklaga ning kütusekaardi PIN-koodi ei pea sisestama (isik suhtleb vahetult klienditeenindajaga ning loob talle ettekujutuse endast kui kaardi omanikust ning allkirjastab kütusetšeki kütusekaardi omanikuna).

3.5 SIM-kaardi ebaseaduslik kasutamine

Arvutikelmusena kvalifitseeritakse teisele isikule kuuluva SIM-kaardi kasutamist helistamiseks ja sõnumite saatmiseks, näiteks erootikatelefonidele, tutvumisportaalidesse, internetibörsidele ja meelelahutusnumbritele.

H.V kasutas varastatud mobiiltelefoni varalise kasu saamiseks, kuna ta laadis telefonis olnud, E.M-ile kuuluva SIM-kaardiga kõneaega nii enda mobiiltelefoni kõnekaardile kui ka teistele tasu eest, helistas ja saatis sõnumeid erootikatelefonidele, tutvumisportaalidesse, internetibörsidele ning meelelahutusnumbrile „mobiilimiljonär“, tekitades sellega E.M-ile varalist kahju 3478,03 krooni.[126]

Maakohus leidis, 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 andmetöötluse funktsiooni“.[127] Sellise seisukohaga tuleb nõustuda.

Noorte hulgas on populaarsed internetiportaalid www.rate.ee ja www.limpa.ru.

Rate.ee-s on kasutusel virtuaalne valuuta nimetusega SOL, millega saab osta rate.ee teenuseid ning teha ülekandeid teistele rate.ee kasutajatele. SOL-e saab eurode eest osta, samuti saab pärast eurode vastu vahetada. Müües ühe SOL-i, saab 0,10 eurot. Ostuhinnad on erinevad- ostes internetipanga kaudu, on kümne SOL-i hind 0,90 eurot (üksikult ostes on ühe hind 0,10 eurot); SMS-iga ning telefonikõnega on ühe SOL-i hind 0,19 eurot; kraapekaardiga on ühe SOL-i hind 0,14 eurot ning krediitkaardiga ühe SOL-i hind 0,12 eurot. Kasutajakontole tehtud sissemakseid saab kasutaja saata oma pangakontole, milleks tuleb tellida väljamakse.[128] SOL-ide saatmine oma pangakontole aitab enamasti tuvastada kahtlustatavat.

Sagenenud on seetõttu ka mobiiltelefoni SIM-kaardi ebaseaduslik kasutamine. Arvutikelmusena kvalifitseeritakse juhtumid, kui isik helistab varalise kasu saamise eesmärgil

[126] 1-10-8347
[127] 1-10-8347
[128] www.rate.ee

teise isiku mobiiltelefoniga ilma omaniku loata tasulisele numbrile 9001222 ning tellib internetikeskkonnast www.rate.ee virtuaalset raha ehk SOL-e.[129]

Näiteks mõisteti J.V süüdi arvutikelmuses, kuna ta kasutas teisele isikule kuuluvat mobiiltelefoni koos seal sees olnud SIM-kaardiga, helistades internetiportaali www.rate.ee kasutajatele mõeldud tasulisele telefoninumbrile 9001222 tariifiga 100 krooni kõne, millele lisandub paketipõhine kõnetasu, saates tasulisele telefoninumbrile 15154 sõnumeid, tariifiga 50 krooni sõnum. Seejärel, kasutades eritariifiga teenusenumbrile 900 1222 teostatud kõnede käigus ja eritariifsele numbrile 15154 saadetud sõnumite eest teenusepakkuja poolt edastatud koode, laadis ta enda kontole SOL-e. Samuti helistas J.V internetiportaali www.limpa.ru kasutajatele mõeldud tasulisele telefoninumbrile 9007775 tariifiga 100 krooni kõne, millele lisandub paketipõhine kõnetasu ning kasutades eritariifiga teenusenumbrile 900 7775 teostatud kõnede käigus teenusepakkuja poolt edastatud koode, laadis ta enda kontole portaalis kasutatavaid maksevahendeid nimega SOL.[130] Sellise tegevusega sekkus J.V andmetöötlusprotsessi mobiiltelefoni ja SIM-kaardi vahendusel, millega ta sai varalist kasu.

R.R ja I.J panid toime arvutikelmuse, mis seisnes selles, et R.R sekkus varalise kasu saamiseks ebaseaduslikult andmetöötlusprotsessi sellega, et olles saanud enda valdusesse AS M-le kuulunud telefoni SIM-kaardi, pani selle omale telefoni ning asus seda kasutama, helistades tavalistele ja eritariifsetele numbritele, saates SMS-sse, tasudes kauba eest ning kasutas Interneti teenust. I.J sekkus varalise kasu saamiseks ebaseaduslikult andmetöötlusprotsessi, mis seisnes selles, et olles saanud enda valdusesse AS-le M kuulunud telefoni SIM-kaardi, pani selle enda telefoni ning asus seda kasutama, helistades järjepidevalt nii tavalistele kui ka eritariifsetele numbritele, saatis SMS-sse, tasus kauba eest, ostis internetikeskkonnas www.rate.ee virtuaalset valuutat ehk SOL-e ning kasutas internetiteenust. R.R sai enda ütluste kohaselt SIM-kaardi oma emalt, sisestas SIM-kaardi oma telefoni ning sisestas PIN-koodi 1234, mis oli õige kood. Ta kasutas seda SIM-kaarti nädala ning andis seejärel edasi I.J-le. I.J pani SIM-kaardi oma telefoni, kuhu sisestas ka PIN-koodi 1234. I.J kasutas SIM-kaarti www.rate.ee internetilehel SOL-ide ning mängude tellimiseks, helistas tasulistele liinidele ning kogus kõneaega (st helistas teatud numbrile ning see number, kuhu helistatakse, kogub kõneaega 30 senti minutis). SIM-kaardi kasutamisega põhjustasid süüdistatavad kahju kokku 10000 euro ringis.[131]

[129] 1-10-8350
[130] 1-11-2755
[131] 1-11-4244

Arvutikelmuse toimepanemises mõisteti süüdi S.T, kes leides OÜ-le SH kuuluva mobiiltelefoni ja selles sisalduva SIM-kaardi, mille osas oli sõlmitud mobiilsideoperaatoriga sideteenuse osutamise leping, teostas kõnesid erinevatele abonentnumbritele ning tellis teenuseid SMS-sõnumite teel tasuliselt numbrilt 15151. SIM-kaardi kasutamiseks ning sel moel mobiilsideoperaatori ja teenuse tarbimiseks õigustatud isiku omavahelisse andmetöötlusprotsessi sekkumiseks puudus S.T-l OÜ SH luba.[132]

Harju Maakohtus mõisteti arvutikelmuse toimepanemises süüdi M.S.P, kes kasutas J.V1-le kuuluvat, kuid J.V2 kasutuses olevat SIM-kaarti varalise kasu saamiseks. J.V2 andis M.S.P kätte SIM-kaardi, mis jäi tagasi küsimata ning M.S.P helistas ja saatis sellelt lühisõnumeid, ilma J.V2 ja JV1 teadmise ja loata, erinevatele tava- ja eritariifsete tasudega mobiil- ja tavatelefonidele. Sellise tegevusega sekkus M.S.P ebaseaduslikult mobiiltelefonifirma arvutisüsteemi andmetöötlusprotsessi, mõjutades andmete töötlemise tulemust.[133]

Saksamaa kohus mõistis arvutikelmuse süüdistuses õigeks telefonipoe koristaja, kes laadis arvutisüsteemi abil oma telefonikaardile kõneaega, kokku 86 korral 2195 euro väärtuses. Ettemaksukaartidele saab kõneaega laadida telefonipoes arvutisüsteemi poolt juhitava terminali kaudu, milleks peab sisestama koodi. Koristaja sai teada, kuidas kõneaja laadimissüsteemid töötavad, sisenes andmebaasi, sisestas enda telefoninumbri ning laadimislepingu numbri, st õiged andmed. Seejärel tuli terminali ekraanile telefonioperaatori kood, mille ta teatas oma kõnekaardi operaatorile ning tänu sellele sai ta oma ettemaksu kontole kõneaega. Kohus leidis, et tegemist ei ole arvutikelmuse ega kelmusega. Tegemist on küll andmete ebaseadusliku kasutamisega, kuid mitte arvutikelmuse tähenduses. Arvutikelmuse koosseis nõuab andmetöötlusprotsessi käivitamist, kuid antud juhul ei käivitanud süüdistatav andmetöötlusprotsessi, vaid sisenes terminali nö nuppude vajutamise teel. Sellele järgnevat automaatset protsessi ei saanud süüdistatav kuidagi mõjutada, seega ei olnud tegemist ka arvutisüsteemi mõjutamisega. Kohus leidis, et tegemist on hoopis Kriminaalkoodeksi §-ga 265a[134] (teenuste saamine pettusega[135]).
Eestis tuleks selline tegu kvalifitseerida siiski arvutikelmusena, kuna meil sellist erikoosseisu nagu Saksamaal ei ole, või arvutisüsteemi ebaseadusliku kasutamisena.

[132] 1-11-9365
[133] 1-11-4737
[134] LG Freiburg Urteil vom 19.11.2008 - 7 Ns 150 Js 4282/08 BeckRS 2009, 00403
[135] Saksamaa kriminaalkoodeks § 265a

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.

Piiritlemine võõra asja omavolilise kasutamise koosseisust. SIM-kaardil endal tavaliselt väärtus puudub, uue SIM-kaardi saab operaatorilt 3,20 kuni 7,99 euro eest[136]. SIM-kaardiga põhjustatud kulu ei ole eseme lisaväärtuseks, seetõttu ei saa kvalifitseerida SIM-kaardi ebaseaduslikku kasutamist asja omavolilise kasutamisena.[137]

Piiritlemine kelmuse koosseisust. „Telefoni SIM-kaart on küll lepinguga seotud konkreetse isikuga, kuid leping ei takista nt SIM-kaardi teisele isikule kasutamiseks andmist (erinevalt nt pangakaardist). Igal isikul on õigus anda oma telefoni koos selles sisalduva SIM-kaardiga teisele isikule kasutamiseks. Kes maksab arve, on nende isikute omavahelise kokkuleppe küsimus, juriidiliselt on kohustatud arve tasuma operaatorfirmaga lepingu sõlminud isik. Seega ei saa ka kõneoperaator eeldada ega peagi eeldama, et SIM-kaardilt helistav inimene on sama inimene, kes sõlmis lepingu ning kellele saadetakse arve. Seega lihtsalt selle asjaoluga, et SIM-kaarti kasutab teine inimene, ei panda toime tegelikest asjaoludest pettekujutuse loomist. Samuti kerkib küsimus sellest, kas operaatorfirma helistamise süsteemi saab petta-eksimus kui teise isiku õiguslikult relevantse tunnetuse mõjutamine s.t eksida saab vaid inimene, masin, automaat või süsteem ei saa inimest uskuda või mitte uskuda. Seega tegemist ei ole kelmusega.“[138]

Piiritlemine varguse koosseisust. Varguse koosseis eeldab võõra vallasasja äravõtmist. SIM-kaardi kasutaja saab õiguse helistada või kasutada muid teenuseid, ta ei saa käegakatsutavat asja ega raha endale.[139]

Piiritlemine omastamise koosseisust. Kui isik annab oma mobiiltelefoni kasutada tuttavale näiteks ühe kõne tegemiseks, kuid tuttav teeb rohkem kõnesid (üle kuriteoks kvalifitseerimise jaoks vajaliku summa), siis võiks kvalifitseerida omastamisena.

Samas on ka vastupidiseid seisukohti. Valduses oleva võõra vallasasjaga tegemist ei ole (vt varguse piiritlemise juures), samuti ei saa olla isikule usaldatud muu võõra vara ebaseaduslikult enda kasuks pööramisega, kuna seda arvet, mille isik põhjustab, ei ole tema kasuks usaldatud.[140]

---

[136] www.tele2.ee
[137] Karistusseadustik § 215
[138] T.Ploom. Mitteametlik juhis arvutikelmuse kvalifitseerimisel. E-kirjavahetus (autori valduses). 16.03.2009
[139] T.Ploom. Mitteametlik juhis arvutikelmuse kvalifitseerimisel. E-kirjavahetus (autori valduses). 16.03.2009
[140] T.Ploom. Mitteametlik juhis arvutikelmuse kvalifitseerimisel. E-kirjavahetus (autori valduses). 16.03.2009

Lähtudes ülaltoodud seisukohtadest saab SIM-kaardi ebaseaduslikku kasutamist kvalifitseerida vaid arvutikelmusena või kui kahjusumma ei anna kokku kuriteoks vajalikku summat, siis KarS § 218-na.

Kui kasutatakse võõrast SIM-kaarti ilma omaniku nõusolekuta ning sellega tekitatakse omanikule helistamisega, parkimisega, SOL-de ostmisega vmt rahalisi kohustusi, on tegemist arvutikelmusega, kuna ilma teise isiku volituseta toimingute tegemisega sisestatakse ebaseaduslikult andmeid § 213 tähenduses süsteemis, mis automaatselt töötleb telefoni kasutamise tulemeid ning tegemist on arvutisüsteemiga, s.o andmeid programmi järgi töötleva seadmega.[141]

3.6 Kiirlaenu taotlemine

Maakohtud on kvalifitseerinud KarS § 213-na ka kuriteod, kus teise isiku nimele võetakse kiirlaenu.

Arvutikelmuses mõisteti süüdi A.I, kes kasutades tema valdusesse sattunud O.G internetipangaga seotud ligipääsu võimaldavaid andmeid, registreeris O.G ilma tema nõusolekuta kiirlaenu saamise eesmärgil, kasutades isiku- ja pangakonto andmeid, internetikeskkonnas laenufirma kasutajaks, mille kinnituskood saadeti laenufirma poolt SMS-i teel kasutajakonto registreerimisel süüdistatava poolt sisestatud elektronpostiaadressile. Seejärel sisenes süüdistatav ebaseaduslikult teise isiku nimele väljastatud internetipangale ligipääsu võimaldavaid andmeid kasutades O.G internetipanka, millega autentis laenufirma internetikeskkonnas registreeritud O.G kasutajaisiku ning täitis tema nimel laenutaotluse. Laenufirma rahuldas laenutaotluse ning kandis laenusumma O.G kontole. Seejärel sisenes süüdistatav uuesti O.G internetipanka ning kandis laenufirmalt laekunud laenusumma üle kolmanda isiku arveldusarvele ning võttis kolmandale isikule väljastatud pangakaarti kasutades sularahaautomaadist raha välja. Maakohus leidis, et sellise teoga pani süüdistatav toime varalise kasu saamise andmete ebaseadusliku sisestamise ja muutmise teel.[142]

Samale järeldusele jõudis Harju Maakohus. Kohus leidis, et süüdistatav, kasutades ilma A.K nõusolekuta tema nimele väljastatud internetipanga kasutajatunnust, püsiparooli ja paroolikaarti, sisenes ebaseaduslikult internetipanga maksekeskkonda ja võttis A.K nimele kiirlaenu ning samal päeval, kasutades ebaseaduslikult A.K andmeid, kandis raha edasi kahele erinevale kolmandate isikute arvelduskontodele, pani toime arvutikelmuse, s.o varalise kasu

[141] T.Ploom. Mitteametlik juhis arvutikelmuse kvalifitseerimisel. E-kirjavahetus (autori valduses). 16.03.2009
[142] 1-11-13715

saamise eesmärgil andmete ebaseadusliku sisestamise ja andmetöötlusprotsessi ebaseadusliku sekkumise.[143]

Kiirlaenude vormistamisel algab katse kiirlaenu taotluse vormistamise ning ärasaatmise hetkest, st isik on teinud kõik endast oleneva, et tagajärg ehk laenusumma saabuks ning kuritegu on lõpule viidud laenuraha laekumisega arvelduskontole.

Viru Maakohus leidis samuti, et A.K ja A.S panid toime arvutikelmuse, kuna A.K, saades A.S-lt V.V nimele vormistatud pangakontot puudutavad dokumendid, mis sisaldasid internetipanka ligipääsu võimaldavat püsiparooli, kasutajatunnust ja internetipanga paroole, sisestas A.K V.V kui kontoomaniku nimel ja viimase teadmata saadud andmed arvutisüsteemi, sekkudes sel moel ebaseaduslikult andmetöötlusprotsessi selle lubamatu käivitamise kaudu, võimaldades endale virtuaalsesse maksekeskkonda– internetipanka-sisenemist ja V.V arvelduskonto kasutamist. Sel moel taotles A.K V.V teadmata ja nõusolekuta tema nimele kiirlaenu erinevatest laenufirmadest. Peale taotluste rahuldamist ning kogu laenusumma laekumist V.V arvelduskontole, kandis A.K osa rahast kokkuleppel A.S-ga nö teenustasuna J.L pangakontole, mille A.K seejärel tema kasutuses olnud deebetkaardi abil sularahana välja võttis ja omastas, ülejäänud raha võttis A.S seejärel tema kasutuses olnud V.V deebetkaardi abil sularahana välja ja omastas.[144]

A.K mõisteti süüdi arvutikelmuses, mis seisnes selles, et tema registreeris varalise kasu saamise eesmärgil V.A nõusolekuta SMS Laen veebilehel V.A kasutajaks ning sisenedes ebaseaduslikult V.A nimele väljastatud internetipanga paroolikaardi paroolide sisestamise teel internetipanga maksekeskkonda, millega autentis SMS Laen veebilehtedel registreeritud V.A kasutajaisiku, avades kannatanu nimele laenukonto, sekkudes sellega ebaseaduslikult panga andmetöötlusprotsessi ning seejärel taotles V.A nimele läbi interneti keskkonna kiirlaenu, mis laekus V.A arvelduskontole, mille A.K omastas. Kohus leidis, et seega pani A.K toime ebaseaduslikult andmetöötlusprotsessi sekkumise teel, andmete ebaseadusliku sisestamisega ja mõjutades andmete töötlemise tulemust, varalise kasu saamise, s.o KarS § 213 lg 1 järgi kvalifitseeritava kuriteo.[145]

Toodud kaasuste puhul tuleks esitada küsimus, kas laenu väljastab laenufirmade arvutiprogramm automaatselt või kontrollib laenusaaja maksevõime üle inimene ning laenu

[143] 1-11-13118
[144] 1-09-9735
[145] 1-11-9551

väljastab inimene. Viimasel juhul oleks küsitav nimetatud kaasuste kvalifitseerimine arvutikelmusena., kuigi andmed on arvutiprogrammi ebaseaduslikult sisestatud ning varaline kasu saadud.

Viru Maakohus on kelmusena kvalifitseerinud kuriteo, kui kiirlaenu taotlus on esitatud mobiiltelefoni teel.[146] Samuti on Harju Maakohus kelmusena kvalifitseerinud juhtumi, kus isik, kasutades ära tema käes olnud A.T internetipanga kasutajatunnust ja paroole, lõi varalise kasu saamise eesmärgil teadvalt ebaõige ettekujutuse laenuvõtja isikust erinevatele kiirlaene pakkuvatele firmadele.[147] Seega petetakse inimest.

3.7 Muud arvutikelmusena kvalifitseeritavad juhtumid

Arvutikelmusena kvalifitseeritakse ka ebaseaduslik tuludeklaratsiooni esitamine, ebaseaduslik taksofoni kasutamine ja ebaseaduslik kinkekaardi kasutamine.

3.7.1. Ebaseaduslik tuludeklaratsiooni esitamine

Arvutikelmusena kvalifitseeritakse ka Maksu- ja Tolliametile ebaseaduslik tuludeklaratsiooni esitamine elektroonilisel teel.

M.J esitas varalise kasu saamise eesmärgil K.J nimelt elektrooniliselt tuludeklaratsiooni Maksu- ja Tolliametile, kasutades K.J teadmata ja nõusolekuta viimase nimele välja antud internetipanga paroolikaarti ja püsiparooli, märkides enammakstud tulumaksu tagastamiseks K.J konto numbri, mida K.J ise ei kasutanud. Enammakstud tulumaks kanti K.J kontole, mille M.J kandis edasi enda isiklikule kontole, saades oma tegevusega varalist kasu.[148] Sellise tegevusega sisestas M.J andmed (andmed tulude ja kulude kohta) arvutiprogrammi (elektrooniline tuludeklaratsiooni vorm) ebaseaduslikult, millega sai varalist kasu. Samas võib siin paralleele tõmmata kiirlaenu taotlemise kaasustega. Arvatavasti vaatab tulumaksu tagastamise läbi maksuametnik ning vaevalt, et arvutiprogramm tagastab automaatselt enammakstud tulumaksu. Seega tuleks taolised juhtumid kvalifitseerida kelmusena.

3.7.2. Ebaseaduslik taksofoni kasutamine

Arvutikelmusena kvalifitseeriti ka juhtumid, kus isikud, kasutades telefonivõtit, mis võimaldas ligipääsu taksofoni ühenduskappi, ühendasid kaasas olnud juhtmed ja telefonitoru mitmel korral AS Eesti Telefonile kuuluva taksofoni ühendusskeemi ning helistasid

[146] 1-07-15253
[147] 1-09-8563
[148] 1-08-6581

erinevatele numbritele, millega isikud sekkusid AS Eesti Telefoni andmetöötlusprotsessi ning mis võimaldas neil tasuta helistada, tekitades sellega AS Eesti Telefonile varalist kahju.[149]

Taolise kuriteo toimepanemises süüdistati J.N-i, kuna ta kasutas raadiotelefoni Panasonic KX-T9080BX telefonikõnede teostamiseks erinevate abonentidega, teades, et nimetatud telefon on ühendatud AS Eesti Telefoni taksofoniga. Süstemaatiliselt telefoni kasutades sai ta sellega võimaluse tasuta kõneaja kasutamiseks AS Eesti Telefoni telefonisüsteemis. Kokku teostas ta 5876 telefonikõnet kestvusega kokku 173 tundi 18 minutit kogumaksumusega 70972,83 krooni. Sellise tegevusega pani J.N toime sekkumise AS Eesti Telefon andmetöötlusprotsessi, mis mõjutas andmete töötlemise tulemust ja põhjustas AS-le Eesti Telefon varalist kahju.[150]

Selliseid kuritegusid ei pea kohtud enam lahendama, kuna 01.12.2010 sulges Elion (endise nimega AS Eesti Telefon) oma taksofonid vähese kasutamise tõttu.[151] Kaaluda võiks kvalifitseerimist ka arvutisüsteemi ebaseadusliku kasutamisena, kuid antud juhtumitel oli eesmärgiks varalise kasu saamine, seega on siiski pigem tegemist arvutikelmusega.

3.7.3 Ebaseaduslik kinkekaardi kasutamine

USA Apellatsioonikohus jättis süüdimõistmise jõusse Timothy Truong´i kohta, kuna ta omas autoriseerimata juurdepääsuseadmeid pettuse eesmärgil. Kohus leidis, et juurdepääsuseadmeteks on varastatud jaemüügi kinkekaardid. Sellise kaardi ostja laeb kaardile raha ning aktiveerib elektrooniliselt selle kasutamise. Aktiveeritud kaarti saab kasutada kaupade ostmiseks samas jaemüügi kohas, kust kaart osteti. Jaemüügi kinkekaartidel on unikaalne identifitseerimisnumber ehk PIN-kood, mida paljudel juhtudel on võimalik näha, kui PIN-koodi peal olev värv maha kraapida. Tarbija saab kasutada PIN-koodi, et jälgida kui palju raha on kaardile jäänud. T.T varastas kinkekaardid kauplusest. Spetsiaalse varustusega kogus ta informatsiooni, mis on salvestatud igale kinkekaardile. Samuti kraapis ta maha värvi, mis paljastas kaardi PIN-koodi. Ta tegi kaartidest duplikaadid ning viis need kauplusesse, kust ta kinkekaardid varastas, jättes originaalid endale. Seejärel jälgis ta PIN-koodi kaudu, kas kinkekaardi duplikaadid on müüdud ning kui palju raha sinna laetud on. Kui keegi ostis duplikaadi ära ning laadis sellele raha ja aktiveeris kaardi, kasutas T.T originaalkaarti, ostes sellega kaupu või vahetas raha vastu. Läbiotsimisel leidis politsei T.T sõidukist peaaegu 4000 kinkekaarti üheksast erinevast kauplusest. Süüdistus esitati U.S.Code § 1029(a)(3) alusel, mis

[149] 1/2-2842/01
[150] 1/1-1258/02
[151] R.Sulbi. Alates detsembrist kaovad Eestist taksofonid.

keelab juurdepääsuseadmete omamise. Juurdepääsuseadmeid tõlgendatakse ka kui juurdepääsu kontole.[152]

Eestis oleks selline tegevus kvalifitseeritav arvutikelmusena ning maksevahendi võltsimisena. Ostmisel kasutas ta originaalkaarte ning neid võib võrrelda võõra pangakaardiga tasumisega. Kuna kaardil oli PIN-kood, siis võib eeldada, et tasumisel pidi ta PIN-koodi sisestama makseterminali, seega sisestas andmed ebaseaduslikult arvutiprogrammi, millega sai varalist kasu.

Samas võib tegemist olla ka kelmusega, kuna T.T pettis klienti, et see kannaks raha originaalkaardile, mis oli T.T käes. Poes makstes kasutas ta originaalkaarti, milline tegevus oleks seaduslik, kui ta oleks need ausal teel ostnud. Seega lõi ta kliendile vale ettekujutuse, et klient kannab raha oma kaardile, kuid tegelikult kandis raha T.T kaardile.

3.8 Arvutikelmuse seotus rahapesu kuriteoga

Rahapesu mõiste annab Rahapesu ja terrorismi rahastamise tõkestamise seadus, mille kohaselt on rahapesu 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.[153]

Paljud kohtud on mõistnud isikuid süüdi arvutikelmuse toimepanemisele lisaks ka rahapesus. Harju Maakohus mõistis rahapesu kuriteos süüdi I.B, kes grupis koos eeluurimisel tuvastamata isikuga teostas pangaülekandeid, et varjata tuvastamata isiku poolt arvutikelmuse tulemusel saadud 8100 krooni tegelikku omanikku, vara asukohta ja ebaseaduslikku päritolu. I.B leppis suhtlusprogrammis ICQ kokku tuvastamata isikuga, et leiab variisiku, kelle kontole raha kanda, mille I.B sularahas välja võtab ning e-raha konto kaudu seni tuvastamata isikule saadab. I.B veenis A.S-i, et viimane annaks oma arvelduskonto numbri ning lubaks sellele ülekande teha. Tuvastamata isik sekkus täpselt tuvastamata viisil T.N-i ja P.J-i poolt internetipanga keskkonnas alustatud andmetöötlusprotsessi (ülekandesse) ning teostas konto omanike teadmata ja loata 6000-kroonise ja 2100-kroonise ülekande A.S-i kontole. Rahaülekannete teostamise järgselt informeeris tuvastamata isik suhtlusportaali MSN vahendusel I.B-d, et see A.S arvel oleva raha sularahaautomaadist välja võtaks. Sularaha

[152] U.S. v. Truong 587 F.3d 1049
[153] Rahapesu ja terrorismi rahastamise tõkestamise seadus § 4

väljavõtmine ning ülekandmine A.S kontolt ebaõnnestus, kuna pank oli A.S konto kasutamise blokeerinud. Sama otsuse kohaselt süüdistati I.B-d lisaks kiirlaenude vormistamisel teise isiku nimele rahapesus, kuna kiirlaenu summad laekusid I.B kasutuses olevatele A.T kontodele, mille I.B edasi kandis A.N ja M.P kontodele. A.N ja M.P võtsid I.B korraldusel oma kontodelt laekunud rahad sularahaautomaatidest välja ning andsid I.B-le üle. Kohus leidis, et sellise tegevuse eesmärk oli varjata kiirlaenufirmadelt kelmuse teel saadud raha ebaseaduslikku päritolu ja asukohta ning kontodele ülekantud summade pangaautomaadist väljavõtmine on varalise nõudena käsitletava summa muundamine sularahaks.[154]

Riigikohus leidis, et: „rahapesuks ei saa kvalifitseerida tegusid, kui süüdistatav kannab kannatanute raha kolmandate isikute arvetele või laseb kannatanutel endil raha kanda kolmandate isikute arvetele, kuna eelkuritegu, st kelmus või arvutikelmus ei ole rahapesu süüdistusest eristatav. T.P 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. 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.“[155]

„Rahapesu koosseisus kirjeldatud käitumise eest karistusõigusliku vastutuse kehtestamisel on seadusandja eesmärgiks seadnud riigi rahandus- ja majandussüsteemi kaitsmise kuritegeliku varaga manipuleerimise eest, mitte aga igasuguse kuritegelikul teel saadud vara kasutamise kriminaliseerimise, mille käigus jääb vara tegelik päritolu varjatuks.“[156]

Lähtudes Riigikohtu otsustest, ei tuleks üldjuhul arvutikelmuse koosseisu kõrval isikuid süüdistada rahapesu toimepanemises, kuna eesmärgiks on enamasti saada pettuse teel raha, mitte varjata, kust see saadud on või kes on selle raha omanik.

[154] 1-09-8563
[155] 3-1-1-21-11 p 12,13,14
[156] 3-1-1- 85-11 p 44

3.9 Arvutikelmuse eristamine arvutiandmetesse sekkumise koosseisust

Arvutiandmetesse sekkumise objektiivse koosseisu moodustab arvutisüsteemis olevate andmete või programmi ebaseaduslik muutmine, kustutamine, rikkumine või sulustamine, samuti arvutisüsteemi andmete või programmi ebaseaduslik sisestamine. Raskendava koosseisu moodustab kuritegu elutähtsa valdkonna arvutisüsteemi vastu või kui sellega on tekitatud oluline kahju.[157]

Arvutiandmetesse sekkumise poolt ohustatav õigushüve on arvutisüsteemi omaniku ja õiguspärase valdaja õigus vallata, kasutada ja käsutada arvutisüsteemi. Koosseisutüübilt on tegemist formaalse kuriteokoosseisuga. Teo lõpuleviimiseks ei ole isegi vajalik, et arvutisüsteemi töö saaks reaalselt häiritud.[158] Minimaalset sekkumist arvutisüsteemi töösse ei olegi võib-olla iga kord põhjendatud kohe kuriteona karistada, eriti kui muudetakse ebaolulisi andmeid arvutisüsteemis.

T.T mõisteti süüdi selles, et tema kõrvaldas arvuti kaudu Venemaa erinevate erakondade poolt korraldatava konverentsi organisaatorite poolt konverentsi kohta informatsiooni edastamiseks AS Eesti Telefoni arvutisüsteemis loodud hot.ee konto russconference kaitsevahendid, arvates ära salaküsimuse vastuse. Saades teada koodi, asendas T.T selle teisega ning sisenes seda koodi kasutades ebaseaduslikult AS Eesti Telefon arvutisüsteemi. Seejärel kustutas ta arvuti kõvakettal kontole russconference eraldatud osas asunud 80 faili, eesmärgiga muuta vene erakondade poolt korraldatava konverentsi organisaatorite poolt internetis aadressile www.hot.ee/russconference loodud konverentsi tutvustavad materjalid loetamatuks. Oma teoga pani T.T toime arvutis olevate andmete ebaseadusliku kustutamise ning arvutisüsteemi ebaseadusliku kasutamise kaitsevahendi kõrvaldamise teel.[159] Kohtuotsusest ei selgu, miks T.T materjalid kustutas, kui tema eesmärgiks oli muuta need loetamatuks. Kui materjalid muudeti loetamatuks, siis tuleks kasutada terminit muutmine. Võib-olla oleks mõistlik, et isik saaks süüdistuse ühe paragrahvi alusel, kaitsevahendi kõrvaldamine neelduks lõpptegevuses ehk andmete kustutamises. Kuriteo toimepanemise eesmärgiks oli andmete kustutamine, mitte lihtsalt parooli kõrvaldmisega siseneda võõrasse arvutisse.

Tartu Maakohtus mõisteti Z.T süüdi KarS § 206 lg 1 järgi, kuna tema kasutas ebaseaduslikult J.S isiku- ja pangakontoandmeid, paroolikaarti, kasutajatunnust ja salasõna ning võttis J.S-i nimel kiirlaenu. Laenusumma laekudes J.S-i kontole, kandis Z.T selle edasi enda

[157] Karistusseadustik § 206
[158] Karistusseadustik. Komm. vln. § 206 komm 1.1
[159] 1/2-1019/02

pangakontole. Z.T tasus J.S-i nimel võetud laenu tähtaegselt.[160] Siin on põhjendatud Z.T tegevuse kvalifitseerimine arvutiandmetesse sekkumisena, kuna ta ei põhjustanud oma tegevusega ühtegi tagajärge (ta ei saanud varalist kasu ning laenufirma ei saanud varalist kahju, kuna Z.T maksis laenu õigeaegselt tagasi). Päris seaduslik tema tegevus aga ei olnud, kuna ta sisestas J.S-i andmed ebaseaduslikult arvutiprogrammi. Kui ta oleks jätnud laenu õigeaegselt tagastamata, ei tuleks tema tegevust kvalifitseerida arvutikelmusena, vaid kelmusena, kui laenutaotluse vaatab läbi ning laenu väljastab inimene, st petetakse inimest.

E.I mõisteti süüdi KarS § 206 lg 1 järgi, kuna tema, olles saanud ebaseaduslikult A.V isikutunnistuse ning isiku tuvastamise ja digiallkirja paroolid, esitas A.V teadmata Tartu Maakohtu registriosakonnale elektrooniliselt kandeavalduse OÜ L äriregistrisse kandmise kohta ning OÜ L osaniku otsuse A.V OÜ L juhatuse liikmeks määramise kohta. Sellega pani E.I toime andmete ebaseadusliku sisestamise arvutisüsteemi.[161] Antud kaasuses on sisestatud andmed arvutiprogrammi ebaseaduslikult, ilma varalise kasu saamise eesmärgita ning süüdistatavale omistatud koosseis seega põhjendatud.

V.N mõisteti süüdi KarS § 206 lg 1 ning § 214 lg 1 alusel, kuna tema kopeeris ja seejärel kustutas ebaseaduslikult arvuti- ja internetiühenduse kasutamise teel Diffusio OÜ serveris kahe kõvaketta sisu, millel olid OÜ tööks vajalikud andmed ja erinevad veebimajutuses olevad kodulehed. Andmete tagastamise eest nõudis V.N Diffusio OÜ-lt 500 USD, lubades raha mitte saamisel andmed hävitada. Sellise tegevusega põhjustas V.N Diffusio OÜ-le olulist kahju.[162] Andmete kopeerimine täidab samuti vajalikud koosseisu tunnused, kuna kopeerimiseks on vaja andmeid sisestada.
Antud kaasuses tuleks põhirõhk asetada väljapressimisele, kuna V.N-i eesmärgiks oli varalist kasu saada.

Arvutikelmuse ja arvutiandmetesse sekkumise koosseisudega kaitstakse erinevaid õigushüvesid. Arvutikelmuse puhul on kaitstavaks õigushüveks vara ning andmetöötlusprosessi sekkumise teoga peab süüdlane saama varalist kasu. Arvutiandmetesse sekkumise koosseisuga kaitstakse õigusi (arvutisüsteemi omaniku ja õiguspärase valdaja õigus vallata, kasutada ja käsutada arvutisüsteemi). Mingi tagajärje saabumist ega varalise kasu või kahju saamist ei ole nõutud, piisab sekkumisest.[163]

[160] 1-11-10794
[161] 1-11-13181
[162] 1-06-5550
[163] Karistusseadustik. Komm.vln. § 206 ja § 213

3.10 Arvutikelmuse eristamine arvutisüsteemi toimimise takistamise koosseisust

Arvutisüsteemi toimimise takistamise objektiivne koosseis on täidetud kui arvutisüsteemi toimimist häiritakse ebaseaduslikult või takistatakse andmete sisestamise, edastamise, kustutamise, rikkumise, muutmise või sulustamise teel.[164] Näiteks sidekaablite, arvutisüsteemide füüsiline rikkumine või hävitamine selle paragrahvi alla ei lähe, vaid on kvalifitseeritav KarS § 203-na.[165]

"Arvutisüsteemi toimimise häirimine on arvutisüsteemi funktsioonide täitmise halvendamine, eelkõige arvutisüsteemi poolt ülesannete täitmise aeglustamine. Arvutisüsteemi toimimise takistamine on arvutisüsteemi funktsioonide täitmise vähemalt ajutise lakkamise põhjustamine".[166]

"Andmete edastamine tähendab siin igasuguste infosüsteemis töötlemiseks sobivas vormis faktide, teabe või mõistete ühest punktist teise edastamine, tavaliselt telekommunikatsiooniühenduses. Siia alla mahuvad kõikvõimalikud teenusetõkkeründed nagu Dos (Denial of Service), DDos (Distributed Denial of Service- hajutatud teenusetõkestusrünnakud ehk intensiivsete päringute saatmine rünnatavale serverile[167]), samuti arvutisüsteemi töö häirimine e-kirjade masspostituse teel ehk spamming".[168]

Raskendavaks koosseisuks on kui sellega tekitatakse oluline kahju või takistatakse elutähtsa valdkonna arvutisüsteemi tööd või avalike teenuste osutamist.[169]

J.K kõrvaldas arvutisüsteemile juurdepääsuks kaitsevahendi ning kasutas ilma loata Rapla Maavalitsuse arvutivõrku sellega, et analüüsis oma koduarvutist arvutivõrgu turvalisust programmiga Nessus, saades interneti kaudu läbi tulemüüri ligipääsu maavalitsuse arvutivõrku, mis sisaldab asutusesiseseks kasutamiseks tunnistatud andmeid. Isikut süüdistati KarS § 217 lg 2 p 2 alusel, kuid mõisteti õigeks.[170]

Lisaks saatis J.K maavalitsuse elektronposti aadressile suure arvu mittevajalikke elektronkirju koos manustega, mille tagajärjel ummistusid töötajate kirjakastid ja takistati elektronkirjade vahetamist, saatmist ning vastuvõtmist. Maakohus muutis selle süüdistuse KarS § 208-st (arvutiviiruse levitamine) § 207-ks. Riigikohus nõustus, et elektronkirjade masspostitus häirib

[164] Karistusseadustik § 207
[165] Karistusseadustik. Komm.vln. § 207
[166] Karistusseadustik. Komm.vln. § 207 komm 2.2
[167] 1-09-3576
[168] Karistusseadustik. Komm.vln. § 207 komm 2.5
[169] Karistusseadustik § 207
[170] 3-1-1-85-08

ja takistab arvutisüsteemi tavapärast toimimist ning tegemist ei ole arvutiviiruse levitamisega, vaid KarS § 207-s sätestatud kuriteoga.[171]

A.B teostas oma elukohas asunud arvutist DDoS rünnakud AS S serverite, M AS veebiserveri ja D portaali vastu. Rünnakud seisnesid selles, et A.B sai kaughaldustarkvara Remote Administration kasutades ebaseaduslikult kontakti 2374 unikaalse IP aadressiga arvutiga ning omandas kontrolli nende üle, paigaldades ülevõetud arvutitesse rünnaku sihtmärgiga programmi, seejärel võtsid kontrolli all olevad ründavad arvutid ühendust AS S serverite, M AS veebiserveri ja D portaaliga, edastades neile massiliselt ebakorrektseid päringuid, saates rünnaku aadressile TCP-SYN pakette, millega üks ründav arvuti edastas 5000-10000 paketti sekundis ja rünnak hõivas keskmiselt 20-40 megabitti sekundis. Sellise tegevuse tagajärjeks oli veebiserveriga ühenduse rikkumine andmesideühenduse kiiruse lubamatu vähenemise ja arvutivõrgu ühenduse katkemise tõttu ning arvutiandmetele juurdepääsu tõkestamine.[172]
Lisaks käivitas A.B kaughaldustarkvara Radmin abil kontrolli üle võetud arvutite serverite kaudu masspostituse mitme asutuse e-posti serverite vastu, mis seisnes suurel hulgal e-kirjade edastamises ja arvutiandmete sulustamises, millega häiris ja takistas serverite võrguühendust ning arvutisüsteemide toimimist.[173]
Oma tegevusega põhjustas A.B kokku kahju 6 560 311,30 krooni.[174]
A.B häiris ja takistas oma tegevusega arvutisüsteemi toimimist andmete edastamisega (edastades massilisi päringuid; saates TCP-SYN pakette, saates masspostitusi) ning sulustamisega (saates masspostitusi).

Arvutikelmuse ja arvutisüsteemi toimimise takistamisel tehakse vahet kaitstava õigushüve järgi. Ühel juhul kaitstakse vara, teisel juhul õiguspärase kasutaja õiguspärast ootust arvutisüsteemide takistamatuks kasutamiseks.

3.11 Arvutikelmuse eristamine arvutisüsteemi ebaseadusliku kasutamise koosseisust

Arvutisüsteemi ebaseadusliku kasutamisega on tegemist kui arvutisüsteemile luuakse ebaseaduslikult juurdepääs koodi, salasõna või muu kaitsevahendi kõrvaldamise või vältimise teel. Raskendavaks koosseisu tunnuseks on: olulise kahju tekitamine; kui on kasutatud

[171] 3-1-1-85-08
[172] 1-09-3576
[173] 1-09-3576
[174] 1-09-3576

riigisaladust, salastatud välisteavet või ainult ametialaseks kasutamiseks ettenähtud andmeid sisaldavat arvutisüsteemi; kui on juurde pääsetud elutähtsa valdkonna arvutisüsteemile. [175]

Kaitstavaks õigushüveks on arvutisüsteemi omaniku huvi selle takistamatuks kasutamiseks ning võimaluseks saada selle teiste isikute poolt kasutamise eest hüvitust.[176]

„Koosseisutüübilt on tegemist formaalse ja spetsiifilise teokirjeldusega kuriteokoosseisuga“.[177]

Objektiivse koosseisu moodustab arvutisüsteemile ebaseadusliku juurdepääsu saamine. Juurdepääs võib seisneda näiteks andmete või programmide edastamises, töötlemises või säilitamises antud arvutisüsteemis.[178]

Juurdepääs arvutisüsteemile on ebaseaduslik siis, kui kasutajal ei ole selleks luba. Piiranguteks võivad olla salasõna või muu kaitsevahendi kasutamine, samuti selgelt väljendatud kasutamise keeld. Ebaseaduslik juurdepääs on karistatav vaid siis, kui see toimub koodi, salasõna või muu kaitsevahendi kõrvaldamise või vältimise teel.[179] Karistatavad on nii sisenemine koodi või salasõnaga kaitstud arvutisse, arvutisüsteemi või –võrku, kui kood murtakse selleks kasutatava programmi abil ning arvuti, arvutisüsteemi või -võrgu kasutamine seetõttu, et kood on sattunud isiku kätte, kellele seda õiguspäraselt ei ole antud.[180]

Koosseis on täidetud kui isik saab endale koodi teadmisega, et sellega pääseb ta võõrasse arvutisse ning et selline tegevus rikub teise isiku õigusi, kuna kood või salasõna paigaldati omaniku poolt selleks, et kaitsta oma vara ja takistada teiste isikute juurdepääsu varale. Kood või salasõna on vaadeldav tõkkena, mille isik peab kõrvaldama, et omandada ligipääs arvutile, arvutisüsteemile või –võrgule.[181]

Tegu on lõpule viidud hetkest, kui sissetungija saab pärast kaitsevahendi kõrvaldamist või selle vältimist esimesed andmed sissemurtud arvutisüsteemist, sisestab sinna uusi andmeid või käivitab selles mõne programmi.[182]

Kood ja salasõna tähendavad andmeid, mida on vaja kasutaja kasutusõiguse tuvastamiseks, seega andmeid, mida peaks teadma ainult kasutusõigusega isik. Muu kaitsevahend võib olla igasugune muu tark- ja riistvaraline lahendus, mis on kasutatav kasutusõiguse tuvastamiseks, näiteks sõrmejälje, hääle või silma võrkkesta järgi isiku tuvastamine või ka

[175] Karistusseadustik § 217
[176] Karistusseadustik. Komm.vln. § 217 komm 1.1
[177] Karistusseadustik. Komm.vln. § 217 komm 1.2
[178] Karistusseadustik. Komm.vln. § 217 komm 2
[179] Karistusseadustik. Komm.vln. § 217 komm 3, 4.1
[180] T.Ploom. Arvutikuritegude kvalifitseerimine. Juridica VIII 2003, lk 577
[181] T.Ploom. Arvutikuritegude kvalifitseerimine. Juridica VIII 2003, lk 577
[182] Karistusseadustik. Komm.vln. § 217 komm 4.1

infotehnoloogiaväline vahend, näiteks füüsiline lukustamine. Kaitsevahendi kõrvaldamist tõlgendab kohus laialt.[183]

Arvutihulkurlus, kus häkker kasutab arvutit, arvutisüsteemi või –võrku, mis ei ole koodi või salasõnaga kaitstud, ei ole karistusseadustiku järgi karistatav.[184]

Niivõrd oluline ei ole mitte see, millisel viisil isik koodi, salasõna või muu takistuse kõrvaldas, kuivõrd asjaolu, et see oli tema tegevuse eesmärgiks ning ta teadis, et arvuti, arvutisüsteemi või –võrgu kasutamine on ebaseaduslik.[185]

A.M tunnistati arvutisüsteemi ebaseaduslikus kasutamises süüdi, kuna ta kasutas enda töökohas Eesti Liikluskindlustuse Fondi arvutisüsteemi, mis oli ainult ametialaseks kasutamiseks. Andmebaasi sisenemiseks kõrvaldas ta arvutisüsteemi kaitsevahendi, sisestades kasutajatunnuse ja parooli. Peale sisenemist Eesti Liikluskindlustuse Fondi andmebaasi, vahetas A.M ära administraatori õigustega kasutaja parooli, mille tulemusena oli andmebaasi võimalik kasutada volitamata isikutel ja tungida seeläbi delikaatseid isikuandmeid sisaldavasse arvutisse ja andmekogusse. Sellise tegevusega pani A.M toime ainult ametialaseks kasutamiseks ettenähtud andmeid sisaldava arvutisüsteemi ebaseadusliku kasutamise selle kaitsevahendi kõrvaldamise teel.[186] Otsusest ei selgu, kas A.M-l oli õigus andmebaasi kasutada ametialasel otstarbel (ta küll töötas seal, kuid kas võis kasutada ka andmebaasi). Otsusest nähtub, et A.M ise seda andmebaasi ei kasutanudki, vaid seda võisid kasutada (otsusest ei nähtu, kas ka kasutasid) volitama isikud. Sellisel juhul seisnes A.M-i tegevus administraatori parooli vahetamises, mitte ametialase andmebaasi kasutamises.

C.A-d süüdistati selles, et tema kasutas ebaseaduslikult Tallinna Kunstigümnaasiumi arvutisüsteemi sellega, et kasutades ADSL Light internetiühendust, sisenes Kunstigümnaasiumi serverisse, milleks kõrvaldas kooli arvutisüsteemi kaitsevahendi, proovides sisestada erinevaid kasutajatunnuseid, mille tulemusel leidis sobiva kasutajatunnuse.[187] Mis oli tema tegevuse eesmärgiks ning kas ta arvutisüsteemi ka reaalselt kasutas või kõrvaldas vaid parooli, ei selgu. Juurdepääsemine tähendab ka kasutamist, kuna juurdepääsemisega on andmeid sisestatud ning seega ka arvutisüsteemi kasutatud.

[183] Karistusseadustik. Komm.vln. § 217 komm 4.2
[184] T.Ploom. Arvutikuritegude kvalifitseerimine. Juridica VIII 2003, lk 577
[185] T.Ploom. Arvutikuritegude kvalifitseerimine. Juridica VIII 2003, lk 578
[186] 1/2-2690/02
[187] 1/1-2558/02

Järgnevast Tartu Maakohtu Valga kohtumaja otsusest on raske päris täpselt aru saada. „Kriminaalasjas süüdistatakse Janek Juus`i selles, et tema, võttis oma elukaaslase isa X elukohast, X maakonnas X vallas X külas X talu, toast laua sahtlist Hansapanga hansanet-i pangakaardi koos kaardi küljes olnud kollasele kleeppaberile kirjutatud salasõnaga, sooviga omastada X arvelt raha ning koodikaarti ja salasõna kasutades kandis internetipanga kaudu X arveldusarvelt Hansapangas 14.veebruaril 2008.aastal X arveldusarvele Hansapangas 10000 krooni, mille viimane võttis samal päeval välja ja andis X ning 21.veebruaril 2008.aastal kandis X arveldusarvele Hansapangas 6000 krooni, mille viimane võttis samal päeval välja ja andis X, kes mõlemad nimetatud summad omastas, pannes oma käitumisega toime arvutikelmuse. Varalise kasu saamisega, andmete ebaseadusliku sisestamise teel, kui sellega on mõjutatud andmete töötlemise tulemust, pani Janek Juus toime KarS § 217 lg 1 järgi kvalifitseeritava kuriteo.“[188]

Küsimusi tekitab, mille täpselt J.J elukaaslase isa lauasahtlist võttis- kas pangakaardi ja PIN-koodi või internetipanga koodikaardi, kasutajatunnuse ja salasõna (ilmselt viimase, kuna ülekanne tehti internetipangas), kes tegi ülekande ning kellele, kes raha välja võttis ning kellele üle kandis, kuna kõik isikud on asendatud X-idega. Lisaks on konflikt asjaolude kirjelduses ning omistatud paragrahvis- J.J pani oma käitumisega toime arvutikelmuse, kuid kvalifitseeritud on KarS § 217-na.

Kuna antud kaasuses on andmed sisestatud küll ebaseaduslikult, kuid saadud on ka varaline kasu, võiks nimetatud kuriteo kvalifitseerida arvutikelmusena.

R.P mõisteti süüdi arvutisüsteemi ebaseaduslikus kasutamises koodi ja salasõna kõrvaldamise teel, kuna tema, olles saanud eelnevalt H.P teadmata enda valdusesse H.P internetipanga kasutajanime, salasõna ja koodi, sisestas need avalikus internetipunktis ebaseaduslikult ning tegi ülekande H.P pangakontolt enda pangakontole.[189]

Kohtuotsuses ei ole küll märgitud, kuhu R.P andmed ebaseaduslikult sisestas, kuid eeldada võib, et internetipanka sisenemisel.

„Prokuröri selgituse kohaselt vältis R.P enda kasutajanime, salasõna ja koodi kasutamist, kasutas ebaseaduslikult H.P internetipanga kasutajanime, salasõna ja koodi.“[190]

Kuna siin on arvutiandmetesse sekkumise eesmärgiks varalise kasu saamine, võiks kvalifitseerida arvutikelmusena.

[188] 1-09-8016
[189] 1-08-4059
[190] 1-08-4059

V.K- le oli seoses tööülesannetega antud ligipääs tööandja kliendihaldustarkvarale, kuid töölepingu lõppedes ekslikult aktiivseks jäetud. Peale töösuhte lõppu sisenes V.K tööandja serverisse, kasutades talle eelnevalt antud kasutajakontot ja parooli, kuid omamata serverisse sisenemiseks õigust, laadis serverisse php programmeerimiskeele faili „tmpxxx.php“, eesmärgiga võimaldada endale ligipääs tööandja serverisse ajaks, mil tema kasutajakonto ja parool enam aktiivne ei ole. Peale faili paigaldamist sisenes V.K oma elukoha arvutites kokku 138 korral oma endise tööandja serverisse üles laetud faili juurde, mis võimaldas tal serveris asuva kliendihaldustarkvara andmebaasi sisenemise kaitsevahenditest möödudes, kasutades seega serverit ja sealset tarkvara, omamata selleks õigustatud isiku nõusolekut. Sellise tegevusega pani V.K toime arvutisüsteemi ebaseadusliku kasutamise kaitsevahendi kõrvaldamise teel.[191]

Nagu nähtub eespool käsitletud kaasustest on probleeme arvutikelmuse ja arvutisüsteemi ebaseaduslike kasutamiste koosseisudel vahet tegemisel. Nagu teistegi käesolevas töös käsitletud arvutikuritegude koosseisude puhul, tuleb vahet teha, kas isiku tegevuse eesmärgiks oli varalise kasu saamine. Oluline ei ole, kas ta hiljem saab sellest tegevusest mingit kasu (nt viimase kaasuse puhul võib oletada, et V.K tahtis juurdepääsu kliendihaldustarkvara andmebaasile seetõttu, et kasutada seal olevat infot enda tarbeks, seega saada mingit kasu).

[191] 1-07-1760

Kokkuvõte

Arvutikelmuste kvalifitseerimisel puudub menetlejatel ühtne seisukoht. Põhilised piiritlemisprobleemid tekivad arvutikelmuste eristamisel omastamise, varguse ja kelmuse koosseisust. Probleeme on ka arvutikelmuste eristamisel teistetest arvutikuritegudest.

Arvutikelmusena kvalifitseeritakse järgmised ebaseaduslikud tegevused: internetipangas ülekande tegemine; pangakaardi, krediitkaardi, kütusekaardi, kinkekaardi kasutamine; mobiiltelefoni SIM-kaardi kasutamine; taksofoni kasutamine; tuludeklaratsiooni esitamine.

Internetipangas ebaseadusliku ülekande puhul tekivad piiritlemisprobleemid arvutikelmuse ja omastamise koosseisu vahel. Välja tuleb selgitada, kuidas süüdistatav sai ligipääsu võõrale pangakontole. Kui kannatanu andis süüdistatavale internetipanga juurdepääsu mingite toimingute tegemiseks, kuid süüdistatav ületas volitusepiire ja tegi ülekande ka enda või kolmanda isiku kasuks, tuleb kuritegu kvalifitseerida omastamisena. Samuti kui süüdistataval oli pangakontole juurdepääs oma tööülesannete tõttu, kuid tema kasutab tööandja pangakontot muul otstarbel, kui tööülesanneteks, näiteks tehes ülekande ka enda pangakontole, tuleb selline tegevus kvalifitseerida omastamisena.
Kui süüdistatav sai ligipääsu võõrale pangakontole kannatanu tahte vastaselt, kasutas paroolide saamiseks mingit programmi, leidis või varastas juurdepääsu koodid, tuleb tema tegevus kvalifitseerida arvutikelmusena.
Ebaseaduslikuks internetipanga ülekandeks on kannatanu tahte vastaselt teostatud: ülekanne kannatanu pangakontolt süüdistatava või kolmanda isiku pangakontole, olenemata sellest, kas rahasumma võetakse hiljem sularahaautomaadist välja või mitte; ülekanne teenuse või kaupade ostmiseks, sh kõneaja laadimine mobiiltelefonile; püsi- või otsekorralduse sõlmimine, millega võetakse raha võõralt pangaarvelt.

Pangakaardi ebaseadusliku kasutamise korral tekivad piiritlemisprobleemid arvutikelmuse, omastamise, varguse ja kelmuse põhikoosseisu vahel.
Ebaseaduslik on võõra kaardiga ilma omaniku nõusolekuta sularaha väljavõtmine pangaautomaadist ning tasumine teenuste või kaupade eest.
Ebaseaduslik pangakaardi kasutamine hõlmab nii omaniku tahte vastaselt kasutatud pangaaarti kui ka võltsitud pangakaarti.
Arvutikelmuse ja kelmuse põhikoosseisu vahel tekivad piiritlemisprobleemid võõra kaardiga kaupluses tasumise korral. Vahetegemisel on määravaks, kus süüdistatav kauba eest tasus -

kas kassas, kus oli makseterminal ning sisestada tuli PIN-kood või kassa, kus oli küll makseterminal, kuid ostu sooritamisel ei pea sisestama PIN-koodi, vaid allkirjastatakse ostutšekk, st luuakse teenindajale vale ettekujutus, et maksja on pangakaardi omanik. Kui süüdistatav sisestab kaupade eest tasumisel PIN-koodi makseterminali, on tegemist arvutikelmusega. Kui süüdistatav loob vale ettekujutuse teenindajale, et tema on pangakaardi omanik, tuleb kuritegu kvalifitseerida kelmusena.

Kaupluses võõra kaardiga tasumist võib kvalifitseerida ka omastamisena. Seda juhul, kui kannatanu andis süüdistatavale oma pangakaardi ning ütles PIN-koodi selleks, et süüdistatav ostaks teatud kindlaid asju teatud kindla rahasumma eest. Süüdistatav aga ületab volituste piire ning kasutab pangakaarti muude asjade ostuks või suurema summa ulatuses, kui teda volitati.

Pangaautomaadist sularaha väljavõtmisel tekivad piiritlemisprobeemid arvutikelmuse, varguse ja omastamise vahel. Kuna pangaautomaat töötab arvutiprogammi põhiselt ning sularaha väljavõtmisel tuleb sisestada andmed ehk PIN-kood, mis käivitab andmetöötlusprotsessi ja see on toime pandud ebaseaduslikult, eesmärgiga varalise kasu saamine, on täidetud kõik arvutikelmuse koosseisuks vajalikud tunnused ning tegu tuleb kvalifitseerida arvutikelmusena. Kuna vargus on pigem üldkoosseisuks ning arvutikelmuse koosseis erikoosseisuks, siis erinormi olemasolul rakendadakse alati viimast.

Arvutikelmuse ja omastamise piiritlemiseks tuleb välja selgitada samad asjaolud, mis võõra kaardiga kaupluses tasumisel- kuidas sattus pangakaart ning PIN-kood süüdistatava valdusesse. Kui ta varastas või leidis selle koos PIN-koodi teadasaamisega, siis on tegemist arvutikelmusega. Kui kannatanu ise andis talle, et süüdistatav võtaks tema arvelt 100 eurot välja, kuid süüdistatav võttis 200, jättes 100 eurot endale, on tegemist omastamisega.

Omastamise piiritlemisel tuleb hinnata ka, kas pangakaardi ja PIN-koodi saamine on toimunud seadustega kooskõlas. Näiteks piiratud teovõimega isikute pangakaarti ja PIN-koodi võivad kasutada vaid nende eestkostjad. Kui isik kasutab ilma seadusliku aluseta piiratud teovõimega isiku pangakaarti enda tarbeks, kuigi ta on töölepingu alusel määratud seda isikut hooldama, siis ei ole tegemist mitte omastamisega, vaid arvutikelmusega (tal ei olnud mingit õigust sisestada PIN-koodi ning talle usaldatud vara oli saadud ilma õigusliku aluseta).

Krediitkaarte on võimalik ebaseaduslikult kasutada kahel viisil- kas varastatakse teise isiku andmed või kasutatakse võltsitud kaarti. Kvalifitseerimisel võivad tekkida probleemid arvutikelmuse, omastamise või kelmuse koosseisude vahel. Koosseisude piiritlemisel tuleb välja selgitada samad asjaolud, mis deebetkaartide ebaseadusliku kasutamise puhul.

Osades riikides kvalifitseeritakse krediitkaardi andmete varastamist ka identiteedivargusena.

Kütusekaardi ebaseadusliku kasutamise puhul tekivad piiritlemisprobleemid arvutikelmuse, varguse, kelmuse ja omastamise koosseisude vahel.

Kui isik tangib ettemaksukaardil olevast summast rohkem kütust, kui maksevahendid võimaldavad, kasutades ära süsteemiriket, ei ole tegemist arvutikelmusega. Riigikohus on sellisel juhul kvalifitiseerinud vargusena, Saksamaa kohus leidis, et tegemist ei ole üldse kuriteoga. Kui isik ise rikub automaati selleks, et rohkem kütust kätte saada, sisestab programmi valesid andmeid või käivitab ebaseaduslikult andmetöötlusprotsessi, võib tegemist olla arvutikelmusega.

Arvutikelmuse ja omastamise koosseisude eristamisel tuleks välja selgitada, millistel asjaoludel sattus kütusekaart isiku valdusesse. Kui ta sai selle seoses oma tööülesannetega, kuid tangib kütust enda või kolmandate isikute tarbeks, on tegemist omastamisega. Kui isik jätab töösuhte lõppemisel kaardi tagastamata, seega ei oma õigust seda kasutada ning tangib kütust enda või kolmandate isikute tarbeks, on tegemist arvutikelmusega.

Arvutikelmuse ja kelmuse põhikoosseisu eristamisel tuleb selgitada, kas kütusekaarti kasutatakse automaattanklas PIN-koodi sisestades või mehhaniseeritud tööjõuga tanklas teenindajale vale ettekujutust luues. Esimesel juhul on tegemist arvutikelmusega, teisel juhul kelmusega.

Mobiiltelefoni SIM-kaardi ebaseaduslik kasutamine (helistamine, sõnumite saatmine) kvalifitseeritakse kas arvutikelmusena või kui kahju jääb alla kuriteona kvalifitseerimiseks vajaliku summa, siis süüteona väheväärtusliku asja vastu. Asja omavolilise kasutamise koosseisu välistab see, et SIM-kaardil puudub rahaline väärtus. Kelmuse koosseisu välistab asjaolu, et helistamise süsteemi ei saa petta ning kõneoperaatoril on ükskõik, kes selle SIM-kaardiga helistab, talle ei saa luua valeettekujutust, et tegemist on sama isikuga, kes lepingu sõlmis. Varguse välistab asjaolu, et helistamise või muude teenuste kasutamisega ei ole võimalik vallasasja ära võtta.

Omastamise koosseis võiks kaalumisele tulla, kui isikule antakse kasutada telefoni ja SIM-kaarti ühe kõne tegemiseks, kuid ta helistab ja tellib endal virtuaalset raha, ületades volituse piire.

Kuna kiirlaenu taotlusi vaatab enamasti läbi ning laene väljastab inimtööjõud, siis kellegi teise nimel ebaseaduslik kiirlaenu võtmine tuleks kvalifitseerida kelmusena, mitte arvutikelmusena. Vale ettekujutus laenuvõtja isikust luuakse inimesele. Arvutiprogramm ei väljasta automaatselt laenu.

Lisaks eespool toodule kvalifitseeritakse arvutikelmusena ka ebaseaduslik tuludeklaratsiooni esitamine, ebaseaduslik taksofoni kasutamine ning ebaseaduslik kinkekaardi kasutamine.

Paljudel juhtudel on arvutikelmuse koosseisu kõrval isikuid süüdi mõistetud ka rahapesus. Kuna üldjuhul on arvutikelmuse toimepanijate eesmärgiks saada varalist kasu, mitte varjata, kust see raha tuleb, siis tuleb välistada rahapesu koosseisu.

Arvutikelmuse eristamisel teistest arvutikuritegudest (arvutiandmetesse sekkumine, arvutisüsteemi toimimise takistamine, arvutisüsteemi ebaseaduslik kasutamine) tuleb lähtuda varalise kasu saamisest. Arvutikelmuse puhul on isiku eesmärgiks saada varalist kasu, ta saab oma tegevusega otsest varalist kasu. Selle koosseisuga kaitstakse vara ning nõutav on tagajärje saabumine. Teiste arvutikuritegude puhul ei ole varalise kasu saamine oluline ning tagajärge ei pea üldse saabuma, piisab teost. Koosseisudega kaitstakse õiguspärase kasutaja huve.

Computer frauds delimiting problems. Summary

Present study examines problems which arise upon computer frauds qualification. As number of computer crimes, including computer frauds, is increasing, it is important that investigators and bodies conducting proceedings, as well as prosecutors and judges would have consistent view when the offence is a computer fraud and when not. The study shows that the issue is current, because similar criminal behaviour is qualified under different sections. If a person does not appeal or file cassation then it seems that the problem does not exist, but in such case we do not need Penal Code and all crimes could be summarized under one section. So the issue is important in regard to uniform application.

The aim of the study is to determine main problems in computer fraud qualification; when a crime should be qualified as computer fraud, when as misappropriation, theft, fraud or other computer crime.
To achieve the aim following tasks are established:

- determine features required in computer fraud qualification;
- determine rules of delimiting computer fraud and other crimes.

The study is divided into three chapters. First chapter examines computer crimes in general – which computer crimes are provided in Penal Code and main definitions used in the study.
Second part of the study examines computer frauds in Estonia, US and Germany.
Third part of the study examines different type of computer frauds and their delimiting problems; computer fraud relation to money laundry and distinguishing computer fraud from interference in computer data, hindering of operation of computer system and illegal use of computer system.
A combined method – judicial practice empirical analysis with views from theoretical literature, is used in the study.

Materials used in the study are mainly Estonian, German and US judicial decisions; different articles about computer frauds and computer crimes; Estonian, German and US law.

Theoretical views base mainly on commented edition of Penal Code and J. Sootak's textbook Offences against property.

Investigators do not have consistent view upon computer fraud qualification. Main delimiting problems arise when distinguishing computer frauds from misappropriation, theft and fraud. Distinguishing computer frauds from other computer crimes may also be problematic.

Following illegal activities are qualified as computer fraud – transfers in the internet bank; use of bankcard, credit card, fuel card, gift card; use of cell phone SIM-card; use of public phone; income declaration presentation.

In case of illegal transfer in the internet bank, delimiting problems arise between computer fraud and misappropriation. It must be determined how accused person got access to bank account of another. If victim gave internet bank access to accused person for some actions, but accused person exceeded authorisation limits and made transfer in his own or third person's favour, then the crime should be qualified as misappropriation. Also if accused person had access to bank account due to duty, but he used employer's bank account in other purpose than duty, for example, made transfer to his own bank account, then such action should be qualified as misappropriation.
If accused person got access to bank account of another against victims will, used some program to get passwords, found or stole access codes, then his action should be qualified as computer fraud.
Illegal internet bank transfer is a transfer made against victim's will from victim's bank account to accused person's or third person's bank account, irrespective of withdrawing cash later from ATM or not, transfer to purchase service or goods, including charging money to cell phone; concluding direct debit or standing orders.

In case of illegal use of bankcard, delimiting problems arise between computer fraud, misappropriation, theft and fraud.
Cash withdrawal from ATM, payments for services or goods with the card of another without owner's consent is illegal.
Illegal use of bankcard includes a bankcard used against owner's will, as well as use of counterfeit bankcard.

Delimiting problems between computer fraud and fraud arise in case of payment with card of another in store. Here it is important where accused person paid for the goods – whether in checkout he had to enter PIN code into the payment terminal or the PIN code in checkout's payment terminal was not required and check had to be signed, this means causing

misconception to salesman that payer is owner of the bankcard. If accused person enters PIN code into the payment terminal when paying for the goods, then it is a computer fraud. If accused person causes misconception to salesman that he is the owner of the bankcard, then the crime should be qualified as fraud.

Payment with card of another in store could also be qualified as misappropriation in case if victim gave to accused person his bankcard and told PIN code, so that accused person could purchase certain goods for certain amount of money. But accused person exceeds authorisation limits and uses bankcard to purchase other goods or for bigger sum than he was authorised.

In case of cash withdrawal from AMT, delimiting problems arise between computer fraud, theft and misappropriation. As ATM operates on the basis of computer program and upon cash withdrawal one must enter data, i.e. PIN code, which activates data processing and it is committed illegally with aim to receive proprietary benefit, then all features on computer fraud exist and the act should be qualified as computer fraud. As theft is rather general elements of crime and computer fraud special elements of crime, then in case of specific legal provision the last one is always implemented.

In order to delimit computer fraud and misappropriation, same circumstances should be determined as in case of paying with card of another in store – how the bankcard and PIN code got in accused person's possession. If he stole or found it with finding out PIN code, then it is computer fraud. If a victim himself gave it to him so that accused person could withdraw 100 euros from victim's account but accused person took 200 and 100 euros kept to himself, then it is misappropriation.

Upon delimiting misappropriation, it should be also considered whether bankcard and PIN code are received in accordance with law. For example, bankcard and PIN code of person with restricted active legal capacity can be used only by his guardian. If a person uses without legal basis bankcard of person with restricted active legal capacity for himself, even though he is designated under employment contract to care, then it is not misappropriation but computer fraud (he did not have right to enter PIN code and property entrusted to him was gained without legal basis).

Credit cards can be used illegally in two ways- whether other person's data is stolen or counterfeit card is used. Delimiting problems may arise between computer fraud, misappropriation or fraud. Upon delimiting, same circumstances should be determined as in case of illegal use of debit card.

In some countries stealing credit card data is also qualified as identity theft.

In case of illegal use of fuel card, delimiting problems arise between computer fraud, theft, fraud and misappropriation.

If a person fills up more fuel than a sum on the prepaid card, if means of payment allow it, by taking advantage of system error, then it is not computer fraud. Supreme Court qualified this case as theft, German court established that it is not crime at all. If person violates automat in order to get more fuel, enters wrong data into the program or activates data processing illegally, then it could be computer fraud.

Distinguishing computer fraud from misappropriation, it should be determined under which circumstances the fuel card got in person's possession. If he got it in relation to duty but fills up fuel for himself or for third person, then it is misappropriation. If person does not return the card upon employment relationship termination, so he does not have right to use it and fills up fuel for himself or for third person, then it is computer fraud.

Upon distinguishing computer fraud from fraud, it should be determined whether fuel card is used in automatic gas station by entering PIN code or in mechanised gas station by causing misconception to the assistant. In first case it is computer fraud, in second case fraud.

Illegal use of cell phone SIM-card (calling, sending messages) is qualified as computer fraud or, if damage is less than needed for crime qualification, then as misdemeanour. Unauthorised use of a thing is precluded by the fact that SIM-card does not have pecuniary value. Fraud is precluded by the circumstance that calling system cannot be deceived and the operator does not care who uses the SIM-card when calling. Misconception that it is the same person who concluded the contract cannot be caused. Theft is precluded by the circumstance that movable cannot be taken away by calling or using other services.

Misappropriation could be considered if a person gets cell phone and SIM-card to make one call but he exceeds authorisation by calling and ordering virtual money.

As loan applications are usually reviewed and loans issued by manpower, then illegal loan taking in behalf of other person should be qualified as fraud not as computer fraud.

Misconception about loan taker is caused to person. Computer program does not automatically issue loan.

In addition to above mentioned, illegal income declaration presentation, illegal use of public phone and illegal use of gift card are qualified as computer fraud.

In many cases persons who are convicted in computer fraud, are at the same time convicted in money laundry. As usually persons who commit computer fraud aim to receive proprietary benefit not to hide source of the money, then money laundry should be precluded.

Upon distinguishing computer fraud from other computer crimes (interference in computer data, hindering of operation of computer system and illegal use of computer system), receiving proprietary benefit needs to be taken into account. In case of computer fraud, persons aim is to receive proprietary benefit, he receives direct proprietary benefit with his action. Here consequence is important. In case of other computer crimes, receiving proprietary benefit is not important and no consequence is required, the act itself is enough. Legitimate users interests are protected in both cases.

Kasutatud kirjandus:

1. Audal, J, Lu, Q, Roman, P. Computer Crimes. American Criminal Law Review Spring, 2008. Arvutivõrgus: http://international.westlaw.com.ezproxy.utlib.ee/result/previewcontroller.aspx?TF=756&TC=4&mt=314&db=0001086&findtype=Y&tc=-1&rp=%2ffind%2fdefault.wl&spa=inttartu2-000&ordoc=0295720756&serialnum=0338338361&vr=2.0&fn=_top&sv=Split&tf=-1&referencepositiontype=S&pbc=05437822&referenceposition=235&rs=WLIN12.01&RP=/find/default.wl&bLinkViewer=true 29.02.2012
2. Elkind, E. Varavastane süütegu internetikeskkonnas: selle piiritlemise probleemid Eesti karistusõiguses. Riigikohtu otsus 3-1-1-83-07. Juridica 5, 2008.
3. Enzer, M. Glossary of Internet Terms. Copyright 1994-2011. Arvutivõrgus: http://www.matisse.net/files/glossary.html#I 02.04.2012
4. Gottschalk, P. Categories of financial crime. Journal of Financial Crime. 2010, 17(4). Arvutivõrgus: http://international.westlaw.com.ezproxy.utlib.ee/result/default.wl?cfid=1&mt=126&origin=Search&sri=15&query=%22BANK+ACCOUNT+FRAUD%22&method=TNC&db=WORLD-JLR&rlt=CLID_QRYRLT1813344212&rltdb=CLID_DB9612011344212&service=Search&eq=Welcome%2f126&rp=%2fWelcome%2f126%2fdefault.wl&sp=inttartu2-000&srch=TRUE&vr=2.0&action=Search&sv=Split&fmqv=s&fn=_top&rs=UKIS1.0 21.02.2012
5. Hanson. V, Tavast. A. Arvutikasutaja sõnastik. Arvutivõrgus: www.keeleveeb.ee. 02.04.2012
6. Icove, D; Seger; VonStorch, W. Computer Crime: A Crimefighter´s Handbook. 1995. USA.
7. IT terministandardi sõnastik. Arvutivõrgus: www.keeleveeb.ee. 02.04.2012
8. Karistusseadustik. Kommenteeritud väljaanne. 3.trükk. 2009
9. Küberjulgeoleku strateegia 2008–2013, Kaitseministeerium, Tallinn 2008. Arvutivõrgus: https://valitsus.ee/UserFiles/valitsus/et/valitsus/arengukavad/kaitseministeerium/kuberjulgeolek.pdf 23.02.2012
10. Liikane, L; Kesa, M.Arvutisõnastik. arvutivõrgus: www.keeleveeb.ee. 02.04.2012
11. Menninger, K. Identity Theft and other misuses of credit and debit cards. 81 Am. Jur. Proof of Facts 3d 113. 2005. Arvutivõrgus:

http://international.westlaw.com.ezproxy.utlib.ee/find/default.wl?carerlt=CLID_CARE1131545252_CaRE_0_N_1&mt=314&tf=781&ncare=6&tc=6&sp=inttartu2-000&vr=2.0&rpcat=AJP&care=Y&sv=Split&fn=_top&serialnum=0303050623&rs=WLIN12.01. 26.02.2012

12. Palo, Catherine, J.D., L.L.M. The Defense of a Computer Crime Case. 70 Am. Jur Trials 435. 1995. Arvutivõrgus: http://international.westlaw.com.ezproxy.utlib.ee/result/previewcontroller.aspx?TF=756&TC=4&mt=314&db=0119406&findtype=Y&tc=-1&rp=%2ffind%2fdefault.wl&spa=inttartu2-000&ordoc=0332168326&serialnum=0112032659&vr=2.0&fn=_top&sv=Split&tf=-1&pbc=43D0CF18&rs=WLIN12.01&RP=/find/default.wl&bLinkViewer=true 29.02.2012
13. Pikamäe, P. Mõningad kelmuse üldkoosseisu sisustamisprobleemid kohtupraktikas. Juridica II, 2011
14. Ploom, T. Mitteametlik juhis arvutikelmuse kvalifitseerimisel. E-kirjavahetus. 16.03.2009
15. .Ploom, T. Arvutikuritegude kvalifitseerimine. Juridica VIII 2003
16. Rosentau, M. loengumaterjalid IT-õigusest. TÜ. 2011
17. Salla, J. Registreeritud kuriteod 2003-2011. Justiitsministeerium. 2012. Arvutivõrgus: http://www.just.ee/56150 23.02.2012
18. Sootak. J, Varavastased süüteod. Tallinn, 2009
19. Sulbi, R. Alates detsembrist kaovad Eestist taksofonid. 2010. Arvutivõrgus: http://www.e24.ee/326096/alatest-detsembrist-kaovad-eestist-taksofonid/ 23.02.2012
20. Swedbank AS koduleht. Arvutivõrgus: www.swedbank.ee. 06.05.2012
21. Tele2 Eesti AS koduleht. Arvutivõrgus: www.tele2.ee 06.05.2012
22. Vikipeedia. Vaba entsüklopeedia. Arvutivõrgus: http://et.wikipedia.org/wiki/Internetiprotokoll 06.05.2012
23. www.rate.ee 11.04.2012
24. www.vallaste.ee 14.03.2012

Kasutatud õigusaktid:

1. Arvutikuritegevusvastane konventsioon. Vastu võetud: 23.11.2001 RT II 2003, 9, 32
2. Karistusseadustik. Vastu võetud: 06.06.2001 RT I 2001, 61, 364
3. Karistusseadustiku muutmise seaduse eelnõu seletuskiri. Arvutivõrgus: www.riigikogu.ee
4. Rahapesu ja terrorismi rahastamise tõkestamise seadus. Vastu võetud 19.12.2007 RT I 2008, 3, 21
5. Saksa kriminaalkoodeks. Kättesaadav internetis: http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#StGBengl_000P263a.
6. U.S Code Title 18- Crimes and Criminal procedure. Arvutivõrgus: http://www.gpo.gov/fdsys/pkg/USCODE-2010-title18/pdf/USCODE-2010-title18-partI.pdf 04.04.2012
7. U.S Code Title 15- Commerce and Trade. Arvutivõrgus: http://www.gpo.gov/fdsys/pkg/USCODE-2010-title15/pdf/USCODE-2010-title15-chap41.pdf

Kasutatud kohtupraktika:

Riigikohus

RK 3-1-1-85-11. Arvutivõrgus: www.riigikohus.ee

RK 3-1-1-42-11. Arvutivõrgus: www.riigikohus.ee

RK 3-1-1-21-11. Arvutivõrgus: www.riigikohus.ee

RK 3-1-1-105-10. Arvutivõrgus: www.riigikohus.ee

RK 3-1-1-70-10. Arvutivõrgus: www.riigikohus.ee

RK 3-1-1-35-10. Arvutivõrgus: www.riigikohus.ee

RK 3-1-1-85-08 RT III 2009, 9, 58

RK 3-1-1-83-07 RT III 2008, 18, 121

RK 3-1-1-78-06 RT III 2006, 36, 302

RK 3-1-1-60-04 RT III 2004, 21, 241

Ringkonnakohtu otsused:

1-10-13009 Tallinna Ringkonnakohus 15.09.2011.

1-09-9855 Tallinna Ringkonnakohus 14.09.2010

1-09-3576 Tallinna Ringkonnakohus 14.06.2010

1-06-14599 Tartu Ringkonnakohus 23.04.2008

1-06-12976, Tallinna Ringkonnakohus 10.11.2006

Kättesaadavad arvutivõrgus: www.riigiteataja.ee

Maakohtu otsused:

1-11-7639 Harju Maakohus 29.02.2012

1-11-12863 Pärnu Maakohus 13.02.2012

1-11-13432 Tartu Maakohus 01.02.2012

1-11-14453 Harju Maakohus 31.01.2012

1-11-10794 Tartu Maakohus 17.01.2012

1-11-13820 Harju Maakohus 11.01.2012

1-11-13549 Harju Maakohus 10.01.2012

1-11-13715 Harju Maakohus 03.01.2012

1-11-2755 Harju Maakohus 20.12.2011

1-11-13118 Harju Maakohus 16.12.2011

1-11-13084 Harju Maakohus 13.12.2011

1-11-13181 Tartu Maakohus 06.12.2011

1-11-7211 Harju Maakohus 25.11.2011

1-11-10596 Harju Maakohus 22.11.2011

1-11-11863 Harju Maakohus 09.11.2011

1-11-9365 Harju Maakohus 07.10.2011

1-11-7609 Harju Maakohus 26.09.2011

1-11-9551 Harju Maakohus 23.09.2011

1-11-8706 Harju Maakohus 30.08.2011

1-11-4737 Harju Maakohus 20.06.2011

1-11-4244 Harju Maakohus 17.06.2011

1-11-4895 Viru Maakohus 26.05.2011

1-11-4870 Harju Maakohus 02.05.2011

1-10-8350 Tartu Maakohus 29.07.2010

1-10-17197 Tartu Maakohus 22.06.2011

1-10-8347 Tartu Maakohus 25.03.2011

1-10-16007 Harju Maakohus 11.03.2011

1-10-15796 Harju Maakohus 08.02.2011

1-09-5395 Pärnu Maakohus 16.04.2009

1-09-5360 Tartu Maakohus 07.05.2009

1-09-8563 Harju Maakohus 18.06.2009

1-09-9735 Viru Maakohus 25.05.2011

1-09-16675 Harju Maakohus 06.11.2009

1-09-8016 Tartu Maakohus 11.06.2009

1-08-6581 Pärnu Maakohus 18.09.2008

1-08-4059 Taru Maakohus 28.05.2008

1-07-5805 Harju Maakohus 12.06.2007

1-07-15253 Viru Maakohus 09.04.2008

1-07-1760 Harju Maakohus 19.02.2007

1-06-5550 Harju Maakohus 05.05.2006

1/2-2690/02 Tallinna Linnakohus 11.12.2002

1/1-2558/02 Tallinna Linnakohus 15.11.2002

1/1-1258/02 Tallinna Linnakohus 05.06.2002

1/2-1019/02 Tallinna Linnakohus 21.05.2002

1/2-2842/01 Tallinna Linnakohus 20.11.2001

Kättesaadavad arvutivõrgus: www.riigiteataja.ee

USA kohtulahendid:

U.S. v. Auguste 392 F.3d 1266. Arvutivõrgus: http://international.westlaw.com.ezproxy.utlib.ee/result/previewcontroller.aspx?TF=756&TC=4&mt=314&db=0000506&tc=-1&rp=%2ffind%2fdefault.wl&sp=inttartu2000&findtype=Y&ordoc=0303050623&serialnum=2005701543&vr=2.0&fn=_top&sv=Split&tf=-1&pbc=F46B39EF&rs=WLIN12.01&RP=/find/default.wl&bLinkViewer=true 26.02.2012

U.S. v. Hakley 101 Fed.Appx. 122 C.A.6. Arvutivõrgus: http://international.westlaw.com.ezproxy.utlib.ee/result/default.wl?cfid=1&mt=314&origin=Search&query=%22ATM+FRAUD%22&db=WHITECLR-CS&rlt=CLID_QRYRLT134514328723&method=TNC&service=Search&eq=search&rp=%2fsearch%2fdefault.wl&sp=inttartu2-000&srch=TRUE&vr=2.0&action=Search&rltdb=CLID_DB452492328723&sv=Split&fmqv=s&fn=_top&rs=WLIN12.01 03.03.2012

U.S. v. Lee 815 F.2d 971 C.A.4. Arvutivõrgus: http://international.westlaw.com.ezproxy.utlib.ee/result/previewcontroller.aspx?TF=756&TC=4&mt=314&db=1000546&docname=18USCAS1029&rp=%2ffind%2fdefault.wl&sp=inttartu2-000&findtype=L&ordoc=0303050623&tc=-1&vr=2.0&fn=_top&sv=Split&tf=-1&pbc=776D6BD4&rs=WLIN12.01&RP=/find/default.wl&bLinkViewer=true 04.03.2012

U.S. v. Rhodes 410 Fed.Appx. 856 C.A.6 (Ky.),2010. Arvutivõrgus: http://international.westlaw.com.ezproxy.utlib.ee/result/default.wl?cfid=1&mt=314&origin=Search&query=%22ELECTRONIC+FUND+TRANSFERS%22&db=WHITECLR-CS&rlt=CLID_QRYRLT215631335643&method=TNC&service=Search&eq=search&rp=%2fsearch%2fdefault.wl&sp=inttartu2-000&srch=TRUE&vr=2.0&action=Search&rltdb=CLID_DB274275233643&sv=Split&fmqv=s&fn=_top&rs=WLIN12.01 04.03.2012

U.S. v. Truong 587 F.3d 1049. Arvutivõrgus: http://international.westlaw.com.ezproxy.utlib.ee/result/previewcontroller.aspx?TF=756&TC=4&mt=314&db=0000506&tc=-1&rp=%2ffind%2fdefault.wl&sp=inttartu2-000&findtype=Y&ordoc=0303050623&serialnum=2020562512&vr=2.0&fn=_top&sv=Split&tf=-1&pbc=48CCA1FA&rs=WLIN12.01&RP=/find/default.wl&bLinkViewer=true 26.02.2012

Saksamaa kohtulahendid:

Forged Cash Card, Re (2 StR 376/91) [1993] E.C.C. 91 Bundesgerichtshof (Germany). Arvutivõrgus: http://international.westlaw.com.ezproxy.utlib.ee/result/default.wl?cfid=1&mt=316&origin=Search&sri=14%2c20%2c21%2c22%2c29&query=%22COMPUTER+FRAUD%22&method=TNC&db=DTLONDON%2cUK-CASELOC%2cUK-RPTS-ALL%2cUK-LIF%2cEU-RPTS-ALL&rlt=CLID_QRYRLT2671640663&rltdb=CLID_DB548041440663&service=Search&eq=Welcome%2f316&rp=%2fWelcome%2f316%2fdefault.wl&sp=inttartu2-000&srch=TRUE&vr=2.0&action=Search&sv=Split&fmqv=s&fn=_top&rs=UKIS1.0 07.03.2012

OLG Jena: Beschluss vom 20.09.2006 - 1 Ss 226/06 BeckRS, 2007, 05394. Arvutivõrgus: http://nomos.beck.de.ezproxy.utlib.ee/Default.aspx?vpath=bibdata\ents\urteile\2007\cont\beckrs_2007_05394.htm&hlwords=#xhlhit 24.03.2012

OLG Braunschweig, Urteil vom 12. 10. 2007 - Ss 64/07, NStZ 2008, 402. Arvutivõrgus: http://nomos.beck.de.ezproxy.utlib.ee/Default.aspx?vpath=bibdata\zeits\nstz\2008\cont\nstz.2008.402.1.htm&hlwords=#xhlhit 24.03.2012

OLG Celle: Beschluss vom 05.11.2010 - 1 Ws 277/10 BeckRS 2010, 28415 Arvutivõrgus: http://nomos.beck.de.ezproxy.utlib.ee/Default.aspx?vpath=bibdata\ents\urteile\2010\cont\beckrs_2010_28415.htm&hlwords=#xhlhit 24.03.2012

LG Freiburg Urteil vom 19.11.2008 - 7 Ns 150 Js 4282/08 BeckRS 2009, 00403. Arvutivõrgus:http://beck-online.beck.de.ezproxy.utlib.ee/Default.aspx?vpath=bibdata\ents\urteile\2009\cont\beckrs_2009_00403.htm&hlwords=#xhlhit 24.03.2012