TARTU ÜLIKOOL
Sotsiaalteaduste valdkond
Ühiskonnateaduste instituut
Infokorralduse õppekava

Monika Prants

Julgeolekuasutuse kõrgendatud tähelepanu all olemise tajutud mõju inimeste sotsiaalmeediakäitumisele

Lõputöö

Juhendaja: Maria Murumaa-Mengel, PhD

Tartu 2019

SISUKORD

SISSEJUHATUS

Õigus privaatsusele puudutab igat inimest. Senikaua aga, kuni seda õigust ei riivata, sellele õigusele enamasti pikemalt ei mõelda. Teema tuleb päevakorda siis, kui inimeste privaatsust on ohustatud ning inimesed on sellest rikkumisest teadlikuks saanud või inimene satub ebamugavustunnet tekitavasse olukorda. Kuna privaatsuse puhul on tegemist laia nähtusega, siis võivad inimesed privaatsust ja privaatsuse rikkumisi väga erinevalt tunnetada ja enda jaoks defineerida.

21. sajandil, mida iseloomustab internet ja tehnoloogia kiire areng, on informatsioon saanud infoühiskonna oluliseks osaks ning interneti laia levikuga on privaatsusest ja isikuandmete kaitsest üldisemalt saanud aktuaalne teema. Inimeste andmed on kolinud virtuaalsetesse keskkondadesse ning erinevad andmetega seonduvad toimingud salvestuvad pikaks ajaks ning andmed on kergemini kättesaadavad. Kompleksses infomaailmas on inimeste jaoks muutunud keeruliseks neid puudutava informatsiooni leviku kontrollimine ning isikliku informatsiooni kaitsmine (Tihanov, 2015).

Varasemaid uuringuid, mis käsitlevad privaatsust ja isiklikku informatsiooni, on palju (Smith, Smith ja Milberg, 1996; Lõhmus-Ein, 2004; Peeterson, 2012; Tamm, 2014), mis näitab taas, et teema on aktuaalne ja oluline. Oluliseks institutsiooniks inimese elus on ka tema töökoht. Veetes seal suure osa ajast ning tegutsedes tööandja kontrolli all, tõstatub tänapäeval privaatsuse küsimus aina enam ka töösuhetes. Näiteks on Eestis privaatsust ja isiklikku informatsiooni organisatsioonisisestes suhetes oma magistritöös uurinud Stina Tihanov (2015). Tulemustest selgus, et peamiselt seostasid uuritavad privaatsust isikliku informatsiooniga ning eraeluga, samuti väärtustati nii enda kui teiste inimeste privaatsust (Tihanov, 2015). Lisaks Tihanov'i magistritööle on privaatsuse käsitlust läbi õigusliku elemendi uurinud Karina Lõhmus-Ein (2004). Greete Kempel on kirjutanud oma magistritöö teemal „Sotsiaalmeedia töösuhtes: tööandjate hinnangud

ning kogemused“ (2014), milles ta on välja toonud asjaolu, et tööle kandideerimisel on populaarseks esmase taustakontrolli tegemise kohaks just sotsiaalmeedia.

Mitmetes uuringutes on jõutud järeldusele, et selleks, et minimaliseerida privaatsuse rikkumist, on vajalik kontrolli säilitamine isikliku informatsiooni üle (Murumaa-Mengel, Laas-Mikko ja Pruulmann-Vengerfeldt, 2014).

Minu lõputöö uurimisprobleemiks on küsimus, mil määral ja kuidas julgeolekuasutuse kõrgendatud tähelepanu all olek mõjutab uuritavate käitumisharjumusi sotsiaalmeedias ja milliseid muudatusi uuritavad oma sotsiaalmeedia käitumises sisse viivad. Laiemalt on minu lõputöö eesmärgiks selgitada ja mõista, kuidas defineerivad valimisse kuuluvad inimesed, kes on läbinud julgeolekukontrolli (N=7), privaatset ja avalikku informatsiooni ning kuidas mõjutas nende sotsiaalmeedia käitumist ja privaatsusharjumusi riigisaladusele juurdepääsuloa julgeolekukontrolli läbimine. Leian, et uuring on vajalik, kuna sellise kontrolli läbimine võib anda inimesele sisendi mõtlemaks privaatsuse ja avalikkuse teemale sügavamalt ning seeläbi on võimalik paremini mõista, millised hoiakud ja normid seonduvad isikliku info avaldamise ja sotsiaalmeediasuhtluses osalemisega. Teema aktuaalsust ilmestavad ka hiljuti ühiskonnalt negatiivse reaktsiooni saanud Kaitseväega seotud teemad, näiteks Tartu Ülikooli ajakirjandustudengite avastatud massiline andmeleke Kaitseväe dokumendiregistris (Loonde jt, 2018) ning ka Kaitseväe enda algatatud seadusemuudatus, et saada laiemad õigused isikutele taustakontrolli teostamiseks (Punamäe, 2019).

Käesolev töö on jätk 2019. aasta jaanuaris kaitstud samateemalisele seminaritööle, milles alustasin töö teoreetilis-empiirilise raamistuse kirjutamist ning töötasin välja uurimuses kasutatava uurimisinstrumendi (semistruktureeritud intervjuud) ja katsetasin analüüsiskeemi (kvalitatiivne sisuanalüüs). Lõputöö jaguneb neljaks peatükiks. Esimeses peatükis annan ülevaate teoreetilistest ja empiirilistest lähtekohtadest, mis aitavad töö tulemusi paremini mõista ja raamistada. Teises peatükis esitan uuringu valimistrateegia ning osalejate kirjelduse ja ülevaate kasutatud uurimismeetoditest. Kolmandas peatükis esitan kvalitatiivse uurimismeetodiga kogutud ja analüüsitud uurimistulemusi. Neljandas peatükis annan ülevaate järeldustest ning paigutan lõputöö tulemused laiemasse raamistikku ning seon eelnevalt teadaolevate akadeemiliste ning praktiliste töödega.

1 TEOREETILISED JA EMPIIRILISED LÄHTEKOHAD

Selles peatükis selgitan mõistet informatsiooniline privaatsus internetis, annan lühikese ülevaate sotsiaalsest järelevalvest sotsiaalmeedias ja Eesti Vabariigi õigusruumis kehtivatest andmekaitse regulatsioonidest. Samuti selgitan avalikele allikatele tuginedes riigisaladusele juurdepääsuloa taotlusprotsessi ning peamisi aspekte, millele julgeolekuasutus julgeolekukontrolli läbi viies tähelepanu pöörab.

1.1 Informatsiooniline privaatsus internetis

Viimastel aastakümnetel aset leidnud sotsiaalmeediakasutuse laia leviku ning üldisemalt erinevate *online*-teenuste ja -keskkondade arvu ja populaarsuse kasvades on hakatud järjest enam rääkima privaatsuse olulisusest (Vidili ja Artini, 2010: 17; Srinivasan, 2018). Selle põhjuseks võib pidada ühiskonda iseloomustavate andmete, sealhulgas inimeste isikliku informatsiooni põhjalikku kogumist ja talletamist, mis on omakorda seotud tehnoloogia ning säilitusvahendite hoogsa arengu ning laialdase kättesaadavusega (Sweeney, 2002).

Web 2.0 domineerimine, mille all peetakse reeglina silmas vahendatud online keskkondasid, mis võimaldavad kiiret suhtlus mitme osapoole vahel (Cormode ja Krishnamurthy, 2008), võimaldab kasutajatevahelist suhtlust üle kogu maailma ning annab kasutajatele võimaluse luua ja vahetada informatsiooni (Mitrou, Kandias, Stavrou ja Gritzalis, 2014; Vidili jt, 2010; Srinivasan, 2018). Veebisuhtluses osalemine võib aga kõrvaliste isikute jaoks olla väärtusliku isikliku informatsiooni allikaks, ka ilma informatsiooniallika enda teadmata või otsese nõusolekuta (Mitrou jt, 2014). Tulenevalt veebisuhtluse iseärasustest, paljastavad kasutajad enda kohta informatsiooni teadmatult laiemale ringile, isegi kui nad teadlikult suhtlevad konkreetse auditooriumiga (*ibid*). Siinkohal on oluline pöörata tähelepanu informatsioonilisele privaatsusele internetis.

Infoajastul on privaatsust käsitletud eelkõige kui teiste inimeste juurdepääsu takistamist erinevatele isiklikele kommunikatsioonivahenditele ning tegevustele internetis (Finn, Wright ja Friedewald, 2013). Samuti on privaatsust defineeritud kui inimese võimalust otsustada teda puudutavate asjaolude üle, kontrollida, kes pääseb ligi teda puudutavale informatsioonile ning luua erinevaid suhteid (Palm, 2009; Tavani, 2008). Tavani (2008: 139-140) toob välja ka neli põhjust, miks infotehnoloogia kiire areng on mõjutanud informatsioonilist privaatsust: kogutava ning andmebaasidesse talletatava informatsiooni hulk on kasvanud; informatsiooni vahetamise kiirus on kasvanud; andmete säilitamise võimalused on kasvanud; säilitusaeg on pikenenud ja omandatava teabe tüübid on muutunud.

Daniel J. Solove (2002) on välja toonud ka kuus privaatsuse aspekti: õigus olla rahule jäetud; piirata ligipääsu endale, võimalus end kaitsta soovimatu juurdepääsu eest; õigus teatud asju teiste eest varjata; omada kontrolli oma isikliku informatsiooni üle; oma isiksuse, sealhulgas väärikuse, individuaalsuse ja isiku kaitse ning õigus intiimsuse info kaitsele.

Nagu eeltoodud kirjeldustest näha, siis puudub privaatsuse defineerimisel ühtne, kokkulepitud lihtne ja kompaktne termin ja seletus. Inimeste privaatsuse defineerimine ja tunnetamine on erinev ning indiviidist sõltuv. Teisisõnu - indiviid määrab ise, millise osa tema isiklikust informatsioonist on liiga tundlik selleks, et seda teistega jagada.

1.2 Sotsiaalne järelevalve sotsiaalmeedias

Isikuandmetest, sealhulgas isikute enda poolt tahtlikult avaldatud andmetest, on tänapäeval saanud oluline valuuta, mis võimaldab erinevaid teenuseid kasutada ning osaleda meediasuhtluses. Üheks valuuta vahetuskohaks on erinevad sotsiaalmeediaplatvormid, mida järjest rohkem kasutatakse.

Sotsiaalmeedia kasutajate arv on viimasel aastakümnel plahvatuslikult kasvanud. Statista (2018) veebilehe andmetel oli näiteks Facebooki aktiivsete kasutajate arv 2008. aastal 100 miljonit, siis 2019. aastaks on aktiivsete kasutajate arv kasvanud 2,32 miljardini (Global social media…, 2019). Aktiivseteks kasutajateks loetakse neid kasutajaid, kes on oma kontole sisse loginud viimase 30 päeva jooksul (Number of monthly..., 2018). Ühtlasi on Facebook kõige populaarsem sotsiaalmeedia platvorm (*ibid*).

Hudsoni (2018) definitsiooni kohaselt tähistab mõiste sotsiaalmeedia veebilehti ja rakendusi, mille kaudu on reaalajas võimalik kiirelt sisu jagada ning sotsiaalmeedia pakutavaid võimalusi

kasutatakse edukalt ka ärilistel eesmärkidel. Kasutajad osalevad sotsiaalmeedias erinevatel põhjustel – näiteks meelelahutuslik eesmärk, suhtlemine või professionaalsete suhete arendamine (Mitrou jt, 2014). Sotsiaalmeedias sisu luues loob kasutaja ka uued infovood (*ibid*), kuid avalikustades „kommunikatsiooni subjektina" oma infot teistele, muutub kasutaja seeläbi „informatsiooni objektiks" ning „jälgimisobjektiks" (Fuchs, 2011; Mitrou jt, 2014 kaudu). „Jälgimisobjektiks" muutumist võib käsitleda ka kui sotsiaalses järelevalves osalemist.

Sotsiaalne järelvalve on kahtlemata lai mõiste, hõlmates endas palju erinevaid kontekste, kuid Alice Marwick'i (2012) definitsiooni kohaselt on sotsiaalne järelevalve pidev teiste inimeste kohta teabe kogumine. See hõlmab sotsiaalmeedia saitide kasutamist teabe levitamiseks kui ka teiste loodud sisu vaatamiseks ning võib toimuda konkreetsetel sotsiaalmeedia lehekülgedel (näiteks Facebook), mitmete lehekülgede üleselt üheaegselt (Marwick, 2012) või ka offline-keskkondades. Minu lõputöös tähistab sotsiaalne järelevalve spetsiifilisemalt indiviidide tegevuste ja sisuloome jälgimist Facebooki kontol erinevate nähtamatute laiendatud võrgustiku liikmete poolt.

Adam Joinson (2008) defineerib sotsiaalset järelevalvet kui indiviidi erinevate sotsiaalmeedia kontode (näiteks Facebook, Twitter) kasutamist eesmärgiga jälgida, millega sõbrad, tuttavad ja perekond tegelevad. Sotsiaalmeedias ja sotsiaalses järelevalves aktiivselt osalemine on seotud ka mõistega omnoptikon. Jeffrey Rosen (2004) kirjutab, et omnoptikon on midagi, mis käib kaasa uue meedia ajastuga ning mida võib käsitleda kui ühisvalvet – toimub pidev üksteise jälgimine, samal ajal teadmata, kes ja millal keda jälgib. Tihti inimesed isegi ei tea, millist informatsiooni nende kohta kogutakse, milleks seda informatsiooni kasutatakse või kas seda talletatakse erinevatesse andmebaasidesse (Vidili jt, 2010). Seda nimetatakse ka sotsiaalse järelevalve horisontaalseks vaateks, mis on omane sotsiaalmeediale – paljud jälgivad paljusid (*ibid*).

Rääkides omnoptikonist, siis seondub see mõiste ka teise omataolisega – panoptikon. Foucault defineerib seda mõistet tänapäeva ühiskonda silmas pidades kui et vähesed jälgivad paljusid (McCullagh, 2005). Seda nimetatakse sotsiaalse järelevalve vertikaalseks vaateks ning see on omane riigiasutustele, ettevõtlusele, kaitseväele jne (Vidili jt, 2010). Ka julgeolekukontrolli läbimist võib käsitleda panoptilise jälgimisena.

Ei tekita kahtlust, et sotsiaalmeedia kasutamine on jätkuvalt tõusev trend. Kõikide sotsiaalmeedias läbiviidud tegevustega jäädvustame me enda kohta tahtlikult või tahtmatult informatsiooni. Sotsiaalmeedias avaldatud teave pakub julgeolekuasutusele laialdase võimaluse andmete kogumiseks ning indiviidide panoptiliseks jälgimiseks, suurendades kindlasti ka informatsiooniga

manipuleerimise võimalusi. Nissen'i (2015) kohaselt pakub sotsiaalmeedia mitmeid erinevaid indiviidide analüüsivõimalusi. Näiteks toob ta välja võrgustikuanalüüsi, mis otsib vastuseid küsimusele kes kellega ja kui tihti räägib; meeleolude analüüsi mis vaatleb emotsioonide väljendamist mingi kindla teema suhtes ja käitumusliku analüüsi, mille eesmärk on kaardistada kasutaja veebilehtede külastused, sirvimine ja veebisuhtlus (Nissen, 2015). Indiviidide analüüs ei pea tingimata toimuma suurandmete läbitöötlemisel, ka konkreetse isiku digitaalse jälje teadlik käsitsi kontrollimine ja vaatlemine annab võimaluse inimese tegevuste, hinnangute jne analüüsimiseks.

Minu uurimistöö teemaga seonduvalt on siinkohal oluline jälgida ja meeles pidada, et sotsiaalmeedia võib julgeolekukontrolli läbimisel osutuda oluliseks mainekujundusplatvormiks.

1.3 Sotsiaalmeedia kasutuse reguleerimine Kaitseväes

Sotsiaalseid institutsioone nagu näiteks kaitsevägi on kirjeldatud "ahnete institutsioonidena", mis esitavad oma liikmetele laiaulatuslikke nõudmisi ja ootusi ning mõjutavad organisatsiooni liikmete erinevaid eluvaldkondi, nagu töö, perekond ja sotsiaalsed suhted väljaspool tööd (Coser, 1974). Kui sotsiaalsete suhete ühe osana silmas pidada osalemist sotsiaalmeediasuhtluses, siis Eesti Kaitsevägi reguleerib oma liikmete sotsiaalmeediakasutust 2011. aastal kehtima hakanud dokumendiga „Juhend kaitseväelaste osalemiseks sotsiaalmeedias". Sotsiaalmeedia kasutuse reguleerimine tuleneb otsesest vajadusest kaitsta organisatsiooni ja selle liikmeid. Püütakse tagada meedias kuvatava maine korrektsus ja vältida sellise informatsiooni avalikustamist, mis võiks soodustada rünnet nii asutuse vastu tervikuna kui ka asutuse liikmete osas. Sotsiaalmeedia pakub võimalust avalikuks ja varjatud teabekogumiseks ja *online*- tegevuste jälgimiseks, mistõttu on seda tegevust nimetatud ka sotsiaalmeedia luureks ehk SOCMINTiks (ingl Social Media Intelligence) (Nissen, 2015). Sotsiaalmeedia luure tähendab püüet kaardistada isikute sotsiaalseid suhteid ja võrgustikke, eesmärgiga välja selgitada kuidas isikud mõjutavad ühiskonda ja vastupidi (*ibid*).

Eesti kaitseväe sotsiaalmeedia juhend (Juhend kaitseväelaste osalemiseks…, 2011) sätestab üldsõnaliselt ära järgmised põhimõtted:

- Üldised põhimõtted – teenistuja on kaitseväe esindaja ka sotsiaalmeedias eraisikuna osaledes, ametialased käitumispõhimõtted kehtivad ka sotsiaalmeedias, internetti üle laetud info jääb sinna pikaks ajaks ning autor võib selle üle kontrolli kaotada, teabe

jagamisel tuleb alati meeles pidada, et info on tõlgendatav ning üle kantav Kaitseväele tervikuna ning keskkonna turvaseaded ei pruugi tagada privaatsust;

- Privaatsus ja isikuandmed – üles laetud andmete abil on võimalik isikut tuvastada, rakendada tuleb keskkonna pakutavaid turvaseadeid, keskkonda ei tohiks sisestada eraelulisi andmeid, näiteks isikukoodi ja andmeid teenistuskoha kohta, avaldatav teave ei tohi kahjustada teisi osapooli ning alati tuleb enne avalikustamist analüüsida teabe sobivust avalikku ruumi;

- Sotsiaal- ja traditsiooniline meedia – igasugust suhtlemist sotsiaalmeedias tuleb käsitleda kui suhtlemist avalikkusega, keelatud on anonüümselt jagada teavet kaitseväge puudutavatel teemadel, enda isiklik arvamus tuleb eristada tööandja omadest;

- Julgeolek – avaldatud teave võib olla väärtuslik kurjategijatele ja välisriikide luureteenistustele, suhelda tuleb nende isikutega, kelle isikusamasuses oled veendunud, avaldada ei tohi tundlikku teavet;

- Arvutiturvalisus – tuleb järgida üldtunnustatud internetiturvalisuse põhimõtteid ning kaitseväe infotehnoloogia eeskirja;

- Tegutsemine probleemide korral – koheselt tuleb teavitada võimalikest rünnetest ja rikkumistest nii enda kui teiste teenistujate suhtes.

On tõenäoline, et indiviidide käitumisharjumused sotsiaalmeedias muutuvad ja jäävad püsima ka peale seda, kui nad on organisatsiooniga töösuhte lõpetanud. Tegemist võib olla hoiakute kujunemisega tänu pikaajalisele organisatsioonipoolsele mõjutamisele. Kaitseväe teenistujate hoiakute kujundamist võib kirjeldada näiteks Lewin'i muudatuste juhtimise kolmeastmelise teooriaga. Nö „jääkuubiku mudeli" eesmärk on kolmeastmeliselt kirjeldada indiviidide hoiakuid kujundavaid tegureid ühiskonnas ja organisatsioonis (Wirth, 2004).

Lewini (Wirth, 2004) muutuste teooria kohaselt toimub muutuste läbiviimine kolme etapina:

a) Lahtisulatamine, mille käigus tekib motivatsioon muudatuste läbiviimiseks;

b) Muutuste läbiviimine, kus tegeletakse muutuste ulatuse ning tegevuste määratlemise ning konkretiseerimisega;

c) Kinnikülmutamine, kus muutunud käitumine kinnistatakse harjumuspäraseks.

Kuna Kaitsevägi eeldab oma teenistujatelt erinevate eeskirjade, sh sotsiaalmeediajuhendi, kõrvalekaldumatut järgmist, siis on tõenäoline, et organisatsiooni liikmete hoiakud kinnistuvad ning nad rakendavad neid ka suure tõenäosusega eraelus.

1.4 Isikuandmete kaitse põhimõtted Eesti Vabariigis

Eesti õigusruumis reguleeris kuni 2018. aastani isikuandmete kaitset „Isikuandmete kaitse seadus“. 2016. aasta 14. aprillil kiitis Euroopa Parlament heaks isikuandmete kaitse üldmääruse, millega asendati seni kehtinud andmekaitsedirektiiv (Andmekaitse…, 2018). Tegemist on otsekohalduva määrusega, mis koos siseriiklike rakendusaktidega hakkas asendama seni kehtivat Eesti isikuandmete kaitse seadust (*ibid*). Määrus jõustus 24.05.2016.a ja seda hakati Eestis kohaldama alates 2018. aasta 25. maist. (Andmekaitse…, 2018) Uue määruse eesmärgiks on kodanikele anda parem kontroll oma andmete üle, arvestades seda, et hüppeliselt on kasvanud sotsiaalmeedia, nutitelefonide ning interneti kasutus (*ibid*). Senised õigusaktid pärinesid ajast, mil netiteenused olid palju algelisemad.

Isikuandmete definitsioon tuleneb isikuandmete kaitse üldmääruse (2016) artiklist 4, mille kohaselt isikuandmed on mis tahes teave tuvastatud või tuvastatava füüsilise isiku kohta, sõltumata sellest, millisel kujul või millises vormis need andmed on ja millega saab isikut otse või kaude tuvastada: nimi, isikukood, asukohateave, võrguidentifikaatorid (tunnused, mis sidevõrgus aitavad viia konkreetse isikuni), samuti füüsilised, geneetilised, vaimsed, majanduslikud, kultuurilised ja mistahes muud tuvastamist võimaldavad tunnused ja nende kombinatsioonid. Sarnase definitsiooni andis ka isikuandmete kaitse seaduse (2016) paragrahv 4. Eraldi defineeritakse veel eri liiki isikuandmed, mis on andmed, millest ilmneb rassiline või etniline päritolu, poliitilised vaated, usulised või filosoofilised veendumused või ametiühingusse kuulumine, geneetilised andmed, isiku kordumatuks tuvastamiseks kasutatavad biomeetrilised andmed, terviseandmed ja andmeid seksuaalelu ja seksuaalse sättumuse kohta (Isikuandmete kaitse üldmäärus, 2016).

Isikuandmete töötlemisena defineeritakse iga isikuandmetega tehtav toiming sõltumata selle teostamise viisist ja kasutatavatest vahenditest (Isikuandmete kaitse üldmäärus, 2016). Näiteks nende kogumine, salvestamine, korrastamine, säilitamine, muutmine ja avalikustamine, juurdepääsu võimaldamine, päringute teostamine ja väljavõtete tegemine, kasutamine,

edastamine, ristkasutamine, ühendamine, sulgemine, kustutamine, hävitamine või mitu eelnimetatud toimingut (*ibid*) .

Isikuandmete kaitse üldmääruse (2016) artikkel 5 määratleb isikuandmete töötlemise põhimõtted, mida ollakse kohustatud järgima alljärgnevalt:

1) seaduslikkus – igasuguseks isikuandmete töötlemiseks peab olema alus;

2) eesmärgipärasus – määratle eesmärk, milleks andmeid vajad. Samade andmete muu eesmärgil töötlemiseks peab olema teine alus;

3) minimaalsus – tuleneb eesmärgist: ära kogu rohkem andmeid kui eesmärgi saavutamiseks vaja on;

4) õigsus ehk andmekvaliteet – tuleneb samuti eesmärgist: andmed olgu eesmärgi saavutamiseks asja- ja ajakohased;

5) säilitamistähtaeg – eesmärgist tuleneb ka säilitamistähtaeg;

6) turvalisus – hoia ja töötle andmeid turvaliselt,

7) vastutus ja läbipaistvus – andmetöötleja vastutab nende põhimõtete järgimise eest ning peab olema andmesubjekti jaoks läbipaistev (andma teavet, võimaldama tutvuda ja nõudeid esitada).

Isikuandmete töötlemine on tihedalt seotud õigusega privaatsusele, seega on oluline määratleda privaatne informatsioon ning tagada selle igakülgne kaitse ka siis, kui see ei tulene otseselt õigusaktidest.

1.5 Riigisaladusele juurdepääsuloa taotlemine

Minu uurimistöö eesmärk on välja selgitada, mil määral muudab julgeolekuasutuse kõrgendatud tähelepanu all olek indiviidi sotsiaalmeediakasutuse harjumusi, seda just indiviidi enda poolt tajutud muudatustena. Julgeolekuasutuse kõrgendatud tähelepanu all olek tähendab käesoleva uurimistöö kontekstis riigisaladusele juurdepääsuloa taotlusprotsessis osalemist – vajalike andmete esitamist Kaitsepolitseiametile, nõusoleku andmist täiendavaks isikuandmete kontrolliks ning julgeolekukontrolli vestluse läbimist.

Selles alapeatükis selgitan, mis on riigisaladus, millistele õigusaktidele tuginedes läbitakse riigisaladuse juurdepääsuloa taotlusprotsess ja väljastatakse luba ning millistele isiklikele andmetele pööratakse suuremat tähelepanu.

Riigisaladus on teave, mille avalikuks tulek seab ohtu Eesti Vabariigi julgeoleku või kahjustab välissuhtlust ning vajab seetõttu kaitset avalikuks tulemise eest (Riigisaladuse ja salastatud ..., 2018). Riigisaladusele juurdepääsuõigust defineerib Riigisaladuse ja salastatud välisteabe seadus (2018) kui isiku õigust töödelda riigisaladust või salastatud välisteavet ametikohajärgselt või asutuse juhi otsuse, juurdepääsuloa- või sertifikaadi, tunnistajakaitse kaitseabinõude kohaldamise või uurimisasutuse, prokuratuuri või kohtu määruse alusel. Riigisaladusele juurdepääsuõigus antakse tähtajaliselt ning juurdepääsuõigus konfidentsiaalsele, salajasele ja täiesti salajasele teabele on vastava tase riigisaladuse juurdepääsuluba omaval isikul. (*ibid*) Riigisaladusele juurdepääsuluba on dokument, mis tõestab füüsilise isiku juurdepääsuõigust vastava taseme riigisaladusele (Riigisaladuse ja salastatud ..., 2018).

Riigisaladusele juurdepääsuloa taotlusprotsessi algatamiseks või juurdepääsuloa kehtivuse pikendamiseks täidab taotleja põhjaliku julgeolekukontrolli ankeedi ja annab julgeolekuasutusele (Kaitsepolitseiamet või Välisluureamet) oma allkirjaga loa põhjalikuks julgeolekukontrolliks (Riigisaladuse ja salastatud ..., 2018). Julgeolekukontrolli käigus kontrollib julgeolekukontrolli teostav asutus, kas isik vastab riigisaladusele juurdepääsuloa väljastamise tingimustele või mitte (*ibid*). Julgeolekukontrolli ei teostata nende isikute suhtes, kellel on riigisaladusele juurdepääsuõigus ametikohajärgselt, näiteks Vabariigi President (Riigisaladuse ja salastatud ..., 2018).

Kaitseväes toimub riigisaladusele juurdepääsuõiguse andmine kas asutuse juhi otsuse alusel (üksnes piiratud tasemel riigisaladusele juurdepääs) või riigisaladusele juurdepääsu loa tingimistega ametikohale nimetamisel.

Asutuse juhi, ehk kaitseväe juhataja otsusel antakse piiratud tasemel riigisaladusele juurdepääs isikule, kes on nimetatud ametikohale, mis eeldab juurdepääsu üksnes piiratud tasemel riigisaladusele (Riigisaladuse ja salastatud…, 2018). Isiku nimetamisel üksnes piiratud tasemel riigisaladusele juurdepääsuõigusega ametikohale, võetakse isikult nõusolek tema isikuandmete kogumiseks ja kinnitus riigisaladuse kaitse nõuete tutvustamiseks, kuid reeglina ei teostata isiku suhtes julgeolekukontrolli (*ibid*). Isiku suhtes kahtluse tekkimisel taotleb Kaitsevägi julgeolekuasutuselt julgeolekukontrolli läbiviimist, mille käigus tuvastatakse riigisaladusele

juurdepääsuloa andmise keeldumise asjaolud ning seejärel otsustab Kaitsevägi isiku teenistusest vabastamise, ülesannete muutmise või teisele ametikohale üleviimise (Riigisaladuse ja salastatud…, 2018).

Riigisaladuse ja salastatud välisteabe seaduse (2018) § 20 lg 5 kohustab riigisaladust valdava asutuse, sealhulgas Kaitseväe, määrama ametikohad, millel töötamise eeltingimusteks on riigisaladusele juurdepääsuõiguse omamine. Ametikohad määratakse eraldi koosseisutabelis ning iga ametikoha juurde märgitakse ka ametikohal nõutav riigisaladusele juurdepääsu õiguse tase (*ibid*). Koosseisutabelist nähtub, millisel ametikohal on nõutav riigisaladusele juurdepääsuluba ning ametikoha täitmisel sellest ka lähtutakse ning algatatakse julgeolekukontroll. Juurdepääsuloa saamiseks edastatakse Kaitseväe poolt julgeolekuasutusele taotlus, millele lisatakse juurdepääsuloa toetaja (Kaitseväe) poolne põhjendus teenistuja riigisaladusele juurdepääsuvajadusele, juurdepääsuloa taotleja ankeet, taotleja kirjalik nõusolek isikuandmete kogumiseks ning kinnitus riigisaladuse nõuete tutvustamisest (Riigisaladuse ja salastatud…, 2018).

Riigisaladusele juurdepääsuloa taotleja peab ankeedis esitama põhjalikud andmed näiteks järgmiste isiklike andmete kohta: perekondlikud- ja tutvussidemed, sh lähimad tuttavad; telefoni- või kõnekaardi number, elektroonilises seadmes kasutatava SIM-kaardi number; kõigi elektrooniliste suhtlusvõrgustike, kõne- ja sõnumirakenduste nimetused, kasutajanimed ja muud identifitseerivad tunnused; kontaktid välisriikidega; tervise ja eluviisiga seotud andmed ning varalised kohustused, sissetulekud ja pangakonto numbrid (Füüsilise isiku…, p.a). Riigisaladusele juurdepääsuloa taotleja/pikendaja ankeedis küsitud andmete täpsem loetelu asub töö lisades (Lisa 1).

Riigisaladusele juurdepääsuloa taotleja omakäelise kirjaliku nõusoleku alusel saab Kaitsepolitseiamet laialdased võimalused isikule julgeolekukontrolli teostamiseks, sooritades isiku kohta päringuid füüsilistele ja juriidilistele isikutele (Riigisaladuse ja salastatud ..., 2008). Julgeolekuasutuste seaduse (2017) alusel on julgeolekukontrolli teostaval asutusel tasuta juurdepääs erinevatele andmekogudele. Julgeolekuasutuste seaduses sätestatakse ka, et oma ülesannete täitmisel ei tohi asutus piirata üksikisiku õigusi ülemääraselt ning teabe kogumine ei tohi kahjustada isiku elu, tervist, vara ega keskkonda (Julgeolekuasutuste seadus, 2017). Julgeolekukontrolli teostamisega selgitatakse välja, kas taotleja suhtes ei esine riigisaladusele juurdepääsuloa andmiseks või kehtivuse pikendamiseks keeldumise aluseid, näiteks ei anta riigisaladusele juurdepääsuluba isikule, kellel on uimasti- või hasartmängusõltuvus või kelle puhul

tuvastatakse koostöö välisriigi luure- või julgeolekuteenistusega (Riigisaladuse ja salastatud..., 2008).

Julgeolekukontrollile järgneb üldjuhul vestlus julgeolekukontrolli läbijaga (Riigisaladuse ja salastatud ..., 2018). Vestluse käigus täpsustatakse ning kontrollitakse isiku poolt esitatud ning julgeolekukontrolli käigus kogutud teavet (*ibid*). Peale julgeolekukontrolli vestluse läbimist vaatab taotleja informatsiooni täiendavalt üle vastav komisjon ning otsustab riigisaladusele juurdepääsuloa väljastamise või keeldumise (Riigisaladuse ja salastatud …, 2018).

Eeltoodust nähtub, et julgeolekuasutustel on laiad volitused sekkumaks isiku põhiõigustesse, näiteks sõnumisaladusse, eesmärgiga tagada riiklik julgeolek. Küll aga peab isiku põhiõiguste piiramine olema proportsionaalne eesmärgiga ning siinkohal on tasakaalu leidmine isiku põhiõiguste ja riikliku julgeoleku vahel keeruline. Oluline on välja tuua ka asjaolu, et vastavalt Riigisaladuse ja salastatud välisteabe seaduse (2018) § 47 lõikele 3 on julgeolekuasutusel õigus kontrollida isiku vastavust riigisaladusele juurdepääsuloa vastavuse nõuetele nii juurdepääsuloa kehtivuse ajal kui ka viie aasta jooksul peale loa kehtivuse lõppemist, seega on alati võimalus, et isiku põhiõiguste riive ei toimu ainult julgeolekukontrolli teostamise ajal.

1.6 Uurimisküsimused

Uurimistöö eesmärk on selgitada välja, mil määral muudab julgeolekuasutuse kõrgendatud tähelepanu all olemine indiviidi käitumist ja kasutatavaid turvaseadeid sotsiaalmeedias, seda eelkõige indiviidi enda poolt tajutud muutustena. Täpsemalt otsin käesolevas töös vastuseid järgmistele uurimisküsimustele:

1. Kuidas defineerivad julgeolekuasutuse kõrgendatud tähelepanu all olnud inimesed privaatset ja avalikku informatsiooni?

2. Millised on uuringus osalejate üldised hoiakud tavapärasest põhjalikuma julgeolekukontrolli teostamisesse?

3. Millised on peamised intervjueeritavate poolt tajutud muutused nende sotsiaalmeediakäitumises julgeolekukontrolli teostamise järgselt?

2 MEETOD JA VALIM

Järgnevates alapeatükkides annan ülevaate sellest, kuidas ja millise strateegiaga lähenesin valimi moodustamisele, samuti annan ülevaate kasutatud andmekogumis- ja andmeanalüüsi meetoditest.

2.1 Valim

Lõputöö valimi moodustasin isikutest, kes ei ole käesolevaks hetkeks enam kaitseväes teenistuses. Intervjueeritavate leidmisel kasutasin sihipärast valimit ja valisin seega uuritavad ettekavatsetult ning kindlate kriteeriumite alusel (Õunapuu, 2014).

Intervjueeritavad pidid vastama järgnevatele kriteeriumitele:

- uuritavad peavad olema läbinud riigisaladusele juurdepääsuloa taotlusprotsessi
- neil pidi olema aktiivselt kasutatav konto sotsiaalmeedias enne ning pärast riigisaladusele juurdepääsuloa taotlusprotsessi läbimist
- eetilistel- ja turvakaalutlustel lisasin täiendavaks kriteeriumiks asjaolu, et uuritavad ei tööta uuringu läbiviimise hetkeks enam riigisaladusele juurdepääsuloa olemasolu nõudval ametikohal. Lisaks võimaldab teatud ajaline distants kõnelda tundlikest teemadest vabamalt ning võib aidata kaasa siiramate vastuste ja kirjelduste saamisele.

Kõikide uuritavatega oman varasemat tööalast kokkupuudet Eesti Kaitseväes, seetõttu on tegemist osaliselt ka mugavusvalimiga. Mugavusvalimisse kaasatakse uuritavaid, kes kuuluvad uurija lähemasse tutvusringi ning keda on lihtne uurimusse saada (Rämmer, 2014). Mugavusvalimi kasutamine esimeses teadustöös tundus minu kui algaja uurija puhul mõistlik, kuna võimaldas mul arendada oma intervjueerimisoskusi pisut vähemate tundmatute teguritega olukorras.

Selle töö jaoks intervjueerisin seitset varasema julgeolekukontrolli kogemusega endist Kaitseväe teenistujat. Intervjueeritavatega kontakteerusin kohtumise kokku leppimiseks e-kirja teel. Uuringus osalemine oli täiesti vabatahtlik ning kõigile uuringus osalejatele selgitasin lõputöö eesmärke. Intervjuud viisin läbi eelnevalt ettevalmistatud kava (Lisa 2: Intervjuu kava) alusel.

Lõputöö jaoks andmete kogumiseks viisin individuaalintervjuud läbi märtsis ja aprillis 2019. a. Tegemist on valimiga, mille tunnused on teatud osas homogeensed (sarnased) ja teatud osas heterogeensed (erinevad). Valimi olulisemateks homogeenseteks tunnusteks on see, et tegemist on isikutega, kes kõik on läbinud korduva julgeolekukontrolli riigisaladusele juurdepääsuloa saamiseks ning on omanud aktiivset kontot sotsiaalmeedias enne ja pärast julgeolekukontrolli teostamist. Heterogeenseteks tunnusteks on intervjueeritavate sugu ja vanus (vanusevahemikus 33-45). Alljärgnevalt toon välja valimisse kuuluvate uuringus osalenud intervjueeritavate lühikirjelduse.

Tabel 1. Intervjueeritavate lühikirjeldus

Tähis	Sugu	Julgeolekukontrollide läbimise aeg	Olemasolevad sotsiaalmeedia kontod	Sotsiaalmeedia kasutamise aeg
INT1	N	2007, 2012, 2017	Facebook, Instagram	Rohkem kui 15 aastat
INT2	N	2006, 2011, 2016	Facebook, Instagram	Üle 10 aasta
INT3	M	2009, 2014	Facebook, Instagram	Rohkem kui 15 aastat
INT4	N	2007, 2012, 2017	Facebook, Instagram	Üle 10 aasta
INT5	M	2008, 2013, 2018	Facebook	Rohkem kui 15 aastat
INT6	N	2006, 2011, 2016	Facebook, Instagram	Üle 10 aasta
INT7	N	2009, 2014, 2019	Facebook	Rohkem kui 15 aastat

Intervjueeritavad olen tähistanud koodidega INT1, INT2, INT3, INT4, INT5, INT6 ja INT7 vastavalt vestluse järjekorrale. Intervjueeritavate anonüümsuse tagamiseks ei kasuta ma oma

teadustöö tekstis intervjueeritavate vanuseid ega muid identifitseerimist võimaldavaid kirjeldusi ega fakte.

2.2 Andmekogumismeetod

Lõputöös kasutasin andmete kogumiseks kvalitatiivse uurimismeetodina silmast silma läbiviidavaid semistruktureeritud individuaalintervjuusid. Selle meetodi valikul lähtusin lõputöö delikaatsest teemast, mis keskendub inimeste ootuste, tunnete ja käitumise uurimisele. Intervjuu võimaldab uurida delikaatseid ja tundlikke teemasid, milleni üldjuhul ei ole võimalik jõuda vaatluse või küsimustiku abil (Õunapuu, 2014). Semistruktureeritud intervjuud kasutades on intervjueerijal võimalik saadud vastuste sisust tulenevalt muuta teemade järjekorda ning esitada täiendavaid lisaküsimusi, täpsustada vastuseid ning muuta vajadusel teemade järjekorda (Hirsjärvi, Remes ja Sajavaara, 2010). Sõltuvalt intervjueerijast ning ka intervjueeritava avatusest on seeläbi võimalik kätte saada võimalikult palju olulist ja indiviidist olenevalt, pisut erinevate fookuspunktidega informatsiooni.

Andmete kogumiseks koostasin intervjuu kava (lisa 2) lähtuvalt uurimisküsimustest. Kava sisaldab nelja alateemat.

Esimese alateema moodustasid küsimused intervjueeritava sotsiaalmeedia kontode ja nende kasutusharjumuste kohta, eesmärgiga saada teada, milliseid kontosid intervjueeritav kasutab ning millist informatsiooni ta sotsiaalmeedias tavapäraselt jagab. Teises alateemas palusin intervjueeritaval selgitada privaatsusega seotud mõisteid ning täpsustada oma sotsiaalmeedia kontode ja postituste turvavõtteid. Kolmandas alateemas olid küsimused, mis puudutavad intervjueeritava julgeolekukontrolli läbimist, sellega kaasnevaid teadmisi ja tundeid. Neljandas alateemaplokis olid täpsustavad küsimused muudatuste kohta, mida intervjueeritavad tajusid või rakendasid oma sotsiaalmeediakäitumises julgeolekukontrolli läbimise järgselt. Intervjuu lõpus andsin intervjueeritavatele täiendavalt võimaluse lisada oma mõtteid seoses antud teemaga ning reeglina intervjueeritavad seda võimalust ka kasutasid.

Intervjuude keskmine kestus oli 45 minutit, kõige lühem intervjuu kestis 38 minutit, kõige pikem intervjuu kestis 1,5 tundi. Intervjuude pikkust mõjutasid ühe asjaoluna minu kui algaja uurija oskused intervjuud läbi viia, näiteks küsida jätkuküsimusi, aktiivselt kuulata ja vajadusel haarata kinni intervjueeritava poolt välja öeldust. Teiseks oli tegemist ühele konkreetsele aspektile fokuseeritud intervjuuga ning seetõttu üritasin hoida teemat fokusseerituna ning mitte minna liiga

laialivalguvaks. Intervjuud lindistasin diktofoniga ning dokumenteerisin transkribeerimise teel. Intervjuude algul tutvustasin kõigile osalistele uurimistöö teemat ning palusin intervjueeritavatelt suulise nõusoleku osalemiseks, intervjuude transkribeerimiseks ning andmete kasutamiseks uurimuse kontekstis. Sõlmisime ka kokkuleppe, mille kohaselt oli intervjueeritavatel õigus küsimustele mitte vastata, kui need tunduvad neile ebamugavust tekitavad. Transkriptsioonidest eemaldasin kõik nimed ning vastaja isikule otseselt viitava informatsiooni.

Intervjuudest esile kerkinud isikuandmete kaitsega seonduvatele probleemsematele teemadele olen hilisema ekspertintervjuu käigus palunud kommentaare ja selgitusi diplomeeritud andmekaitsespetsialistilt, kes tegutseb aktiivselt andmekaitse valdkonnas. Ekspertintervjuu tähendab intervjuud, kus vastajaks on mingi valdkonna asjatundja ehk ekspert ning küsimused puudutavad tema spetsiifilisi süvateadmisi mingist valdkonnast (Kelt, 2009). Intervjuu viisin läbi 20. mail 2019. aastal, et suudaksin oma uuringu esimese etapi tulemusi sügavamalt mõtestada. Andmekaitsespetsialisti kommentaarid on lisatud tulemuste peatükki vastava teemakäsitluse juurde eristatavas kirjas.

2.3 Andmeanalüüsi meetod

Andmeanalüüsiga alustamiseks transkribeerisin kõik intervjuud. Saadud andmete analüüsiks kasutasin kvalitatiivset sisuanalüüsi ja teemapõhist kodeerimist. Teemapõhise kodeerimise puhul koondatakse sarnase tähendusega tekstiosad, mis sisaldavad nii selgelt välja öeldud kui ka mõista antud sõnumeid, vastavate kategooriate alla (Laherand, 2008: 290).

Lugesin transkribeeringud mitu korda läbi ning otsisin lõputöö eesmärgist ja püstitatud uurimisküsimustest lähtudes tähtsamad märksõnad ja mõtted, tekitades seeläbi koodid ja koondasin koodid omakorda laiematesse kategooriatesse (Laherand, 2008: 285, 286).

Kodeerimisel otsisin tekstiosasid, mis seostuksid uurimisküsimuste teemadega. Seejärel tuletasin nende tekstiosade põhjal kategooriad, mida analüüsisin uurimisküsimuste teemade lõikes. Keskendusin teemadele nagu näiteks peamised põhjused sotsiaalmeedia kasutamisel, privaatse ja isikliku informatsiooni defineerimine, suhtumine julgeolekukontrolli ja käitumuslikud muudatused sotsiaalmeedia kasutuses peale julgeolekukontrolli läbimist.

Samuti kasutasin intervjuude analüüsimisel juhtumiülest ehk horisontaalanalüüsi (*cross-case analysis*), mille puhul kõrvutasin saadud vastused erinevate vastajate lõikes, et leida nii ühiseid

kui ka erinevaid jooni (Kalmus, 2015). Intervjuude käigus saadud andmete läbitöötamisel ja tõlgendamisel keskendusin tõlgendustele ja tähendustele, mida uuringus osalejad intervjuu käigus väljendasid (Laherand, 2008) ehk peamiselt manifestsele sisule.

3 TULEMUSED

Selles peatükis annan ülevaate uuringu tulemustest, mis jagunevad neljaks osaks. Kõigepealt kirjeldan, milliseid sotsiaalmeedia platvorme uuringus osalejad kasutavad ja milline on nende tavapärane sotsiaalmeediakasutus. Seejärel kirjeldan uuritavate arvamust privaatsusest, isiklikest ja avalikest andmetest. Kolmandas alapeatükis kirjeldan uuringus osalejate suhtumist julgeolekukontrolli teostamisesse, nende andmete kogumisse ja talletamisse tööandja ja julgeolekuasutuse poolt ning nende jälgimisse sotsiaalmeedias. Neljandas alapeapeatükis kirjeldan, kuidas hindavad uuringus osalejad Kaitseväe siseregulatsioonide ja julgeolekukontrolli läbimise rolli sotsiaalmeedia käitumisharjumuste kujunemisel ning millise hinnangu annavad uuringus osalejad endiste kolleegide sotsiaalmeediakäitumisele. Oma väidete ja analüütiliste üldistuste juurde olen toonud tsitaadid intervjuudest.

3.1 Uuringus osalejate tavapärane sotsiaalmeediakasutus

Uuringu valimi koostamise üheks kehtestasin, et uuringus osalejatel pidi aktiivne konto sotsiaalmeedias enne ja pärast julgeolekukontrolli teostamist. Intervjuudest selgus, et kõik osalejad on olnud pikaajalised sotsiaalmeedia kasutajad, kümme aastat ja rohkem. Uuringu kontekstis on pikaajaline sotsiaalmeediakasutus relevantne, kuna julgeolekukontrolli teostatakse üldjuhul iga viie aasta järel, seega on kõik uuringus osalejad läbinud julgeolekukontrolli korduvalt.

Hetkel on kõik uuringus osalejad aktiivsed Facebooki kasutajad. Varasemalt kasutatud sotsiaalmeedia platvormidest toodi välja veel Orkut, Rate, MySpace ja Instagram. Osadel uuringus osalejatel on hetkel aktiivne ka Instagrami konto, kuid selle kasutusaktiivsus on pigem juhuslik.

Kõik uuringus osalejad kirjeldavad oma sotsiaalmeediakasutust eelkõige ajaviitetegevusena. Facebooki külastatakse hommikuti kohvijoomise kõrvale, tööl või üldiselt juhuslike pauside ajal

ning õhtul enne magamajäämist, ühe uuringus osaleja puhul ka tööle ja töölt kojusõitmise ajal bussis.

Ühe ühise asjana toodi välja sotsiaalmeedia kasutamine päevakajaliste uudistega kursis olemiseks. Toodi välja ka Messengeri kasutamine peamise suhtlusvahendina helistamise asemel, tuues põhjuseks Messengeri kasutusmugavuse ning kättesaadavuse.

Väikese ühisosana sotsiaalmeedia kasutusest toodi välja loosimistes ja jagamismängudes osalemine ning aeg-ajalt ühiskonna teadlikkust suurendava informatsiooni jagamine:

> *INT7: Mingeid mänge jagan, ja siis pigem mingeid sellised a'la ära viska prügi maha, ära kasuta telefoni autoroolis, selliseid laiemale üldsusele suunatud asju.*

Ükski uuringus osaleja ei kasuta enda sõnul sotsiaalmeedia kontot selleks, et enda kohta eraelulist informatsiooni jagada. Pigem kirjeldatakse sotsiaalmeediat kui kiiret ja mugavat infovahetuse kohta, kus ise ollakse enamasti jälgija rollis.

Kokkuvõtvalt võiks öelda, et uuringus osalejad kasutavad sotsiaalmeediat igapäevaselt, kuid jagatakse enamasti teiste poolt juba avalikustatud informatsiooni. Enda andmete jagamise juures jäädakse tagasihoidlikuks ning enda loodud informatsiooni avalikustamine on muutunud aja jooksul tagasihoidlikumaks. Peamine sotsiaalmeediakasutus seisneb ajaviitetegevusena teiste loodud sisu jälgimises.

3.2 Privaatse ja avaliku info eristamine

Uuringu seisukohalt oli oluline ka välja selgitada, kuidas defineerivad uuringus osalejad privaatsust, isiklikke ja avalikke andmeid. Kõik uuringus osalejad seostasid privaatsust isikliku ja eraelulise informatsiooniga, samuti peeti oluliseks kõrvaliste isikute juurdepääsu piiramist isiklikule informatsioonile. Osalejad leidsid, et privaatsus on seotud võimalusega ise otsustada, kui palju ja millist isiklikku informatsiooni enda kohta jagatakse ning oluliseks peeti ka kontrolli omamist oma jagatava info üle.

Privaatseteks andmeteks pidasid uuringus osalejad täpsemaid andmeid oma perekonna ja laste kohta, lisaks peeti privaatseteks andmeid tervise- ja majandusliku olukorra kohta, isiklikke vestlusi ja e-kirju, ja ka oluliste teiste (eelkõige perekond) kohta käivat infot, mida soovitakse kõrvaliste

isikute eest varjata. Leiti ka, et on andmeid, mis ei ole vaja küll otseselt varjata, näiteks perekonnaseisu, kuid leiti et sellist informatsiooni ei peaks valimatult avalikustama.

> *INT4: Jah, ma ei pea vajalikuks varjata oma perekonnaseisu või lapsi, aga seda pole vaja ka otseselt reklaamida, kes teab, see teab.*

Mitmel korral mainiti kriitiliselt ära ka laste fotode avalikustamine, seda siis nii üleüldiselt kui ka alastipiltidele või lihtsalt piinlikele fotodele viidates. Kuigi mitmed uuringus osalejad olid ise varasemalt oma sotsiaalmeedia kontol laste fotosid avalikustanud, siis käesolevaks ajaks on nad fotod eemaldanud.

> *INT1: Oma laste alastipilte ei jagaks. Praegu võib küll nunnu või naljakas olla, aga ise ju küll ei tahaks et keegi sinu alasti titepilte kunagi avalikust netist leiaks. Jumal teab kui valedesse kätesse sellised pildid võivad jõuda.*

Lisaks arvasid uuringus osalejad, et mõtlematult ei peaks avaldama oma personaalseid kontaktandmeid (silmas peeti eelkõige mobiiltelefoni numbrit, meiliaadressi ja koduaadressi) ja täpsemat informatsiooni töökoha kohta.

Ühe aspektina toodi välja ka avalikel üritustel tehtud meediakajastused fotode näol. Intervjueeritav leidis, et kuigi avalikul üritusel, näiteks Ööjooksul osalemine ei ole otseselt delikaatne, siis ta ei soovi, et tema nimega sooritatud infootsing leiaks temast pilte avalikul üritusel osalemisest ning seetõttu peaks selliselt avalikustatud info olema eelnevalt isikuga kooskõlastatud.

Andmekaitsespetsialisti kommentaar: Üldjuhul lubavad regulatsioonid avalikus kohas ja avalikke üritusi filmida ning pildistada, kui seda tehakse avalikustamise eesmärgil. Samuti ei kehti teavitamiskohustus jäädvustamiste osa, mida võib mõistlikult eeldada. Eelpool loetletud rahvaspordiüritused käivad just sellesse kategooriasse. Kas just foto seostamine nimega on vajalik ning käib eeltoodud sätte alla… ? Teisalt on inimesel võimalik alati põhjendatud juhul pöörduda nii kodumaiste, kui ka välismaiste teenusepakkujate poole taotlusega lõpetada tema isikuandmete töötlemine ja foto eemaldada.

Uuringus osalejad pidasid oluliseks ka privaatsust sotsiaalmeedias ning selgitasid, et nende sotsiaalmeedia kontod ei ole laiemale üldsusele avalikud ning jagatav info on mõeldud sõbralistile. Üldiselt leidsid uuringus osalejad, et nende sotsiaalmeedia kontod on väga lakoonilised ning

võõras inimene ei tohiks sealt leida või kätte saada informatsiooni, mida konto kasutaja ise privaatseks on määranud.

> *INT4: ...kõik Messengeri vestlused peaks olema privaatsed. Üldse sellised tegevused või informatsioon, mida ma teen varjatult, mida ma ei jaga avalikul seinal näiteks.*

Enda postituste kaitsmist pidasid uuringus osalejad oluliseks ning kasutasid selleks üksteisega sarnaseid võtteid: enesetsensuuri kasutamine, sõbralisti piiramine, puhastamine ning sõbrakutsete kaalutletud aktsepteerimine. Toodi välja ka *tag*'imisvõimaluse eemaldamist ning vajadusel konkreetsete postituste seadete muutmist selliselt, et sellele saavad ligipääsu vaid valitud sõbralisti liikmed. Enesetsensuuri rakendades vaatavad uuritavad aeg-ajalt üle ka oma sotsiaalmeedia kontod ja vanemad postitused, et seal poleks sisu, mida teised võiks mitmeti tõlgendada.

Selgus ka, et kaks intervjueeritavat kasutavad oma privaatsuse kaitsmiseks sotsiaalmeedias erinevaid identiteete: ühel juhul osales uuritav sotsiaalmeedias pseudonüümi ja suvalise profiilipildiga, teine ei olnud konto profiilipildiks lisanud isiklikku fotot.

Lisaks toodi välja, et oma privaatsuse ja sotsiaalmeedia kontode kaitsmiseks kasutatakse platvormi poolt pakutavaid turvaseadeid, näiteks kahekordset autentimist. Uuritavad sõnasid, et aeg-ajalt kontrollivad nad oma konto seadistused üle ning kasutavad maksimaalselt kõiki platvormi poolt pakutavaid turvaseadeid. Vaid üks uuringus osaleja tõdes, et peale elementaarse parooli ta muid turvaseadeid ei kasuta, kuid lubas peale intervjuu läbiviimist oma turvaseaded üle vaadata. Samas lisas ta, et sulges rahvusvahelisel sõjalisel missioonil viibimise ajaks on sotsiaalmeedia konto just turvakaalutlustel.

Uuringus osalejad tõid välja ka inimeste erineva privaatsustaju ja privaatsusetunnetuse ning leidsid, et kohati on inimestel kalduvus oma eraeluga seonduvat – näiteks reisidel käimist või peredraamasid – liigselt sotsiaalmeedias väljendada. Ka uuringus osalejate jaoks privaatseks osutunud laste piltide jagamine on mõne nende sõbralisti liikme jaoks täiesti tavapärane tegevus, millest räägiti kriitilisel toonil:

Avalikke andmeid seevastu defineerisid uuringus osalejad kui informatsiooni, mis on laiemale üldsusele teada ning mille leviku üle on raske kontrolli omada. Avalikuks informatsiooniks liigitati need andmed, mida isik ise on enda kohta teadlikult jaganud.

INT2: Avalik info on see, mis on laiemale üldsuse teada ning mida ei ole võimalik endal piirata ja mõjutada. Näiteks abielustaatus, laste arv, elukoht. See on info, milleni igaüks ilma suurema pingutuseta jõuab. Info, mis ei anna hinnanguid vaid tugineb faktidele.

Avalike andmete näidetena toodi välja perekonnaseisu, omandatud haridust ja töökohta üldisemas tähenduses. Huvitaval kombel näeme ka, et ehkki ühes eelnevas näites toodi aadress välja tundliku isikliku informatsioonina, võib seda tajuda ka avaliku informatsioonina, mis omakorda iseloomustab seda, et inimeste privaatsusetaju võib olla täiesti erinev ka pisiasjades.

Andmekaitsespetsialisti kommentaar: Nii nagu privaatsete andmete puhul, on ka avalike andmete osas suur roll isikul endal. Tihti avaldame paratamatult või ka tahtmatult oma andmeid nii riigile, kui ka teistele isikutele. Seega võib inimene ühelt poolt enda isikuandmed ise avalikustada, teisalt anda nõusoleku nende avalikustamiseks või toimub avalikustamine seaduse alusel. Näiteks ei käsitle avaliku teabe seadus isiku nime ning ka sellele sünniaja või isikukoodi lisamist veel juurdepääsupiirangu määramise alusena. Nimelt puudutab taoline informatsioon konkreetselt isiku tuvastamise põhiteavet, kuid ka seejuures peab lähtuma eelkõige just minimaalsuse printsiibist. Vastustena loetleti perekonnaseisu, haridust, töökohta – kuid tahan taas siinkohal meenutada privaatsuse subjektiivse tunnetuse aspekti.

Kokkuvõtvalt võiks öelda, et privaatsust ning avalikke andmeid defineerivad uuringus osalejad üsna sarnaselt. Enda privaatsuse kaitsmiseks sotsiaalmeedias kasutatakse enesetsensuuri, valikulist informatsiooni jagamist, kontrolli sõbralisti üle ning sotsiaalmeedia platvormi poolt pakutavaid turvaseadeid.

3.3 Uuringus osalejate suhtumine julgeolekukontrolli teostamisesse

Kõik uuringus osalejad on astunud Kaitseväe teenistusse ajal, mil neile Kaitsepolitseiameti poolt julgeolekukontrolli veel ei kohaldatud. Julgeolekukontrollina teostati tööle asumise ajal päring koolidesse haridust tõendavate dokumentide õigsuse kontrollimiseks ning vajadusel pöörduti varasemate tööandjate poole töösuhte kinnitamiseks.

Esmakordset julgeolekukontrolli teostamist kirjeldavad uuringus osalejad kui ehmatavat kogemust. Osalejad kirjeldavad, et ei osanud esimesesse julgeolekukontrolli mingite eriliste ootustega suhtuda ning alles peale julgeolekukontrolli vestluse läbimist tabas neid arusaam teostatava kontrolli laiaulatuslikkusest ja põhjalikkusest.

INT1: Täitsid hunniku tüütuid ankeete ja jäid vestlust ootama. Ega ma siis ei osanud arvata, mismoodi nad seda kontrolli teevad, arvasin et vaatavad ankeete ja vsjo. See puuga pähe tunne tuli alles pärast esimest taustaka vestlust. Siis nagu said alles aru, kui palju sinu kohta tegelikult teatakse. Päriselt küsiti minult ka asju, mida ma ise ei mäletanudki, ega pidanud vajalikuks ankeeti kirja panna. Ja see kontrolli põhjalikkus on ju kogu aeg kasvanud, nii palju võimalusi on erinevate andmebaaside ja kiire andmete kättesaadavuse pärast juures.

Julgeolekukontrolli läbimist üldiselt kirjeldavad uuritavad ebamugava kogemusena. Leiti, et kuigi uuritavad on oma tegevustes olnud korrektsed, tekitab julgeolekukontroll siiski tunde, nagu oleksid midagi valesti teinud või varjanud.

INT4: See on ebameeldiv, midagi ei ole parata. See teadmine, et sinust teatakse rohkem, kui ankeedis küsitud ja sa ise avalikustanud oled… tekitab alastiolekutunde. On ebamugav, kui minu kohta teatakse sügavalt isiklikke või isegi piinlikke asju, isegi kui see riigisaladusele juurdepääsuloa andmist otseselt ei mõjuta.

Julgeolekukontrolli teostamise vajalikkust seostavad uuringus osalejad riigisaladusele juurdepääsuloa väljastamisega, kuid siiski esines arvamus, et osa kontrolli käigus kogutud infost ei ole loa väljastamisel määrava tähtsusega. Näitena toodi välja pangaülekannetele lisatud selgitused, mille kohta pidi julgeolekukontrolli vestlusel andma täiendavaid selgitusi.

INT3: ..seal ikka küsiti selliseid asju, mis võisid nagu tunduda isegi sel ajal väga sellised, no privaatsed nagu. Need ei tohiks nagu mõjutada riigisaladuse loa saamist aga ometi see huvitas nagu kõiki.

Andmekaitsespetsialisti kommentaar: Raske on anda hinnangut, kas kõik kogutud informatsioon on loa väljastamisel määrava tähtsusega, kuid teoreetiliselt peab see siiski nii olema, sest töötlemise eesmärgiks on anda hinnang isiku vastavusele RS loa väljastamise tingimustele. Iga telefonikõne, interneti kasutamine või kaardimakse jätab maha jäljed, mille abil võib kokku panna kuvandi inimese eelistustest, eluviisist, tegevusest, mis aga jällegi kõik tervikuna vähendab meie privaatsuse määra. Kas see on õigustatud, kui isiku jälgimine on põhjendatud näiteks riiklike julgeolekukaalutlustega, jah, see on tõesti küsitav?

Julgekontrolli teostamise vajalikkuses uuritavad ei kahtle, pigem leitakse et riikliku julgeoleku tagamise huvides on vajalik teostada laiapõhjalist kontrolli, siinhulgas kaasata julgekontrolli ka

riigisaladuse juurdepääsuloa taotleja sotsiaalmeediakontode kontrollimine. Sotsiaalmeedia konto kontrollimist kirjeldati kui fakti, millega tuleb teenistusse astumisel arvestada ja seda ei peetud otseselt häirivaks ega piiravaks asjaoluks, kuna uuringus osalejate kontod on nende enda arvates piisavalt lakoonilised, et mitte sattuda julgeolekuasutuse huviorbiiti. Samas esines uuritavatel arvamust, et kontrolli põhjalikkus võiks sõltuda taotletava riigisaladuse juurdepääsuloa tasemest.

> *INT2: Mõistan, et riigi julgeoleku huvides on oluline kaasata info kogumisse ka isikute sotsiaalmeedia kontod kuid mõnel juhul võib isik tunda, et see riivab tema põhiõigusi.*

Uuritavad leidsid ka seda, et sotsiaalmeediat on võimalik kasutada mainekujunduse tööriistana. Mõtlematult või tahtlikult jagatud info võib isiku profileerimisel anda aluse vale kuvandi loomisele, mis omakorda võib lõppeda isikule riigisaladusele juurdepääsuloa väljastamisest keeldumisega. Näiteks lisati üks uuringus osaleja tema enda teadmata erinevatesse pagulaste vastastesse gruppidesse, mis andis julgeolekukontrolli teostajale aluse arvata, et isik tegeleb erinevates sotsiaalmeedia gruppides viha õhutamisega.

Küll aga toodi välja asjaolu, et inimeste jälgimine sotsiaalmeedias ja seeläbi andmete kogumine ei tohiks muutuda tavapäraseks tegevuseks, kuna see on agressiivne sekkumine isiku eraellu. Kõik uuringus osalejad on seisukohal, et tavainimeste jälgimine sotsiaalmeedias ei tohiks olla tavapärane tegevus. Isikute või grupeeringute jälgimine peaks olema lubatud juhul, kui on märke ohuteguritest ning sel juhul tuleb jälgida Eesti õigusruumis kehtivat seadusandlust.

> *INT5: See ei tohiks muutuda kergekäeliseks ja massiliseks, muidu juhtub see olukord, kus hakatakse seda kuritarvitama ja nii või naa, kuna neid andmeid kogutakse ja andmelekkeid ikka juhtub, siis see info mis kogutakse mis kogutakse enda inimeste kohta, läheb nö vastasvõistkonna kätte ja siis see võib omajagu kurja teha.*

Uuringus soovisin teada ka uuritavate üldist teadlikkust nende kohta kogutavatest isikuandmetest ning isikuandmete kaitse põhimõtetest. Isikuandmete kaitse põhimõtetega olid uuringus osalejad kursis valdavalt tänu meedias kajastatud informatsioonile. Ükski uuringus osaleja ei olnud otseselt tutvunud isikuandmete kaitse üldmäärusega. Üks uuringus osaleja ütles, et uues töökohas kehtestati isikuandmete töötlemise juhend, millega ta on tutvunud ning mis vastab sellele, mida on meedias kajastatud.

> *INT4: See on viimasel ajal nii aktuaalne, et midagi ikka tean. Otseselt õigusakti pole lugenud, aga niipalju kui meedia on kajastanud ja uuel ametikohal kehtestatud*

isikuandmete töötlemise juhendiga olen tutvunud. Nõusolek töötlemiseks ja õigus oma andmetega tutvuda näiteks on meeles.

Enda kohta kogutavatest isikuandmetest olles teenistuses kaitseväes, oskasid uuringus osalejad nimetada neid andmeid, mida nad olid ise tööandjale üldiseks töökorralduseks esitanud, nt haridust tõendavad dokumendid, läbitud koolitused, elukoha andmed ja andmed laste kohta. Julgeolekukontrolli teostamiseks kogutavaid andmeid seostati julgeolekukontrolli ankeedis küsitud andmetega, kuid selles osas puudus kõigil uuritavatel täielik ülevaade nende kohta kogutavates andmetest.

INT5: Me teame nö vaikimisi, mis andmeid meie kohta kogutakse, seda pole otseselt kuskil välja öeldud.

Käesoleva uuringu üks üllatavamaid ning olulisemaid leide on see, et uuringus osalejad olid veendunud, et julgeolekukontrolli teostatakse laiemalt, kui ainult ankeedis esitatud andmetele ning uuritavad ei ole kindlad andmetöötluse seaduspärasuses. Ära märgiti ka andmete kuritarvitamine nii tööandja kui ka julgeolekuasutuse poolt. Toodi välja, et tööandja poolt on esinenud isikuandmete kuritarvitamist uudishimulike poolt ning loata avaldamist, samuti mainiti, et tuttava Kaitsepolitsei ametniku käest on vajadusel võimalik saada nii tööalast kui erahuvides vajalikku informatsiooni.

INT1: Eks töö juures jah vaadati rohkem, kui vaja oli, uudishimulikke oli ikka. Ja mis seal salata, kui on tuttavaid õigel kohal, siis sai ise ka infot küsida… Seda et vajadusel sain tuttava KAPO ametniku käest infot.

Andmekaitsespetsialisti kommentaar: Kahtlemata saab andmetöötleja personali, ka julgeolekuasutuste oma, pidada üheks võimalikuks andmelekke või isikuandmete kuritarvitamise ohuallikaks, kuid siinkohal on asutusel võimalik ja lausa kohustus tegeleda ka ennetavate meetmete kasutusele võtmisega, olgu nendeks siis personali koolitus, organisatsioonilised meetmed vms. 100% rikkumisi loomulikult välistada ei saa, küll saab riske aga maandada ja minimeerida.

Intervjueeritavad kirjeldasid ka oma kokkupuuteid andmekaitse rikkumistega. Mitmel juhul toodi välja personaliandmebaasi kuritarvitamist ja kaitset vajavate dokumentide (näiteks terviseandmete) avalikustamist elektroonilises dokumendihaldussüsteemis.

INT6: Personali andmebaasile juurdepääsu omavad isikud on avalikult rääkinud andmete vaatamisest tööga mitte seotud juhtudel ehk isiklikust huvist lähtuvalt, näiteks isiku vanus, perekonnaseis ja laste arv.

Andmekaitsespetsialisti kommentaar: Andmetöötleja seisukohalt on äärmiselt oluline just töötajate teadlikkus ja nende poolt töötlemise reeglite järgmine. Turvalisust ei saavutata üksnes sobiva tark- ja riistvaralise lahenduse soetamisega, vaid kasutusele peab võtma ka organisatsioonilised meetmed, näiteks töötajate regulaarne koolitamine, konkreetsete ja selgete ülesannete ning pädevuste jaotus, ka kontroll auditi näol ning reeglid nende elluviimiseks. Ka õigusaktid panevad töötlejale kohustuse koolitada isikuandmeid töötlevaid isikuid. Konkreetse töötaja seisukohalt on oluline, et seadus kohustab teda hoidma saladuses talle tööülesannete täitmisel teatavaks saanud isikuandmeid ning see nõue säilib ka pärast nimetatud tööülesannete täitmist või töölt lahkumist (töösuhte lõppemist). Töötajad, kes töötlevad isikuandmeid ametiülesannete täitmiseks peavad järgida nii õigusaktidest, kui asutuse poolt kehtestatud reegleid. Lisaks toob ka avaliku teabe seadus üheselt välja ka avaliku teabe valdaja kohustuse tagada, et juurdepääsupiiranguga teave ei satuks pääsuõigusteta isikute kätte.

Kahel juhul kirjeldati ka tööandja ebaseaduslikku kontrolli teenistuja isiklike e-kirjade üle ja isiklike vestluste lugemist tööandja kiirvestlussüsteemis. Kuigi need juhtumid põhinevad pigem isiklikul arvamusel, kui kinnitatud faktidel, ei ole kunagi võimalik täielikult välistada, et tööandja ei loe töötaja e-postkastis olevaid erasõnumeid.

INT4: Abikaasa töötas ühes teises riigiasutuses, ja seal tuli mingil hetkel välja, et nende töö-skype vestlusi loeti. Otseselt pole isikuandmete kaitse rikkumine, aga põhiõiguste riive siiski ju?

Andmekaitsespetsialisti kommentaar: Digitaalne jälgimine on tänu tehnoloogiale üha lihtsam ning enam ei ole tehniliselt mingi probleem hoida nn silma peal töötajate tegemistel ja nende harjumustel. Siinkohal peaks eetilises plaanis tõstatuma siiski küsimus tööandja õiguste ulatusest, et kas tööandajal on ikka õigus lugeda töötaja privaatseid e-kirju ning jälgida milliseid veebisaite külastatakse. Internetiprivaatsus tähendab õigust, et keegi ei pääse ilma isiku loata ligi tema arvutis või veebis asuvatele failidele, kirjadele, samuti saitide külastuse ajaloole jm andmetele, mis vähendavad isiku anonüümsust. Töötajaid võib kontrollida ainult juhul, kui neile on kehtestatud kas mingi nõue või kohustus ning sellest tulenevalt soovibki nüüd tööandja selle täitmist või siis järgmist kontrollida. Tähtis on, et töötajat teavitatakse kontrolli teostamise faktist ning selle

läbiviimise tingimustest. Tööandja ei tohiks kindlasti aga seejuures jätta tähelepanuta töötaja inimväärikuse tagamise olulisust. Samas olen seisukohal, et kontroll, kui selline on paljuski tagajärgedega tegelemine, esmatähtis peaks siiski olema just ennetustöö.

Peamiseks andmekaitsete rikkumise põhjustajaks töösuhte korraldamisel peeti inimfaktorit – uudishimu, teadmatust andmete töötlemisel ja inimlikke eksitusi.

> *INT6: Leian, et ametialaselt lohakad või lihtsalt rumalad andmeid töötlevad isikud on kõige suuremaks ohu allikaks. Eriti sellised inimesed, kes ei oska näha suuremat pilti vaid lähtuvad rangelt oma vaatevinklist. Näiteks seaduse järgi on distsiplinaarmenetluse kokkuvõte avalik dokument, aga kui see sisaldab isiku eriliigilisi andmeid, siis on tegu infoga, mis vajab kaitset. Selliseid rikkumisi oli meie asutuses korduvalt.*

Ka julgeolekukontrolli teostamisel toimuvate rikkumiste peamiseks põhjuseks peeti isiklikku huvi, lisaks peeti rikkumiseks ka seda, et isikul puudub täielik ülevaade tema kohta kogutavatest andmetest.

> *INT6: Kuna julgeolekukontrolli teostatakse enamjaolt nii, et sellest märki maha ei jää, siis inimlikust aspektist lähtuvalt või julgeolekuametnikul tekkida isiklik huvi andmete vastu. Kuna nendel on vaja andmeid koguda isikute kohta, siis arvan et mõnelgi juhul vaadatakse seadusest kõrvale.*

Andmekaitsespetsialisti kommentaar: Kommentaariks eelnevatele väidetele leian, et isiku varasemad negatiivsed kogemused võivad mõjutada ka edaspidi tema suhtumist isikuandmete töötlemisse, nende avaldamisse. Kui ollakse varasemalt kokku puutunud informatsiooni kuritarvitamisega või andmete puhul, mida peetakse väga privaatseteks, on andmesubjektil tõenäoliselt raskem enda kohta käivat teavet avaldada.

Uuringus osalejad ei pidanud vajalikuks ka kaitseväele täiendava taustakontrolli võimaluse andmist, viidates mitmel korral hiljuti toimunud andmelekke skandaalile kui ka sellele, et nende arvates puudub kaitseväel pädev instants taustakontrolli funktsiooni teostamiseks. Samuti viidati täiendavale halduskoormusele, kuna teenistusse asumisel teostatakse isikule nagunii elementaarne taustakontroll, millele hiljem lisandub põhjalik julgeolekukontroll riigisaladusele juurdepääsuloa taotlemisel.

INT7: Leian, et see pole vajalik, sest teenistujatele tehakse niigi juba esmane taustakontroll ning ametid peavad omavahel suhtlema ja andmeid vahetama, mitte iga amet teostab oma kontrolli. Kaitseväel ei pruugi olla teenistuses piisaval määral professionaalseid teenistujaid, kes oleksid usaldusväärsed andmeid töötlema.

Kokkuvõtvalt võib öelda, et uuringus osalejad on teadlikud julgeolekukontrolli teostamise vajalikkusest seoses riigisaladusele juurdepääsuloa taotlemisega ja töösuhtega. Ka on nad teadlikud, et tööandja ja julgeolekuasutus koguvad ja talletavad nendega seotud informatsiooni, kuid on veendunud, et lisaks nende poolt esitatud andmetele teostatakse kontrolli laiemalt kui õiguslikult lubatud. Toodi välja ka informatsiooni kuritarvitamist nii tööandja kui julgeolekuasutuse poolt, mistõttu pole uuringus osalejatel täit kindlustunnet oma andmete turvalise käitlemise osas.

3.4 Kaitseväe siseregulatsioonide ja julgeolekukontrolli läbimise tajutud mõju uuringus osalejate sotsiaalmeedia käitumise kujunemisel

Uuringus osalejad tõid positiivsena näitena välja endiste Kaitseväe aegsete töökaaslaste suurenenud teadlikkuse sotsiaalmeediaga kaasnevatest ohtudest ning võimalustest. Uuringus osalejad leidsid, et endiste kolleegide poolt jagatav info on pigem neutraalne ning vähese isikliku seosega ning suhtlemine ja infovahetus toimub rohkem privaatselt ning peamine infovahetus on avalikult seinalt liikunud kinnistesse gruppidesse või privaatvestlustesse.

INT2: Ilmselt on see seotud üldise ja ka organisatsioonisisese teavitustöö ja teadlikkusega, töökaaslased postivad vähe infot, mis võiks neid mingil moel kahjustada. Suhtlus on avaliku Facebooki seina pealt kolinud grupivestlustesse või spetsiaalsetesse loodud gruppidesse.

Leiti, et endised kolleegid jälgisid sarnaselt uuritavatele eneseregulatsiooni põhimõtteid, kuid toodi välja ka erandeid, näiteks ebasobivate peopiltide postitamine. Kahel juhul leidsid uuritavad, et tööalase informatsiooni avalikustamine toimub pigem nooremate või äsja teenistusse asunud kaitseväelaste seas. Vanemate teenistujate informatsiooni avaldamises on toimunud nihe privaatsuse suunas.

INT5: Mida ma olen tähele pannud, on see, et teised tegevväelased, kes on pikemat aega olnud, need ei postita tööga seoses üldjuhul mitte midagi, samamoodi on igasugused

missioonipildid ära kaotatud, isegi kui need varem olid olemas. See on trend, mida olen märkand. Samas nooremad kolleegid, nende puhul pigem panevad pilte üles, kus on metsalaagris.

Intervjueeritavad mäletasid ka kokkupuudet Kaitseväes kehtestatud juhendiga „Juhend kaitseväelaste osalemiseks sotsiaalmeedias“. Kuigi nad ei mäletanud juhendit väga konkreetselt, siis oskasid nad siiski välja tuua peamisi aspekte, mida juhend endas on sätestanud.

Tõdeti ka, et kuna kehtestatud juhend on üldine kogum elementaarsetest käitumisnõuetest sotsiaalmeedias, siis on uuritavad vaistlikult oma sotsiaalmeedia tegevustes nimetatud juhendist lähtunud. Juhendit peeti vajalikuks ka üldise julgeoleku mõttes, et liigset informatsiooni ei tuleks avalikuks ja seda ei oleks võimalik kasutada isiku manipuleerimiseks. Lisaks nimetatud juhendile toetab sotsiaalmeedia käitumisnormide kinnistumist iga-aastane küberhügieeni test, milles samuti käsitletakse sotsiaalmeediat ning muud erinevad meedialoengud.

INT5: Seda küsiti iga-aastases IKT testis ka. Eks seal mingid põhilisemad nõuded olid toodud, a la et kaitseväega seotud infot mitte kajastada ja turvanõudeid jälgida. See juhend, kuigi juba aegunud, on kindlasti vajalik ja vajab ka meeldetuletamist. Tean et minu töökoht kaitseväes võib olla potentsiaalne allikas riigi vastu suunatud jõudude eesmärkide kasutamisel. Seega pidi minu käitumine sotsiaalmeedias olema selline, mida ei saaks minu vastu suunata.

Samuti leidsid uuringus osalejad, et Kaitseväe teenistujate teadlikkus sotsiaalmeedia kasutamisest on tõenäoliselt suurem, kui tavakodanikul ning seetõttu osatakse pöörata suuremat tähelepanu oma jagatavale infole, seda siis nii isikliku informatsiooni jagamise osas kui ka teiste loodud info jagamisel.

Huvitava tähelepanekuna selgus ka, et isikute jälgimine sotsiaalmeedias võib viia hoopis selleni, et isikud loobuvad edaspidi sotsiaalmeedia kasutamisest täielikult ning sel juhul jääb edaspidi julgeolekukontrolli teostamisel vajalik informatsioon üldse saamata.

INT3: ...paljud inimesed võivadki minna kiviaega tagasi, loobuda täielikult igasugusest sotsiaalmeedia kasutusest ja kogu see teave jääb ikka saamata, võib-olla mida nagu loodetakse.

Kõik uuringus osalejad tajusid julgeolekukontrolli teostamise järgselt muudatusi oma sotsiaalmeediakäitumises. Kuid lisaks julgeolekukontrolli läbimisele mõjutas uuritavate arvates

nende sotsiaalmeedia kasutamist ka üldine teadlikkuse kasv ning asutusepoolsed juhised ja piirangud sotsiaalmeedia kasutamiseks.

> *INT5: Ma täiesti teadlikult väldin enda kohta informatsiooni jagamist. Ma arvan et osalt on selle taga enda teadlikkuse kasv, mida selle informatsiooniga saab peale hakata. Ja eks see on suuresti tingitud ka sellest, missuguses ametis ma töötasin.*

Toodi välja muudatuste tegemist kontode turvaseadetes ja turvaseadete üldist üle kontrollimist. Käitumuslike muudatustena toodi välja enesetsensuuri, oma postituste arvukuse piiramist, fotode eemaldamist albumitest ja ajajoonelt ning üldise käitumise kõrgendatud jälgimist. Oluliseks peeti ka sõbralisti jälgimist ning toodi välja sõbralisti puhastamist ja suuremat kaalutlemist sõbrakutsete vastuvõtmisel. Siinkohal tõi mitu intervjueeritavat välja ka asjaolu, et kahtlastest sõbrakutsetest antakse teada julgeolekule.

Enda informatsiooni jagamise kohta ütlevad uuringus osalejad, et isiklike asjade avalikustamine ja jagamine on aja jooksul muutunud tagasihoidlikumaks ja läbimõeldumaks. Uuringus osalejad on seadnud piirangud oma postituste auditooriumile ning eemaldanud sotsiaalmeedia kontolt perepildid ja tööalased fotod, välditakse ka laste kohta käiva informatsiooni ja fotode avalikustamist ning varasemalt üles laetud fotod on eemaldatud. Üks uuringus osaleja leidis, et ta pigem edastab fotod privaatselt läbi Messengeri, selle asemel et fotosid avalikule seinale või fotoalbumisse üles laadida.

Sotsiaalmeedia kasutusharjumuste kujunemise meenutamisel tajusid uuritavad peamise ühisosana jagatava informatsioonikoguse vähenemist. Leiti, et algselt oldi inimlikust uudishimust tulenevalt julgemad sotsiaalmeedia platvormi erinevaid võimalusi kasutama.

> *INT4: … alguses oli ju see Facebook nii uus ja huvitav, oli vaja kõiki funktsioone proovida. Näiteks alguses panin enda ja pere kohta ka pilte üles. Hiljem panin juba albumile piirangud peale ja tänaseks olen pildid ära kustutanud üldse.*

Toodi välja asjaolu, et enne julgeolekukontrolli läbimist olid uuritavad julgemad erineva info jagamises, kuid julgeolekukontrolli läbimise järgselt suurenes nende üldine teadlikkus sotsiaalmeedia käitumisest ja erinevatest turvaseadete võimalikkusest. Enesetsensuuri rakendades on uuritavad julgeolekukontrolli järgselt korduvalt oma sotsiaalmeedia kontod üle vaadanud, et seal ei leiduks sisu, mis võiks anda võimaluse neid negatiivselt profileerida . Toodi välja ka

asjaolu, et eneseregulatsioon paneb oma tegevusi sotsiaalmeedias hoolikalt läbi mõtlema ning kahtluse korral jäetakse informatsioon pigem avaldamata.

> *INT2: Vaatan end kõrvalt. Kuidas postitus võiks teiste isikute puhul mulle tunduda. Pigem jätan tegemata, kui kahtlen. Vähese postituse asemel veel vähem. Puhastused sõbralistis, postituste vähesus. Aegajalt vaatan konto karmi pilguga üle ja puhastan.*

Kõik intervjueeritavad tundsid, et muutused nende sotsiaalmeedia käitumises on püsivad ning Kaitseväe teenistusest lahkumine ja riigisaladusele juurdepääsuloa mittevajamine ei too kaasa muutuseid juba selleks ajaks kinnistunud läbimõeldud ja info tagasihoidlikul jagamisel põhinevas sotsiaalmeediakäitumises. Omandatud muudatusi soovitatakse ka näiteks oma lastele või lähematele tuttavatele.

4 JÄRELDUSED JA DISKUSSIOON

Minu lõputöö eesmärk oli tuvastada, kuidas defineerivad julgeolekuasutuse kõrgendatud tähelepanu all olnud inimesed privaatset ja avalikku informatsiooni, milline on nende teadlikkus isikuandmete kaitse põhimõtetest ja milliseid muutuseid tajusid uuringus osalejad oma sotsiaalmeedia käitumises riigisaladusele juurdepääsuloa julgeolekukontrolli teostamise järgselt. Selles peatükis esitan järeldused, milleni olen jõudnud uuringu tulemusi analüüsides ning arutlen tulemuste üle laiemas kontekstis.

4.1 Privaatsuse, privaatse ja avaliku info eristamine julgeolekuasutuse kõrgendatud tähelepanu all olnud isikute näitel

Privaatsuse ja privaatsete andmete kirjeldamisel puudub ühtne ja konkreetne definitsioon, siinkohal saab rääkida subjektiivsest mõistest, mille tajumine on indiviidipõhine (Palm, 2009; Tavani, 2008). Uuringus osalejadki tõid välja asjaolu, et inimeste privaatsuse tunnetus on väga erinev – kui ühel inimesel pole probleemi teha oma sünnitusest otseülekannet, siis teine inimene võib olla häiritud juba ainuüksi tema isikukoodi avalikustamisest. Leiti, et laiemas kontekstis võib privaatseks informatsiooniks pidada kõike seda, mida inimene soovib teiste eest varjata ning et oluline on jätta indiviidile otsustusõigus, millist informatsiooni ja kui suures ulatuses ta teiste inimestega jagada soovib.

Privaatseteks andmeteks pidasid uuringus osalejad peamiselt sellist informatsiooni, mille erinevaid osasid kombineerides on võimalik luua tervikpilti näiteks isiku tervislikust ja majanduslikust seisundist. Avalike andmetena defineeriti kõike seda, mida isik vabatahtlikult on enda kohta avalikustanud. Samas võib isiku poolt vabatahtlikult avalikustatud andme osas tekkida vastuolu tulevikus, kui isik enam ei taha, et kunagi tema poolt avalikustatud andmete põhjal oleks võimalik tema kohta mingit kuvandit luua. Tavani (2008) on informatsioonilist privaatsust

ohustavate teguritena välja toonud asjaolud, et kogutava informatsiooni hulk on kasvanud ning säilitusaeg pikenenud. Olles kord informatsiooni avaldanud ja veebikeskkonda üles laadinud, jääb see sinna ja on leitav tõenäoliselt ka väga pika aja pärast.

Uuringust ilmnes, et intervjueeritavad kasutavad sotsiaalmeedias oma privaatsuse kaitsmiseks üksteisega sarnaseid turvastrateegiaid, tuues välja valikulise informatsiooni jagamise ja enesetsensuuri. Kui algselt oldi erineva informatsiooni jagamisel julgemad, siis tänaseks on kasutusharjumused kujunenud selliseks, et jagatav informatsioon on vähenenud miinimumini ning jagatakse ja avalikustatakse valikulisele auditooriumile. Auditooriumi valimist teostatakse valikuliste sõbrakutsete vastuvõtmisega, sõbralisti kontrollimise ja puhastamisega, samuti postitustele erinevate privaatsusseadete rakendamisega. Samuti hoitakse kontrolli all erineva sisu avalikustamist ja jagamist, pidades silmas nii isikliku maine kui kaitseväe üldise maine kahjustamise võimalikkust. Kuigi ükski intervjueeritavatest ei olnud otseselt kursis Kaitseväes kehtestatud juhendiga "Juhend kaitseväelaste osalemiseks sotsiaalmeedias" (2011), siis võrreldes juhendiga kehtestatud norme ja intervjueeritavate enda kirjeldatud sotsiaalmeediakasutust, võib väita, et intervjueeritavate sotsiaalmeedia kasutusharjumused vastasid kehtestatud juhendile. Sellest võib järeldada, et Kaitseväe, kui „ahne organisatsiooni" (Coser, 1974) poolt tehtud ettekirjutused sotsiaalmeedias osalemiseks on intervjueeritavate poolt omaks võetud. Lewin'i muudatuste juhtimise kolmeastmelise teooria kolm etappi on läbitud ning viimases etapis toimunud muudatuste kinnikülmutamise käigus (Wirth, 2004) on Kaitseväes rakendatava sotsiaalmeedia juhendiga (2011) kehtestatud käitumisreeglid muutunud intervjueeritavate jaoks harjumuspärasteks.

Kasutusharjumuste kujunemisel mängis uuritavate sõnul rolli nii üldine teadlikkuse kasv, kaitseväe poolne regulatsioon kui ka julgeolekukontrolli läbimine. Intervjuudest ei selgunud otseselt, milline eelmainitud asjaoludest oli põhiline sotsiaalmeedia kasutusharjumuste kujundaja. Samuti on intervjueeritavate tausta arvestades tõenäoline, et uuringus osalejad kirjeldavad oma sotsiaalmeedia kasutusharjumusi oluliselt tagasihoidlikumana, kui see tegelikult on, kuna nende jaoks on tagasihoidlik sotsiaalmeediaprofiil kinnistunud sotsiaalseks normiks. Kahjuks aga ilmnes intervjuudest asjaolu, et sotsiaalmeediat on võimalik kasutada mainekujundusplatvormina. Inimese maine on justkui kollektiivne looming, mille üle pole inimesel endal 100% kontrolli. Isegi, kui inimene ise käitub korrektselt, võimaldavad sotsiaalmeediaplatvormid kolmandatel isikutel tekitada olulist mainekahju ja anda alust isiku negatiivseks profileerimiseks.

Uurisin intervjueeritavatelt, kas neil esineb mingeid teemasid, mida nad peavad liiga privaatseteks sotsiaalmeedias suhtlemiseks. Sügavalt privaatseid teemasid intervjueeritavatel meelde ei tulnud, vähemalt ei osanud nad nimetada ühtegi, mille puhul nad jätaks sotsiaalmeediakanalite suhtlusvõimalused kasutamata. Intervjuudest selgus ka, et Facebooki kiirsõnumi rakendus Messenger on uuritavate peamiseks suhtluskanaliks just selle kiiruse ja kättesaadavuse tõttu. Sellest järeldan, et vaatamata erinevatele skandaalidele, on inimestel säilinud usk sotsiaalmeediagigantidesse. Samuti on suure tõenäosusega tegemist lõivsuhtega, ehk siis selleks, et näiteks Facebooki veebikeskkonna teenuseid üldse tarbida, tuleb maksta lõivu, esitades veebikeskkonnale täiendavaid andmeid enda kohta. Isikliku info jagamine lõivsuhtes osalemiseks on välja toodud nii Inimõiguste Instituudi 2014. a läbiviidud uuringus „Privaatsusõigus inimõigusena ja igapäevatehnoloogiad“ (Murumaa-Mengel, Laas-Mikko ja Pruulmann-Vengerfeldt, 2014) kui ka Eurobaromeetri 2011. aastal läbiviidud privaatsust käsitlevas eriuuringus (Eurobaromeetri eriuuring 359, 2011).

4.2 Uuringus osalejate üldised hoiakud tavapärasest põhjalikuma julgeolekukontrolli teostamisesse

Intervjuudest selgus, et uuritavad pidasid vajalikuks isikuandmete kogumist nii töösuhte korraldamiseks, kui ka julgeolekukontrolli teostamiseks. Kaitseväe spetsiifikast lähtuvalt olid kõik uuritavad arvamusel, et ametikohast lähtuvalt on põhjaliku julgeolekukontrolli teostamine oluline, et tagada riiklik julgeolek.

Kõik intervjueeritavad aga olid arvamusel, et isikuandmete töötlemisel esines rikkumisi nii töösuhte korraldamisel, dokumentide menetlemisel kui julgeolekukontrolli teostamisel. Rikkumiste põhjustena toodi välja teadmatust, inimlikku uudishimu ja hooletust, kuid ka teadlikku rikkumist ja seetõttu ei ole ühelgi uuringus osalejal kindlustunnet oma andmete seaduspärases ning turvalises töötlemises.

Tööandjapoolsete rikkumistena peeti peamisteks hooletust dokumendihaldussüsteemi kasutamisel ja personalitöötajate poolset personaliandmebaasi ning teiste andmebaaside kuritarvitamist. Sarnased rikkumised ja nende tehiolud on välja toodud ka Andmekaitse Inspektsiooni aastaraamatus (2019).

Julgeolekukontrolli teostamise peamiseks rikkumiseks pidasid intervjueeritavad isiklikel kogemustel tuginevat arvamust, et julgeolekukontrolliks teostatavad andmete päringud ning

jälgimine on laiaulatuslikum, kui seaduslik raamistik ette näeb. Kuigi isikuandmete kaitse üldmääruse (2016) artikkel 5 sätestab isikuandete töötlemise põhimõtetena seaduslikkuse ja eesmärgipärasuse, esines uuritavatel arvamus, et lisaks nende poolt julgeolekukontrolli ankeedis esitatud andmetele teostati kontrolli oluliselt laiemalt ning inimestel puudus täielik ülevaade nende kohta kogutavatest andmetest. Siit tuleneb asjaolu, et teadmatus põhjustab ebakindlust ning usaldamatust. Kui Inimõiguste Instituudi 2014. a läbiviidud uuringust „Privaatsusõigus inimõigusena ja igapäevatehnoloogiad" selgus, et andmete eesmärgipärasel töötlemisel usaldati kõige rohkem riiki üldise institutsioonina (Murumaa-Mengel, Laas-Mikko ja Pruulmann-Vengerfeldt, 2014), siis minu intervjueeritavatel esines pigem vastupidine arvamus. Leian, et töötaja, kellel on ülevaade, kuidas tööandja tema kohta kogutavaid andmeid töötleb ja millistele osapooltele seda informatsiooni veel võidakse edastada, usaldab ja suhestub oma tööandja paremini ning oskab ka oma tegevusi paremini planeerida.

Inimeste jälgimise kohta sotsiaalmeedias olid uuritavad ühisel arvamusel- riiklikud institutsioonid ei tohiks tavainimest jälgida ilma mõjuva põhjuseta. See võib põhjustada tervisekahjusid või sotsiaalmeedia kasutamisest loobumist. Panoptilist jälgimist, ehk siis julgeolekuasutust silmas pidades olukorda, kus vähesed jälgivad paljusid (McCullagh, 2005), peeti lubatavaks olukorras, kui on ilmnenud märke ohuteguritest. Paraku on tänapäeva tehnoloogiate areng loonud arvukalt võimalusi inimeste privaatsuse rikkumiseks ning pannud inimesed olukorda, kus nad ei oskagi aimata, et nende privaatsust rikutakse. Sageli ei tunta ka kõiki turvaseadeid ega osata oma privaatsust kaitsta.

Leian et julgeolekuasutused ei jälgi julgeolekukontrolli läbivate isikute sotsiaalmeedia kontosid ainult indiviidist lähtuvalt. Tõenäoliselt püütakse nii leida ning elimineerida ka asjaolud, mis võiksid pälvida võimaliku vastase huvi. Seega aitab sotsiaalmeedia kontroll ja seeläbi informatsiooni valdamine jõuda ka tõhusamate julgeolekumeetmeteni. Ühe võimalusena tõhustada julgeolekut ongi Kaitseväe poolne panustamine oma liikmete teadlikusse sotsiaalmeedias käitumiseks – väike investeering organisatsiooni liikmete teadmistesse võimaldab tõhustada julgeolekut.

Julgeolekukontrolli teostav julgeolekuasutus osaleb sotsiaalse järelevalve vertikaalses vaates (Vidili jt, 2010) asutuse põhimääruses sätestatud ülesannete täitmiseks, kuid nagu intervjuudest selgus, siis esineb seadustes sätestatud volituste ületamist. Tänapäeval on peaaegu kogu sotsiaalne sfäär kolinud *online* keskkondadesse ja seal avaldatud informatsioon on digitalletatav, kopeeritav ja jagatav, pakkudes seega ka võimalust seda informatsiooni kergelt kätte saada. Edward Snowden

paljastas 2013. aastal USA valitsusasutuste laiaulatusliku ja ebaseadusliku jälitustegevuse (MacAskill ja Hern, 2018), öeldes et loodud programmide abil toimub lakkamatu informatsiooni kogumine (Greenwald ja MacAskill, 2013) ja seda just sotsiaalvõrgustikest, kuhu inimesed oma privaatset informatsiooni vabatahtlikult üles laevad (Alas, 2013). Snowden'i sõnum oli lihtne – kõik me tehtu ja öeldu talletatakse (Greenwald ja MacAskill, 2013). Nimetatud paljastus toetab ka intervjueeritavate arvamust, et riik teostab ebaseaduslikku jälitustegevust ning andmete kogumine on oluliselt laiaulatuslikum, kui avalikkusele seda näidatakse.

Mitme intervjueeritava jutust tuli välja, et kuna nad pole konkreetselt enda isikuandmete töötlemise rikkumisega kokku puutunud, siis nad tõenäoliselt ei oskagi rikkumist defineerida või ära tunda. Erinevalt suhtuti ka enda ja teiste andmete töötlemise rikkumistesse ning üllataval kombel ei tajutud rikkumisena seda, kui Kaitsepolitsei ametnikult infot küsiti. Kuna intervjuude analüüsist selgus, et intervjueeritavate üldine teadlikkus 25.05.2018 jõustunud andmekaitsereformist on madal, siis võib see olla üheks asjaoluks rikkumiste erineval tunnetamisel.

4.3 Julgeolekukontrolli järgselt tajutud peamised muudatused uuritavate sotsiaalmeediakäitumises

Kõik intervjueeritavad olid veendunud, et nende sotsiaalmeedia kasutusharjumused on aja jooksul muutunud. Peamisteks muudatusteks oli teadlikkuse suurenemine turvaseadete rakendamise osas ning enesetsensuuri põhjalikumaks muutumine ja auditooriumi valimine. Isikliku informatsiooni jagamine vähenes oluliselt ning vähese isikliku informatsiooni avalikustamine muutus läbimõeldumaks ja kaalutlevamaks. Intervjuudest selgus, et uuritavad valivad hoolikalt, millist informatsiooni nad sotsiaalmeedias avalikustavad ning nende kontod on seadistatud selliselt, et informatsioon on kättesaadav vaid sõbralisti vastuvõetud isikutele. Ka sõbrakutsete vastuvõtmisel ollakse ettevaatlikud ja kaalutlevad. Kaks intervjueeritavat kasutavad enda privaatsuse kaitsmiseks täiendavalt pseudonüüme, et nende sotsiaalmeediast ülesleidmine oleks raskendatud. Tulemused näitavad, et uuritavate sotsiaalmeediakäitumises on toimunud nihe privaatsuse suunas. Leian et julgeolekualastel kaalutlustel on aset leidnud muudatused ja toimunud nihe äärmiselt tervitatav nähtus. Sotsiaalmeedias on võimalik näiteks libakontode või identiteedivarguste abil ületada suhtlusbarjäär ning seeläbi mõjutada inimest avalikustama riigi julgeoleku seisukohalt tundlikku informatsiooni.

Kasutusharjumuste muudatuste otsest mõjutajat ei osanud uuritavad välja tuua, vaid viitasid üldise teadlikkuse kasvu, organisatsioonipoolsete regulatsioonide ja julgeolekukontrolli läbimise koosmõjule. Ühiseks nimetajaks kasutusharjumuste kujunemisel võiks seega nimetada kaitseväge tervikuna, mis ühelt poolt on panustanud oma teenistujate teadlikkuse kasvu ja teisalt kohaldanud põhjalikku julgeolekukontrolli läbimist, mõjutades ka seeläbi teenistujate käitumuslikke harjumusi.

Sotsiaalmeediat kasutavad uuritavad käesolevaks ajaks peamiselt meelelahutuslikul eesmärgil, mitte enda isiku eksponeerimiseks ning Kaitseväe teenistusest lahkumine ja riigisaladusele juurdepääsuloa mittevajamine ei ole kaasa toonud muutuseid juba kinnistunud läbimõeldud ja info tagasihoidlikul jagamisel põhinevas sotsiaalmeediakäitumises. Omandatud muudatusi soovitatakse ka peresiseselt ja lähematele sõpradele.

4.4 Meetodi kriitika

Käesoleva lõputöö eesmärgi saavutamiseks valitud kvalitatiivne uurimismeetod (poolstruktureeritud individuaalintervjuud) sobis, kuna intervjueerimine andis võimalusi uurida osalejate arvamusi ja leida tõlgendusi (Laherand, 2008). Poolstruktureeritud intervjuude paindlikkus võimaldas muuta teemade järjekorda ja esitada täiendavaid küsimusi, et saada uurimisküsimustele vastamiseks vajalikku informatsiooni.

Ühe kriitilise aspektina võiks esile tõsta uuritava teema delikaatsuse. Kuna tegemist on julgeolekualaselt tundliku teemaga, siis võis julgeolekukontrollist läbimine mõjutada intervjueeritavate avatust küsimustele vastamisel. Seevastu andmekaitsespetsialisti intervjueerimine andis tulemuste lahtimõtestamisele lisandväärtuse, kuna intervjuu läbiviimine sujus ning sain uurimistulemustes väljatoodud probleemkohtadele sügavad ja sisukad kommentaarid.

Leian, et privaatsuse ja isikliku informatsiooni uurimine on aktuaalne ja oluline teema. Oma töös keskendusin ühe osana ka organisatsioonisisesele isikliku informatsiooni käsitlemisele. Arvan et antud uurimisteemat saaks edasi arendada ning uurida näiteks isikliku informatsiooni ning töösuhte vahelist seost indiviidi meediakäitumise mõjutajana. Oluliseks uurimisteemaks võiks olla ka minu töös tõstatunud isikuandmete väärkasutus töösuhetes või nö „pealesunnitud nõusolek“ isikuandmete töötlemiseks, selleks et saada mingit teenust või osaleda töösuhtes. Tuginedes intervjueeritavate tähelepanekule, et äsja teenistusse astunute ja nö „vanade olijate“ sotsiaalmeedia

kasutusharjumused tööalase informatsiooni osas on tunduvalt erinevad, võiks ka see olla uurimisteemaks ning annaks võimaluse kaitseväe jaoks välja töötada täiendav või põhjalikum sotsiaalmeedia kasutusjuhend.

KOKKUVÕTE

Minu lõputöö on kirjutatud teemal „Julgeolekuasutuse kõrgendatud tähelepanu all olemise tajutud mõju inimeste sotsiaalmeediakäitumisele“. Uuritav valdkond on uudne ja huvitav, kuna tehnoloogiate arenguga on privaatsuse tajumine ja isikliku informatsiooni kaitsmine muutunud üha keerulisemaks. Teemavaliku ajendiks oli seminaritöö raames läbiviidud uuring, mis tuvastas mitmeid probleemkohti indiviidide privaatsuse tagamisel.

Lõputöö eesmärgiks oli läbiviidud uuringu põhjal selgitada, kuidas defineerivad julgeolekuasutuse kõrgendatud tähelepanu all olnud isikud privaatset ja avalikku informatsiooni ning kuidas mõjutas nende sotsiaalmeedia käitumist ja privaatsusharjumusi riigisaladusele juurdepääsuloa julgeolekukontrolli läbimine.

Uurimisküsimustele vastuste saamiseks viisin läbi semistruktureeritud individuaalintervjuud seitsme varasemalt riigisaladusele juurdepääsuloa julgeolekukontrolli läbinud isikuga. Intervjuudest saadud tulemuste sügavamaks lahtimõtestamiseks palusin kommentaari andmekaitsespetsialistilt.

21. sajandit nimetatakse infoajastuks, mil erinevate tehnoloogiate arengu negatiivseks tagajärjeks võib pidada seda, et järjest keerulisem on säilitada kontrolli privaatsuse üle ning kaitsta isiklikku informatsiooni. Läbiviidud uuringu tulemustest selgus, et vastajad väärtustavad enda privaatsust ning kaitsevad seda sotsiaalmeedias erinevate turvavõtetega. Isikliku informatsiooni alla kuuluvad vastajate arvates peamiselt perekonda, majanduslikku ja tervislikku olukorda puudutav informatsioon. Siiski selgus nii intervjuude transkriptsioone analüüsides kui ka uuritavate enda arvates, et privaatsuse taju on individuaalne ja konkreetset piiri tõmmata ei ole võimalik.

Uuringu tulemused tõid välja, et kuigi uuritavad peavad julgeolekukontrolli teostamist ametikoha spetsiifikast lähtuvalt vajalikuks, ei ole neil täielikku selgust, millist informatsiooni nende kohta

julgeolekukontrolli käigus kogutakse. Esines arvamus, et julgeolekukontrolli teostatakse laiaulatuslikumalt, kui julgeolekukontrolli ankeedis küsitud informatsioonile. Ka ei olnud uuritavad kindlad nende andmete töötlemise turvalisuses, kuna organisatsioonisiseselt oli korduvalt esinenud isikuandmete töötlemise rikkumisi.

Uuringu tulemustele toetudes võib väita, et uuritavate sotsiaalmeediakäitumine muutus aja jooksul läbimõeldumaks, samuti pööratakse täna rohkem tähelepanu turvaseadetele ning jälgitakse, millise auditooriumini uuritavate postitused jõuavad. Otseselt ei selgunud, milline oli kõige olulisem uuritavate sotsiaalmeedia käitumist mõjutav tegur, kuid kaitseväe roll käitumusharjumuste suunamisel leidis kinnitust. Kõik uuringus osalejad tajusid oma sotsiaalmeediakäitumises sarnaseid ja püsivaid muudatusi, mida plaanivad kasutada ka edaspidi.

SUMMARY

This thesis, "**The perceived impact of being under the heightened attention of the Security Agency on people's social media behavior"** explores a new and interesting topic, as the perception of privacy and the protection of personal information have become increasingly difficult with the development of technology. The theme choice was prompted by a study carried out as part of the seminar work, which identified a number of problems in ensuring privacy for individuals.

The aim of this thesis was to clarify and understand how individuals who have been under the heightened attention of the security authority define private and public information and how their social media behavior and privacy habits were affected by the passing of security clearances to national secrecy.

In order to get answers to my research questions, I conducted semi-structured individual interviews with seven people who had previously undergone security clearances for access to national secrecy.

The 21st century is called an information age, when the negative consequence of the development of various technologies can be considered that it is increasingly difficult to maintain control over privacy and protect personal information. The results of this thesis revealed that participants value their own privacy and protect it on social media with various security techniques. Personal information is, according to respondents, mainly about the family, information about the economic and health situation. However, it was revealed both in analyzing transcripts of interviews and in the opinion of the investigators themselves that the perception of privacy was individual and that it was not possible to draw a specific boundary.

The findings of the thesis pointed out that while the investigators consider it necessary to carry out security checks on the basis of the specificity of the post, they do not have full clarity on what information about them will be gathered during the security check. There was an opinion that

security controls would be carried out more widely than information asked in the security control questionnaire. Neither were the investigators confident in the security of processing these data, as there were repeated breaches of personal data processing within the organization.

Based on the results of the thesis, it can be argued that the behavior of social media being investigated became more thoughtful over time, as well as paying more attention to security devices today and monitoring which auditorium the posts being examined will reach. It was not directly revealed what was the most important factor affecting the behavior of social media being investigated, but the role of the Estonian Defence forces in guiding behavioral habits was confirmed. All participants in the study perceived similar and permanent changes in their social media behavior, which are planned to be used in the future.

KASUTATUD KIRJANDUS

Alas, A. (2013). Viis asja, mida tähele panna nuhkimisskandaalidest. *Eesti Ekspress*, 7. august. Kasutatud 08.05.2019, https://ekspress.delfi.ee/kuum/viis-asja-mida-tahele-panna-nuhkimisskandaalidest?id=66552124

Andmekaitse Inspektsiooni kodulehekülg (2018). Kasutatud 14.08.2018, http://www.aki.ee/et/eraelu-kaitse/euroopa-andmekaitse-reform

Andmekaitseinspektsiooni aastaraamat 2018- avaliku teabe seaduse täitmisest ja isikuandmete kaitse tagamisest aastal 2018 (2019). Kasutatud 10.05.2019, https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Aastaraamat%202018%20kohta.%20Soovitused%20aastaks%202019.pdf

Cormode, G., Krishnamurthy, B. (2008). Key differences between Web 1.0 and Web 2.0. *First Monday*, *13*(6). Kasutatud 10.05.2019, https://ojphi.org/ojs/index.php/fm/article/view/2125/1972

Coser, L.A. (1974). Greedy Institutions: Patterns of Undivided Commitment, *History: Reviews of New Books*, 2:8, 207-208, DOI: 10.1080/03612759.1974.9946454

Eurobaromeetri eriuuring 359: Attitudes on Data Protection and Electronic Identity in the European Union. (2011). *Euroopa Komisjon*. URL: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

Finn, R., Wright, D., Friedewald, M. (2013). *Seven types of privacy*. European Data Protection: Coming of Age, lk 1-26. Kasutatud 16.08.2018, https://www.researchgate.net/profile/Michael_Friedewald2/publication/258892458_Seven_Types_of_Privacy/links/0c9605295d271f1575000000/Seven-Types-of-Privacy.pdf

Füüsilise isiku täiesti salajase, salajase või konfidentsiaalse taseme riigisaladusele juurdepääsu loa taotleja ja juurdepääsuloa kehtivusaja pikendaja ankeet (p.a). Kasutatud 13.08.2018, https://www.kapo.ee/sites/default/files/public/content_page/Taotleja%20ja%20pikendaja%20ankeet%20(f%c3%bc%c3%bcsiline%20isik)_0.docx

Global social networks ranked by number of users 2019. (2019). Kasutatud 21.05.2019, https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

Greenwald, G., MacAskill, E. (2013). Edward Snowden: ma ei taha elada ilmas, kus kõik mu tehtu ja öeldu talletatakse. *Eesti Päevaleht*, 11. juuni. Kasutatud 08.05.2019, https://epl.delfi.ee/valismaa/edward-snowden-ma-ei-taha-elada-ilmas-kus-koik-mu-tehtu-ja-oeldu-talletatakse?id=66269340

Hirsjärvi, S., Remes, P. ja Sajavaara, P. (2010). *Uuri ja kirjuta*. Tallinn: Medicina.

Hudson, M. (2018). What is Social Media? Kasutatud 11.09.2018, https://www.thebalancesmb.com/what-is-social-media-2890301

Isikuandmete kaitse seadus (16.01.2016). *Riigi Teataja I*. Kasutatud 14.08.2018, https://www.riigiteataja.ee/akt/106012016010?leiaKehtiv

Isikuandmete kaitse üldmäärus (2016). Kasutatud 14.08.2018, https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32016R0679

Joinson, Adam, N. (2008). "Looking at“, "Looking up“ or "Keeping up with’ People? Motives and Uses of Facebook. *CHI '08 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Florence, Italy. Kasutatud 16.08.2018, https://digitalwellbeing.org/downloads/Joinson_Facebook.pdf

Juhend kaitseväelaste osalemiseks sotsiaalmeedias. (2011). Kasutatud 21.03.2019

Julgeolekuasutuste seadus (01.07.2017). *Riigi Teataja I.* Kasutatud 14.08.2018, https://www.riigiteataja.ee/akt/105052017002?leiaKehtiv

Kalmus, V. (2015). Kvalitatiivne sisuanalüüs. V. Kalmus, A. Masso M.Linno (toim), *Sotsiaalse analüüsi meetodite ja metodoloogia õpibaas*. http://samm.ut.ee/kvalitatiivne-sisuanalyys

Kelt, T. (2009). *Eesti Rahvusringhäälingu raadiointervjuude intervjueerimispraktikad.* Magistritöö. Tartu Ülikool, ajakirjanduse ja kommunikatsiooni instituut

Kempel, G. (2014). *Sotsiaalmeedia töösuhtes: tööandjate hinnangud ning kogemused*. Magistritöö. Tartu Ülikool, sotsiaal- ja haridusteaduskond, ühiskonnateaduste instituut

Laherand, M-L. (2008). *Kvalitatiivne uurimisviis*. Tallinn: Infotrükk OÜ.

Loonde, E., Riives, A., Tismus, M, A., Saar, C., Randoja, M., Köidam, L.,… Rosenberg, S. (2018). Kaitseväe salajased dokumendid rippusid aastaid avalikult internetis. *Eesti Päevaleht,* 9. november. Kasutatud 18.03.2019, https://epl.delfi.ee/news/eesti/kaitsevae-salajased-dokumendid-rippusid-aastaid-avalikult-internetis?id=84260115

Lõhmus-Ein, K. (2004). *Eraelu ja selle elementide õiguslik kaitse*. Magistritöö. Tartu Ülikool, Õigusteaduskond.

MacAskill, E., Hern, A. (2018). Edward Snowden: The people are still powerless, but now they're aware. *The Guardian*, 04. juuni. Kasutatud 08.05.2019, https://www.theguardian.com/us-news/2018/jun/04/edward-snowden-people-still-powerless-but-aware

Marwick, A. (2012). The Public Domain: Surveillance in Everyday Life. *Surveillance and Society*, 9(4), lk 378-393. Kasutatud 04.01.2018, http://www.a51.nl/storage/pdf/4342_7878_1_PB1.pdf

McCullagh, K. (2005). Identity information: the tension between privacy and the societal benefits associated with biometric database surveillance. *Ettekanne, 20th BILETA Conference, Belfast,* 28. aprill Kasutatud 23.08.2018, http://bileta.nsdesign7.net/content/files/conference%20papers/2005/Identity%20Information%20%20The%20Tension%20Between%20Privacy%20and%20the%20Societal%20Benefits%20Associated%20With%20Biometric%20Database%20Surveillance.pdf

Mitrou, L., Kandias, M., Stavrou, V., Gritzalis, D. (2014) Social media profiling: a panopticon or omniopticon tool? *Ettekanne, The 6th biannual surveillance and society conference, Barcelona, Hispaania,* 24.-26.aprill

Murumaa-Mengel, M., Laas-Mikko, K., Pruulmann-Vengerfeldt, P. (2014). Privaatsusõigus inimõigusena ja igapäevatehnoloogiad. *Inimõiguste instituudi uuring 2014.* Kasutatud 12.01.2019,

https://www.humanrightsestonia.ee/inimoiguste_uuringud/privaatsus-inimoigusena-ja-igapaevatehnoloogiad/

Nissen, T.E. (2015). *Sotsiaalmeedia kasutamine relvasüsteemina.* Tallinn: Tallinna Raamatutrükikoda

Number of daily active Instagram Stories users from October 2016 to June 2018 (in millions). (2018). Kasutatud 11.09.2018, https://www.statista.com/statistics/730315/instagram-stories-dau/

Number of monthly active Facebook users worldwide as of 2nd quarter 2018 (in millions). (2018). Kasutatud 11.09.2018, https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

Number of monthly active Twitter users worldwide from 1st quarter 2010 to 2nd quarter 2018 (in millions). (2018). Kasutatud 11.09.2018, https://www.statista.com/statistics/282087/number-of-monthly-active-twitter-users/

Palm, E. (2009). Privacy Expectation at Work – What is Reasonable and Why? *Ethic Theory Moral Practice 2009/12,* No 2

Peeterson, M. (2012). *Töötaja privaatsusõigus ja selle piiramine töösuhetes*. Magistritöö. Tartu Ülikool, õigusteaduskond.

Punamäe, S. (2019). President otsustas: kaitsevägi ei saa suuremaid jälitamisõigusi. *Postimees*, 7. märts. Kasutatud 18.03.2019, https://www.postimees.ee/6539807/president-otsustas-kaitsevagi-ei-saa-suuremaid-jalitamisoigusi

Riigisaladuse ja salastatud välisteabe seadus (01.07.2018). *Riigi Teataja I*. Kasutatud 13.08.2018, https://www.riigiteataja.ee/akt/113032019150?leiaKehtiv

Rosen, J. (2004). The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age. Kasutatud 23.08.2018, http://www.antoniocasella.eu/nume/rosen_2004.pdf

Rämmer, A. (2014). Mugavusvalim. K. Rootalu, V. Kalmus, A. Masso, ja T. Vihalemm (toim), *Sotsiaalse analüüsi meetodite ja metodoloogia õpibaas*. http://samm.ut.ee/valimid

Smith, J. H., Milberg, S. J., Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns About Organizational Practices. *MIS Quarterly*, 1996, Vol. 20, Issue 2, lk 167-196. Kasutatud 08.05.2019, http://130.18.86.27/faculty/warkentin/SecurityPapers/Merrill/SmithMilbergBurke1996_MISQ_InfoPrivacy.pdf

Solove, D. J. (2002). Conceptualizing Privacy. *California Law Review*, 90, lk 1087–1155. Kasutatud 23.08.2018, https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1408&context=californialawreview

Srinivasan, D. (2018). The Antitrust Case Against Facebook. Kasutatud 14.09.2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3247362

Sweeney, L. (2002). k-Anonymity: A Model for Protecting Privacy. *International Journal of Uncertainty, Fuzziness & Knowledge-Based Systems*, vol 10, issue 5, lk 557-570. Kasutatud 15.08.2018, https://epic.org/privacy/reidentification/Sweeney_Article.pdf

Tamm, D. (2014). *Isikuandmete kaitse põhimõtted*. Magistritöö. Tartu Ülikool, õigusteaduskond.

Tavani, H. T. (2008). Informational Privacy: Concepts, Theories, and Controversies. *The Handbook on Information and Computer Ethics* (lk 131-164). New Jersey: Wiley

Tihanov, S. (2015). *Privaatsus ja isiklik informatsioon organisatsioonisisestes suhetes*. Magistritöö. Tartu Ülikool, majandusteaduskond.

Vidili, A., Artini, C. (2010). The change of Surveillance and its issues. Privacy, sense of self and Facebook as a case on study. University of Aarhus, information and media studies. https://en.calameo.com/read/001087220b1a7a09fa247

Wirth, R. (2004). *Lewin/Schein's Change Theory.* Kasutatud 22.04.2019, https://www.researchgate.net/profile/Ross_Wirth/publication/237112705_LewinSchein%27s_Change_Theory/links/5ad4cb97a6fdcc29358091db/Lewin-Scheins-Change-Theory.pdf?origin=publication_detail

Õunapuu, L. (2014). *Kvalitatiivne ja kvantitatiivne uurimisviis sotsiaalteadustes*. Tartu: Tartu Ülikool

LISAD

Lisa 1. Julgeolekukontrolli ankeedis taotleja kohta küsitud andmete loetelu

- Isikuandmed – nimi, sünniaeg, sünnikoht, isikukood, varasemad nimed, nende ajavahemik ja muutumise põhjus;
- Kontaktandmed ja kasutajakontod – viimase viia aasta jooksul loa taotleja kasutuses või nimel olnud laua- või mobiiltelefoni numbrid, kõnekaardi numbrid, erinevad SIM-kaardi numbrid, elektronposti aadressid, elektrooniliste suhtlusvõrgustike ja kõne – või sõnumirakenduste kasutajanimed või muud identifitseerivad tunnused;
- Kodakondsus;
- Elukohad – ajalises järjestuses viimase 7 aasta jooksul;
- Perekondlikud ja tutvussidemed: perekonnaseis, abikaasa või elukaaslase nimi sünniaeg ja –koht, isikukood, tema kodakondsus, varem kasutatud nimed, suhte alguskuupäev, kaaslase kontaktandmed; vanemate, kasuvanemate, õdede-vendade, laste, abikaasa või elukaaslase vanemate, kasuvanemate, õdede-vendade ja laste isikuandmed, kontaktandmed ning töö- ja ametikoht, lisaks tuleb nimetada kaks lähemat tuttavat isikut, kes taotlejat lähemalt tunnevad ja iseloomustada oskavad;
- Hariduskäik – alates algastmest, sealhulgas lõpetamata koolid, osalemine koolitustel, seminarides ja töögruppides, mis toimusid EL või NATO liikmesriigis või väljaspool neid;
- Varasem tööalane tegevus, sh välisriikides, ajalises järjestuses – tööandja nimi, töösuhte algus ja lõpp, ametikoht tööandja juures, otsese ülemuse nimi, töölt lahkumise põhjus, tööandja aadress ja kontaktandmed;
- Sõjaväeteenistus – väeosa nimi, andmed ja asukoht, teenistuse ajavahemik, väeliik, auaste ja eriala;
- Kontaktid välisriikidega – ajalises järjestuses viimase 10. aasta jooksul külastatud välisriigid, reisi aeg, eesmärk ja riik;

- Osalemine ühingutes/organisatsioonides/ühistegevustes/liikumises – ühingu, organisatsiooni, partei, erakonna või muu osaluse nimi, asukoht, liitumise või lahkumise aeg ning staatus;

- Tervis ja eluviis – psühhiaatri või psühholoogiga konsulteerimise aeg ja kirjeldus, alkoholi tarvitamisest põhjustatud probleemide kirjeldus, narkootikumide ja psühhotroopsete ainete kasutamise kirjeldus, hasartmängude mängimise kirjeldus;

- Karistused – andmed distsiplinaar-, haldus-, väärteo- või kriminaalkaristuste kohta;

- Varanduslik seis – andmed kinnisvara, aktsiate ja väärtpaberite, täiendavate tuluallikate, transpordivahendite kohta, sealhulgas pangakonto numbrid ning andmed digitaalraha kasutamise või omamise kohta;

- Harrastused ja erihuvid. (Füüsilise isiku…, p.a)

Lisa 2. Intervjuu kava

Sotsiaalmeediakontode ja selle kasutusharjumuste täpsustamine

1. Millised sotsiaalmeedia kontod sul olemas on? (Hetkel, varasemalt)
2. Milline on peamine sotsiaalmeedia konto, mida sa kasutad?
3. Kui kaua sa umbes oled erinevate sotsiaalmeedia platvormide kasutaja olnud?
4. Kirjelda oma tavapärast sotsiaalmeediakasutust.
5. Millisteks tegevusteks sa tavaliselt sotsiaalmeediat kasutad? Otsid näiteks mingit informatsiooni?
6. Millist informatsiooni sa tavaliselt sotsiaalmeedias jagad? Enda kohta? Teiste kohta?
7. Meenuta palun oma sotsiaalmeedia kasutuse kujunemist. Kas su kasutusharjumised ja jagatav info on ajas muutunud? Too mõned näited.
8. Mis need muutused sinu arvates põhjustas?

Intervjueeritava arvamus privaatsusest ja isiklikest andmetest

9. Palun kirjelda oma sõnadega, mida tähendab Sinu jaoks mõiste avalikkus/avalik informatsioon?
10. Palun kirjelda oma sõnadega, mida tähendab Sinu jaoks mõiste privaatsus/privaatne informatsioon?
11. Mida sa pead privaatseks sotsiaalmeedia kontekstis?
12. Kui palju sa mõtled üldse privaatsusele igapäevastes toimingutes sotsiaalmeedias?
13. Milliste andmete osas tunned, et tegu on privaatsete andmetega? Mida sa näiteks mitte iial sotsiaalmeedias ei jagaks?
14. Oled sa näinud, et sinu tutvusringkonnas inimesed jagavad midagi sellist?
15. Sinu kolleegide puhul, mida oled märganud?
16. On sul mingeid kartusi netis privaatsetel teemadel suheldes?
17. Milliseid võtteid sa enda postituste ja oma sotsiaalmeedia kontode privaatsuse kaitsmiseks kasutad?
18. Kas turvaseaded on sul kogu aeg olnud samad või oled neid aja jooksul muutnud? Kuidas?
19. Kaitseväes on kehtestatud sotsiaalmeedia kasutusjuhend. Kui palju sa sellest mäletad? Too mõned näited seal kehtestatud olulisematest teemadest sinu jaoks.

20. Kui palju sa oma sotsiaalmeediaga seotud tegevustes lähtud Kaitseväes kehtestatud sotsiaalmeedia juhendist?

Intervjueeritava suhtumine julgeolekukontrolli teostamisse

21. Kui sa läksid Kaitseväkke tööle, siis mida see sinu jaoks tähendas just selle julgeolekukontrolli ja sotsmeedia mõttes? Mida siis tehti?

22. Mitu korda sa oled julgeolekukontrolli läbinud?

23. Meenuta palun oma julgeolekukontrolli vestlust/vestluseid. Kas sa valmistusid selleks/nendeks kuidagi?

24. Kirjelda palun, milliseid tundeid julgeolekukontrolli teostamine sinus tekitas.

25. Kuidas suhtud sellesse, et sinu sotsiaalmeedia kontol olev info vaadatakse julgeolekukontrolli käigus julgeolekuasutuse poolt põhjalikult läbi?

26. Millal on sinu arvates lubatud inimeste tegevust sotsiaalmeedias jälgida? Kas mingite teatud gruppide, indiviidide, mingis teatud olukorras, vms?

27. Millised ohud võivad kaasneda sellega, kui inimesi jälgitakse sotsiaalmeedias?

28. Kas tead, millist informatsiooni tööandja/KAPO sinu kohta kogub ja talletab?

29. Kuidas suhtud sellesse, et tööandja/KAPO kogub ja talletab sind puudutavat informatsiooni?

30. Seoses sinu kohta kogutavate isikuandmetega, kui palju sa oled kursis isikuandmete kaitse nõuetega ja enda õigustega/võimalustega oma andmete kaitsmiseks?

31. Meenub sulle mõni olukord, kus sinu arvates on isikuandmete kaitse põhimõtteid rikutud? Sinu puhul, teiste puhul? Palun kirjelda.

32. Oled kuulnud mõnest juhtumist, kus su töökaaslane on sattunud sarnasesse olukorda?

33. Kus/millised on sinu arust peamised võimalused isikuandmete kaitse nõuete rikkumisteks Kaitseväes?

34. Kus/millised on sinu arust peamised võimalused isikuandmete kaitse nõuete rikkumisteks julgeolekukontrolli teostamisel?

35. Kui suures ulatuses sinu arust võiks tööandja töösuhte korraldamiseks sinu privaatsete andmetega tutvuda?

36. Kuidas sa suhtud sellesse, et Kaitsevägi soovib täiendavaid õiguseid taustakontrolli teostamiseks? Mis sellega võiks sinu arust kaasneda?

Intervjueeritava poolt tajutud muutused sotsiaalmeedia käitumises

37. Kas julgeolekukontroll ja KV liikmeks olemine pani sind sotsiaalmeedias kuidagi teisiti käituma? Kuidas?

38. Oskad sa lühidalt võrrelda enda sotsiaalmeediakäitumist enne ja pärast julgeolekukontrolli läbimist?

39. Palun too välja peamised muutused oma sotsiaalmeediakäitumises, mis ilmnesid peale julgeolekukontrolli läbimist.

40. Kas soovitad omandatud muudatusi ka teisele? Näiteks oma lastele, perele, sõpradele? Annad neile näpunäiteid?

41. Enam Sa ei tööta riigisaladuse luba nõudval ametikohal ja julgeolekukontrolli sulle ei kohaldata, millised on sinu sotsiaalmeedia käitumisharjumused nüüd võrreldes julgeolekukontrolli järgse ajaga? (Kas need muutused olid pigem lühiajalised või muutusid su käitumisharjumused püsivalt?)

42. Kas soovid midagi veel lisada selle teema kohta, mille kohta ma ei taibanud küsida, aga mis on sinu arvates oluline?

Tänan, et leidsid aega vastamiseks!

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, **Monika Prants**

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose
„**Julgeolekuasutuse kõrgendatud tähelepanu all olemise tajutud mõju inimeste sotsiaalmeediakäitumisele“**,
mille juhendaja on **Maria Murumaa-Mengel**, PhD,

   reprodutseerimiseks eesmärgiga seda säilitada, sealhulgas lisada digitaalarhiivi DSpace kuni autoriõiguse kehtivuse lõppemiseni.

2. Annan Tartu Ülikoolile loa teha punktis 1 nimetatud teos üldsusele kättesaadavaks Tartu Ülikooli veebikeskkonna, sealhulgas digitaalarhiivi DSpace kaudu Creative Commonsi litsentsiga CC BY NC ND 3.0, mis lubab autorile viidates teost reprodutseerida, levitada ja üldsusele suunata ning keelab luua tuletatud teost ja kasutada teost ärieesmärgil, kuni autoriõiguse kehtivuse lõppemiseni.

3. Olen teadlik, et punktides 1 ja 2 nimetatud õigused jäävad alles ka autorile.

4. Kinnitan, et lihtlitsentsi andmisega ei riku ma teiste isikute intellektuaalomandi ega isikuandmete kaitse õigusaktidest tulenevaid õigusi.

Monika Prants
31.05.2019