TARTU ÜLIKOOL

ÕIGUSTEADUSKOND

Avaliku õiguse instituut

Kriminaalõiguse, kriminoloogia ja kognitiivse psühholoogia õppetool

Merika Nimmo

INTERNETIGA SEOTUD IDENTITEEDIVARGUS JA SELLE REGULATSIOON EESTI KARISTUSÕIGUSES

Magistritöö

Juhendaja dr. iur. Priit Pikamäe

Kaasjuhendaja dr. iur. Jaan Ginter

Tartu 2014

SISUKORD

SISSEJUHATUS

Erinevad infotehnoloogilised vahendid nagu internet ja mobiiltelefon, on aidanud kaasa infoühiskonna tekkele.[1] Tänapäevast ühiskonda iseloomustab tehnika üha kiirenev areng. Näiteks kahekordistub G. E. Moore'i poolt väljapakutud teooria kohaselt arvuti protsessori arvutusvõimsus iga kahe aastaga.[2] Selline hüppeline areng suurendab elektroonika ja infotehnoloogia mõju ning tähtsust pea igas majandussektoris.[3] Tehnoloogia tähendab ühiskonna jaoks uusi võimalusi, millega aga kaasnevad alati uued ning suurenevad juba olemasolevad riskid.

Küberkuritegevuse levik on aastatega märgatavalt suurenenud.[4] Internet on anonüümne ning koondab suurel arvul potentsiaalseid ohvreid, luues sellega soodsa pinnase arvutikuritegevusele.[5] Teisisõnu kasvab üheaegselt tehnika arenguga kuritegude hulk, mida uute tehnoloogiliste võimaluste abil on üha kergem internetikeskkonnas toime panna. Küberkuritegevuse kasvu mõjutab olulisel määral ka aastast aastasse suurenev interneti kättesaadavus. Rahvusvahelise Telekommunikatsiooni Liidu uuringu tulemustest nähtub, et interneti individuaalkasutajate arv kasvab iga aastaga oluliselt, moodustades praeguseks ligikaudu 40% maailma kogurahvastikust.[6]

Internet on üks kiiremini kasvavaid valdkondi tehnoloogilise infrastruktuuri arengus ning samuti kasvab trend digitaliseerimise suunas, mistõttu on arvutitehnoloogia muutumas igapäevaelu lahutamatuks osaks. E-kirjad, ajakirjanduse internetiväljaanded ja internetipõhised kommunikatsioonimeediumid on asendamas seni tuntud paberkandjal kirju ning füüsilisi kokkusaamisi. Samuti on üha kiiremini arenevad e-riik, e-kool ning muud ühiskonna igapäevaluga seotud internetikeskkonnad. E-keskkondade haldamine on finantsiliselt ressursisäästlikum, kui seda on paberipõhine asjaajamine. Seetõttu toob erinevate

---

[1] Euroopa Liit. Euroopa Liidu õiguse kokkuvõtted. Infoühiskond. Arvutivõrgus: http://europa.eu/legislation_summaries/information_society/index_et.htm, 12.03.2014

[2] G. E. Moore. Moore's Law or how overall processing power of computers will double every two years. Arvutivõrgus: http://www.mooreslaw.org, 12.03.2014.

[3] *Ibid*.

[4] Aastast 2001 kuni aastani 2009 on küberkuritegude intsidentide arv kasvanud ligikaudu 100% võrra, millest 22,3% kasv toimus aastatel 2008 kuni 2009. Vt: W. Gragido, J. Pirc, (Edit.) R. Rogers. Cybercrime and Espionage. An Analysis of Subversive Multivector Threats. Syngress Publications. Burlington: Elsevier 2011, p. 10.

[5] Internet Crime Complaint Center, Mass Market Fraud, p. 1. Arvutivõrgus: https://www.ic3.gov/media/MassMarketFraud.pdf, 12.03.2014.

[6] Uuringu kohaselt oli 2013. aasta lõpuks interneti kasutajaid maailmas umbes 3,9 miljardit, mida on rohkem kui kolm korda enam võrreldes 10 aasta taguse ajaga, kus interneti kasutajaid oli kokku 1,2 miljardit. Viimase aastaga on interneti kasutajate arv kasvanud 0,3 miljardi võrra ning 2013 aasta seisuga kasutab internetti umbes 40% maailma kogurahvastikust. Vt: International Telecommunication Union, Information and Communication Technology. Facts and Figures 2013, tbl. 1. Arvutivõrgus: http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx, 12.03.2014.

ühiskondlike teenuste internetivõrku suunamine kaasa produktiivsuse ja efektiivsuse kasvu, teenuste kättesaadavamaks muutumise ning nende kvaliteedi tõusu, vähendades sealjuures teenuste hinda.[7] Samal ajal kasvab aga isikuandmete jõudmisega internetikeskkonda identiteedivarguste ning personaalse informatsiooni kuritegeliku kasutamise risk.

Isikuandmete väärkasutamine võib toimuda paljudel erinevatel viisidel ning eesmärkidel, samuti nii võrguvabas keskkonnas (*offline identity theft*) kui ka küberruumis (*online identity theft*).[8] Seetõttu on raske leida identiteedivargusele ühtset ning kõikehõlmavat definitsiooni.[9] Võttes aga arvesse küberkuritegevuse, sealjuures ka internetiga seotud identiteedivarguste laialdast arvulist kasvu, on oluline luua mehhanisme, mis tagaksid isikutele tõhusa kaitse nende isikuandmete kuritarvitamise vastu. Olulisimaks neist on efektiivne rahvusvaheline koostöö, sest internetis toime pandud kuriteod on enamasti internatsionaalsed ega tunne riigipiire. Riikidevahelise koostöö edendamiseks ning võimalike konfliktide vältimiseks on oluline, et identiteedivargus oleks kriminaliseeritud kõikides riikides ning samuti, et selle regulatsioon oleks võimalikult ühetaoline.[10]

Paljudes riikides on identiteedivarguse elemendid reguleeritud osaliselt mõne teise kuriteokoosseisuga, kuid siiski puudub üks kõikehõlmav säte. Eestis kriminaliseeriti identiteedivargus eriregulatsiooniga aga juba 15.11.2009 kui karistusseadustiku muutmise seadusega[11] täiendati karistusseadustikku[12] (KarS) §-ga 157[2], mille kohaselt on karistatav teise isiku identiteedi ebaseaduslik kasutamine, mis seisneb teist isikut tuvastavate või tuvastada võimaldavate isikuandmete tema nõusolekuta edastamises, nendele juurdepääsu võimaldamises või nende kasutamises, eesmärgiga luua teise isikuna esinemise teel temast teadvalt ebaõige ettekujutus, kui sellega on tekitatud kahju teise isiku seadusega kaitstud

[7] Nii on ka Euroopa digitaalse tegevuskava eesmärgiks digitaaltehnoloogia tõhusama kasutamise ning ulatuslikuma kasutuselevõtu abil parandada eurooplaste elukvaliteeti paremate tervishoiu, tõhusamate transpordilahenduste ning avalikele teenustele lihtsama juurdepääsu kaudu. Vt: Euroopa Komisjoni teatis Euroopa Parlamendile, Nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele. Euroopa digitaalne tegevuskava, p 1. Arvutivõrgus: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:REV1:ET:HTML, 12.03.2014.

[8] McAfee, Inc. What you need to know to avoid identity theft. *Sine anno, sine loco.* p. 22-23. Arvutivõrgus: http://promos.mcafee.com/en-US/PDF/IDTheft_eguide_US.pdf, 02.05.2014.

[9] M.Gercke. Internet-related Identity Theft. A discussion paper. Strasbourg: Council of Europe 2007, p. 4. Arvutivõrgus: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20activity_events_on_identity_theft/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf, 12.03.2014.

[10] United Nations. Office on Drugs and Crime. Handbook on Identity-related Crime.New York: United Nations 2011, p. 38. Arvutivõrgus: https://www.unodc.org/documents/treaties/UNCAC/Publications/Handbook_on_ID_Crime/10-57802_ebooke.pdf, 12.03.2014.
Edaspidi allmärkustes: UNODC

[11] Karistusseadustiku muutmise seadus. - RT I 2009, 51, 348.

[12] Karistusseadustik. - RT I 2001, 61, 364… RT I, 26.02.2014, 6.

õigustele või huvidele, või varjata kuritegu.

Tänaseks ei ole ülemaailmsel ega ka Euroopa Liidu tasandil välja töötatud ühtset identiteedivarguse eriregulatsiooni. Samas on ühetaolise regulatsiooni loomist ning identiteedivarguse kriminaliseerimist kõigis Euroopa Liidu liikmesriikides vajalikuks pidanud ka Euroopa Nõukogu. [13]

Kõige laiaulatuslikumaks olemasolevaks identiteedivargust reguleerivaks sätteks võib pidada Ameerika Ühendriikide seadustikust (*United States Code*[14], U.S.C.) tulenevat ning kõigis osariikides kohaldatavat spetsiaalset identiteedivarguse kuriteokoosseisu. Samas võib sarnaselt siseriiklikele lähenemistele leida identiteedivarguse eri faaside kriminaliseerimist läbi teiste kuriteokoosseisude ka rahvusvahelisel tasandil. Nii on asjakohaseks näiteks Euroopa Nõukogu arvutikuritegevusvastane konventsioon [15] ning Euroopa Parlamendi ja Nõukogu 12.08.2013. a direktiiv 2013/40/EL, milles käsitletakse infosüsteemide vastu suunatud ründeid ja millega asendatakse nõukogu raamotsus 2005/222/JSK (direktiiv 2013/40) [16] . Nimetatud õigusaktid käsitlevad mõlemad rohkemal või vähemal määral internetiga seotud identiteedivargusele iseloomulikke elemente. Kusjuures sisaldab dirketiivi 2013/40 Art 9 punkt 5 raskendava asjaoluna seda, kui direktiivi 2013/40 artiklites 4 ja 5 osutatud kuriteod pannakse toime teise isiku isikuandmete väärkasutamise teel, eesmärgiga võita kolmanda isiku usaldus, ning tekitatakse seeläbi kahju tegeliku identiteedi omanikule, olles ainsaks Eestit puudutavaks rahvusvahelistest õigusaktidest tulenevaks sätteks, milles on otseselt identiteedivargusega seonduvat reguleeritud.

Autori uurimiseesmärgiks on magistritöös analüüsida Eesti karistusseadustikus identiteedivarguse sätte vastavust rahvusvahelistest õigusaktidest tulenevatele eriregulatsioonile kehtestatud nõuetele ning hinnata karistusseadustikus sisalduva identiteedivarguse regulatsiooni kaitseala analüüsides KarS §-s 157^2 sätestatud kuriteo koosseisutunnuseid rahvusvaheliste identiteedivarguse ühtsete põhimõtete kontekstis.

[13] Council of the European Union. Justice and Home Affairs. Press Release. 2827th Council meeting. Brussels: Council of the European Union 2007, p. 20. Arvutivõrgus: http://europa.eu/rapid/pressReleasesAction.do?reference=PRES/07/253&format=DOC&aged=1&language=EN&guiLanguage=en, 12.03.2014.
[14] United States Code (U.S.C.). July 30, 1947, ch. 388, 61 Stat. 633. Arvutivõrgus: http://uscode.house.gov, 12.03.2014.
[15] Arvutikuritegevusvastane konventsioon. - RT II 2003, 9,32.
[16] Euroopa Parlamendi ja Nõukogu 12.08.2013. a direktiiv 2013/40/EL, milles käsitletakse infosüsteemide vastu suunatud ründeid ja millega asendatakse nõukogu raamotsus 2005/222/JSK. - Euroopa Liidu Teataja (ELT) L 218/8, 14.08.2013, lk 8-14.

Töö eesmärgi täitmiseks keskendub autor eelkõige Eesti identiteedivarguse eriregulatsiooniga seotud probleemide hindamisele seoses internetis toimepandavate juhtumitega. Autor on varasemalt uurimistöö raames käsitlenud identiteedivarguse sätte otstarbekust Eesti karistusseaduses, et selgitada, kas identiteedivarguse kriminaliseerimine end praktikas õigustab või pigem koormab kriminaalmenetlust.[17] Käesolevas töös annab autor aga hinnangu karistusseadustikus sisalduva internetiga seotud identiteedivarguse eriregulatsiooni vastavusele üldistele ühistele internetiga seotud identiteedivarguse põhimõtetele ja tunnustele ning rahvusvahelistest õigusaktidest tulenevatele nõuetele. Samuti tuuakse välja teised karistusseadustikus sisalduvad kuriteokoosseisud, mille kaudu on karistusseadustikus identiteedivarguse eri etapid reguleeritud.

Internetiga seotud identiteedivargusetele iseloomulike tunnuste leidmiseks selgitab autor identiteedivarguse mõistet, üritades leida definitsioonide rohkuses isikuandmete kuritarvitamisega seotud tegevustes ühiseid põhimõtteid, mis võimaldaksid avada identiteedivarguse sisu. Mõiste sisustamisel võtab autor arvesse internetis toime pandud identiteedivarguste erinevaid eesmärke, isikuandmete kogumiseks kasutatud meetodeid ning kogutava informatsiooni iseloomu, et seejärel koondada kõiki juhtumeid ühendavad tunnused, mis võiksid olla abiks ühtse ning kõikehõlmava regulatsiooni väljatöötamisel ning hindab, kas ja millistele leitud tunnustele peaks isikuandmete väärkasutamisele internetis suunatud kuriteokoosseis vastama, et tagada isikute tõhus ning efektiivne kaitse. Samuti, kas nimetatud tunnused peaksid kõik olema sätestatud identiteedivargust reguleerivas erinormis või on isikutele efektiivne kaitse tagatud toodud tunnuste reguleerimisega läbi teiste asjakohaste kuriteokoosseisude.

Teiseks toob autor välja antud küsimuses relevantsed Eestit puudutavad piiriülesed õigusaktid ning analüüsib, kas ja millisel määral need reguleerivad identiteedivargust üldiselt ning selle spetsiaalnormi. Alles seejärel saab autor anda võrdlevõigusliku hinnangu sellele, kas karistusseadustikus sisalduv teise isiku identiteedi ebaseaduslikku kasutamist kriminaliseeriv säte täidab nimetatud lepingutest või õigusaktidest tulenevaid eriregulatsioonile seatud nõudeid ning eesmärke. Muuhulgas hindab autor, millised internetiga seotud identiteedivarguse tunnused on nimetatud õigusaktidest tulenevate regulatsioonidega kaetud, et võtta seisukoht, milliste identiteedivarguse elementide kriminaliseerimist on juba rahvusvahelisel tasandil oluliseks peetud ning hinnata internetiga seotud identiteedivarguse regulatsiooni tervikuna. Samuti analüüsib autor töös läbivalt KarS § 157^2 koosseisutunnuseid

[17] M. Nimmo. Identiteedivargus Eesti karistusseadustikus. Uurimistöö. Tallinn: Tartu Ülikooli Õigusteaduskond 2012.

ning teisi asjakohaseid karistusseadustiku kuriteokoosseise, et anda hinnang, kas karistusseadustik tagab isikutele efektiivse kaitse kõikides identiteedivarguse etappides. Lisaks hinnangu andmisele teeb autor parandusettepanekud seal, kus kehtiv regulatsioon on ilmselt puudulik või ebaselge.

Magistritöö hüpoteesiks on, et Eestis kehtiv identiteedivarguse regulatsioon ei hõlma kõiki internetiga seotud identiteedivarguse ühiseid tunnuseid ning sisaldab koosseisutunnustena asjaolusid, mis muudavad sätte kohaldamisala liialt kitsaks ega taga seega isikutele tõhusat kaitset internetis toime pandud personaalse informatsiooni väärkasutamise vastu. Teiseks hüpoteesiks on see, et Eestis kehtiv identiteedivarguse spetsiaalnorm ei ole kooskõlas rahvusvahelistest õigusaktidest ja lepingutest tulenevate eriregulatsioonile seatud nõuetega ning seetõttu tuleb karistusseadustiku regulatsiooni muuta, et see nõutud eesmärke täidaks.

Töö esimeses peatükis käsitletakse internetiga seotud identiteedivarguse mõistet ning ühtse definitsiooni leidmisega seonduvaid probleeme. Kuivõrd ühtne identiteedivarguse sisustamine on vajalik eelkõige rahvusvahelise koostöö edendamiseks, siis käsitleb autor samas peatükis ka juba olemasolevate asjakohaste rahvusvaheliste õigusaktide ning lepingute panust identiteedivarguse reguleerimisel. Tulenevalt töö eesmärkidest, keskendutakse töös eelkõige siiski identiteedivarguse spetsiaalnormi puudutavatele õigusnormidele, kuid ei jäeta tähelepanuta ka teisi asjakohaseid regulatsioone, mis on seotud identiteedivarguse erinevate etappidega.

Töö teises peatükis uuritakse Eestis karistusseadustikus sätestatud identiteedivargusega kaitstavat õigushüve, määratletakse sätte kaitse- ning vastutusalasse kuuluvad õigussubjektid ning analüüsitakse reguleerimisetappide kaudu sätte koosseisutunnuseid. Samuti tuuakse välja teised karistusseadustikus identiteedivarguse erinevaid etappe reguleerivad kuriteokoosseisud. Toodud elemente käsitletakse internetiga seotud identiteedivarguse juhtumeid siduvate üldiste ühiste põhimõtete kontekstis, millega vastavuse saavutamine võiks töö hüpoteesi kohaselt olla tõhusa kriminaalmenetlusliku kaitse tagamise oluliseks tingimuseks. Samuti hinnatakse Eestis kehtiva identiteedivarguse regulatsiooni vastavust rahvusvahelistest õigusaktidest ja lepingutest tulenevatele nõuetele ja eesmärkidele ning tehakse parandusettepanekuid seal, kus regulatsioon vajaks muutmist. Muuhulgas käsitleb autor seda, kas Justiitsministeeriumi

programmi „Parema õigusloome arendamine“ [18] raames kavandatavad muudatused parandavad Eestis kehtiva identiteedivarguse regulatsiooniga seonduvaid probleeme.

Püstitatud eesmärkide saavutamiseks on rakendatud süsteemset ja võrdlevõiguslikku uurimismeetodit. Töö põhiallikateks on Euroopa Parlamendi ja Nõukogu direktiiv 2013/40/EL, Euroopa Nõukogu arvutikuritegevusvastane konventsioon ning Eesti karistusseadustik. KarS sätete tõlgendamisel on kasutatud peamiselt Riigikohtu ning madalama astmete kohtute otsuseid ning karistusseadustiku muutmise seaduse eelnõude 554 SE[19] ja 530 SE I[20] seletuskirjasid. Töö teisesteks allikateks on identiteedivargustega seotud küsimusi käsitlev õiguskirjandus, sealhulgas erinevate organisatsioonide juhtkirjad ning muud identiteedivarguse temaatikaga seonduvad artiklid.

Autor märgib täiendavalt, et töö ei käsitle kõiki identiteedivarguse juhtumeid, vaid keskendub ainult internetiga seotud identiteedivargustele. Autori hinnangul on töö teemat ning eesmärki arvesse võttes kasutatud asjakohast teemajaotust. Samuti on autor seisukohal, et töö sisaldab endas uudseid põhimõtteid, kuivõrd Eesti õigusmaastikul on identiteedivargusega seonduvat uuritud vähe ning siseriikliku karistusõiguse vastavuse hindamine kõrgemalseisvatele õigusaktidele ning põhimõtetele on käesoleval ajal aktuaalne ning vajalik karistusõigust reguleerivate seaduste kvaliteedi tõstmiseks ning isikutele tõhusama karistusõigusliku kaitse tagamiseks.

[18] Eelnõu töögrupi (tuntud ka kui karistusõiguse revisjon) esmärgid ning tulemused on avaldatud justiitsministeeriumi koduleheküljel. Vt: Justiitsministeerium. Karistusõiguse Revisjon. Arvutivõrgus: http://www.just.ee/revisjon, 12.03.2014.

[19] Karistusseadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu seletuskiri 554 SE. Arvutivõrgus: http://www.riigikogu.ee/?op=ems&page=eelnou&eid=78433b29-8b2f-4281-a582-0efb9631e2ad&, 28.04.2014.
Edaspidi allmärkustes: Seletuskiri 554 SE

[20] Karistusseadustiku muutmise seaduse eelnõu seletuskiri 530 SE I. Arvutivõrgus: http://www.riigikogu.ee/?page=eelnou&op=ems&emshelp=true&eid=673140&u=20120410162824, 12.03.2014.
Edaspidi allmärkustes: Seletuskiri 530 SE I.

1. Identiteedivargus üldiselt

1.1. Identiteedivarguse mõiste sisustamine

1.1.1. Hõivatav informatsioon

Identiteedivarguse mõistel ei ole ühtset definitsiooni, mida oleks järjekindlalt kasutatud.[21] Identiteedivarguse sisu avamisel on oluline ennekõike selgitada "identiteedi" mõistet identiteedivarguse kontekstis. Keelelises tähenduses on identiteeti defineeritud kui teadmist endast sotsiaalseis olukordades ja suhetes.[22] Õiguslikus mõttes ei ole identiteedi mõistet defineeritud, kuid autori hinnangul võiks seda mõista kui iseloomulike omaduste hulka, mis võimaldab ühe õigussubjekti eristamist teisest. Seega räägime isikulisest identiteedist, mis aitab isiku kellenagi ära tunda, samastada. Identiteedivargus ongi seotud eelkõige identifitseeriva informatsiooniga ega nõua, et kuriteo objektiks oleks ühe isiku terviklik identiteet.[23] Seejuures võib identiteedivarguse objektiks olla ka sünteesitud identiteet (*Synthetic identity*), kus kombineeritakse omavahel tükikesi erinevate isikute personaalsest informatsioonist ning luuakse fiktiivne identiteet.[24] Selliste juhtumite korral kasutatakse näiteks ühe isiku isikukoodi, kuid teise isiku nime. Identifitseeriva informatsiooni mõiste on samuti vägagi relatiivne, sõltudes kasutatud andmete iseloomust ja ka näiteks isikust kelle andmeid on kasutatud. Mõningatel juhtudel võib identifitseerimiseks piisata vaid isiku telefoninumbrist või e-maili aadressist, mida on erinevaid tehnilisi vahendeid kasutades võimalik seostada (*linking*) isiku kohta käiva muu informatsiooniga.[25]

Küll aga eeldab identiteedivargus võõrast identiteeti puudutavate andmete olemasolu. Kurjategijate jaoks on väärtuslikuks informatsiooniks igasugused ainulaadsed identifitseerimise andmed, nagu näiteks individuaalsed koodid. Ameerika Ühendriikides oli personaalse sotsiaalkindlustuse numbri (*Social Security Number - SSN)* kasutuselevõtu eesmärgiks luua isiku tulu täpse arvestamise võimalus. Siiski on see tänasel päeval kasutusel pigem identifitseerimisvahendina. Samas ei loodud aga sellele tõhusat turvasüsteemi, mistõttu on hakatud *SSN*-i kuritegelikult ära kasutama.[26] Käesoleva töö autor usub, et sama risk esineb

[21] M.Gercke. *op. cit 9*, p. 4.
[22] T. Erelt. *et al*. Eesti õigekeelsussõnaraamat ÕS 2013. Kirjakeele normi alus alates 1. jaanuar 2014. Tallinn: Eesti Keele Sihtasutus: 2013. Veebiväljaanne. – Arvutivõrgus: http://www.eki.ee/dict/qs/, 23.04.2014.
[23] M.Gercke, *op. cit 9* p. 18.
[24] C. J. Hoofnagle. Identity Theft: Making the Known Unknowns Known. Harvard Journal of Law & Technology 2007/1, p. 100-102.
[25] N. Mitchison, *et al*. Identity Theft. A discussion paper. European Commission Joint Research Centre. *Sine loco*: European Communities 2004, p. 16. Arvutivõrgus: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf, 12.03.2014.
[26] N. Mitchison, *op. cit 25* pp. 6-7.

Eestis kasutusel oleva isikukoodiga, mistõttu on selle kasutamise turvalisuse tagamiseks vajalik pidevalt arendada olemasolevaid ning luua täiendavaid ja efektiivseid kaitsemeetmeid.[27] Käesoleval ajal ei laiene isikukoodile isikuandmete kaitse seadusest tulenevad delikaatsete isikuandmete töötlemist kaitsvad sätted. Kuivõrd isikukoodi kasutatakse aga üsna tihti identifitseerimisvahendina, siis võib selle käsitlemine avaliku informatsioonina soodustada identiteedivarguste toimepanemist. Seda põhjusel, et isikukoodi kombineerimine isiku aadressi või telefoninumbriga võib kurjategijale anda head võimalused erinevate asutuste tuvastamisprotsesside läbimiseks.[28] Seetõttu tuleks autori hinnangul kaaluda isikukoodi klassifitseerimist delikaatsete isikuandmete alla ning edaspidi avaliku identifitseerimisvahendina kasutada isiku ees- ning perekonnanime kõrval vaid isiku sünniaega, keelates seega avalikult märkida isikukoodi erilised neli viimast numbrit.

On selge, et majandusliku kasu saamise eesmärgil tegutsevate kurjategijate jaoks on kõige väärtuslikum saada juurdepääs isiku pangakontole ning muude finantslepingute sõlmimiseks vajalikele andmetele. Sellegipoolest soodustavad identiteedivargust ka finantssfääri mittekuuluvate internetiteenuste nagu näiteks suhtlusportaalide "facebook"[29], "myspace"[30] ning "rate"[31] kasutajakontode informatsioon, kus inimesed kannavad osa enda igapäevaelu tegevustest üle internetti. Andmeid, mida isikud nendel lehekülgedel avaldavad on lihtne kätte saada ning kuritegelikel eesmärkidel ära kasutada. Mida rohkem inimesed enda andmeid internetis avaldavad ning mida rohkem on kurjategijatel võimalik isikute kohta käivat informatsiooni koguda, seda lihtsam on kuritegelikke vahendeid kasutamata luua teisest isikust terviklik profiil, mida kasutades identiteedivargusi toime panna.[32]

See, millises mahus ja millise iseloomuga teise isiku personaalsete andmete hankimine, valdamine, töötlemine või muul viisil kasutamine moodustab identiteedivarguse koosseisu sõltub aga juba konkreetsest kriminaliseerivast sättest. Ameerika Ühendriikides kasutatakse

[27] 2005.a. on õiguskantsler Allar Jõks leidnud, et isikukoodi avalikustamine rikub põhiõigusi. Toonane õiguskantsler leidis, et "Eestis on isikut tuvastavaks tunnuseks valitud universaalne isikukood. Kuid kui universaalne tunnus on igaühele vabalt kättesaadav, võib suureneda oht selle kuritarvitamiseks". Vt: A. Pau (toim). Jõks: isikukoodide vaba avaldamine rikub põhiõigusi. Eesti Rahvusringhääling (ERR) 2005. Arvutivõrgus: http://uudised.err.ee/v/05b3d228-3da9-47d0-9d4b-ac28ed767d8f, 02.05.2014. Ka täna on Andmekaitse Inspektsioon endiselt seisukohal, et: "Isikukood kuulub tavaliste, mitte delikaatsete isikuandmete hulka. Isikukood avalikustatakse, kui on vaja konkreetset isikut tuvastada (ühenimeliste isikute puhul). Samuti võib isikukoodi asemel avalikustada vaid sünniaja." Vt: Andmekaitse Inspektsioon. Isikukood. Arvutivõrgus: http://www.aki.ee/et/kas-isikukood-delikaatne, 12.03.2014.

[28] B.Givens. Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions. Written Testimony for U.S. Senate Judiciary Subcommittee on Technology, Terrorism and Government Information Senator Jon Kyl, Chairman. Arvutivõrgus: https://www.privacyrights.org/ar/id_theft.htm, 12.03.2014.

[29] www.facebook.com, 23.04.2014.

[30] www.myspace.com, 23.04.2014.

[31] www.rate.ee, 23.04.2014.

[32] M.Gercke, *op. cit 9*, pp. 7, 16-17.

identifitseerimisvahendi (*means of identification*) mõistet, mida on defineeritud, kui mis tahes nime või numbrit, mis kas üksikult või koos teiste andmetega kasutades võimaldavad identifitseerida konkreetset isikut.[33] Kuivõrd töö teises peatükis analüüsitakse KarS §-s 157[2] sätestatud identiteedivarguse koosseisutunnuseid, siis käsitleb autor Eestis identiteedivargust reguleeriva sätte koosseisus silmas peetud tuvastavaid või tuvastamist võimaldavaid andmeid täpsemalt alapeatükis 2.2.1.

1.1.2 Isikuandmete hõivamise viisid

Isikuandmete saamiseks on mitmeid viise. Kõige lihtsam neist on näiteks rahakoti või mobiiltelefoni vargus, mis enamikel juhtudel sisaldavad isikuttõendavaid dokumente või andmeid, samuti krediit- ning pangakaarte või nende kohta käivat informatsiooni ja halvimal juhul isegi erinevaid paroole.[34] Olgugi, et selliseid vargusi ei saa pidada arvutiga seotud õigusrikkumisteks, siis on siiski ka füüsiliste meetodite abil võimalik koguda isikute kohta käivaid personaalseid andmeid, mida saab hiljem arvuti ning internetiga seotud identiteedivargustes kuritegelikel eesmärkidel ära kasutada.[35]

Internetist kogutavateks isiku kohta käivateks andmeteks on kõige sagedanimi isiku enda poolt internetis avalikustatud andmed. Samas võib internetis isiku kohta käiva personaalse informatsiooni kogumine ja saamine nõuda ka suuremamahulist läbimõeldud eeltööd. Internetiga seotud identiteedivargused põhinevad tavaliselt laiaulatuslikel skeemidel, kasutades ära kõiki tehnilisi vahendeid ning interneti võimalusi. Üks levinumaid viise personaalsete isikuandmete leidmiseks infotehnoloogia võimalusi kasutades on otsida neid kustutatud andmete hulgast ning taastada personaalseid andmeid sisaldavaid dokumente (*Dumpster diving).*[36] Lisaks sellele on väga levinud ka maskeeringut kasutavad skeemid, kus luuakse usaldusväärne sisend elektroonilises suhtluses, näiteks saadetakse ohvrile usaldusväärse isikuna mingi e-kiri, milles palutakse tal saata enda kohta käivaid andmeid või lisatakse ohvrile saadetavale e-kirjale viide veebiaadressile, mis on omakorda nakatatud paha- või nuhkvaraga. Kui isik avab nimetatud veebiaadressi, siis annab ta sellega juurdepääsu enda

[33] U.S. C. Title 18, Part I, Chapter 47, § 1028, Subsection (d), p 7.
[34] N. Mitchison, *op. cit 25*, p. 18.
[35] 2010.a. Ameerika Ühendriikides läbiviidud uuringus osalejatest 34% oli langenud mobiiltelefoni varguse või kaotamise ohvriks. Suurem osa, 69% oli kogenud enda arvuti nakatamist pahavaraga. Vt: Computer Security Institute. 2010/2011 Computer Crime and Security Survey, p. 17. Arvutivõrgus: http://gocsi.com/survey, 12.03.2014. Eeltoodust nähtub, et internetis kasutatavad informatsiooni hankimise vahendid muutuvad üha populaarsemaks. Samal ajal tuleb aga olla väga tähelepanelik milliseid isikuandmeid me igapäevaselt füüsiliselt kaasas kanname, sest ka vargusega kogutud informatsiooni võib kurjategija hiljem identiteedivarguse toimepanemiseks ära kasutada.
[36] Federal Deposit Insurance Corporation (FDIC). Putting an end to Account-Hijacking Identity Theft, pp. 10-11, Arvutivõrgus: http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf, 30.04.2014.

kontoga seotud andmetele nagu näiteks kasutajanimed, salasõnad, krediitkaardi informatsioon ja palju muud (*Phishing)*. [37] Neljakndaks tihti kasutatavaks meetodiks on andmete kuritarvitamine nendele juurdepääsu omavate inimeste poolt. Selliselt müüvad või kasutavad klientide andmeid omavate ettevõtete töötajad personaalseid isikuandmeid identiteedivarguste toimepanemiseks.[38] Viienda levinud meetodina toob autor välja isikuandmete varastamise läbi erinevate finantsettevõtete või teenusepakkujate andmebaaside, kes omavad enda klientide kohta väga väärtuslikku personaalset teavet. [39] Samuti saab isikuandmetele juurdepääsu nakatades personaal- või üldkasutatavaid arvuteid nuhkvara või pahavaraga (*Malware või ka Spyware*)[40], mille tööeesmärgiks on koguda arvutites sisalduvat informatsiooni.

1.1.3. Isikuandmete kogumise eesmärgid

Hoolimata sellest, millist meetodit andmete saamiseks kasutatakse, on teise isiku personaalsete isikuandmete kogumine enamikel juhtudel suunatud edasiste kuritegude toimepanemisele ega piirdu ainult andmete hõivamise endaga.[41] Pahatihti on need kuriteod suunatud varalise kasu saamisele. Sellistel juhtudel taotletakse identiteedivarguse ohvri nimel krediitkaarte või laene, samuti sõlmitakse mobiiltelefonilepinguid ning üüri- ja rendilepinguid ning arved jäetakse tasumata.[42] Seetõttu on identiteedivargused lisaks arvulisele rohkusele ka üheks enim majanduslikku kahju tekitavaks kuriteoks tänapäevases ühiskonnas.[43] Eeltoodust tuleneb omakorda identiteedivarguste tugev seos riikide majandusega. Näiteks lähevad identiteedivarguse juhtumid Ühendkuningriigis riigile maksma ligikaudu 1,3 miljardit Briti naela aastas, Austraalias 1-3 miljardit USA dollarit aastas ning Ameerika Ühendriikides oli kahju 2005. aastal 56,6 miljardit USA dollarit.[44]

Võttes arvesse, milliseid kahjusid identiteedivargused maailma majandusele tervikuna igal aastal põhjustavad, on selge, et tuleb astuda täiendavaid samme identiteedivarguste

---

[37] FDIC, *op. cit 36,* pp. 6-9.
[38] B. Givens, *op. cit 28.*
[39] UNODC, *op. cit 10*, p. 16.
[40] Enim kasutatud personaalsete isikuandmete kogumise meetodeid on käsitletud ning selgitatud mitmetes internetiga seotud identiteedivargusi puudutavates artiklites ning uurimustes, millest on käesolevas töös välja toodud 5 peamist meetodit. Sisu täpsema ning tehnilisema selgituse ja vähemlevinud meetodite kohta täpsemalt vt: FDIC. *op.cit 36,* pp. 6-11; Organization for Economic Co-operation and Development (OECD). Analysis on "Online Identity Theft". *sine loco:* OECD 2009, pp. 8-9, 21-32. Edaspidi allmärkustes OECD 1; Microsoft Corporation. Online Identity Theft: Changing the Game. Redmond: Microsoft Corp. 2008, p. 3. Arvutivõrgus: http://blogs.technet.com/b/identity/archive/2010/03/30/a-microsoft-perspective-on-online-identity-theft-2008.aspx, 12.03.2014.
[41] M.Gercke. *op. cit 9*, p. 17.
[42] B.Givens. o*p. cit 28.*
[43] Javelin Stragedy & Report. 2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters. Selected Key Findings. Arvutivõrgus: https://www.javelinstrategy.com/brochure/276, 12.03.2014.
[44] M.Gercke. *op. cit 9*, pp. 5-6.

tõkestamiseks. Siiski võib peale majandusliku kasu saamise eesmärgi identiteedivarguste toimepanemine olla seotud ka teistsuguste motiividega. Nii võib personaalsete andmete kogumine olla toime pandud eesmärgiga kedagi laimata, solvata või hoopiski müüa informatsioon edasi kolmandatele osapooltele.[45] Samuti võib eesmärgiks olla enda identiteedi varjamine selleks, et vabaneda kriminaalvastutusest.[46] Viimati nimetatud juhtumeid on esinenud ka Eestis. Näiteks on Riigikohus 6. novembril 2013.a prokuratuuri teistmisavalduse alusel tühistanud esimese astme kohtuotsuse seoses sellega, et KarS § 424 järgi kvalifitseeritavas kuriteos süüdi mõistetud isik ei saanud toime panna nimetatud kuritegu ning esineb põhjendatud kahtlus, et vaidlustatud kohtuotsuse esemeks oleva kuriteo pani toime isik, kes on end kriminaalmenetluse vältel, sealhulgas maakohtus, esitlenud teise isikuna.[47] Toodud näide on siiski ainult üks mitmest Eesti kohtupraktikas ette tulnud intsidendist.

1.1.4. Identiteedivarguse rahvusvahelisus

Enamasti on internetiga seotud identiteedivargus internatsionaalne nähtus ega tunne riigipiire, ühendades sealjuures pea kõiki riike maailmas. Nii on näiteks võimalik, et Saksamaal elav kurjategija varastab Singapuri kodaniku pangakontolt 10 000 eurot ja tema isikuandmed ning viimasena esinedes ründab Ameerika Ühendriikide karistusregistrit haldavat infosüsteemi. Karistusregistri infosüsteemist kopeerib kurjategija mitmete Mehhiko kõrgete riigiametnike karistusandmed ning avaldab seejärel need internetis, põhjustades sellega viimastele kahju kokku summas 150 000 eurot. Meedias kajastatakse kurjategijana Singapuri kodanikku, kes investeerimisettevõtte juhina kaotab ajakirjanduse halva reklaami tõttu pea pooled oma klientidest, tuues sellega kaasa ulatusliku kahju summas 500 000 eurot. Seega on nimetatud kuriteoga Singapuri kodanikule tekitatud kahju kokku summas 510 000 eurot.

Nimetatud juhtumi puhul on tegemist mitme erineva kannatanuga. Esiteks on identiteedivarguse ohvriks langenud ning selle tõttu suurt majanduslikku kahju kannatanud Singapuri kodanik, teiseks Ameerika Ühendriikides infosüsteemi vastu suunatud ründe ohvriks langenud karistusregistrit pidav asutus ning kolmandaks kõik need Mehhiko riigiametnikud, kelle andmeid kopeeriti ning avaldati.

[45] M.Gercke. *op. cit 9*, p. 17.
[46] B.Givens. *op. cit 28.*
[47] Riigikohtu kriminaalkolleegiumi otsus (RKKKo) 06.11.2013, 3-1-2-10-13. (Põhja Ringkonnaprokuratuuri ringkonnaprokurör Rainer Amuri teistmisavaldus Harju Maakohtu 20. märtsi 2013. a kohtuotsuse peale kriminaalasjas Egert Ostraki süüditunnistamises KarS § 424 järgi). Sarnaseid juhtumeid on Eesti kohtupraktikas ette tulnud veel teisigi, näiteks: Harju Maakohtu otsus (HMKo) 07.06.2010, 1-10-1119. ((Marko Rohtlaan'e süüdistuses KarS § 424 järgi). Toodud lahendiga mõistis kohus õigeks Marko Rohtlaan'e süüdistuses KarS § 424 järgi seoses prokuröri poolt esitatud süüdistusest loobumisega kohtuistungil, kuivõrd süüdistuses kirjeldatud tegu ei olnud toime pannud Marko Rohtlaan.

Muutes situatsiooni näiliselt veelgi keerulisemaks, siis oletame, et Singapuris ning Mehhikos ei ole identiteedivargus kriminaalkorras karistatavaks teoks ning infosüsteemi loata tungimine ja sealt andmete kopeerimine ja avaldamine täidavad vaid väärteokoosseisu, seejuures nii Saksamaal kui Ameerika Ühendriikides on nii identiteedivargus kui ka infosüsteemide vastu suunatud rünne kuritegu. Seega tõusetub küsimus jurisdiktsioonist, milline riik peaks antud kuritegu menetlema. Kas riik, kus tekitati kuriteoga kõige rohkem kahju, kus pandi toime kuritegu, kus on täideviija elukoht, kus on kuriteo tagajärje saabumise koht või kus asub rünnatud infosüsteemi haldav asutus. Selline situatsioon võib tuua kaasa olukorra, kus jurisdiktsiooni taotlevad kõik asjasse puutuvad neli riiki või olukorra, kus seda ei taotle ükski eeltoodud riikidest.[48] Nimetatud näite näol on tegemist küll eelkõige jurisdiktsiooni ning kohtualluvust puudutava küsimusega, mis on pigem kriminaalmenetlusõiguslik probleem ega kuulu seega käesoleva töö uurimissfääri. Siiski illustreerib toodud näide väga ilmekalt seda, miks küberkuritegevuse, sealjuures ka internetiga seotud identiteedivarguste puhul on oluline rahvusvaheline koostöö.

Tähelepanu väärib ka asjaolu, et laiaulatuslikke identiteedivarguse juhtumeid on ette tulnud ka praktikas. Näiteks on Ameerika Ühendriikide üheks suurimaks identiteedivarguse juhtumiks peetud 2011. aastal aset leidnud intsidenti, kus ühele abielupaarile laekus informatsiooni paljude erinevate isikute kohta erinevatest riikidest nagu näiteks Venemaalt ning Hiinast. Isikuandmete kogumiseks kasutati erinevaid meetodeid, erinevaid informatsiooni koguvaid veebilehekülgi ning ka krediitkaardi informatsiooni salvestavaid seadmeid kauplustes ning mujal. Seejärel palkas abielupaar isikuid, kes varastatud informatsiooni kasutades ohvrite nimel erinevaid lepinguid sõlmisid. Kokku tekitasid nad enda tegevusega kahju ligikaudu 13 miljoni dollari ulatuses ning skeemi oli kaasatud 111 isikut.[49]

Selleks, et tagada isikute kaitse piiriüleste kuritegude puhul ning tõhustada riikidevahelist koostööd küberkuritegevuse vastases võitluses, on seeega vajalik, et tegu oleks kriminaliseeritud kõikides riikides. Samuti ei piisa ainult teo kriminaliseerimisest, vaid regulatsioon ja koosseisutunnused peaksid tõhusama koostöö saavutamiseks olema sätestatud ka võimalikult ühetaolisena. Selleks on ennekõike aga vaja leida identiteedivarguse mõiste ühtne definitsioon. Samal seisukohal on ka Majanduskoostöö ja Arengu Organisatsioon

[48] Positiivse ja negatiivse jurisdiktsioonikonflikti ja lahenduste kohta täpsemalt vt: S.W. Brenner, B.-J. Koops. Approaches to Cybercrime Jurisdiction. *Sine loco:* Journal Of High Technology Law, 2004/1, pp. 40-45, Arvutivõrgus: http://www.joemoakley.org/documents/jhtl_publications/brenner.pdf, 12.03.2014.

[49] A. Compton. Largest Identity Theft Case In U.S. History: Amar Singh And Wife, Neha Punjani-Singh, Plead Guilty To Massive Fraud. - The Huffington post 2012. Arvutivõrgus: http://www.huffingtonpost.com/2012/08/07/largest-id-theft-in-history_n_1751241.html, 30.04.2014.

(*Organization for Economic Co-operation and Development*, OECD), tuues välja, et: "ka OECD liikmesriikides on identiteedivargus defineeritud erinevalt: mõned riigid käsitlevad seda kui spetsiifilist kuritegu, samal ajal osad riigid lähenevad sellele kui teiste õigusvastaste tegude või kuritegude ettevalmistusstaadiumile. Ühtse definitsiooni puudumine muudab keeruliseks piiriülese ning kõikehõlmava lahenduse leidmise.[50]" Teise suure takistusena toob OECD välja võrreldavate andmete puudumise, sest kuivõrd kõik riigid ei vaatle identiteedivargust eraldi kuriteona, siis puuduvad hetkeolukorra hindamist võimaldavad statistilised andmed.[51]

1.1.5. Identiteedivarguse defineerimine

Võttes arvesse identiteedivarguse toimepanemise laiaulatuslikult varieeruvaid eesmärke, ühendab nimetatud kuritegu mitmeid erinevaid valdkondi ja huvigruppe olles seotud näiteks nii privaatsuse, turvalisuse kui ka tarbijakaitsega.[52] Ühtse definitsiooni loomise peamiseks takistuseks ongi see, et identiteedivargusest esineb mitmeid erinevaid variante[53], mis toob kaasa identiteedivargusega seotud juhtumeid tähistavate terminite rohkuse ja nende kasutamise järjepidamatuse[54]. Näiteks on teise isiku andmete kasutamisega seotud juhtumite puhul kasutatud ka termineid "identiteedipettus (*identity fraud*)[55]", "konto ülevõtmine (*account takeover*)" ning "konto kaaperdamine (*account hijacking*)".[56]

Termini kasutamise kõrval on püütud õiguskirjanduses identiteedivargust defineerida ka teo elementide kirjeldamise kaudu. Näiteks on B. Givens leidnud, et: "identiteedivargus esineb siis, kui keegi kasutab teise isiku kohta käivat informatsiooni selleks, et kuritegelikel eesmärkidel temana esineda."[57] Majanduskoostöö ja Arengu Organisatsioon (*Organization for Economic Co-operation and Development*, OECD) on identiteedivargust defineeritud järgmiselt: "Identiteedivargus esineb siis kui üks pool omandab, vahendab, valdab või kasutab füüsilise või juriidilise isiku personaalset informatsiooni ebaseaduslikult internetis seoses

[50] OECD 1, *op. cit 40*, p. 9.
[51] *Ibid*, p. 9.
[52] *Ibid*, p. 3
[53] B.Givens, *op.cit 28.*
[54] M.Grecke, *op. cit 9*, p. 10.
[55] Termin "identiteedipettus" on kasutusel näiteks Ühendkuningriikides. Identiteedivarguse sellise terminiga tähistamise peamiseks põhjuseks on see, et Ühendkuningriigis ei ole identiteedivargus karistatav *per se*, vaid ainult juhul, kui sellele järgneb kriminaalne või pettuslik tegu. Vt: N. Mitchison. *op. cit 29*, p. 23.
[56] M.Grecke, *op. cit 9*, p 10. Arutluspaberi punktis 3.1.1. toob M. Gercke välja konkreetsed näited identiteedivargusega seotud terminite kasutamisest erinevates uuringutes ning publikatsioonides.
[57] B.Givens. *op. cit 28.*

pettuse või teiste kuritegudega." [58] Üks paljudest lähenemistest on samuti, et: "identiteedivargus on võõra identiteedi varastamine või ülevõtmine, selle isiku nõusolekul või nõusolekuta, hoolimata sellest, kas isik on surnud või mitte".[59] Lisaks on identiteedivargust õiguskirjanduses defineeritud, kui: "kuritegelikku tegevust, kus kuriteo täideviija pettuslikul viisil hangib ning kasutab teise isiku identiteeti."[60]

Samuti leidub erinevaid definitsioone eri riikide identiteedivargusi reguleerivatest sätetest.[61] U.S.C. kohaselt esineb identiteedivargus siis, kui isik "teadvalt edastab, valdab või kasutab, ilma seadusest tuleneva õiguseta teist isikut identifitseerida võivaid vahendeid, kavatsusega panna toime või abistada või kihutada või seoses mistahes föderaalseadust *(Federal law*) rikkuva ebaseadusliku tegevusega või tegevusega, mis on kuritegu mistahes kohaldatava riigi või kohaliku õiguse alusel."[62] Paljudes riikides ei ole siiski aga identiteedivargus eraldi kuriteona sätestatud, vaid identiteedivarguse sisule vastavad tegevused on kriminaliseeritud läbi teiste kuritegude.[63] Nii puudub näiteks Ühendkuningriikides konkreetne eriregulatsioon, kuid identiteedivargusele omaseid elemente on kriminaliseeritud seoses pettusega ning ka isikut tõendava dokumendi võltsimisega.[64] Ka Eesti karistusseadustikus on samuti võimalik leida mitmeid teisi identiteedivargustega seotud juhtumeid reguleerivaid kuriteokoosseise nagu näiteks kelmus (KarS § 209), arvutikelmus (§ 213) või ka tähtsa isikliku dokumendi kuritarvitamine (KarS § 349).

1.1.6. Üldised ühised põhimõtted identiteedivarguse reguleerimisel

Nagu eeltoodust nähtub, on identiteedivargusel mitmeid erinevaid lähenemisviise. Mõnel juhul hõlmab definitsioon võõra identiteedi kasutamist seoses kuritegeliku tegevusega. Teisel juhul peetakse identiteedivarguseks juba seda, kui on varastatud või üle võetud teise isiku identiteet, sidumata sellega nende kasutamist kuritegelikus tegevuses või veelgi enam

[58] OECD. Policy Guidance on Online Identity Theft. Seoul: OECD 2008, p. 2. Arvutivõrgus: http://www.oecd.org/sti/consumer/40879136.pdf, 24.04.2014 Edaspidi allmärkustes: OECD 2

[59] M.Grecke, *op. cit 9*, p. 10.

[60] M. Peeters. Identity theft scandal in the US: Opportunity to improve data protection. München: Multimedia und recht 2005/7, p. 415.

[61] Ülevaade Ameerika Ühendriikides termini "identiteedivargus" kasutamisest erinevates õigusaktides vt: M.Grecke. *op. cit 9*, p. 12. Lisaks leiab nii Euroopa riikide kui ka Ameerika Ühendriikide identiteedivargust reguleerivate sätete kohta ülevaate näiteks: N. Mitchison, *op. cit 25*, pp. 23-26.

[62] U.S.C., Title 18, Part I, Chapter 47, § 1028, Subsection (a), p 7.

[63] N. Mitchison, *op. cit 25*, p. 24.

[64] Ühendkuningriigis võib leida isikuandmete töötlemisega, isikukaartide kasutamisega ja erinevate pettustega seotud regulatsioonidest ka identiteedivarguse mõistega seotud elemente kriminaliseerivaid sätteid või nende osi. Vt: Data Protection Act. - 1998. c 29. Arvutivõrgus: http://www.legislation.gov.uk/ukpga/1998/29/contents, 12.03.2014; Identity Cards Act. - 2006. c 15. Arvutivõrgus: http://www.legislation.gov.uk/ukpga/2006/15/contents, 12.03.2014, Fraud Act. - 2005. c 35. Arvutivõrgus: http://www.legislation.gov.uk/ukpga/2006/35/contents, 12.03.2014.

kasutamist üldse. Samuti jätab mõni definitsioon välja isikuandmete saamise viisi, öeldes, et ei ole oluline, kas selleks oli teise isiku nõusolek või mitte. Viimases eelmises alapeatükis toodud õiguskirjanduses kasutatud definitsiooni puhul mängib aga erilist rolli just isikuandmete saamise viis, leides, et identiteedivargus esineb vaid juhul, kui kasutatav võõra isiku identiteet on saadud pettuslikul teel.

Nagu autor juba eelnevalt mainis, on internetiga seotud identiteedivargustele iseloomulikku piiriülesust silmas pidades selle tõkestamisel esmajärjekohal just rahvusvaheline koostöö. Samal seisukohal on ka Euroopa Komisjon, kes 2007. aastal märkis, et õiguskaitseorganite koostööd oleks Euroopa Liidus lihtsam tagada, kui identiteedivargus oleks kriminaliseeritud kõikides liikmesriikides.[65] Seega on erinevatest definitsioonidest tulenevate ühiste põhimõtete väljaselgitamine identiteedivargust reguleerivate õigusaktide väljatöötamise ja ühtlustamise kohustuslikuks eeltingimuseks.[66]

Erialakirjanduses kasutatud ning riikide identiteedivargusi kriminaliseerivates sätetes kasutatud mõistete rohkuse ja mitmekesisuse rägastikust ei ole võimalik leida käsitluste võrdlemise teel identiteedivargusele ühtset ning kõikehõlmavat definitsiooni. Küll aga leiab autor, et ka käesolevas töös välja toodud definitsioonide puhul saab nõustuda M. Gercke poolt leituga, mille kohaselt on ühise joonena iga identiteedivarguse käsitlus seotud vähemalt ühega neljast astmest:

1) Ettevalmistusstaadium;
2) Informatsiooni hõivamise (*obtain*) tegu;
3) Identiteediga seotud informatsiooni omamise või edastamise tegu;
4) Identiteediga seotud informatsiooni kasutamine kuritegelikel eesmärkidel.[67]

Ettevalmistusstaadiumina võib mõista näiteks internetist personaalsete isikuandmete leidmiseks vajalike programmide või skeemide väljatöötamist, mille kasutamine identifitseeriva informatsiooni leidmiseks kuulub aga juba teise faasi. Teise astme moodustavad ka kõik muud personaalsete isikuandmete saamist võimaldavate meetodite kasutamised. Kolmas faas eeldab tuvastamist võimaldavate isikuandmete olemasolu, hõlmateski selliste andmete omamise ning edastamise kolmandatele isikutele. Viimases,

[65] M. Gercke, *op.cit 9*, p. 6.
[66] *Ibid*, p. 10.
[67] M. Gercke, *op.cit 9*, pp. 19-20; M. Gercke, *et al*. Handbook on Identity-related Crime. UNODC 2011, pp. 31-33. Arvutivõrgus: http://www.unodc.org/documents/treaties/UNCAC/Publications/Handbook_on_ID_Crime/10-57802_ebooke.pdf, 12.03.2013.

neljandas astmes on tegevus seotud kogutud andmete kasutamisega kuritegelikel eesmärkidel õigusrikkumiste toimepanemiseks.

Käesoleva töö autor on seisukohal, et isikutele peaks olema tagatud kaitse kõikides eelnevalt loetletud identiteedivarguse faasides. Võttes arvesse identiteedivarguste massilist kasvu on suuremate kahjude ärahoidmiseks vajalik ennetada ning tõkestada nimetatud kuritegude toimepanemist juba nende ettevalmistusfaasis. Samuti on oluline, et karistatav oleks lisaks teise isiku isikuandmete kasutamisele kuritegelikel eesmärkidel ka isikuandmete kogumine ning edastamine. Seega hindab töö autor järgnevas peatükis muuhulgas seda, kas tervikliku ning rahvusvahelist koostööd enam tagava kuriteokoosseisu puhul peaksid karistatava teo koosseisu kuuluma kõik neli eelnevalt loetletud identiteedivarguse etappi või tagab tõhusa kaitse juba see, kui vastutus tuleneb karistusõiguse üldsätetest või teistest kuriteokoosseisudest.

1.2. Eestit puudutavad rahvusvahelised identiteedivargust reguleerivad õigusaktid

1.2.1. Euroopa Nõukogu Arvutikuritegevusvastane konventsioon

1.2.1.1. Konventsiooni reguleerimisala

Arvutikuritegevusvastane konventsioon on ainuke rahvusvaheline konventsioon, mis tagab kõikehõlmava juriidilise raamistiku küberkuritegevuse vastasele võitlusele. [68] Arvutikuritegevusvastane konventsioon võeti vastu Euroopa Nõukogu Ministrite Komitee poolt 8. novembril 2001. aastal. [69] Arvutikuritegevusvastase konventsiooni loomise vajalikkuse tingis asjaolu, et uued tehnoloogilised lahendused esitavad olemasolevatele õiguslikele lahendustele uusi väljakutseid. Info- ning kommunikatsioonitehnoloogia levib üle maailma, mille abil panevad kurjategijad toime õigusrikkumisi ka riikides, kus nad ise ei asu. Riikide seadused piirnevad aga kindla territooriumiga, mistõttu tuleb uute tehnoloogiliste võimaluste tõttu tekkinud probleemid lahendada rahvusvahelisel tasandil, milleks on vajalik asjakohaste rahvusvaheliste õigusaktide vastuvõtmine. Sellest tulenevalt ongi Arvutikuritegevusvastase konventsiooni eesmärgiks tagada inimõiguste kaitset üha arenevas infoühiskonnas.[70] Konventsiooni on ratifitseerinud 42 riiki. Euroopa Nõukogu liikmetest ei ole konventsiooni ratifitseerinud Andorra, Kreeka, Iirimaa, Lichtenstein, Luksemburg,

[68] M. Gercke, *op. cit 9*, p. 6.
[69] Council of Europe. Convention on cybercrime. Explanatory report, p I. Arvutivõrgus: http://conventions.coe.int/Treaty/EN/Reports/html/185.htm, 30.04.2014. Edaspidi allmärkustes: C.C. Explanatory report.
[70] C.C. Explanatory report, chap. I, p 6.

Monaco, Poola, Venemaa, San Marino, Rootsi ega Türgi. Samas on konventsioon ratifitseeritud sellistes suurriikides nagu Ameerika Ühendriigid, Austraalia ning Jaapan.[71]

Arvutikuritegevusvastane konventsioon on suunatud küll küberkuritegevusvastasele võitlusele, kuid ei sisalda ega defineeri siiski eraldi isikuandmete väärkasutamisega seonduvaid küberkuritegusid. Seega ei kata konventsioon ka kõiki võimalikke personaalse informatsiooni väärkasutamise juhtumeid. Arvutikuritegevusvastase konventsiooni eesmärk on ühtlustada Euroopa Nõukogu liikmesriikide ning teiste konventsiooniga liitunud riikide regulatsioone ning koostööd arvutikuritegevuse vastases võitluses. Selleks sätestab konventsioon siseriikliku kriminaalmenetlusõiguse volitused, mis tagaksid uurimisasutustele ja prokuratuurile efektiivse menetluse arvutisüsteemide abil toime pandud kuritegudes ning digitaalsete tõenditega seotud kuritegudes.[72] Samuti sisaldab kataloogi kuritegudest, mis peaksid konventsiooniga liitunud riikide siseriikliku õiguse alusel olema kriminaliseeritud.

Käesoleva töö autor peab vajalikuks märkida, et kuigi Arvutikuritegevusvastane konventsioon ei reguleeri konkreetselt identiteedivargust, ei ole konventsioon identiteedivarguse elementide reguleerimisel siiski täiesti asjakohatu. Eelnevas alapeatükis on autor välja toonud identiteedivarguse puhul eristatavad etapid. Arvutikuritegevusvastase konventsiooni sätted ei käsitle küll sõnaselgelt identiteedivargust, kuid teiste kuritegude reguleerimise kaudu on siiski enamus identiteedivarguse astmed konventsioonist puudutatud.[73]

1.2.1.2. Konventsioonis sisalduv identiteedivarguse regulatsioon

Arvutikuritegevusvastase konventsiooni osalised on konventsiooni Art 6 järgi kohustatud kriminaliseerima tahtlikult ning õigusliku aluseta arvutisüsteemi või selle osasse ebaseaduslikku sisenemist, arvutiandmete pealtkuulamist, arvutiandmetesse või arvutisüsteemi sekkumist võimaldavate arvutiprogrammide või salasõnade tootmise, müümise, kasutamiseks hankimise, importimise, turustamise või muul viisil kättesaadavaks tegemise. Selliselt reguleerib konventsioon identiteedivarguse ettevalmistusstaadiumit, olukorras, kus selline arvutiprogramm või salasõna on loodud just personaalsete isikuandmete hankimise eesmärgil ning seda on kavas toime panna teistes konventsiooni artiklites sätestatud kuritegelikel viisidel. Samuti seondub ettevalmistusstaadiumiga Arvutikuritegevusvastase konventsiooni Art-s 7 sisalduv arvutiandmete võltsimise säte.

[71] Council of Europe. Treaty Office. Convention on Cybercrime. Status as of 12.03.2014. Arvutivõrgus: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG, 30.04.2014.
[72] C.C. Explanatory report, p. 16.
[73]Arvutikuritegevusvastase konventsiooni seost identiteedivaguse ning selle eri etappidega on käsitlenud ka M. Gercke. Vt: M. Gercke *op.cit 9*, lk 22.

Nimetatu on seotud eelkõige *phishing* skeemidega, kus võltsitakse isikutele saadetavaid e-kirju, et nakatada arvuteid nuhkvaraga või saada muul viisil juurdepääs arvutis olevatele andmetele.[74]

Muuhulgas võib Arvutikuritegevusvastase konventsiooni Art-s 2 sätestatud arvutisüsteemi või selle osasse ebaseaduslik sisenemine *per se* olla seotud eesmärgiga koguda teise isiku personaalseid isikuandmeid. Samuti Arvutikuritegevusvastase konventsiooni Art-s 3 sisalduv arvutiandmete pealtkuulamine nende konfidentsiaalse edastamise ajal, kui pealtkuulatavateks andmeteks on isikuandmed ning seda tehakse kavatsusega neid hõivata. Samuti seondub pahavara kasutamise teel isikuandmete hõivamisega Arvutikuritegevusvastase konventsiooni Art 4, mis käsitleb andmetesse sekkumist ning mille kohaselt võtab konventsiooniosaline seadusandlikke ja muid meetmeid, et oma seaduses määratleda kuriteona arvutiandmete kustutamine, rikkumine, muutmine või sulustamine või muul viisil kahjustamine, kui see pannakse toime tahtlikult ja ilma õigusliku aluseta. Lisaks reguleerib isikuandmete hõivamist ka Art-s 5 sisalduv arvutisüsteemi toimimise takistamine arvutiandmete sisestamise, edastamise, kustutamise, rikkumise või sulustamise teel, kuid vaid juhul, kui sellega takistatakse oluliselt arvutisüsteemi toimimist.

Identiteedivarguse kolmandat astet reguleerivaid sätteid, mis oleksid seotud isikute kohta käiva informatsiooni omamise ja edastamisega, käesoleva töö autori hinnangul konventsioonist ei nähtu.

Neljanda astme puhul, mis on suunatud teist isikut identifitseerivate andmete kasutamisega kuritegude toimepanemisel, saab Arvutikuritegevusvastasest konventsioonist välja tuua Art-s 8 sisalduva arvutikelmuse, mille puhul peavad konventsiooniosalised võtma vastu 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. Selle regulatsiooni alla kuuluvad näiteks krediitkaardipettused, mis ongi üheks personaalsete isikuandmete kasutamise peamiseks eesmärgiks.[75]

[74] M. Gercke, *op.cit 9*, p. 29; FDIC. *op.cit 36*, pp. 6-9.
[75] M. Gercke, *op cit 9*, lk 27.

1.2.1.3 Kaitse- ja vastutusala

Kuivõrd Arvutikuritegevusvastane konventsioon ei ole suunatud otseselt isiku kohta käivate andmete kaitsele ning identiteedivarguse kriminaliseerimisele, siis ei ole võimalik võtta kindlat seisukohta, kas konventsioonist tulenevate isikuandmete väärkasutamisega seostatavate kuriteokoosseisude kaitseala võiks laieneda ka juriidiliste isikute kohta käivatele andmetele. Kaitse laieneb küll juriidilistele isikutele, kelle arvutiandmete või infosüsteemide vastu suunatud rünnete kaudu isikuandmeid hõivatakse, kuid andmete sisu kaitse ulatust konventsioonist ei tulene.

Oluline on ka selgitada, kas Arvutikuritegevusvastasest konventsioonist tulenevalt peaks nimetatud kuritegude toimepanemise eest vastutus laienema juriidilistele isikutele. Nii ütlebki konventsiooni Art 12 lg 1, et juriidilist isikut on võimalik vastutusele võtta, kui kuritegu on toime pandud juriidilise isiku kasuks ning seda kas iseseisvalt või juriidilise isiku organi liikmena tegutsev juhtkonda kuuluv füüsiline isik, kui sellisel isikul on õigus esindada, kontrollida või teha juriidilise isiku nimel otsuseid. Lisaks on konventsiooni artikli 12 lõikes 2 sätestatud, et juriidilist isikut võiks vastutusele võtta ka siis, kui juriidilise isiku alluvuses tegutsenud füüsilisel isikul on olnud võimalik panna juriidilise isiku kasuks toime konventsioonis nimetatud kuritegu, tulenevalt sellest, et nimetatud füüsilise isiku tegevuse üle teostatav järelevalve on olnud puudulik. Seega laieneb konventsiooni alusel vastutus juriidilistele isikutele identiteedivargusega seotud tegevuste eest, mida konventsioonis sisalduvad sätted reguleerivad.

1.2.2. Euroopa Parlamendi ja nõukogu direktiiv 2013/40/EL

1.2.2.1. Direktiivi reguleerimisala

Direktiivi 2013/40 eesmärkideks on ühtlustada liikmesriikides kehtivaid infosüsteemide vastu suunatud kuritegude regulatsioone ning muuta tõhusamaks koostööd liikmesriikide ning liidu pädevate asutuste ning organite vahel. Direktiivi 2013/40 preambula punktide 1, 4 ja 5 kohaselt moodustavad infosüsteemid olulise osa liidu poliitilisest, majanduslikust ja sotsiaalsest koostoimimisest. Võttes arvesse, et infosüsteemide vastu suunatud rünnete oht on kasvanud kogu maailmas, siis on oluline, et liidu tasandil oleks ühtne õiguslik raamistik, mis tagaks efektiivse kaitse liikmesriikide ja liidu elutähtsale infrastruktuurile.

Direktiivi 2013/40 preambula punkti 15 kohaselt tugineb nimetatud direktiiv Euroopa Nõukogu Arvutikuritegevusvastasele konventsioonile. Selliselt peavad liikmesriigid ka

direktiivi 2013/40 Art-st 3-8 tulenevalt kriminaliseerima mitmed olulisemad ning enam levinumad küberkuriteod, nendele kihutamise ning kaasaaitamise. Niisiis on direktiivi 2013/40 eesmärgiks sarnaselt Arvutikuritegevusvastasele konventsioonile reguleerida suuremaid ning ohtlikumaid küberkuritegusid piiriülesel tasandil, et tõhustada läbi ühetaolise regulatsiooni küberkuritegude menetlemist. Eeltoodust nähtub, et Euroopa Nõukogu, Euroopa Parlamendi ning Euroopa Liidu Nõukogu on korduvalt rõhutanud küberkuritegevuse vastase võitluse edendamise olulisust, mis kinnitab auori seisukohta, et ka identiteedivarguse puhul oleks tarvilik välja töötada ühetaoline regulatsioon, mille abil muutuks efektiivsemaks identiteedivarguste vastane võitlus ja kiireneks ning lihtsustuks selliste kuritegude menetlemine.

1.2.2.2. Direktiivis sisalduv identiteedivarguse regulatsioon

Kuivõrd direktiiv 2013/40 on olulisel määral seotud Arvutikuritegevusvastase konventsiooniga, siis leidub ka direktiivis 2013/40 sarnaselt konventsioonile kuritegusid, mis kaudselt identiteedivarguse erinevaid etappe reguleerivad. Selliselt kohustab direktiivi 2013/40 Art 7, sarnaselt Arvutikuritegevusvastase konventsiooni Art-le 6, liikmesriike tagama, et vähemalt raskemate juhtumite korral oleks karistatav infosüsteemi ebaseadusliku sisenemise, infosüsteemi ebaseadusliku häirimise, andmetesse ebaseadusliku sekkumise ja teabe ebaseadusliku pealtkuulamise jaoks loodud või kohandatud arvutiprogrammi või muude infosüsteemidesse sisenemist võimaldavate salasõnade, juurdepääsukoodide või muude samalaadsete andmete tahtlik tootmine, müük, kasutamiseks hankimine, importimine, levitamine või muul viisil kättesaadavaks tegemine õigusliku aluseta ja kavatsusega kasutada seda mõne eelnevalt loetletud kuriteo toimepanemiseks. Selliselt reguleerib ka direktiivi 2013/40 Art 7 identiteedivarguse ettevalmistusstaadiumit, kui arvutiprogramm või salasõna on loodud isikuandmete hankimise eesmärgil ning mida plaanitakse rakendada direktiivi 2013/40 Art-s 3-6 sätestatud viisidel.

Erinevalt Arvutikuritegevusvastase konventsiooni Art-s 7 sisalduvast, et näe direktiiv 2013/40 ette vastutust arvutiandmete võltsimisega seotud kuritegude eest, mis teatud juhtudel võib samuti kuuluda identiteedivarguse ettevalmistusstaadiumisse.

Samuti on sarnaselt Arvutikuritegevusvastasele konventsioonile arvutisüsteemi või selle osasse ebaseaduslik sisenemine reguleeritud direktiivi 2013/40 Art-s 3. Arvutikuritegevusvastase konventsiooni Art- 3 sisalduv arvutiandmete pealtkuulamine nende konfidentsiaalse edastamise ajal on sätestatud direktiivi 2013/40 Art- 6, mis on relevantne

identiteedivarguste seisukohalt siis, kui pealtkuulatavateks andmeteks on isikuandmed. Samuti seondub pahavara kasutamise teel isikuandmete hõivamisega sarnaselt Arvutikuritegevusvastase konventsiooni Art-le 4, direktiivi 2013/40 Art 5, mis käsitleb ebaseaduslikku andmetesse sekkumist. Lisaks ka direktiivi 2013/40 Art-s 4 sisalduv infosüsteemi töö tõsine takistamine või katkestamine arvutiandmete sisestamise, edastamise, kahjustamise, kustutamise, rikkumise, muutmise või sulustamise või ligipääsmatuks muutmise teel. Nimetatud kuriteod on identiteedivarguse teise, isikuandmete hõivamise etapi puhul asjakohased vaid osas, kus nimetatud teod pannakse toime seoses isikuandmete hõivamisega.

Isikute kohta käiva personaalse informatsiooni omamise ning edastamisega seonduvaid kuritegusid, sarnaselt arvutikuritegevusvastasele konventsioonile, ei nähtu ka direktiivi 2013/40 sätetest.

Neljanda astme puhul, mis on suunatud teist isikut identifitseerivate andmete kasutamisega kuritegude toimepanemisel, tõi autor Arvutikuritegevusvastase konventsiooni puhul välja Art-s 8 sisalduva arvutikelmuse. Nimetatud kuritegu direktiiv 2013/40 ei sätesta. Oluline on aga neljanda astme puhul direktiivi 2013/40 Art 9 p 5, mille kohaselt võtab liikmesriik vajalikud meetmed tagamaks, et kui Art-s 4[76] ja 5[77] osutatud kuriteod pannakse toime teise isiku isikuandmete väärkasutamise teel, eesmärgiga võita kolmanda isiku usaldus, ning tekitatakse seeläbi kahju identiteedi tegelikule omanikule, võib seda siseriikliku õiguse kohaselt käsitada raskendava asjaoluna, välja arvatud juhul, kui need asjaolud kuuluvad teise siseriikliku õiguse alusel karistatava kuriteo koosseisu. Kusjuures selline direktiivis 2013/40 sisalduv regulatsioon toob sisuliselt kaasa asjaolu, et kui Art-s 4 ning 5 nimetatud kuriteod on toime pandud isikuandmete hõivamiseks, siis on selliste tegude puhul raskendavaks asjaoluks see, kui isik on enda identiteeti varjanud.

Direktiivi 2013/40 Art 9 p-s 5 sisalduva näol on tegemist ainsa sättega Eestit puudutavatest rahvusvahelistest õigusaktidest, mis otseselt identiteedivargusega seonduvat reguleerib. Samas, nagu eeltoodust nähtub, ei ole tegemist kohustusliku ettekirjutusega. Liikmesriik võib raskendava asjaoluna identiteedivarguse infosüsteemide vastu suunatud rünnete korral ette

[76] Direktiivi 2013/40, *op.cit 16*, artikkel 4 sätestab, et: "Liikmesriik võtab vajalikud meetmed tagamaks, et tahtlikult ja õigusliku aluseta infosüsteemi töö tõsine takistamine või katkestamine arvutiandmete sisestamise, edastamise, kahjustamise, kustutamise, rikkumise, muutmise või sulustamise või ligipääsmatuks muutmise teel on vähemalt raskemate juhtumite puhul kriminaalkorras karistatav."

[77] *Ibid*, artikkel 5 sätestab**:** "Liikmesriik võtab vajalikud meetmed tagamaks, et tahtlikult ja õigusliku aluseta infosüsteemis olevate arvutiandmete kustuta mine, kahjustamine, rikkumine, muutmine või sulustamine või ligipääsmatuks muutmine on vähemalt raskete juhtumite puhul kriminaalkorras karistatav."

näha, kuid kriminaliseerimise üle otsustamiseks on jäetud liikmesriigile diskretsiooniõigus. Samas ütleb direktiivi 2013/40 preambula, et identiteediga seonduvate kuritegude suhtes tuleks hinnata liidu tasandil ulatuslike horisontaalsete meetmete vastuvõtmise vajadust. Eeltooduga väljendab Euroopa Liit kavatsust luua täiendavaid meetmeid identiteedivarguste kriminaliseerimiseks liidu tasandil. Samuti on ka Euroopa Liidu Nõukogu 8.-9.11.2007 avaldatud pressiväljaandes leidnud, et tuleks kaaluda, kas identiteedivargus tuleks iseseisva kuriteona kriminaliseerida kõikides liikmesriikides.[78] Seega on ka Euroopa Liidu tasandil sedastatud identiteedivarguse kriminaliseerimise vajalikkust.

Lisaks tuleneb direktiivi 2013/40 preambula p-st 4, et identiteedivarguse ja teiste identiteediga seonduvate kuritegude vastu võitlemiseks kehtestatud meetmed on oluliseks elemendiks küberkuritegevuse vastase võitluse integreeritud lähenemisviisis. Euroopa Majandus- ja Sotsiaalkomitee arvamuse kohaselt on samuti asjakohane rakendada rangemaid karistusi, kui süütegu on toime pandud täideviija identiteeti varjates ja tegelikku identiteedi omanikku kahjustades, et need toimiksid kurjategijatele reaalse hirmutusvahendina.[79] Euroopa Komisjoni ettepaneku "Euroopa Parlamendi ja Nõukogu direktiiv, milles käsitletakse infosüsteemide vastu suunatud ründeid ja millega tunnistatakse kehtetuks nõukogu raamotsus 2005/222/JSK" kohaselt oli esialgne kavatsus määrata ka täideviija tegelikku identiteeti varjates ja tegelikku identiteedi omanikku kahjustades toime pandud infosüsteemide vastu suunatud kuritegude eest kriminaalkaristus, mille maksimaalne määr on vähemalt viieaastane vangistus.[80] Jõustunud direktiivi 2013/40 sätetes on identiteedivargusega seotud rünnete puhul siiski loobutud vangistuse maksimaalse alammäära kehtestamisest.

Eestis on identiteedivargus kriminaliseeritud eriregulatsiooniga, millistel juhtudel ei pea direktiiv 2013/40 vajalikuks enam täiendavalt raskendavate asjaolude sätestamist Art-tes 4 ning 5 loetletud kuritegude puhuks. Sõnastusest nähtub, et raskendava asjaoluna võiks identiteedivarguse sätestada juhul, kui siseriiklikult ei kuulu eraldi kuriteokoosseisu kõik direktiivi 2013/40 Art 9 p-s 5 nimetatud asjaolud. Siinkohal peab autor tarvilikuks aga

[78] Council of the European Union, Justice and Home Affairs, Press Release, 2827th Council meeting, Brussels: 8-9.11.2007, p. 20. Kättesaadav arvutivõrgus: http://europa.eu/rapid/pressReleasesAction.do?reference=PRES/07/253&format=DOC&aged=1&language=EN&guiLanguage=en, 25.04.2014

[79] P. Morgan (raportöör). Euroopa Majandus- ja Sotsiaalkomitee arvamus teemal „Ettepanek: Euroopa Parlamendi ja nõukogu direktiiv, milles käsitletakse infosüsteemide vastu suunatud ründeid ja millega tunnistatakse kehtetuks nõukogu raamotsus 2005/222/JSK", 23.072011. p 1.10. Arvutivõrgus: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2011:218:0130:0134:ET:PDF, 25.04.2014.

[80] Euroopa Komisjoni ettepanek "Euroopa Parlamendi ja Nõukogu direktiiv, milles käsitletakse infosüsteemide vastu suunatud ründeid ja millega tunnistatakse kehtetuks nõukogu raamotsus 2005/222/JSK." Brüssel: 2010, art. 10, p 3. Arvutivõrgus: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:ET:PDF, 25.04.2014.

selgitada, et kuigi direktiivist 2013/40 ei tulene liikmesriikidele kohustust identiteedivargust raskendava asjaoluna sätestada või kriminaliseerida selline kuritegu erinormiga, siis viitab olemasolev KarS §-s 157[2] sätestatud teise isiku identiteedi kasutamine Eesti riigi kriminaalpoliitilisele seisukohale nimetatud teo karistatavuse vajalikkuse küsimuses. Toodud seisukohta kinnitab autori hinnangul ka Riigikogu Riigikaitsekomisjoni 25.11.2010 istungil esitatud arvamus, milles kritiseeriti Vabariigi Valitsuse seisukohta, et identiteedivargust ei tuleks käsitleda raskendava asjaoluna.[81] Võttes veel arvesse, et nimetatud õiguste efektiivse kaitse tagamiseks on esmatähtis ühetaoline regulatsioon ning seadusandja on olemasoleva regulatsiooni loomisega identiteedivarguse sätte vajalikkust sedastanud ning sama on teinud ka Euroopa Liit, siis leiab käesoleva töö autor, et hoolimata reguleerimise kohustuse puudumisest, on sellegipoolest rahvusvahelise koostöö seisukohalt vajalik ning oluline, et Eestis kehtiv regulatsioon kataks vähemalt kõiki direktiivi 2013/40 Art 9 p-s 5 nimetatud identiteedivargusega seotud asjaolusid.

1.2.2.3. Kaitse- ja vastutusala

Lissaboni lepinguga[82] kasutusele võetud Euroopa Liidu toimimise lepingu Art 16 lõikega 1 on sätestatud põhimõte, et igaühel on õigus tema kohta käivate isikuandmete kaitsele[83], samuti on Euroopa Liidu põhiõiguste harta Art-s 8 isikuandmete kaitse sätestatud ühe põhiõigusena[84]. Seega tekib autoril põhjendatud küsimus, kas teise isiku isikuandmete väärkasutamise puhul laieneb direktiivi 2013/40 mõistes kaitse ka juriidilistele isikutele.

Direktiivi 2013/40 seletuskirja kohaselt peavad identiteediga seonduvatele kuritegudele suunatud eeskirjad olema kooskõlas isikuandmete kaitset käsitlevate õigusaktidega, tuues Euroopa Liidu tasandil välja näiteks Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiivi 2002/58/EÜ (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv)[85], milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris

[81] Vt: M.Randma. Riigikaitsekomisjoni arvamus Euroopa Parlamendi ja Nõukogu direktiivi eelnõu suhtes, milles käsitletakse infosüsteemide vastu suunatud ründeid ja millega tunnistatakse kehtetuks nõukogu raamotsus 2005/222/JSK Eesti seisukohtade kohta. Toompea 25.11.2010, lk 2. Arvutivõrgus: http://www.riigikogu.ee/?op=emsplain&page=pub_file&file_id=71ced2aa-ec1c-dfb0-9b70-f55ff4e0158b&, 30.04.2014

[82] Lissaboni leping, millega muudetakse Euroopa Liidu lepingut ja Euroopa Ühenduse asutamislepingut sõlmitud Lissabonis 13. detsembril 2007 - ELT C 306, 17.12.2007, lk 1-231.

[83] Euroopa Liidu toimimise leping (konsolideeritud versioon). – LTE C 326, 26.10.2012, lk 47-201.

[84] Euroopa Liidu põhiõiguste harta. 30.03.2010 – ELT C 326, 26.10.2012, lk 392-410.

[85] Euroopa Parlamendi ja Nõukogu 12.07.2002 direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv). – ELT L 201, 31.07.2002, lk 37-48.

ning üldise andmekaitse direktiivi 95/46/EÜ[86]. Mõlema direktiivi kohaselt on isikuandmeteks igasugune teave tuvastatud või tuvastatava füüsilise isiku kohta, mitte aga juriidiliste isikute kohta käivad andmed.

Kohtuotsuses Volker und Markus Schecke ja Eifert[87] on Euroopa Kohus selgitanud Euroopa Liidu põhiõiguste hartast tulenevat isikuandmete kaitset juriidiliste isikute suhtes ning jõudnud järeldusele, et kuna isikuandmed on teave tuvastatud või tuvastatava füüsilise isiku kohta, on juriidilistel isikutel võimalik Euroopa Liidu põhiõiguste harta Art-tele 7 ja 8 tugineda ainult siis, kui juriidilise isiku ametliku nime kaudu on võimalik tuvastada üks või mitu füüsilist isikut. Nimetatud käsitluse järgi laieneks kaitse ka juriidilistele isikutele, kuid seda vaid niivõrd, kuivõrd juriidilise isiku kohta käiv informatsioon samastub füüsiliste isikute kohta käivate andmetega.

Samas on aga Euroopa Komisjon on teinud ettepaneku võtta vastu Euroopa Parlamendi ja Nõukogu määrus üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (isikuandmete kaitse üldmäärus)[88] ja Euroopa Parlamendi ja Nõukogu direktiiv üksikisikute kaitse kohta seoses pädevates asutustes isikuandmete töötlemisega kuritegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumise kohta.[89] Ettepanekute tegemise põhjuseks on asjaolu, et andmekaitsedirektiiv 95/46/EÜ võeti vastu 1995. aastal ning tehnoloogia kiire areng on põhjustanud uued probleemid isikuandmete kaitse valdkonnas, mistõttu on vaja tõhusa kaitse eesmärgil luua uusi kaasajastatud regulatsioone.[90]

Ettepaneku seletuskirja kohaselt laieneb määrusega pakutav kaitse füüsiliste isikute isikuandmete töötlemisele ega taga määrusega ettenähtavat kaitset seoses selliste andmete

[86] Euroopa Parlamendi ja Nõukogu 24.10.1995 direktiiv 95/46/EÜ, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. – ELT L 281, 23.11.1995, lk 31-51.
[87] Euroopa Kohtu otsus (EKo) 9.112010, C-92/09,C-93/09, *Volker und Markus Schecke GbR, Harmut Eifert vs. Land Hessen*, p 53.
[88] Euroopa Komisjoni ettepanek „Euroopa Parlamendi ja Nõukogu määrus üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (isikuandmete kaitse üldmäärus)“, Brüssel: 25.11.2012. Arvutivõrgus: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ET:PDF, 26.04.2014. Edaspidi allmärkustes: Euroopa Komisjoni ettepanek 1.
[89] Euroopa Komisjoni ettepanek „Euroopa Parlamendi ja Nõukogu direktiiv üksikisikute kaitse kohta seoses pädevates asutustes isikuandmete töötlemisega kuritegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumise kohta“. 25.11.2012. Arvutivõrgus: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:ET:PDF, 26.04.2014. Edaspidi allmärkustes: Euroopa Komisjoni ettepanek 2.
[90] Euroopa Komisjoni ettepanek 2, lk 1.

töötlemisega, mis käsitlevad juriidilisi isikuid, eelkõige juriidiliste isikutena asutatud ettevõtteid, sealhulgas juriidilise isiku nime ja vormi ning kontaktandmetega. Seda kohaldatakse ka juhul, kui juriidilise isiku nimi sisaldab ühe või mitme füüsilise isiku nime. Toodud ettepanekute kohaselt on seega isikuandmeteks vaid füüsilise isiku kohta käivad andmed.[91] Sellest tulenevalt ei laiene kavandatavatest õigusaktidest tulenev isikuandmete kaitse juriidilistele isikutele ka juhul, kui juriidilise isiku nimi sisaldab füüsiliste isikute nimesid. Nimetatu viitab selgelt Euroopa Liidu suunitlusele piiritleda isikuandmete kaitseala vaid füüsiliste isikute kohta käiva informatsiooniga.

Nagu eelnevalt öeldud, peavad identiteedivargusi reguleerivad eeskirjad olema kooskõlas teiste isikuandmete kaitset reguleerivate õigusaktidega. Võttes aga arvesse, et olemasolevatest ega ka kavandatavatest Euroopa Liidu isikuandmete kaitset reguleerivatest õigusaktidest ei tulene isikuandmete kaitse laienemine juriidilistele isikutele, siis leiab autor, et on põhjendatud järeldada, et direktiivist 2013/40 tuleneva identiteedivarguse regulatsiooni kaitseala laienemist ei ole ette nähtud juriidilistele isikutele.

Olles leidnud, et direktiivi kaitseala juriidilistele isikutele ei laiene, tuleks hinnata, kas direktiiv 2013/40 lubab identiteedivarguse toimepanemise eest võtta vastutusele ka juriidilisi isikuid. Eelnevalt tõi autor välja direktiivis 2013/40 sisalduvad kuriteokoosseisud, mis on seotud identiteedivarguse erinevate etappidega. Juriidilise isiku vastutuse sätestab direktiivi 2013/40 Art 11, mille kohaselt tuleb liikmesriigil tagada, et juriidilist isikut saaks vastutusele võtta direktiivis osutatud kuritegude eest, mille on tema kasuks toime pannud eraisikuna või juriidilise isiku organi liikmena tegutsenud isik, kellel on õigus esindada juriidilist isikut, õigus teha tema nimel otsuseid või õigus juriidilist isikut kontrollida. Seega tuleb jaatada juriidilise isiku vastutust identiteedivarguse elementide toimepanemisel läbi teiste direktiivis 2013/40 sisalduvate asjakohaste sätete.

Lähtudes ka direktiivi 2013/40 Art 9 p-s 5 sätestatud sõnastusest, mis näeb ette raskendava asjaoluna identiteedivarguse Art-tes 4 ja 5 toime pandud kuritegude puhul, mille endi toimepanemise eest on võimalik võtta vastutusele ka juriidilist isikut, on autori hinnangul sätet võimalik tõlgendada nii, et ka raskendavate asjaolude eest laieneb vastutus juriidilistele isikutele. Autori hinnangul toetab toodud seisukohta ka direktiivi 2013/40 Art 9 lg-tes 3 ja 4 sätestatu, mille eesmärgiks on määratleda direktiivis nimetatud kuritegude raskemad juhud ning nende eest mõistetavad raskemad karistused. Kuivõrd sellised raskemad asjaolud ei sõltu teo toimepanijast, vaid kuriteo sihtobjektist, tagajärjest ning teoviisist, siis ei leia autor, et

[91] Vt: Euroopa Komisjoni ettepanek 1, Art 4 p 1; Euroopa Komisjoni ettepanek 2, Art 3 p 1.

oleks põhjendatud näha raskem karistus ette vaid füüsiliste isikute poolt toimepandud kuritegude korral.

Sellest tulenevalt järeldab autor, et direktiivis 2013/40 on Euroopa Liit ette näinud vastutuse juriidilistele isikutele ka Art-s 9 sätestatud raskendavate asjaolude eest. See tähendab, et teise isiku isikuandmete väärkasutamise teel, eesmärgiga võita kolmanda isiku usaldus, kui sellega tekitatakse seeläbi kahju tegelikule identiteedi omanikule, toime pandud ebaseadusliku süsteemi häirimise ja ebaseadusliku andmetesse sekkumise eest on võimalik direktiivi kohaselt karistada ka juriidilisi isikuid.

Autor leiab, et tegemist on põhjendatud lähenemisviisiga ka seetõttu, et praktikas ei ole välistatud olukorrad, kus näiteks juriidilise isiku huvides temaga mitteseotud füüsiliste või ka juriidiliste isikute nime all identiteedi varjamise eesmärgil teise füüsilise või ka juriidilise isiku kohta käivaid andmeid kasutades häiritakse konkurendi infosüsteemi või sekkutakse arvuti andmetesse.

Juriidilistele isikutele kohaldatavate karistustena lubab direktiivi 2013/40 Art 12 kohaldada kriminaalõiguslikke või muid trahve, samuti ka näiteks riiklike hüvitiste või abi saamise õigusest ilmajätmist, ettevõtluskeeldu, sundlõpetamist, kuriteo toimepanemiseks kasutatud üksuste sulgemist ning kohtu järelevalve alla võtmist. Identiteedivargus on direktiivis 2013/40 sätestatud raskendava asjaoluna, mis tähendab, et juhul kui kuriteos mõistetakse süüdi juriidiline isik, siis peaks sellele järgnema loetelus toodud raskema karistusliigi kohaldamine.

2. Eestis kehtiva identiteedivarguse regulatsiooni vastavus rahvusvahelistest õigusaktidest tulenevatele nõuetele ja eesmärkidele ning ühistele põhimõtetele.

2.1. KarS § 157^2 kaitseala

2.1.1. Kaitstav õigushüve

Nagu autor eelnevalt mainis, on Euroopa Liidu põhiõiguste harta Art 8 p-de 1 ja 2 kohaselt igaühel õigus oma isikuandmete kaitsele. Selliseid andmeid tuleb töödelda asjakohaselt ning kindlaksmääratud eesmärkidel ja asjaomase isiku nõusolekul või muul seaduses ettenähtud õiguslikul alusel. Inimõiguste ja põhivabaduste kaitse konventsiooni[92] Art 8 kohaselt on igaühel on õigus sellele, et austataks tema era- ja perekonnaelu ja kodu ning korrespondentsi saladust. Eeltoodust selgub, et identiteedivargusega kaitstav õigushüve on, sarnaselt KarS §-

[92] Euroopa inimõiguste ja põhivabaduste kaitse konventsioon. - RT II 2000, 11, 57.

des 157 ja 157[1] sätestatud süütegudega, informatsioonilise enesemääramise õigus ja eraelu kaitse.[93] Õigus perekonna- ning eraelu puutumatusele on kaitstud ka Eesti Vabariigi põhiseaduse[94] §-ga 26. Samuti kaitseb nimetatu isiku õigust sõnale ning kujutisele, mis seondub eelkõige isiku näitamisega meedias ning tema nime alt tehtud avaldustega.[95]

PS §-st 17 tuleneb isikute õigus aule ja heale nimele. Au ning nimi on osa inimväärikusest, millel on eetilis-sotsiaalne tähendus[96] ning selle kaitse tuleneb ka Euroopa Liidu põhiõiguste harta Art-st 1, mille kohaselt on inimväärikus puutumatu, seda tuleb austada ning kaitsta. Au ja hea nime kriminaalõiguslik kaitse on tagatud ka analüüsitava karistusseadustiku identiteedivargust reguleeriva sättega.

Nimetatud õiguste rikkumiste korral on põhiõigusena põhiseaduses toodud igaühe õigus talle ükskõik kelle poolt õigusvastaselt tekitatud moraalse ja materiaalse kahju hüvitamisele. Võlaõigusseaduse[97] (VÕS) § 1045 lg 1 p 4 kohaselt on kahju tekitamine õigusvastane eelkõige siis, kui see tekitati kannatanu isikliku õiguse rikkumisega. VÕS § 1046 lg 1 järgi on isiklike õiguste kahjustamine õigusvastane kui rikutakse isiku eraelu puutumatust, teotatakse isiku au, näiteks ebakohase väärtushinnanguga, samuti kui õigustamatult kasutatakse isiku kujutist või nime ning ka muu isikliku õiguse rikkumine, kui seadus ei sätesta teisiti ning kui rikkumise õigusvastasus tuleneb VÕS § 1046 lg 2 kohaselt rikkumise põhjusest, ajendist ja liigist ning seda ei õigusta kolmandate isikute või avalikkuse huvi või muud seadusega kaitstud hüved.

Olgugi, et karistusõigusega isiku põhiõigustesse sekkumine lähtub *ultima ratio,* põhimõttest, mis tähendab, et juhul kui isiku õigusi oleks võimalik kaitsta efektiivselt ka muul vähem koormaval moel, võiks kaaluda isikut vähem koormava lahenduse kasutamist[98], ning et õigusvastase isiklike õiguste rikkumisega tekitatud kahju hüvitamiseks on seadusega ettenähtud tsiviilõiguslikud vahendid, siis on seadusandja leidnud, et näiteks rikutud hea nime taastamine võib osutuda väga raskeks, mistõttu on sellisteks puhkudeks siiski vajalik täiendav karistusõiguslik kaitse.[99] Seega on toodud põhiõiguste tagamise läbi identiteedivarguse sätte eesmärgiks eelkõige tagada isikutele efektiivne kaitse identiteedi väärkasutamise juhtumitega

[93] A. Nõmper. KarS § 157/p 1; § 157[1]/ p 1. - J. Sootak, P. Pikamäe. *et al.* Karistusseadustik. Kommenteeritud vlj. Tallinn, Juura 2009, 3 trk. Edaspidi allmärkustes: KarSK.
[94] Eesti Vabariigi põhiseadus. - RT 1992, 26, 349... RT I, 27.04.2011, 2
[95] U. Lõhmus. PõhiSK § 26/ p 9.6. - E.-J. Truuväli, *et al* (toim). Eesti Vabariigi põhiseadus. Kommenteeritud vlj. Veebiväljaanne. Tartu Ülikool 2012. Arvutivõrgus: http://pohiseadus.ee
[96] R. Maruste. PõhiSK § 17/ p 1. - E.-J. Truuväli, *op cit 95*.
[97] Võlaõigusseadus. - RT I 2001, 81, 487... RT I, 29.11.2013, 4
[98] T. Reinthal. Ülekriminaliseerimine. Analüüs. Tartu: Riigikohus, õigusteabe osakond 2010, p 4. Arvutivõrgus: http://www.riigikohus.ee/vfs/995/2010_Lisa%202%20(Ulekriminaliseerimine_analuus).pdf, 30.04.2014
[99] Seletuskiri 530 SE I, lk 6.

tekitatud mittevaralise kahju hüvitamiseks.[100]

Kuivõrd põhiõiguste juured ning nende kaitse ulatuvad piiriülesele tasandile, siis on selge, et ka direktiivi 2013/40 Art 9 p-s 5 toodud teise isiku isikuandmete väärkasutamist käsitlev raskendav asjaolu on suunatud samade õigushüvede kaitsmisele. Samuti ka eelnevas peatükis leitud ühiste põhimõtete kontekstis on oluline identiteedivarguse vastases võitluses karistusõiguslikult reguleerida isikuid identifitseeriva informatsiooni väärkasutamise juhtumeid ning nii nagu siseriiklikul ja Euroopa Liidu tasandil, on ka üldistest ühistest põhimõtetest tulenevateks eesmärkideks tagada isikute põhiõiguste ja -vabaduste tõhus kaitse identiteedivarguse mõiste alla käivate isikuandmete kuritarvitamise juhtumite eest.

2.1.2. Regulatsioonist puudutatud õigussubjektid

2.1.2.1. Sätte kaitsealasse kuuluvad isikud

KarS §-s 157[2] sätestatud teise isiku identiteedi ebaseaduslik kasutamine põhineb isikuandmete kaitsel isikuandmete kaitse seaduse[101] (IKS) tähenduses. IKS § 4 lg 1 ja direktiivi 95/46/EÜ Art 5 kohaselt on isikuandmeteks mis tahes andmed tuvastatud või tuvastatava füüsilise isiku kohta, sõltumata sellest, millisel kujul või millises vormis need andmed on. Sellisteks andmeteks võivad olla näiteks nimi, sugu, isikukood, sünniaeg ja -koht, vanemate või laste nimed ning elukoht. Lisaks eespool nimetatud andmetele on võimalik isikut tuvastada ka näiteks arvutisüsteemi kasutajanime ja parooli, kodulehe, e-posti aadressi, blogi, IP-aadressi ja pangakonto numbri järgi. Oluline on siinjuures aga see, kelle kohta nimetatud andmeid kasutatakse.

Karistusseadustiku muutmise seaduse eelnõu 530 SE I seletuskirja kohaselt võib teoorias eristada kolme eriliiki andmesubjekti:

1) reaalselt eksisteeriv isik;
2) surnud isik;
3) väljamõeldud ehk fiktiivne isik.[102]

Eestis laieneb karistusõiguslik kaitse üksnes olemasolevatele isikutele, kaitstes sealjuures IKS-is sätestatud põhimõtetest tulenevalt ka surnud isikuid 30 aasta jooksul pärast nende

[100] Seletuskiri 530 SE I, lk 4.
[101] Isikuandmete kaitse seadus. - RT I 2007, 24, 127... RT I, 30.12.2010, 11
[102] Seletuskiri 530 SE I, lk 5.

surma.[103] Samas ei hõlma KarS §-s 157[2] sätestatud identiteedivargus olukordi, kus kasutatakse fiktiivse isiku andmeid, sest ei eksisteeri isikut, keda kasutatud andmete abil oleks võimalik tuvastada. Küsimus tekib aga sünteesitud identiteedi [104] puhul, sest sellistel juhtudel kasutatakse mitme erineva isiku andmeid ning eesmärgiks on luua reaalselt eksisteerivaid andmeid kombineerides fiktiivne isik. Eraldi võetuna on siiski tegemist aga ühe konkreetse isiku kohta käivate andmetega, mis võivad teatud juhtudel võimaldada isiku tuvastamist.[105] Autor on seisukohal, et KarS §-st 157[2] tulenev kaitse laieneb sünteesitud identiteedi puhul isikutele vaid niivõrd, kuivõrd on reaalselt eksisteerivaid isikuid esitatud informatsiooni kaudu võimalik tuvastada. Teisisõnu ei ole oluline, et lisatud on mitme isiku andmeid, kui esitatud andmete põhjal on tuvastatavad siiski kõik või vähemalt üks isikutest.[106]

Perekonna- ja eraelusfäär on iseloomulik vaid füüsilistele isikutele, mille kaitse juriidilistele isikutele ei laiene.[107] Samuti ei põhine KarS-i teise isiku identiteedi ebaseaduslik kasutamine "identiteedi" mõistel, mida saaks teatud juhtudel ka juriidiliste isikute puhul kasutada või millise mõiste sisustamine võiks jääda kohtupraktika ülesandeks. Seega ei ole Eestis kehtiva identiteedivarguse regulatsiooniga tagatud kaitset juriidilistele isikutele ning nende kohta käivatele andmetele.

Nagu eelnevalt leitud, ei laiene ka direktiivi 2013/40 Art 9 p-st 5 tulenev identiteedivarguse regulatsiooni kaitseala juriidilistele isikutele. Identiteedivarguse ühiste tunnuste kontekstist ei tulene seisukohta, kas identiteedivarguse regulatsiooniga peaks olema kaitstud ka juriidiliste isikute kohta käiv informatsioon, kuid näiteks OECD definitsiooni kohaselt peaks kaitse laienema ka juriidiliste isikute kohta käivale personaalsele informatsioonile.[108]

Karistusseadustiku muutmise seaduse eelnõu 554 SE toob Eesti karistusseadustikku olulisel määral muudatusi. Siiski ei sisaldu nimetatud eelnõus muudatusi seoses §-ga 157[2]. Küll aga muudetakse delikaatsete isikuandmete ebaseadusliku avaldamist reguleerivat sätet ning eelnõus 554 SE kavandatu järgi tunnistatakse kehtetuks KarS § 157, mille kohaselt on karistatav kutse- või ametitegevuses teatavaks saanud teise isiku tervist, eraelu või äritegevust puudutava teabe avaldamine isiku poolt, kellel on seadusest tulenev kohustus hoida sellist teavet saladuses. Muudatuste kohaselt oleks KarS § 157[1] uue sõnastuse järgi karistatav

[103] Seletuskiri 530 SE I, lk 6.
[104] Sünteesitud identiteedi (*Synthetic identity*) mõistet on autor selgitanud töö alapeatükis 1.1.1.
[105] Selliseid juhtumeid, kus osa informatsiooni pärineb ühe ning osa teise isiku kohta käivatest andmetest on ette tulnud ka Eesti kohtupraktikas. Vt :alaptk. 2.1.1.
[106] Toodud seisukohta kinnitab ka Pärnu Maakohtu otsus kriminaalasjas nr 1-10-13433. Vt: alaptk. 2.2.1.
[107] U. Lõhmus. § 26/ p 10. - E.-J. Truuväli, *op. cit 95.*
[108] Vt: alaptk. 1.1.5

delikaatsete isikuandmete ebaseaduslik avaldamine või edastamine või neile ebaseadusliku juurdepääsu võimaldamine.[109] Delikaatsete isikuandmete mõiste ammendav loetelu on toodud IKS § 4 lg-s 2. Nimetatud muudatusega laiendatakse küll pisut KarS § 157[1] kohaldamisala ning nähakse ette vastutus juriidilistele isikutele. Samas ahendatakse eelnõus 554 SE kavandavate muudatustega juriidiliste isikute kohta käivale informatsioonile ulatuvat kaitset. Nimelt eelnõu 554 SE seletuskirja kohaselt jäetakse uuest seadusest välja karistamine äritegevust puudutava teabe avalikustamise eest. Nimetatut põhjendatakse seletuskirjas asjaoluga, et "puudub vajadus mingi muu äritegevust puudutava teabe, mis ei ole ärisaladus, karistusõiguslikuks kaitsmiseks."[110]

Eeltoodust nähtub, et ka siseriiklikul tasandil ei peeta vajalikuks tagada karistusõiguslikku kaitset juriidiliste isikute kohta käiva informatsiooni väärkasutamise korral. Võttes aga arvesse, et KarS § 157[2] eesmärk on peamiselt anda täiendav karistusõiguslik kaitse isiku PS-st tulenevale hea nime ning maine õigusele[111], siis tuleks autori hinnangul siiski sedastada, et hea nime kandjateks võivad olla ka juriidilised isikud.

Riigikohus on küll asunud seisukohale, et "äriühingule kui sisemist tunnetemaailma mitteomavale ja avalikke huve mitteteenivale eraõiguslikule juriidilisele isikule ei ole võimalik tekitada mittevaralist kahju ning [...] kuna äriühingud teostavad üldtunnustatult oma isekaid huve, siis puudub kolmandatel isikutel õiguslikult kaitstud ootus ja põhjendatud üldine huvi äriühingute usaldusväärse ja õiguskuuleka toimimise suhtes."[112] Autor toodud seisukohaga nõustuda ei saa, sest olgugi, et juriidiline isik ei saa kannatada hingelisi üleelamisi või tunnetada muid vaimseid kannatusi, siis võib hea nime ning usaldusväärsuse rikkumisega siiski tekkida kahju juriidilise isiku seadusega kaitstud õigustele või huvidele. Olgugi, et ka VÕS § 128 lg-s 5 on sätestatud, et mittevaraline kahju hõlmab eelkõige kahjustatud isiku füüsilist ja hingelist valu ning kannatusi, siis ei seo VÕS siiski mittevaralise kahju mõistet füüsiliste isikute mõistega.

Muuhulgas on ka õiguskirjanduses juriidilise isiku mittevaralise kahju võimalikkusega nõustutud ning peamist juhtumitena käsitletud just tema maine kahjustamist ebaõigete väidete

[109] Karistusseadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu seletuskiri 554 SE. Lisa 1, lk 52. Arvutivõrgus: http://www.riigikogu.ee/?op=ems&page=eelnou&eid=78433b29-8b2f-4281-a582-0efb9631e2ad&, 28.04.2014.
[110] Seletuskiri 554 SE, lk 54.
[111] Seletuskiri 530 SE I, lk 6.
[112] RKKKo, 04.11.2005, 3-1-1-24-05, p 6.5. (Jaan Mugra kaitsja vandeadvokaat Leon Glikmani kassatsioon Tartu Ringkonnakohtu 17. novembri 2004. a otsuse peale Jaan Mugra süüdistusasjas KrK § 161 järgi.)

levitamise korral.[113] Veelgi enam, Euroopa Inimõiguste Kohus on leidnud, et mittevaralise kahju hüvitamise nõudmist võib nõuda ka juriidiline isik ning puudub asjaolu, mis välistaks üldiselt juriidilise isiku õiguse mittevaralise kahju nõudmiseks, vaid asjaolusid tuleb hinnata iga konkreetse juhtumi üksikasjadest lähtuvalt.[114]

Samuti ei saa autori hinnangul väita, nagu saaks identiteedivargusega tekitatud kahju olla vaid mittevaraline. Nii hea nime kui usalduse rikkumisega võib isikule tekitada ka varalist kahju, mis võib seisneda näiteks saamata jäänud tulus.[115] Samuti on autor seisukohal, et olgugi, et juriidilistel isikutel, nagu ka füüsilistel isikutel, on igasuguse õigusvastaselt tekitatud kahju korral võimalus pöörduda enda õiguste kaitseks nõudega kohtusse tsiviilkorras, on siiski põhjendamatu siduda identiteedivarguse juhtumeid reguleeriv karistusõiguslik säte rangelt vaid füüsiliste isikute kohta käivate isikuandmete mõistega ning jätta sätte kaitsealast välja juriidilised isikud.

Samuti leiab töö autor, et eelkõige just internetiga seotud identiteedivarguse juhtumite puhul ähvardab maine kahjustamise oht võrdselt nii füüsilisi kui juriidilisi isikuid. Nii nagu füüsilise isiku kohta käivaid andmeid kasutades on võimalik teise isiku nime all näiteks laimava või solvava sisuga artikleid avaldada on interneti anonüümsuse tõttu võimalik sama teha ka juriidiliste isikute nimel. Veelgi enam, kuivõrd arvutialaste identiteedivarguste juhtumite korral võib kasutatavaks identifitseerimisvahendiks olla näiteks vaid IP-aadress koos asukoha, nime või muu kasutajakontoga, siis on arvutisüsteemidesse ebaseadusliku tungimise teel võimalik ka juriidilise isiku nime all toime panna erinevaid arvutialaseid kuritegusid. Sellistel puhkudel jäetakse toimepanijana jälg mingile juriidilise isikule või viited tema nimele registreeritud arvutile, mille kaudu infosüsteemi ebaseaduslikult sekkuti. Sellistel puhkudel võib sarnaselt füüsiliste isikutega olla juriidilisel isikul väga raske enda mainet ning usaldust klientide ja avalikkuse ees taastada.

Antud juhul on seadusandja pidanud piisavaks kaitseks tsiviilkohtusse pöördumise võimalust, kuid autor on seisukohal, et nimetatud õiguskaitsevahend ei pruugi väikese ning keskmise suurusega ettevõtjate puhul olla kõrgete kohtukulude tõttu efektiivseks lahenduseks.

[113] L. Kanger. Kahju hüvitamise nõue riigivastutuse seaduse alusel. Kohtupraktika analüüs. Tartu: Riigikohus, õigusteabe osakond 2008, lk 20. Arvutivõrgus: http://www.riigikohus.ee/vfs/775/Analyys%20Riigivastutus(L_Kanger).pdf, 29.04.2014.; M. Punab. Ebaõigete ja au teotavate andmete avaldamine ja sellega tekitatud mittevaraline kahju. Bakalaureusetöö. Tartu: Tartu Ülikool 2009, lk 11. Arvutivõrgus: http://www.just.ee/orb.aw/class=file/action=preview/id=49247/Eba%F5igete+ja+au+teotavate+andmete+avaldamine+ja+sellega+tekitatud+mittevaraline+kahju.pdf, 19.04.2014.

[114] Euroopa Inimõiguste Kohtu otsus (EIKo) 06.04.200, 35382/97, *Comingersoll S.A. vs. Portugal*, p 32.

[115] Kahjuga seonduvat käsitleb autor pikemalt alapeatükis 2.2.2.4.2.1.

Ettevõtlus üha enam seotud internetiga ning interneti turvalisuse tagamine on samuti oluline majanduse kasvu seisukohalt. Sarnase seisukoha on 2012. aastal esitanud ka kaheteistkümne Euroopa Liidu liikmesriigi valitsusjuhid, kes kirjutasid alla ühisele kirjale, mis sisaldas konkreetseid ettepanekuid majanduskasvu elavdamiseks ning Euroopa siseturu arendamiseks.[116] Nimetatud Euroopa Majanduskasvu kava kohaselt vajavad liikmesriigid, et Euroopa Liidu tasandil võetakse kasutusele meetmed, mis tekitaksid nii ettevõtetes kui ka tarbijates usaldust internetiga seotud ettevõtluse suhtes.[117] Seega on käesoleva töö autor seisukohal, et identiteedivarguste sidumine isikuandmete mõistega, mis ei laiene juriidilistele isikutele pärsib majanduse arengut ning jätab põhjendamatult juriidilised isikud ilma efektiivsest kaitsest rünnete ees, mille ohvriks sattumise oht üha arenevas internetikeskkonnas suureneb võrdselt nii füüsiliste kui juriidiliste isikute jaoks.

Autori hinnangul on eeltoodu tõttu seadusandjatel nii siseriiklikul kui Euroopa Liidu tasandil ilmselt otstarbekas tulevikus kaaluda, kas võiks siiski olla põhjendatud internetiga seotud kuritegevuse iseärasusi arvesse võttes laiendada identiteedivarguse juhtumite puhul kaitseala selliselt, et see hõlmaks ka juriidilisi isikuid ning nende kohta käivaid andmeid, et tagada võrdne kaitse kõigile kõneall oleva kuriteo potentsiaalsetele ohvritele.[118]

2.1.2.2. Vastutus

Kehtiv KarS § 157^2 ei näe ette vastutust juriidilistele isikutele. Autor leidis, et direktiivist 2013/40 tulenevalt peaks Art-tes 4 ja 5 toime pandud infosüsteemide vastu suunatud rünnete puhul isiku tegeliku identiteedi varjamise korral vastutus laienema ka juriidilistele isikutele, kui nimetatud kuriteod pannakse toime juriidilise isiku huvides.[119] Samuti on ette nähtud juriidilise isiku vastutus nii direktiivi 2013/40 kui ka Arvutikuritegevusvastase konventsiooni identiteedivargusega relevantsetes teistes kuriteokoosseisudes.

Töö punktis 1.2.2.2. on autor toetanud direktiivi 2013/40 regulatsiooni juriidilise isiku vastutuse osas. Olgugi, et KarS §-st 14 tulenevalt vastutab juriidiline isik üksnes füüsilise isiku kaudu ning koosseisupärasuse kontrollimist alustatakse siiski füüsilise isiku tegevuse kontrollimisest[120], siis on teatud juhtudel siiski põhjendatud vastutuse üleviimine juriidilisele isikule. Seda just KarS § 14 lg-s 1 sätestatud juhtudel, kui kuritegu on toime pandud juriidilise

[116] Peaminister David Cameron, *et al.* Ühiskiri Euroopa Ülemkogu eesistujale Herman van Rompuyle ja Euroopa Komisjoni presidendile José Manuel Barrosole. Euroopa majanduskasvu kava. Brüssel: 2012, lk 1. Arvutivõrgus: http://valitsus.ee/et/uudised/taustamaterjalid/56192/euroopa-majanduskasvu-kava, 19.04.20.14.
[117] *Ibid*, lk 2.
[118] Autori poolt pakutud lahenduse kohta vt: alaptk 2.2.1.
[119] Direktiivis 2013/40 sätestatud juriidilise isiku vastutuse kohta vt: alaptk. 1.2.2.2.
[120] Seletuskiri 554 SE, lk 116.

isiku organi, selle liikme, pädeva esindaja või juhtivtöötaja poolt nimetatud juriidilise isiku huvides. Hea nime ning maine kahjustamise motiivil toime pandud identiteedivargustega kaasneb tihti kahju tekitamine, mis käesoleval ajal on ka Eestis kehtiva identiteedivarguse üheks koosseisuelemendiks. Juriidilise isiku huvides toime pandud teo puhul on autori hinnangul igati põhjendatud pidada teo toimepanijaks ning seejuures võimaldada määratleda kahju tekitajaks just juriidiline isik. Teatud juhtudel võib kuriteo ohvri jaoks tekitatud kahju eest hüvitise saamine juriidiliselt isikult olla tõenäolisem, mis tagaks seega kahju kannatanud isikutele efektiivsema võimaluse enda seadusest tulenevaid õigusi realiseerida.

Juriidilise isiku vastutus on karistusseadustiku ja sellega seonduvalt teiste seaduste muutmise eelnõus 554 SE lisatud mitmetele erinevatele kuritegudele[121], millega laieneb oluliselt juriidiliste isikute vastutus erinavte karistusseadustikus kriminaliseeritud tegevuste eest. Mingil põhjusel ei ole siiski vajalikuks peetud laiendada juriidiliste isikute vastutust identiteedivarguse juhtumite puhuks. Muuhulgas nähakse aga kavandatava 2015. aastal kehtima hakkava karistusseadustiku uue redaktsiooniga ette juriidilistele isikutele vastutus näiteks delikaatsete isikuandmete ebaseadusliku avaldamise eest.[122] Samas kitsendatakse juriidilise isiku vastutust KarS § 37^1 lisamisega. Nimetatud sätte kohaselt puudub juriidilisel isikul süü, kui tema pädeva esindaja toime pandud tegu oli juriidilise isiku jaoks vältimatu. Regulatsiooni eesmärgiks on välistada juriidiliste isikute vastutus kui juriidiline isik on ise teinud kõik selleks, et vältida pädeva esindaja kuritegelikku käitumist. Samas on paragrahvi kohaldamine võimalik vaid pädeva esindaja poolt toime pandud süüteo korral ning välistatud, kui vastutuse aluseks olnud süütegu on toime pandud juhtivtöötaja, organi või selle liikme poolt juriidilise isiku huvides.[123] Direktiivi 2013/40 Art 10 lg 2 kohaselt peab liikmesriik võtma vajalikud meetmed, et juriidilist isikut saaks vastutusele võtta ka juhul, kui eraisikuna või juriidilise isiku organi liikmena tegutsenud isikul, kellel on õigus esindada juriidilist isikut, õigus teha juriidilise isiku nimel otsuseid või õigus kontrollida juriidilist isikut, on järelevalve või kontrolli puudumise tõttu olnud võimalik juriidilise isiku kasuks toime panna direktiivi 2013/40 Art-tes 3–8 osundatud kuritegu.

Autor leiab, et karistusseadustikku täiendav kavandatav KarS § 37^1 ning direktiivist 2013/40 tulenev nõue on enda sisult kattuvad, kuivõrd tõenäoliselt olukorras, kus juriidiline isik on

[121] Näiteks KarS § paragrahve 113, 120, 123, 124, 129, 130, 131, 132, 139, 148, 149, 150, 158, 186, 195, 203, 235^2, 235^3, 236, 238, 243, 245, 249, 250, 262, 265, 278, 308, 314, 315, 316, 316^1, 322, 341, 348, 404 ja 419 täiendatakse juriidilise isiku vastutuse lisamiseks lõikega kaks ning paragrahve 117, 119, 135, 136, 140, 152, 153, 156, 161, 174, 183, 187, 188, 217^1 ja 239 täiendatakse lõikega 3, mis näeb ette juriidilise isiku vastutuse. Vt: Seletuskiri 554 SE, lk 42-43.
[122] Seletuskiri 554 SE Lisa 1, lk 52.
[123] Seletuskiri 554 SE, lk 21.

jätnud teostamata vajaliku kontrolli, ei ole nimetatud teo toimepanemine olnud tema suhtes vältimatu. Seega ei esine kavandatava karistusseadustiku ning direktiivi 2013/40 vahel vastuolusid juriidilise isiku vastutuse aluste puhul, küll aga näeb autor vastuolu selles, et KarS § 157^2 puhul on juriidiliste isikute vastutus jäetud sätestamata.

Kuivõrd autor on eelnevalt asunud seisukohale, et identiteedivarguse seonduv säte peaks katma vähemalt direktiivi 2013/40 Art 9 p-s 5 nimetatud asjaolud ning direktiivi Art-est 4 ning 5 tulenevate karistusseadustikus sisalduvate kuritegude puhul ei ole seadustiku eriosas ettenähtud eraldi teise isiku identiteedi kasutamisega seonduvat raskendavat asjaolu ka uue kavandatava redaktsiooniga, siis peaks direktiiviga 2013/40 kooskõla saavutamiseks nimetatud sätete ning identiteedivarguse puhul olema võimalik vähemalt kogumi moodustamine KarS §-s 206 ning §-s 207 sätestatud kuritegudega. Iseenesest on karistusseadustikus sätestatud arvutikuritegude eest vastutus nii juriidilistele kui füüsilistele isikutele, kuid juriidilise isiku vastutuse puudumine identiteedivarguse sättes välistab nimetatud sätetega kogumi moodustamise ning teise isiku identiteedi väärkasutamise eest raskema karistuse mõistmise juhul, kui nimetatud kuriteod on toime pandud juriidilise isiku poolt. Seetõttu asub autor seisukohale, et direktiiviga 2013/40 kooskõla saavutamiseks oleks tarvilik ette näha juriidilise isiku vastus ka KarS §-s 157^2 ning seadusandja peaks kaaluma sätte täiendamist juriidilise isiku vastutust ettenägeva lõikega.

2.2. KarS § 157^2 reguleerimisala

2.2.1. Tuvastavad ja tuvastamist võimaldavad isikuandmed

Nagu eelnevalt öeldud, siis andmete iseloom ning nende maht, mille edastamine või kasutamine täidab identiteedivarguse kuriteokoosseisu, tuleneb igast konkreetsest sättest. Eesti identiteedivarguse sätte tõlgendamisel tõusetub autori hinnangul kehtiva regulatsiooni seonduv peamine probleem, milleks on isikuandmete kasutamisega seostatud isiku tuvastamise või tuvastamise võimalikkuse range nõue. Autori hinnangul ei ole üheselt mõistetav, millisel juhul saab rääkida, et isik on teatud andmete põhjal kindlasti reaalselt tuvastatav.

Olukorras, kus räägime väga laialdaste ja üldiste tunnuste avaldamisest, ei saa tõenäoliselt sedastada teist isikut tuvastada võimaldavate andmete kasutamist. Näiteks, kui üks isik esitleb ennast blondide juustega noormehena, kes on pärit Saaremaalt, siis ei saa öelda, et nimetatud olukorras elukohta ja välimust kirjeldavate andmete avaldamine aitaks kuidagi täpset isikut tuvastada. Samal ajal, kui räägime aga näiteks mustanahalisest blondide juustega noormehest

Saaremaalt, siis võib tuvastamise võimalikkus tulla kõne alla, sest suure tõenäosusega ei leidu nimetatud piirkonnas taoliste eritunnustega inimesi arvukalt.

Kohtutesse on jõudnud mitmeid kriminaalasju, mille sisuks on teise isiku identiteedi ebaseaduslik kasutamine, kuid mis siiski ei anna lahendust autori poolt tõstatatud probleemile. Näiteks pärineb 2010. aastast Pärnu Maakohtu otsus kokkuleppemenetluses, millega mõisteti Virkko Ojare süüdi selles, et ta avas alaealise tütarlapse nimel viimase teadmata konto täiskasvanutele mõeldud internetikeskkonna portaalis "Iha"[124]. Noormees laadis kontole lisaks tütarlapse teisest interneti suhtlusvõrgustikust pärit fotodele üles ka tundmatu neiu fotosid ning esitas valeinfot tütarlapse vanuse ja tutvumissoovide kohta.[125] Tundmatu isiku fotode lisamine ning ebaõige informatsiooni avaldamine isiku vanuse kohta viitab antud juhtumi puhul autori hinnangul pigem sünteesitud identiteedi kasutamisele. Siiski nähtub, et kohus nõustus antud kaasuse puhul, et esitatud andmed olid sellegipoolest tütarlapse identifitseerimiseks piisavad ning erilist tähelepanu ei pälvinud ka asjaolu, et andmete koostoimes oli püütud luua vaid osaliselt kannatanu profiilile vastav isik. Kuivõrd teine isik, kelle fotosid avaldati, jäi menetluse käigus tuvastamata, on võimatu anda hinnangut, kas ka nimetatud isikut oleks antud kriminaalasjas käsitletud kannatanuna.

Pärnu Maakohtust pärineb veel teinegi identiteedivarguse juhtumit lahendav kohtuotsus, milles kirjeldatud asjaolude kohaselt esitas Maris Teearu Lääne Prefektuuri Pärnu politseijaoskonna patrullpolitseinikule väärteoprotokolli koostamisel valeandmeid, püüdes esineda teise isikuna ning pääseda väärteokaristusest.[126] Esitatud andmete hulka kuulusid nimi, sünniaeg ning elukoht. Tegu kvalifitseeriti KarS § 157^2 järgi ning nimetatud juhtumi puhul jäi teise isiku identiteedi ebaseaduslik kasutamine katsestaadiumisse, sest patrullpolitseinik tuvastas, et teise isiku nime all esinev isik on tegelikult Maris Teearu. Sarnased juhtumid vastavad tihti pigem KarS §-s 349 toodud kuriteokoosseisule, mis sätestab tähtsa isikliku dokumendi kuritarvitamise, mis seisneb teise isiku nimele väljaantud tähtsa isikliku dokumendi kasutamises või enda nimele väljaantud tähtsa isikliku dokumendi teisele isikule kasutamiseks andmises eesmärgiga omandada õigusi või vabaneda kohustustest. Kuivõrd antud kaasuse puhul ei esitanud isik politseinikule mitte teise isiku dokumenti, vaid isiku tuvastamine käis suuliselt edastatud informatsiooni ning andmebaaside abil, siis ei vastanud Maris Teearu tegevus, sarnaselt ka järgnevas lõigus toodava juhtumiga, tähtsa isikliku dokumendi kuritarvitamise koosseisu tunnustele.

[124] www.iha.ee, 29.04.2014.
[125] Pärnu Maakohtu otsus (PMKo) 24.11.2010, 1-10-13433. (Virkko Ojare süüdistuses KarS § 157^2 järgi.)
[126] PMKo 14.09.2011, 1-11-4952. (Maris Teearu süüdistuses KarS § 121; § 25 lg 1, 2 - § 157^2 järgi ja Veronika Harjus süüdistuses KarS § 121 järgi.)

Eesti kohtupraktikas esineb ka juhtumeid, kus võõra isiku isikuandmete kasutamine tuvastatakse alles kohtumenetluses. Selliselt on näiteks Harju Maakohus tunnistanud Rene Rohtlaan'e süüdi KarS § 157^2 järgi selles, et olles kinni peetud mootorsõiduki joobeseisundis juhtimiselt, esitles ta ennast politseile oma venna Marko Rohtlaan'ena ning kasutas Marko Rohtlaan'e isikuandmeid ilma viimase nõusolekuta kogu kriminaalmenetluse vältel, eesmärgiga varjata tema poolt toime pandud kuritegu, mistõttu mõistetigi Harju Maakohtus KarS § 424 järgi süüdi hoopis Marko Rohtlaan.[127] Sarnaseid juhtumeid on esinenud ka hiljem, näiteks tunnistati 2011. aastal Julia Bašlõkova süüdi KarS § 157^2 järgi selles, et süüdistatuna varguse toimepanemises, kasutas ta Julia Trofimova isikuandmeid kogu kriminaalmenetluse vältel.[128] Seega, esinedes Julia Trofimova'na, mõisteti sisuliselt kohtu poolt süüdi mitte Julia Bašlõkova, vaid Julia Trofimova ning Julia Bašlõkova täitis teist isikut tuvastavate isikuandmete tema nõusolekuta kasutamisega, eesmärgiga teise isikuna esinemise teel varjata kuritegu, KarS §-s 157^2 sätestatud kuriteokoosseisu.[129] Kohtuotsustest selgub, et süüdistatavad kasutasid kuriteo täideviimiseks teise isiku nime, sünniaega, kodakondsust ning elukohta.

Osundatud juhtumitest selgub, et tuvastamiseks võib piisata väga minimaalses mahus andmete kasutamisest. Võttes arvesse politsei võimalusi kasutada erinevaid andmebaase isikuandmete kontrollimiseks, on käesoleva töö autor seisukohal, et igapäevaelus, kus isikutel on esitatud teabe õigsuse kontrollimiseks oluliselt piiratumad vahendid, tuleks seda igal konkreetsel juhul kindlasti kuriteo asjaolude hindamisel pigem kannatanute kasuks arvesse võtta. Seda põhjusel, et kahtluse korral ei ole isikutel politseile sarnaseid võimalusi andmete õigsuse kontrollimiseks, mistõttu võib veendumus isiku identifikatsioonis tekkida kergemini. Autor leiabki, et tuvastamist võimaldavate andmete loetelu ei saa olla esitatud suletud kataloogina ning vajab kindlasti igas konkreetses olukorras eraldi hindamist ning analüüsimist.

Eeltoodu tõstatab järgnevalt küsimuse selle kohta, kellele peaks kuriteokoosseisu täitmiseks isik väärkasutatud andmete alusel olema tuvastatav. Võib eeldada, et isikule endale on tema kohta käivate andmete põhjal enda isiku tuvastamine oluliselt lihtsam kui kõrvalseisvatele isikutele. Selgusetuks jääb see, kas KarS §-s 157^2 toodud kuriteokoosseisu täitmiseks peaks piisama sellest, kui isik ise ennast tuvastada suudab või oleks vajalik veel vähemalt ühe teise isiku poolt tuvastamine.

[127] HMKo 13.12.2010, 1-10-13878. (Rene Rohtlaane süüdistuses KarS § 157^2; § 424; § 329 järgi.)
[128] Mõlemad nimetatud juhtumid on kaasa toonud esialgse kuriteo toimepanemises süüdistatud isikute õigeksmõistmise. Vt: viide 44.
[129] HMKo 18.05.2011, 1-11-2698. (Julia Bašlõkova süüdistuses KarS § 1572 ja § 199 lg 2 p 9 järgi.)

Täna puudub kohtupraktika, mis määratleks selgelt, millises mahus ning milliseid andmeid konkreetselt peab olema töödeldud selleks, et võiksime tõdeda isiku tuvastamist. Oluline on see, millisel määral on mingid andmed konkreetse isikuga seostatavad. Käesoleva töö autor on seisukohal, et kui kasutatakse mõnes portaalis ainult isiku poolt mujal kasutatavat kasutajanime, milleks on mingi liigitunnustega asi nagu näiteks "Kiisuke" või "Lilleke35", siis ei saa sellise kasutajanime all esinemist teise isiku poolt pidada identiteedivarguseks, sest tegemist ei ole isikut tuvastada võimaldavate isikuandmetega ning jõuaksime absurdse lahenduseni. Seos isiku ja mingi tunnussõna vahel ei saa olla niivõrd tugev, et tuvastamine oleks igal juhul võimalik. Teisalt, kui töötlemise objektiks on foto, nimi või telefoninumber, siis on aga nende andmete põhjal võimalik isikut suhteliselt lihtsalt tuvastada.

Meedia on korduvalt kajastanud identiteedivarguse ning isikuandmete väärkasutamise juhtumeid. Aastatel 2010-2013 on teise isiku identiteedi ebaseadusliku kasutamisega seonduvate juhtumite tõttu esitatud Eestis kokku 271 kuriteoteadet.[130] Viimati ajakirjanduses päevakorda kerkinud juhtumite puhul avaldati internetis seksuaalteenuste müümise kuulutusi ning kuulutusele lisati isikute, kui väidetava teenuse müüjate, telefoninumbrid ning mõnel juhul ka fotod.[131] Isikud pöördusid avaldustega politseisse, kuid kriminaalmenetlus jäi vaid telefoninumbri avaldamise juhtumi puhul alustamata põhjendusel, et telefoninumber ei ole isiku tuvastamiseks piisav informatsioon. Sellist seisukohta on väljendanud ka Riigiprokuratuur ühtse menetluspraktika väljakujundamiseks ja kuriteokoosseisu paremaks mõistmiseks antud "Riigiprokuratuuri juhises identiteedivarguse asjades"[132], leides, et rikkumine on toime pandud siis, kui isikut on esitletud avalikkusele ära tuntaval viisil. Samuti jagab juhis isikuandmed kahte gruppi, otsesed ning kaudsed isikuandmed. Esimese moodustavad andmed nagu isikukood ning teise sünniaeg või nimi. Muuhulgas piirab juhis oluliselt sätte grammatilisest tõlgendamisest tulenevaid võimalusi ning eelnõus 530 SE I sätestatut, leides, et tuvastamist võimaldavate isikuandmete alla ei kuulu näiteks sugu ja silmade värv, mis küll IKS § 4 kohaselt kuuluvad isikuandmete hulka.

Riigiprokuratuuri soovituste kohaselt ei piisa isiku tuvastamiseks reeglina ainult ühe kaudse isikuandme avaldamisest, vaid kuriteokoosseisu täitmiseks peaks neid samaaegselt esinema vähemalt kaks. Viimasel juhul jätab juhis küll diskretsiooniruumi, leides, et teatud juhtudel võib piisata vaid ka ühe kaudse isikuandme kasutamisest, sest näiteks ei teki kahtlust, kellega

[130] Justiitsministeerium. Kriminaalstatistika. Registreeritud kuriteod 2003-2013. Justiitsministeerium: 2014. Arvutivõrgus: http://www.just.ee/59292, 29.04.2014.
[131] R. Kagge. Fiktiivseid seksikuulutusi avaldavad kiusajad jäävad enamasti karistuseta. - ERR 2014. Arvutivõrgus: http://uudised.err.ee/v/eesti/3e3b9e96-1c3f-41d9-bf67-0125f89c261e, 29.04.2014.
[132] Riigiprokuratuur. Riigiprokuratuuri juhis identiteedivarguse asjades. Tallinn: Riigiprokuratuur 2011, lk 1.

on tegemist, kui kasutatakse meiliaadressi "norman.aas@prokuratuur.ee." [133] Mõningate andmete puhul on töö autori hinnangul tõepoolest tarvilik andmete koosmõju, nime ja sünniaja koos esitamise korral võivad need võimaldada isikut tuvastada, kui pelgalt sünniaja järgi konkreetset isikut siiski tuvastada võimalik ei oleks.

Samas näeb autor ohtu, et sellise tingimuse loomisega muutub identiteedivarguse kohaldamisala liialt kitsaks ning seda eriti internetiga seotud identiteedivarguse juhtumite puhul. Võttes muuhulgas arvesse interneti laialdasi võimalusi, siis võib näiteks telefoninumbri avaldamise korral olla võimalik andmete seostamise (*linking*) kaudu jõuda isiku nime ning identiteedi juurde. Selliseks juhtumiks võib olla näiteks füüsilisest isikust ettevõtjana tegutsev põllumajandussaaduste müüja, kes on teenuse pakkumiseks loonud kodulehe enda nime kasutades ning kasutanud kontaktnumbrina enda isiklikku telefoninumbrit. Sellises olukorras võib seksuaalteenuste müügiga seonduvas kuulutuses olla kirjas küll vaid isiku telefoninumber, kuid avalikkusele kättesaadavate vahendite kaudu on kergelt võimalik jõuda isiku nime ning muude tuvastamist võimaldavate andmeteni. Samuti võib isiku tuvastamine teatud juhtudel olla võimalik lihtsalt avaldatud telefoninumbrile helistades.

Riigiprokuratuuri juhise kohaselt tuleb küll hinnata andmete alusel tuvastamise tõenäosust[134], kuid eelnevalt mainitud hiljutise meediakajastuse raames prokuröri poolt antud intervjuust[135] nähtub, et sellist tõenäosuse hindamist praktikas ei toimu ega võeta arvesse ka seda, kas mingi lisategevusega võib siiski esitatud andmete abil olla võimalik isikut tuvastada. Samas on ka direktiivi 95/46/EÜ Art 29 alusel loodud andmekaitse töörühm kinnitanud, et isiku tuvastatavuse kindlakstegemisel tuleb arvesse võtta kõiki vahendeid, mida võidakse andmesubjekti tuvastamiseks tõenäoliselt kasutada.[136]

Autor nõustub Riigiprokuratuuri seisukohaga selles osas, et asjaolusid tuleks hinnata kogumis[137] ning tuvastamise küsimuse lahendamiseks peab igal konkreetsel juhul kasutatud andmete abil tuvastatavuse väljaselgitamiseks rakendama mõistliku hindamise põhimõtet selleks pädeva isiku poolt. Kohtul tuleb välja selgitada ning kaaluda, kas ning kuivõrd on tegelikult töötlemise objektiks olnud andmete põhjal võimalik konkreetset isikut tuvastada, võttes arvesse kolmandate isikute võimalusi andmeid avalikkusele kättesaadavate vahendite

[133] Riigiprokuratuur, *op. cit 132*, lk 1.
[134] *Ibid*, lk 1.
[135] Intervjuu ringkonnaprokurör Rainer Amur'iga. Telesaade "Pealtnägija". ERR 2014. Arvutivõrgus: http://etv.err.ee/arhiiv.php?id=146055, 29.04.2014.
[136] P. Schaar (eesistuja). Arvamus 4/2007 isikuandmete mõiste kohta. Direktiivi 95/46/EÜ artikli 29 alusel loodud andmekaitse töörühm. Euroopa Komisjon. Arvutivõrgus: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_et.pdf, 30.04.2014.
[137] Riigiprokuratuur, *op cit 132*, lk 1.

kaudu omavahel siduda.

Autor ei välistaks juhtumeid, kus identiteedivargusega kaitstavad isiklikud õigused võivad olla rikutud ka juhul, kui avaldatud on vaid üks kaudsetest isikuandmetest või on avaldatud andmeid, mida üleüldse IKS alusel isikuandmetena ei käsitleta. Näitena võib tuua selle, et juhul kui isikule on loodud konto, mille kaudu ta väidetavalt müüb seksuaalteenuseid, kuid avaldatud ei ole tema fotot vaid ainult telefoninumber ning olgugi, et isikut ei ole võimalik kolmandate isikute poolt tuvastada, siis on sellegipoolest loodud nimetatud isikust ebaõige ettekujutus ning riivatud tema au ja väärikust sellega, et teenuse soovijad temaga ühendust võtavad. Autor leiab, et sellised juhtumid ei tohiks nende kasvava arvukuse ning toimepanemise lihtsuse tõttu jääda tähelepanuta ning isikud karistusõigusliku kaitseta.

Arvutikuritegevusvastane konventsioon ei ava isikuandmete või muu identiteedivarguse koosseisu moodustava väärkasutatud informatsiooni mõistet. Direktiivi 2013/40 kohaselt peaks raskendava asjaoluna olema aga kriminaliseeritud teise isiku isikuandmete väärkasutamise teel toime pandud teatud arvutialased kuriteod, kui sellega on tekitatud tegeliku identiteedi omanikule kahju. Seega ei erine direktiivi 2013/40 käsitlus Eesti siseriiklikust identiteedivarguse käsitlusest, sisustades koosseisu isikuandmete väärkasutamise mõistega. Andmed, mida Euroopa Liidu õiguse alusel isikuandmetena käsitletakse, tõi autor välja töö alapeatükis 1.2.2.2. Ka ei esine IKS-s ning Euroopa Liidu õiguses isikuandmete mõistet käsitlevate direktiivide vahel sisulisi erinevusi isikuandmete mõiste sisustamise osas.[138] Eeltoodust tulenevalt tuleb asuda seisukohale, et ka direktiiv 2013/40 ei näe ette identiteedivargusele isikuandmete mõiste osas laiaulatuslikumaid tõlgendamisvõimalusi ning seega ei tuvasta autor selles küsimuses vastuolusid direktiivis 2013/40 ning Eesti karistusseadustikus sisalduvate identiteedivarguse regulatsioonide vahel.

Sellegi poolest leiab autor, et karistusseadustikus sisalduvad normid peavad tagama isikutele kaitset reaalses elus eksisteerivate juhtumite puhuks. Seega peab autor identiteedivarguse regulatsiooni kohaldamisala internetis toime pandavate identiteedivarguste puhul liialt kitsaks osas, milles see seob identiteedivargused rangelt vaid isikuandmete mõistega. Autor mõistab, et liiga laia tõlgendamisruumi jätmine võib tuua kaasa ülekriminaliseerimise ohu, kuid kuna libakontode loomine ning erinevate kuulutuste vale nime või numbri alt avaldamine on muutumas üha lihtsamaks ning populaarsemaks ega ole probleemiks ainult Eestis, siis ei ole põhjendatud jätta isikud nimetatud situatsioonides tõhusa kaitseta. Näiteks on Belgia kohus

[138] Nii Euroopa Parlamendi ja Nõukogu direktiiv 2002/58/EÜ, kui ka Euroopa Parlamendi ja Nõukogu direktiiv 95/46/EÜ, sisustavad isikuandmete mõistet, kui: "igasugust teavet tuvastatud või tuvastatava füüsilise isiku kohta".

leidnud, et sotsiaalvõrgustikke ei tohiks kasutada isiklike vandenõude lahendamiseks ning isikuid tuleb kaitsta selle eest, et nende identiteeti ei kasutataks valekontode loomiseks, mille eesmärgiks on isikutele nii personaalses kui ka professionaalses elusfääris võimalikult palju kahju tekitada.[139]

Seega võiks nii siseriiklikul ka ka Euroopa Liidu tasandil kaaluda, kas teise isiku identiteedi kasutamisega seonduvate juhtumite puhul ei oleks siiski tõhusama kaitse tagamise eesmärgil mõistlikum ette näha laiemat kohaldamisala võimaldav regulatsioon, mis lubaks uurimisasutustel ning prokuratuuril kriminaalmenetlust alustada ka olukorras, kus isikule on tekkinud kahju juba vaid näiteks telefoninumbri või muu kaudse informatsiooni avaldamise või kasutamisega teise isiku poolt, mille kaudu on võimalik jõuda isiku teiste andmeteni või loodud ebaõige ettekujutus nimetatud kontol või kuulutuses viidatud isikust ning libakonto või muu andmete väärkasutaja tegevus on ilmselgelt olnud pahatahtlik. Kusjuures võimalust tuvastada isik arvutisüsteemi kasutajanime, parooli, e-posti aadressi, blogi, IP-aadressi või pangakonto numbri järgi on sedastanud ka seadusandja identiteedivarguse sätte loomisel.[140] Autori arvates ei ole näiteks IP-aadressi näol tegemist isikuandmete alla käiva informatsiooniga, sest viitab kasutatavale arvutile, mitte aga seda kasutanud isikule. Samuti on teisigi interneti- ja arvutikeskkonnas kasutatavaid identifitseerimist võimaldavaid andmeid, mille pidamist klassikalisteks isikuandmeteks võiks kahtluse alla seada. Muuhulgas ei saa eitada, et kõik eelnevalt loetletud andmed võivad oma iseloomult samuti kuuluda juriidilistele isikutele. Samas on kõigi eelnevalt loetletud andmete kaudu teatud juhtudel siiski võimalik reeglina jõuda konkreetse isikuni.

Sellest tulenevalt teeb käesoleva töö autor ettepaneku muuta senist KarS §-s 157^2 kasutatud lähenemisviisi ning asendada identiteedivarguse sättes sisalduv isikuandmete mõiste näiteks U.S.C-s kasutatava mõistega "identifitseerimisvahend". Toodud termin võimaldaks sätet kohaldada ka juriidiliste isikute kohta käiva informatsiooni väärkasutamise juhtumite puhul ning laiendaks kaitset samuti muule füüsilist isikut tuvastada võimaldava informatsiooni väärkasutamisele lisaks isikuandmetele. Teise võimalusena näeb autor ette isikuandmete kaitse seaduse muutmist selliselt, et seadusest tulenev kaitse laieneks ka juriidiliste isikute kohta käivatele andmetele. Kuid sellisel juhul peaks probleemi lahendamiseks kaaluma muuhulgas isikuandmete enda mõiste laiendamist selliselt, et isikuandmetena oleks võimalik mõista ka küberruumis isikute kohta käivat informatsiooni nagu IP-aadress, blogi või

[139] R. Tigner. Belgium - Court condemns identity theft on Facebook. Technology, Media & Telecommunications News, Linklaters 2012. Arvutivõrgus: http://www.linklaters.com/Publications/Publication1403Newsletter/TMT-News-July-2012/Pages/Belgium-Court-condemns-identity-theft-on-Facebook.aspx, 29.04.2014.
[140] Seletuskiri 530 SE I, lk 7.

telefoninumber. Viimase variandiga kaasnevate määratlemisprobleemide tõttu peaks autori hinnangul eelistama pigem esimesena pakutud lahenduse kasutuselevõttu.

2.2.2. Identiteedivarguse reguleerimisfaasid karistusseadustikus

2.2.2.1. Ettevalmistusstaadium

Ettevalmistusstaadiumi internetiga seotud identiteedivarguste puhul moodustab näiteks isikuandmete kogumiseks arvutisüsteemi salvestatava või edastatava arvutiprogrammi, nuhkvara või pahavara väljatöötamine.

Töö alapeatükkides 1.2.1.2. ning 1.2.2.2. leidis autor Arvutikuritegevusvastasest konventsioonist ning direktiivist 2013/40 sätteid, mis küll ei reguleeri otseselt identiteedivargusega seonduvat, kuid mida on võimalik kohaldada internetiga seotud identiteedivarguse ettevalmistusstaadiumile.

Kuigi KarS §-s 157^2 sätestatud identiteedivarguse eriregulatsioon identiteedivarguse ettevalmistamist koosseisutunnusena ette ei näe, siis reguleerib Eesti karistusseadustikus arvutikuriteo ettevalmistamist arvutikuritegevusvastase konventsiooni alusel sätestatud KarS § 216^1, mis näeb ette vastutuse KarS §-s 206, 207, 208, 213 või 217 sätestatud kuritegude toimepanemise eesmärgil selleks vastavalt kavandatud või kohandatud seadme, programmi, ka salasõna, kaitsekoodi või muude arvutisüsteemile juurdepääsuks vajalike andmete valmistamise, valdamise, levitamise või muul viisil kättesaadavaks tegemise eest, samuti muude käesolevas paragrahvis nimetatud kuritegude toimepanemiseks vajalike andmete kasutamise, levitamise või muul viisil kättesaadavaks tegemise eest. Identiteedivargust reguleerib nimetatud säte vaid niivõrd, kuivõrd selliste programmide või seadmete tööeesmärgiks on hõivata või väärkasutada personaalseid isikuandmeid KarS §-s 206, 207, 208, 213 või 217 sätestatud viisidel või siis, kui arvutisüsteemile juurdepääsuks vallatakse teiste isikute isikuandmeid. Toodud regulatsioon vastab identiteedivarguse seisukohalt Arvutikurtegevusvastase konventsiooni Art-s 6 ning direktiivi 2013/40 Art-s 7 sätestatule ning seega on karistusseadustik kooskõlas Arvutikuritegevusvastasest konventsioonist ning direktiivist 2013/40 tulenevaga osas, milles näeb ette vastutuse identiteedivarguse ettevalmistamisstaadiumi kriminaliseerimise võimalikkuse eelnevalt toodud juhtumite puhul.

Arvutiandmete võltsimine, mis on seotud eelkõige *phishing* skeemidega, on sätestatud vaid Arvutikuritegevusvastase konventsiooni Art-s 7. Direktiivis 2013/40 ega ka Eesti karistusseadustikus toodud tegevust kriminaliseeritud ei ole. Iseenesest on isikutele

saadetavate e-kirjade võltsimine ning selle kaudu nende arvuti paha- või nuhkvaraga nakatamine üheks levinumaks isikuandmete kogumise meetodiks, mistõttu on sellise tegevuse kriminaliseermine autori hinnangul põhjendatud.

Olgugi, et karisutsseadustikust ei tulene sõnaselgelt toodud meetodile iseloomuliku tegevuse karistatavus, reguleerib sellist tegevust KarS § 208, mis näeb ette vastutuse nuhkvara, pahavara või arvutiviiruse levitamise eest. Identiteedivargusega seondub eeltoodu niivõrd, kuivõrd edastatava nuhkvara, pahavara või arvutiviiruse tööeesmärgiks on koguda isikuandmeid. Toodud tegevus kuulub identiteedivarguse ettevalmistusstaadiumisse, kusjuures KarS § 216^1 alusel on karistatavaks juba ka sellise tegevuse enda ettevalmistamine.

Karistusseadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõust 554 SE tulenevalt tunnistatakse aga KarS § 208 kehtetuks. Seda põhjusel, et hoolimata sätte tõlgendusest on nimetatud tegevus hõlmatud juba kas KarS § 216^1 või KarS §-dega 206, 207 ja 217 tooduga.[141] Samuti muudetakse KarS § 216^1 sõnastust, mille uue sõnastuse kohaselt sätestatakse vastutus seadme või arvutiprogrammi, mis on loodud või kohandatud eelkõige käesoleva seadustiku §-s 206, 207, 213 või 217 sätestatud kuritegude toimepanemiseks, või kaitsevahendi, mille abil on võimalik hankida juurdepääs arvutisüsteemile, hankimise, valmistamise, valdamise, levitamise või muul viisil kättesaadavaks tegemise eest, et panna ise või võimaldada kolmandal isikul panna toime käesoleva seadustiku §-s 206, 207, 2013 või 217 sätestatud kuritegu. [142] Identiteedivarguse ettevalmistusstaadiumi kriminaliseeritust kavandatavad muudatused oluliselt ei mõjuta, sest ka eelnevalt seostus säte identiteedivarguse ettevalmistamisega vaid niivõrd, kuivõrd isikuandmete hõivamine või nende hilisem kasutamine on seotud mõne paragrahvis suletud loeteluna toodud kuriteoga.

KarS §-s 216^1 toodud loetelus sisaldub KarS § 206, milleks on arvutiandmetesse sekkumine ning mille moodustab "arvututisüsteemis olevate andmete ebaseaduslik muutmine, kustutamine, rikkumine või sulustamine."[143] Eelnõus 554 SE sätestatakse nimetatud kuriteo juurde direktiivist 2013/40 tulenevalt raskendavad asjaolud nagu näiteks kuriteo toimepanemine grupi poolt või elutähtsa valdkonna süsteemis olevate andmete vastu. [144] Hetkel kehtiva karistusseadustiku kohaselt on KarS § 206 alusel karistatav lisaks eeltoodule ka arvutisüsteemi andmete või programmi ebaseaduslik sisestamine, mis muudatuse kohaselt enam kuriteokoosseisu ei kuulu. Põhjuseks on see, et kuivõrd selline koosseisutunnus ei

[141] Seletuskiri 554 SE, lk 61-62.
[142] Seletuskiri 554 SE Lisa 1, lk 6.
[143] Seletuskiri 554 SE, lk 61.
[144] *Ibid*, lk 61.

tulene ei Arvutikuritegevusvastasest konventsioonist ega ka direktiivist 2013/40 SE, siis on asutud seisukohale, et rahvusvahelised normiloojad on soovinud kaitsta õigustatud isiku selliseid huve, mis seonduvad juba olemasolevate andmetega.[145]

Seega, kui kehtiva seaduse kohaselt on karistatav isikuandmete kogumiseks loodud arvutiprogrammi, nuhkvara, pahavara või arvutiviiruse väljatöötamine, kui KarS § 208 koosseisu täitmiseks sellist programmi edastatakse või KarS § 206 täitmiseks seda näiteks kellegi arvutisüsteemi sisestatakse, siis eelnõuga 554 SE kavandatavate muudatuste kohaselt laieneb identiteedivarguse ettevalmistamisele karistusõiguslik kaitse sisuliselt vaid läbi KarS § 217, mille kohaselt on karistatav "arvutisüsteemile ebaseaduslikult juurdepääsu hankimine kaitsevahendi kõrvaldamise või vältimise teel."[146] Seega juhul, kui luuakse programm, mille eesmärgiks on saada juurdepääs ning koguda isikuandmeid ja selline programm on loodud kasutamiseks arvutisüsteemi kaitsevahendi vältimise või kõrvaldamise kaudu, siis laieneb autori hinnangul kaitseala ka identiteedivarguse ettevalmistusstaadiumile.

Seega KarS § 157^2 ise identiteedivarguse ettevalmistamisstaadiumit ei kriminaliseeri. Võttes aga arvesse, et läbi teiste karistusseadustikus sätestatud kuriteokoosseisude on teatud juhtudel siiski internetiga seotud identiteedivarguse ettevalmistamine karistatav, siis tekib autoril küsimus, kas oleks põhjendatud ette näha identiteedivarguse ettevalmistamise karistatavus ka identiteedivargust reguleerivas erikoosseisus.

Ettevalmistusstaadiumid on määratletuse nõudele[147] mittevastavuse tõttu enamikes riikides õigusriiklikel kaalutlustel jäetud kriminaliseerimata.[148] Ka Eestis on seega KarS §-st 25 tulenevalt karistatavaks vaid juba katsestaadiumisse jõudnud tegu ning vastutus ettevalmistuse eest kaasneb siis, kui selline asjaolu on ettenähtud eriosas toodud kuriteokoosseisus.[149] Juhul, kui KarS §-s 216^1 ning KarS § 217 sätestatu kõrval eksisteeriks identiteedivarguse ettevalmistamine koosseisutunnusena ka KarS §-s 157^2, siis oleks viimase näol tegemist erinormiga ning spetsiaalsuspõhimõtte (*lex specialis derogat legi generali*)

[145] Seletuskiri 554 SE, lk 60.
[146] *Ibid*, lk 65.
[147] "PS § 23 lg-st 1 ja § 13 lg-st 2 tulenev karistusseaduse määratletuse nõue eeldab, et isiku teole antav karistusõiguslik väljendus ehk kvalifikatsioon vastaks võimalikult täpselt isiku faktilisele teole." Vt: RKKKo 24.10.2005, 3-1-1-83-05, p 8. (Põhja Ringkonnaprokuratuuri eriasjade prokurör Laura Feldmanise kassatsioon Tallinna Ringkonnakohtu 28. märtsi 2005. a otsuse peale Kalle Mälbergi ja Uno Siitani süüdistusasjas KrK § 141-1 lg 3 p 1 järgi.)
[148] J. Sootak. Karistusõigus.Üldosa. Tallinn: Juura 2010, lk 469, IX p 9. Edaspidi allmärkustes: KarS Üldosa.
[149] Nimetatut on korduvalt rõhutanud ka Riigikohtu kriminaalkolleegium. Vt: RKKKo 05.05.2003, 3-1-1-17-03, p 20. (Vitali Semjonovi kaitsja vandeadvokaat Aleksander Glikmani kassatsioonkaebus Tartu Ringkonnakohtu kriminaalkolleegiumi 19.11.2002 otsusele Vitali Semjonovi süüditunnistamises KrK § 15 lg 1 ja § 100 järgi.)

kohaselt tuleks konkurentsi korral üld- ja erinormi vahel kohaldada erinormi.[150] Spetsiaalnormina hõlmaks KarS § 157[2] sellisel juhul nii KarS §-s 216[1] kui ka §-s 208 sätestatud koosseisutunnused isikuandmete hõivamisega seotud osas, kuid lisaks sinna veel ülejäänud identiteedivarguse elemendid.[151]

Võttes aga arvesse, et KarS-is sisalduv identiteedivarguse koosseis peab hõlmama ka väljaspool internetikeskkonda toime pandud identiteedivarguse juhtumeid, siis asub autor seisukohale, et ettevalmistusstaadiumi alla käivate tegevuste maht võib minna liialt suureks ning nende määratlemine muutuda võimatuks. Töö punktis 2.2.1. tõi autor näiteid Eesti kohtupraktikast, kus kuriteos kahtlustatavad isikud esitlesid end terve kriminaalmenetluse vältel teise isikuna. Nimetatud kaasuste puhul kasutasid isikuandmete väärkasutajad teise isiku kohta käivat informatsiooni väga vähesel määral. Peamiselt kasutati vaid nime, elukoha aadressi ning sünniaega. Võttes arvesse, et identiteedivarguste toimepanemine ei pruugi olla massiline, vaid võibki toimuda vaid ühe isiku poolt ühe isiku suhtes, kelle andmed on isikule teatavaks saanud igapäevaelu käigus, siis muutub identiteedivarguse ettevalmistamise kriminaliseerimine isikuandmete hõivamise planeerimise näol praktiliselt võimatuks.

Samuti on autor seisukohal, et hoolimata asjaolust, et KarS § 216[1] ning § 217 kaudu saab sedastada identiteedivarguse ettevalmistamise karistatavust vaid väga piiratud juhtumite puhul, siis on nimetatud juhtumite näol tegemist internetiga seotud identiteedivarguste korral levinuimate, suurimat eeltööd nõudvate ning kurjategija professionaalsust vajavate meetoditega mille puhul on põhjendatud näha ette vastutus ka ettevalmistamise eest.

Muus osas asub autor aga seisukohale, et õigusselguse huvides ning ülekriminaliseerimise vältimiseks on siiski põhjendatud loobuda ettevalmistusstaadiumi sätestamisest identiteedivarguse erikoosseisu tunnusena ning näha ette vastutus nimetatud tegevuse eest ohtlikumate juhtude puhuks vaid läbi teiste karistusseadustiku eriosa kuriteokoosseisude.

2.2.2.2. Informatsiooni hõivamine

Informatsiooni hõivamise faasi moodustab näiteks eelnevalt mainitud nuhkvara, arvutiviiruste või muude programmide kasutamine, mis on suunatud isikuandmete kogumisele. Samuti

[150] RKKKo 02.06.2011, 3-1-1-28-11, p 13.2. (Simmo Saare kaitsja vandeadvokaat Aivar Pilve ja Lääne Ringkonnaprokuratuuri ringkonnaprokurör Elle Keemani kassatsioonid Tallinna Ringkonnakohtu 14. detsembri 2010. a kohtuotsuse peale kriminaalasjas Simmo Saare ja Mart Viisitamme õigeksmõistmises süüdistuses KarS § 217-2 lg 1 ja § 25 lg 2 ning § 157 järgi.)
[151] KarS Üldosa, lk 125, III/147.

kuulub nimetatud etapi alla muude meetodite kasutamine, mis toovad kaasa isikuandmete hõivamise.

KarS §-s 157^2 sisalduv identiteedivarguse koosseis isikuandmete hõivamise tegu karistatavaks ei pea. Samuti räägib direktiivi 2013/40 Art 9 p-s 5 sätestatud identiteedivargus isikuandmete väärkasutamisest, mitte aga isikuandmete hõivamisest. Sarnaselt ettevalmistusstaadiumiga on aga ka isikuandmete hõivamise faas karistatav läbi teiste karistusseadustikus sisalduvate kuriteokoosseisude. Nagu öeldud on isikuandmete hõivamisega seotud Arvutikuritegevusvastase konventsiooni Art-d 2, 3, 4 ja 5 ning direktiivi 2013/40 Art-d 3, 4, 5 ja 6.

Arvutikuritegevusvastase konventsiooni Art-s 2 ning direktiivi 2013/40 Art-s 3 on sätestatud arvuti- või infosüsteemi ebaseaduslik sisenemine. Karistusseadustikus kriminaliseerib taolist tegevust KarS § 217, mida karistusseadustiku muutmise eelnõuga 554 SE muudetakse selliselt, et karistatavaks on kaitsevahendi kõrvaldamise või vältimise teel ebaseaduslikult arvutisüsisteemile juurdepääsu hankimine. Muudatuse põhjuseks on asjaolu, et normi senine pealkiri oli eksitav ning karistatav on juba arvutisüsteemile juurdepääsu hankimine, mitte aga ainult alles selle hilisem kasutamine.[152] Identiteedivarguse seisukohalt on sellise tegevuse karistatavus asjakohane, sest arvutisüsteemi või infosüsteemi ilma loata sisenemine ja selle kasutamine võib olla toime pandud isikuandmete kogumiseks ning on oluline tagada isikutele kaitse ka nende isikuandmete sellisel viisil hõivamise eest.

Karistusseadustik ei sätesta kuriteona otseselt arvutiandmete pealtkuulamist nende konfidentsiaalse edastamise ajal, kuid milline tegevus peaks olema kriminaliseeritud Arvutikuritegevusvastase konventsiooni Art-st 3 ning direktiivi 2013/40 Art-st 6 tulenevalt. Taolise tegevuse kriminaliseerimist eraldi koosseisuna ei ole ette nähtud ka karistusseadustiku muutmise seaduse eelnõuga 554 SE. Identiteedivarguste toimepanemiseks vajaminevate isikuandmete hõivamine võib toimuda aga ka selliste andmete konfidentsiaalse edastamise pealtkuulamise teel. Toodud tegevus on kriminaliseeritud läbi KarS §-s 137 sätestatu, mis näeb ette vastutuse jälitustegevuse eest teise inimese kohta käivate andmete kogumise eesmärgil selleks seadusliku õiguseta isiku poolt. KarS § 137 objektiivne koosseis sisaldab teona teise inimese jälgimist jälitustegevuseks seadusliku õiguseta isiku poolt. Inimese jälgimine hõlmab näiteks tema korduvat või pikemaajalist visuaalset vaatlemist vahetult või tehniliste seadmete abil, inimeste või asjade kohta andmeid sisaldavate andmekogude või ka

[152] Seletuskiri 554 SE, lk 64.

sõnumite salajast läbivaatamist või pealtkuulamist.[153] Selliselt on KarS § 137 kaudu tagatud kaitse ning ette nähtud vastutus ka arvutiandmete ebaseadusliku ebaseadusliku pealtkuulamise eest nende konfidentsiaalse edastamise ajal, kui eesmärgiks on koguda teise isiku kohta käivaid isikuandmeid.

Arvutüsteemi sekkumine ja arvutisüsteemi toimimise oluline takistamine peavad kriminaliseeritud olema Arvutikuritegevusvastase konventsiooni Art-test 4 ja 5 ning direktiivi 2013/40 Art-test 5 ja 4 tulenevalt. Sellised tegevused on sätestatud karistusseadustiku §-des 206 ning 207. Eelnõuga 554 kavandatakse muudatusi mõlemas eelnevalt nimetatud paragrahvis. Muudatuste eesmärgiks on viia sätted vastavusse direktiivist 2013/40 tulenevate nõuetega. Identiteedivarguse seisukohalt kavandatavad muudatused isikuandmete hõivamise kriminaliseeritust toodud sätete alusel ei mõjuta. Seega on nii kehtivate kui ka muudetavate õigusnormide alusel karistavaks isikuandmete hõivamine arvutiandmetesse sekkumisega, näiteks paha- või nuhkvara edastamisega ning samuti kui sellega takistatakse oluliselt arvutisüsteemi toimimist.

KarS §-s 213 reguleerib isikuandmete hõivamisega seonduvat veel näiteks arvutikelmus osas, mil andmetöötlusprotsessi on sekkutud selleks, et hõivata isikuandmeid. Samas ei jää ka toodud säte karistusseadustikku planeeritavatest muudatustest puutumata. Kavandatav säte kriminaliseerib teisele isikule kahju tekitamise andmete ebaseadusliku muutmise, kustutamise, sisestamise, rikkumise, sulustamise ning andmetöötlusprotsessi muul viisil sekkumise teel vaid niivõrd, kuivõrd see on seotud varalise kasu saamise eesmärgiga. Hetkel kehtiva KarS § 213 kohaselt ei ole varalise kasu saamise eesmärki koosseisutunnusena sätestatud. Seega olukorrale, kus andmetöötlusprotsessi sekkumine on suunatud isikuandmete hõivamisele, millele ei järgne varalise kasu saamist, Eestis karistusõiguslik kaitse edaspidi ei laiene. Samas sedastab autor, et arvutikelmust reguleeriva sätte kohaldamine isikuandmete hõivamise faasis oleks pigem erandlik, sest kohaldub eelkõige isikuandmete kasutamise etapis näiteks krediitkaardi pettuste korral.

Ka isikuandmete hõivamise puhul saab sedastada selle kriminaliseeritust läbi teiste kuriteokoosseisude, mis tõstatab jällegi küsimuse selle sätestamisest KarS § 157^2 koosseisutunnusena. Sarnaselt ettevalmistusstaadiumiga näeb autor aga ohtu, et isikuandmete hõivamise kriminaliseerimine identiteedivarguse erikoosseisus võiks kaasa tuua määratlemise nõudele vastavusega seonduvad probleemid, sest isikuandmete hõivamiseks kasutatavaid

[153] M. Kurm, T. Ploom Kars § 137/ p 3.3. - KarSK

meetodeid võib olla palju ning teatud juhtudel võib identiteedivarguseks kasutatav informatsioon olla kurjategijani jõudnud juhuslikult või seaduslikul viisil.

Lisaks tuleks hinnata, kas isikuandmete hõivamine võib vastata KarS § 25 lg 1 kohaselt kuriteokatse tunnustele, juhul, kui isikuandmete hõivamisega on kurjategija vastavalt enda ettekujutusele vahetult alustanud teo toimepanemist. Nimetatu toob sellegipoolest kaasa piiritlemisprobleemi ettevalmistusstaadiumist, sest ka "Riigikohus on korduvalt selgitanud, et katse ja ettevalmistamine on erinevad kuriteo toimepanemise staadiumid, mida tuleb selgelt eristada."[154] Riigikohtu seisukohast tulenevalt on üksiktäideviija puhul katse alguspunkti võimalik määratleda objektiivsete ning subjektiivsete elementide kaudu. Subjektiivse külje moodustab isiku ettekujutus ning plaan täideviidavast teost. Objektiivsed elemendid on selleks, et hinnata, kas ning millises ulatuses on täideviija enda kavandatud plaani ellu viinud. Katse alustamiseks on oluline, et isik alustaks vahetult kuriteokoosseisu elluviimist. Juhul kui kuriteokoosseisu elluviimise alustamiseks on vajalik teha veel mingi tegu või muu käitumisakt, siis on täideviija oma tegevusega alles ettevalmistusstaadiumis ega ole süüteokatsega vahetult alustanud. Kuriteokoosseisu ellu viiva tegevusega alustamist tuleb Riigikohtu sõnul "hinnata ning otsustada konkreetse juhtumi asjaolude põhjal, võttes arvesse nii süüteo liiki kui ka täideviija süüteo toimepanemise plaani."[155]

Eeltoodust tulenevalt ei ole võimalik asuda ühesele seisukohale, kas isikuandmete hõivamine võiks teatud juhtudel olla käsitletav süüteokatse algusena. Autor leiab, et süüteokatse alguseks võiks isikuandmete hõivamist pidada siis, kui see nõuab suuremahulist eeltööd ning moodustab olulise osa identiteedivarguse toimepanemiseks kavandatud koguskeemist. Siiski võib reaalses elus tekkida olukordi, kus on raske eristada, millal on isikuandmete hõivamine ebaseaduslik ning millal on informatsiooni enda valdusesse saamine olnud juhuslik ning osa igapäevaelust. Samuti on praktikas tõenäoliselt väga raske või lausa võimatu isiku tegelikke kavatsusi välja selgitada ning tõendada. Internetiga seotud identiteedivarguste korral saab isikuandmete hõivamise ebaseaduslikkust tõenäoliselt sedastada küll kergemini, sest nimetatud tegevus nõuab reeglina põhjalikumat ettevalmistust. Siiski leiab autor, et isikuandmete hõivamist ei saa veel pidada kuriteokoosseisu elluviiva tegevuse alustamiseks, sest isikuandmete hõivamise näol on tegemist KarS §-s 157^2 sätestatud tegevustele eelneva staadiumiga, mis seisab liiga kaugel kuriteokoosseisus kriminaliseeritud tegevusest.

[154] Riigikohtu kriminaalkolleegiumi määrus (RKKKm) 01.02.2012, 3-1-1-105-11, p 19. (Marko Armas Juvoneni kaitsja vandeadvokaat Jugans Grossmanni määruskaebus Tallinna Ringkonnakohtu 26. septembri 2011. a määruse peale, millega jäeti Harju Maakohtu 8. septembri 2011. a vahistamismäärus muutmata.)
[155] RKKKo 3-1-1-17-03, *op. cit 149,* p 26.

Muuhulgas on autor seisukohal, et olulisematel interneti ning arvutiga seotud juhtudel on isikuandmete hõivamise staadium kriminaliseeritud läbi teiste karistusseadustiku koosseisude, mistõttu ei ole vajalik isikuandmete hõivamise faasi identiteedivarguse regulatsioonis eraldi koosseisutunnusena ette näha.

2.2.2.3. Informatsiooni omamine või edastamine

Nimetatud faasi alla, nagu sõnastusest nähtub, paigutub identiteedivarguse toimepanemiseks vajaliku isikute kohta käiva informatsiooni omamine või edastamine. Tegemist on kolmanda sammuga isikuandmete saamiseks vajalike ettevalmistustoimingute ning isikuandmete hõivamise järel. Esmapilgul ehk triviaalsena tunduva etapi puhul tõusetub aga mitmeid lahendamist vajavaid küsimusi. Esiteks, milliste andmete omamine või edastamine täidab kuriteokoosseisu ning teiseks, millal on sellise informatsiooni omamine või edastamine kuritegelik.

Informatsiooni enda poolest eeldab kuritegelik käitumine seda, et valduses olevad või edastatavad andmed kuuluksid enda iseloomult identiteedivargust kriminaliseeriva sätte kuriteokoosseisu elementide hulka. Näiteks karistusseadustikus sisalduva sätte kohaselt saab selliseks informatsiooniks pidada seega vaid isikut tuvastavaid või tuvastada võimaldavaid isikuandmeid. Karistusseadustikus sisalduv identiteedivarguse regulatsioon ei näe kuriteo koosseisutunnusena ette isikuandmete tema nõusolekuta omamist, vaid sätestab vastutuse nende edastamise, nendele juurdepääsu võimaldamise ning nende kasutamise eest. Ka direktiivi 2013/40 Art 9 p 5 kriminaliseerib ainult isikuandmete väärkasutamise. Samuti ei leidnud autor Arvutikuritegevusvastasest konventsioonist ning direktiivist 2013/40 teisi nimetatud staadiumiga seonduvaid sätteid.

IKS § 5 kohaselt on iga isikuandmetega tehtav toiming, sealhulgas nende salvestamine, korrastamine, kogumine, säilitamine, muutmine ja avalikustamine, samuti nendele juurdepääsu võimaldamine, päringute teostamine ja väljavõtete tegemine, kasutamine, edastamine ning ristkasutamine, ühendamine, sulgemine, kustutamine või hävitamine isikuandmete töötlemine, mistõttu on need tegevused omavahel seotud ning peavad vastama seaduses toodud ühistele nõuetele. Kõik isikuandmete töötlemisega seonduvad tegevused kuriteokoosseisu tunnustena eeldavad, et nimetatud tegevused oleksid ebaseaduslikud.

KarS § 157^2 seob isikuandmete edastamise, nendele juurdepääsu võimaldamise ning kasutamise ebaseaduslikkuse andmesubjekti nõusoleku puudumisega. Riigikohtu kriminaalkolleegium on selgitanud, et tunnus "ebaseaduslik" võib esineda blanketse

koosseisutunnusena, mille sisustamine toimub karistusseadusest väljapoole jäävate õigusnormidega või süüteokoosseisu dispositsioonis kirjeldatud käitumisena, mis on mingist konkreetsest normist tulenevalt eelduslikult alati ebaseaduslik.[156] Autori hinnangul on identiteedivarguse sätte puhul tegemist viitenormiga, mille sisustamiseks tuleb pöörduda era- või avaliku õiguse asjakohase normatiivakti poole, mis täidab karistusõiguse koosseisu normiblanketi ning kuulub lahutamatult koosseisu hulka.[157]

Isikuandmete töötlemiseks kehtestab nõuded IKS § 10 lg 1, mille kohaselt on isikuandmete töötlemine ebaseaduslik kui selleks ei ole andmesubjekti nõusolekut või muud seadusest tulenevat alust. Seega tuleb isikuandmete töötlemise lubatavus kõne alla siis, kui andmesubjekt on enda isikuandmed avalikustanud ise või andnud nende töötlemiseks nõusoleku (IKS § 10 lg 2). Lubatavuse alusena võib esineda ka näiteks isikuandmete töötlemine ajakirjanduslikul eesmärgil ning nende avalikustamine meedias, kui selleks on ülekaalukas avalik huvi ning kui see on kooskõlas ajakirjanduseetika põhimõtetega. Andmete avalikustamine ei tohi sealjuures aga ülemääraselt kahjustada andmesubjekti õigusi (IKS § 11 lg 2). Samuti on andmete töötlemine lubatud IKS § 11 lg-tes 6 ja 7 sätestatud juhtudel isiku krediidivõimelisuse hindamiseks. Lisaks on seadusega lubatud isiku kujutise avalikustamine, kui see on jäädvustatud avalikul üritusel, mille avalikustamise eesmärgil jäädvustamist võib mõistlikult eeldada. Kui tegemist ei ole avaliku üritusega, tuleb isikut enne tema kujutise jäädvustamist selle avalikustamisest teavitada ning anda talle võimalus enda jäädvustamist soovi korral vältida (IKS § 11 lg 8).

Juhul kui andmetöötlejal puudub muu seadusest tulenev alus, ega esine ka mõni eelnevalt loetletud eranditest, siis peab isikuandmete töötlusprotsessi lubatavuseks esinema andmesubjekti nõusolek. Isiku nõusolekuks IKS §-st 12 tulenevalt, ning seda ka karistusseadustiku tähenduses, on üldjuhul andmesubjekti kirjalikku taasesitamist võimaldavas vormis esitatud tahteavaldus, mis tugineb isiku vabale tahtele ning millega ta lubab enda isikuandmeid töödelda. Selline nõusolek peab olema piisavalt täpne ning määratlema andmed, mille töötlemiseks luba antakse, samuti nende töötlemise eesmärk ning isikute ring, kellele andmete töötlemise luba antakse. Lisaks eeltoodule peab IKS § 12 kohaselt nõusolek sisaldama andmete kolmandatele isikutele edastamise tingimusi.

Nõusolek isikuandmete töötlemiseks peab olema ka juhul, kui isik on ise enda isikuandmed

[156] RKKKo 13.12.2013, 3-1-1-106-13, p 9. (Harry Mäkkeri kaitsja vandeadvokaadi vanemabi Anne Vissaku kassatsioon Tallinna Ringkonnakohtu 23. aprilli 2013. a kohtuotsuse peale kriminaalasjas Harry Mäkkeri süüdistuses KarS 291 järgi.)
[157] J. Sootak. Viiteline norm ja koosseisuteo ebaseaduslikkus. Juridica 2014/2, lk 160-161.

avalikustanud. Hoolimata nõusolekule kehtestatud nõuetest võib sellega praktikas kaasneda mitmeid probleeme. Nagu autor eelnevalt sedastas, on internetiga seotud identiteedivarguste puhul üha suurenevaks probleemiks erinevad internetikeskkonna suhtlusportaalid, kuhu inimesed ise enda andmeid ülesse laevad ning avalikustavad. Probleeme nimetatud portaalide puhul tekitab lisaks andmete kättesaadavaks muutumisele ka piiritlemine, millisel juhul isiku enda poolt avalikustatud andmete edasine töötlemine või avalikustamine on keelatud. Olukorra muudab keeruliseks asjaolu, et liitudes erinevate suhtlusportaalidega ei pööra inimesed tähelepanu tingimustele, millega nad liitumisprotsessi käigus nõustuvad. Näiteks sisaldab tänapäeval üha enam populaarsust kogunud suhtlusportaali „facebook[158]“ andmekasutuspoliitika tingimusi, millistel juhtudel ja millisel moel võib portaal talle andmesubjekti poolt avalikustatud andmeid töödelda. Uus kasutaja nõustub ja annab liitumisel loa, et tema poolt avalikustatud andmeid ja muid andmeid, mida portaal muul viisil tema kohta saab, on nimetatud suhtlusportaalil õigus erinevatel eesmärkidel kasutada. Andmeid võivad nad avaldada ning edastada, kui nad on teavitanud andmete avaldamisest isikut või kui andmetelt on eemaldatud identifitseerimist võimaldavad isikuandmed.[159]

Olgugi, et kasutajad annavad enamikel juhtudel juba portaalidega liitumisel nõusoleku enda isikuandmete töötlemiseks, seab sellele piiranguid Euroopa Liidu direktiiv 95/46/EÜ, mille Art-test 6, 7, 10–12, 14, 18–21 ja 23 tulenevalt peab isikuandmeid töötlema õiglaselt ja seaduslikult, selgelt õiguspärastel ning selgelt määratletud eesmärkidel, isikuandmed peavad olema piisavad ja asjakohased ega tohi ületada selle otstarbe piire, mille tarvis neid kogutakse või hiljem töödeldakse, andmed peavad olema täpsed ja vajaduse korral ajakohastatud, vastu peavad olema võetud mõistlikud meetmed, et kustutada või parandada andmete kogumise või hilisema töötlemise eesmärgi seisukohast ebaõiged või mittetäielikud andmed ning isikuandmed peavad olema säilitatud kujul, mis võimaldavad andmesubjekte tuvastada ainult seni, kuni see on vajalik seoses andmete kogumise või hilisema töötlemise eesmärkidega. Seega on ka isiku enda poolt avalikustatud andmed kaitstud isikuandmete töötlemist reguleerivate õigusaktidega ning nende edasine töötlemine interneti portaalide poolt ei saa olla piiramatu.

Juhul kui suhtlusportaalis avalikustatud andmeid kasutab aga kolmas isik, näiteks mõni teine portaali kasutaja, kellel selleks luba puudub, on olukord mõnevõrra keerulisem. Tuleb kaaluda, kas andmesubjekt ise oma isikuandmeid avalikustades annab loa nende samas mahus

[158] www.facebook.com, 23.04.2014.
[159] Facebook.com. Andmekasutuspoliitika. Arvutivõrgus: http://www.facebook.com/about/privacy/your-info#howweuse, 29.04.2014.

edasisele töötlemisele ka kolmandale isikule. Õiguskirjanduses on jõutud järeldusele, et selleks, et tagada isikute tõhus kaitse nende isikuandmete töötlemisele teiste kasutajate poolt, tuleks nõustuda Euroopa Komisjoni ettepanekuga töötada sotsiaalvõrgustike kasutajatele välja direktiivist tulenevate kohustuste lihtsustatud variant. Käesoleval hetkel võib mõnel juhul kohalduda teiste kasutajate poolt isikuandmete töötlemisele mitmeid erandeid, nagu näiteks isikuandmete töötlemine isiklikel ja kodustel eesmärkidel, isikuandmete töötlemine ajakirjandusliku, kirjandusliku või kunstilise eneseväljenduse eesmärgil. Need erandid võivad potentsiaalselt kehtida ka erinevate suhtlusvõrgustike kasutajate suhtes.[160]

Käesolev on identiteedivarguse kontekstis oluline eelkõige varikontode loomise puhul, kus isiku enda poolt mõnes suhtlusportaalis kasutatud isikuandmeid kasutatakse mõne teise, tihti ka ebasündsa suhtlusportaali profiili loomisel. Selline situatsioon esines eelnevalt mainitud 2010. a aset leidnud Virkko Ojare kohtuasjas. Sellisel juhul on andmete avalikustaja puhul enamasti tegemist mõne suhtlusportaali kaaskasutajaga või kolmanda isikuga, kes avalikustatud andmetele läbi interneti juurdepääsu omab. Siinkohal on selge, et ebasündsa konto loomisega internetis kahjustatakse isiku põhiseadusest tulenevaid õigusi informatsioonilisele enesemääramisele ja eraelu puutumatusele ning võib kaasa tuua andmesubjektist ebaõige ettekujutuse loomise ja kahjustada sealjuures isiku seadusega kaitstud õigusi ja huvisid. Seda, kas suhtlusportaalides avalikustatud andmete kasutamine võiks olla kolmandatele isikutele lubatud, tuleb kaaluda eelkõige läbi selle, kas kohalduvad eelpool mainitud erandid, mille valguses võiks isikuandmete kasutamine olla õigustatud ja õiguspärane. Kuriteokoosseis puudub näiteks siis, kui isikuandmete kasutamine või edastamine toimub isiklikel või tööalastel eesmärkidel.[161]

Täna kehtiva isikuandmete kaitse seaduse valguses saab siiski sedastada, et ka isiku enda poolt avalikustatud andmete osas ei saa vaikimisi eeldada isiku nõusoleku olemasolu nende edasiseks töötlemiseks või avaldamiseks kolmandate isikute poolt. Probleem võiks tekkida aga olukorras, kui kuriteokoosseisus autori eelneva soovituse järgselt asendada isikuandmete mõiste identifitseerimisvahendi mõistega ning laiendada KarS § 157^2 kohaldamisvõimalusi ka juriidilistele isikutele, kelle kohta käivatele andmetele isikuandmete kaitse seadus ei laiene. Sellisel juhul tuleks muuta ka sättes sisalduv ebaseaduslikkuse blanketne koosseisutunnus selliselt, et teise isikuna sättes loetletud kuritegelikel eesmärkidel oleks eelduslikult alati ebaseaduslik. Juhul, kui muuta aga isikuandmete kaitse seaduses sisalduvat isikuandmete

[160] C. Mody. Euroopa andmekaitsedirektiivi kohaldamine Facebooki kasutajatele. Juridica 2010/10, lk 725.
[161] Seletuskiri 530 SE I, lk 8.

mõistet, siis võiks isikuandmete edastamise, kasutamise ja nendele juurdepääsu võimaldamise ebaseaduslikkuse jätta seotuks andmesubjekti nõusoleku puudumisega.

Lahendades küsimuse tegevuse ebaseaduslikkusest, tuleb hinnata tegevuste enda kuriteokoosseisu kuulumise otstarbekust. Isegi kui andmete hõivamine on toimunud õiguspärasel viisil, siis ei pruugi sellele järgneda alati omamise õiguspärasust. Samas leiab autor, et igasugune isikuandmete ebaseaduslik omamine ei viita veel kavatsusele kasutada neid identiteedivarguse toimepanemiseks. Olukorras, kus isikul selline eesmärk aga tuvastatakse, kuuluks sarnaselt isikuandmete hõivamisele ka isikuandmete omamise etapp identiteedivarguse katsestaadiumisse, mida autor on käsitlenud täpsemalt alapeatükis 2.2.2.2. Seetõttu ei leia autor, et isikuandmete omamise faasi puudumine karistusseadustikus sisalduvast identiteedivarguse regulatsioonist tooks kaasa vastuolu identiteedivarguse üldiste ühtsete põhimõtetega tagatavate eesmärkidega.

Isikuandmete edastamise all peetakse eelnõu kohaselt silmas olukordi, kus isik ise ei soovi kogutud isikuandmeid kasutada, vaid edastab need kolmandale isikule. Vastutuse tekkimise aluseks on siinkohal teadmine sellest, et isik, kellele andmed edastati, neid kasutab või võib kasutada identiteedivarguse toimepanemiseks. Muuhulgas juhib eelnõu tähelepanu sellele, et teisele isikule isikuandmete edastamine võib olla käsitletav ka vahendliku täideviimisena.[162] Riigikohtu praktika kohaselt seda küll vaid juhul, kui vahendlik täideviija viib või kasutab ära vahendi eksimust selliselt, et ärakasutatud isik teostab vahendliku täideviija teoplaani tahtmatult.[163] Seega on isikuandmeid ebaseaduslikult edastanud isiku tegevuse puhul samuti vaja tuvastada subjektiivsest küljest vähemalt kaudse tahtluse olemasolu. Sama kehtiks ka juhul kui edastamise tegu ei sisalduks kuriteokoosseisu asjaoluna, vaid oleks karistatav karistusseadustikus sisalduva osavõtu institutsiooni kaudu, sest ka kaasaaitaja tegu peab subjektiivsete tunnuste poolest olema tahtlik ning lisaks peab tahtlus ulatuma ka täideviija teoni.[164]

Ebaseadusliku juurdepääsu võimaldamine isikuandmetele tähendab seda, et isikuandmeid õiguspäraselt valdav isik annab kolmandale isikule ebaseaduslikult sellistele andmetele ligipääsu, kuid ei edasta neid talle ise. Nimetatud tegevust ei leia identiteedivarguse eri käsitlusi koondavate etappide hulgast, kuid et andmete kuritarvitamine nendele juurdepääsu

[162] Seletuskiri 530 SE I, lk 7.
[163] RKKKo 09.09.2005, 3-1-1-64-05, p 11. (Andrus Kööp'i ja OÜ Mayersons kaitsja vandeadvokaadi vanemabi Tiit Vajaku kassatsioonid Tartu Ringkonnakohtu 15. veebruari 2005. a otsuse peale Andrus Kööp'i süüteoasjas KarS § 356 lg 2 ja OÜ Mayersons süüteoasjas KarS § 356 lg 3 järgi.)
[164] RKKKo 23.11.2009, nr 3-1-1-97-09, p 7.4. (Indrek Vainlo kaitsja vandeadvokaat Aivar Ennoki kassatsioon Tallinna Ringkonnakohtu 15. juuni 2009. a kohtuotsuse peale kriminaalasjas Indrek Vainlo süüdistuses KarS § 200 lg 2 p 7 - § 22 lg 3; § 215 lg 2 p 3 - § 22 lg 3 järgi.)

omavate isikute poolt on ühest viiest levinuimast informatsiooni saamise viisist[165], siis tuleb kahtlemata nõustuda selle tegevuse kriminaliseerimise vajalikkusega.

Nagu öeldud, ei kriminaliseeri karistusseadustiku identiteedivarguse säte isikuandmete omamist, samuti ei tee seda ka direktiivi 2013/40 regulatsioon. Samas kasutab direktiiv 2013/40 isikuandmete väärkasutamise mõistet, mille alla võib autori hinnangul mahtuda mitmeid erinevaid tegevusi, mis vastavad sättes nõutud eesmärgile ning kui sellise kasutamise teel on toime pandud artiklites 4 ja 5 osutatud kuriteod. Silmas tuleb pidada, et direktiivi 2013/40 regulatsioon ongi suunatud raskendava asjaolu loomisele, mistõttu ei saa ega peagi direktiivis sisalduv regulatsioon ette nägema kõiki võimalikke isikuandmetega tehtavaid toiminguid, mille kriminaliseerimine identiteedivarguse seisukohast peaks olema oluline, vaid on suunatud vaid artiklites 4 ning 5 kirjeldatud kuriteo toimepanemisega relevantsetele tegevustele.

Siiski on andmete ebaseaduslik omamine, edastamine ning nendele juurdepääsu võimaldamine tegevused, mis on lõppfaasis isikuandmete kasutamisega tugevalt seotud. Autori hinnangul on igati põhjendatud väljatoodud tegevuste kriminaliseerimine, sest kuigi karistusõigusel ei ole preventiivset, vaid ta omab retrospektiivselt repressiivset iseloomu, võib hirm kriminaalkaristuse ees isikuid siiski veenda hoiduma enda valduses olevate isikuandmete kergekäelisest edastamisest või neile juurdepääsu võimaldamisest. Võttes arvesse informatsiooni olulisust tänapäeva ühiskonnas ning selle kaitse tagamise tähtsust, siis on autori hinnangul karistusõiguse üldpreventiivseid eesmärke silmas pidades võrdväärselt tähtis isikute karistamine isikuandmete töötlemisel rikutud normide eest, et saata ühiskonnale sõnum õigushüve kahjustava teo keelatuse, keelava normi kehtivuse ja normi järgimise karistusvõimuga tagamise osas.[166]

2.2.2.4. Identiteediga seotud informatsiooni kasutamine kuritegelikel eesmärkidel.

2.2.2.4.1 Informatsiooni kasutamine

Isikuga seotud informatsiooni kasutamise näol on tegemist viimase identiteedivarguse etapiga. Isikuandmete kasutamine on kriminaliseeritud nii KarS §-s 157[2] kui ka direktiivi 2013/40 Art 9 p-s 5 toodud identiteedivarguse regulatsioonis. Kasutamise puhul on tegemist äärmiselt laia

[165] Vt: alaptk. 1.1.2.
[166] Karistusõiguse üld- ja eripreventiivse iseloomu kohta täpsemalt vt: J. Sootak. Karistusõiguse adekvaatsus – õiguse iseolemine ja mida ühiskond õigusest ootab. Ettekanne Presidendi mõttekojas. Ärma: 27.08.2010, lk 5. Arvutivõrgus: http://www.president.ee/images/stories/pdf/2010-08-27_jaan-sootak.pdf, 19.04.2014.

mõistega, mis võib endas sisaldada mitmeid erinevaid tegevusvorme. Seega peab koosseisutunnusena olema määratletud, milline või millisel eesmärgil isikuandmete kasutamine on karistatav.

Eeltoodust tulenevalt ei ole autori hinnangul kasutamine koosseisutunnusena sisustatav mitte tegevuste loetelu kaudu, vaid avab ennast läbi kasutamise eesmärkide või tagajärgede. Järgmises punktis käsitlebki autor, millistele eesmärkidele peab KarS § 157^2 ning direktiivi 2013/40 Art 9 p-st 5 tulenevalt olema isikuandmete kasutamine suunatud, et tegevus täidaks kuriteokoosseisu.

Kõnealuses faasis tõusetub teo kvalifitseerimise problemaatika. Kuivõrd isikuandmeid saab kasutada mitmel erineval viisil ning mitmel erineval eesmärgil, siis võib isikuandmete kasutamisega seonduv tegevus vastata ka mõne teise karistusseadustikus sätestatud kuriteokoosseisu tunnustele. Asjakohasteks on siin näiteks Kars §-s 157^1 sätestatud delikaatsete isikuandmete avalikustamine, kui näiteks libakonto loomisel kurjategija isiku kohta IKS § 4 lg-s 2 loetletud delikaatseid isikuandmeid avalikustab. Samuti KarS §-s 349 sätestatud tähtsa isikliku dokumendi kuritarvitamine, kui teise isikuna esinemiseks on kasutatud teise isiku nimele väljastatud KarS §-s 350 nimetatud dokumenti. Kõne alla võib tulla ka valeandmete esitamine, mis on sätestatud KarS §-s 280, kui ametiasutusele on valeandmetena esitatud teise isiku isikuandmeid. Kuivõrd käesoleva töö eesmärgiks on analüüsida identiteedivarguse sätte vastavust rahvusvahelistest õigusaktidest tulenevatele ja identiteedivarguse üldistest põhimõtetest tulenevatele nõutele ja eesmärkidele, siis ei käsitle autor töös täpsemalt teiste karistusseadustiku kuriteokoosseisudega tekkida võivat kogumi moodustamise problemaatikat peale Kars §-s 209 sätestatud kelmuse.

KarS §-s 209 sisalduv kelmus ning ka teised asjakohased kelmuse eriliigid, näiteks KarS §-s 213 sätestatud arvutikelmus, on identiteedivargustega enda olemuselt tugevalt seotud. Seda põhjusel, et kuigi KarS §-s 157^2 sisalduv identiteedivargus seob isikuandmete kasutamise vaid isikust ebaõige ettekujutuse loomise või kuriteo varjamise eesmärgiga, siis ei jää isikud ilma kriminaalõiguslikust kaitsest ka siis, kui selline eesmärk puudub ning tegevus on toime pandud varalise kasu saamise eesmärgil. Sellisel juhul võib tegevus sõltuvalt asjaoludest vastata, kas KarS §-s 209 toodud kelmuse või mõne karistusseadustikus sätestatud kelmuse eriliigi koosseisutunnustele. Enamikel sellistest juhtudest saab ilmselt tuvastada isiku kindla teadmise oma tegevusega kaasneva teisest isikust ebaõige ettekujutuse loomise osas. Selliselt võib osutuda võimalikuks otsesese tahtluse esinemine, mis on seotud isiku põhitagajärje, varalise kasu, saavutamise eesmärgiga ning kõrvaltagajärg, teisest isikust ebaõige ettekujutuse

loomine, on eesmärgiga paratamatult kaasnev.[167] Kuid, kui varalise kasu saamise eesmärgil toime pandud identiteedivarguse puhul saab sedastada isikust ebaõige ettekujutuse loomist ning sellega on tekkinud kahju isiku seadusega kaitstud õigustele või huvidele, siis ei täida isik siiski KarS §-s 157^2 sätestatud subjektiivset koosseisutunnust kavatsuse puudumise tõttu.

Piiritlemisprobleem kelmusega tekib aga olukordades, kus teise isikuna esinedes temast teadvalt ebaõige ettekujutuse loomise tulemusena on tekitatud kahju isiku seadusega kaitstud huvidele või õigustele või on olnud eesmärk varjata kuritegu ning on saadud ka varalist kasu. Varaline kahju tekib tavapäraste kelmuste korral mitte identiteedivarguse ohvriks langenud identiteedi tegelikule omanikule, vaid kolmandale isikule, kes on pettuse ohvriks langemise tulemusel teinud varakäsutuse. Eeltoodu selgitab identiteedivarguse ning kelmuse piiritlemisega seonduva problemaatika käsitlemist käesolevas töös, sest kurjategija teo kvalifikatsioon määratleb ära isikute ringi, keda kriminaalmenetluses kannatanuna käsitletakse. Võttes arvesse, et identiteedivarguse ning kelmuse puhul on reeglina tegemist kahe erineva kannatanuga, siis on identiteedivarguse juhtumite puhuks isikutele tagatava kaitse ulatuse väljaselgitamiseks vajalik määratleda, millistele kuritegudele peaks sellistel juhtudel kurjategija tegevus vastama.

KarS § 209 sätestab vastutuse varalise kasu saamise eest tegelikest asjaoludest teadvalt ebaõige ettekujutuse loomise teel. Illustreeriva näitena võib siin tuua näiteks olukorra, kus kurjategija A soovib kahjustada enda vihavaenlase B mainet, kuid soovib selle tulemusel ka ise varalist kasu saada. Selleks postitab A internetti fiktiivse müügikuulutuse, kus esineb internetis kauba müüjana kasutades selleks B isikuandmeid. Tegelikult B müügikuulutuses olevat kaupa ostjale edastada ei kavatse, kuid kaubast väga huvitatud C kannab pahaaimamatult ostusumma juba enne kauba saamist A poolt edastatud pangakontole. Sellisel juhul on kannatanuks nii identiteedivarguse ohvriks langenud B kui ka kelmuse ohvriks langenud ning varakäsutuse teinud C.

Toodud näite puhul on tegemist ideaalkogumiga, kus teoainsus vastab mitme süüteo koosseisutunnustele. PS §-s 23 ja KarS § 2 lg-s 3 sisalduva *ne bis in idem* põhimõtte kohaselt ei tohi aga sama süüteo eest kedagi karistada mitu korda. Näiteks on topeltkaristamise keeldu rikutud siis, kui isikut on sama teo eest karistatud nii kriminaal- kui ka väärteomenetluses.[168] Samuti on tegemist topeltkaristamise keelu rikkumisega, kui isikule mõistetakse karistus kahe süüteokoosseisu alusel, mille koosseisutunnustele ta käitumine vastas, kuid need

[167] KarS Üldosa, lk 299, VI/250.
[168] RKKKo 01.04.2004, 3-1-1-4-04, p 9. (Denis Stetsenko kassatsioonkaebus Tallinna Ringkonnakohtu kriminaalkolleegiumi 23.09.2003 otsusele Denis Stetsenko süüditunnistamises KarS § 184 lg 1 järgi.)

süüteokoosseisud on omavahel olulisel määral sarnased. Asjaolu, et ühele teole võib kohaldada mitut normi ei ole vastuolus Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni 7. lisaprotokolli At-ga 4[169] on kinnitanud ka Euroopa Inimõiguste kohus.[170] Toodud seisukohta on kinnitanud ka Riigikohus, kuid rõhutanud siiski, et juhul kui süütegude koosseisutnnused langevad olulisel määral kokku, siis tohib isikut karistada siiski vaid ühe süüteokoosseisu järgi.[171]

Riigikohus on teinud mitmeid KarS § 209 järgi kvalifitseeritud lahendeid, kus teise isikuna esinemise teel on saadud varalist kasu.[172] Siiski ei ole üheski neist tuvastatud varalise kasu saamise eesmärgi kõrval isiku eesmärki teise isikuna esinemise teel tekitada kahju tema seadusega kaitstud õigustele või huvidele, mistõttu puudub täna toodud probleemi lahendav kohtupraktika.

Autor on aga seisukohal, et hoolimata sellest, et kelmuse ja identiteedivarguse puhul on mõlemal juhul oluline, et loodud on ebaõige ettekujutus tegelikest asjaoludest või reaalsetest faktidest, siis eelnevalt toodud illustreeriva näite korral, kus teist isikut tuvastavate või tuvastada võimaldavate isikuandmete tema nõusolekuta kasutamine on toime pandud eesmärgiga luua teise isikuna esinemise teel temast teadvalt ebaõige ettekujutus, kui sellega on tekitatud kahju isiku seadusega kaitstud õigustele või huvidele ning eesmärgiga saada varalist kasu, on tegemist küll ühe teoga, kuid tegu on suunatud kahe erinevas kuriteokoosseisus asuva eesmärgi täitmisele ning toob kaasa kahe erineva isiku erineva sisuga õiguste kahjustamise. Seetõttu on autor seisukohal, et toodud juhtumi puhul kuriteokoosseisud olulisel määral pigem kokku ei lange ning isik tuleks süüdi mõista nii KarS §-s 157^2 kui ka KarS §-s 157^2 sätestatud kuriteo toimepanemise eest. Sama käsitlus kohaldub autori hinnangul siis, kui kurjategija täidab enda tegevusega identiteedivarguse teise alternatiivse eesmärgi ning kasutab teise isiku isikuandmeid selleks, et varjata seda sama enda poolt toimepandavat kelmust.

[169] Euroopa põhiõiguste ja vabaduste kaitse konventsiooni 7. lisaprotokoll. – RT II 1996, 11, 3.
[170] EIKo 29.05.2001, 37950/97, *Franz Fischer vs. Austria.* p 25.
[171] RKKKo 16.04.2007, 3-1-1-120-06, p 8. (Guldar Vinni kaitsja vandeadvokaadi vanemabi Raivo Bergsoni kassatsioon Tallinna Ringkonnakohtu 12. oktoobri 2006. a kohtuotsuse peale kriminaalasjas Guldar Vinni süüdistuses KarS § 424 järgi.)
[172] Vt näiteks: RKKKo 15.11.2010, 3-1-1-70-10. (Vello Loidi (Loit) kaitsja vandeadvokaat Liis Toomsalu ja Liis Haaveli kaitsjate vandeadvokaadi vanemabide Marina Leisi ja Owe Ladva kassatsioonid Tallinna Ringkonnakohtu 17. mai 2010. a kohtuotsuse peale kriminaalasjas Vello Loidi süüdistuses KarS § 209 lg 2 p-de 1, 2 ja 3 järgi ja Liis Haaveli süüdistuses KarS § 209 lg 2 p-de 1, 2 ja 3, § 349, § 213 ja § 199 lg 1 järgi.)

2.2.2.4.2. Kuritegelikud eesmärgid

2.2.2.4.2.1. Eesmärk luua teisest isikust ebaõige ettekujutus, kui sellega on tekitatud kahju isiku seadusega kaitstud õigustele või huvidele

KarS § 157^2 koosseisus sisaldub eesmärk luua teise isikuna esinemise teel temast teadvalt ebaõige ettekujutus. "Eesmärk on inimese teadliku teo taotletava tulemuse mõtteline kujund."[173] Seega on koosseisu täitmiseks oluline, et isikul oleks enda kujutluses tekkinud kavatsus isikust ebaõige ettekujutus luua, kuid selle eesmärgi saavutamine koosseisu täitmise seisukohalt enam oluline ei ole. Toodud seisukohta kinnitab ka Riigikohus, kes on KarS 184 lg 2^1 p-s 1 sätestatud kuriteokoosseisus sisalduva varalise kasu saamise eesmärgi kohta leidnud, et nimetatu kujutab subjektiivset koosseisutunnust, mis iseloomustab teo toimepanija käitumise sihte tema teadvuse tasandil. Tegemist on mittekongruentse süüteokoosseisuga, kus süüteo toimepanija eesmärk ulatub kaugemale objektiivsetest koosseisutunnustest.[174] Seega tuleb KarS § 157^2 puhul tuvastada teisest isikust ebaõige ettekujutuse loomise eesmärk, millele koosseisu objektiivsest küljest vaste puudub. Kusjuures teiste koosseisuelementide puhul piisab vaid vähemalt kaudse tahtluse tuvastamisest.

Eeltoodu tähendab, et KarS § 157^2 seisukohast ei ole oluline tuvastada, kas kellelgi isikust ebaõige ettekujutus reaalselt ka tekkis või mitte. Autor leiab, et isikutele efektiivse kaitse tagamise seisukohalt on tegemist väga olulise punktiga, tuues kaasa selle, et isik, kellena esinemise teel on temast loodud teadvalt ebaõige ettekujutus, ei pea talle tekitatud kahju nõudmiseks hakkama tõendama seda, kas kellelgi selle tegevuse tulemusena temast ebaõige ettekujutus reaalselt ka tekkis või mitte. Ebaõige ettekujutus on seotud eelkõige kolmandate isikute subjektiivsete omaduste ja hinnangutega ning võib juhtuda, et ei olegi võimalik tuvastada, milline oleks tegelik ettekujutus inimesest ning milline on sel juhul ebaõige. Seega on autori hinnangul igati põhjendatud, et kuriteokoosseis sisaldab vaid sellist eesmärki, ega sisalda koosseisutunnusena ebaõige kujutuse tekkimist ennast, mille tõendamine oleks kannatanu jaoks ilmselgelt liialt koormav või lausa võimatu.

Lisaks ebaõige ettekujutuse loomise eesmärgi tuvastamisele on koosseisu täitmiseks vajalik tuvastada ka isiku seadusega kaitstud õigustele või huvidele tekkinud kahju. Riigiprokuratuuri

[173] J. Sootak § 12/ p 15 - KarsK.
[174] RKKKo 23.05.2008, 3-1-1-18-08, p 17. (Arvo Laksbergi kaitsja vandeadvokaat Priit Tartu ja prokuratuuri kassatsioon Tallinna Ringkonnakohtu 28. detsembri 2007. a kohtuotsuse peale kriminaalasjas Arvo Laksbergi süüdistuses KarS § 184 lg 2-1 p 1 ja § 392 lg 2 p 2 järgi.)

juhise kohaselt on isiku õigusi kahjustavateks tegudeks näiteks tema nime alt e-kirjade saatmine, blogi pidamine, internetis kommenteerimine, suhtlusvõrgustike portaalidesse konto loomine ja muu sarnane tegevus. Kusjuures juhise kohaselt kahjustab isiku õigusi oluliselt see, kui eelpool nimetatud viisil edastatud informatsioon on ebaõige, solvav või laimav, mainet kahjustav, isikut naeruvääristav või rikub isiku suhteid teiste isikutega.[175] Seega tuleb huvide kahjustamise juures nentida, et ilmselt on kahjustatud isiku huve mistahes negatiivse ebaõige ettekujutuse loomise korral. Ka identiteedivarguse kriminaliseerinud seaduse eelnõu seletuskirjas 530 SE I on leitud, et koosseisu täitmiseks on oluline, et isikule omistatakse midagi, mida ta ise teinud ei oleks.[176]

Sätestades kahju tekkimise isiku õigustele või huvidele koosseisutunnusena on KarS § 157^2 näol tegemist tagajärjedeliktiga, mille puhul ei piisa vaid tagajärje väidetava saabumise deklareerimisest vaid "isiku süüditunnistamine tagajärjedelikti toimepanemises eeldab vältimatult lisaks koosseisupärase teo tuvastamisele ka selle tuvastamist, et on saabunud teost nii ajaliselt kui ruumiliselt eraldatud tagajärg, mis on käsitatav kas konkreetse välismaailma muudatusena või sellise põhjendatult ootuspärase muudatuse ärajäämisena. Samuti peab isiku süüditunnistamiseks tagajärjedelikti toimepanemises olema tõendatud, et koosseisupärased tegu ja tagajärg on omavahelises põhjuslikus seoses." [177] See tähendab, et kahju isiku seadusega kaistud õigustele või huvidele peab olema tõendatud ning tekkinud kahju peab olema põhjuslikus seoses teisest isikust ebaõige ettekujutuse loomise eesmärgil teda tuvastavate või tuvastada võimaldavate isikuandmete tema nõusolekuta edastamise, nendele juurdepääsu võimaldamise või nende kasutamisega.

Identiteedivargustega tekitatud kahju puhul on regulatsiooni kaitsealast tulenevalt kahju mõiste eelkõige seotud inimese põhiõiguste ja põhivabaduste rikkumisega.[178] Lisaks PS teises peatükis toodule võib põhiõigusteks formaalses mõttes pidada ka muudes peatükkides sätestatud individuaalseid õigusi, mis sisalduvad näiteks PS §-s 57, §-s 60 lg 1 lauses 2, 3, 4 ja lg 2 ning § 124 lg-s 2.[179] See tähendab, et mis tahes õigustamata või ebaseaduslik riive sellistele õigustele võib kaasa kaasa isiku põhiõiguste rikkumise. Samuti on Riigiprokuratuuri juhises on märgitud, et isiku seadusega kaitstud huvide all on silmas peetud nii põhiseadusest

[175] Riigiprokuratuur, *op. cit 132*, lk 1.
[176] Seletuskiri 530 SE I, lk 8.
[177] RKKKo, 10.40.2006, 3-1-1-117-05, p 26. (Lauris Kaplinski kaitsja vandeadvokaat Li Uiga kassatsioon Tartu Ringkonnakohtu 13. juuni 2005. a otsuse peale Lauris Kaplinski süüdistuses KarS § 151 järgi.)
[178] Vt: alaptk 2.1.1.
[179] Eesti Vabariigi põhiseaduse ekspertiisikomisjon. Põhiseaduse analüüs. Põhiseaduse 2. peatükk "Põhiõigused, vabadused ja kohustused", p 1.1. Justiitsministeerium. Arvutivõrgus: http://www.just.ee/10731, 30.04.2014.

kui ka VÕS-ist tulenevate õiguste rikkumist.[180] VÕS § 1046 lg 1 järgi on isiklike õiguste kahjustamisega tegemist näiteks õigusvastase isiku eraelu puutumatuse rikkumise, au teotamise, isiku kujutise või nime kasutamise korral. Praktikas seonduvadki identiteedivargused tihti just isiku hea nime ning au kahjustamisega.

Hea nime puhul on tegemist välimise objektiivse kategooriaga, mida kannab avalik arvamus. Au ja väärikuse riive võib seevastu aset leida ka mitteavalikult. Samas ei saa igasugust objektiivset heas usu kriitikat pidada au ning hea nime rikkumiseks. Au ja väärikuse kahjustamisega võib tegemist olla siis, kui inimesele on antud hinnang, talle omistatakse ebaõigeid väljaütlemisi, teda pannakse alandavatesse olukordadesse või omistatakse tegusid, mille eesmärk on isiku au ja väärikustunnet riivata, alandada, kahjustada või teotada. Hea nime kahjustamise puhul on tegemist inimese maine kahjustamisega avaliku arvamuse mõjutamise teel. Selleks võib olla näiteks meediakanalite, avaliku esinemise või küberruumi kaudu avalikustatud reputatsiooni kahjustavad avalikud hinnangud. Seega on oluliseks tunnuseks siin ründe pahatahtlik iseloom ning häbistav ja alandav viis.[181] See tähendab, et põhiseaduse §-s 17 nimetatud keeld teotada kellegi au ja head nime saab identiteedivarguse valguses kahjustatud siis, kui ettekujutus mis inimesest luuakse on isiku enda arvamuse kohaselt negatiivne. Mis puudutab aga näiteks enesemääramise õigust või eraelu puutumatust, saavad need autori hinnangul rikutud juba siis, kui andmeid on ebaseaduslikult kasutatud ning selle tulemusena sekkutud isiku eraellu ja piiratud enesemääramise õigust mistahes ebaõige ettekujutuse loomise korral.

Igal juhul toovad nimetatud rikkumised isikule kaasa ennekõike just mittevaralise kahju tekkimise. Isiku seadusega kaitstud õiguste ning huvide kahjustamisega tekkiva mittevaralise kahju võimalikkusega on nõustunud ka Riigikohus kriminaalkoodeksi[182] (KrK) §-s 161, mis sätestas vastutuse "ametiisiku poolt oma ametiseisundi tahtliku ärakasutamise eest, kui sellega põhjustati oluline kahju isiku, ettevõtte, asutuse või organisatsiooni seadusega kaitstud õigustele ja huvidele või riigi huvidele", ning käesolevaks ajaks kehtetuks tunnistatud[183] KarS §.s 289, mis sätestas vastutuse "ametiisiku poolt oma ametiseisundi ebaseadusliku ärakasutamise eest eesmärgiga tekitada või kui sellega on tekitatud oluline kahju teise isiku seadusega kaitstud õigustele või huvidele või avalikele huvidele", sätestatud tagajärgede sisustamisel. Autor leiab, et kuivõrd toodud paragrahvides on tagajärg sõnastatud

[180] Riigiprokuratuur, *op. cit 132*, lk 1.
[181] R. Maruste. PõhiSK § 17/ p 3. - E.-J. Truuväli, *op cit 95*.
[182] Kriminaalkoodeks. - RT 1992, 20, 288. (*Kehtetu alates 31.08.2002*)
[183] KarS § 289 tunnistati kehtetuks 15.03.2007 karistusseadustiku ja sellega seonduvate teiste seaduste muutmise seaduse § 9 p-s 41. Vt: Karistusseadustiku ja sellega seondute teiste seaduste muutmise seadus. - RT I 2007, 13, 69.

analoogiliselt KarS §-le 157^2, siis on võimalik KarS §-s 157^2 sätestatud kahju mõiste sisustamisel toetuda Riigikohtu tõlgendustele KrK §-s 161 ning KarS §-s 289 sisaldunud kahju mõiste selgitamisel. Selliselt on Riigikohus leidnud, et "kohaliku omavalitsuse seadusega õigustele ja huvidele tekitatud oluline kahju võib seisneda ka konkreetse asutuse, ametkonna või kogu riigi maine kahjustamises."[184] Samuti on Riigikohtu kriminaalkolleegium KrK § 166 sisustamisel tõdenud, et "kahtluse tekitamine ühe või teise institutsiooni või isiku aususes ja usaldusväärsuses on kahtlemata käsitletav moraalse kahjuna."[185]

Võttes arvesse, et Riigikohus on vältimatult aktsepteerinud kuriteo koosseisulise tunusena mittevaralist kahju võimalikkust, sest kriminaalõiguslikult kaitstakse ka väärtusi, mis ei ole rahaliselt hinnatavad[186] ning samuti arvestades KarS § 157^2 eesmärke, sättega kaitstavaid õigushüvesid ning toetudes Riigikohtu varasemale praktikale, siis tuleb autori hinnangul ilmselt jaatada, et KarS §-s 1572 sätestatud isiku õigustele ja huvidele tekitatud kahju mõiste hõlmab isikule tekitatud mittevaralise kahju juhtumeid.[187]

Mittevaralise kahju olemasolu tuleb aga tuvastada igal konkreetsel juhul eraldi.[188] Samas leiab autor, et isikuandmete kasutamise tagajärjel isikule tekitatud mittevaralise kahju tuvastamine võib menetlejale iseseisvalt olla praktiliselt võimatu ning põhineb eelkõige kannatanu enda subjektiivsel hinnangul. Ka Riigiprokuratuur on identiteedivargustele suunatud juhises rõhutanud, et kahju olemasolu sedastamiseks on vajalik tuvastada kuriteoteates kannatanu konkreetne viide sellele kuidas ning milliseid tema seadusest tulenevaid õigusi või huvisid on kahjustatud.[189] Autor on seisukohal, et kui kannatanu on kinnitanud enda õiguste või huvide rikkumist, siis ei mängigi täpsema kahju määratlemine selle olemasolu hindamisel enam olulist rolli. Siinkohal on oluline veel märkida Riigikohtu poolt leitut, mille kohaselt "mittevaralise kahju täpse suuruse kindlaks määramine ja tõendamine ei ole võimalik ja seetõttu on isikliku õiguste kaitseks esitatud hagi puhul üldjuhul piisavaks asjaolude

[184] RKKKo 06.06.2000, 3-1-1-65-00, p 5.2. (Tartu Ringkonnakohtu kriminaalkolleegiumi 04.04.2000 otsus Vello Ootsingu õigeks mõistmises süüdistuses KrK § 161 järgi.)
[185] RKKKo 18.01.2000, 3-1-1-5-00, p III. (Tallinna Ringkonnakohtu kriminaalkolleegiumi 25.10.1999 otsus Raili Kuningas-Kuld süüditunnistamises KrK § 17 lg 4 - 166 lg 1 järgi.)
[186] RKKKo 04.12.2003, 3-1-1-138-03, p 13.2. (Juri Jemeldjaževi kaitsja vandeadvokaat Janek Valdma kassatsioonkaebus Tallinna Ringkonnakohtu kriminaalkolleegiumi 27.08.2003 otsusele Juri Jemeldjaževi süüditunnistamises KrK § 161 järgi.)
[187] Samuti peab autor vajalikuks märkida, et kuivõrd Riigikohus on aktepteerinud asjaolu, et maine ning usaldusväärsuse kahjustamise puhul võib mittevaraline kahju tekkida avalik-õiguslikel juriidilistel isikutel, siis kinnitab toodu jällegi autori seisukohta, et hea nime rikkumisega võib mittevaraline kahju tekkida ka juriidilistele isikutele, mistõttu tuleks kaaluda identiteedivarguse sättega tagatava kaitse laiendamist juriidilistele isikutele. Vt: alaptk. 2.1.2.1.
[188] RKKKo 04.12.2003, 3-1-1-138-03, p 13.2; Sama seisukohta on Riigikohtu kriminaalkolleegium väljendanud ka teistes kohtuotsustes. Vt ntks: RKKKo 05.05.2003, 3-1-1-43-03, p 14. (Urve Vooli kaitsja vandeadvokaat Jüri Leppiku kassatsioonkaebus Tallinna Ringkonnakohtu kriminaalkolleegiumi 16.12.2002 otsusele Urve Vooli süüditunnistamises KarS § 289 järgi.)
[189] Riigiprokuratuur, *op. cit 132,* lk 1.

tõendamine, millega mittevaralise kahju hüvitamise nõue on seotud. Hüvitise suuruse määramine on siiski aga kohtu diskretsiooniotsus."[190] Seega ei pea identiteedivarguse ohvriks langenud isik temale tekitatud mittevaralise kahju hüvitamise nõudmiseks hakkama tõendama talle tekkinud kahju suurust, vaid tõendatud peab olema vaid tema õigustele või huvidele kahju tekitamise fakt iseenesest, milleks teatud juhtudel piisab ka näiteks kannatanu enda ütlustest.

Karistusseadustiku muutmise eelnõu 554 SE seletuskirjas KarS § 292 juures, mis näeb ette vastutuse andmekogu pidamise nõuete rikkumise eest, kui sellega on tekitatud oluline kahju teise isiku seadusega kaitstud õigustele või huvidele, on leitud, et sellise kahju näol tegemist määratlematu mõistega. mille puhul on tegemist on mitteainelise kahjuga.[191] Samas ei saa autori hinnangul välistada, et isiku seadusega kaitstud õiguste või huvide kahjustamisega ei võiks kaasneda ka varalise kahju tekitamine. Seda näiteks olukorras, kus isiku maine avaliku kahjustamisega võetakse isikult ära edaspidine kasu saamise võimalus või tekitatakse muul moel otsene varaline kahju. Siinkohal toetub autor jällegi KrK §-i 161 käsitlenud kohtupraktikale, milles Riigikohus on leidnud, et "kahju KrK § 161 tähenduses võib olla nii varaline kui ka mittevaraline. Varaline kahju KrK § 161 tähenduses võib olla nii otsene varaline kahju kui ka saamata jäänud tulu."[192] Saamata jäänud tulu nõudeõiguse tekkimise alusena on Riigikohus leidnud, et tõendatud peab olema isiku kavatsus ning võimalus tulu saada." [193] Seega võiks identiteedivarguse ohvriks langenud isikul tekkida õigus nõuda saamata jäänud tulu hüvitamist, kui sellise tulu saamata jäämine oli tingitud näiteks tema hea nime ja maine kahjustamisest tulenevate asjaolude tõttu. Samuti on kohtupraktikas leidnud tuvastamist, et osaühingu õiguste ja huvide kahjustamisega on olnud tehemist näiteks nii finantstegevuse tahtliku rikkumise kui ka otsese varalise kahju tekitamise korral.[194]

Siiski puudub täna kohtupraktika, mis nimetatud kahju mõistet KarS §-s 157^2 sätestatud füüsilise isiku seadusega kaitstud õiguste ning huvide rikkumise kontekstis selgitaks, kuid samas leiab autor, et isiku seadusega kaitstud õigustele ning huvidele tekitatud kahju all peaks

[190] RKTKo 26.06.2013, 3-2-1-18-13, p 21, 22. (Kinnine menetlus. Avalikustada käesoleva otsuse sissejuhatav osa, resolutsiooni p-d 1-2, kirjeldava osa p-d 1, 3 ja 5-7 osaliselt ja põhjendava osa p-d 10-30.)
[191] Seletuskiri 554 SE, lk 76.
[192] RKKKo 11.06.2003, 3-1-1-58-03, p 12. (Andres Männarti kaitsja vandeadvokaat Leon Glikmani kassatsioonkaebus Tallinna Ringkonnakohtu kriminaalkolleegiumi 10.02.2003 otsusele Andres Männarti süüditunnistamises KrK § 161 järgi.)
[193] RKTKo 20.09.2009, 3-2-1-50-09, p 13. (AS Esmar kassatsioonkaebus Tallinna Ringkonnakohtu 30.12.2008. a otsusele AS Esmar hagis Arvi Redi vastu asja väljanõudmiseks ebaseaduslikust valdusest ja 201 400 krooni kahju hüvitamiseks.)
[194] RKKKo 06.04.1999, 3-1-1-34-99, III/p 2. (Tallinna Ringkonnakohtu kriminaalkolleegiumi 04.02.1999 otsus Enely Murre (Jäägeri) süüditunnistamises KrK § 141-1 lg 1 ; § 161 ja § 166 lg 1 järgi. Õigeks mõistetud KrK § 148-1 lg 3,4 järgi.)

varasemast kohtupraktikast tulenevalt olema võimalik mõista nii isikule tekkinud mittevaralist kui ka varalist kahju.

Autor nõustub Riigikohtu praktikaga ka selles osas, et sarnaselt KrK §-s 161 sätestatuga, näeb KarS § 157^2 ette, et tekkinud kahju osas piisab koosseisu täitmiseks ettevaatamatusest.[195] See tähendab, et eesmärk peab hõlmama üksnes objektiivse koosseisu tunnuse, teisest isikust ebaõige ettekujutuse loomise, mitte aga tagajärge teise isiku seadusega kaitstud õiguste või huvide kahjustamise näol.

Seda, kas KarS §-s 157^2 sisalduv kahju mõiste on kooskõlas direktiivi 2013/40 artikli 9 punktis 5 sätestatuga käsitleb autor töö alapeatükis 2.2.2.4.2.3.

2.2.2.4.2.2. Eesmärk varjata kuritegu

Alternatiivselt teise isikuna esinemise teel temast teadvalt ebaõige ettekujutuse loomisele on karistusseadustikus identiteedivarguse sättes märgitud teise eesmärgina ka kuriteo varjamine. Nimetatud eesmärki direktiivi 2013/40 Art 9 p-st 5 ei tulene.

Kuriteo varjamine võib iseenesest seisneda nii tegevuses kui tegevusetuses, mille eesmärk on raskendada kuriteo asjaolude tõendamist, teo toimepanija või teo enda avastamist.[196] Selline tegevus suunab uurimisasutust valedele jälgedele ning raskendab menetluse efektiivset kulgu. Identiteedivarguse sättes peetakse kuriteo varjamise kui koosseisulise eesmärgitunnuse all silmas olukordi, kus kuriteo toimepannud isik kasutab teise isiku isikuandmeid, et esineda teise isikuna ning vabaneda seeläbi kriminaalvastutusest.[197] Seega peab isikul olema tahe raskendada kuriteo avastamist identiteedivarguse kaudu, mis ühtlasi tähendab, et kuriteo varjamine seisneb kindlasti tegevuses.

Samuti tuleb ka siin eristada kuriteokoosseisu objektiivset ning subjektiivset külge, sest ka antud juhul ei ole oluline, et teo toimepanija enda kavatsuse ka reaalselt ellu suudaks viia. Juhul kui isik on juba esitanud teise isiku isikuandmeid selleks, et enda poolt toime pandud kuritegu varjata, siis ei ole koosseisu täitmise seisukohast enam oluline, et kaasneks näiteks politseiametniku või kohtu eksimusse sattumine.

Oluline on siinkohal aga veel see, et kurjategija käitumismotiiv peab sisaldama just kuriteo varjamise eesmärki. KarS § 3 lg 3 kohaselt on kuriteoks karistusseadustikus sätestatud

[195] RKKKo 06.04.1999, 3-1-1-34-99, III/p 2.
[196] S. Laos § 306/ p 3.2. - KarSK.
[197] Seletuskiri 530 SE I, lk 8.

süütegu, mille eest on füüsilisele isikule põhikaristusena ette nähtud rahaline karistus või vangistus ja juriidilisele isikule rahaline karistus või sundlõpetamine. See tähendab, et teiste karistusseadustikus sisalduvate süütegude, väärtegude, varjamise korral ei ole KarS §-s 157^2 sätestatud kuriteo subjektiivse koosseisu tunnused täidetud. Praktikas on sellisel puhul on näiteks Pärnu Maakohus kohaldanud sättes loetletud motiivide esimest alternatiivi isikust ebaõige ettekujutuse loomise näol.[198] Pärnu Maakohtu tõlgendusega autor aga nõustuda ei saa, sest olukorras, kus isik soovib vabaneda väärteokaristusest, ei ole tema teo eesmärk suunatud siiski teisest isikust ebaõige ettekujutuse loomisele vaid enda identiteedi varjamisele karistusest pääsemise eesmärgil. Nimetatut kinnitab ka juba asjaolu, et kuriteo varjamise eesmärk on seadusandja poolt sätestatud koosseisus eraldiseisva eesmärgina.

Seega on autori hinnangul Pärnu Maakohus kohtuasjas nr 1-11-4952 ebaõigesti kohaldanud materiaalõigust, tõlgendades KarS §-s 157^2 toodud isikust ebaõige ettekujutuse loomise koosseisutunnust lubamatult laialt. Autor küll nõustub sellega, et isikuid, kes panevad identiteedivarguse toime väärteo varjamise eesmärgil, ei tohiks karistusõiguse üld- ja eripreventiivsetest eesmärkidest tulenevalt jätta karistamata, kuid selle teostamiseks ei saa lubada õigusnormi ebaõiget kohaldamist ning lubamatult laia tõlgendamist.

Toodud probleemi ületamiseks võiks seadusandja kaaluda koosseisus sisalduva termini „kuriteo“ asendamist ka väärteo puhul kohalduva mõiste „süüteo“ varjamise eesmärgiga. Samuti on autor seisukohal, et kuigi direktiiv 2013/40 ei sisalda kuriteo varjamise eesmärki, siis küberkuritegude puhul on tõenäoline, et kuriteo toimepanija üritab enda jälgi varjata ning kasutab selleks teise isiku identiteeti. Sellist tegevust ei saa aga siduda kolmandas isikus usalduse tekitamise eesmärgiga, mis ainsana on direktiivis sätestatud. Samuti ei ole selline raskendav asjaolu vastuolus direktiivi 2013/40 artiklis 2013/40 tooduga, kuna direktiivi sõnastusest tuleneb selgelt, et kriminaliseeritud võiksid olla vähemalt kõik direktiivi 2013/40 aritkli 9 punktis 5 loetletud asjaolud, kuid ei keelda täiendavate asjaolude sätestamist.

Seega leiab autor, et direktiivi 2013/40 artikli 9 punktis 5 raskendava asjaoluna sätestatud identiteedivargus võiks samuti sisaldada süüteo varjamise eesmärki, sest kui kurjategija enda jälgi varjab või jätab toimepanijana jälje teisele isikule, siis raskendab see oluliselt menetlejate tööd süüteo toimepanija avastamisel ning samuti võib kahjustada identiteedi tegeliku omaniku õigusi, mistõttu võiks autori arvates selline tegu toimepanija tabamise korral talle kaasa tuua raskema karistuse mõistmise.

[198] PMKo 1-11-4952, *op. cit 126.*

2.2.2.4.2.3. Eesmärk võita kolmanda isiku usaldus, tekitades seeläbi kahju identiteedi tegelikule omanikule

Kolmanda isiku usalduse võitmise eesmärk on sätestatud direktiivi 2013/40 Art 9 p-s 5, mille kontekstis tähendab nimetatud eesmärk eelkõige seda, et identiteedivargus pannakse toime selleks, et kolmandas isikus usalduse tekitamise kaudu hõlbustada ebaseaduslik süsteemi häirimise või ebaseaduslikku andmetesse sekkumise toimepanemist. Kolmanda isiku usalduse võitmise eesmärki karistusseadustiku §-st 157^2 ei tulene.

Praktikas võib toodud eesmärk välja näha näiteks selliselt, et kasutatakse kellegi kasutajakontot selleks, et saada kuriteo toimepanemiseks vajalik ligipääs või vältida arvutisüsteemi turvakontrolli. Kolmandate isikute usalduse võitmise eesmärki võib esineda ka väljaspool infosüsteemide vastu suunatud ründeid. Harvad ei ole juhtumid, kus kelmid postitavad internetti fiktiivseid müügikuulutusi ning kasutavad kontaktina näiteks mõne avaliku elu tegelase või muu usaldusväärse isiku e-posti aadressi[199], et tekitada usaldust potentsiaalsetes ostjates, mille tõttu viimased kergemini nende kasuks varakäsutuse teeksid.

Seetõttu on identiteedivarguse juhtumite puhul kolmandates isikutes usalduse tekitamise eesmärgi kriminaliseerimine igati põhjendatud, sest pettuslik tegu muudab kannatanute jaoks keerulisemaks ennast kurjategijate eest kaitsta ning ohvrite eksitamine ja eksimusse sattumise korral abitu seisundi kuritarvitamine väärib kindlasti rangemat kriminaalõiguslikku reageeringut.

Autor leiab, et põhjendatud oleks kolmandates isikutes usalduse tekitamise eesmärk kriminaliseerida ka karistusseadustiku identiteedivarguse koosseisutunnusena kuivõrd nimetatud asjaolu ei ole täna kehtiva identiteedivarguse koosseisutunnusena sätestatud. Toodud seisukohta põhjendab autor sellega, et isikust ebaõige ettekujutuse loomise eemärki ei saa laiendada ka kolmandates isikutes usalduse tekitamise eesmärgile. Võttes arvesse, et eesmärk nõuab kõrgeima tahtlusastme tuvastamist, siis ei saa automaatselt eeldada, et kolmanda isiku usalduse võitmise eesmärgiga kaasneb alati ka eesmärk luua teisest isikust ebaõige ettekujutus. Teatud juhtudel võib ebaõige ettekujutuse loomine eesmärgi täitmisega küll kaasneda, kuid ei eelda siiski koheselt sellise eesmärgi olemasolu.

[199] Näitena võib tuua prügifirma AS Ragn Sells turundusjuhi Rainer Pesti juhtumi, kus tema nimelise e-posti aadressi kaudu müüakse internetis juba mitmendat aastat erinevat kaupa. Vt: R. Kagge. *op cit 131*.

Võttes arvesse, et kolmanda isiku usalduse eesmärgil toime pandud identiteedivargused on praktikas üsna tihti ette tulevad, samuti et ka nimetatud eesmärgi puhul võib andmesubjekti õiguste ja huvide kahjustamisega tekkida oluline kahju, siis on autori hinnangul põhjendatud ette näha vastutus ka nimetatud eesmärgil toime pandud identiteedivarguste eest kui sellega on tekitatud kahju tegeliku identiteedi omanikule. Lisaks kõrvaldaks kolmanda isiku usalduse võitmise eesmärgi lülitamine karistusseadustikus sisalduvasse identiteedivarguse koosseisu vastuolu direktiivi 2013/40 artikli 9 punktid 5 ning KarS § 157^2 sätestatu vahel.

Sarnaselt KarS §-s 157^2 sätestatuga näeb ka direktiivi 2013/40 artikli 9 punkti 5 regulatsioon koosseisutunnusena ette selle, et isikuandmete väärkasutamise teel, eesmärgiga võita kolmanda isiku usaldus, tekitatakse kahju identiteedi tegelikule omanikule.

Erinevalt KarS §-s 157^2 sätestatust ei seo direktiivi 2013/40 regulatsioon kahju tekkimist isiku seadusega kaitstud õigustele või huvidele, vaid räägib kahjust üldiselt. VÕS § 128 kohaselt jaguneb kahju varaliseks ning mittevaraliseks kahjuks, millest esimese moodustab otsene varaline kahju ning saamata jäänud tulu ja teine kahju liik hõlmab eelkõige kahjustatud isiku füüsilist ja hingelist valu ning kannatusi. Eelnevalt leidis autor, et analoogiliselt sõnastatud tagajärgedega süüteokoosseisude tõlgendamisel on Riigikohus asunud seisukohale, et KarS §-s 157^2 sisalduv kahju mõiste peaks hõlmama nii isikule tekitatud varalise kui ka mittevaralise kahju juhtumeid.

Samas leiab autor, et KarS § 157^2 kontekstis puudub käesoleval ajal kohtupraktika, mis toodud kahju mõistet selgelt määratleks, mistõttu ei saa välistada olukordi, kus tulevikus tekkiva kohtupraktika valguses võib direktiivi 2013/40 Art 9 p-s 5 sisalduv üldine kahju mõiste võimaldada laiaulatuslikumat tõlgendamist. Võttes veel ka arvesse, et üldine kahju mõiste on selgemini määratletav ning tagab isikutele kaitse vähemalt kõigi KarS §-s 157^2 sisalduva kahju mõistega hõlmatud juhtumite puhuks, siis võiks autori hinnangul direktiivi 2013/40 Art 9 p-s 5 sisalduva regulatsiooniga võimalike vastuolude vältimiseks KarS §-s 157^2 sätestatud isiku seadusega kaitstud õigustele ja huvidele tekitatud kahju mõiste asendandada direktiivi 2013/40 Art 9 p-s 5 kasutatava üldise kahju mõistega. Samuti leiab autor, et koosseisutunnusena isikule kahju tekkimise sätestamine tagaks isikutele selgema ning laiaulatuslikuma kaitse internetiga seotud identiteedivarguse juhtumite puhuks ning vastaks seega paremini identiteedivarguse üldistele ühtsetele tunnustele, mille kaudu omakorda tõhustaks rahvusvahelist koostööd internetiga seotud identiteedivarguste asjades.

KOKKUVÕTE

Erinevate teenuste internetikeskkonda viimisega jõuab internetti üha rohkem isikuandmeid, mistõttu kasvab tänases infoühiskonnas personaalse informatsiooni kuritarvitamise ning identiteedivarguste ohvriks langemise risk. Seetõttu otsis autor käesolevas magistritöös personaalse informatsiooni kuritarvitamisega seotud tegevustes nende eesmärke ning meetodeid arvesse võttes ühiseid tunnuseid, mis võiksid olla abiks ühtse ning kõikehõlmava regulatsiooni väljatöötamisel, et tagada isikutele võimalikult tõhus kaitse selliste kuritegude vastu.

Analüüsi tulemusena leidis autor, et internetis toime pandud identiteedivarguste puhul on kuritegu seotud alati vähemalt ühega neljast identiteedivargusele iseloomulikust etapist. Esimeseks etapiks on ettevalmistusstaadium, milleks võib pidada näiteks internetist personaalsete isikuandmete leidmiseks vajalike programmide või skeemide väljatöötamist. Selliste programmide kasutamine teisi isikuid identifitseeriva informatsiooni leidmiseks moodustab aga juba identiteedivargusele iseloomuliku teise faasi, milleks on isikuandmete hõivamine. Kolmandasse etappi kuulub isiku kohta käivate andmete omamine ning edastamine. Viimases, neljandas astmes on tegevus seotud kogutud andmete kasutamisega kuritegelikel eesmärkidel.

Autori hinnangul peaks isikutele ja nende kohta käivatele andmetele olema tagatud kriminaalõiguslik kaitse kõikides eelnevalt loetletud identiteedivarguse faasides. Seetõttu seadis autor üheks töö eemärgiks hinnata seda, millised identiteedivarguse etapid on KarS §-s 157^2 sätestatud koosseisutunnuste kaudu kriminaliseeritud ning kas tervikliku ning rahvusvahelist koostööd enam tagava kuriteokoosseisu puhul peaksid karistatava teo koosseisu kuuluma kõik neli identiteedivarguse etappi või tagab tõhusa kaitse juba see, kui vastutus tuleneb karistusõiguse üldsätetest või teistest kuriteokoosseisudest.

Magistritöö teiseks eesmärgiks oli analüüsida Eesti identiteedivarguse sätte vastavust rahvusvahelistest õigusaktidest tulenevatele eriregulatsioonile kehtestatud nõuetele ning eesmärkidele. Asjakohaste Eestit puudutavate piiriüleste õigusaktidena tõi autor välja Euroopa Nõukogu Arvutikuritegevusvastase konventsiooni ning Euroopa Parlamendi ja Nõukogu 12.08.2013. a direktiivi 2013/40/EL, mis mõlemad rohkemal või vähemal määral identiteedivargusega seotud elemente reguleerivad. Samuti sätestab dirketiivi 2013/40 Art 9 p 5, et kui direktiivi artiklites 4 ja 5 osutatud kuriteod pannakse toime teise isiku isikuandmete väärkasutamise teel, eesmärgiga võita kolmanda isiku usaldus ning tekitatakse seeläbi kahju tegeliku identiteedi omanikule, võib seda siseriikliku õiguse kohaselt käsitada raskendava

asjaoluna. Seejuures on direktiivi 2013/40 Art 9 p-st 5 tulenev regulatsioon ainsaks Eestit puudutavaks rahvusvahelistest õigusaktidest tulenevaks sätteks, milles on otseselt identiteedivargusega seonduvat reguleeritud.

Autor leidis, et kuigi direktiivist 2013/40 ei tulene liikmesriikidele identiteedivarguse kriminaliseerimise kohustuslikkust, on Eesti kriminaalpoliitilistest kaalutlustest ning rahvusvahelise kootsöö seisukohalt siiski oluline, et Eestis kehtiv regulatsioon kataks vähemalt kõiki direktiivi 2013/40 Art 9 p-s 5 nimetatud identiteedivargusega seotud asjaoludsid. Seetõttu keskendus autor KarS §-s 157^2 sätestatud teise isiku identiteedi ebaseadusliku kasutamisele rahvusvahelistest õigusaktidest tulenevate nõuetega vastuolu hindamisel direktiivi 2013/40 Art 9 p-s 5 sätestatule.

Töö eesmärgi täitmiseks analüüsis autor regulatsioonide omavahelise vastavuse ning reguleerimisala väljasegitamiseks KarS § 157^2 ja Arvutikuritegevusvastasest konventsioonist ning direktiivist 2013/40 tulenevaid asjakohaseid sätteid identiteedivarguse nelja reguleerimisetapi ning reguleerimisfaasidest väljapoole jäävate koosseisuelementide kaudu.

Esmalt võrdles autor sätete kaitse- ja vastutusala ning leidis, et nii KarS §-ga 157^2 kui ka direktiivi 2013/40 Art 9 p-ga 5 kaitstavateks õigushüvedeks on peamiselt informatsioonilise enesemääramise õigus ja eraelu kaitse. Perekonna- ja eraelusfäär on iseloomulik aga vaid füüsilistele isikutele, mistõttu ei ole KarS §-s 157^2 ega direktiivi 2013/40 Art 9 p-s 5 sätestatud identiteedivarguse regulatsiooniga tagatud kaitset juriidilistele isikutele ning nende kohta käivatele andmetele. Sellegipoolest asus autor Euroopa Inimõiguste kohtu seinisele praktikale ning õiguskirjanduses käsitletule tuginedes seisukohale, et hea nime ning maine kandjateks võivad olla ka juriidilised isikud, mille kahjustamise oht ähvardab internetiga seotud identiteedivarguse puhul võrdselt nii füüsilisi kui juriidilisi isikuid. Seetõttu leidis autor, et nii siseriiklikul kui ka Euroopa Liidu tasandil oleks otstarbekas tulevikus kaaluda kas internetiga seotud kuritegevuse iseärasusi arvesse võttes võiks olla põhjendatud laiendada identiteedivarguse sättega tagatavat kaitset ka juriidilistele isikutele.

Vastutusala analüüsimisel leidis autor, et kehtiv KarS § 157^2 regulatsioon juriidiliste isikute vastutust ei sätesta. Samas jõudis autor järeldusele, et direktiivist 2013/40 tulenevalt laieneb artiklites 4 ja 5 toime pandud infosüsteemide vastu suunatud rünnete puhul isiku tegeliku identiteedi varjamise korral vastutus ka juriidilistele isikutele. Kuivõrd aga direktiiviga 2013/40 kooskõla saavutamiseks on oluline, et KarS §-s 206 ning §-s 207 sätestatud kuritegude puhul oleks võimalk identiteedivargusega kogumi moodustamine ning et toodud probleemi ei lahendata ka karistusseadustiku muutmise eelnõuga 554 SE kavandavate

muudatustega, siis on autori hinnangul tarvilik karistusseadustikku täiendavalt muuta ning näha ette juriidilise isiku vastus ka KarS §-s 157^2.

Samuti hindas autor, kas KarS §-s 157^2 toodud identiteedivarguse seotus isikuandmete mõistega toob kaasa vastuolu direktiivi 2013/40 Art 9 p-s 5 sätestatuga ning leidis, et direktiivis 2013/40 toodu ei erine KarS §-s 157^2 toodust käsitluses. Ka ei tuvastanud autor IKS-s ning Euroopa Liidu õiguses isikuandmete mõistet käsitlevate direktiivide vahel erinevusi isikuandmete mõiste sisustamise osas, mistõttu ei tuvastanud autor selles küsimuses vastuolusid direktiivi 2013/40 Art 9 p-s 5 ning KarS §-s 157^2 sätestatud identiteedivarguse regulatsioonide vahel. Siiski leidis autor, et kuivõrd karistusseadustikus sisalduvad normid peaksid tagama isikutele kaitset reaalses elus eksisteerivate juhtumite puhuks ning praktikas võivad isikute õigused olla rikutud ka muude andmete, peale isikuandmete, väärkasutamise korral, siis võiks nii siseriiklikul ka Euroopa Liidu tasandil kaaluda, kas teise isiku identiteedi kasutamisega seonduvate juhtumite puhul oleks tõhusama kaitse tagamise eesmärgil otstarbekam muuta senist lähenemisviisi ning asendada identiteedivarguse sättes sisalduv "isikuandmete" mõiste näiteks U.S.C-s kasutatava mõistega "identifitseerimisvahend", mis võimaldaks muuhulgas sätte kohaldamist ka juriidiliste isikute kohta käiva informatsiooni väärkasutamise juhtumite puhul.

Ettevalmistusstaadiumi analüüsimisel leidis autor, et KarS §-s 157^2 ning direktiivi 2013/40 Art 9 p-s 5 sätestatud identiteedivarguse regulatsioon ettevalmistamist koosseisutunnusena ette ei näe. Siiski tõi autor välja nii Arvutikuritegevusvastasest konventsioonist, direktiivist 2013/40 kui ka karistusseadustikust teisi sätteid, mida on internetiga seotud identiteedivarguse ettevalmistusstaadiumile võimalik kohaldada. Selliselt saab ettevalmistusstaadiumit pidada kriminaliseerituks läbi KarS § 216^1, mis vastab identiteedivarguse reguleerimise osas Arvutikuritegevusvastase konventsiooni Art-s 6 ning direktiivi 2013/40 Art-s 7 sätestatule. Samuti on ettevalmistusstaadiumi kriminaliseeritud läbi Arvutikuritegevusvastase konventsiooni Art-s 7 sätestatud arvutiandmete võltsimise, mille all mõistetavaid tegevusi saab pidada karistatavaks läbi KarS §-217. Lisaks hindas autor töös seda, kas võiks olla põhjendatud ette näha identiteedivarguse ettevalmistamise karistatavus ka identiteedivargust reguleerivas erinormis ning jõudis järeldusele, et selle kriminaliseerimine isikuandmete hõivamise planeerimise näol muutub määratlematuse tõttu praktiliselt võimatuks ning KarS § 216^1 ja § 217 kaudu on internetiga seotud olulisemate identiteedivarguse juhtumite korral ettevalmistamine karistatav ning isikute õigused seega piisavas ulatuses kaitstud, mistõttu on õigusselguse huvides ning ülekriminaliseerimise vältimiseks põhjendatud loobuda ettevalmistusstaadiumi sätestamisest identiteedivarguse eriregulatsiooni koosseisutunnusena.

Informatsiooni hõivamise faasi puhul leidis autor, et KarS §-s 157^2 ning direktiivi 2013/40 Art 9 p-s 5 sisalduv identiteedivarguse koosseis isikuandmete hõivamise tegu karistatavaks ei pea. Sarnaselt ettevalmistusstaadiumiga on aga ka isikuandmete hõivamise faas karistatav läbi teiste karistusseadustikus sisalduvate kuriteokoosseisude. Selliselt on isikuandmete hõivamisega seotud Arvutikuritegevusvastase konventsiooni Art-id 2, 3, 4 ja 5 ning direktiivi 2013/40 Art-id 3, 4, 5 ja 6, millele vastavad KarS §-s 217, KarS §-s 137, KarS §-s 206 ning KarS §-s 207 sätestatud kuriteod. Samuti saab isikuandmete hõivamist pidada karistatavaks läbi KarS §-s 213 säestatud arvutikelmuse. Ka siinkohal tõstatas autor küsimuse isikuandmete hõivamise faasi sätestamisest KarS § 157^2 koosseisutunnusena ning sarnaselt ettevalmistusstaadiumiga leidis, et isikuandmete hõivamise kriminaliseerimine identiteedivarguse erikoosseisus võiks kaasa tuua määratlemise nõudele vastavusega seonduvad probleemid, samuti on teiste kuriteokoosseisude kaudu interneti ning arvutiga seotud olulisematel juhtudel isikuandmete hõivamise staadium kriminaliseeritud, mistõttu ei ole vajalik isikuandmete hõivamise faasi identiteedivarguse regulatsioonis eraldi koosseisutunnusena ette näha.

Identiteedivarguse kolmandasse, isikute kohta käiva informatsiooni omamise või edastamise staadiumisse kuuluvaid elemente Arvutikuritegevusvastane konventsioon ega direktiiv 2013/40 ei kriminaliseeri. KarS § 157^2 sätestab vastutuse nende nõusolekuta edastamise ning nendele juurdepääsu võimaldamise eest, reguleerides seega toodud faasi vaid osaliselt. Samas leidis autor, et hoolimata sellest on nimetatud faasi puhul Eestis kehtiva regulatsiooniga tagatud isikutele kaitse piisavas ulatuses. Nimetatud etapi analüüsimisel tõstatas autor kaks küsimust. Esiteks, milliste andmete omamine või edastamine täidab kuriteokoosseisu ning teiseks, millal on sellise informatsiooni omamine või edastamine kuritegelik. Vastuseks esimesele küsimusele leidis autor, et informatsiooni iseloomu poolest eeldab kuritegelik käitumine seda, et valduses olevad või edastatavad andmed kuuluksid oma iseloomult identiteedivargust kriminaliseeriva sätte kuriteokoosseisu elementide hulka. Teisele küsimusele vastamisel leidis autor, et sellise tegevuse kuritegelikkus on sisustatav läbi koosseisus sisalduva teo ebaseaduslikkust sätestavate asjaolude, milleks KarS § 157^2 puhul on sätestatud andmesubjekti nõusoleku puudumine.

Identiteedivarguse viimane, neljas staadium moodustub isiku kohta käiva informatsiooni kasutamisest kuritegelikel eesmärkidel, mis on kriminaliseeritud nii KarS §-s 157^2 kui ka direktiivi 2013/40 Art 9 p-s 5 toodud identiteedivarguse regulatsioonis. Kasutamise puhul on tegemist mõistega, mis avab ennast läbi kasutamise eesmärkide või sellega kaasnevate tagajärgede. KarS § 157^2 seob isikuandmete kasutamise isikust ebaõige ettekujutuse loomise

või kuriteo varjamise eesmärgiga, milliseid eesmärke direktiivi 2013/40 Art 9 p-s 5 toodud regulatsioonist ei tulene. Autor selgitas, et KarS §-s 157^2 toodud koosseisu täitmiseks on oluline tuvastada kurjategija kavatsus luua isikust ebaõige ettekujutus, kuid selle eesmärgi saavutamine koosseisu täitmise seisukohalt enam oluline ei ole. Ebaõige ettekujutuse mõiste seondub autori hinnangul aga eelkõige kolmandate isikute subjektiivsete omaduste ja hinnangutega, mistõttu piisab KarS § 157^2 koosseisu täitmiseks juba sellest, kui isikule omistatakse midagi, mida ta ise teinud ei oleks.

KarS § 157^2 seob ebaõige ettekujutuse loomise isiku seadusega kaitstud õigustele või huvidele tekitatud kahjuga. Isiku seadusega kaitstud õiguste või huvide rikkumiseks võib pidada nii põhiseaduses sätestatud põhiõiguste kui ka näiteks VÕS-ist tulenevate õiguste rikkumist. Analoogiliselt sõnastatud tagajärgi sisaldanud sätteid tõlgendanud kohtupraktika analüüsimise tulemusel leidis autor, et KarS §-s 157^2 sätestatud kahju all peaks olema võimalik mõista isikule tekitatud nii varalist kui ka mittevaralist kahju. Direktiiv 2013/40 sisaldab üldist kahju mõistet, mistõttu on direktiiviga vastavuse seisukohast oluline, et KarS § 157^2 võimaldaks kahju all käsitleda mõlemaid kahju liike. Samuti leidis autor, et KarS §-s 157^2 ettenähtud kahju tekitamise osas piisab koosseisu täitmiseks ettevaatamatusest.

Teise eesmärgina sätestab KarS §-s 157^2 kuriteo varjamise, mille puhul tuleb samuti eristada kuriteokoosseisu objektiivset ning subjektiivset külge, sest koosseisu täitmise seisukohalt ei ole oluline, kas toimepanija suutis oma kavatsuse reaalselt ellu viia või mitte. Tähelepanu tuleb pöörata ka sellele, et tegevus peab sisaldama just kuriteo varjamise eesmärki ning väärteo varjamise korral kuriteokoosseis täidetud ei ole. Õigeks ei saa pidada ka selliste tegude kvalifitseerimine isikust ebaõige ettekujutuse loomise eesmärgi alla. Seega võiks seadusandja kaaluda koosseisus sisalduva termini „kuriteo“ asendamist „süüteo“ varjamise eesmärgiga, mis võimaldaks KarS § 157^2 kohaldamist ka väärtegude varjamise korral. Samuti leidis autor, et direktiivi 2013/40 Art 9 p-s 5 raskendava asjaoluna sätestatud identiteedivargus võiks sisaldada süüteo varjamise eesmärgi kriminaliseeritust.

Direktiivi 2013/40 Art 9 p-s 5 on sätestatud kolmanda isiku usalduse võitmise eesmärk kui sellega on tekitatud kahju identiteedi tegelikule omanikule, mida karistusseadustiku §-st 157^2 ei tulene. Seega tuleks toodud eesmärgil tegutsemine kriminaliseerida ka karistusseadustiku identiteedivarguse koosseisutunnusena, et kõrvaldada vastuolu KarS §-s 157^2 ning direktiivi 2013/40 artikli 9 punktis 5 sätestatu vahel.

Töö sissejuhatuses esitas autor esmalt hüpoteesi, mille kohaselt ei hõlma Eestis kehtiv

identiteedivarguse regulatsioon üldisi ja ühiseid identiteedivarguse tunnuseid ning sisaldab koosseisutunnustena asjaolusid, mis muudavad sätte kohaldamisala liialt kitsaks ega taga seega isikutele tõhusat kaitset internetis toime pandud personaalse informatsiooni väärkasutamise juhtumite puhul. Eeltoodut arvestades sellega siiski aga päris üheselt nõustuda ei saa. Kindlasti tuleb autori hinnangul jaatada, et KarS §-s 157^2 ei kriminaliseeri kõiki internetiga seotud identiteedivarguse etappe. Samuti võib nõustuda, et kuivõrd KarS §-s 157^2 sisalduv isikuandmete mõiste on kohaldatav vaid füüsilistele isikutele, siis ei ole tagatud personaalse informatsiooni väärkasutamise juhtude puhuks kaitset juriidilistele isikutele ning füüsilistele isikutele kui kasutatud on isikuandmete mõistest väljapoole jäävat personaalset informatsiooni, siis ei ole KarS §-ga 157^2 tagatud isikutele efektiivset kaitset kõigi identiteedivarguse juhtumite puhuks. Samas ei näe autor probleemi selles, et KarS § 157^2 ei sisalda kõigi identiteedivarguse etappide kriminaliseeritust, kuivõrd olulisemate internetiga seotud juhtumite puhul on isikutele kaitse tagatud läbi teiste asjakohaste karistusseadustikus sisalduvate kuriteokoosseisude.

Teiseks hüpoteesiks võttis autor selle, et Eestis kehtiv identiteedivarguse spetsiaalnorm ei ole kooskõlas rahvusvahelistest õigusaktidest ja lepingutest tulenevate eriregulatsioonile seatud nõuetega ning seetõttu tuleb karistusseadustiku regulatsiooni muuta, et see täidaks nõutud eesmärke. Teine töös püstitatud hüpotees leidis autori hinnangul kinnitust, kuivõrd KarS § 157^2 ei kata kõiki direktiivi 2013/40 Art 9 p-s 5 toodud isikuandmete väärkasutamisega seotud asjaolusid. Sellisel näeb autor vastuolu seal, kus KarS § 157^2 ei näe ette juriidilise isiku vastutust ning ei näe koosseisutunnusena ette kolmandas isikus usalduse tekitamise eesmärki kui sellega on tekitatud kahju identiteedi tegelikule omanikule. Toodud vastuolusid ei kõrvaldata ka karistusseadustiku muutmise eelnõuga 554 SE. Seetõttu leiab autor, et direktiivis 2013/40 sätestatuga vastavuse saavutamiseks oleks vaja KarS § 157^2 muuta selliselt, et see sisaldaks ka kolmandas isikus usalduse tekitamise eesmärki ning näeks ette juriidlise isiku vastutuse.

___ . ___ . _____ _____ /allkiri./

Merika Nimmo

INTERNET-RELATED IDENTITY THEFT AND ITS REGULATION IN ESTONIAN PENAL LAW

Summary

The number of personal Internet users increases every year and covers today nearly 40% of the world's total population. E-mails, online press releases and other Internet based means of communication are starting to replace the traditional paper-based mail and face-to-face meetings. There is also an increasing number of state services that are being offered via Internet, which brings about a raise in the amount of personal data reaching the Internet. Due to the fact that more and more personal data becomes accessible online, the risk of identity thefts and other misuses of personal information increases rapidly.

Because of the growth in the number of potential Internet-related identity theft victims and that the topic of identity thefts becomes more actual, the author aimed this master's thesis to analyse the conformity of the Estonian identity theft regulations' to the objectives and requirements that have arisen from relevant international legal instruments. The author also assessed the area protected by the identity theft regulation included in the Estonian Penal Code by analysing the necessary elements of an offence provided in the subsection 157^2 of the Estonian Penal Code in the context of common principles regarding Internet-related identity theft.

The author chose this topic because the subject associated to identity theft is not very widely analyzed in the Estonian law-related literature. Additonally to improve the quality of the Estonian legal acts regulating the Penal Law and in order to ensure the effective protection of people, it is necessary to evaluate the compatibility of the Estonian national criminal law to superior legal acts and principles.

To achieve the objectives mentioned above the author uses systematic and comparative legal research methods and refers to the following sources: the Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, the Council of Europe Convention on Cybercrime and the Estonian Penal Code, as well as relevant case law and legal literature related to identity theft.

In order to achieve the abovementioned goal, the author formulated two hypotheses. The first hypothesis stipulates that the valid identity theft regulation in the Estonian Penal Code does not cover all general and common principles of identity theft and involves elements of an

offence which narrow the scope of the ambit of this regulation so it does not ensure effective protection of individuals in the cases of personal information misuse related to the Internet. The second hypothesis was that the identity theft regulation provided in subsection 157^2 of the Estonian Penal Code is not in compatibility with the requirements derived from international legal acts and international treaties. Hence, in order to achieve the consistency with the objectives ensued from these international legal acts and treaties, the identity theft regulation provided in Estonian Penal Code needs to be revised.

The author finds that to prevent and to ensure effective fight against cybercrimes involving misuse of personal information, identity theft needs to be criminalized in as many countries as possible. This leads to the need to develop a consistent and a comprehensive regulation for Internet-related identity thefts.

In order to find the common elements that combine all incidents of Internet-related identity thefts, which might be helpful to develop such a regulation the author evaluated in the first part of the first chapter the different goals and methods used to gather personal data and the nature of personal information used to commit Internet-related identity thefts. As a result of this analysis the author found that in Internet-related identity theft the crime is always associated with at least one of four phases characteristic to identity theft. The first step is the preparation phase; which can be regarded as a development and an elaboration of computer programs to find personal data online. The use of such programs to find identifying information is however characteristic to the second phase, which is obtaining identity-related information. The third phase includes the act of possessing and transferring identity-related data. In the final, fourth phase the activities are related to using the personal information for criminal purposes.

In the second part of the first chapter of this master's thesis the author pointed out the international legal acts related to internet-related identity theft that are relevant to the Estonian law in order to analyse whether and to what extent they regulate identity theft and establish requirements governing the special regulation of identity theft. Those legal acts are the Council of Europe Convention on Cybercrime and the Directive 2013/40/EU of the European Parliament and of the Council mentioned above. The author ascertained that the only provision directly regulating identity-theft is provided in p 5 of Art 9 of the Directive 2013/40/EU which provides that all Member States shall take the necessary measures to ensure that when the offences referred to in Art-s 4 and 5 of the Directive 2013/40/EU are committed by misusing the personal data of another person, with the aim of gaining the trust

of a third party, thereby causing prejudice to the rightful identity owner, this may, in accordance with national law, be regarded as aggravating circumstances, unless those circumstances are already covered by another offence, punishable under national law. In other parts the legal acts mentioned above regulate the elements inherent to internet-related identity theft only trough other criminal offences provided throughout the regulations.

In order to achieve the aforementioned goals the author analysed in the second chapter of this master's thesis, through the four phases related to identity theft and through other necessary elements that stand outside of those phases, the real scope of the regulation for illegal use of another person's identity provided in the subsection 157^2 of the Estonian Penal Code. Under that Code it is punishable to transmit personal data that establish or may enable to establish the identity of another person, grant access to the data or use thereof, without the consent of that person, with the aim to knowingly cause a misconception of that person by means of assuming that person's identity, if damage is caused thereby to the rights or interests of another person that are protected by law, or to conceal a criminal offence. The author also analysed whether this regulation is matching the requirements for criminal offences related to identity theft provided in the Cybercrime Convention and Directive 2013/40 mentioned afore.

Firstly the author compared the legal provisions regulating the protection and liability in identity theft regulations and found that within both provisions, in the one provided in subsection 157^2 of the Estonian Penal Code and in the one provided in p 5 of Art 9 of the Directive 2013/40/EU, the main aim of the provision is to protect the right for informational self-determination and the inviolability of private life. Those rights are however characteristic only to natural persons, which means that the provisions in subsection 157^2 of the Estonian Penal Code and in p 5 of Art 9 of the Directive 2013/40/EU do not provide protection for legal entities nor for the personal data related to legal entities. The author found that since crimes involving identity theft most commonly cause damage to persons' reputation and right for a good name and that it is repeatedly found that legal entities are also able to carry reputation and good name, then the risk of those rights to get harmed by internet-related identity theft threatens equally both natural and legal persons. Due to that the author considered that it would be necessary to supplement the provisions both on national and European Union level so that the criminal protection for personal information would also ensure protection for legal entities. While analysing the area of liability, the author found that it is reasonable to provide liability for legal entities if the act of abusing identity-related information is committed by a legal person and also that the identity theft regulation provided in subsection 157^2 of the Estonian Penal Code is not in conformity with the regulation

provided in p 5 of Art 9 of the Directive 2013/40/EU in part where it does not establish liability of legal persons.

The author also assessed if the use of the term "personal data" in the objective elements necessary to constitute an identity theft offence in the regulation provided in subsection 157^2 of the Estonian Penal Code leads to a contradiction with the regulation provided in p 5 of Art 9 of the Directive 2013/40/EU and concluded that there is no contradiction. However, the author found that so far as the Penal Code should contain provisions that ensure the protection of persons for the cases that exist in real life and the practice shows that persons' rights can be violated also by using other personal information that is not considered as personal data by the Estonian Data Protection Act or by the relevant European Union legal acts, it should be considered to substitute the term "personal data" contained in provisions regulating identity theft with the term "means of identification", used in the United States Code, which among other things would allow to apply provisions in cases of misuse of the information of legal entities.

In the preparation phase of the identity theft, the author found that the regulation provided in subsection 157^2 of the Estonian Penal Code and in p 5 of Art 9 of the Directive 2013/40/EU does not contain acts characteristic to the preparation phase in the catalogue of elements necessary to constitute an identity theft offence. However the author stated that there are other offences provided in the Convention on Cybercrime, in the Directive 2013/40/EU and in the Estonian Penal Code that can be applicable to the preparation phase of internet-related identity theft in most significant and common cases, so there is no need to further criminalize the preparation phase in the special provision of illegal use of another person's identity provided in subsection 157^2 of the Estonian Penal Code.

The similar thing was found in the second phase that contains the obtaining of personal information, where the author stated that even though the regulation provided in subsection 157^2 of the Estonian Penal Code and in p 5 of Art 9 of the Directive 2013/40/EU does not criminalize the phase of obtaining personal information, the there are other offences provided in the Convention on Cybercrime, in the Directive 2013/40/EU and in the Estonian Penal Code that can be applicable to the second phase of internet-related identity theft, so there is no need to further criminalize the phase of obtaining personal information in the special provision of identity theft provided in subsection 157^2 of the Estonian Penal Code.

There are no criminal offences provided in the Convention on Cybercrime and in the Directive 2013/40/EU that would in any way criminalize the third phase, directed to the act of

possessing or transferring the identity-related information. However, the phase is partly regulated by the subsection 157^2 of the Estonian Penal Code, where it has been prescribed the liability for transmitting and granting of access to the personal data used to commit identity theft. Even though the phase is only partly covered by the provision in the Estonian Penal Code, the author found that the existing regulation ensures protection in an adequate level. While clarifying the concept of the third phase of identity theft, the author posed two questions:

1) What kind on personal data possession and transmission performs a criminal offence;

2) When is the possession and transmission of such data considered unlawful.

In regard to the first question, the author found that a criminal conduct requires that the information possessed or used would, by its nature, be included in the elements necessary to constitute an offence described in the provision. As a response the second question the author found that obsession and transmission of personal data can be considered unlawful if such acts are covered by the circumstances of illegality described in the identity theft provision. Subsection 157^2 of the Estonian Penal Code states such circumstance to be the absence of the consent of the owner of the personal data.

The fourth phase is constituted by the act of using identity-related information for criminal purposes. The use of personal data for certain criminal purposes is also provided in the subsection 157^2 of the Estonian Penal Code and in p 5 of Art 9 of the Directive 2013/40/EU. Subsection 157^2 of the Estonian Penal Code provides that the use of personal data should be punishable if the use knowingly causes a misconception of that person by means of assuming that person's identity, if damage is caused thereby to the rights or interests of another person that are protected by law, or to conceal a criminal offence. Point 5 of Art 9 of the Directive 2013/40/EU criminalises the misuse of another person’s identity-related data if it is in relation to offences referred in Art-s 4 and 5 of the Directive 2013/40/EU and with the aim of gaining the trust of a third party, thereby causing prejudice to the rightful identity owner. The fact that the provision in subsection 157^2 of the Estonian Penal Code does not cover the aims of usage mentioned in the p 5 of Art 9 of the Directive 2013/40/EU and *vice versa* leads to a contradiction. Hence, the author finds that it is necessary to add the aim of gaining the trust of a third party to the identity theft provision in the Estonian Penal Code to eliminate the inconsistency mentioned above. Defining the concept of damages caused by such acts in both provisions, the author found that it could be considered to be patrimonial or non-patrimonial. Therefore, the author suggests for the sake of explicitness and to prevent potential conflicts to

replace the term "damage caused to the rights or interests of another person that are protected by law" with the general concept of damage to another person used in the p 5 of Art 9 of the Directive 2013/40/EU.

Based on the previous, the author concludes that the first hypothesis is confirmed only partially. It must be accepted that because of the lack of protection for legal entities and the use of the term "personal data" in the list of necessary elements of the identity theft provisions, the current provisions do not ensure effective and equal protection to natural and legal persons in personal information misuse cases related to Internet. On the other hand the author did not consider it as a deficiency that the identity theft provision in subsection 157^2 of the Estonian Penal Code does not criminalise all four phases characteristic to internet-related identity theft, since the protection is ensured in a sufficient extent by other offences provided in the Estonian Penal Code.

The second hypothesis is confirmed as the identity theft provision in the subsection 157^2 of the Estonian Penal Code does not provide liability for legal persons and does not contain the aim of gaining the trust of a third party, thereby causing prejudice to the rightful identity owner as a necessary element to the offence of illegally using another person's identity.

___ . ___ . _____ _____ /signature./

Merika Nimmo

LÜHENDID

1)	**Direktiiv 2013/40**	Euroopa Parlamendi ja Nõukogu 12.08.2013. a direktiiv 2013/40/EL, milles käsitletakse infosüsteemide vastu suunatud ründeid ja millega asendatakse nõukogu raamotsus 2005/222/JSK.
2)	**Direktiiv 95/46/EÜ**	Euroopa Parlamendi ja Nõukogu 24.10.1995 direktiiv 95/46/EÜ, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta.
3)	**EIKo**	Euroopa Inimõiguste Kohtu otsus
4)	**EKo**	Euroopa Kohtu otsus
5)	**ELT**	Euroopa Liidu Teataja
6)	**FDIC**	Federal Deposit Insurance Corporation
7)	**IKS**	Isikuandmete kaitse seadus
8)	**KarS**	Karistusseadustik
9)	**KrK**	Kriminaalkoodeks
10)	**OECD**	Organization for Economic Co-operation and Development
11)	**PS**	Põhiseadus
12)	**RKKKm**	Riigikohtu kriminaalkolleegiumi määrus
13)	**RKKKo**	Riigikohtu kriminaalkolleegiumi otsus
14)	**RKTKo**	Riigikohtu tsiviilkolleeriumi otsus
15)	**RT**	Riigi Teataja
16)	**Seletuskiri 530 SE I**	Karistusseadustiku muutmise seaduse eelnõu seletuskiri 530 SE I.
17)	**Seletuskiri 554 SE**	Karistusseadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu seletuskiri 554 SE
18)	**SSN**	Social Security Number
19)	**U.S.C**	United States Code
20)	**UNODC**	United Nations. Office on Drugs and Crime
21)	**VÕS**	Võlaõigusseadus

KASUTATUD KIRJANDUS

1) Analysis on "Online Identity Theft“. Organization for Economic Co-operation and Development. *Sine loco:* OECD 2009.

2) Brenner, S. W., Koops, B.-J. Approaches to Cybercrime Jurisdiction. *Sine loco:* Journal Of High Technology Law, 2004/1. Arvutivõrgus: http://www.joemoakley.org/documents/jhtl_publications/brenner.pdf, 12.03.2014.

3) E.-J. Truuväli, *et al* (toim). Eesti Vabariigi põhiseadus. Kommenteeritud vlj. Veebiväljaanne. Tartu Ülikool 2012. Arvutivõrgus: http://pohiseadus.ee

4) Eesti Vabariigi põhiseaduse ekspertiisikomisjon. Põhiseaduse analüüs. Põhiseaduse 2. peatükk "Põhiõigused, vabadused ja kohustused". Justiitsministeerium. Arvutivõrgus: http://www.just.ee/10731, 30.04.2014.

5) Federal Deposit Insurance Corporation (FDIC). Putting an end to Account-Hijacking Identity Theft. Arvutivõrgus: http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf, 30.04.2014.

6) Givens, B. Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions. Written Testimony for U.S. Senate Judiciary Subcommittee on Technology, Terrorism and Government Information Senator Jon Kyl, Chairman**.** Arvutivõrgus: https://www.privacyrights.org/ar/id_theft.htm, 12.03.2014.

7) Gragido, W., Pirc, J. (Edit.) Rogers, R. Cybercrime and Espionage. An Analysis of Subversive Multivector Threats. Syngress Publications. Burlington: Elsevier 2011.

8) Handbook on Identyty-related crime. Gercke, M. *et al*. UNODC 2011. Arvutivõrgus: http://www.unodc.org/documents/treaties/UNCAC/Publications/Handbook_on_ID_Crime/10-57802_ebooke.pdf, 12.03.2013.

9) Hoofnagle C. J. Identity Theft: Making the Known Unknowns Known. Harvard Journal of Law & Technology 2007/1.

10) Internet-related Identity Theft. Gercke, M. A discussion paper. Strasbourg: Council of Europe 2007. Arvutivõrgus: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20activity_events_on_identity_theft/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf, 12.03.2014.

11) Kanger, L. Kahju hüvitamise nõue riigivastutuse seaduse alusel. Kohtupraktika analüüs. Tartu: Riigikohus, õigusteabe osakond 2008. Arvutivõrgus: http://www.riigikohus.ee/vfs/775/Analyys%20Riigivastutus(L_Kanger).pdf, 29.04.2014.

12) Karistusõigus. Üldosa. Sootak, J. Tallinn: Juura 2010.

13) Karistusõiguse adekvaatsus –õiguse iseolemine ja mida ühiskond õigusest ootab. Ettekanne Presidendi mõttekojas. Sootak, J. Ärma: 27.08.2010. Arvutivõrgus: http://www.president.ee/images/stories/pdf/2010-08-27_jaan-sootak.pdf, 19.04.2014.

14) Microsoft Corporation. Online Identity Theft: Changing the Game. Redmond: Microsoft Corp. 2008. Arvutivõrgus: http://blogs.technet.com/b/identity/archive/2010/03/30/a-microsoft-perspective-on-online-identity-theft-2008.aspx, 12.03.2014.

15) Mitchison, N. *et al*. Identity Theft. A discussion paper. European Commission Joint Research Centre. *Sine loco*: European Communities 2004. Arvutivõrgus: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf, 12.03.2014.

16) Mody, C. Euroopa andmekaitsedirektiivi kohaldamine Facebooki kasutajatele. Juridica 2010/10.

17) Nimmo, M. Identiteedivargus Eesti karistusseadustikus. Uurimistöö. Tallinn: Tartu Ülikooli Õigusteaduskond 2012.

18) Peeters, M. Identity theft scandal in the US: Opportunity to improve data protection. München: Multimedia und recht 2005/7.

19) Policy Guidance on Online Identity Theft. Organization for Economic Co-operation and Development. Seoul: OECD 2008. Arvutivõrgus: http://www.oecd.org/sti/consumer/40879136.pdf, 24.04.2014

20) Punab, M. Ebaõigete ja au teotavate andmete avaldamine ja sellega tekitatud mittevaraline kahju. Bakalaureusetöö. Tartu: Tartu Ülikool 2009, lk 11. Arvutivõrgus: http://www.just.ee/orb.aw/class=file/action=preview/id=49247/Eba%F5igete+ja+au+teotavate+andmete+avaldamine+ja+sellega+tekitatud+mittevaraline+kahju.pdf,19.04.2014

21) Reinthal, T. Ülekriminaliseerimine. Analüüs. Tartu: Riigikohus, õigusteabe osakond 2010. Arvutivõrgus: http://www.riigikohus.ee/vfs/995/2010_Lisa%202%20(Ulekriminaliseerimine_analuus).pdf, 30.04.2014.

22) Sootak, J. Pikamäe, P. *et al*. Karistusseadustik. Kommenteeritud vlj. 3. trk. Tallinn: Juura 2009.

23) United Nations. Office on Drugs and Crime. Handbook on Identity-related Crime.New York: United Nations 2011. Arvutivõrgus: https://www.unodc.org/documents/treaties/UNCAC/Publications/Handbook_on_ID_Crime/10-57802_ebooke.pdf, 12.03.2014.

24) Viiteline norm ja koosseisuteo ebaseaduslikkus. Sootak, J. Juridica 2014/2.

KASUTATUD NORMATIIVMATERJAL

25) Arvutikuritegevusvastane konventsioon. - RT II 2003, 9,32.

26) Eesti Vabariigi põhiseadus. - RT 1992, 26, 349... RT I, 27.04.2011, 2.

27) Euroopa inimõiguste ja põhivabaduste kaitse konventsioon. - RT II 2000, 11, 57.

28) Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni 7. lisaprotokoll. – RT II 1996, 11, 34.

29) Euroopa Liidu põhiõiguste harta. 30.03.2010 – ELT C 326, 26.10.2012. Lk 392-410.

30) Euroopa Liidu toimimise leping (konsolideeritud versioon). 0.03.2010 – LTE C 326, 26.10.2012. Lk 47-201.

31) Euroopa Parlamendi ja Nõukogu 12.07.2002 direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv). – ELT L 201, 31.07.2002. Lk 37-48.

32) Euroopa Parlamendi ja Nõukogu 12.08.2013. a direktiiv 2013/40/EL, milles käsitletakse infosüsteemide vastu suunatud ründeid ja millega asendatakse nõukogu raamotsus 2005/222/JSK. - Euroopa Liidu Teataja (ELT) L 218/8, 14.08.2013. Lk 8-14.

33) Euroopa Parlamendi ja Nõukogu 24.10.1995 direktiiv 95/46/EÜ, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. – ELT L 281, 23.11.1995. Lk 31-51.

34) Fraud Act. - 2005. c 35. Arvutivõrgus: http://www.legislation.gov.uk/ukpga/2006/35/contents, 12.03.2014.

35) Identity Cards Act. - 2006. c 15. Arvutivõrgus: http://www.legislation.gov.uk/ukpga/2006/15/contents, 12.03.2014,

36) Isikuandmete kaitse seadus. - RT I 2007, 24, 127... RT I, 30.12.2010, 11.

37) Karistusseadustik. - RT I 2001, 61, 364… RT I, 26.02.2014, 6.

38) Karistusseadustiku muutmise seadus. - RT I 2009, 51, 348.

39) Lissaboni leping, millega muudetakse Euroopa Liidu lepingut ja Euroopa Ühenduse asutamislepingut sõlmitud Lissabonis 13. detsembril 2007 - ELT C 306, 17.12.2007. Lk 1-231.

40) Protection Act. - 1998. c 29. Arvutivõrgus: http://www.legislation.gov.uk/ukpga/1998/29/contents, 12.03.2014.

41) United States Code (U.S.C.). July 30, 1947, ch. 388, 61 Stat. 633. Arvutivõrgus: http://uscode.house.gov, 12.03.2014.

42) Võlaõigusseadus. - RT I 2001, 81, 487... RT I, 29.11.2013, 4

43) Karistusseadustiku ja sellega seondute teiste seaduste muutmise seadus. - RT I 2007, 13, 69.

44) Kriminaalkoodeks. - RT 1992, 20, 288. (*Kehtetu alates 31.08.2002*)

KASUTATUD KOHTUPRAKTIKA

45) EIKo 06.04.200, 35382/97, *Comingersoll S.A. vs. Portugal*.

46) EIKo 29.05.2001, 37950/97, *Franz Fischer vs. Austria*.

47) EKo 9.112010, C-92/09,C-93/09, *Volker und Markus Schecke GbR, Harmut Eifert vs. Land Hessen.*

48) HMKo 07.06.2010, 1-10-1119.
49) HMKo 13.12.2010, 1-10-13878.
50) HMKo 18.05.2011, 1-11-2698.
51) PMKo 14.09.2011, 1-11-4952.
52) PMKo 24.11.2010, 1-10-13433.
53) RKKKm 01.02.2012, 3-1-1-105-11.
54) RKKKo 06.04.1999, 3-1-1-34-99.
55) RKKKo 01.04.2004, 3-1-1-4-04.
56) RKKKo 02.06.2011, 3-1-1-28-11.
57) RKKKo 04.11.2005, 3-1-1-24-05.
58) RKKKo 04.12.2003, 3-1-1-138-03.
59) RKKKo 05.05.2003, 3-1-1-17-03.
60) RKKKo 05.05.2003, 3-1-1-43-03.
61) RKKKo 06.06.2000, 3-1-1-65-00.
62) RKKKo 06.11.2013, 3-1-2-10-13.
63) RKKKo 09.09.2005, 3-1-1-64-05.
64) RKKKo 10.40.2006, 3-1-1-117-05.
65) RKKKo 11.06.2003, 3-1-1-58-03.
66) RKKKo 13.12.2013, 3-1-1-106-13.
67) RKKKo 15.11.2010, 3-1-1-70-10.
68) RKKKo 16.04.2007, 3-1-1-120-06.
69) RKKKo 18.01.2000, 3-1-1-5-00.
70) RKKKo 23.05.2008, 3-1-1-18-08.
71) RKKKo 23.11.2009, nr 3-1-1-97-09.
72) RKKKo 24.10.2005, 3-1-1-83-05.
73) RKTKo 10.01.2007, 3-2-1-135-06.
74) RKTKo 20.09.2009, 3-2-1-50-09.
75) RKTKo 26.06.2013, 3-2-1-18-13.

MUUD KASUTATUD ALLIKAD

76) Andmekaitse Inspektsioon. Isikukood. Arvutivõrgus: http://www.aki.ee/et/kas-isikukood-delikaatne, 12.03.2014.
77) Compton, A. Largest Identity Theft Case In U.S. History: Amar Singh And Wife, Neha

Punjani-Singh, Plead Guilty To Massive Fraud. - The Huffington post 2012. Arvutivõrgus: http://www.huffingtonpost.com/2012/08/07/largest-id-theft-in-history_n_1751241.html, 30.04.2014.

78) Computer Security Institute. 2010/2011 Computer Crime and Security Survey. Arvutivõrgus: http://gocsi.com/survey, 12.03.2014.

79) Council of Europe. Convention on cybercrime. Explanatory report. Arvutivõrgus: http://conventions.coe.int/Treaty/EN/Reports/html/185.htm, 30.04.2014

80) Council of Europe. Treaty Office. Convention on Cybercrime. Status as of 12.03.2014. Arvutivõrgus: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG, 30.04.2014.

81) Council of the European Union. Justice and Home Affairs. Press Release. 2827th Council meeting. Brussels: Council of the European Union 2007. Arvutivõrgus: http://europa.eu/rapid/pressReleasesAction.do?reference=PRES/07/253&format=DOC&aged=1&language=EN&guiLanguage=en, 12.03.2014.

82) Erelt, T. *et al*. Eesti õigekeelsussõnaraamat ÕS 2013. Kirjakeele normi alus alates 1. jaanuar 2014. Tallinn: Eesti Keele Sihtasutus: 2013. Veebiväljaanne. – Arvutivõrgus: http://www.eki.ee/dict/qs/, 23.04.2014.

83) Euroopa Komisjoni ettepanek "Euroopa Parlamendi ja Nõukogu direktiiv, milles käsitletakse infosüsteemide vastu suunatud ründeid ja millega tunnistatakse kehtetuks nõukogu raamotsus 2005/222/JSK." Brüssel: 2010. Arvutivõrgus: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:ET:PDF, 25.04.2014.

84) Euroopa Komisjoni ettepanek „Euroopa Parlamendi ja Nõukogu direktiiv üksikisikute kaitse kohta seoses pädevates asutustes isikuandmete töötlemisega kuritegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumise kohta“. 25.11.2012. Arvutivõrgus: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:ET:PDF, 26.04.2014.

85) Euroopa Komisjoni ettepanek „Euroopa Parlamendi ja Nõukogu määrus üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (isikuandmete kaitse üldmäärus)“, Brüssel: 25.11.2012. Arvutivõrgus: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ET:PDF, 26.04.2014.

86) Euroopa Komisjoni teatis Euroopa Parlamendile, Nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele. Euroopa digitaalne tegevuskava. Arvutivõrgus: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:REV1:ET:HTML, 12.03.2014.

87) Euroopa Liit. Euroopa Liidu õiguse kokkuvõtted. Infoühiskond. Arvutivõrgus: http://europa.eu/legislation_summaries/information_society/index_et.htm, 12.03.2014.

88) Facebook andmekasutuspoliitika. Facebook.com. Arvutivõrgus: http://www.facebook.com/about/privacy/your-info#howweuse, 29.04.2014.

89) G. E. Moore. Moore's Law or how overall processing power of computers will double every two years. Arvutivõrgus: http://www.mooreslaw.org, 12.03.2014.

90) International Telecommunication Union, Information and Communication Technology. Facts and Figures 2013. Arvutivõrgus: http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx, 12.03.2014.

91) Internet Crime Complaint Center, Mass Market Fraud. Arvutivõrgus: https://www.ic3.gov/media/MassMarketFraud.pdf, 12.03.2014.

92) Intervjuu ringkonnaprokurör Rainer Amur'iga. Telesaade "Pealtnägija". ERR 2014. Arvutivõrgus: http://etv.err.ee/arhiiv.php?id=146055, 29.04.2014.

93) Javelin Stragedy & Report. 2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters. Selected Key Findings. Arvutivõrgus: https://www.javelinstrategy.com/brochure/276, 12.03.2014.

94) Justiitsministeerium. Karistusõiguse Revisjon. Arvutivõrgus: http://www.just.ee/revisjon, 12.03.2014.

95) Justiitsministeerium. Kriminaalstatistika. Registreeritud kuriteod 2003-2013. Justiitsministeerium: 2014. Arvutivõrgus: http://www.just.ee/59292, 29.04.2014.

96) Kagge, R. Fiktiivseid seksikuulutusi avaldavad kiusajad jäävad enamasti karistuseta. - ERR 2014. Arvutivõrgus: http://uudised.err.ee/v/eesti/3e3b9e96-1c3f-41d9-bf67-0125f89c261e, 29.04.2014.

97) Karistusseadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu seletuskiri 554 SE. Arvutivõrgus: http://www.riigikogu.ee/?op=ems&page=eelnou&eid=78433b29-8b2f-4281-a582-0efb9631e2ad&, 28.04.2014.

98) Karistusseadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu seletuskiri 554 SE. Lisa 1. Arvutivõrgus: http://www.riigikogu.ee/?op=ems&page=eelnou&eid=78433b29-8b2f-4281-a582-0efb9631e2ad&, 28.04.2014.

99) Karistusseadustiku muutmise seaduse eelnõu seletuskiri 530 SE I. Arvutivõrgus: http://www.riigikogu.ee/?page=eelnou&op=ems&emshelp=true&eid=673140&u=20120410162824, 12.03.2014.

100) McAfee. What you need to know to avoid identity theft. *Sine anno, Sine loco.* p. 22-23. Arvutivõrgus: http://promos.mcafee.com/en-US/PDF/IDTheft_eguide_US.pdf, 02.05.2014.

101) Morgan, P (raportöör). Euroopa Majandus- ja Sotsiaalkomitee arvamus teemal „Ettepanek: Euroopa Parlamendi ja nõukogu direktiiv, milles käsitletakse infosüsteemide vastu suunatud ründeid ja millega tunnistatakse kehtetuks nõukogu raamotsus 2005/222/JSK", 23.072011. Arvutivõrgus: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2011:218:0130:0134:ET:PDF, 25.04.2014.

102) Pau, A (toim). Jõks: isikukoodide vaba avaldamine rikub põhiõigusi. Eesti Rahvusringhääling (ERR) 2005. Arvutivõrgus: http://uudised.err.ee/v/05b3d228-3da9-47d0-9d4b-ac28ed767d8f, 02.05.2014.

103) Peaminister Cameron, D. *et al.* Ühiskiri Euroopa Ülemkogu eesistujale Herman van Rompuyle ja Euroopa Komisjoni presidendile José Manuel Barrosole. Euroopa majanduskasvu kava. Brüssel: 2012. Arvutivõrgus: http://valitsus.ee/et/uudised/taustamaterjalid/56192/euroopa-majanduskasvu-kava, 19.04.20.14.

104) R. Tigner. Belgium - Court condemns identity theft on Facebook. Technology, Media & Telecommunications News, Linklaters 2012. Arvutivõrgus: http://www.linklaters.com/Publications/Publication1403Newsletter/TMT-News-July-2012/Pages/Belgium-Court-condemns-identity-theft-on-Facebook.aspx, 29.04.2014.

105) Randma, M. Riigikaitsekomisjoni arvamus Euroopa Parlamendi ja Nõukogu direktiivi eelnõu suhtes, milles käsitletakse infosüsteemide vastu suunatud ründeid ja millega tunnistatakse kehtetuks nõukogu raamotsus 2005/222/JSK Eesti seisukohtade kohta. Toompea 25.11.2010. Arvutivõrgus: http://www.riigikogu.ee/?op=emsplain&page=pub_file&file_id=71ced2aa-ec1c-dfb0-9b70-f55ff4e0158b&, 30.04.2014

106) Riigiprokuratuur. Riigiprokuratuuri juhis identiteedivarguse asjades. Tallinn: Riigiprokuratuur 2011. (*Koopia Riigiprokuratuuri loal autori valduses*)

107) Schaar, P (eesistuja). Arvamus 4/2007 isikuandmete mõiste kohta. Direktiivi 95/46/EÜ artikli 29 alusel loodud andmekaitse töörühm. Euroopa Komisjon. Arvutivõrgus: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_et.pdf, 30.04.2014.

108) www.facebook.com, 02.05.2014.

109) www.myspace.com, 02.05.2014.

110) www.rate.ee, 02.05.2014.

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina Merika Nimmo

sünnikuupäev: 02. veebruar 1990

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

"Internetiga seotud identiteedivargus ja selle regulasioon Eesti karistusõiguses"

mille juhendajad on dr. iur Priit Pikamäe ja dr. iur Jaan Ginter

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

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

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

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

Tartus, 05.05.2014