Sisekaitseakadeemia

Politsei- ja piirivalvekolledž

Muraste kool

Kadi Kase

IDENTITEEDIVARGUSE VÕIMALUSED JA TAGAJÄRJED EESTI NÄITEL

Lõputöö

Juhendaja:

Piret Teppan, MA

Muraste 2012

ANNOTATSIOON

SISEKAITSEAKADEEMIA

Kolledž: Politsei- ja piirivalvekolledži Muraste kool	Kuu ja aasta: juuni 2012
Töö pealkiri: ”Identiteedivarguse võimalused ja tagajärjed Eesti näitel”	
Töö autor: Kadi Kase	Olen nõus oma lõputöö kättesaadavaks tegemisega elektroonilises keskkonnas. Allkiri:
Lühikokkuvõte: Käesolev lõputöö on koostatud Sisekaitseakadeemia Politsei- ja Piirivalvekolledži piirivalveteenistuse rühma BS 080 üliõpilase Kadi Kase poolt teemal ”Identiteedivarguse võimalused ja tagajärjed Eesti näitel”. Lõputöö on kirjutatud eesti keeles ning selles on ära toodud inglise keelne sisukokkuvõte. Töö on kirjutatud 37 lehel (pluss LISA 16 lehel). Lõputöö koosneb tiitellehest, annotatsioonist, sisukorrast, sissejuhatusest, töö põhiosast, kokkuvõttest, viidatud allikate loetelust ning lisadest. Lõputöö eesmärgiks on uurida erinevad identiteedivarguste skeeme ning põhjused, mis on rikkumise võimalikuks teinud, miks langeb üha enam inimesi Eestis identiteedivarguste ohvriks. Lõputöös analüüsib autor ka seda, millisest infost identiteedivarguste osas on kõige enam puudust, et inimesed nendele ei reageeri. Lõputöö eesmärgi saavutamiseks püstitatud uurimisülesanded on: 1. Seletada lahti, mis on identiteedivargus ja tuua välja selle erinevad võimalused. 2. Selgitada välja, millised identiteedivarguste liigid on Eestis peamised ning kuidas soodustatakse, on soodustatud, identiteedivarguste võimalikkust.	

Töö uurimisülesannete täitmisel jõudis autor järeldusele, et Eestis on kõige enam levinud kolme liiki identiteedivargusi: phishing, skimming ja taotluste võltsimine.

Autor jõudis ka järeldusele, et identiteedivargusi on Eestis soodustatud vähese teavitustöö ja suhteliselt laialivalguva mõistete määratlusega seadusandluses. Seadustes jäävad mõisted arusaamatuks ja keerulisteks just tavakodanikule, kes ei ole juriidikaga igapäevaselt seotud. Intervjuusid analüüsides jõudis autor järeldusele, et kõige enam peetakse Eestis probleemiks teise isiku nimel kontode loomist Internetis.

Lõputööst kõige otsesemat kasu saab esmalt Politsei- ja Piirivalveamet, sest tööst selgub, missugust teavitustööd ja infot inimesed reaalselt vajavad identiteedivarguste ennetamise, toimumise ja selle kahjude likvideerimise osas.

Võtmesõnad: identiteet, identiteedivargus, isikuandmed, phishing, pharming, phishing-Trooja viirus, skimming, šaakali pettus, konto ülevõtmine, taotluste võltsimine, siseinfo kasutamine

Keywords: identity, identity theft, personal data, phishing, pharming, phishing Trojan, skimming, jackal fraud, account takeover, application fraud, use of inside information.

Säilitamise koht:

Vastab lõputöö nõuetele

Juhendaja: Piret Teppan Allkiri:

Kaitsmisele lubatud

Kolledži direktor: Aivar Toompere Allkiri:

SISUKORD

SISSEJUHATUS

Identiteedivarguse vorme ja võimalusi on palju. Üha enam virtuaalmaailma liikuval ja Internetiajastul elavas ühiskonnas peab arvestama riskidega, mis inimesi ohustavad selles uues keskkonnas. Samuti koonduvad kõik isikuandmed ja andmebaasid ühte kohta, mis lihtsustavad kelmide tööd ja annavad rohkelt võimalusi identiteedivargusteks ning sellega seonduvateks pettusteks. Samal ajal ei toimu identiteedivargused ainult virtuaalmaailmas. Esialgu ka kõige süütumana tunduva personaalse informatsiooni edastamine kolmandatele isikutele või lihtne pangakaardi kaotamine võib hiljem osutuda väga tülikaks ja aeganõudvaks probleemide lahendamiseks. Paljud inimesed aga ei tea üldse, et üks või teine tegu kvalifitseerub identiteedivargusena ning karistatav on.

Töö autor valis lõputöö teemaks „Identiteedivarguse võimalused ja tagajärjed Eesti näitel“ kuna identiteedivargused on üha laiemalt leviv kuritegude liik, mida varem pole Eestis veel väga suureks probleemiks peetud, kuid viimasel ajal eriti levinud. Teema uurimine on hädavajalik, sest identiteedivarguste erinevad vormid arenevad jõudsalt ning kahju, mis taolise teoga tekitatakse suur. Sarnaseid töid on tehtud varemgi, kuid põhjalikumad ülevaated, mis identiteedivargusi käsitlevad, jäävad 2005. aastasse ning needki tuginevad välisriikide kogemustele. Eesti olusid ja elu arvestades, on see uurimus vajalik ning annab ülevaate käsitletava valdkonna valupunktidest.

Teema **aktuaalsus** on päevakorda kerkinud iga aastaga üha enam. Inimesed kajastavad oma elu aina rohkem Internetis ja see tendents on kasvav üha nooremate inimeste hulgas. Riskigrupi moodustavad Internetti kasutavad noored ja vanemad inimesed, kelle jaoks on virtuaalmaailm võõras. Just need grupid vajavad ennetustööd ja teavitamist. Autori jaoks on teema huvitav seetõttu, et on ise puutunud kokku identiteedivargusega ning antud teema süvitsi uurimine tekitab ka isiklikku huvi.

Antud lõputöö panus identiteedivarguste ja isikuandmete töötlemise valdkonda on suur, sest saadakse selgem ülevaade hetkeolukorrast ja nõrkadest kohtadest. Lõputööst kõige otsesemat kasu saab esmalt Politsei- ja Piirivalveamet, sest tööst selgub, missugust teavitustööd ja infot inimesed reaalselt vajavad identiteedivarguste ennetamise, toimumise

ja selle kahjude likvideerimise osas. Kui inimestele jääb teavitustöö ja uurimused tegemata, siis ei ole enam kaua jäänud, et Eesti praegune rahulik olukord identiteedi väärkasutamise vallas muutuks kaoseks ja sellele järgneksid juba laiahaardelisemad ning kahjuderohkemad kuriteod. Hetkel on lihtsam lahendada tekkinud probleeme ja otsida neile lahendusi, kui hakata hiljem selgust tooma kuritegudesse, kus on kümneid tuhandeid kannatajaid

Töö **eesmärgiks** on uurida erinevad identiteedivarguste skeeme ning põhjused, mis on rikkumise võimalikuks teinud, miks langeb üha enam inimesi Eestis identiteedivarguste ohvriks. Lõputöös tahab autor analüüsida ka seda, millisest infost identiteedivarguste osas on kõige enam puudust, et inimesed nendele ei reageeri.

Töö teoreetilises osas uurib autor identiteedivarguste erinevaid vorme ja võimalusi ning analüüsib kaasusi. Neist saab lõputöö autor kinnitust sellele, missugused identiteedivarguse liigid on Eestis levinuimad, millega on loodud alus identiteedivarguste võimalikkuseks.

Käesoleva lõputöö raames viib autor uuringu läbi ekspertintervjuude vormis. Antud töös on kasutatud õigusaktide 12.04.2012 seisuga redaktsioone.

Lõputöö eesmärgi saavutamiseks püstitatud uurimisülesanded on:

3. Seletada lahti, mis on identiteedivargus ja tuua välja selle erinevad võimalused.
4. Selgitada välja, millised identiteedivarguste liigid on Eestis peamised ning kuidas soodustatakse, on soodustatud, identiteedivarguste võimalikkust.

1. IDENTITEEDI MÕISTE JA ÕIGUSLIK ALUS

Ajalooliselt on inimese identiteedi määranud tema sünnijärgne päritolu ja isiklikud saavutused (Allik, Realo, Konstabel 2003:244). Identiteedi küsimus ei ole uus, küll aga on see moodsal ajal eristuv. Identiteet on igal inimesel personaalne ning koosneb isiku andmetest, nagu näiteks isikukood, biomeetrilised andmed, nimi, sünnikoht ja aeg. Identiteet on isikusamasus, mille abil on võimalik isiku andmed samastada isiku endaga. Igaühel on õigus oma isiklikule identiteedile ning kui keegi on ära kasutanud inimese isiklikke andmeid, fotosid vm, tuleb fikseerida võimalikult palju andmeid võõra identiteedi kasutamise kohta ning teha antud rikkumise kohta avaldus politseisse. (Identiteedivargus...29.12.2010)

Identiteet viitab isiku eristatavale loomusele või iseloomule. Inimese tõeline, sisemine identiteet – tema mõtted, tunded ja eelistused – ei ole otseselt jälgitavad. See, mille järgi teised inimese just selle persooni ära tunnevad, on tema väline identiteet, mis koosneb isiku kõikidest tunnusjoontest: sünnikuupäev, silmade värv, aadress, vanemate nimed, lemmikvärv, pangakonto number, kohalikus toidupoes käimise sagedus jne. Nimekirja kuuluvad mittemuutuvad tunnused (sünnikuupäev, vanemate nimed), käitumuslikud mustrid (kohalikus toidupoes käimise sagedus) ja teiste poolt määratud identifikaatorid isiku äratundmiseks (pangakonto number, isikukood, juhiloa number). Iga punkt nimekirjas on isikliku identifitseerimise informatsiooni osa ja kogu nimekiri esindab isiku identiteeti. Teised tunnevad inimese ära kui nad võrdlevad teda neile teadaolevate nimekirja punktidega. Sõbrad, sugulased ja kolleegid tuginevad tavaliselt füüsilistele omadustele – näiteks selle inimese välimus ja hääl – et inimest identifitseerida. Need, kellega isik äriasju ajab, tuginevad identifikaatoritele, millega on hea kaugelt asju ajada, nagu nimi, aadress, telefoninumber ja isikukood. (Schreft 2007:5,6) Isiku identiteet hõlmab isiku nime, tema välimust, tundeid ja mõtteid, isiku minevikku, usutunnistust ja muid veendumusi. Nime kaudu samastab isik end teatud grupiga – pere- või sugukonnaga. Isiku identiteedi oluliseks osaks on tema nimi. Vaatamata sellele, et kaasajal on suurenenud

isikukoodide kasutus, on nimel isiku tuvastamisel suur roll. (Truuväli, Aaviksoo, Kask 2008:281, 293)

Psühholoogias on lähenetud identiteedi olemusele mitmeti. Üks võimalus on identiteedi vaadelda **sotsioloogilises traditsioonis**, kus seda ei käsitleta üldjuhul kui püsivat indiviidi omadust, vaid seda nähakse hoopis situatiivsena, ajas, ruumis ja kontekstis muutlikuna. Sellest lähtuvalt võib identiteet olla küll indiviidi minakontseptsiooni osa, kuid tema koostis ei ole ühtne tervik ja võib olla pidevas muutumises. Kui räägitakse sotsiaalsest identiteedist, mõeldakse seejuures identiteedi seotust sotsiaalsete gruppide, suhete ja rollidega. Sotsiaalsed rollid ja grupid on lihtsalt identifitseerumise võimalused, mida inimesed katsetavad, ja kui need sobivad, võivad need saada identiteedi olulisteks osadeks. (Allik jt 2003:228-231)

Teise võimalusena saab identiteedile läheneda läbi indiviidi enda, personaalselt. **Personaalseks identiteediks** võib pidada unikaalset osa indiviidi mina-kontseptsioonist: spetsiifilisi detaile eluloost, oma kogemustest, ka individuaalsete omaduste, hobide, eelistuste jms enesetaju. Personaalset identiteeti rõhuvad käsitlused toovad esile inimese sisemise potentsiaali ja tõelise mina, kui identiteedi kujunemise peamised alused. Samas on ka personaalne identiteet oma olemuselt sotsiaalne. Vaid sotsiaalsete instrumentide abil, nagu keel, omandatud mõtlemiskujundid, stereotüübid, saab inimene tegeleda oma sisemise minaga ning kujundada seda. Identiteet kui suhteliselt kindel ja püsiv, seostatud arusaam iseendast ja oma suhetest saab põhineda ainult teataval stabiilsuses inimeses ja teda ümbritsevas keskkonnas. (Allik jt 2003:228-231) Kaalutletud jõud, mis annavad inimesele võime omandada personaalset identiteeti, on otseses seoses indiviidi võimega järjestada maailmas prioriteetsuse alusel oma mured, sealhulgas ka inimese oma sotsiaalse maailma mured. Kui inimese personaalne identiteet esindab tema unikaalset subjektiivsust, siis tema olemus on välja kujunenud maailma peegeldusena. (Archer 2000:313) Inimese keha vahendab omavahelist seost personaalse identiteedi ja sotsiaalse identiteedi vahel. Järelikult sotsiaalsed tähendused lisatud füüsilisele kuvapildile ja väljendus on ülimalt tähtsad tegurid indiviidi enesetaju ja sisemiste väärtuste kujunemisel. (Coupland, Gwyn 2003:2)

Sotsiaalteadlased tõlgendavad identiteeti jälle teise nurga alt lähtuvalt. Teistega lävides alustab inimene vaikimisi eeldusest, et on olemas mingi ühtne läbiv joon, mis seob

üksikisiku erinevad teod tervikuks, terviklikuks isiksuseks. Tegelikult on selline eeldus „oma näost“ nii tugev, et püütakse lihtsameelselt leida järjekindlust, järjepidevust ja loogikat käitumises, mis esialgu paistab olevat täiesti plaanitu. Tehes tõlgendavat tööd kellelegi näo andmisel, toetavad inimesed üksteise identiteeti. See ei tähenda, nagu eeldaks „identiteediraam“ iga inimese puhul täiesti jäika ja paigaletardunud identiteeti. Vastupidi, identiteediraam jätab isikule ruumi muutusteks, kasvuks, arenguks ja identiteedi ümbermõtlemiseks, aga igal ajahetkel eeldatakse, et inimesel on oma mina või identiteet ja tema teod pigem peegeldavad seda identiteeti, mitte ei loo seda kui illusoorset mõistet. (Alasuutari 2004: 121-123)

Identiteedi põhikomponente on suhteliselt kerge mõista. Põhikomponendid tuginevad peamiselt kindlatel tunnustel, mis on enamasti ametlikult kindlustatud ja fikseeritud avalike autoriteetide poolt. Need tunnused sisaldavad indiviidi sugu, ees- ja perekonnanime ja osades riikides ka isikule määratud sotsiaalkindlustuse numbrit. Isikuid saab identifitseerida muidugi veel mitmete teiste tunnuste abil, kaasa arvatud arvuti kasutajanime ja parooli, Internetilehekülje, arvuti IP-aadressi (selle kaudu on võimalik tuvastada arvuti Internetis), e-maili aadressi, panga kontonumbri ja PIN koodi alusel. Mõistes identiteedi kontseptsiooni ja kuidas selle osad tegutsevad erinevas meedias, on ülioluline paika panna eesmärgijärgsed vahendid, viisid identiteedi kaitsmiseks. (Online Identity Theft 2009:16,17)

Informatsiooniline enesemääramine, kui õiguslik kontseptsioon, tekkis 1960-ndate aastate lõpus 1970-ndate alguses. Sel ajal toimusid debatid enesemääramisõiguse üle, kus puudutati väga paljusid teemasid, näiteks õigust autonoomiale, õigust olla üksi jäetud, õigust eraelule, õigust kontrollida oma andmeid, õigust piirata ligipääsu oma andmetele, õigust säilitada eksklusiivne kontroll eraellu sekkumise üle, õigust minimeerida sekkumisi, õigust eeldada konfidentsiaalsust, õigust üksiolemisele, õigust nautida intiimsust, õigust nautida anonüümsust, õigust nautida salastatust jne. (Tikk, Nõmper 2007:37)

Tänapäevast informatsioonilise enesemääramisõiguse kontseptsiooni on kõige enam mõjutanud eespool mainitud aruteludest kõlama jäänud neli seisukohta:

1. kontroll isikuandmete üle, mis väljendub andmesubjektilt nõusoleku küsimises;
2. mittesekkumise piiramise vajaduse põhimõtted (eraellu mittesekkumine);
3. sekkumise vajaduse põhimõtted (eraellu sekkumine);

4. intiimsus, mille väljenduseks on tavaliste ja delikaatsete isikuandmete eristamine.

(Tikk, Nõmper 2007 37-38)

Rahvusvahelise õiguse allikatest on suurima panuse informatsioonilise enesemääramisõiguse arengusse andnud **Euroopa inimõiguste ja põhivabaduste konventsioon** (edaspidi EIÕK). Muud allikad lihtsalt märgivad vajadust eraelu puutumatuse kaitsmiseks või viitavad EIÕK-ile. Eesti Vabariigi põhiseaduse § 26 kohaselt on igaühel õigus eraelu puutumatusele. Antud sätte eeskujuks oli EIÕK-i artikkel 8. EIÕK-is on (informatsioonilise) enesemääramisõiguse keskseks sätteks artikkel 8:

1. igaühel on õiguse sellele, et austataks tema era- ja perekonnaelu ja kodu ning korrespondentsi saladust;
2. võimud ei sekku selle õiguse kasutamisse muidu, kui kooskõlas seadusega ja kui see on demokraatlikus ühiskonnas vajalik riigi julgeoleku, ühiskondliku turvalisuse või riigi majandusliku heaolu huvides, korratuse või kuriteo ärahoidmiseks, tervise või kõlbluse või kaasinimese õiguste ja vabaduste kaitseks.

(Tikk, Nõmper 2007:38-39, 47)

Isikuandmete kaitse seaduse (edaspidi IKS) alusel loetakse isikuandmeteks mis tahes andmeid tuvastatud või tuvastatava füüsilise isiku kohta, sõltumata sellest, millisel kujul või millises vormis need andmed on. Delikaatseteks isikuandmeteks peetakse:

1. poliitilisi vaateid, usulisi ja maailmavaatelisi veendumusi kirjeldavaid andmeid, välja arvatud andmed seadusega ettenähtud korras registreeritud eraõiguslike juriidiliste isikute liikmeks olemise kohta;
2. etnilist päritolu ja rassilist kuuluvust kirjeldavaid andmeid;
3. andmeid terviseseisundi või puude kohta;
4. andmeid pärilikkuse informatsiooni kohta;
5. biomeetrilised andmed (eelkõige sõrmejälje-, peopesajälje- ja silmaiirisekujutis ning geeniandmed);
6. andmed seksuaalelu kohta;
7. andmed ametiühingu liikmelisuse kohta;
8. andmed süüteo toimepanemise või selle ohvriks langemise kohta enne avalikku kohtuistungit või õigusrikkumise asjas otsuse langetamist või asja menetluse lõpetamist.

(Isikuandmete kaitse seadus, 15.02.2007)

Andmed, mis ei ole delikaatsed, kuid on hõlmatud isikuandmete mõistega, nimetatakse muudeks või tavalisteks isikuandmeteks. Tavaliste isikuandmete hulgas võib lähtuvalt töötlemise erinõuetest ja –tingimustest eristada veel avalikustatud ja anonüümsete andmete kategooriaid. Anonüümsele kujule viidud andmed ei ole käsitletavad isikuandmetena IKS-i mõistes. Anonüümseteks loetakse andmeid, mis on viidud sellisele kujule, et andmesubjekti ei ole võimalik nende põhjal tuvastada. Samas jääb andmete anonüümsele kujule viimine IKS-i mõttes siiski töötlemiseks. Anonüümseks muutmisel tuleb tagada, et andmete põhjal ei oleks isik enam tuvastatud ega tuvastatav. Teatud juhtudel on isikuandmete töötlemine mõne teenuse osutamise eeldus ja vältimatu osa, näiteks on telefonioperaatoritel ülevaade sellest, kes, kellele, kus ja millal on helistanud ja kui kaua rääkinud. Antud andmed on teenusepakkujale olulised, et hiljem tasumisele kuuluvat makset arvutada. (Tikk, Nõmper:2007:91)

Isikuandmete kaitset iseloomustavad kaks vastandlikku tendentsi. Ühelt poolt kaitseala avardub ja samal ajal teiselt poolt sekkumine sellesse sfääri aina laieneb. Andmekaitse põhimõtted ja reeglid on sätestatud Euroopa Nõukogu konventsioonis, Euroopa Parlamendi ja Nõukogu direktiivis 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. Sellest direktiivist on üle võetud ka isikuandmete kaitse seadus. (Truuväli, Aaviksoo, Kask 2008:282, 293)

Isikuandmete töötlemiseks loeb seadus igat isikuandmetega tehtavat toimingut, sealhulgas ka isikuandmete kogumist, salvestamist, korrastamist, säilitamist, muutmist ja avalikustamist, juurdepääsu võimaldamist isikuandmetele, päringute teostamist ja väljavõtete tegemist, isikuandmete kasutamist, edastamist, rikastamist, ühendamist, sulgemist, kustutamist või hävitamist sõltumata teostamise viisist ja kasutatavatest vahenditest. Samuti on seaduses hästi välja toodud isikuandmete töötlemise põhimõtted, mille alusel võib isikuandmeid koguda vaid ausal ja seaduslikul teel. Andmete talletamine peab toimuma määratletud ja õiguspärase eesmärgi saavutamiseks. Muudel eesmärkidel on lubatud andmeid kasutada üksnes andmesubjekti nõusolekul või selleks pädeva organi loal. (Isikuandmete kaitse seadus 01.01.2011)

Isikuandmete töötlemine, milleks võib olla andmete kogumine, salvestamine, säilitamine, avalikustamine ja muud isikuandmetega tehtavad toimingud (nii riigi kui eraisikute poolt) ohustavad isiku põhiõigusi. See oht on tehnoloogia arenguga üha kasvanud, sest moodsa

aja tehnoloogilised lahendused võimaldavad valida, võrrelda, risttöödelda lühikese aja jooksul tohutut hulka andmeid samal ajal isikust täielikku pilti luues. (Truuväli, Aaviksoo, Kask 2008:281)

Isikuandmete töötlemine füüsilise isiku poolt on lubatud ainult sellisel juhul, kui see toimub isiklikuks otstarbeks (nt kirjavahetus, kontaktandmete loetelud, sünnipäevade kalendrid jms). Sellistel juhtudel ei laiene töötlemisele IKS ega ka Euroopa Liidu õigusaktid. Isikliku otstarbe all tuleb silmas pidada eelkõige olukordi, kus füüsiline isik töötleb isikuandmeid üksnes omaenese vajadusteks ning sellise töötlemisega võivad olla seotud ka perekonnaliikmed ja teised lähedased inimesed. (Tikk, Nõmper 2007:71)

Isikuandmete töötlemise põhimõtted on IKS § 6 väga selgelt välja toodud:
Isikuandmete töötleja on kohustatud isikuandmete töötlemisel järgima järgmisi põhimõtteid:

2. seaduslikkuse põhimõte – isikuandmeid võib koguda vaid ausal ja seaduslikul teel;
3. eesmärgikohasuse põhimõte – isikuandmeid võib koguda üksnes määratletud ja õiguspäraste eesmärkide saavutamiseks ning neid ei või töödelda viisil, mis ei ole andmetöötluse eesmärkidega kooskõlas;
4. minimaalsuse põhimõte – isikuandmeid võib koguda vaid ulatuses, mis on vajalik määratletud eesmärkide saavutamiseks;
5. kasutuse piiramise põhimõte – isikuandmeid võib muudel eesmärkidel kasutada üksnes andmesubjekti nõusolekul või selleks pädeva organi loal;
6. andmete kvaliteedi põhimõte – isikuandmed peavad olema ajakohased, täielikud ning vajalikud seatud andmetöötluse eesmärgi saavutamiseks;
7. turvalisuse põhimõte – isikuandmete kaitseks tuleb rakendada turvameetmeid, et kaitsta neid tahtmatu või volitamata töötlemise, avalikuks tuleku või hävimise eest;
8. individuaalse osaluse põhimõte – andmesubjekti tuleb teavitada tema kohta kogutavatest andmetest, talle tuleb võimaldada juurdepääs tema kohta käivatele andmetele ja tal on õigus nõuda ebatäpsete või eksitavate andmete parandamist.

Isikuandmetega töötamise üle teostab kontrolli Eesti Andmekaitse Inspektsioon (edaspidi AKI) ning seal tuleb registreerida kõik delikaatsete isikuandmetega seonduvad toimingud. Andmekaitse Inspektsioon menetleb isikuandmetega seonduvaid väärtegusid kohtuvälise menetlejana. AKI-l on õigus teha rikkumise kõrvaldamiseks nii ettekirjutusi kui ka trahve.

Väärteomenetlusi alustas Andmekaitse Inspektsioon 2011. aastal isikuandmete kaitse suunal 30 korral. Isikute saadetud kirjalikke selgitustaotlusi laekus 2011. aastal kokku 654, neist valdav enamus ehk 601 olid isikuandmete kaitse suunal. Enim küsimusi tekitanud teemadeks oli andmete avalikustamine seoses maksehäiretega ning sugupuu koostamine ja avalikustamine võrgulehel geni.com, ning tunti huvi ka andmete avaldamise kohta blogides ja suhtluskeskkondades. (Avaliku...2011)

Andmekaitse Inspektsioon rakendas tööle 2009. aastal nõuandetelefoni, kuhu saab helistada igal tööpäeval 4h jooksul. 2011. aastal tuli nõuandetelefonile 816, neist 615 puudutasid isikuandmete kaitset, 111 avaliku teabe seaduse rakendamist ja 90 delikaatsete isikuandmete töötlemise registreerimist. Kõige enam muretsesid helistajad selle pärast, et isikuandmed on kättesaadavad Internetis, avaldatuna mõne ajalehe võrguväljaandes, blogis, suhtluskeskkonnas või sugupuu koostamise võimalust pakkuval võrgulehel. Samuti oli arvestataval hulgal ka küsimusi, mis puudutasid tööandja õigusi töötaja isikuandmete töötlemisel. (Avaliku...2011)

Autori arvates näitab suur kõnede hulk nõuandetelefonile seda, et inimesed tunnevad huvi isikuandmete kasutamise ning nende töötlemise vastu. Inimesed on hakanud huvi tundma oma õiguste vastu ja asunud neid kaitsma. Fakt, et tähelepanu on hakatud pöörama ka Internetis avaldatavatele isikuandmetele (eriti, mis puudutab blogisid ja suhtluskeskkondasid, milles avaldatavate andmete osa on reguleerida keeruline) näitab seda, et see on muutumas inimeste jaoks probleemiks ja tunnetatakse, et keegi võib avaldatud andmeid kuritahtlikult nende endi vastu kasutada. Mis aga puudutab huvi tööandja õigustesse isikuandmete töötlemisel, siis oleks hea, kui tööandjad ise tunneksid selle vastu huvi, mitte ei oleks helistajateks murelikud tööintervjuudel käijad või juba töötavad alluvad. Mõlemal juhul on aga olukord hea, kui tööandjad, töötajad tunnevad huvi oma õiguste ja kohustuste vastu.

2. IDENTITEEDIVARGUSE VORMID

Väljend „identiteedivargus“ on väär, kuna identiteedivargus ei võta tegelikult inimeselt tema identiteeti ära. Vargus hõlmab tavaliselt teise isiku vara võõrandamist kavatsusega isik sellest varast jäädavalt ilma jätta. Inimese isikliku informatsioonile õigusevastane ligipääsemine ja selle kasutamine või isikut tõendavate dokumentide võltsimine, ilma füüsiliselt mingit dokumenti või eset võtmata, ei jäta inimest ilma võimalusest seda informatsiooni kasutada. (Sullivan 2009:79,80)

Palju vaieldakse selle üle, mis on identiteedivargus ja missugune on selle üldine suhe identiteetidega seotud kuritegevusega tegelikult. Üldjoontes võib identiteedi kuritegusid kirjeldada kuritegudena, mille toime panemist võimaldab mingil moel võõra identiteedi kasutamine.

Kõige tavalisem identiteedi kuritegu on identiteedipettus, mille puhul kasutab kurjategija kasu saamise nimel alternatiivset identiteeti ja mille puhul ohvrit veendakse uskuma, et see alternatiivne identiteet on tegelikult kurjategija tõeline identiteet. Nende laiemate üldistuste järgi kasutatakse identiteedivargust tihti selleks, et kirjeldada kuritegelikku tegu, mille käigus omistatakse kolmanda poole (ohvri) isikliku identiteedi informatsioon selleks, et kasutada seda alternatiivse identiteedina kuriteos. Termini laiem kasutus laieneb ükskõik millisele kuriteole, mis on sooritatud alternatiivset identiteeti kasutades. Laiem kasutus üritab kirjeldada kahju, mida ohver kogeb ja rahalist vastutust või teisi tagajärgi, mis on talle tema isikutunnistuse petturliku kasutamise tõttu kaela langenud. (Steel 2010:520)

Identiteedivargus on väga mitmekülgne ja lubamatu tegevus. Üldjoontes on see osa suuremast ebaõigluse või kuritegude ahelast. Tegu on väga keerulise kuriteoga ning liigitamisvõimalusi on palju. Identiteedivargus kvalifitseerub spetsiifilise kuriteona, väärasjana tsiviilõiguses või ettevalmistava sammuna teistele seaduserikkumistele nagu nt pettused, võltsimised, terrorism või rahapesu. Ühe identiteedivarguse definitsiooni järgi toimub vargus siis, kui osapool hangib, kannab üle, omandab või kasutab juriidilise või

füüsilise isiku kohta käivat personaalset informatsiooni omavoliliselt või seoses pettuse, muu kuriteoga. (Online Identity Theft 2009:16)

Paljudel juhtudel on kurjategija eesmärgiks identiteedivargusega ühendada mitmed muud erinevate eesmärkidega kuriteod, nt krediidi, raha, kaupade, teenuste, töökohajärgsete soodustuste või muu väärtusliku hankimiseks, mida saab kasutada ohvri nimel. Identiteedivargad ei pruugi alati ohvri identiteeti kuriteo sooritamiseks isiklikult kasutada. Selle asemel võidakse see müüa teistele osapooltele, kes ise kuriteo toime panevad või teevad uue ebaseadusliku isikutunnistuse, nt sünnitunnistuse, autojuhiload või passi. (Online Identity Theft 2009:17)

Oluline on eristada arvamuse avaldamist ja teise isikuna esinemist ning teise isiku nimel avalduse tegemist. Tuleb vahet teha laimamise, solvamise ja identiteedivarguse vahel. Identiteedivarguse puhul toimub teise isiku identiteedi ekspluateerimine, mis tähendab, et isik esineb teise isikuna. (Avaliku...2010)

Identiteedivargusteks on mitmeid võimalusi:

1. kasutades Internetis e-mailide saatmist;
2. pankade ja firmade kodulehekülgede järele tegemine ja sealt klientide personaalse informatsiooni kogumine;
3. viiruse välja töötamine, mis ohvri tegevusi arvutis ja Internetis salvestama hakkab;
4. magnetriba kasutamine, mis kaardi andmed kopeerib;
5. isikuandmete hankimine surmakuulutustelt ja hiljem nende andmete alusel dokumentide taotlemine;
6. võttes vajalike andmete kogunedes üle isiku konto pangas;
7. võltsides valesid andmeid kasutades taotlusi;
8. kasutades ametikoha kuritarvitamist ning kogudes siseinfot kasutades teiste isikute andmeid.

Identiteedivarguse tüüpe levib palju ning skeeme, millega petetakse inimestelt erinevaid kelmidele vajalikke andmeid välja, luuakse iga päev üha juurde. Antud valdkond laieneb jõudsalt nii Internetis, kui ka reaalses maailmas. Erinevaid skeeme, mille alusel identiteedivargad töötavad, on palju, kuid tuntumaid kirjeldab lõputöö autor alljärgnevalt.

Phishing tüüpi pettus sai alguse nn Nigeeria petuskeemi e-mailidest. Skeemi kasutajad üritavad sooritada edasiarenenud maksupettust, milles palutakse oma sihtmärkidelt ettemaksu või rahaülekannet. Tavaliselt pakuvad petturid oma potentsiaalsele ohvrile võimalust jagada nendega suurt summat raha, mille petturid oma riigist välja viia tahavad. Ohvritel palutakse teha ettemakse, kulutusi või makse, et aidata raha vabastada või ülekannet teostada. Tänu selle petuskeemi enda laiale levikule on skeem Interneti kasutajate hulgas hästi teada ning informeerituse tõttu seda väga enam ei kasutata. (Online Identity Theft 2009:22)

Phishing-tüüpi identiteedivarguse käigus saadavad kurjategijad e-maile kasutades erinevate firmade andmeid, et petta isikutelt välja personaalset finantsinfot nagu arvenumbrid, PIN-koodid vm. E-maili ehtsuse kinnitamiseks loovad kurjategijad Internetilehekülgi, kasutades finantsasutuse logosid ja muid eritunnuseid. Petturid tuginevad laialt levivatele juhuslikele rämpsposti alla kuuluvatele e-mailidele, mis saadetakse ohvrile. Ohvrite e-maili aadressid ostetakse Internetist või kogutakse Internetilehekülgedelt ja uudistegruppidest, kasutades selleks spetsiaalset tarkvara. Sellise tegevusega loodetakse jõuda isikuteni, kes langeksid skeemi ohvriks ja avaldaksid oma pangaandmed, mille tulemusena kasutatakse pettuse ohvrite andmeid krediitkaardipettustes, identiteedivargustes. Esialgsetes phishingu-rünnakutes kasutati e-maile, mis olid halvasti sõnastatud ja sisaldasid palju grammatikavigu. Viimasel ajal on aga petturid alla laadinud Internetilehekülgi, mis koostavad e-maili ja lingi, mis on eristamatud algsest, originaalsest leheküljest. Olenemata finantsilistest kaotustest, mis järgnevad pankadele, kelle nimel sellist petuskeemi tehti, on potentsiaalne mõju klientide usalduse kaotamisel, Internetis teenuste kasutamisel (arvestades kasvutendentsi Internetipankade kasutajate hulgas) märksa suurem ja olulisem. (Countering...2004).

Phishing ja pharming tüüpi identiteedivargused on väga sarnased ning Eestis levinud. Eestis levinud skeemide puhul on keeruline eristada, kumma tüübi identiteedivarguse skeemiga täpselt tegu on, sest need on väga tihedalt teineteisega seotud ning omavahel segunenud. Phishing skeemi järgi koostatud pettuse koostasid kurjategijad, kes saatsid Swedbanki klientidele e-maile, milles paluti kliendil edastada e-maili teel väidetavale panga esindajale oma konto kohta käivaid andmeid. Hiljem, kui pettus oli avalikuks tulnud, rõhutasid Swedbanki esindajad meedias, et pank ei küsi kunagi kliendilt sellist informatsiooni ning eriti veel sellisel viisil.

Kuigi maailmas pole nn Nigeeria petuskeem enam väga levinud, siis Eestis on igal aastal üha uusi juhtumeid, kus inimesed on sellise e-maili ohvriks langenud. Ohvrile räägitakse lisaks raha ülekandmise soovile ka südantlõhestavaid lugusid perekondade kurvast saatusest ning soovist välismaale elama minna. Inimesed langevad nende lugude ohvriks ja kannavad petturitele üle suuri summasid. Autor peab oluliseks veelgi laiemat informeerimist antud teemas. Hetkel ei ole ohvritelt nõutud isiklikke andmeid või pangakonto andmeid, kuid kurjategijad võivad skeeme muuta ning hakata ka sellise loo taustal identiteedivarguseid sooritama.

Pharming on Internetipettuste teine vorm, mis on väga sarnane phishingule. See tugineb samasugustel võltsitud Internetilehekülgedel ja salastatud andmete vargusel, et sooritada Internetipettust. Sellist pettust on keerulisem avastada, sest infot salvestav programm on peidetud nii kaua, kuni ohver võtab vastu söödana kasutatava sõnumi. Selle asemel, et jääda lootma ainult kasutajate klikkidele neid ahvatlevatel linkidel viirusega e-mailides, suunab petuskeem ohvrid ümber järele tehtud Internetilehele isegi, kui ohver on sisestanud õige panga aadressi oma veebilehitsejasse. (Online...29.12.2010) Näiteks 2006. aastal Hansapanga (praegune Swedbank) pealehe, millelt toimus Internetipanka sisse logimine, kopeerimine. Paroolid sattusid kurjategijate valdusesse läbi vastava ründeprogrammi, mis kasutas ära operatsioonisüsteemide turvaauke ning suunas kliendi Internetipanga asemel petturite poolt loodud võltsleheküljele, mille kujundus matkis täielikult Hansapanga Internetipanka. Küll aga jäid klientide kahjud kokkuvõttes alla 50 000 krooni, sest petturite poolt tehtud võltslehekülg oli koostatud väga amatöörlikult ja esines kirjavigu. (Hansapank...17.07.2006)

Antud petuskeemi puhul omastatakse ebaseaduslikult teise isiku isiklikud andmed ning pangakontoga seotud informatsioon. Sellist tüüpi petukirjade ja võltslehekülgede eest hoiatavad pangad läbi meedia inimesi operatiivselt. Ometi on iga kord neid heauskseid inimesi, kes skeemide ohvriteks langevad.

Phishing Trooja viirused on enamasti sellised, mis end automaatselt järele tehtud Internetilehekülgedelt arvutisse laevad ja salaja klahvivajutused salvestavad, kui tarbija Internetipanka külastab. Sellised viirused on peidetud süsteemi kataloogidesse ja jälgivad, kui ohver avab krüpteeritud ühenduse konkreetse panga Internetileheküljega. Kord, kui

ühendus on loodud, hakkab Trooja jäädvustama pilte sisselogimise protsessist hankimaks kliendi informatsiooni. Viirus kogub konto informatsiooni ja saadab selle kurjategijale. (Identiteedi...08.07.2010)

Trooja-viirusega varustatud e-maile saadetakse inimestele ka elektronpostile. Sellisel juhul on e-maili sisuks tavaliselt mõne inimese poolt kasutatud saidi kasutajatingimuste link või mõne paroolivahetusega seotud toimingu viide. Linkidel klikkides, mis e-mailiga kaasas on, laeb inimene aga arvutisse alla paroole salvestava viiruse, mis ühtlasi avab kurjategijale tagaukse inimese arvutisse. (Ära...09.04.2011) Seda tüüpi e-mailid on väga levinud ning neid saadakse tihti, kuid õnneks ei ava enamik inimesi võõrastelt aadressidelt tulevaid kirju ja kahtlust äratavaid linke kergekäeliselt. Ka kasutavad paljud inimesed korralike teenusepakkujate e-posti võimalusi, kus teenusepakkuja teavitab klienti ebaturvalise kirja saabumisest või paigutab selle automaatselt rämpsposti alla.

Skimming-laadse pettuse puhul kasutavad kurjategijad väikest pangakaadri magnetriba lugejat, mille abil saadakse kõik vajalikud andmed, et tühjendada hetkega ohvri pangakonto, teha täiesti uus pangakaart või kasutada andmeid Internetis kaupade eest tasumisel. Sellist vargust on keeruline avastada, sest ohver pole kaarti füüsiliselt kaotanud ning jälile saab vaid kontot jälgides. Sellist magnetriba kopeerimist võivad kasutada ka ebaausad teenindajad, kes poodides, baarides, restoranides maksete vastu võtmisega tegelevad. Seda kasutatakse sellistel juhtudel, kui maksmiseks on vajalik koos kaardiga kliendi silme alt lahkumine.

Skimming-pettust rakendatakse ka ohvri prügis tuhnides, kust võib leida dokumente, arveid, panga väljavõtteid, millelt saadakse ohvri andmeid ning neid andmeid järgides tehakse uus kaart. (Identiteedi...08.07.2010)

Otsestest skimming tüüpi identiteedivargusi Eesti meedias kajastatud ei ole, küll aga sarnastest, kus pangaautomaadi külge lisati väike kaameraga mehhanism, mis salvestas isiku PIN-koodi sisestamise ning seejärel jäi kelmidel üle vaid isikult kott varastada, et pangakaart kätte saada.

Autori arvates ei ole taoline skeem pettusteks väga aktuaalne ning reaalne hetkel, sest inimesed on palju teadlikumad, informeeritumad. Pööratakse tähelepanu

pangaautomaatidele ning et makstes teenindaja kaardiga kuhugi tagaruumidesse ei läheks. Praegusel ajal on enamus teeninduskohtades siiski sellised maksevõimalused, et makseterminal on kliendi lähedal, see kas tuuakse kliendi juurde või asub letil.

Šaakali pettuse skeem on saanud oma nime Frederick Forsythi esikromaani "Šaakali päev" järgi. Šaakali skeem seisneb selles, et kurjategijad võtavad surmakuulutustest ning hauakividelt surnud inimeste nimed ja taotlevad nende identiteedi all dokumente. (Identiteedi...08.07.2010)

Taolistest petuskeemi kasutajatest Eestis info puudub ning autor arvab, et selline petuviis ei ole meil aktuaalne. Autori arvamus tugineb sellele, et ajalehtede surmakuulutused on enamasti sellistest inimestest, kellest jäid maha lähedased, kes on hoolitsenud selle eest, et kõigil vajalikel asutustel ja instantsidel oleks info isiku surmast. Sellises väikeriigis nagu Eesti on tõenäosus, et tuleb välja surnud isiku nime kasutamine, väga suur.

Konto ülevõtmise teel identiteedi varastamise skeem on lihtne: kurjategijad koguvad ohvri kohta informatsiooni ning vajaminevate andmete kokkusaamisel helistatakse krediidipakkujale uue kaardi väljastamiseks, mis lastakse saata kurjategijate poolt valitud aadressile. (Identiteedi...08.07.2010)

Autor arvab, et selline identiteedivarguse vorm paistab väga lihtne ja praegusel infoajastul, kus inimesed kogu enda kohta käiva informatsiooni Internetist kõigile kättesaadavaks teevad, väga tõenäoline ka Eestis toimima hakkama.

Taotlusi võltsides isiku dokumente, kas võltsitakse või varastatakse eesmärgiga avada taotleja nimele arvet, võtta laenu, sõlmida lepinguid vm. Eestis on taolised pettused, kus taotlusi võltsitakse, väga levinud mobiilsete kiirlaenude võtmisel. Isikud annavad oma andmeid pahaaimamatult kolmandatele isikutele või varastatakse neilt dokumendid. (Identiteedi...08.07.2010; Kõiv 18.09.2007) Autor peab tähelepanuväärseks pettuste hulka kiirlaenude võtmisel ning arvab, et sellisele teole järgnevaid kahjusid arvestades, tuleks suhtuda rikkumistesse tõsisemalt ning pöörata rohkem tähelepanu Eestis toimivale mobiilsete laenude võtmise tingimustele ja süsteemile. Tähelepanuväärne on ka laenude võtmise lihtsus, mida tõestab ilmekalt mitmed võõra nimele võetud laenud BIG pangast, kus üheks identiteedivarguse ohvriks langes Saaremaa mees (vaata Lisa 1).

Autori arvates on praegune süsteem, kus piisab laenu võtmisest vaid teise isiku isikukoodi teadmisest, liiga läbimõtlematu ning identiteedivarastele soodne keskkond. Samuti on Eestis väga levinud juhtumid, kus teise isiku andmeid kasutades (saades andmed nt isiku enda käest või otsides need Internetist) luuakse erinevatesse suhtlusportaalidesse nn libakontosid, kus esitletakse end teise isikuna, kasutades isikuandmetele vastava inimese fotosid jm. Selliseid kontosid luuakse nalja pärast, isiku maine kahjustamise eesmärgil. Kontole lisatakse enamasti halvustavat, ebaõiget ning kohati ka ebatsensuurset informatsiooni. Teise isiku andmete kasutamine Internetis on väga keeruline teema ning mõnikord on raske saada aru, kas tegu on siiski identiteedivargusega või kvalifitseerub teguviis pettusena. (vaata Lisa 2) Enamasti ei ole selliste kontode loojad teadlikud, et taoline teguviis on kriminaalkorras karistatav. Vaatamata mitmetele juhtumitele, kus isikuid on karistatud antud tegude eest ning need on ka meediasse jõudnud, ei ole siiski libakontode tegemise tendents langenud.

Samal ajal käib sellise skeemi alla ka teise isiku dokumentide kasutamine enda huvides ning võõra dokumendi kasutamist vanemaks tegemise eesmärgil. Laenude võtmiseks teise isiku dokumentide kasutamist ei ole siiani autori arvates märkimisväärselt kasutatud.

Teisele isikule saab kahju teha mitmeti. Näiteks esinedes rikkumisega vahele jäädes politseile teise isikuna. Sellise identiteedivargusega jäi vahele, näiteks Rene Rohtlaan, kes esines politseile purjus peaga roolis vahele jäädes oma venna Marko Rohtlaanena. Isik tegi seda nii edukalt, et venna nimele määrati isegi rahaline karistus ja ohver ise sai sellest teada alles ametikohale kandideerides, mille eelduseks oli kriminaalkaristuse puudumine. (vaata Lisa 3)

Võõra dokumendi enda huvides kasutamisi esineb palju ka noorte seas, kes võtavad dokumendi, kelleltki kellega ollakse sarnane, ning üritatakse saada sisse klubidesse, pidudele, kus vanusepiirangud või ostetakse alkoholi ja tubakatooteid. Samuti kasutatakse teistele isikutele kuuluvaid dokumente palju reisimisel. Dokumendid tehakse ise, ostetakse kellegi käest, kes on need varastanud vm viisil omastanud muudetakse ära vajalikud andmed või vahetatakse foto ja ületatakse riigipiire kellegi teise identiteedi all. Taolised juhtumid on väga levinud, kuid õnneks värskendatakse dokumentide turvaelemente ja kujundusi aja ning võimaluste uuenedes, millega tehakse kurjategijatele võltsimine võimalikult keeruliseks.

Autori arvates on teise isiku dokumentide kasutamisest reisimise eesmärgil ja vanemaks tegemisest palju räägitud ning kajastatud. Politsei- ja Piirivalveamet tegi eelmisel aastal kampaania noortele, kus kuulsused andsid oma näo ja hääle reklaamile, milles kutsuti üles noori kasutama ainult isiklikke dokumente ja mitte minema seaduse rikkumise teed. Sellist teguviisi kasutades enamus noori, kes vanemana paistmise eesmärgil ja inimesi, kes reisimise eesmärgil dokumenti on võltsinud, ei mõtle, et tegu on identiteedivargusega.

Siseinfo kasutamisel kuritarvitavad töötajad oma ligipääsuvõimalusi personalidokumentidele. Sellise tegevuse eesmärgiks on hankida isikuandmeid. Eelpool mainitud ohust lähtuvalt ärgitatakse ettevõtteid tegema oma töötajate suhtes hoolikamat taustakontrolli. (Identiteedi...08.07.2010)

Eestis reguleerib antud valdkonda Isikuandmete kaitse seadus, mis sätestab isikuandmete töötlemise tingimused ja korra, isikuandmete töötlemise riikliku järelevalve korra ja vastutuse, mis kaasneb isikuandmete töötlemise nõuete rikkumise eest. (Isikuandmete...09.04.2011)

Siseinfo kasutamisest tulenevate identiteedivarguste valdkond pole praegu veel Eestis aktuaalne, kuid töö autor peab hetkeolukorda väga heaks, et alustada eeltööga, ennetamaks eelpool kirjeldatud skeemi järgivate kuritegude hulka. Autor peab väga vajalikuks põhjalikku taustakontrolli ning täiendavaid vestlusi jm nende valdkondade töötajatega, kes puutuvad kokku ja peavad töötama teiste isikute isikuandmetega, nende töötlemisega. Autor peab oluliseks pidevat järelkontrolli töö ajal.

3. IDENTITEEDIVARGUSE EEST MÕISTETAVAD KARISTUSED JA HETKEOLUKORD EESTIS

Et välja selgitada, millised on identiteedivarguste eest mõistetavad karistused Eestis, tutvus autor erinevate seadustega. Ülevaate saamiseks hetkeolukorrast identiteedivargustest, isikuandmete kaitsest ning sellest isikute teavitamisest ja ennetustööst, viis ta läbi neli ekspertintervjuud. Intervjuude osad vastused sai autor e-posti teel ning osad viidi läbi intervjueeritavatele kõige sobivamas kohas, kas intervjueeritavate kodus või tööl.

Intervjueeritavate isikute valiku tegi autor lõputöö kirjutamise käigus. Teoreetilise osa põhjal selgus, et identiteedivargused on enim levinud Internetis. Seega oli üheks intervjueeritavaks Internetikeskkonnas tegutsev veebikonstaabel, kes alustas tööd eelmisel aastal ning tegutseb suhtlusportaalides Rate, Facebook ja teistes foorumites, kus ta on avanud oma nime ja pildiga kontod. Veebikonstaabli ülesandeks on anda inimestele veebis nõu ning jälgida Internetis toimuvat.

Teiseks intervjueeritavaks oli Politsei- ja Piirivalveameti kodakondsus- ja migratsioonibüroo (edaspidi KMO) ametnik, kes on töötanud selles valdkonnas 12 aastat ning tegeleb dokumentide taotlemiste avaldute vastu võtmisega ning valmis dokumentide väljastamisega. Intervjuu KMO ametnikuga viis autor läbi silmast silma.

Kolmas intervjueeritav oli Andmekaitse Inspektsiooni nõunik, sest AKI on üks neid organisatsioone, kes tegeleb isikuandmete kaitse seaduse järgimise üle kontrolli teostamisega. Andmekaitse Inspektsioonist sai autor küsimustele vastused e-posti teel.

Neljas intervjueeritav oli jurist, kes omandab hetkel Tartu Ülikoolis magistrikraadi. Juriidika ja õigusvaldkonnaga on intervjueeritav olnud seotud neli aastat ning sellel alal ka töötanud.

Vaatamata faktile, et palju inimesed ei ole teadlikud, et mõni teguviis kvalifitseerub identiteedivarguse alla ning on karistatav, on tegemist siiski kriminaalkorras karistatava teoga. Sanktsioonid, mis järgnevad tegija arvates tühisele Internetinaljale või kergelt saadud rahale, ei ole väikesed. Kuna karistusseadustiku (edaspidi KarS) § 157², mis identiteedivargusi reguleerib, jõustus alles 15.11.2009, seega on tegemist meie õigussüsteemis üsna uue rikkumisega. Teise isiku identiteedi ebaseaduslik kasutamine muutus selle paragrahviga II astme kuriteoks.

KarS § 157² sätestab teise isiku identiteedi ebaseadusliku kasutamise ning on sõnastatud järgmiselt: teist isikut tuvastavate või tuvastada võimaldavate isikuandmete edastamine ilma isiku nõusolekuta, nendele dokumentidele juurdepääsu võimaldamine või nende kasutamise eest eesmärgiga luua sellest isikust ebaõige ettekujutus, kui sellega tekitati kahju teise isiku seadusega kaitstud õigustele või huvidele, või varjata kuritegu – karistatakse rahalise karistuse või kuni kolmeaastase vangistusega. Normi rikkumisel sooritatakse kuritegu. (Karistusseadustik, 06.06.2001) § 157² rakendamisel on oluline, et kuriteo subjektiivne külg, tegutsemine eelpool nimetatud eesmärgil, peab olema täidetud kõikidel juhtudel, milleks on kasutamine, edastamine, juurdepääsu võimaldamine. Seega, kui isik paneb identiteedivarguse toime ilma eelpool nimetatud eesmärgita, on see ikkagi karistatav. Sellisel juhul tuleb karistus väärteo korras isikuandmete kaitse seaduse alusel ja sellele laieneb Andmekaitse Inspektsiooni järelevalvepädevus. (Avaliku...2009)

Samuti redigeerib võõra identiteedi kasutamist võlaõigusseaduse (edaspidi VÕS) § 1046, milles on öeldud, et isiklike õiguste kahjustamise õigusvastasus, milles sätestatakse isiku au teotamine, ka ebakohase väärtushinnanguga, eraelu puutumatuse või muu isikliku õiguse rikkumine on õigusvastane, kui seadusega pole sätestatud teisiti. Õigusvastasuse tuvastamisel tuleb arvestada rikkumise liiki, põhjust ja ajendit, samuti suhet rikkumisega taotletud eesmärgi ja rikkumise raskuse vahel. Isikliku õiguse rikkumine ei ole õigusvastane, kui rikkumine on õigustatud, arvestades muid seadusega kaitstud hüvesid ja kolmandate isikute või avalikkuse huve. Õigusvastasuse tuvastamisel tuleb sellisel juhul lähtuda erinevate kaitstud hüvede ja huvide võrdlevast hindamisest. (Võlaõigusseadus, 26.09.2001)

Igaühe isikuandmete kaitset ja puutumatust koordineerivad ka Põhiseaduse (edaspidi PS) § 17 ja § 26, mis sätestavad vastavalt, et mitte kellegi au ja head nime ei tohi teotada ning

kõigil on õigus perekonna- ja eraelu puutumatusele. Samuti keelab riigiasutustel, kohalikel omavalitsustel ja nende ametiisikutel perekonna- ega eraellu sekkuda muidu, kui seaduses sätestatud juhtudel ja korras tervise, kõlbluse, avaliku korra, teiste inimeste õiguste, vabaduste kaitseks, kuriteo tõkestamiseks või kurjategija tabamiseks. (Põhiseadus, 28.06.1992)

Isikuandmete ja delikaatsete isikuandmete töötlemise nõuete rikkumist reguleerib Isikuandmete kaitse seaduse § 42 ja § 43. Nende alusel saab teha isikuandmete ja delikaatsete isikuandmete töötlemise nõuete rikkumise eest rahatrahvi kuni 300 trahviühikut ning kui teo on pannud toime juriidiline isik, trahvi suuruses kuni 32 000 eurot. Mõlema rikkumise puhul on kohtuväliseks menetlejaks Andmekaitse Inspektsioon. (Isikuandmete kaitse seadus, 15.02.2007)

Eesti kohtupraktikas on juhtumeid, kus isikuid on identiteedivarguses süüdi mõistetud (vaata Lisa 3), kuid neid võiks olla autori arvates rohkem, kuna tegemist on suhteliselt uue teemaga, siis pigem jääb vajaka teadmistest, mis teod on identiteedivargused ja kuidas neile reageerida.

Autori hinnangul on isikuandmete ja delikaatsete isikuandmete töötlemise ning identiteedi vargusega seonduv Eesti õigussüsteemis üsna hästi reguleeritud. Kohati tundub, et isikuandmete mõiste jääb seaduses liiga laialivalguvaks ja ebamääraseks. Ka intervjueeritud jurist leidis, et hetkeseisul on Eestis seadusandlus selles valdkonnas üldine. Reguleeritud on kõige olulisem ning rikkumised, mis puudutavad isikuandmete õigusvastast käitlemist, on sanktsioneeritud. Samas aga tuleb meeles pidada, et isikuandmete kaitse küsimus on Eestis veel suhteliselt noor ning võrdlus riikidega, kus on aastaid isikuandmetega seotud juriidiliste küsimuste üle vaieldud, oleks kohatu. Jurist leidis aga, et oluline osa on siiski reguleeritud ning otseseid seaduse lünki esineb vähe. Lugedes IKS § 4 lg 1, siis see ütleb, et isikuandmed on mis tahes andmed tuvastatud või tuvastatava füüsilise isiku kohta, sõltumata sellest, millisel kujul või millises vormis need andmed on. See tähendab aga, et seaduse järgi on isikuandmeteks ka tema jalanumber, telefoninumber, aadress jne. Ühelt poolt on tegu väga ähmase mõistega, millest mitte-jurist ei loeks kindlasti välja, et tema telefoninumber võiks olla isikuandmetena käsitletav. Samas on juristi hinnangul seadusandja loonud säärase laiapiirilise kaitse taotluslikult.

Tänapäevases muutuvas maailmas arenevad nii ühiskond, kui ka kuritegevus väga kiiresti. 2007. aastal vastu võetud seadus ei pruugitud ette näha, milliseid (nt IT-alaseid) isikuandmete vastaseid kuritegusid 2012. aastal toime pannakse. Oluliselt lihtsam aga on aru saada mõistest "delikaatsed isikuandmed", mille seadusandja on üles loetlenud IKS § 4 lg 2 p 1-8. Tegemist on konkreetse nimekirjaga sellest, mis on delikaatsed isikuandmed. Kuivõrd delikaatsete isikuandmete töötlemiseks on ette nähtud suuremad piirangud ning karistusõiguslik vastutus delikaatsete isikuandmete ebaseadusliku avaldamise eest (KarS § 157^1), on säärane erinevus mõistete lahti selgitamisel juristi hinnangul igati õigustatud. Samas aga leidis veebikonstaabel, et isikuandmed mõistena on seaduses piisavalt hästi lahti selgitatud.

Kui lõputöö autor leidis teemat lähemalt uurides, et inimesed on vaid üsna põgusalt teadlikud identiteedivarguste temaatikast, oma õigustest (mis puudutab isikuandmete töötlemist ning küsimist), siis samal arvamusel olid ka intervjueeritavad. Juristi hinnangul avaldatakse enda kohta käivat informatsiooni suhteliselt kergekäeliselt (kliendikaartide saamiseks, tuttavatele, kampaaniates osalemiseks jne). Samal arvamusel oli ka veebikonstaabel, kes lisas, et Eestis on identiteedivarguste teema noor ning teadlikkus madal. Probleemina tõid intervjueeritavad välja, et inimesed ei loe läbi kasutajatingimusi, mis on erinevatesse portaalidesse kontode loomiseks seatud. Nagu töö autor teooria osas välja tõi (lk 14), siis oletas ka AKI esindaja, et inimeste teadlikkus on võrreldes 2006. aastaga (millesse jäävad viimased sellekohased uuringud) tõusnud. Sellele viitavad erinevad statistilised näitajad nagu näiteks laekuvate kaebuste arvu jätkuv kasv nõuandetelefonile. Positiivseks loeti meedias kajastuse tõusu iga-aastaselt, mis on suureks abiks inimeste teadlikkuse kasvul oma andmetega seotud õigustest.

Kui inimeste teadlikkust identiteedivarguste valdkonnas võib pidada kesiseks, siis veidi paremaks saab lugeda inimeste teadmisi selles valdkonnas, mis puudutab seaduserikkumist. Intervjueeritavate hinnangul teavad inimesed üldiselt, et identiteedivargus on karistatav, kuid ei teata identiteedivarguse täpsemat koosseisu. Samas on identiteedivarguse koosseisu täitmiseks oluline, et on tekitatud kahju isiku õigustele või huvidele, kelle identiteeti on kasutatud, kuid inimene ei pruugi alati teada tema huvide kahjustamisest. Kannatanuni jõuab tema vastu suunatud rikkumine alles siis, kui puututakse kokku tagajärgedega või avastatakse enda isikuandmete kasutamine. Kõik intervjueeritavad leidsid, et inimesed ei pruugi alati teadvustada probleemi kui nad on

langenud identiteedivarguse ohvriks.

Nii veebikonstaabel kui ka jurist tõid välja, et identiteedivarguste ohvriks langenute pöördumisi, abipalveid, laekub neile harva või ei täida need juhtumid alati kuriteo koosseisu. Mõlemad intervjueeritavad leidsid, et ohvrite peamiseks mureks on tavaliselt see, et teine isik on esinenud ohvri nime all ning sellega kahjustanud isiku nime ja mainet. Autori hinnangul võib pöördujate madal hulk näidata üheltpoolt seda, et inimesed ei pruugi teadvustada, et nime või andmete kasutamine ilma luba küsimata (sh kontode avamine Internetis jne), on kuritegu, kuid samas võib see ka tõesti näidata hetkel nende juhtumite vähesust.

KMO poolt vaadatuna on identiteedivargused ja teiste isikutena esinemine haruharvad juhtumid ning pigem peetakse seda aastate taguseks probleemiks ning rohkem Internetis levinud mureks. Samal arvamusel olid ka teised intervjueeritavad. Identiteedivargused on selgelt Internetis leviv probleem, mis on esile tõusnud erinevate populaarsete suhtlusportaalide loomisega.

Intervjueerimise käigus tõi KMO ametnik välja, et dokumentide taotlemisel teise isiku identiteedi kasutamist on tulnud ette väga harva. Kindlasti on üheks määravamaks faktiks see, et alates 2009. aastast on kõikidel reisidokumentidel sõrmejälg kiibil kohustuslik, mis on reguleeritud ka Isikut tõendavate dokumentide seadusega. Samuti on dokumentide taotlemisel näha andmebaasides eelnevate dokumentide fotosid. Näitena toob KMO ametnik välja ainult juhused kaksikutega, kus üks teadlikult soovib taotleda teise dokumenti.

Rohkem on esinenud juhtumeid, kus KMO-st käest soovitakse taotleda dokumente, milleks isikul õigused puuduvad. Kui vaadelda üldiselt, siis on Eestis selliste juhtumite protsentuaalne suhe äärmiselt väike. Seega leiab autor, et hetkel ei ole Eestis probleemiks teise isiku andmeid ning olemasolevaid dokumente kasutades uute dokumentide taotlemine. Antud järeldusele jõudis töö autor ka erinevaid meediasse jõudnud identiteedivarguse juhtumeid analüüsides. Samuti ei ole märkimisväärselt neid olukordi, kus dokumendi valdajale sarnane isik taotleks teisele kuuluvat dokumenti.

Dokumendi taotlemisel kontrollitakse seoseid dokumendi taotleja ja esitatavate dokumentide vahel KMO-s põhjalikult: eelnevalt väljastatud dokumentide põhjal, sõrmejälgede alusel, visuaalselt. Kui isikul eelnevad dokumendid andmebaasides puuduvad, siis võidakse küsida täiendavaid dokumente, mis juba ammu kehtivuse kaotanud, kuid ikka alles või uuritakse sissekirjutust. Tänu sõrmejälgede võtmisele ja tehnika arengule on muutunud dokumentide taotlemine küll keerulisemaks, kuid samas ka turvalisemaks.

Seoses identiteedivarguste ja isikuandmetega seotud valdkondade keerukuse ja raskete tagajärgedega on suur roll teavitusel ja ennetustööl. KMO on selles vallas teinud palju tööd esimeste isikutunnistuste (ID-kaartide) kasutusele võtmise juures. Välja on antud buklette, teatmikke, erinevaid infomaterjale ning ka vestluse käigus inimesi teavitatud isikuandmete väärkasutamisest, dokumentide hoidmisest ja tähtsusest neid mitte teistele isikutele edasi anda. KMO ametnik tõi välja, et üldiselt on inimesed üsna teadlikud ja täiendavat teavitustööd oleks vaja teha ainult vanemate inimeste puhul. Ka on KMO ametnikel olemas erinevatelt dokumentide alastelt koolitustelt omandatud teadmised ja ülevaade erinevatest võimalikest (nende töös) ette juhtuvatest isikuandmete väärkasutamise võimalustest dokumente taotlevate isikute poolt.

AKI on ennetustööna algatanud kolm kampaaniat, mis on suunatud erinevatele vanusegruppidele. Väikelastele on tehtud multifilm „Juss ei jaga oma andmeid!“. Teine kampaania on üritus, mis suunatud ühiskonnaõpetuse õpetajatele („Vigade parandus: laste andmete kaitse“). Kolmas kampaania on ainult Interneti-keskkonda suunatud „Päästa Liisa ID!“. AKI otsustas viimase kampaania viia läbi ainult Internetis just sel põhjusel, et teavitada sihtgruppi varitsevatest ohtudest neile omases keskkonnas ja keeles. Liisal on suhtlusvõrgustikus Facebook oma konto, kus saab neiut aidata erinevate murede lahendamisel ning samas jagab Liisa ka näpunäiteid ja nõuandeid, kuidas oma andmeid kaitsta. Ühelt poolt leiab autor, et teavituskampaaniaid on tehtud ja tehakse, kuid samas on need keskendunud erinevatele spetsiifilisematele valdkondadele nagu dokumendid ja Internetiturvalisus. Miinuseks on AKI poolt läbi viidava kampaania puhul see, et kampaania peamine reklaamimine (peale AKI koduleheküljе) toimub siiski Internetis ainult ühes suhtlusportaalis. Samas peab autor väga heaks seda, et noori õpetatakse juba väga varajases eas Internetis varitsevaid ohte märkama ja vältima (läbi Jussi multifilm) ning seda tööd, teavitust jätkatakse ka koolides ühiskonnaõpetuse tundide raames.

Oma vastuses tõi AKI nõunik välja, et nad ei ole profileerinud kõige tõenäolisemat identiteedivarguse ohvriks langeva inimese tüüpi ega vanusegruppi. Vastaja leidis, et see oht varitseb kõiki arvutikasutajaid, kes pole mõelnud oma privaatsuse kaitsmise tähtsusele. Juristi hinnangul on kõige tõenäolisemaks identiteedivarguse ohvriks langeja keskmine Interneti kasutaja, kes üldiselt ei tutvu erinevate portaalide kasutajatingimustega ja avaldab enda kohta käivaid andmeid veebikeskkonnas kergekäeliselt. Samas leidis intervjueeritav, et probleemiks on ka mobiiltelefonide, sülearvutite, dokumentide kaotamine ning selliste juhtumite puhul on teisel isikul ohvri andmeid kerge leida. Veebikonstaabel pidas peamisteks ohvriteks selliseid inimesi, kes on sattunud konflikti klassi- või koolikaaslastega või hoopis armukadeda ning kättemaksuhimulise inimese piiramisse. Samas peab töö autor kõige tõenäolisemalt sellise kuriteo ohvriks langejaks pigem nooremaid inimesi (alates sellest vanusest, mil Internetti kasutama hakatakse – u 25 eluaastani), kes veedavad aega Internetis suhtlusportaalides ning kasutavad erinevaid lehekülgi, kus pakutakse osalemisi loosimistes jms. Selles vanusevahemikus on inimesed, kas liiga kärsitud ja täiesti teadmatuses neid varitsevatest ohtudest või ei soovi süvenenult läbi lugeda kõiki tingimusi ja lehekülgi.

Mõlemad intervjueeritavad, kellele küsimus esitati, tõid välja lihtsad põhitõed, kuidas mitte identiteedivarguse ohvriks langeda:

1. enne andmete avaldamist tuleb hoolikalt järele mõelda, kas avaldatavad andmed on ikka asjakohased ja kindlasti vajalikud avaldamiseks antud kohas;
2. tuleb hoolikalt uurida, kellele andmed avaldatakse;
3. tuleks mõelda, endale selgeks teha, kuidas kasutatakse avaldatavaid andmeid hiljem edasi;
4. enda kohta käivate andmete avaldamisel tuleks lähtuda minimaalsuse põhimõttest;
5. tuleb teadvustada riske, mis kaasnevad andmete avaldamisega.

Identiteedivarguste juhtumite vähendamiseks leidis veebikonstaabel olevat kõige vajalikumaks sammuks inimeste informeerimise. Üldsusele tuleks selgeks teha, et identiteedivarguse puhul on tegemist kuriteoga, mille eest on ette nähtud ka reaalne vanglakaristus. Intervjueeritav lisas, et laiemale avalikkusele on hetkel jäänud pigem mulje, et identiteedivarguse puhul on tegemist väärteoga. Samale arvamusele jõudis teooria

osa põhjal ka käesoleva töö autor. Paljud inimesed, kas ei teadvusta tegu rikkumisena või identiteedivargusele järgnevaid sanktsioone.

Kunagi, aastaid tagasi, oli väga levinud situatsioonid, kus alla kehtestatud vanusepiirangu eas olevad noorukid võtsid võõra dokumendi ning proovisid sisse pääseda ööklubidesse. Autor uuris nii juristilt, kui ka veebikonstaablilt, kas selline tegevus on levinud ka praegusel hetkel ja kas see kvalifitseerub identiteedivarguse alla. Juristi definitsioon identiteedivargusele: "*Identiteedivargus on teise isiku identiteedi volituseta kasutamine siis, kui ilma nõusolekuta teise isikuna esinemise tulemusena on teise inimese õigustele või huvidele kahju tekitatud või see on toime pandud kuriteo varjamiseks.*" Sellest järeldab autor, et üheltpoolt võiks tegu küll identiteedivargusena kvalifitseeruda, kuid samas ei ole sellise tegevusega teise isiku õigustele või huvidele õigusrikkuja poolt kahju tehtud ning samas ei esine võõra dokumendi kasutaja teise identiteedi all ka kuriteo varjamiseks. Samas leidis veebikonstaabel, et antud tegu võiks mingis osas identiteedivarguseks pidada, kuid siiski lahendatakse selline rikkumine KarS § 349 alusel. Vaatamata sellele, et viimasel ajal pole taoline rikkumine nii levinud, kui varasematel aastatel ja pole võõra isiku dokumendiga ööklubidesse sisenemise üritamine saanud ajalooks.

KarS § 349 sätestab tähtsa isikliku dokumendi kuritarvitamise, milleks on teise isiku nimele väljaantud tähtsa isikliku dokumendi kasutamine või enda nimel väljaantud tähtsa isikliku dokumendi teisele isikule kasutamiseks andmise eesmärgiga omandada õigusi või vabaneda kohustustest ning määrab sellise teo eest rahalise karistuse või kuni kolme aastase vangistuse. (Karistusseadustik, 06.06.2001)

KarS § 350 seletab lahti mõiste tähtis isiklik dokument. Sellisteks dokumentideks on isikutunnistus, digitaalne isikutunnistus, elamisloakaart, Eesti kodaniku pass, diplomaatiline pass, meremehe teenistusraamat, välismaalase pass, ajutine reisidokument, pagulase reisidokument, meresõidutunnistus, tagasipöördumistunnistus, tagasipöördumise luba, välisriigi reisidokument, rahvusvahelise organisatsiooni reisidokument ja mootorsõidukijuhi juhiluba. (Karistusseadustik, 06.06.2001) ehk tegemist on eelkõige dokumentidega, mis on mõeldud reisimiseks.

Seega võib väita, uurides identiteedivarguste eest määratavaid karistusi ja analüüsides intervjuusid, et praegusel hetkel ei ole identiteedivargused Eestis massiliselt levinud, vaid

enamus jääb Internetis infoportaalides valeprofiilide loomise tasemele ning identiteedivarguse eest määratavad karistused autori arvates piisavad. Teavitustööd on tehtud erinevatele vanusegruppidele erinevates kommunikatsioonivahendite kaudu. Kuid ohte, mis võivad kaasneda isiklike andmete edastamisega, ei ole kõik inimesed veel endale teadvustanud. Nii jääbki risk, et identiteedivarguste kasutamiseks leitakse järjest uuemaid mooduseid.

KOKKUVÕTE

Üsna sageli on inimesed teiste suhtes heausksed, ei osata midagi karta ning antakse kellegi teise valdusesse personaalseid andmeid, mida pahatahtlikud tihti ära kasutavad. Inimesed justkui ei oleks teadlikud neist ohtudest, mis kaasnevad informatsiooni sattumisega valedesse kätesse. Seda tõestavad ka faktid, sest iga uue petuskeemi välja tulles on hulk isikuid, kes selle lõksu langevad ja hiljem väga siiralt väidavad, et nad pole kuulnudki sarnastest juhtumitest, mille eest meedia ja avalikkus rahvast hoiatanud on.

Vaatamata sellele, et identiteedivargus kuriteo liigina on meie karistusõiguses veel väga noor ja uus rikkumine, peaks sellele valdkonnale oluliselt rohkem tähelepanu pöörama. Inimeste teavitamine peaks olema märkimisväärselt intensiivsem ja järjepidevam. Praegusel hetkel toimub inimeste harimine ja teavitamine alles siis, kui laiahaardeline petuskeem on juba toimunud ning ohvreid ja kannatajaid palju.

Töö eesmärgi saavutamiseks püstitatud uurimisülesannete täitmisel jõudis autor järeldusele, et Eestis on kõige enam levinud kolme liiki identiteedivargusi:

1. phishing;
2. skimming;
3. taotluste võltsimine.

Esimesed kaks levivad Internetis ning muutuvad paralleelselt tehnika ja infoajastu arenemisega üha läbimõeldumaks, keerulisemaks. Kolmas identiteedivarguse vorm on levinud Eestis kõige laialdasemalt. Kord kasutatakse teisele isiku identiteeti laenu võtmiseks, teisel hetkel hoopis isiku maine kahjustamise eesmärgil. Autori väide selle kohta, et just need kolm liiki kõige levinumad on, tugineb meediasse jõudnud ja seal kajastamist leidnud juhtumitel.

Uurimisülesandeid täites jõudis autor ka järeldusele, et identiteedivarguste võimalikkust on Eestis soodustatud äärmiselt vähese teavitustöö ja suhteliselt laialivalguva mõistete

määratlusega seadusandluses. Seadustes jäävad mõisted arusaamatuks ja keerulisteks just tavakodanikule, kes ei ole juriidikaga igapäevaselt seotud.

Intervjuusid analüüsides jõudis autor järeldusele, et kõige enam peetakse Eestis probleemiks teise isiku nimel kontode loomist Internetis. Sellise tegevuse eesmärgiks on tavaliselt kättemaks ning soov selle isiku mainet kahjustada, kelle nime all esinetakse.

Samuti jõudis autor järeldusele, et hetkeolukord Eestis identiteedivarguste valdkonnas on rahuldav, kuid ettevaatlikuks tegev ning on viimane aeg hakata tegelema inimeste veelgi intensiivsema informeerimise ja e-keskkonna turvalisemaks muutmisega. Olukord on hea, kui arvestada identiteedivarguste juhtumite ja kaebuste vähesust, mis politseisse, juristideni jõudnud. Samas aga võib kaebuste vähesus olla tingitud hoopis teadmatus probleemist või sellest, kuhu murega pöörduda. Autor peab väga oluliseks inimeste teavitamist ja harimist identiteedivarguste erinevate vormide alal, et inimestel oleks ülevaade võimalikest ohtudest. Hetkel pööratakse tähelepanu vaid toimunud ja levivatele skeemidele. Vaatamata sellele, et ülejäänud identiteedivarguse vormid (skimming, šaakali pettus, konto ülevõtmine ja siseinfo kasutamine) pole Eestis väga levinud või nende toimimise kohta Eestis üldse info puudub, peaks tähelepanu neile pöörama.

Autor teeb ettepaneku alustada intensiivse teavitustööga sarnaste kampaaniatena nagu korraldab Politsei- ja Piirivalveamet liiklusohutuse alast teavitust. Sellised kampaaniad peaksid olema lisaks Internetile kajastatud ka tänavapildis ja ajakirjanduses. Samuti peaks hakkama käima noortele identiteedivarguste ja isikuandmete kaitse temaatikat koolides tutvustamas (sarnaselt narkootikumide ohtlikust kajastavatele projektidele, mida politseiametnikud koolides läbi viimas käivad).

Autor peab käesoleva lõputöö arendamist edasi magistritööks võimalikuks, sest uuritav teema on väga lai ning pidevas muutumises, mille tõttu tekib kogu aeg juurde erinevaid identiteedivarguse skeeme. Antud teema vajaks kindlasti edasist ja rohkem süvitsi uurimist.

SUMMARY

The graduation thesis „Possibilities of identity theft and its consequences exemplified by Estonia“ is written in Estonian, with a summary in English included. The paper consists of 35 pages (plus a 16-page APPENDIX). The graduation thesis consists of a title page, an abstract, a table of contents, the main section of the text, conclusion, references and appendices.

The objective of this graduation thesis is to study different identity theft schemes, factors that enable such infringements and causes why increasing number of people in Estonia fall victim of identity thefts. In the graduation thesis the author also analyses why people fail to react to identity thefts and what kind of information is primarily lacking.

The research objectives set to achieve the goal of the thesis are:

1. to define identity theft and list different possible methods;
2. to determine the main types of identity theft in Estonia and how those identity thefts have been facilitated.

Performing research tasks for the thesis, the author came to the conclusion that three most widespread types of indentity theft in Estonia are phishing, skimming and application fraud. The author also concluded that identity thefts in Estonia have been facilitated by failure to provide sufficient information to the public and relatively diffuse definition of terms in our legislation. Legal terms in legislation remain unclear and complicated for laymen who don’t come to into contact with legal matters on a daily basis.

Analysing the interviews, the author came to the conclusion that creating Internet accounts under other person’s name is considered to be the biggest problem in Estonia.

Police and Border Guard Board benefits most directly from this final thesis because this paper clarifies what kind of notification and information people actually need about occurrence and prevention of identity thefts and damage control.

VIIDATUD ALLIKATE LOETELU

Alasuutari, P. 2004. Social Theory and Human Reality. SAGE Publications

Allik, J., Realo, A. ja Konstabel, K. 2003. Isiksusepsühholoogia. Tartu Ülikooli Kirjastus

Archer, M. S. 2000. Being Human: the Problem og Agency. Cambridge University Press

Avaliku teabe seaduse ja isikuandmete kaitse seaduse täitmisest aastal 2010. Andmekaitse inspektsiooni kodulehelt http://www.aki.ee/download/1862/AKI%202010%20aasta%20ettekanne.pdf välja otsitud 18.04.2011

Avaliku teabe seaduse ja isikuandmete kaitse seaduse täitmisest aastal 2012. Andmekaitse inspektsiooni kodulehelt http://www.aki.ee/est/index.php?part=html&id=258 välja otsitud 10.04.2012

Countering Financial Crime Risks in Information Security. Financial Services Authority. 2004. The Financial Services Authority kodulehelt http://www.fsa.gov.uk/pubs/other/fcrime_sector.pdf välja otsitud 28.12.2010

Coupland, J. ja Gwyn, R. 2003. Discourse, the Body, and Identity. Palgrave Macmillan

Hansapank hoiatab Internetipetturite eest. 17.07.2006. Postimees Online kodulehelt http://www.postimees.ee/170706/esileht/majandus/209695.php välja otsitud 18.04.2011

Hirsjärvi, S., Remes, P. ja Sajavaara, P. 2005. Uuri ja kirjuta [Tutki ja kirjoita]. Tõlge eesti keelde: I. Kraav, T. Kuurme, U. Kala, M.-L. Laherand, V. Maansoo. ja J. Orn. Tallinn, Kirjastus Medicina. (Originaal on publitseeritud Kustannusosakeyhtiö Tammi, Helsinki, 2004)

Identiteedivargus 08.07.2010. Tarbijakaitseameti kodulehelt www.tka.riik.ee/public/identiteedi_vargus.doc välja otsitud 29.12.2010

Identiteedivargus. Politsei- ja Piirivalveameti kodulehelt http://www.politsei.ee/et/nouanded/it-kuriteod/identiteedivargus/ välja otsitud 29.12.2010

Identiteedivargus: pätt võttis 38 000 laenu. Eesti Tarbijakaitse Liit. http://www.tarbijakaitse.ee/modules.php?op=modload&name=News&file=article&sid=7051&mode=thread&order=0&thold=0 välja otsitud 29.12.2010

Isikuandmete kaitse seadus 15.02.2007, jõustunud 01.01.2008 - RT I 2007, 68, 421... RT I, 30.12.2010, 2

Karistusseadustik 06.06.2001, jõustunud 01.09.2002 - RT I 2002, 44, 284… RT I, 11.03.2011, 1

Kuul, M. 13.12.2010. Venna identiteeti kuritarvitanu pandi vangi. Eesti Rahvusringhäälingu uudiste kodulehelt http://uudised.err.ee/index.php?06220809 välja otsitud 29.12.2010

Kõiv, M. 18.09.2007. Turvalisus Internetis: identiteedivargus kui uus pahalaste „hitt". Eesti Päevalehe Ärileht. Eesti Päevalehe kodulehelt http://www.arileht.ee/artikkel/400404 välja otsitud 29.12.2010

Online Fraud: Pharming. Norton kodulehelt http://us.norton.com/cybercrime/pharming.jsp välja otsitud 29.12.2010

OECD. 2009. Online Identity Theft. OECD publishing

Põhiseadus 28.06.1992, jõustunud 03.07.1992 - RT I 2003, 29, 174... RT I, 27.04.2011, 1

Schreft, S. L. 2007. Risks of Identity Theft: Can the Market Protect the Payment System? Economic Review (01612387); 2007 4th Quarter, Vol. 92 Issue 4, p5-40, 36p, 3 Graphs. EBSCO andmebaasist välja otsitud 01.05.2011

Steel, A. 2010. The True Identity of Australian Identity Theft Offences: a Measured Response or an Unjustified Status Offence? University of New South Wales Law Journal, Vol 33 Issue 2, p503-531, 29p, 1 Chart. EBSCO andmebaasist välja otsitud 01.05.2011

Sullivan, C. 2009. Is Identity Theft Really Theft? International Review of Law, Computers & Technology, Vol. 23, Nos. 1–2, March–July 2009, 77–87. EBSCO andmebaasist välja otsitud 01.05.2011

Tikk, E. ja Nõmper, A. 2007. Informatsioon ja õigus. Kirjastus Juura.

Truuväli, E-J., Aaviksoo, B., Kask, O., Lehis, L., Madise, L., Madise, Ü., Merusk, K., Mälksoo, L., Narits, L., Olle, V. ja Pruks, P. 2008. Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. Kirjastus Juura.

Võlaõigusseadus 26.09.2001, jõustunud 01.07.2002 - RT I 2002, 53, 336... RT I, 08.07.2011, 6

Ära usalda pealtnäha autoriteetseid linke. Arvutikaitse. http://www.arvutikaitse.ee/category/rampspost välja otsitud 09.04.2011.

LISA 1

Saaremaal elav mees sattus identiteedivarguse ohvriks, kui tema nimel avati BIG pangas võltsitud dokumentidega konto ja võeti 38 000 krooni laenu. Saarlane sai laenust teada, kui talle helistati pangast ja öeldi, et ta pole laenu tagasi maksnud. Laen oli võetud Tartus Lõunakeskuse BIG panga kontorist, kuid mees polnud Tartus paar aastat käinud, rääkimata nimetatud pangakontorist. Edasise uurimise käigus selgus, et laenu võtmiseks oli esitatud mehe juhiluba. Võrdluses selgus, et mehe enda juhiloa number ei vastanud sellele numbrile, mis oli esitatud juhilubadel. Selgus, et võltsitud juhilube on kasutatud suisa kolmel korral erinevate firmade juures. Kurjategija oli käinud esmalt Swedbanki kontoris ning võtnud laenu saamiseks saarlase konto väljavõtted. Seejärel avas kurjategija Nordea pangas saarlase nimel konto, millele BIG pangast võetud laen kanti. Paari järgneva päeva jooksul võeti sularahaautomaatidest kogu raha välja. Saarlane käis ka Nordea pangas avatud kontot vaatamas ning see oli tühi, lisaks sai ta ka vaadata juhiloa koopiat, mis konto avamisel tehti. Koopial oli näha, et juhiloal oli küll tema nimi ja isikukood, kuid foto oli kellestki teisest. Koheselt, peale BIG pangast tulnud kõnet, tegi mees politseisse avalduse. Kõige kummalisem antud loo juures on aga see, et pangast anti teada, et Tartu postkontorist oli laenu esimene tagasimakse tehtud. (Identiteedivargus...29.12.2010)

Antud identiteedivarguse juhtum toimus täielikult taotluse võltsimise skeemi järgi. Kuna autojuhiluba on pankade poolt aktsepteeritud isikut tõendava dokumendina, siis praegusel infoajastul, kus kõik vajalik on Internetis olemas, ei olnud kurjategijal keeruline uurida välja saarlase nime ja isikukoodi, mis on ainsad isikuandmed autojuhilubadel, ning seejärel tema nimel pangas esineda.

LISA 2

Käesoleva töö autoriga võttis 2011. aasta augustis ühendust tuttav neiu, kes oli saanud paari-kolme päeva jooksul kõnesid ja sõnumeid mobiiltelefonile meestelt, kes soovisid osta kannatanult erinevaid teenuseid. Esmalt ei saanud kannatanu aru, miks tulevad temale sellised kõned. Ühelt helistajalt uurides sai tütarlaps teada, et telefoni number on saadud portaali litsid.com üles pandud kuulutusest, kus neiu olevat pakkunud raha eest intiimteenuseid. Tuttavale selgitas, et tegu on ilmselt mingi eksitusega. Internetti uurima minnes selgus, et vastav teade selles portaalis tema telefoni numbriga tõesti nähtav oli ning kuulutuse juurde oli lisatud ka pilt, mis ilmselt Internetist suvaliselt võetud.

Neiu leidis nimetatud leheküljelt ka teisi analoogseid kuulutusi, mis samasuguse skeemina postitatud (sama sisuga tekst ja Internetist võetud foto kuulutuse kõrval), kuid kõigil olid märgitud erinevad telefoninumbrid. Võttes ühendust märgitud kontakttelefonil, sai telefoninumbri omanik ühendust vanemate naisterahvastega, kes kõik olid väga üllatunud ning väitsid, et ei tea antud kuulutustest midagi.

Ohver võttis ühendust ka litsid.com portaali moderaatoriga, kus kuulutus üleval oli, kuid vastust ega lahendust probleemile sealt koheselt ei tulnud. Kuna aga aeg läks edasi ning kõned ja sõnumid jätkusid, kontakteerus kannatanud suhtlusportaalis Facebook seal tegutseva veebikonstaabliga, et saada nõu, kuidas tegutseda. Veebikonstaablilt tuli vastus, et antud tegu identiteedivarguse alla ei kvalifitseeru. Süüteo koosseis oleks ilmselt seotud autoriõiguste rikkumisega, kuna fotod, mida kuulutuste juures kasutatud, ei kuulunud teates märgitud kontaktisikutele (telefoninumbri omanikele).

Tuttav pöördus peale eelpool mainitud kirjavahetust uuesti töö autori poole ning selgitas veebikonstaablilt saadud vastust. Töö autori nõuande peale saata küsimus, kas telefoninumber on käsitletav isikuandmetena ning kas tegu võib olla identiteedivargusega, AKI-le ohver seda ka tegi.

Andmekaitse Inspektsioonist tuli vastus selgitustaotlusele AKI peadirektorilt, kes märkis, et vastavalt isikuandmete kaitse seaduse § 4-le on isikuandmed mis tahes andmed tuvastatud või tuvastatava füüsilise isiku kohta, sõltumata sellest, millisel kujul või millises vormis need andmed on. Sellest tulenevalt võib füüsilise isiku telefoninumber olla käsitletav isikuandmetena, kui selle põhjal on võimalik otseselt või kaudselt isiku tuvastada. Vastuses viidati ka IKS § 11-le, milles öeldakse, et andmesubjektil on õigus ise avaldada enda kohta käivaid andmeid, kuid kui seda on tehtud ilma andmesubjekti nõusolekuta, siis on tegu rikkumisega. AKI vastusest selgus: kuna andmeid on avalikustatud ilma andmesubjekti nõusolekuta, siis võib tegu olla pettuse või identiteedivargusega, mille üle teostab järelevalvet politsei.

Kogu kirjavahetus võttis aga nii palju aega, et enne AKI-st vastuse saamist oli portaali administraator kuulutuse maha võtnud ning kannatanu ei pöördunud antud juhtumiga edasi politseisse.

LISA 3

Rene Rohtlaan esines politseile Tallinnas Suur-Karja tänaval purjus peaga roolis vahele jäädes oma venna Marko Rohtlaanena. Kogu kriminaalmenetluse vältel esines R. Rohtlaan oma vennana ning roolijoodik anti kohtu alla, kus talle määrati 12 300 krooni suurune rahaline karistus. Marko Rohtlaan sai enda alusetust süüdimõistmisest teada aga alles tükk aega hiljem, mil mees kandideeris ametikohale, mille eelduseks oli kriminaalkaristuse puudumine, soovitud töökoht jäi mehel saamata, sest andmebaasis oli tal karistus joobes juhtimise eest. M. Rohtlaan tegi politseile avalduse, milles soovis saada selgitust eksituse toimumise kohta. Kriminaaluurimise käigus tuvastati, et segaduse põhjustajaks oli tema vend, kes tunnistas ka oma teo üles ning ütles, et on ka varem oma venna, M. Rohtlaane nime all esinenud. Juunis mõisteti Marko Rohtlaan maakohtus õigeks. R. Rohtlaan sai aga lisaks joobes juhtimisele ka süüdistuse identiteedi varguses ja karistuse kandmisest kõrvale hoidmises. Harju maakohus mõistis 13.12.2010 süüdi purjuspäi roolis tabatud 33aastase Rene Rohtlaane vangi. Mees sai koos varasema kandmata karistuse liitmisega kokku ühe aasta, 11 kuu ja 17 päeva pikkuse vangistuse. (Kuul 2010)

Ka antud kaasuse puhul kasutas kurjategija teise isiku andmeid, et end kellegi teisena esitleda. Seekord ei olnud küll eesmärgiks otsese kasu saamine, vaid karistusest pääsemine, mis isikul õnnestus. Kõige enam segadust tekitav fakt aga loo juures on see, et ei politsei ega ka kohtuinstantsid saanud aru, et Rene Rohtlaan esineb oma venna Marko Rohtlaanena, kellega on neil vanusevahe 7 aastat. Kahjuks jääb selgusetuks selle loo puhul fakt, kas Rene Rohtlaan kasutas oma isiku tõendamiseks venna originaaldokumente või olid isikul venna andmetega võltsitud dokumendid.

LISA 4

Politsei- ja Piirivalveameti kodakondsus- ja migratsioonibüroo ametnikule esitatud intervjuu küsimused:

1. Kui tihti on tulnud Teie töös ette, et tullakse dokumente taotlema kasutades võõrast identiteeti?

Seda on väga harva, seda enam, et tänapäeval võetakse dokumendi taotlemisel sõrmejäljed ju. Ausalt öeldes minul isiklikult ei olegi olnud sellist juhust. Mis on küll paar korda olnud, mida ma olen kuulnud, on kaksikud tulnud. Üks kaksik on teise eest tulnud, teadlikult siis. Võib-olla kunagi oli see protsent suurem aga see on ikka ääretult väike protsent, võib-olla kunagi oli neid palju aga kuna nüüd on sõrmejäljed, siis see on üsna välistatud. Esiteks sul on ju pildid kogu aeg, eelmiste taotluste pildid on ees, et seda praktiliselt pole. Minul ei ole seda ette tulnud, see protsent on olnud kogu aeg väga väike.

2. Kui palju on neid juhtumeid, kus keegi teine (kel selleks õigust pole) soovib, et talle väljastatakse teise isiku dokumente?

No neid juhtumeid on võib-olla rohkem, kuid siiski väga harv juhus. Ma ütlen, olen ise töötanud 12-aastat selles vallas ja selle aja jooksul on olnud 2 juhust. Tegelikult on need protsendid ikka väga väiksed. Kui mitmed tuhanded on meie käest läbi käinud ja see kaks juhust, see protsent on ikka ääretult väike.

3. Kuidas/kui põhjalikult kontrollitakse isikusamasust (dokumentide taotlemisel) dokumendi taotleja ja esitatavate andmete vahel?

Esimest korda taotletakse tänapäeval lapsele dokumente ning see kontroll saab olla ainult visuaalne ja mingite eelnevalt väljastatud paberite põhjal, näiteks sünnitunnistus vms. Üldiselt ikka eelnevate dokumentide järgi ning sõrmejälgede alusel. Inimesel on alati mingigi dokument olemas ning mida hakatakse siis uurima on sissekirjutust, dokumendi

õigsust, kas see on õiges kohas väljastatud. Inimestel on kasvõi mingidki vanad dokumendid alles jäänud, näiteks vanad sõjaväe piletid vms.

4. Kas KMO poolt vaadatuna on identiteedivargused ja teiste isikutena esinemine Eestis aktuaalne probleem?

Ei ole.

5. Kas KMO on teinud teavituskampaaniaid või reklaame isikuandmete ja dokumentide väärkasutuse kohta?

Jah, selleks on antud ju välja igasuguseid buklette ja teatmikke, infomaterjale, et ära anna sõbrale ja sõbrannale oma dokumente ja isikutunnistust ja passi ja võõraste dokumentide kasutamine on kuritegu, selliseid voldikuid on küll olnud. Ega sa muudmoodi ju ei saa inimest kaitsta, kui et ütled, et see tegu on seadusevastane ja ongi kõik.

6. Kas KMO on teinud oma töötajatele ka identiteedivarguste temaatikat puudutavaid koolitusi?

Kindlasti on teinud, kuidas muidu on selgeks saadud need asjad. Mida on nüüd väga palju on need võltsdokumentide koolitused ja koolitusi, et millised riigid väljastavad mis dokumente aga et päris ainult identiteedivarguse teemalisi koolitusi...pigem on see teema seotud kuidagi teistesse koolitustesse.

7. Mis on Teie isiklik arvamus, kas identiteedivargused on Eestis hetkel probleemiks ning kas inimesi on selle valdkonna ohtudest piisavalt teavitatud? Põhjendage

Ei ole. Mina leian küll nii. Pigem on see aastatetagune probleem. Võib-olla on see rohkem Internetis levinud. Ma arvan, et inimesed on ise üsna teadlikud, mis puudutab dokumente ja nendega ümber käimist. Esimeste ID-kaardiga seoses räägiti ju sellest palju ja olid meelespead, et ära kanna PIN-koode rahakoti vahel kaasas ja kuidas isikutunnistusega ümber käia. Inimesed on ise üsna teadlikud. See on ikka iga inimese oma vastutus, isiku oma probleem ja ma ei leia, et oleks vaja eraldi teavitust, võib-olla siis ainult vanemate inimeste hulgas.

LISA 5

Veebikonstaablile esitatud küsimused:

1. Kas Teie hinnangul on inimesed teadlikud, et üks või teine rikkumine kvalifitseerub identiteedivarguse alla (nt teise isikuna esinemine) ja kui teadlikud on kannatanud, et nad identiteedivarguse ohvriks langesid?

Identiteedivarguse koosseise on minu teada Karistusseadustikus ainul üks. St saab olla ainult üks konkreetsete tunnustega rikkumine, mida on võimalik sellisse koosseisu alla kvalifitseerida, elulisi tunnuseid võib olla jah erinevaid. Samuti on natukene kohatu näide: nt teise isikuna esinemine. Millisel viisil on veel võimalik siis identiteedivargust toime panna?

Teine asi on nüüd tõesti teadlikus, teatakse et identiteedivargus on karistatav, aga ei teata täpselt, mida see endast kujutab. Kannatanu saab teadvaks oma ohvriks langemisest hetkel kui ta tagajärgedega kokku puutub või ise kogemata enda nimele loodud valeidentiteedi avastab.

2. Kui tihti pöördutakse Teie poole kahtlusega, et ollakse langenud identiteedivarguse ohvriks?

Minu poole pöördumisel enam reeglina kahtluseid kui selliseid ei ole, on jäänud veendumus. Keskmiselt tuleb nädala kohta 4 pöördumist, millest suurem osas siiski koosseisu ei täida.

3. Mis on peamised identiteedivarguste ohvrite mured? (nt. Võõras on avanud konto tema nime all suhtlusportaalis? On võetud laen ohvri nime all? Jne)

Mure on reeglina selline, et keegi on esinemas temana ja kahjustanud tema mainet. Laenu võtmist ohvri nimel esineb üsna vähe

4. Millised on levinuimad viisid identiteedivarguse ohvriks langemisel? (nt. Internetis küsimustikke täites avaldatakse andmeid? Suhtlusportaalides avaldatakse ise liiga palju enda kohta käivaid andmeid? Dokumendid varastatakse? Jne)

Levinuim on vast siiski klassi- ja koolikaaslaste vaheline konflikt või siis õnnetu armastuse tagajärjel tekkinud konflikt ja sellisel viisil siis loodetakse kätte maksta. Seega enamasti on andmed juba teo toimepanijale teada.

5. Kas inimesed on üldse teadlikud oma õigustest (mis puudutab isikuandmete küsimist erinevatel lehekülgedel Internetis ning erinevate asutuste poolt) ja kui teadlikud ollakse isikuandmete töötlemisega kaasnevatest kitsendustest?

Inimeste teadlikus on madal. Meenutagem millal Te viimati mõnda tarkvarajuppi arvutisse paigaldades kasutustingimused läbi lugesite? Pigem käis see ikka next, next, next, install ja kõik. Samuti käib kontode loomine, andmete avaldamine ja kõik muud. Teadlikkuse pool tõusetub mureks siis, kui probleem juba olemas.

6. Kui hea on Teie hinnangul inimeste teadlikkus identiteedivarguste teemast? Kas ollakse altid avaldama enda kohta käivat informatsiooni vabatahtlikult/ilma küsimata (Internetis, tänaval/kaubanduskeskuses küsitlejatele jne)?

Korraldage mõni kampaania, mis nõuab isikuankeedi täitmist ja andmed on Teil olemas. Seega üsna kergekäeliselt jagatakse oma andmeid. Identiteedivarguse teema on Eestis üsna noor ja teadlikkus madal.

7. Kas Teie hinnangul on praegu kehtivas Isikuandmete kaitse seaduses piisavalt hästi lahti selgitatud mõiste isikuandmed?

Jah, minu meelest on piisavalt hästi.

8. Kui tihe ja milline on koostöö Andmekaitse Inspektsiooni ja Politsei- ja Piirivalveameti vahel isikuandmetega seonduvate rikkumiste lahendamisel?

Koostöövormi PPA ja AKI vahel kommenteerida ei oska, kuna puudub kokkupuude.

9. Mis oleks need sammud, mida peaksid erinevad ametiasutused (nt AKI, PPA) astuma, et teavitada üldsust antud probleemist ning vähendada identiteedivarguste juhtumeid?

Üldsuseni peaks jõudma tõdemus, et tegemist on kuriteoga, mille eest ette nähtud reaalne vanglakaristus. Loengutelt on saanud selgeks, et pigem ollakse arvamusel, et on identiteedivargus väärtegu.

10. Mis on need nö lihtsad põhitõed, mida inimesed peaksid meeles pidama, et ei langeks identiteedivarguse ohvriks?

Enda kohta käivate andmete avalikustamisel tuleks lähtuda minimaalsuse põhimõttest. Seda eeskätt just suhtlusvõrgustikes.

11. Kas on tegu identiteedivargusega, kui alaealine kasutab teisele isikule kuuluvat dokumenti ööklubisse sisse saamiseks? Kas selline tegevus on ka hetkel Eestis probleemiks?

Võõra dokumendi kasutamist lahendatakse pigem KarS § 349 järgi. Kuigi mingis osas võiks seda tõesti ka identiteedivarguseks pidada. Probleemiks ta viimasel ajal enam nii väga ei ole, kui varasematel aastatel. Kuigi jah, välja surnud selline probleem ei ole.

LISA 6

Andmekaitse Inspektsiooni nõunikule esitatud küsimused:

1. Kas inimesed on üldse teadlikud oma õigustest (mis puudutab isikuandmete küsimist erinevatel lehekülgedel Internetis ning erinevate asutuste poolt) ja kui teadlikud ollakse isikuandmete töötlemisega kaasnevatest kitsendustest?

Inimeste teadlikkuse uuringut ei ole kaua aastaid tehtud. Viimane pärineb aastast 2006, mille tulemused ei ole täna enam ilmselt päevakohased. Oletame, et inimeste teadlikkus on võrreldes nimetatud ajaga tõusnud, millele viitavad statistilised näitajad (näiteks kaebuste arvu jätkuv kasv). Ka ajakirjanduses valdkonna kajastus tõuseb iga aastaselt, mis on suureks abiks inimeste teadlikkuse kasvul oma andmetega seotud õigustest.

2. Mis andis AKI-le tõuke algatada teavituskampaaniat „Päästa Liisa ID“?

„Päästa Liisa ID!“ kampaania on jätk möödunud aastal tehtud väikelastele mõeldud multifilmile „Juss ei jaga oma andmeid!“ http://www.youtube.com/watch?v=XQeulPuqk_c.

Kuna Andmekaitse Inspektsiooni huvi on suunata oma ressursid ka pro-aktiivsetele tegevustele, et tulevikus vähendada kaebuste laviini ja suurendada teadlikke inimeste hulka, siis soovime teavitada valdkonnast ka noori ja nooremaid inimesi. Teavituskampaania kanalivalik langes Internetile seetõttu, et seekordne sihtgrupp on väga aktiivne Interneti kasutaja. On teemast lähtuvaltki loogiline, et otsustasime Internetis (Facebookis on Liisal oma konto) valdkonna uudiseid vahendada, sihtgrupile omases keeles. Tegelikult oli jaanuaris ühiskonna õpetuse õpetajatele suunatud üritus „Vigade parandus: laste andmete kaitse“ – vaadake konverentsimaterjale siit: http://www.aki.ee/est/?part=html&id=25 - kus samuti sai tutvustatud „Päästa Liisa ID“ mängu kui õppevahendit koolis.

3. Kas AKI poolt vaadatuna on identiteedivargused ja teiste isikutena esinemine Eestis aktuaalne probleem?

Jah, AKI leiab, et identiteedivargused on praeguses ühiskonnas probleem. Kuivõrd tegemist on tehnoloogia kiire arengu tulemusel tekkinud väljundiga, siis oma uudsuse tõttu ei saa inimesed, kes teise inimese identiteeti kuritarvitavad, tihti aru, et tegemist on karistatava teoga.

4. Kas erinevate juhtumite taustal on AKI-l välja kujunenud nö kõige tõenäolisemalt identiteedivarguse ohvriks langeva inimese profiil?

AKI ei ole profileerinud inimtüüpi ega vanusegruppi, kes on kõige tõenäolisem identiteedivarguse ohvriks langeja. Leiame, et see ohustab kõiki arvuti kasutajaid, kes ei ole mõelnud oma privaatsuse kaitsmise tähtsusele, selliseid inimesi on igast soost ja vanuses.

5. Kui tihe ja milline on koostöö AKI ja Politsei- ja piirivalveameti vahel isikuandmetega seonduvate rikkumiste lahendamisel?

AKI ja Politsei-ja Piirivalveameti vahel toimub pidev ja tihe koostöö, kuid eelkõige puudutab see politsei infosüsteemi väärkasutamist.

LISA 7

Juristile esitatud küsimused:

1. Kas Teie hinnangul on inimesed teadlikud, et üks või teine rikkumine kvalifitseerub identiteedivarguse alla (nt teise isikuna esinemine) ja kui teadlikud on kannatanud, et nad identiteedivarguse ohvriks langesid?

KarS § 157^2 järgi on teist isikut tuvastavate või tuvastada võimaldavate isikuandmete tema nõusolekuta edastamise, nendele juurdepääsu võimaldamise või nende kasutamise eest eesmärgiga luua teise isikuna esinemise teel temast teadvalt ebaõige ettekujutus, kui sellega on tekitatud kahju teise isiku seadusega kaitstud õigusele või huvidele, või varjata kuritegu. Seega on identiteedivarguse koosseisu täitmiseks oluline see, et on tekitatud kahju isiku õigustele või huvidele, kelle identiteeti on kasutatud. Inimene ei pruugi aga alati teada, et tema huvisid on kahjustatud.

Üldiselt on tänapäeval inimesed suhteliselt teadlikud erinevatest rikkumistest. Inimene ei pruugi teada, mis on isikuandmed ja spetsiifilisi juriidilisi probleeme, kuid üldiselt nad teavad, millised tegevused rikuvad nende huvisid või õigusi. Iseasi, kas sellele ka reageeritakse.

2. Kui sagedased on juhtumid, kus kannatanu isikuandmete töötlemise rikkumise või identiteedivarguse juhtumiga juristi poole pöördub?

Väga sage ei ole, aga ette on tulnud.

3. Mis on peamised identiteedivarguste ohvrite mured? (nt. Võõras on avanud konto tema nime all suhtlusportaalis? On võetud laen ohvri nime all? Jne)

Vajalike isikuandmete soetamiseks on mitmeid viise. Levinumad on näiteks andmekandjate, sh sülearvutite ja mobiiltelefonide vargus, teise isiku prügi läbivaatamine

(dumpster diving), postisaadetiste vargus. Praktikas on olnud juhtumeid, kus andmekogude haldamise eest vastutavad isikud kopeerivad ebaseaduslikult andmekogus sisalduvad isikuandmed ka endale või teisele isikule. Internetis on isikuandmeid, sh kasutajanimesid võimalik saada Interneti otsingumootoreid kasutades, samuti suhtlusvõrgustikest (social networking), nagu rate, orkut, facebook, secondlife jne, kus isikud ise on avalikustanud oma andmed või loonud digitaalse identiteedi. Isikuandmeid võidakse isikult välja petta e-maili või telefoni teel (phishing, social engineering). Viimaste aastate jooksul on sagedamaks muutunud ka arvutisüsteemide vastu rünnete sooritamine ning nuhkvara (spyware) levitamine andmetele juurdepääsu saamise eesmärgil.

Mis puudutab identiteedivargust isiku maine kahjustamise eesmärgil, siis seoses Interneti levikuga on sagenenud teise isikuna esinemine kas foorumites, Interneti jututubades või muudes suhtluskeskkondades. Isiku õigusi kahjustavateks tegudeks saab lugeda teise isiku poolt tema nime all Internetis kommenteerimise, blogi pidamise, e-kirjade saatmise, kodulehe loomise, erinevatesse suhtlusvõrgustiku portaalidesse konto ja profiili loomise jne. Juhul, kui eelpool nimetatud viisil edastatakse informatsiooni, mis on ebaõige, laimav või solvav, kahjustab see oluliselt isiku õigusi. Tegemist ei ole samas mitte üksnes küberruumi probleemiga, vaid sellised rikkumised võivad toimuda ka reaalses maailmas. Isik võib ka füüsilises maailmas saata kirju, avaldada ajalehtedes, raadios jne libakuulutusi, teha telefonikõnesid, esitleda ennast teise isikuna ning sellise käitumisega kahjustada identiteedi õige omaniku mainet, teda naeruvääristada, rikkuda tema suhteid teiste isikutega või teha varalist iseloomu mitteomavaid tehinguid.

Samamoodi kahjustab isiku õigusi, kui kuriteo toime pannud isik kasutab tema andmeid ning selle tulemusena tekib teistel väärettekujutus kuriteo toime pannud isiku kohta. Ka sellisel juhul, saab seda lugeda isiku õiguste rikkumiseks ning talle kahju tekitamiseks.

4. Kas inimesed on üldse teadlikud oma õigustest (mis puudutab isikuandmete küsimist erinevatel lehekülgedel Internetis ning erinevate asutuste poolt) ja kui teadlikud ollakse isikuandmete töötlemisega kaasnevatest kitsendustest?

Enamik inimesi ei loe läbi saitide kasutajatingimusi. Üldiselt on kõik õigused ja kohustused seal kirjas ja need, kes kasutajatingimused läbi loevad, neid ka teavad. Sellistel juhtudel võivad nii mõnedki tingimused üllatuseks tulla.

Isikuandmete töötlejad ei ole tihti kursis sellega, millistel tingimustel võib antud andmeid kasutada. Lihtsaim näide – lähed poodi, teed kliendikaardi, annad oma telefoni numbri või e-maili aadressi ning elu lõpuni saad neilt sõnumeid ja meile uusimate toodete ja parimate pakkumistega. See on õigustatud aga ainult sellisel juhul, kui oled eelnevalt nõustunud sellega. Muuks otstarbeks ei või andmeid ju kasutada.

5. Kui hea on Teie hinnangul inimeste teadlikkus identiteedivarguste teemast? Kas ollakse altid avaldama enda kohta käivat informatsiooni vabatahtlikult/ilma küsimata (Internetis, tänaval/kaubanduskeskuses küsitlejatele jne)?

Üldiselt antakse oma informatsiooni (eriti e-maili aadresse) suhteliselt kergekäeliselt ära. Ma ei pea siinkohal silmas muidugi suvalistele inimestele, aga ennekõike kliendikaartide saamiseks, tuttavatele, kampaaniates osalemiseks jne. Inimesed ei ole väga teadlikud identiteedivarguseid puudutava teema osas ja kindlasti tuleks rahvast sellest rohkem informeerida.

6. Kui heaks/piisavaks peate Eesti seadusandlust, mis reguleerib isikuandmetega seonduvat?

Hetkeseisuga on Eestis suhteliselt üldine seadusandlus. Reguleeritud on kõige olulisem ning sanktsioneeritud on ka rikkumised, mis puudutavad isikuandmete õigusvastast käitlemist. Siinkohal ei saa unustada, et isikuandmete kaitse küsimus on Eestis suhteliselt noor ning Eestit ei saa võrrelda selles osas riikidega, kus on aastaid isikuandmetega seotud küsimuste juriidilise külje üle vaieldud. Minu hinnangul on siiski oluline osa reguleeritud ning otseselt seaduse lünki esineb vähe.

7. Kas Teie hinnangul on praegu kehtivas Isikuandmete kaitse seaduses piisavalt hästi lahti selgitatud mõiste isikuandmed?

IKS § 4 lg 1 järgi on isikuandmed mis tahes andmed tuvastatud või tuvastatava füüsilise isiku kohta, sõltumata sellest, millisel kujul või millises vormis need andmed on. See tähendab, et seaduse järgi on isikuandmeteks ka tema jalanumber, rinnahoidja suurus, telefoni number, aadress jne.

Ühest küljest on tegemist väga ähmase mõistega, mitte-jurist ei loeks kindlasti seaduse tekstist välja, et tema rinnahoidja number võiks olla isikuanne. Samas on seadusandja loonud säärase laiapiirilise kaitse taotluslikult. Tänapäevases arenevas maailmas arenevad nii ühiskond, kui ka kuritegevus. 2007. aastal vastu võetud seadus ei pruugi ette näha, milliseid (nt IT-alaseid) isikuandmete vastaseid kuritegusid 2012. aastal toime pannakse. Loomulikult on alati võimalikud seadusemuudatused, kuid isiku vastutusele võtmiseks on oluline, et tema tegu oli teo toime panemise ajal seadusevastane.

Palju lihtsam on aru saada mõistest "delikaatsed isikuandmed" seadusandja on need üles loetlenud IKS § 4 lg 2 p 1-8. Tegemist on konkreetse nimekirjaga sellest, mis on delikaatsed isikuandmed. Kuivõrd delikaatsete isikuandmete töötlemiseks on ette nähtud suuremad piirangud ning karistusõiguslik vastutus delikaatsete isikuandmete ebaseadusliku avaldamise eest (KarS § 157^1), on säärane erinevus mõistete lahti selgitamisel igati õigustatud.

8. Mis on need nö lihtsad põhitõed, mida inimesed peaksid meeles pidama, et ei langeks identiteedivarguse ohvriks?

Kindlasti on oluline mõelda selle peale, kellele ja kuhu oma andmeid (ja milliseid andmeid) anda. Kindlasti ei tuleks siinkohal laskuda debiilsusteni ja küsida iga kord, et miks teil on vaja mu isikukoodi, kui ma juba oma ID kaardi numbri olen andnud. Aga tuleb alati hoolikalt järele mõelda.

Näiteks juhtus ühel mu sõbrannal selline lugu: käisid õega Pariisis klubis ja klubis tehti pilte. Selleks, et neid pilte kätte saada, tuli luua endale konto, selleks tuli anda oma e-maili aadress. Nemad siis toksisid selle rõõmsalt sisse ning tänase päevani saavad nad igal nädalal u 7 meili selle kohta, mis erinevates ööklubides Pariisis toimub. Kumbki neist Pariisis ei ela ja esimesest üritusest on möödas u 5-6 aastat. Nendest listides on pea võimatu ennast välja saada ning kui juba oma e-maili aadressi annad, võib arvestada, et sinna laekub pidevalt soovimatuid kirju. See ei ole küll otseselt seotud identiteedivargusega, ent õpetlik lugu sellegipoolest.

9. Kas on tegu identiteedivargusega, kui alaealine kasutab teisele isikule kuuluvat dokumenti ööklubisse sisse saamiseks? Kas selline tegevus on ka hetkel Eestis probleemiks?

Identiteedivargus on teise isiku identiteedi volituseta kasutamine siis, kui ilma nõusolekuta teise isikuna esinemise tulemusena on teise inimese õigustele või huvidele kahju tekitatud või see on toime pandud kuriteo varjamiseks.