TARTU ÜLIKOOL

Sotsiaalteaduste valdkond

Ühiskonnateaduste instituut

Ühiskonna ja infoprotsesside analüüsi õppekava

Kati Randma

Riigipoolse digijälgimise aktsepteeritavus ja seosed internetikäitumisega

Magistritöö

Juhendaja: prof. Veronika Kalmus

Tartu 2023

SISUKORD

SISSEJUHATUS

Digitaalmeedia kasutamisulatus on tänasel päeval kasvanud äärmiselt suureks ja järk-järgult liigub üha enam inimeste igapäevategevustest just digiplatvormidele. Me kasutame neid lahendusi, et muuta elu mugavamaks ja kiirendada protsesse, mille peale kuluks muidu tunduvalt rohkem väärtuslikku aega. Kuigi digilahendused aitavad meie elu muuta lihtsamaks, on sellel ka peidetum külg, millele nii palju tähelepanu tihti ei pöörata. Kõigist meie tegevustest erinevatel digiplatvormidel jääb maha jälg (Büchi jt, 2020) ning sageli jääb varjatuks kes, kuidas ning millisel eesmärgil meie andmeid hiljem kasutab.

Oma andmete üle kontrolli omamine sõltub nii andmekogujast kui ka igast inimesest endast. Oluline on andmekogujate tegevuse läbipaistvus ehk kas ollakse konkreetsed ja ausad oma eesmärkidest rääkides ning andmekogumise, -töötlemise, hoidmise ja kasutamise suhtes. Teine küsimus on inimeste enda kontroll selle üle, milliste tingimustega nõustutakse erinevaid digiplatvorme kasutades. Tihti on äppide ja veebilehtede kasutustingimused liiga pikad ja keerulised, et inimesed neid loeksid ning aru saaksid, milliseid vabadusi vabatahtlikult näiteks sotsiaalmeedias tingimuste aktsepteerimisel loovutatakse (Smith, 2014). Teadmatus, mida meie andmetega tegelikult tehakse, võibki põhjustada olukorra, kus inimesed ei oska probleemi üle muret tunda, samas tänapäevases andmestunud maailmas ei saa sellest küsimusest mööda vaadata.

Kui aastakümneid on peamiseks murekohaks isiklike andmete ja privaatsuse küsimuses olnud pigem andmete äriline ärakasutamine (ettevõtete suunatud reklaamid jms), siis peale mitmeid privaatsus- ja jälgimisskandaale on aina enam hakatud tähelepanu pöörama asjaolule, et valitsuste seiretegevus ja turvapoliitikad võivad samuti endaga kaasa tuua suuri privaatsusriske ja ohustada inimeste õigusi (Wilton, 2017). Üks suuremaid ja tuntumaid skandaale on Edward Snowdeni paljastused valitsuste massjälgimiste kohta (Lyon, 2015) või 2016. aasta USA presidendivalimiste juhtum, kus president Trumpiga seotud andmeanalüüsifirma Cambridge Analytica lõi tarkvara prognoosimaks ja mõjutamaks valijate valikuid, varastades selleks ligi 50 miljoni Facebooki kasutaja profiililt andmeid (Cadwalladr ja Graham-Harrison, 2018).

Valitsused teostavad järelevalvet, analüüsides ja vahetades üha suuremas koguses teavet oma kodanike kohta, kasutades selleks andmekaevetööriistu, et tuvastada huvipakkuvaid isikuid (Brown, 2014). Suuremat pilti vaadates on privaatsus seega midagi enamat kui üksikisiku mure - see on vabade demokraatlike ühiskondade toimimise funktsionaalne eeldus (Büscher jt, 2015). Kuid massilist andmete kogumist digitaalses meedias on järjest enam hakatud pidama ohuks demokraatiale.

Covid pandeemia tõi 2020. aastal endaga kaasa erakorralised meetmed haiguse leviku tõkestamiseks. Barriga (2020) tõstatas olulise küsimuse – kas need meetmed, mida rakendati pandeemia ajal, võivad jääda ka püsivalt ühiskonda eksisteerima? Ning kui jah, siis millised on selle tagajärjed privaatsusele ja demokraatiale? Göteborgi ülikooli demokraatia aruande (Lührmann jt, 2020) kohaselt, milles uuriti ülemaailmses mastaabis õiguste ja vabaduste piiramise kaudu pandeemia ohjeldamiseks mõeldud erakorraliste meetmete mõju demokraatiale, täheldati demokraatia nõrgenemist vähemalt 82 riigis. Ühe ekstreemse näitena saab tuua Ungari, kus võitlus koroonaviiruse vastu hõlmas muuhulgas nende isikute vahistamist, kes kritiseerisid peaminister Viktor Orbanit sotsiaalmeedia vahendusel (Sandford, 2020).

Kriisiolukorras võivad uued jälgimissüsteemid olla legitimeeritud ning nende kasutamine jätkub seega ka peale kriisi seljatamist. Sellisel juhul on tegemist nö hiiliva jälgimistegevusega (*surveillance creep)*, mis tähendab, et konkreetsel eesmärgil kasutusele võetud tööriista hakatakse kasutama muudel eesmärkidel (Marx, 2005). See aga ohustab privaatsust ning poliitilisi ja kodanikuõigusi. Eurobaromeetri (Euroopa Komisjon, 2015) uuringust selgus, et eestlased kuuluvad Euroopas nende hulka, kes tunnevad kõige vähem muret, kui ametiasutused ja eraettevõtted peaksid kasutama nende isiklikke andmeid muudel eesmärkidel, kui selleks, mille jaoks neid algselt koguti. Selline tulemus võib viidata asjaolule, et Eesti inimesed pole sellise hiiliva jälgimistegevuse tagajärgedest eriti informeeritud ega tea, mida see endaga kaasa võib tuua.

Kuid nii nagu mujal maailmas, tõi pandeemia ka Eestis riigipoolse digitaalse jälgimise küsimuse tugevamalt inimeste teadvusesse. Kõige rohkem kerkis teema esile liikuvusanalüüsi kontekstis, mille eesmärgiks oli mobiilioperaatorite kaudu jälgida inimeste liikumist 2020. aasta kevadel, kontrollimaks, kuidas elanikud rakendavad eriolukorra meetmeid (Statistikaamet, 2020; ERR, 2020). Kuigi andmekaitse inspektsiooni (AKI) hinnangul oli kõik õiguspärane (ERR, 2020), siis taoline uuring pani paljud inimesed küsima, kui eetiline ja seaduspärane selline isiklike andmete jälgimine ikkagi on. Lisaks arendati välja koroonaäpp HOIA, mis esialgu valmistas ka AKI-le muret, sest pandeemia alguses polnud teada, kas nendest äppidest ka tegelikult mingit kasut oleks või riivaksid need hoopis inimeste põhiõigusi ja -vabadusi (Liive, 2020).

Praegust olukorda digitaalses jälgimises tajutakse seega erinevalt, kuna ei teadvustata lõpuni välja, mida meie andmetega tehakse. Oma magistritöös püüangi saada selgust, milline on üldine tolerantsus riigipoolse digijälgimise suhtes, millest see sõltuda võiks, mil määral on inimesed valmis loobuma oma privaatsusest, et aidata võitluses pandeemia või ka mõne muu ohu korral,

ning kuidas võiks digijälgimise aktsepteeritavus olla seotud internetiosaluse ja privaatsuskäitumisega.

Magistritöö koosneb viiest suuremast osas, milles esimeses annan ülevaate teemakohasest teooriast ja varasematest empiirilistest uurimustest. Töö teises osas toon välja uurimisprobleemi, peamised uurimisküsimused ning hüpoteesid vastavalt teoreetilisele raamistikule. Kolmandas osas kirjeldan töö metoodikat. Neljas osa koosneb analüüsist, mille käigus püüan testida töös sõnastatud hüpoteese risttabelite, keskmiste võrdluse ja multinomiaalse regressioonanalüüsi kaudu, ning viies osa sisaldab järeldusi ja diskussiooni. Analüüs põhineb rahvusvahelise projekti „Sotsiaalmeedia jälgimine ja autoritarismikogemused“ (Bolin, Kalmus jt, 2023) andmetel ning töö põhifookuses on Eesti tulemused, mida võrdlen ka kahe teise uuringus osalenud riigi – Rootsi ja Portugali – tulemustega.

1 TEOREETILINE JA EMPIIRILINE TAUST

Lyon (2001) on väitnud, et infoühiskond on jälgimisühiskond, sest infotehnoloogiad nii lihtsustavad kui ka nõuavad isiklike andmete kogumist. Jälgimist võib olla kahte liiki - füüsiline (nt turvakontroll riigipiiril) ja digitaalne (Nam, 2019). Digitaalne jälgimine on mistahes süstemaatiline ja rutiinne tähelepanu kellegi isiklikele üksikasjadele mingil määratletud eesmärgil kasutades digitaaltehnoloogiat (Lyon, 2015). Peale 2001. aasta 9. septembri terrorirünnakuid hakkasid läänemaailm ja Euroopa Liidu riigid ajama oluliselt aktiivsemalt poliitikat, mis toetus palju suuremal määral jälgimisele orienteeritud turvatehnoloogiatele (Pavone ja Degli-Esposti, 2010). Valitsuste digitaalse jälgimise poliitikate ja meetmete hulka kuuluvad üldjuhul kodanike kommunikatsiooni jälgimine (kogudes ja analüüsides inimeste kõnelogisid, e-kirju ja informatsiooni sotsiaalmeediakanalitest), asukoha määramine mobiiltelefonide geolokatsiooni järgi, visuaalne jälgimine avalike kaamerate kaudu (*CCTV*), mere- ja lennureisijate andmete kogumine ja analüüsimine ning biomeetriline isikutuvastamine (nt sõrmejälje või näotuvastuse kaudu) (Nam, 2019; Trüdinger ja Steckermeier, 2017).

Kodanike jälgimiseks mõeldud turvatehnoloogiaid peetakse ühest küljest turvalisust suurendavateks, kuid samal ajal ka privaatsust rikkuvateks. Seetõttu eeldatakse, et inimesed peaksid vahetama osa oma privaatsusest kõrgema turvalisuse vastu. Tegemist on nn *trade-off* ehk vahetustehingu lähenemisega (Pavone & Esposti, 2010). Ka globaalse riskijuhtimise vaatepunktist (Spence, 2005) tagatakse turvalisem ühiskond läbi turvapoliitikate, mis sõltuvad üha enam turvatehnoloogiate ja omavahel ühendatud andmevahetussüsteemide kasutuselevõtust, eesmärgiga seeläbi muuta tundmatud ohud prognoositavateks sündmusteks (Amoore, 2006; Lyon, 2007; Zureik ja Hindle, 2004).

Riigipoolne jälgimine pälvis uue teadusliku tähelepanu seoses interneti ja muu arenenud info- ja kommunikatsioonitehnoloogia (IKT) tulekuga, mis suurendab tohutult valitsuste jõudu, ulatust ja suutlikkust jälgida oma elanikkonda (Lyon, 2007).

1.1 Jälgimine tänapäevases (digi)ühiskonnas – demokraatia ja autoritaarsuse seosed

Mitmed autorid on viidanud, et jälgimistegevuse ja autoritaarsuse vahel on kausaalne seos (nt Hadjimatheou, 2013) ning järeldanud, et riigipoolne jälgimistegevus võib kujutada ohtu liberaalsetele demokraatlikele ühiskondadele. Tänapäeval teavad meie valitsused meist tänu

tehnoloogia arengule rohkem, kui enamik totalitaarseid režiime võisid kunagi varem loota teada oma kodanike kohta (Grayling, 2007).

Hadjimatheou (2013) järgi saab lihtsustatult öelda, et liberaalsete demokraatiate eesmärk on esindada rahvast ja valitseda viisil, mis on kooskõlas üksikisikute vabaduse, autonoomia ja võrdsuse austamisega. Seevastu autoritaarsete valitsuste eesmärk on juhtida ja hallata inimesi viisil, mis tagab nende vastavuse riigi seatud eesmärkidega (Hadjimatheou, 2013). Autoritaarsetes ühiskondades kasutatakse inimeste jälgimist, küberrünnakuid ja desinformatsiooni, et tugevdada oma võimu ja laiendada seda üle piiride (Morozov, 2011). Samuti toetutakse üha enam eraettevõtetele, kes haldavad erinevaid platvorme ja infrastruktuure ning pakuvad valitsustele tarkvara ja tehnilisi teadmisi (Michaelsen ja Glasius, 2018). Jälgimine toimub autoritaarsel viisil, kui tegu on salajase jälgimisega, jälgimisega väljaspool õiguslikku raamistikku, jälgimistegevusega, mille üle teostatakse halba järelevalvet jms (Hadjimatheou, 2013).

Reeglina on kaasaegsed jälgimissüsteemid demokraatlike ideaalidega vastuolus, seda nii oma ülesehituselt kui ka rakenduselt, sest individualiseerivad, objektiseerivad ja kontrollivad inimesi viisil, mis tekitab sotsiaalset ebavõrdsust, hägustavad läbipaistvuse puudumise tõttu sotsiaalseid kontekste ning inimesed ei ole suures osas teadlikud süsteemide toimimisest ega oma õigustest (Monahan, 2010). Kuid see ei tähenda, et jälgimissüsteemide kasutamine valituste poolt viitaks automaatselt autoritarimisi suunas liikumisele, vaid seda saab ära hoida, rakendades liberaalset demokraatlikku järelevalvet (Hadjimatheou, 2013). Demokraatlik järelevalve tähendab jälgimise kontrollifunktsioonide tahtlikku rakendamist õigluse ja võrdsuse sotsiaalsetel eesmärkidel (Monahan, 2010).

Kuigi jälgimine ei tähenda automaatselt vastuolu liberaalse demokraatia põhimõtetega, on lähiminevikust teada mitmeid suuremaid skandaale, kus demokraatlikud valitsused on kasutanud autoritaarseid jälgimise meetodeid. 2013. aastal avalikustas Edward Snowden, kuidas juhtivates Lääne demokraatlikes riikides toimus inimeste massjälgimine, mis tõestas, et läbipaistmatud ja salajased jälgimisviisid ei kuulu ainult autoritaarsete režiimide praktikate hulka (Bauman jt, 2014; Lyon, 2015). Hiljutisem näide on mobiilinumbrite häkkimiseks kasutatava nuhkvara Pegasus kasutamine mitmete riikide valitsuste poolt (Pegg, ja Cutler, 2021; in ‘t Veld, 2022). Tegemist on Iisraeli ettevõtte NSO poolt loodud võimsa nuhkvaraga, mis võimaldab sihikule võetud mobiiltelefoni kaudu ligi pääseda praktiliselt kogu sealsele informatsioonile (nt fotodele, videosalvestustele, kontaktandmetele ja sõnumitele) ja seda ilma, et mobiili kasutaja peaks kuhugi andmepüügi lingile vajutama. Teadaolevalt on nuhkvara kasutatud valitsuse vastaste aktivistide,

ajakirjanike ja poliitiliste isikute jälgimiseks (in ‘t Veld, 2022). Ka Eesti valitsus oli 2018. aastal huvitatud Pegasuse ostmisest, lootes seeläbi häkkida Venemaa mobiilinumbritesse (Kirchgaessner, 2022), ning tehes ka esialgse sissemakse 30 miljoni dollari ulatuses (in ‘t Veld, 2022). Tehing jäi aga katki, sest Iisraeli kaitseministeerium keeldus müümast tarkvara, kui seda kasutatakse Venemaa vastu, kartes selle tõttu ise suhete halvenemist Venemaaga (Kirchgaessner, 2022).

Covid-19 pandeemia ajal otsustati kasutada nii demokraatlikes kui autoritaarsetes riikides inimeste jälgimist peamise taktikana, kontrollimaks pandeemiaga seotud informatsiooni, ning eriti murettekitav on selline olukord demokraatlikes ühiskondades, mis tugineb põhimõtetele nagu sõnavabadus ja õigus eraelu puutumatusele (Eck ja Hatz, 2020). Pandeemia tõttu on andmejälgimise ulatus väga lühikese ajaga oluliselt kasvanud ning lisandunud on andmekogumise meetodid nagu termoskännerid, GPS-põhised asukohateenused ja näotuvastussüsteemid, luues nö „uue normaalsuse“, mis põhineb läbival ja tervisepõhisel jälgimisel (Chiusi jt, 2020).

Tänapäevases digitaalses ühiskonnas on ühe andmekaitsemeetmena kasutusel olnud *end-to-end* krüpteerimine, mis tagab kindluse, et digitaalselt peetavad vestlused jääksid privaatseks ning rangelt vaid vestluses osalevate inimeste vahele. Nüüd plaanib Euroopa Liit aga vastu võtta seadust, millega keelustaks krüpteeritud sõnumite kasutamise ning peamise põhjusena tuuakse välja, et see aitaks võidelda internetis alaealiste seksuaalse kuritarvitamise vastu (Koomen, 2021). Esile on aga tõusnud debatt, kus andmekaitseekspertide sõnul kaotab selline määrus konfidentsiaalse suhtluse veebis (Kübarsepp, 2022). Kuigi määruse järgi peaks teoreetiliselt jätkuma suhtlus erinevatel suhtlusplatvormidel endiselt privaatselt ja turvaliselt, hoidudes samal ajal selle eest, et kurjategijad saaksid neid platvorme ära kasutada, tähendaks see siiski kõigile *end-to-end* krüpteeringu nõrgenemist, mis võib omakorda kahjustada kõikide internetikasutajate turvalisust ja privaatsust, sealhulgas ka nende laste turvalisust ja privaatsust, mida õigusaktidega püütakse kaitsta (Voge, 2022). Kolmandate osapoolte ligipääsetavus meie privaatsetele andmetele on seega ülimalt oluline teema, kuna me tegelikult ei saa kuidagi kontrollida, kas meie andmeid ikkagi kasutatakse riigiasutuste poolt vastavalt eesmärgile või teostatakse jälgimist oma kodanike üle tegelikult muudel põhjustel või nii öelda igaks-juhuks, kuna andmed on kergesti kättesaadavad.

Kodanike jälgimist riigiasutuste poolt õigustatakse peamiselt turvalisema ühiskonna tagamisega, kuid tegelikult puuduvad meil teadmised, kas me oleme ikka rohkem kaitstud erinevate ohtude suhtes. Need meetmed, mida rakendatakse näiteks terrorismi ennetamiseks või haiguse leviku tõkestamiseks, ei pruugigi tegelikult mingit kaitset pakkuda, kuid me ei saa seda kuidagi

kontrollida ning seeläbi usume, et teatud korraldustele alludes me saame lubatud kaitset. Schneier (2003) nimetab sellist olukorda turvateatriks (*security theater*), kus kasutusele võetud turvameetmed pakuvad näilist kaitset, kuid tegelikult teevad turvalisuse suurendamiseks väga vähe või üldse mitte midagi. Ta piltlikustab ka olukorda, kuidas büroohoonetes on tihti fotoga isikut tõendava dokumendi kontrollid, kuid keegi pole kunagi selgitanud, miks sellise dokumendi olemasolu kontrollimine tegelikku turvalisust pakub ning pigem tundub, et turvalisus on see, kui vormiriietuses palgatud valvur vaatab ID-kaarte (Schneier, 2009). Sama olukord võib olla digitaalsel jälgimisel, kus näiteks haiguse leviku tõkestamise eesmärgil võetakse kasutusele äpp, mis jälgib sinu liikumisi, kuid kas haiguse levik ka tegelikult pidurdub just nimelt selle äpi kasutusele võtmise tõttu, ei ole tegelikult otseselt teada. Kuna see rakendus on aga just sellel eesmärgil kasutusele võetud ja riigiasutuste poolt sellisena põhjendatud, siis me tihti usumegi, et see on meie kaitseks vajalik, saamata tegelikult selle kohta konkreetset kinnitust.

Andmejälgimine võib lõpuks viia muuhulgas ka selliste problemaatiliste tagajärgedeni nagu enesetsensuur, konformism ja ennetav kuulekus (Büchi jt, 2022). See tähendab, et mida suurem on inimeste teadlikkus selle üle, et nende tegevusi jälgitakse, seda enam võidakse hakata piirama oma tegevusi ja käituma vastavalt tajutud ühiskondlikele normidele (Manokha, 2018). Sellised jahutavad mõjud (*chilling effects*) pärsivad põhiõiguste teostamist ja kujutavad endast seega riski üksikisiku autonoomiale, heaolule ja demokraatlikule osalemisele digitaalsetes ühiskondades (Véliz, 2020). Kuna antud magistritöös soovin lisaanalüüsina ka jahutavate mõjude kohta uurida, siis põhjalikum kirjanduslik ülevaade selle teema kohta on toodud edasises töös, alapeatükis 1.3.

1.2 Tolerantsus riigipoolse digijälgimise suhtes

1.2.1 Riigipoolse jälgimise tajumine

Sotsiaalvõrgustikud toetuvad tihti sellele, et kasutajad jagavad vabatahtlikult rakendust kasutades enda isiklikke andmeid, eesmärgiga saada nendest interaktiivsetest teabepõhistest teenustest vastu mingit kasu (Humphreys, 2011). Varasematest uurimustest on selgunud, et inimesed üldjuhul ei tunne muret oma privaatsuse pärast senikaua kuni tunnetavad, et omavad kontrolli enda isiklike andmete üle (Humphreys, 2011; Gandy, 1989). Privaatsuse ja jälgimise teemal on veel leitud, et pigem peavad kasutajad privaatsusest rääkides silmas sotsiaalset privaatsust (Raynes-Goldie, 2010) ehk seda, millised kasutajad millist informatsiooni näevad, kuid harvem mõeldakse riigi- või ettevõtete-poolse jälgimise peale (Humphreys, 2011; Raynes-Goldie, 2010; Young ja Quan-Haase, 2013), sest sellised mured on üldiselt mittemateriaalsed või mitte tajutavad (Whitaker,

1999). Selline jälgimine võib aga potentsiaalselt viia diskrimineerimise ja sotsiaalse kontrollini (Andrejevic, 2007; Gandy, 1993).

Young ja Quan-Haase (2013) toovad oma töös veel välja, et Facebooki kasutajatel üldiselt puuduvad institutsionaalse jälgimise vastu privaatsusstrateegiad, mis kaitseksid asutuste poolt isikuandmete kasutamisest tulenevate ohtude eest, ning see omakorda viitab sellele, et isikuandmete kogumine, koondamine ja kasutamine näiteks suunatud reklaamide jaoks on muutunud aktsepteeritud sotsiaalseks normiks, millega tuleb leppida vastutasuks, et kasutada tasuta mõnda rakendust.

Kui eespool sai mainitud, et sotsiaalvõrgustike kasutajad, kes tunnetavad kontrolli oma andmete üle, tunnevad üldjuhul vähem muret oma privaatsuse pärast, siis üsna sageli võib kohata ka nn privaatsuse paradoksi (Barnes, 2006; Norberg jt, 2007), kus internetikasutajad küll väljendavad suurt muret privaatsuse pärast, kuid teevad olukorra parandamiseks ja enda kaitseks väga vähe. See võib jällegi tuleneda sellest, et kasutajad peavad privaatsuse all tihti silmas vaid sotsiaalset privaatsust puudutavaid turvameetmeid ning jätavad tähelepanuta institutsionaalse privaatsuse (Raynes-Goldie, 2010).

Young ja Quan-Haase (2013) väidavad, et privaatsuse ja andmekaevandamisega seotud sotsiaalsed normid süvenevad, kuna inimesed jätkavad suhtlemist võrgustatud digitaalsetes ruumides nagu Facebook, seevastu suhtlemist asutuste või ettevõtetega, kes seda teavet haldavad, on vähe. Võib-olla ei lase otsese suhtluse puudumine koos vähese läbipaistvusega kasutajatel mõista, millist mõju avaldab enda kohta jagatud teave institutsionaalsele privaatsusele (Young ja Quan-Haase, 2013).

Sotsiaalvõrgustike või muude digitaalsete platvormide kaudu jälgimine on tänapäeval nii laialt levinud ja käib nii automaatselt, et inimesed tihti ei tajugi seda (Meyrowitz, 2007). Samas on aga Wright ja Watson (2013) leidnud, et kuna inimestel ei ole piisavalt teadmisi uute tehnoloogiate mõjust oma privaatsusele, siis teadmiste puudumine just suurendab muret privaatsuse pärast ning seega peaksid inimesed tajuma nende üle teostatavat jälgimist paremini. Büchi jt (2022) on välja toonud, et viimastel aastatel on inimesed tänu mitmetele privaatsus – ja jälgimisskandaalidele muutunud järjest teadlikumaks, et nende üle teostatakse pidevat andmejälgimist. Samuti aitab jälgimise tajumisele kaasa isiklikust kasutusest tulenevad asjaolud ning oskused ja kogemused – näiteks arusaam, et varem kasutatud otsinguterminid viivad väga spetsiifiliste reklaamideni erinevatel platvormidel või seadmetes (Tanner, 2015).

Kalmus, Bolin ja Figueiras (2022), kes on käesoleva magistritöö aluseks oleva projekti „Sotsiaalmeedia jälgimine ja autoritarismikogemused“ läbiviijad vastavalt Eestis, Rootsis ja

Portugalis, on andmestiku põhjal samuti analüüsinud, kes ja mil määral kardab andmejälgimist, uurides suhtumist nii korporatiivsesse kui ka riigipoolsesse digijälgimisse. Minu poolt teostatav analüüs on seega edasiarendus nende töös väljatoodule, vaadates täpsemalt, mis põhjustel teostatav riigipoolne digijälgimine on rohkem ja mis põhjustel vähem aktsepteeritav. Kalmuse jt (2022) uurimusest selgus, et Eesti ja Rootsi vastajad näitasid sarnaselt üles suuremat tolerantsust riigipoolse digijälgimise suhtes kui Portugali vastajad. Selgus ka, et mõlemas riigis on aktsepteerivam pigem vanem põlvkond ning Eesti puhul toodi põhjenduseks asjaolu, et vanemal põlvkonnal on olemas vastumeelsed kogemused autoritaarses ühiskonnas elamise kohta ning seetõttu ollakse tunduvalt usaldavamad oma praeguse iseseisva riigi vastu, sest see vastandub radikaalselt Nõukogude Liidule. Kuna Kalmuse jt (2022) analüüs oli tehtud keskmiste võrdluse kaudu koondtunnusest *sallivus riigipoolse digijälgimise suhtes*, mis on üheks oluliseks tunnuseks ka minu analüüsis, siis minu eesmärgiks on hinnata üldist sallivust läbi viie väite, mis on selle koondtunnuse aluseks. Seega on teada, et Eestis ja Rootsis oli aktsepteeritavus kõrgem kui Portugalis, kuid soovin lisaks keskmistele väärtustele vaadata täpsemalt ka vastuste jaotusi, et näha, kas see kõrgem aktsepteeritavus tähistab pigem neutraalseid või selgelt aktsepteerivaid hoiakuid.

Kuigi inimeste teadlikkus digijälgimise osas on tänapäeval tänu mitmetele skandaalidele kõrgem kui kunagi varem (Büchi jt, 2022), on Preibusch (2015) toonud välja asjaolu, et skandaalidest tulenev huvi privaatsuse ja andmekaitse vastu igapäevases digitaalmeedia kasutamises on lühike ehk inimesed pööravad probleemile tähelepanu siis, kui skandaal on aktuaalne, kuid aja möödudes kipub tähelepanu teemalt hajuma. Kuna valdav osa inimestest ei pruugi siiski kursis olla või selle peale mõelda, mil määral riigipoolne digitaalne jälgimine toimub, ning selgus, et pigem tuntakse muret sotsiaalse privaatsuse pärast, siis eeldan, et ka *üldine tolerantsus riigipoolse digijälgimise suhtes võib Eestis jääda pigem neutraalsele tasemele* ehk vastajate suhtumine jääb rohkem skaala keskmiste vastuste juurde ning ei olda kindlalt jälgimise poolt ega vastu.

1.2.2 Riigipoolse jälgimise aktsepteerimine sõltuvalt eesmärgist

Ühe uurimisküsimusena soovin analüüsida, mil määral sõltub riigipoolse digijälgimise aktsepteeritavus jälgimise eesmärgist ning kas ja kuivõrd see erineb suhtumisest jälgimisse üldiselt, kui konkreetset põhjendust pole antud. Varasematest uurimustest on teada, et inimeste valmisolek leppida isikuvabaduste ja privaatsusõiguste riivamisega sõltub olukorrast tingitud teguritest, nagu näiteks silmapaistev oht (nt Davis ja Silver, 2004).

Zilleri ja Helbingi (2021) järgi on avalik toetus jälgimismeetmetele oma olemuselt „sõltuv ulatusest", mistõttu tuleb arvesse võtta nii rakendamise konteksti kui ka individuaalseid poliitilisi eelistusi. Jälgimise vajalikkusega on reaalne või tajutav oht asjakohane tingimus, mis on otseselt seotud seirepoliitika elluviimise eesmärgiga (Ziller ja Helbling, 2021). Seoses sellega näivad julgeolekuohud olevat kriitilise tähtsusega selles osas, kuidas üksikisikud toetavad näiteks terrorismivastaseid meetmeid (Huddy jt, 2002), ning samuti selles osas, kuivõrd inimesed on valmis terrorismi ennetamise nimel loobuma kodanikuvabadustest.

Seega saab kokkuvõtteks öelda, et kodanike jälgimise vajadus peaks olema selgelt tajutav, et riigipoolset jälgimist aktsepteerida (Kininmonth jt, 2018; Dinev jt, 2008). Eespool öeldust tulenevalt võib oletada, et *riigipoolne digijälgimine on aktsepteeritavam, kui sellel on konkreetne eesmärk, ning eelkõige tolereeritakse jälgimist nendel juhtudel, kus oht ühiskonnale on suurem ja tajutavam*.

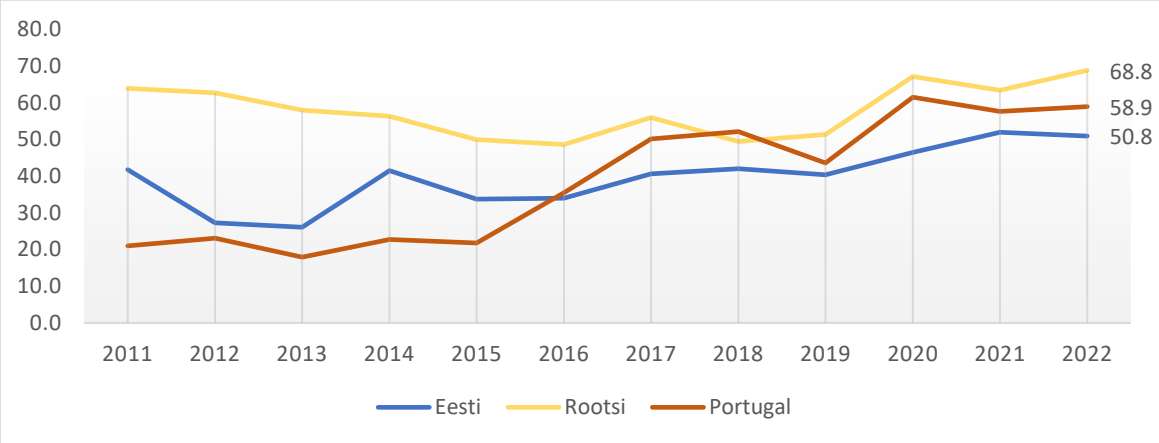
1.2.3 Riigipoolse digijälgimise aktsepteerimist kirjeldavad tegurid

Üheks oluliseks märksõnaks isikuandmetega ümberkäimisel on läbipaistvus. Läbipaistvus tähendab seda, et kõigile on üheselt ja arusaadavalt selge, kes ja milliseid andmeid kogub ning millistel eesmärkidel seda tehakse. Tegemist on seega olulise faktoriga, mis võib avaldada mõju inimeste suhtumisele nende isikuandmete kogumise osas (Nam, 2019; Wester ja Giesecke, 2019; Wright, 2017; Flyverbom jt, 2017). Kuid algusest peale on massilise jälgimise üheks suurimaks kriitikaks olnud just selle läbipaistvuse puudumine (Lyon, 2015).

Wester ja Giesecke (2019) on oma uurimuses välja toonud, et kuigi Rootsi kodanike üldised hoiakud jälgimistehnoloogiate suhtes perioodil 2009-2017 oluliselt ei muutunud, oli drastilist tõusu märgata nõudluses läbipaistvuse järele ja teisest küljest jällegi olulist langust riski tunnetamisel uute jälgimistehnoloogiate vastu. Sellised tulemused viitavad, et otseselt jälgimist ei kardeta, kuid oluline on, et inimesed teaksid, kuidas ja mille jaoks nende andmeid kasutatakse. Samuti leiti, et privaatsuse ja turvalisuse vahetustehingut ei tohiks vaadelda liiga lihtsustatult ja eeldada, et karmide turvameetmete suurendamine suurendab automaatselt ka ühiskondlikku turvalisust ning kodanikud on valmis kergekäeliselt tegema kompromissi privaatsuse ja turvalisuse vahel. Tegelikult kaaluvad ja hindavad kodanikud jälgimistegevuse plusse ja miinuseid läbi ning eristavad ka erinevat tüüpi jälgimisviise (Wester ja Giesecke, 2019). Seega soovivad inimesed korraga ikkagi mõlemat - nii turvalisust kui privaatsust.

Jälgimistehnoloogia tüüp mõjutab Wrighti ja Watsoni (2013) sõnul avalikkuse suhtumist jälgimisse ning kaasatud tehnoloogia ja jälgimismeetme sihtmärk mõjutavad tugevalt inimeste toetust neile. Näiteks leitakse, et inimesed on üldjuhul oma suhtluse jälgimise vastu, kuid vastuseis on suurem seoses telefonisuhtluse jälgimisega võrreldes võrgujälgimisega (Wright ja Watson, 2013).

Läbipaistvus on tihedalt seotud ka usaldusega. Seega võiks järeldada, et mida läbipaistvam ja põhjendatum on mõne asutuse jälgimise põhjus ja muud tagamaad, seda rohkem usaldatakse neid oma andmetega läbikäimisel ja aktsepteeritakse jälgimist. Kuna magistritöö keskmes on riigiasutused, siis kaasan analüüsi ühe sõltumatu tunnusena elanike usalduse riigiorganisatsioonide vastu. Usaldus institutsioonide vastu on seotud erinevate rühmade privaatsusmuredega ning võib olla üks võtmemuutujaid, mis selgitab uute tehnoloogiate kasutuselevõttu Eestis (Männiste ja Masso, 2018). Varasemalt on selgunud, et mida usaldavam ollakse valitsuse suhtes, seda positiivsemalt suhtutakse jälgimistehnoloogiatesse, pidades neid efektiivseteks lahendusteks turvalisuse suurendamisel (Pavone ja Esposti, 2010). Seega peavad inimesed selliste tehnoloogiate aktsepteerimiseks uskuma, et riigivõimu esindajad tegutsevad nende huvidest ja vajadustest lähtuvalt, sealhulgas kaitstes ka iga inimese isiklikku privaatsust. Sellest tulenevalt on peale suuremaid intsidente (nt 9/11 terrorirünnakud, Covid-19) märgata inimeste suuremat usaldust riigiasutuste vastu ning ollakse rohkem valmis oma kodanikuõigustest (nt privaatsusest) loobuma suurema turvalisuse tagamiseks (Davis ja Silver, 2004). Joonis 1 paistab seda väidet samuti kinnitavat, kus nii Eesti, Rootsi kui ka Portugali usaldus valitsuse vastu kasvas Covid-19 kriisi alguses 2020. aastal. Eestis on OECD (2023) andmetel usaldus valitsuse vastu üsna kõrge – 2022. aasta andmete järgi 50,8%. Võrdlusriikide Rootsi ja Portugali usaldusnäitajad on aga veelgi kõrgemad (vt Joonis 1).



Joonis 1. Usaldus riigiasutuste vastu 2011-2020. Allikas: OECD (2023), autori joonis

Svenonius ja Björklund (2018) on oma uurimuses postkommunistlike riikide riigipoolse jälgimise aktsepteerimist uurinud kahe-dimensiooniliselt - ühelt poolt on arvesse võetud ratsionaalsed, teiselt poolt aga emotsionaalsed kaalutlused. Selgus, et inimeste üldine ebakindlus, sügavamad isiklikud või kultuurilise päritoluga seotud tunded ning mure oma privaatsuse pärast võivad isegi rohkem mõju avaldada jälgimise aktsepteeritavusele kui näiteks riigiorganisatsioonide usaldamine. Kultuuridevahelisi erinevusi vaadates on veel leitud, et näiteks individualistlikes riikides aktsepteeritakse jälgimist rohkem (Dinev jt, 2005). Hofstede kultuuridimensioonide kohaselt kuuluvad Eesti ja Rootsi oma väärtushinnangute poolest just individualistlike riikide hulka ning Portugal kollektivistliku kultuuriga riikide hulka (Hofstede Insight, 2023).

Kuna magistritöös on esindatud kolme riigi elanikud erinevatest põlvkondadest ning seega erineva kultuurilise tausta ja kogemustega, siis loodan analüüsi kokkuvõttes teha mõningaid järeldusi ka kultuurilise päritolu seoste kohta. Kui võtta näiteks Eesti näitel aluseks riigiorganisatsioonide usaldus, siis võiks arvata, et muu rahvus aktsepteerib riigipoolset jälgimist vähem, kuna 2022. aastal selgus riigikantselei tellitud Turu-uuringute AS-i üle-eestilisest küsitlusest, et muu rahvuse usaldus selliste institutsioonide vastu nagu Riigikogu ja Vabariigi Valitsus olid eestlastega võrreldes oluliselt madalamad – Riigikogu usaldas 57% eestlastest ning vaid 36% muu rahvuse esindajatest, Vabariigi Valitsuse usalduse osakaalud olid vastavalt 64% ja 32% (ERR, 2022).

Vaadates veel postkommunistlike maade internetikasutajate seas teostatud uurimusi selgub, et pigem usaldavad vanemad inimesed riigiasutusi vähem ning sellest tulenevalt rakendavad rohkem turvameetmeid ning avaldavad vähem isiklikke andmeid veebis (Budak ja Rajh, 2018). Kalmuse jt (2022) analüüsist on aga teada, et magistritöös kasutatava andmestiku põhjal on vanemad inimesed just vastupidiselt riigiasutuste suhtes usaldavamad kui noored. Põlvkondade erinevused avaldavad mõju jälgimise aktsepteeritavusele, kuna põlvkondade teooria järgi mõjutavad just nn kujundavad noorusaastad (üldiselt vanuses 17-25) inimeste maailmavaateid (Mannheim 1928/1952; Nugin ja Kalmus, 2018). Lisaks võivad põlvkonniti esineda erinevad arusaamad sellest, mil moel riigipoolne (digi)jälgimine tänapäeval üldse toimub. Igal juhul on vanus oluline faktor kirjeldamaks riigipoolse digijälgimise aktsepteerimist ning magistritöös on võrdluses samuti kaks vanuserühma - noorem ja vanem põlvkond.

Vaadates veel sotsiaaldemograafilisi tunnuseid, on näiteks sooliselt leitud, et naised muretsevad rohkem selle üle, kes nende isiklikele andmetele ligi pääseb (Tufekci, 2008) ja kaitsevad seetõttu oluliselt rohkem oma privaatsust internetis (Walrave jt, 2012). Ka kõrghariduse olemasolu on tihti peetud oluliseks mõjutajaks jälgimise aktsepteerimisel ning kõrgharidusega inimesed on tavaliselt

skeptilisemad jälgimise suhtes kui need, kellel kõrgharidus puudub (Budak jt, 2015; Grenville, 2010). Svenonius ja Björklund (2018) uurisid samuti haridustaseme mõju Eesti, Poola ja Serbia näitel ning jõudsid samale järeldusele, kuid seda tänu Poola näitajatele. Seega arvestades, et magistritöö analüüs põhineb Eestile, võib eeldada, et kõrghariduse olemasolu niivõrd suurt rolli ei mängi. Kuna aga eelnevad uurimused on kõrghariduse olulisust rõhutanud, kaasan ka selle ühe sõltumatu tunnusena siiski analüüsi.

Kuna Kalmuse jt (2022) tööst selgus, et *riigipoolse jälgimise aktsepteerimine on seotud põlvkonna, korporatiivse digijälgimise tolereerimise, privaatsuse olulisuse, demokraatia/sõnavabaduse pooldamise, tugeva riigi pooldamise ning usaldusega riigiasutuste vastu*, siis lisan need tunnused kindlasti ka käesoleva töö regressioonanalüüsi, et panna kokku mudel, mis kirjeldaks võimalikult hästi riigipoolse digijälgimise aktsepteerimist. Toetudes eelpool väljatoodud varasematele uurimustele, soovin omaltpoolt analüüsida sõltumatute tunnustena lisaks *soo, rahvuse, kõrghariduse olemasolu, riigipoolse jälgimise kogemuse, mure oma andmete kontrolli üle ning privaatsusesse sekkumise kogemuste tunnuseid.*

Eurobaromeetri uuringud (Euroopa Komisjon, 2011; 2015) viitavad Eesti ja Rootsi sarnasele suhtumisele isiklike andmetega ümberkäimisesse ja privaatsusega seonduvatesse muredesse, ning samuti on mõlema puhul tegemist individualistlike riikidega, kus varasematele uuringutele toetudes aktsepteeritakse enam riigipoolset jälgimist. Seega eeldan, et nende riikide tulemused võivad olla küllaltki sarnased. Portugali vastajad vastanduvad nendes samades uuringutes täielikult Eesti ja Rootsi vastajatele, tundes tunduvalt enam muret oma andmete turvalisuse üle ning kuuludes individualistlikuma ühiskonna asemel kollektivistlikumasse ühiskonda. Seega võib ka nende näitajate põhjal öelda, et Eestis ja Rootsis aktsepteeritakse jälgimist enam kui Portugalis. Kalmuse jt (2022) uurimus kinnitab samuti *Eesti ja Rootsi sarnaseid tulemusi ning riigipoolse digijälgimise kõrgemat aktsepteerimist võrreldes Portugali tulemustega*. Oma analüüsi käigus uurin, kas see peab paika ka kõigi analüüsitavate väidete puhul.

1.3 Riigipoolse digijälgimise „jahutav mõju“ internetiosalusele ja seos privaatsuskäitumisega

Riigipoolse massilise jälgimise kohta on tihti tõmmatud paralleele panoptikumi metafooriga. Panoptikum tähistab inglise filosoofi Jeremy Benthami teoreetilist vanglakujundust, mille keskkohast ehk vaatetornist on ülevaade kogu asutuses toimuva üle ning kinnipeetavad on teadlikud, et neid võidakse jälgida, kuid nad ei suuda täpselt kindlaks teha, millal seda tehakse

(Bentham, 1791). Selline olukord peaks toimima sotsiaalse kontrolli ülima mehhanismina, kuna inimesed hakkavad pideva jälgimise hirmus reformima oma käitumist ning järgima eeldatavaid norme (Foucault, 1977). Selle teooria järgi peaks panoptikum vallandama inimestes sellise vaimse seisundi, kus nad hakkavad pidevalt hindama seaduslike ja ebaseaduslike tegevuste kulusid ja tulusid ning muudavad vastavalt oma käitumist. Sealjuures teadlikkus jälgimise võimalikkusest võib mõjuda käitumisele sama pärssivalt kui tegelik reaalne jälgimine (Solove, 2006).

Ebademokraatlikes riikides, kus sõna- ja käitumisvabadust ongi seadustega oluliselt piiratud, on riigil võim läbi pideva jälgimise kartuse panna inimesi alluma enda korrale ja reeglitele. Demokraatlikes riikides võiks ebaseadusliku käitumise ohjeldamist üldjoontes pidada positiivseks eesmärgiks, kuid sellegipoolest on panoptikumi-sarnast jälgimist laialdaselt kritiseeritud kodanike universaalsete privaatsusõiguste rikkumise (nt Brown, 2014) ja demokraatia jaoks kahjulike tagajärgede tõttu (Penney, 2016), mille mõjul hakatakse ennetavalt piirama oma sõna- ja käitumisvabadust. Seda tehakse läbi erinevate tegevuste vältimise, nagu näiteks internetist (tundliku) informatsiooni otsimine, oma arvamuse avaldamine mõne teema kohta, postituste jagamine, kommenteerimine, piltide üles laadimine, aga ka ebaseaduslikud tegevused nagu illegaalselt muusika/filmide alla laadimine jms. Hirm tekitada digitaalseid jälgi, millel võivad olla negatiivsed tagajärjed, mõjutab oluliselt inimeste valikuid (Büchi jt, 2022).

Kuid Benthami panoptikumi visand oli rohkem ehk iseloomulikum oma ajastule ning tänapäeval on jälgimine muutunud oluliselt hajuvamaks. See tähendab, et jälgimist teostatakse üha rohkem, kasutades erinevaid tehnoloogilisi lahendusi, mille tõttu koguneb andmeid enneolematul hulgal ning jälgimine levib kujuteldamatul viisil kõikjale, muutudes oma vormilt justkui voolavaks ja igale poole laialivalguvaks (Bauman ja Lyon, 2012). Kui panoptikumi jälgimisviisi põhjal on inimesed enam teadlikud enda üle teostatavast jälgimisest, siis Baumani ja Lyoni (2012) kirjeldatav tänapäevane nö pehmem jälgimisviis on justkui kõikjal, toimudes automaatselt kõige muu taustal.

Kui Preibusch (2015) rääkis sellest, kuidas skandaalide mõjul pööratakse lühiajaliselt suuremat tähelepanu oma privaatsusele ja andmekaitsele, siis Büchi jt (2022) on arutlenud selle üle, kuidas sõna- ja käitumisvabaduse piiramine kujunebki välja järk-järgult pikema aja jooksul, olles mõjutatud kõigist vahepealsetest skandaalidest. Põhjenduseks tuuakse välja, et kuigi skandaali mõju on lühiajaline, siis inimeste digitaalne käitumine ei taastu kunagi tagasi päris samale tasemele, vaid jääb alati veidi ettevaatlikumaks (Büchi jt, 2022).

„Jahutava mõju“ eeltingimuseks on seega teadlikkus selle üle, et digiplatvormidel tehtavate tegevuste üle teostatakse jälgimist ehk inimene peab olema kursis sellega, et tema andmeid automaatselt kogutakse ja analüüsitakse (Büchi jt, 2022). Kuid kas teadlikkus ja suhtumine riigipoolse digijälgimise üle võib avaldada mõju ka privaatsuskäitumisele veebis? Privaatsuskäitumiseks võib olla näiteks identiteedi varjamine, sagedane paroolide muutmine, küpsiste eemaldamine ja virtuaalse privaatvõrgu (VPN) kasutamine (Chen jt, 2016). Stoycheff jt (2018) analüüsist selgus, et see, kuivõrd ollakse teadlikud andmejälgimisest, ei avaldanud tegelikult mõju privaatsuskäitumisele. Ka eelpool sai mainitud Facebooki näitel, et kasutajatel puuduvad üldjuhul privaatsusstrateegiad institutsionaalse jälgimise vastu, sest selline jälgimine on muutunud pigem sotsiaalseks normiks, millega tuleb leppida (Young ja Quan-Haase, 2013) ning teadlikud ollakse pigem privaatsusstrateegiatest, mis aitavad kaitsta sotsiaalset privaatsust (Raynes-Goldie, 2010).

Kuna mure privaatsuse pärast on siiski varasemates uuringutes tõusnud esile ühe peamise tegurina jälgimise aktsepteerimisel (Nam, 2019; Ioannou ja Tussyadiah, 2021) ning uute tehnoloogiate juurutamiseks on vajalik aru saada inimeste privaatsusprobleemidest ja -käitumisest (Pavlou, 2011), siis uurin töös lisaks riigipoolse jälgimise „jahutava mõju“ kohta ka seda, kuidas inimeste privaatsuskäitumine on seotud riigipoolse digijälgimise aktsepteeritavusega ning eeldan, et kuna nii internetiosalus kui ka privaatsuskäitumine on digijälgimisest rääkides olulised tegurid, võiks nende vahel esineda seos. Oletan, et *mida suurem on sallivus riigipoolse digijälgimise suhtes, seda suurem on internetiosalus, kuid väiksem privaatsuskäitumine.*

2 UURIMISPROBLEEM JA KESKSED UURIMISKÜSIMUSED

Töö eesmärgiks on uurida inimeste suhtumist riigipoolsesse digitaalsesse jälgimisse. Millistel juhtudel on aktsepteeritav riigiasutuste digipoolne jälgimine ning millistel juhtudel tunnetatakse seda kui privaatsuse rikkumist. Nagu teooria peatükist selgus, on varasemad uurimused näidanud, et kui jutt käib sotsiaalmeedia jälgimisest ja kasutajate andmete kogumisest, siis pigem nähakse probleemi teiste kasutajate või korporatsioonide-poolses jälgimises, kuid riigipoolset jälgimist niivõrd hästi ei tajuta. Samas võib selline jälgimine kujutada endast ohtu inimeste privaatsusele ja kodanikuõigustele. Kuna riigipoolse jälgimise eesmärgiks demokraatlikes riikides peaks üldjuhul olema elanike turvalisuse tagamine, on seega huvitav uurida, kas inimesed pigem hindavad oma privaatsust ning peavad riigiasutuste poolset digijälgimist mitteaktsepteeritavaks või on vastupidiselt nõus turvalisuse nimel loobuma osaliselt oma privaatsusest.

Eesti kontekstis pole inimeste riigipoolse digijälgimise aktsepteeritavust palju uuritud, seetõttu annab magistritöös kasutatav küsitlusuuring selleks hea võimaluse. Samal uuringul põhinev analüüs valmis ka Kalmuse jt (2022) poolt, milles käsitleti samuti suhtumist riigiasutuste ning lisaks ka korporatsioonide-poolsesse jälgimisse ja seega kattub osaliselt käesoleva magistritööga. Erinevused kahe uurimuse vahel seisnevad analüüsimeetodi valikus, mis võimaldab andmeid veidi teise nurga alt vaadata, ning lisaks püüan tunnuse *sallivus riigipoolse digijälgimise suhtes* sisse veidi põhjalikumalt vaadata, analüüsides eraldi ka väiteid, millest koondtunnus on moodustatud, eesmärgiga saada selgem ülevaade, milliste eesmärkide korral ollakse jälgimise suhtes tolereerivamad. Samuti analüüsin, kuidas on seotud hoiakud jälgimise suhtes internetiosaluse ja privaatsuskäitumisega.

Magistritöös sõnastan kokkuvõtvalt viis uurimisküsimust, millele on teooriapõhiselt tuletatud järgmised hüpoteesid:

1. Milline on üldine aktsepteeritavus riigipoolse digijälgimise suhtes Eestis?

Hüpotees: Üldine aktsepteeritavus riigipoolse digijälgimise suhtes on Eestis pigem neutraalsel tasemel.

2. Kas konkreetse eesmärgiga (ennetada terrorirünnakuid, tõkestada haiguste levikut vms) isiklike andmete jälgimine on aktsepteeritavam? Milliste eesmärkide korral ollakse enam valmis oma privaatsusest loobuma, milliste korral vähem?

Hüpotees: Riigipoolne digijälgimine on aktsepteeritavam, kui sellel on konkreetne eesmärk ning eelkõige tolereeritakse jälgimist nendel juhtudel, kus oht ühiskonnale on suurem ja tajutavam.

3. Kuidas erinevad Eesti tulemused üldise ning konkreetse eesmärgiga teostatud jälgimise aktsepteeritavuse suhtes võrdlusriikide Rootsi ja Portugali tulemustest?

Hüpotees: Eesti sarnaneb oma tulemustega riigipoolse jälgimise aktsepteerimise suhtes Rootsile ning mõlema riigi vastajad on võrreldes Portugali vastajatega jälgimise suhtes aktsepteerivamad.

4. Mis mõjutab sallivust riigipoolsesse digitaalsesse jälgimisse Eestis?

Hüpotees: Riigipoolse digijälgimise aktsepteerimine on seotud põlvkonna, soo, rahvuse, kõrghariduse olemasolu, usaldusega riigiorganisatsioonide vastu, tugeva riigi pooldamise, demokraatia/sõnavabaduse pooldamise, korporatsioonide-poolse digijälgimise tolereerimise, riigipoolse jälgimise kogemuste, privaatsuse olulisuse, murega oma andmete kontrolli üle ja privaatsusesse sekkumise kogemustega.

5. Kuidas on riigipoolne digijälgimine seotud internetiosaluse ja privaatsuskäitumisega ehk millised on seosed hoiakute ja käitumise vahel?

Hüpotees: Riigipoolne digijälgimine on positiivselt seotud internetiosalusega ja negatiivselt privaatsuskäitumisega ehk jälgimise sallimine suurendab internetiosalust, kuid vähendab privaatsuskäitumist.

3 METODOLOOGIA

Magistritöö põhineb rahvusvahelise projekti „Sotsiaalmeedia jälgimine ja autoritarismikogemused“ (*Social Media Surveillance and Experiences of Authoritarianism, 2020-2023*) (Bolin, Kalmus jt, 2023) andmetel, mille eesmärk oli uurida, millistel tingimustel aktsepteerivad meediakasutajad digitaalset jälgimist ja kuidas avaldavad sellele mõju varasemad jälgimiskogemused totalitarismi, autoritarismi ja liberaalse demokraatia tingimustes. Projekti valitud riikide valik tugineb seega ajaloole ja autoritaarse režiimi kogemustele. Eesti kuulus Nõukogude Liidu koosseisu perioodil 1940-1991 ning on seega totalitaarse ühiskonnakorralduse taustaga. Portugalis eksisteeris aastatel 1926-1974 parempoolne diktatuuririik ja seega omab ühiskond samuti autoritaarse riigikorra kogemusi. Nende kahe riigi kõrval on kontrastiks valitud Rootsi, kellel puudub autoritaarse riigikorra taust ning kus on pikka aega valitsenud liberaalne demokraatia.

2020. aasta sügisel toimus projekti esimese etapi raames veebiküsitlus, milles osales kokku 3221 vastajat Eestist, Rootsist ja Portugalist (Eestis 1083, Rootsis 1094, Portugalis 1044). Küsitlusuuring annab seega hea võimaluse suunata põhifookus Eesti andmetele, kuid samal ajal võrrelda tulemusi ka Portugali ja Rootsi näitajatega.

3.1 Valim

Andmete kogumismeetodiks on küsitlused veebipaneelides. Uuring telliti Rootsi turu-uuringute firmast Enkätfabriken ning Eestis teostas andmekogumist allhankena Norstat. Projekt keskendub kahe põlvkonna hoiakute ja kogemuste väljaselgitamisele ning seega on uuringusse valitud kaks kohorti järgmised:

- sündinud aastatel 1946-1953 ja nn kujunemisperiood (*formative years*) jääb Eesti puhul Nõukogude Liidu aega ning Portugali puhul autoritaarsesse režiimi. Kohorti kuuluvad inimesed olid 21-28-aastased, kui Portugal väljus autoritaarsest režiimist. Kohordi sünniaastad on valitud Portugali järgi, kuna Portugal väljus režiimist varem kui Eesti Nõukogude Liidust.
- sündinud 1988-1995 ja kelle nn kujunemisperiood nii Eestis kui Portugalis jääb post-totalitaarsesse/-autoritaarsesse aega. Kuna Eesti taasiseseisvumine toimus hiljem kui Portugalis, on kohordi sünniaastad valitud nii, et kujunemisperiood ei jääks enne 1991. aasta taasiseseisvumist.

Valimis arvestati piirkonda ja sugu kahes vanusegrupis. Mõlema vanusegrupi plaanitav valim oli igas riigis 500 inimest. Tegelikud vastamissagedused on toodud Tabelis 1. Uuringu valim ei ole esinduslik riikide elanikkondade suhtes ning uuring viidi läbi vaid internetikasutajate seas.

Tabel 1. Küsitluses osalejate arvud riigi, soo ja vanuse lõikes

		Vastamissagedused		
		Noorem põlvkond (sünd. 1988-1995)	**Vanem põlvkond (sünd.1946-1953)**	**Kokku**
Eesti	Vastajad kokku	556	527	1083
	Mees	244	203	447
	Naine	312	324	636
Rootsi	Vastajad kokku	553	541	1094
	Mees	266	283	549
	Naine	287	258	545
Portugal	Vastajad kokku	525	440	1044
	Mees	253	304	557
	Naine	272	136	408

3.2 Analüüsimeetod

Analüüsiks kasutan töös kvantitatiivseid meetodeid. Analüüsi esimeses etapis annan ülevaate kirjeldavast statistikast, kus uurin risttabelite ja keskmiste võrdluse kaudu viite analüüsi kaasatud väidet riigipoolse digijälgimise aktsepteerimise kohta Eestis ja kahes võrdlusriigis. Statistilise olulisuse hindamiseks kasutan Crameri V seosekordajat ning statistilise olulisuse kohta on järeldused tehtud olulisuse nivool 5%. Andmete analüüsi teostan igas analüüsietapis R statistikatarkvara abil.

Töö teises etapis teostan Eesti andmetega multinomiaalse logistilise regressioonanalüüsi, mille abil uurin sõltuva tunnusena viiest väitest kokku pandud indeksit ehk koondtunnust *sallivus riigipoolse digitaalse jälgimise suhtes* ja analüüsin, kuidas kirjeldavad analüüsi valitud sõltumatud tunnused üldist suhtumist riigipoolsesse digijälgimisse. Peale multinomiaalse regressioonanalüüsi koostan lisaks mudelid samade sõltumatute tunnustega ka kõigi viie väite kohta eraldi. Kuna väidete skaalad on koondtunnusest erinevad ega võimalda luua kolmandat, „neutraalsete hoiakutega“ gruppi, siis olen väidete puhul kasutanud binaarset logistilist regressioonanalüüsi prognoosimaks kuulumist jälgimist aktsepteerijate või mitte-aktsepteerijate hulka.

Analüüsi kolmandas etapis uurin risttabelite abil ka seda, kuidas on omavahel seotud hoiakud riigipoolsesse digijälgimisse ning internetiosalus ja privaatsuskäitumine.

3.3 Tunnused

Tunnuste alapeatükis tutvustan analüüsi kaasatud sõltuvaid ja sõltumatuid tunnuseid. Kuna magistritöö põhifookus on Eesti andmetel, siis on tekstisiseselt toodud tabelitena iga tunnuse kirjeldav statistika (vastamissagedused, keskmised väärtused ja standardhälbed) vaid Eesti kohta. Samasugused kirjeldava statistika ülevaated võrdlusriikide Rootsi ja Portugali kohta on olemas töö lisade hulgas (vt LISA 1).

Töös on kasutatud lisaks originaaltunnustele ka tuletatud koondtunnuseid. Koondtunnuste puhul on väärtused arvutatud selliselt, et originaaltunnuse iga väärtus annab teatud arvu punkte ning vastamata jätmine annab null punkti (Bolin, Kalmus jt, 2023). Seega ei teki koondtunnuste puhul andmelünki. Koondtunnuste mõõtmistäpsuse hindamiseks on Bolin, Kalmus jt (2023) teostanud sisereliaabluse kontrolli, mille tulemused on välja toodud samuti töö lisade hulgas (vt LISA 2). Enamus tunnused on hea sisereliaablusega, kuid näiteks tunnuse *tugeva riigi pooldamine* puhul on näitaja teiste tunnustega võrreldes madalama reliaabluskoefitsiendiga.

3.3.1 Sõltuv tunnus

Regressioonanalüüsis on sõltuvaks tunnuseks *sallivus riigipoolse digitaalse jälgimise suhtes*, mille väärtused jagunevad järgmiselt: 0- tolerantsus puudub, 1- madal tolerantsus, 2- keskmine tolerantsus, 3- kõrge tolerantsus, 4- väga kõrge tolerantsus.

Sõltuv tunnus on tuletatud viiest väitest, mille kohta küsiti osalejate arvamust privaatsuse ja andmete haldamise küsimusteplokis. Küsimused sisaldasid hoiakuid selle kohta, mil määral tunnetavad vastajad, et riigiasutustel on õigus erinevatel eesmärkidel nende andmetele ligi pääseda. Kõikide väidete puhul kasutati 4-pallist skaalat, mille väärtused jagunesid järgmiselt: 1- ei ole üldse nõus, 2- pigem ei ole nõus, 3- üldiselt nõus, 4- olen täiesti nõus. Kirjeldav statistika nii väidete kui koondtunnuse kohta on toodud Tabelis 2.

Tabel 2. Sõltuvate tunnuste kirjeldav statistika Eesti kohta

Tunnus	**Vastanute arv**	**Keskmine**	**Standard-hälve**	**Min**	**Max**	**Vastamata**
Sallivus riigipoolse digitaalse jälgimise suhtes	1083	1,84	1,25	0	4	0
1. väide: Mind ei häiri, et riigivõimu asutustel on juurdepääs minu andmetele sotsiaalmeedias	1018	2,28	0,91	1	4	65
2. väide: Riigivõimu asutustel on õigus jälgida kodanike internetisuhtlust, et ennetada terrorirünnakuid	1021	2,68	0,90	1	4	62

Tunnus	Vastanute arv	Keskmine	Standard-hälve	Min	Max	Vastamata
3. väide: Riigivõimu asutustel on õigus jälgida kodanike internetisuhtlust, et ennetada vägivaldseid proteste või tänavarahutusi	1008	2,44	0,91	1	4	75
4. väide: Riigivõimu asutustel on õigus jälgida kodanike internetisuhtlust, et ennetada välisriikide sekkumist (nt valimistesse);	986	2,58	0,95	1	4	97
5. väide: Riigivõimu asutustel on õigus jälgida kodanikke digitaalselt (nt droonide, äppide, mobiil-positsioneeringu abil), et ennetada haiguste levikut.)	1007	2,43	0,95	1	4	76

3.3.2 Sõltumatud tunnused

Aitamaks mõista, millised tunnused on seotud üldise suhtumisega riigipoolsesse digijälgimisse, olen analüüsi kaasanud sotsiaaldemograafiliste tunnustena *soo* (1 - mees, 2 - naine), *vanuserühma* (0 - noorem põlvkond, 1 - vanem põlvkond), *rahvuse* (1 - eestlane, 2 - muu rahvus; rahvust on küsitud ainult Eesti andmetes) ja *kõrghariduse olemasolu* (1 - ei, 2 - jah). Kõrghariduse tunnus on ümberkodeeritud 6-väärtuselisest kõrgeima haridustaseme tunnusest, kus kõik, kellel on kõrgharidusest madalam haridustase, lähevad väärtuse 1 alla ning kõrgharidusega vastajad väärtuse 2 alla.

Tabel 3. Sotsiaaldemograafiliste tunnuste sagedusjaotused Eesti kohta

		Vastanute arv	Osakaal
Sugu	Mees	447	41,3%
	Naine	636	58,7%
Vanuserühm	Noorem põlvkond	556	51,3%
	Vanem põlvkond	527	48,7%
Rahvus	Eestlane	905	83,6%
	Muu rahvus	138	12,8%
	Vastamata	40	3,7%
Kõrghariduse olemasolu	Ei	556	51,3%
	Jah	515	47,6%
	Vastamata	12	1,1%

Lisaks sotsiaaldemograafilistele tunnustele analüüsin regressioonanalüüsi käigus veel teisigi taustatunnuseid. Esimeseks on *usaldus riigiasutuste vastu*. Vastajatel paluti hinnata, mil määral usaldatakse loetletud institutsioone ja rühmi. Väärtused olid vahemikus 1 kuni 5 (1 - ei usalda üldse, 2 - vähesel määral, 3 - ei seda ega teist, 4 - suurel määral, 5 - usaldan täiesti). Riigiasutuste usaldus koosneb järgmistest institutsioonidest: Eesti riik, valitsus, riigikogu, politsei, kaitsevägi,

kohtusüsteem, Eesti Pank, tervishoiusüsteem. Moodustunud koondtunnuse väärtused on 0 - usaldus puudub, 1 - madal, 2 - keskmine, 3 - kõrge, 4 - väga kõrge.

Privaatsuse olulisuse tunnus koosneb seitsmest väitest, mille kohta avaldasid vastajad oma arvamust küsimuse juures „Privaatsus tähendab tänapäeval erinevate inimeste jaoks eri asju. Mõeldes kogu oma igapäevasele suhtlusele – nii vahetule kui internetisuhtlusele – öelge palun, kui oluline on Teie jaoks…“ – (1) suuta kontrollida, kes saab Teie kohta infot; (2) et keegi ei saaks Teid ilma Teie loata vaadelda või pealt kuulata; (3) suuta kontrollida, millist infot Teie kohta kogutakse; (4) et inimesed ei küsiks suhtluses või töö juures asju, mis on väga isiklikud; (5) et saaksin jagada salajasi asju kellegagi, keda usaldan; (6) et mind töö juures ei jälgitaks; (7) et saaksin käia avalikes kohtades, ilma et mind iga kord identifitseeritaks. Vastusevariandid olid 4-pallisel skaalal: 1 - täiesti ebaoluline, 2 - pigem ebaoluline, 3 - pigem oluline, 4 - väga oluline. Seitsmest väitest kokku pandud koondtunnuse väärtused on järgmised: 1 – privaatsuse olulisus väga madal, 2 – madal, 3 – keskmine, 4 – kõrge, 5 – väga kõrge.

Tunnus *mure privaatsuse ja oma andmete kontrollimise üle* tuleneb küsimusest „Kas Te tunnete muret selle üle, et Te ei suuda täielikult kontrollida infot, mida Te internetis enda kohta annate? Kas Te olete…?“ Küsimus esitati 4-pallisel skaalal, kus 1 - üldse mitte murelik, 2 - mitte eriti murelik, 3 - üpris murelik, 4 - väga murelik.

Riigipoolse jälgimise kogemuste tunnus koosneb kahest küsimusest: (1) Kas teate Eestis kedagi, kes on harrastanud mõnd poliitilist või usulist tegevust (lugenud raamatuid, kuulanud raadiot, käinud koosolekutel või jutlustel) salaja, et vältida halbu tagajärgi? (2) Kas teate Eestis kedagi, kellel pole lubatud midagi teha (minna välismaale, astuda ülikooli, saada teatud tööd) seetõttu, et riigivõimu asutustel on info tema mineviku, perekonna ajaloo, poliitiliste vaadete vms kohta? Koondtunnuse väärtused on 0 - kogemused puuduvad, 1 - vähe kogemusi, 2 - keskmiselt kogemusi, 3 - palju kogemusi, 4 - väga palju kogemusi.

Demokraatia ja sõnavabaduse väärtustamise tunnus koosneb kahest küsimusest, milles paluti vastata, mil määral nõustutakse väidetega „Kõigil inimestel peaks olema õigus avaldada oma arvamust“ ja „Meedial (nt televisioon, ajalehed, veebiväljaanded) on õigus kritiseerida poliitikuid ja valitsust“. Küsimused olid 5-pallisel skaalal, kus 1 – üldse ei nõustu, 2 – pigem ei nõustu, 3 – ei ole nõus ega vastu, 4 – pigem nõustun, 5 – nõustun täiesti. Demokraatia pooldamise koondtunnuse väärtused on 0 – ei poolda, 1 – pooldab vähe, 2 – pooldab keskmisel tasemel, 3 – pooldab kõrgelt, 4 – pooldab väga kõrgelt.

Tugeva riigi või autoritaarsemate hoiakute pooldamise tunnus koosnes samuti kahest küsimusest, milles paluti vastata, mil määral nõustutakse väidetega „Meie riigil on vaja tugevat valitsust, mis hoiaks korra majas ja juhiks meid õiges suunas“ ja „Kodanikuõiguste ja -vabaduste asemel on meie riigil tarvis ainult seadusi ja korda“. Küsimused olid 5-pallisel skaalal, kus 1 – üldse ei nõustu, 2 – pigem ei nõustu, 3 – ei ole nõus ega vastu, 4 – pigem nõustun, 5 – nõustun täiesti. Tugeva riigi pooldamise indekstunnuse väärtused on: 0 – ei poolda, 1 – pooldab vähe, 2 – pooldab keskmisel tasemel, 3 – pooldab kõrgelt, 4 – pooldab väga kõrgelt.

Tunnus, mis sisaldab *privaatsusesse sekkumise kogemusi internetis või sotsiaalmeedias*, tuleneb küsimusest „Kas Teil on olnud tunnet, et allpool nimetatud asutused, äriettevõtted, inimesed rikuvad interneti või sotsiaalmeedia kasutamise kaudu Teie privaatsust?“. Valida sai järgmiste vastusevariantide vahel: riigivõimu asutused (Maksuamet, politsei vms), kohaliku võimu asutused, tööandja, äriettevõtted, tervishoiusüsteem, haridussüsteem, võõrad inimesed, sõbrad/tuttavad, pereliikmed. Sekkumiste sageduse määramiseks kasutasid vastajad 5-pallist skaalat, kus 1 – üldse mitte, 2 – harva, 3 – mõnikord, 4 – küllalt sageli/korduvalt, 5 – pidevalt, väga sageli. Privaatsusesse sekkumise kogemuse koondtunnuse väärtused on 0 - kogemused puuduvad, 1 - vähe kogemusi, 2 - keskmiselt kogemusi, 3 - palju kogemusi, 4 - väga palju kogemusi.

Viimase tunnusena on regressioonanalüüsis *sallivus korporatsioonide-poolse digijälgimise suhtes*, mis koosneb seitsmest väitest. Esimeseks (1) väiteks on „Mind ei häiri, et eraettevõtetel on juurdepääs minu andmetele sotsiaalmeedias“ ning vastusevariantideks olid 1 – ei ole üldse nõus, 2 – pigem ei ole nõus, 3 – üldiselt nõus, 4 – olen täiesti nõus. Järgmise kuue väite kohta sai vastaja märkida, kas etteantud lause käib tema kohta või ei käi tema kohta: (2) „Ma saan vastutasuks personaalse teenuse, näiteks (minu asukohal põhineva) ilmaennustuse oma telefonis“; (3) „Nad kasutavad neid andmeid, et näidata mulle reklaami või infot, mis võib olla minu jaoks olulisem“; (4) „Nad kasutavad neid andmeid, et saata mulle olulisi eripakkumisi / soodustusi toodete või teenuste osas, mis nende arvates mulle meeldivad“, (5) „Nad ütlevad selgelt, kuidas nad minu andmeid kasutavad“; (6) „Ma saan igal hetkel teenusest loobuda ja nad lõpetavad minu andmete kasutamise“, (7) „Nad lubavad mulle, et nad ei jaga minu andmeid teiste ettevõtetega“. Vastuste põhjal loodud koondtunnuse väärtused on 0 – sallivus puudub, 1 – madal sallivus, 2 – keskmine sallivus, 3 – kõrge sallivus, 4 – väga kõrge sallivus.

Tabel 4. Sõltumatute tunnuste kirjeldav statistika Eesti kohta

Tunnus	Vastanute arv	Keskmine	Standardhälve	Min	Max	Vastamata
Usaldus riigiasutuste vastu	1083	2,08	1,12	0	4	0
Privaatsuse olulisus	1083	3,84	1,32	1	5	0
Riigipoolse jälgimise kogemus	1083	1,42	1,48	0	4	0
Mure andmete kontrolli üle*	877	2,37	0,69	1	4	206
Demokraatia pooldamine	1083	2,50	1,17	0	4	0
Tugeva riigi pooldamine	1083	1,19	1,05	0	4	0
Privaatsuse riive kogemused	1083	1,64	1,22	0	4	0
Sallivus korporatsioonide-poolse digijälgimise suhtes	1083	1,63	1,09	0	4	0

* Tunnus *mure andmete kontrolli üle* on originaaltunnus ja seetõttu on selles andmelünki (’vastamata/ei oska öelda’). Ülejäänud tunnused on arvutuslikult saadud koondtunnused, millel andmelüngad puuduvad.

Lisaanalüüsina uurin ka riigipoolse digijälgimise aktsepteerimise seost internetiosalusega, mida vaatan läbi kaheksa veebitegevuse, mis on toodud Tabelis 5. Küsimused esitati 6-pallisel skaalal, mille väärtused jagunesid järgmiselt: 1 – pole mitte kunagi teinud, 2 – varem tegin seda, enam mitte, 3 – väga harva, 4 – paar korda kuus, 5 – paar korda nädalas, 6 – iga päev.

Tabel 5. Internetis tehtavate tegevuste vastuste sagedusjaotused Eesti kohta

	Mitte kunagi	Varem tegin seda, enam mitte	Väga harva	Paar korda kuus	Vähemalt paar korda nädalas
Piltide üleslaadimine	18,4%	4,8%	35,4%	24,7%	16,7%
Videote üleslaadimine	40,8%	5,7%	39,1%	9,2%	5,3%
Muusika, filmide, programmide allalaadimine või jagamine	47,3%	8,9%	27,0%	10,2%	6,6%
Iseenda kohta info jagamine sotsiaalmeedias	33,1%	7,5%	36,2%	13,7%	9,5%
Meediauudiste jagamine sotsiaalmeedias	39,6%	3,2%	35,6%	10,8%	10,7%
Uudiste või artiklite kommenteerimine portaalides/sotsiaalvõrgustikes	51,1%	4,8%	29,4%	5,9%	8,7%
Foorumites sõnavõtmine	49,8%	5,4%	29,0%	6,6%	9,3%
Liitumine mõne kampaania/protestiga/petitsioonile allkirja andmine	40,2%	5,0%	49,2%	4,6%	0,9%

Riigipoolse digijälgimise aktsepteerimise seost privaatsuskäitumisega uurin läbi kolme küsimuse (vt Tabel 6). Küsimused olid esitatud 3-pallisel skaalal, kus 1 – pole mitte kunagi teinud, 2 – Jah, üks kord, 3 – Jah, mitmel korral.

Tabel 6. Privaatsuskäitumist puudutavate küsimuste vastuste jaotus Eesti kohta

	Ei, mitte kunagi	**Jah, üks kord**	**Jah, mitmel korral**	**Ei oska öelda/ei puutu minusse**
Reeglite ja tingimuste lugemine enne uue rakenduse või veebikeskkonna kasutamist	17,8%	19,4%	49,5%	13,2%
Privaatsussätete muutmine mõnes sotsiaalvõrgustikus, eesmärgiga piirata enda andmete kasutamist	18,1%	12,1%	53,6%	16,2%
Mõne veebilehe või äpi kasutamisest loobumine, kuna ei soovinud, et Teid seal jälgitakse	22,4%	14,7%	39,4%	23,5%

4 ANALÜÜS

Analüüsi peatükis uurin kõigepealt esimese etapi raames risttabelite ja keskmiste väärtuste kaudu viite riigipoolset digijälgimist puudutavat väidet, mis moodustavad kokku uurimuse sõltuva koondtunnuse *sallivus riigipoolse digijälgimise suhtes*. Analüüsides kõigepealt, kuidas erinevatel põhjustel teostatavat jälgimist aktsepteeritakse kolmes riigis sotsiaaldemograafiliste tunnuste lõikes iga väite puhul eraldi, teen lõpetuseks alapeatükis 4.1.6 kokkuvõtte üldisest riigipoolse digijälgimise aktsepteeritavusest. Analüüsi teises etapis teostan regressioonanalüüsi, saamaks Eesti andmete põhjal selgemalt ülevaadet, millised taustatunnused on seotud riigipoolse digijälgimise aktsepteerimisega. Peale väidete ja regressioonmudeli analüüsimist püüan kolmandas etapis risttabelite kaudu välja selgitada, kas riigipoolse jälgimise aktsepteeritavus on seotud ka inimeste internetis tehtavate tegevuste ning privaatsuskäitumisega.

4.1 Väidete analüüs

4.1.1 Väide 1. Mind ei häiri, et riigivõimu asutustel on juurdepääs minu andmetele sotsiaalmeedias

Esimeseks analüüsitavaks väiteks on küsimus, millega uuriti, kuivõrd häirib inimesi asjaolu, et riigiasutused omavad ligipääsu nende sotsiaalmeedia andmetele. Väite puhul polnud ette antud jälgimise konkreetset põhjust, vaid küsiti vastajate üldist suhtumist.

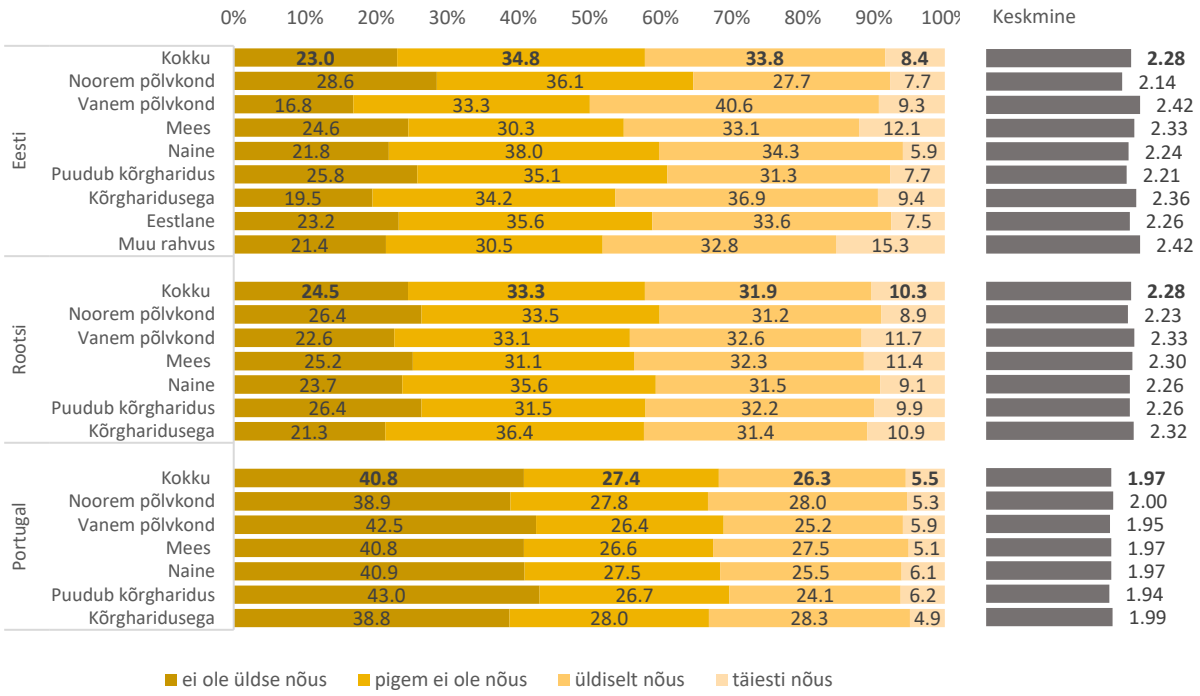
Selgub, et riigiti on tulemustes statistiliselt olulised erinevused (Crameri V=0,129, p<0,01). Kõige tugevamalt hakkab silma Portugali vastajate väga suur osakaal vastusevariandi „ei ole üldse nõus“ juures (vt Joonis 2). Kui Portugalis ei ole väitega üldse nõus ligi 41% vastajatest, siis Eestis ja Rootsis on seda varianti valinud tunduvalt väiksem osa vastajatest (vastavalt 23% ja 25%). Üldiselt või täiesti nõus on väitega 42% nii Eesti kui Rootsi vastajatest. Portugalis nõustus väitega 32% vastajatest.

Joonist 2 vaadates tuleb esile ka eestlaste suurem erinevus põlvkondade lõikes (Crameri V=0,170, p<0,01), kus vanem põlvkond on oluliselt enam nõus, et riigiasutustel on õigus inimeste andmetele sotsiaalmeedias ligi pääseda. Noorem põlvkond on tunduvalt kriitilisem ja üldse või pigem ei ole väitega nõus 65% (vanemas põlvkonnas on sama näitaja 50%). Teistel riikidel puudusid põlvkondlikud erinevused selle väite osas.

Eesti puhul kujunesid statistiliselt oluliseks ka soolised, hariduslikud ning rahvuslikud erinevused (soo tunnusel Crameri V=0,127, p<0,01; kõrghariduse tunnusel Crameri V=0,087, p<0,1 ning

rahvuse tunnusel Crameri V=0,095, p=0,03). Eesti naiste puhul paistab silma, et pigem on koondutud kesksete vastuste ümber, mehed on rohkem valinud äärmuslikke vastusevariante. Keskmiseid väärtuseid võrreldes saaks aga järeldada, et mehed on võrreldes naistega enam nõus, et riigiasutustel on õigus pääseda ligi inimeste sotsiaalmeedia andmetele. Kõrghariduse olemasolu võib samuti viidata sellele, et ollakse enam väitega nõus ning need, kellel kõrgharidus puudub, suhtuvad antud väitesse skeptilisemalt. Mõnevõrra üllatav on muust rahvusest vastajate suurem nõustumine ning eestlaste kriitilisem suhtumine väitesse.

Rootsis ja Portugalis polnud soo ja kõrghariduse olemasolu lõikes gruppide vahelised erinevused statistiliselt olulised.



Joonis 2. Väite „Mind ei häiri, et riigivõimu asutustel on ligipääs minu andmetele sotsiaalmeedias“ vastuste jaotus ja keskmised väärtused sotsiaaldemograafiliste tunnuste lõikes

4.1.2 Väide 2. Riigivõimu asutustel on õigus jälgida kodanike internetisuhtlust, et ennetada terrorirünnakuid

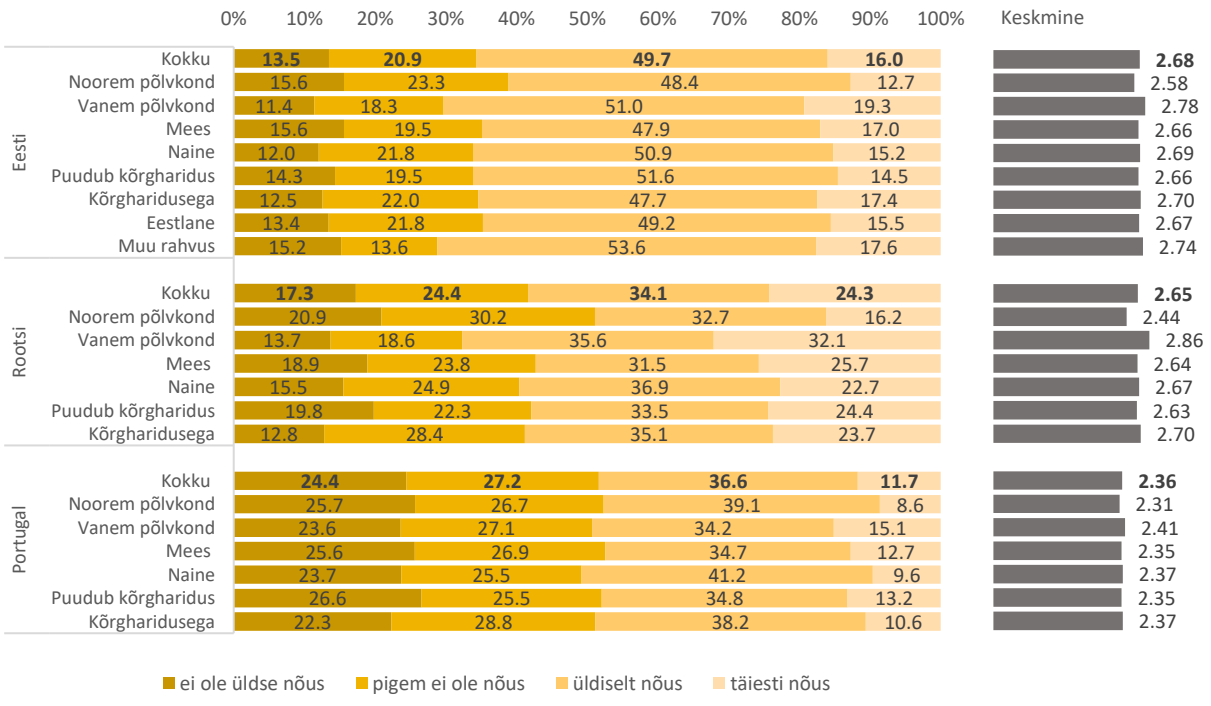
Järgnevalt on vaatluse all väited, kus jälgimine on põhjendatud mingi konkreetse eesmärgiga. Alustuseks analüüsin suhtumist sellesse, kuivõrd on riigiasutustel õigus jälgida kodanike internetisuhtlust terrorirünnakute ennetamiseks.

Võrreldes eelmise väitega, kus küsiti suhtumist riigipoolsesse digijälgimisse ilma konkreetse eesmärgita, selgub, et kõikides võrdlusriikides aktsepteeritakse riigipoolset digijälgimist tunduvalt

rohkem, kui eesmärgiks on terrorirünnakute ennetamine (vt Joonis 3). Väite puhul ilmnevad riigiti olulised erinevused (Crameri V=0,143, p<0,01), kus Portugali vastajad on taaskord tunduvalt kriitilisemad digijälgimise suhtes kui Eesti ja Rootsi vastajad.

Huvitavad tulemused ilmnevad, kui vaadata väidet põlvkondade lõikes. Kõige suuremad põlvkondade erinevused on Rootsi vastajate hulgas (Crameri V=0,218, p<0,01) – 51% nooremast põlvkonnast leiab, et riigivõimu asutustel pigem ei ole õigust jälgida kodanike internetisuhtlust terrorirünnakute ennetamiseks, vanemas põlvkonnas on see näitaja vaid 32%. Statistiliselt oluline erinevus on ka Eesti põlvkondade vahel (Crameri V=0,116, p=0,003), kus nooremas põlvkonnas on sellise jälgimise vastu 39% ja seega poolt 61%, vanemas põlvkonnas on vastu 30% ja poolt 70%. Seega on sarnaselt mõlemas riigis nooremad vastajad oluliselt kriitilisemad. Portugalis on põlvkondade vahelised erinevused kõige väiksemad, kuid siiski statistiliselt olulised (Crameri V=0,105, p=0,01) ning peamine erinevus tuleneb vastusevariantidest „täiesti nõus“ ja „üldiselt nõus“, kus vanemas põlvkonnas on väitega täiesti nõus 15% ja üldiselt nõus 34%, nooremas põlvkonnas ollakse veidi kriitilisemad ning täiesti nõus on 9% ja üldiselt nõus 39%.

Teiste sotsiaaldemograafiliste tunnuste lõikes statistiliselt olulised erinevused kõikides riikides puuduvad, va Rootsis, kus kõrgharidusega vastajad olid väitega enam nõus võrreldes nendega, kellel kõrgharidus puudus (Crameri V=0,100; p=0,02).



Joonis 3. Väite „Riigivõimu asutustel on õigus jälgida kodanike internetisuhtlust, et ennetada terrorirünnakuid“ vastuste jaotus ja keskmised väärtused sotsiaaldemograafiliste tunnuste lõikes

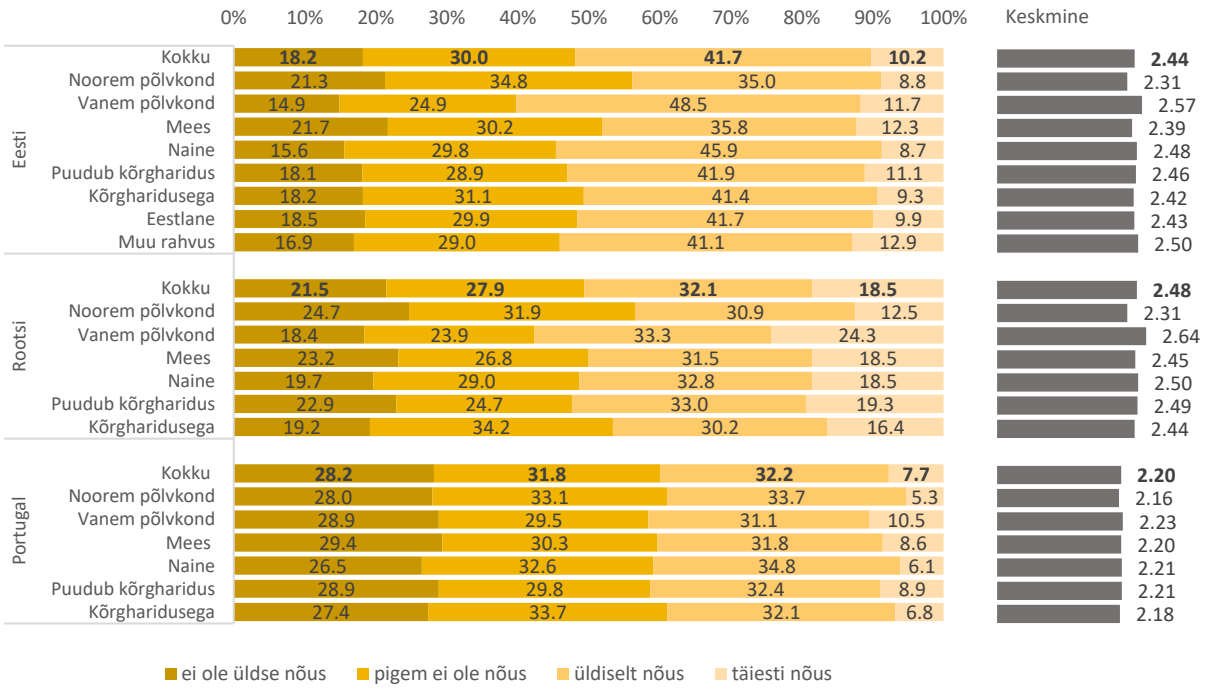
4.1.3 Väide 3. Riigivõimu asutustel on õigus jälgida kodanike internetisuhtlust, et ennetada vägivaldseid proteste või tänavarahutusi

Vägivaldsete protestide ja tänavarahutuste ennetamise eesmärgiga riigipoolsesse digijälgimisse suhtutakse kriitilisemalt võrreldes terrorirünnakute ennetamisega. Ka väite 3 puhul esinevad statistiliselt olulised erinevused riigiti (Crameri V=0,125, p<0,01). Taaskord on Portugali vastajad kõige enam väitele vastu - 60% ei ole üldse või pigem nõus, Rootsi ja Eesti vastajad olid sarnaste tulemustega, vastavalt 49% ja 48% (vt Joonis 4).

Ka põlvkonniti on igas riigis olulised erinevused (Eesti Crameri V=0,164, p<0,01; Rootsi Crameri V=0,172, p<0,01; Portugali Crameri V = 0,101, p=0,02). Eestis ja Rootsis on jällegi selgelt näha noorema põlvkonna suuremat vastuseisu riigipoolsele digijälgimisele, vanemaealised on aktsepteerivamad. Portugali vastajate hulgas on peamine vanusegruppide vaheline erinevus vastusevariandis „täiesti nõus“, kus vanemaealistel on see 10,5% ja nooremaealistel vaid 5,3%.

Teistest sotsiaaldemograafilistest tunnustest on Eesti puhul olulised erinevused sooliselt (Crameri V=0,118; p<0,01), kus naised kipuvad väitega enam nõustuma. Kõrghariduse olemasolu ja rahvus olulised ei ole.

Portugalis puuduvad samuti olulised erinevused soo ja kõrghariduse olemasolu lõikes. Rootsi puhul kujunes oluliseks kõrghariduse olemasolu (Crameri V=0,101, p=0,01) ning vastupidiselt eelnevatele väidetele on kõrgharitud kriitilisemad selle väite suhtes. Soolised erinevused Rootsis puuduvad.



Joonis 4. Väite „Riigivõimu asutustel on õigus jälgida kodanike internetisuhtlust, et ennetada vägivaldseid proteste või tänavarahutusi“ vastuste jaotus ja keskmised väärtused sotsiaaldemograafiliste tunnuste lõikes

4.1.4 Väide 4. Riigivõimu asutustel on õigus jälgida kodanike internetisuhtlust, et ennetada välisriikide sekkumist (nt valimistesse)

Kodanike internetisuhtluse jälgimine välisriikide sekkumise ennetamiseks on kõige mitteaktsepteeritavam taaskord Portugalis, kus vastusevariante „ei ole üldse nõus“ või „pigem ei ole nõus“ on valinud 60% vastanutest. Rootsis ja Eestis on väitega mitte-nõustujaid 42%. Neid, kes on väitega täiesti nõus on Rootsis 23%, Eestis 16% ning Portugalis 9%. Ka selle väite puhul on tegemist statistiliselt oluliste erinevustega riikide vahel (Crameri V=0,151, p<0,01).

Vaadates põlvkondade vahelisi erinevusi riigiti (vt Joonis 5), on näha, et kõige suuremad erinevused noorema ja vanema põlvkonna vahel esinevad jällegi Rootsis (Crameri V=0,262 ja p<0,01), kus vanemas põlvkonnas on väitega täiesti nõus tervelt 34% vastajatest, nooremas põlvkonnas aga vaid 13%. Nooremas põlvkonnas on täiesti või pigem vastu sellisele digijälgimisele 52% vastajatest, vanemas vanuserühmas 33%.

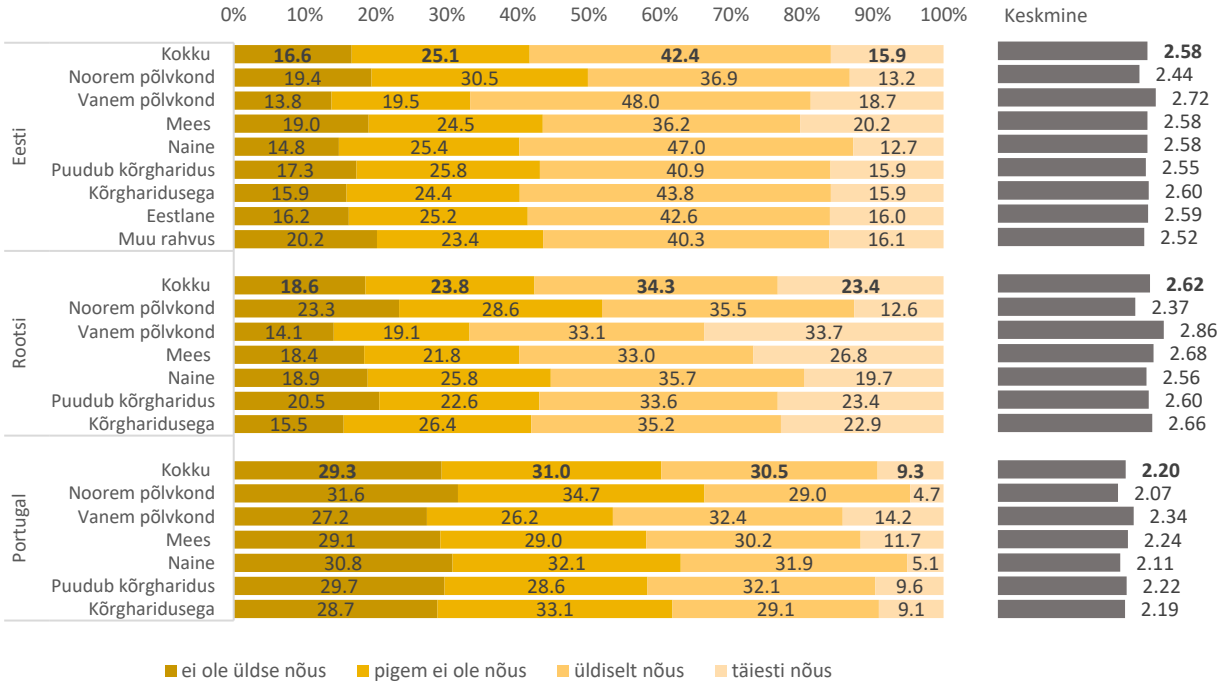
Eesti noorte suhtumine ühtib Rootsi noorte arvamusega ja vastuste osakaalud on praktiliselt samad (Eesti põlvkondade Crameri V=0,170, p<0,01). Erinevused tekivad vanemas vanuserühmas variantide „üldiselt nõus“ ja „täiesti nõus“ juures, kus eestlastel pole nii kindlameelset seisukohta

kui rootslastel. Kui Rootsis oli täielikult nõustujaid 34%, siis Eesti vanemaealistest oli vaid 19% täiesti nõus väitega. See-eest kuulub suurem enamus Eesti vanemast põlvkonnast siiski „üldiselt nõustujate“ sekka (48%). Rootsis kuulus sinna gruppi 33%. Kui need kaks gruppi kokku liita üheks „nõustujate“ grupiks, on tulemused ümardatult identsed ja mõlemas riigis 67%. Rootsis on seega julgemalt valitud äärmuslikemaid variante, mis viitab konkreetsematele hoiakutele antud küsimuse suhtes ning teadvustatakse paremini, kas aktsepteeritakse taolist jälgimist või mitte, samas kui Eesti vastajate hulgas valiti pigem skaala keskpunkti lähedasi väärtuseid ja võib-olla nii kindlat arvamust ei omata.

Kui eelnevalt analüüsitud väidete puhul olid Portugali nooremate ja vanemate arvamused suhteliselt sarnased, siis selle väite puhul ilmnevad andmetes juba suuremad põlvkondlikud erinevused (Crameri V=0,181, p<0,01). Selgelt eristub noorema põlvkonna suurem vastumeelsus jälgimise suhtes ning vanem vanusegrupp peab riigipoolset digijälgimist mõnevõrra aktsepteeritavamaks, kui selle eesmärgiks on ennetada välisriikide sekkumist. Noorte seas on väitega täiesti või pigem nõus 34% ning vanemate seas 47%.

Eesti puhul kujunes oluliseks tunnuseks ka sugu (Crameri V=0,135, p<0,01). Keskmiste väärtuste järgi oleks suhtumine riigipoolsesse jälgimisse välisriikide sekkumise ärahoidmiseks justkui sama – 2,58, kuid vastuste jaotusi vaadates selgub, et mehed on taaskord kindlamate hoiakutega, valides enam äärmuslikke vastusevariante. Naised on oluliselt enam valinud varianti „üldiselt nõus“ (47%) ja varianti „täiesti nõus“ on valinud 12%. Meestel on samad näitajad vastavalt 36% ja 20%.

Rootsis ja Portugalis ilmnesid samuti sooliselt olulised erinevused (Rootsi Crameri V=0,087, p=0,05; Portugali Crameri V=0,113, p<0,01) ning mõlemas riigis toetavad mehed naistest enam välisriikide sekkumise ennetamiseks teostatavat riigipoolset jälgimist.

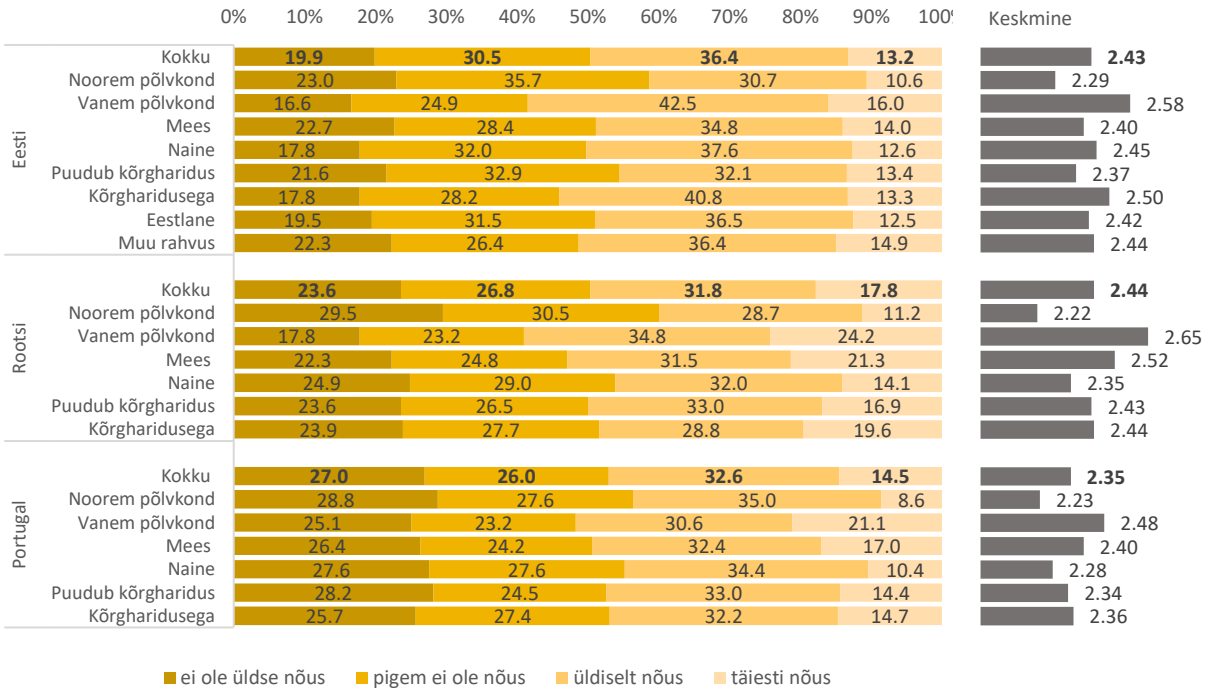


Joonis 5. Väite „Riigivõimu asutustel on õigus jälgida kodanike internetisuhtlust, et ennetada välisriikide sekkumist (nt valimistesse)“ vastuste jaotus ja keskmised väärtused sotsiaaldemograafiliste tunnuste lõikes

4.1.5 Väide 5. Riigivõimu asutustel on õigus jälgida kodanikke digitaalselt (nt droonide, äppide, mobiil-positsioneeringu abil), et ennetada haiguste levikut

Viimase väite puhul analüüsin, kuivõrd õigeks peetakse kodanike digijälgimist, et ennetada haiguste levikut. Selgus, et kõigist viiest väitest on just haiguste leviku ennetamise eesmärgil jälgimine see, kus esineb riigiti kõige vähem erinevusi (Crameri V=0,066, p<0,01). Siiski on need erinevused statistiliselt olulised. Täielikult vastu on sellisel põhjusel jälgimisele Portugalis 27%, Rootsis 24% ning Eestis 20% (vt Joonis 6). Täiesti või pigem nõus ollakse vastavalt 47%, 50% ja 50%. Põlvkonniti esinevad kõikides riikides statistiliselt olulised erinevused (Eesti Crameri V = 0,172, Rootsi Crameri V=0,215 ja Portugali Crameri V=0,178, igas riigis p<0,01). Crameri V seosekordajast nähtub, et kõige suuremad põlvkondlikud erinevused on taaskord Rootsis, kus jällegi on noorem põlvkond tunduvalt vähem nõus digijälgimisega kui vanem põlvkond. Sama muster on nähtav ka kahes teises võrdlusriigis. Kui eelnevate väidete puhul olid kõige enam jälgimise vastu Portugali vastajad (nii noorem kui vanem põlvkond), siis haiguste leviku ennetamiseks teostatav digijälgimine on kõige vastumeelsem hoopis Rootsi nooremale põlvkonnale, vanemas põlvkonnas aga endiselt Portugalis.

Muude sotsiaaldemograafiliste tunnuste lõikes on Eesti puhul oluline kõrghariduse olemasolu (Crameri V= 0,094, p=0,03) ning kõrgharidust omavad vastajad nõustusid väitega enam kui need, kellel kõrgharidus puudus. Rootsi ja Portugali puhul esines statistiliselt olulisi erinevusi meeste ja naiste vahel (Rootsi Crameri V= 0,099, p=0,02, Portugali Crameri V= 0,095, p=0,04) ning mõlemas riigis olid mehed oluliselt enam nõus jälgimisega, kui selle eesmärgiks on ennetada haiguse levikut.



Joonis 6. Väite „Riigivõimu asutustel on õigus jälgida kodanikke digitaalselt (nt droonide, äppide, mobiil-positsioneeringu abil), et ennetada haiguste levikut“ vastuste jaotus ja keskmised väärtused sotsiaaldemograafiliste tunnuste lõikes

4.1.6 Üldine suhtumine riigipoolsesse digijälgimisse

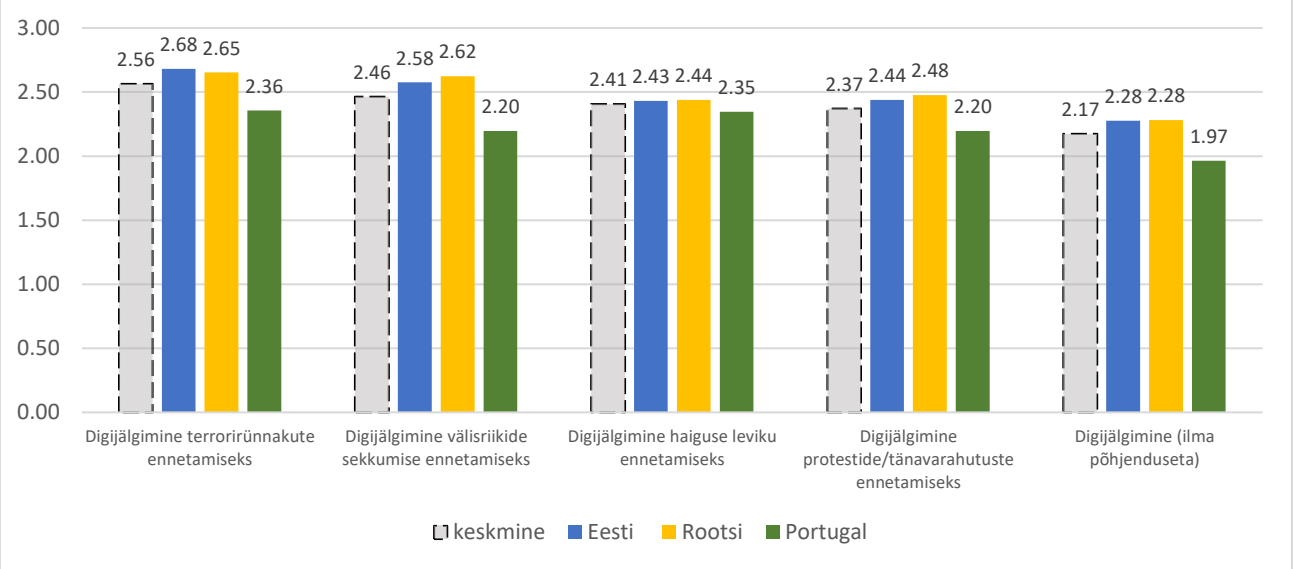
Järgnevas alapeatükis teen kokkuvõte viie väite analüüsist ja nendest moodustatud koondtunnusest *sallivus riigiasutuste poolse digitaalse jälgimise suhtes*.

Joonisel 7 on toodud kõigi viie väite keskmised väärtused riigiti, andmaks paremat ülevaadet, millistel põhjustel on riigipoolne digijälgimine aktsepteeritavam ja millistel mitte. Tulemustest saab järeldada, et jälgimine on tõepoolest aktsepteeritavam, kui selleks on olemas konkreetne põhjus. Esimese väite korral, millega uuriti, kuivõrd on riigiasutustel õigus pääseda ligi inimeste sotsiaalmeedia andmetele, oli nõustumist kõige vähem (keskmine väärtus 2,17). Selle väite puhul polnud välja toodud ühtegi konkreetset põhjust jälgimiseks. Ka riigiti analüüsides, nõustuti selle

väitega kõigis kolmes riigis kõige vähem (Eesti ja Rootsi keskmine on 2,28 ja Portugalil 1,97). Sellest saab järeldada, et inimesed aktsepteerivad jälgimist juhul, kui see on nende jaoks piisavalt põhjendatud ning saavad enda arust või näiliselt sellest jälgimisest teatavat kasu – näiteks kaitset terrorirünnakute vastu, haiguste leviku tõkestamist vms. Seega peab riigiasutuste jälgimistegevus olema läbipaistev ja hästi põhjendatud.

Kõige aktsepteeritavam on riigipoolne digijälgimine juhul, kui sellega ennetatakse terrorirünnakuid. (keskmine väärtus 2,56). Järgnevad jälgimine välisriikide sekkumise ennetamiseks (2,46), haiguse leviku ennetamiseks (2,41) ning seejärel protestide ja tänavarahutuste ennetamiseks (2,37).

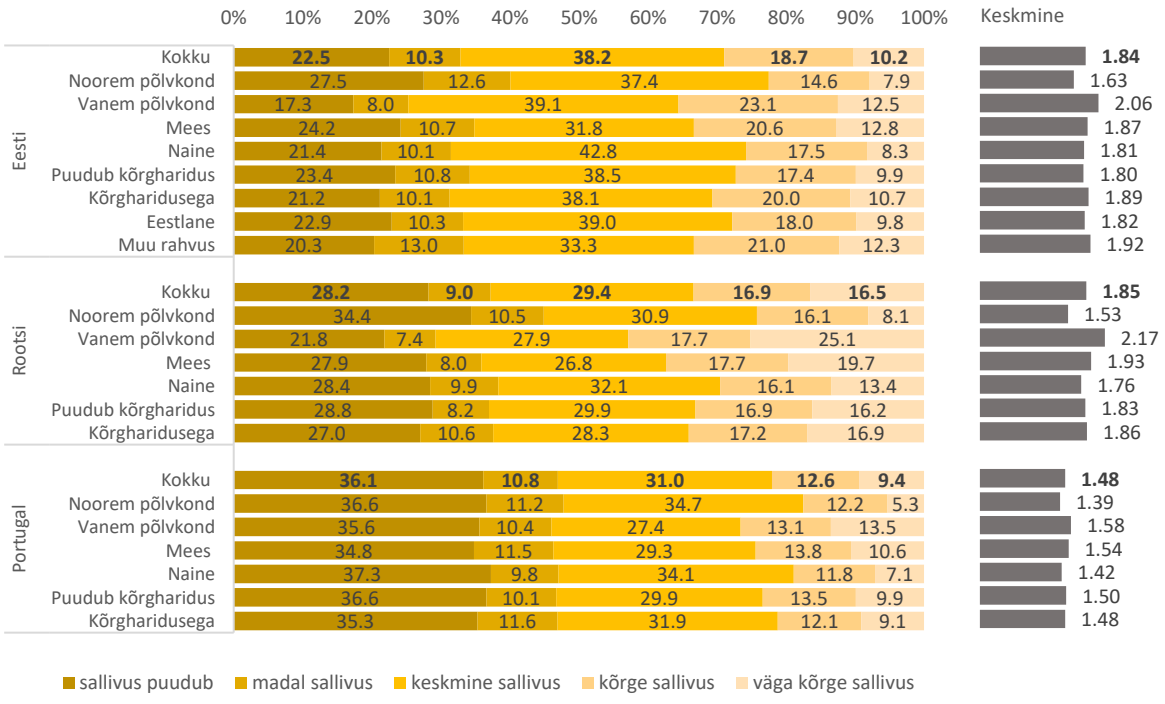
Jooniselt 7 nähtub ka, et magistritöö uurimisküsimuse 3 juures sõnastatud hüpotees saab kinnitust, sest Eesti tulemused sarnanevad Rootsi tulemustele ning Portugali näitajad erinevad oluliselt kahest võrdlusriigist. Ka Kruskal-Wallise test gruppide võrdluseks kinnitab, et Eesti ja Rootsi keskmistes väärtustes pole üheski väites statistiliselt olulisi erinevusi. Küll aga omab statistiliselt olulisi erinevusi Portugal mõlema võrdlusriigiga, välja arvatud väitega, kus riigipoolset digijälgimist selgitatakse haiguse leviku ennetamisega. Selle väite puhul on kõigi kolme riigi keskmised tulemused sarnased.



Joonis 7. Erinevatel eesmärkidel teostatava riigipoolse digijälgimise aktsepteerimine riigiti, keskmised väärtused

Ka Jooniselt 8 on näha, et kokkuvõtliku koondtunnuse *sallivus riigiasutuste poolse digitaalse jälgimise suhtes* tulemused on Eestis ja Rootsis sarnased ning keskmised väärtused on vastavalt 1,84 ja 1,85. Portugali vastajate hulgas on märgata oluliselt madalamat sallivust ning keskmine

väärtus jääb 1,48 juurde. Ka vastusevariantide protsentuaalset jaotust vaadates esineb riigiti statistiliselt olulisi erinevusi (Crameri V=0,119, p<0,01). Kõigis kolmes riigis on näha, kuidas noorte suhtumine riigipoolsesse jälgimisse kipub olema vastumeelsem võrreldes vanema põlvkonnaga ning iga riigi puhul on põlvkondade vahelised erinevused samuti statistiliselt olulised (Eesti Crameri V=0,179; p<0,01, Rootsi Crameri V=0,248, p<0,01, Portugali Crameri V=0,156, p<0,01). Kui Portugalis on vastumeelsus (sallivus puudub või on madal) noorte vastajate seas 48%, siis vanemate vastajate hulgas on osakaal küllaltki sarnane - 46%. Eesti ja Rootsi puhul on aga erinevused suuremad. Eesti noorte seas avaldas riigipoolse jälgimise suhtes vastumeelsust 40% vastajatest, vanemate hulgas oli osakaal aga vaid 25%. Rootsis oli noorte hulgas vastumeelsuse osakaal 45% sihtrühma vastajatest ning vanemate vastajate seas 29%. See-eest kõrge või väga kõrge sallivusega olid eelkõige Rootsi vastajad (33%), järgnesid Eesti vastajad (29%) ning kolmandaks Portugali vastajad (22%). Kõige neutraalsemad olid oma vastustes eestlased (38%), kellele järgnesid portugallased (31%) ning seejärel rootslased (29%).



Joonis 8. Koondtunnuse „Sallivus riigiasutuste poolse digitaalse jälgimise suhtes“ kategooriate jaotus ja keskmised väärtused sotsiaaldemograafiliste tunnuste lõikes

4.2 Riigipoolse digijälgimise aktsepteerimisega seotud tegurid

Analüüsi teises etapis uurin magistritöösse kaasatud taustatunnuste seoseid riigipoolse digijälgimise aktsepteerimisega. Selleks teostasin multinomiaalse logistilise regressioonanalüüsi

(vt Tabel 7), mis võimaldab luua mudeli olemasolevate andmete pealt, hindamaks erinevatesse klassidesse või gruppidesse kuulumise tõenäosust (Tooding, 2015). Regressioonmudeli sõltuvaks tunnuseks on *sallivus riigipoolse digijälgimise suhtes*, mis on jagatud kolmeks grupiks – (1) need, kes ei aktsepteeri/ei salli riigipoolset digijälgimist, (2) need, kes jäävad oma hoiakutelt neutraalseks riigipoolse digijälgimise suhtes ning (3) need, kes aktsepteerivad/sallivad riigipoolset digijälgimist. Sõltuva tunnuse taustakategooriaks on valitud esimene grupp ehk need, kes ei aktsepteeri riigipoolset digijälgimist.

Analüüsis on kaks võrdluspaari:

- Ei aktsepteeri riigipoolset digijälgimist vs neutraalne hoiak;
- Ei aktsepteeri riigipoolset digijälgimist vs aktsepteerib riigipoolset digijälgimist.

Sõltumatute tunnuste taustarühmades on piisaval arvul vastajaid, mis väldib suuremate standardhälvete tekkimist ning annab täpsemaid tulemusi analüüsil. McFaddeni kordaja on 0,1, mis viitab sellele, et sõltumatud tunnused seletavad riigipoolsesse digijälgimisse suhtumist vaid osaliselt ning mudeli kirjeldusvõime pole kuigi tugev. Tulemuste tõlgendamiseks on kasutatud eksponenditud regressioonikoefitsiente.

Tulemustest on näha, et tunnused, mis prognoosivad tõenäosust selle kohta, kas riigipoolse digijälgimise suhtes ollakse neutraalsed või pigem ei aktsepteerita seda, on sugu, põlvkond, usaldus riigiasutuste vastu, privaatsuse olulisus, demokraatia pooldamine, sallivus eraettevõtete digijälgimise suhtes. Kahte äärmuslikku gruppi – aktsepteerijad ja mitte-aktsepteerijad – kuulumist prognoosivad põlvkond, usaldus riigiasutuste vastu, privaatsuse olulisus, mure oma andmete kontrolli üle, demokraatia pooldamine, tugeva riigi pooldamine ning sallivus eraettevõtete jälgimise suhtes. Üldise riigipoolse digijälgimise aktsepteerimine Eestis ei ole regressioonanalüüsi põhjal seotud selliste tunnustega nagu rahvus, kõrghariduse olemasolu ja riigipoolse jälgimise kogemused.

Soo tunnuse puhul on olulisusnivool 0,05 tegemist statistiliselt olulise seosega prognoosimaks kuulumist kas mitte-aktsepteerijate või neutraalsete hoiakutega rühma ($p<0,05$). Võrreldes meestega, kuuluvad naised sagedamini gruppi, kus riigipoolsesse digijälgimisse suhtutakse pigem neutraalselt ning mehed seega kuuluvad rohkem mitte-aktsepteerijate hulka. Kõikide mudelisse kaasatud tunnuste samaks jäädes on naistel meestega võrreldes 1,56 korda suurem tõenäosus omada neutraalset hoiakut digijälgimise suhtes. Soolised erinevused puuduvad võrdluses mitte-aktsepteerijad vs aktsepteerijad, seega on meestel ja naistel sarnane tõenäosus kuuluda kas ühte või teise gruppi.

Põlvkondade analüüsimisel on taustakategooriaks noorem põlvkond. Mõlemad võrdluspaarid (mitte-aktsepteerijad vs neutraalsed ja mitte-aktsepteerijad vs aktsepteerijad) puhul esineb statistiliselt olulisi erinevusi gruppide vahel ($p<0,05$ ja $p<0,01$). Selgub, et võrreldes noorema põlvkonnaga on vanemal põlvkonnal 1,53 korda suurem tõenäosus omada neutraalsemat hoiakut ning 2,44 korda suurem tõenäosus kuuluda aktsepteerijate hulka kui mitte-aktsepteerijate hulka. Seega joonistub selgelt välja, et noored suhtuvad riigipoolsesse digijälgimisse kriitilisemalt ja kuuluvad suurema tõenäosusega nende hulka, kes jälgimist ei aktsepteeri. Vanem põlvkond on jälgimise suhtes leplikum.

Järgmine oluline tunnus, mis on seotud riigipoolse digijälgimise aktsepteeritavusega, on *usaldus riigiasutuste vastu*. Mõlema võrdluspaari puhul on tegemist statistiliselt oluliste grupisiseste erinevustega ($p<0,01$). Selgub, et mida kõrgem on usaldus, seda tõenäolisemalt kuulutakse mitte-aktsepteerijate asemel neutraalsete ja aktsepteerijate hulka. Kui usaldus riigiasutuste vastu tõuseb ühe ühiku võrra, suureneb tõenäosus kuuluda mitte-aktsepteerijate grupi asemel neutraalsete hulka 1,46 korda ning aktsepteerijate hulka 1,73 korda.

Inimeste hinnangud *privaatsuse olulisusele* kujunes samuti oluliseks tunnuseks prognoosimaks riigipoolse digijälgimise aktsepteerimist ($p<0,1$ ja $p<0,01$). Privaatsuse olulisus on negatiivselt seotud jälgimise aktsepteeritavusega, mis tähendab, et mida kõrgemalt hinnatakse enda privaatsust, seda enam kuulutakse nende hulka, kes jälgimist ei aktsepteeri ning vähem ollakse kas neutraalsed või aktsepteerivad. Riskisuhteid hinnates selgub, et kui privaatsuse olulisus tõuseb ühe ühiku võrra, on tõenäosus kuuluda mitte-aktsepteerijate asemel neutraalsete hulka 1,14 korda väiksem ning aktsepteerijate hulka 1,35 korda väiksem.

Mure enda isiklike andmete privaatsuse ja kontrolli üle on oluliseks tunnuseks prognoosimaks, kas kuulutakse mitte-aktsepteerijate või aktsepteerijate hulka ($p<0,1$). Võrdluspaaril mitte-aktsepteerijad *vs* neutraalsed puuduvad selle tunnuse lõikes statistiliselt olulised grupisisesed erinevused ning sarnase tõenäosusega kuulutakse mõlemasse gruppi. Kui mure andmete kontrolli üle kasvab ühe ühiku võrra, väheneb tõenäosus aktsepteerida riigipoolset digijälgimist 1,01 korda.

Oluline seos riigipoolse jälgimise aktsepteerimisega on ka varasemad *kokkupuuted privaatsusesse sekkumisega* ($p<0,05$) ehk kui privaatsuse sekkumise kogemuste näitaja kasvab ühe ühiku võrra, väheneb kuulumine aktsepteerijate hulka 1,22 korda ehk 22% ning kuulutakse enam mitte-aktsepteerijate gruppi. Mitte-aktsepteerijate ja neutraalsete vahel statistiline olulisus puudub ning mõlemasse gruppi kuulutakse seega sarnase tõenäosusega.

Vastajad, kes kaldusid uuringus *pooldama demokraatiat ning sõnavabadust*, kuuluvad mitte-demokraatlike hoiakutega vastajatega võrreldes suurema tõenäosusega nende hulka, kes riigipoolset digijälgimist ei aktsepteeri ($p<0,05$). Kui demokraatiat pooldavad hoiakud kasvavad ühe ühiku võrra, väheneb tõenäosus kuuluda mitte-aktsepteerijate grupi asemel neutraalsesse gruppi 1,18 korda ehk 18% võrra ning aktsepteerijate gruppi 1,23 korda ehk 23% võrra. Seega tuleb tulemustest selgelt välja, et mida rohkem hinnatakse sõnavabadust ja demokraatlikke põhimõtteid, seda tugevamalt ollakse riigipoolse digijälgimise vastu.

Vastupidiselt demokraatia pooldajatele, ilmneb andmetest, et *tugevama riigi pooldajad* või siis *autoritaarsemate hoiakutega* vastajad on riigipoolse jälgimise suhtes aktsepteerivamad ($p<0,05$). Analüüsides nende vastajate kuulumist mitte-aktsepteerijate vs aktsepteerijate hulka, selgub, et kui autoritaarsed hoiakud suurenevad ühe ühiku võrra, suureneb tõenäosus kuuluda pigem aktsepteerijate hulka 1,27 korda.

Analüüsi kaasatud viimane statistiliselt oluline tunnus prognoosimaks riigipoolse digijälgimise aktsepteerimist on *sallivus eraettevõtete digijälgimise suhtes*. Jällegi on mõlema võrdluspaari puhul tegemist statistiliselt oluliste erinevustega ($p<0,01$) ning selgub, et tunnus on riigipoolse jälgimise aktsepteerimise suhtes positiivse seosega. See tähendab, et mida suurem on sallivus eraettevõtete poolt teostatava jälgimise suhtes, seda enam kuulutakse nende hulka, kes suhtuvad ka riigipoolsesse digijälgimisse neutraalselt või aktsepteerivalt ning vähem kuulutakse nende hulka, kes jälgimist ei aktsepteeri. Kui ettevõtete poolne jälgimine kasvab ühe ühiku võrra, suureneb tõenäosus kuuluda neutraalsesse gruppi 1,41 korda ning aktsepteerijate hulka 1,90 korda võrreldes kuulumisega mitte-aktsepteerijate hulka.

Tabel 7. Multinomiaalse logistilise regressioonanalüüsi mudel

	Sallivus riigipoolse digijälgimise suhtes			
	Neutraalne hoiak		**Aktsepteerib jälgimist**	
	Regressiooni-kordaja	Riskisuhe	Regressiooni-kordaja	Riskisuhe
Sugu (naine)	**0.445****	**1.56**	0.007	1.01
	-0.176		-0.199	
Põlvkond (vanem)	**0.424****	**1.53**	**0.894*****	**2.44**
	-0.182		-0.209	
Rahvus (muu rahvus)	-0.017	0.98	0.354	1.42
	-0.266		-0.293	
Kõrgharidus (olemas)	-0.043	0.96	-0.026	0.97
	-0.12		-0.137	
Usaldus riigiasutuste vastu	**0.376*****	**1.46**	**0.551*****	**1.73**

	Sallivus riigipoolse digijälgimise suhtes			
	Neutraalne hoiak		Aktsepteerib jälgimist	
	Regressiooni-kordaja	Riskisuhe	Regressiooni-kordaja	Riskisuhe
	-0.081		-0.095	
Privaatsuse olulisus	**-0.129***	**0.88**	**-0.299*****	**0.74**
	-0.071		-0.078	
Mure privaatsuse ja andmete kontrolli üle	-0.004	1.00	**-0.009***	**0.99**
	-0.004		-0.005	
Privaatsusesse sekkumise kogemused	-0.08	0.92	**-0.204****	**0.82**
	-0.074		-0.086	
Riigipoolse jälgimise kogemus	0.098	1.10	0.069	1.10
	-0.061		-0.069	
Demokraatia pooldamine	**-0.159****	**0.85**	**-0.205****	**0.81**
	-0.076		-0.087	
Tugeva riigi pooldamine	0.044	1.04	**0.240****	**1.27**
	-0.087		-0.096	
Sallivus eraettevõtete digijälgimise suhtes	**0.341*****	**1.41**	**0.643*****	**1.90**
	-0.085		-0.096	
Vabaliige	-0.66	0.52	**-1.231****	**0.29**
	-0.434		-0.496	
N	1083			
McFaddeni kordaja	0.098			

*p<0.1; **p<0.05, ***p<0.01
Usaldusnivoo 95%
Sõltuva tunnuse taustakategooria: ei aktsepteeri riigipoolset digijälgimist
Taustakategooria 'sugu': mees
Taustakategooria 'põlvkond': noorem põlvkond
Taustakategooria 'rahvus': eestlane
Taustakategooria 'kõrgharidus': ei ole kõrgharidust

4.3 Seosed hoiakute ja käitumise vahel – kas riigipoolse digijälgimise aktsepteerimine mõjutab internetiosalust ja privaatsuskäitumist?

Järgnevalt analüüsin, kas riigipoolsesse digijälgimisse suhtumine on seotud nn jahutava mõjuga (*chilling effect*) ehk kas jälgimise aktsepteerimine või mitte-aktsepteerimine võib muuta inimeste internetikäitumist suunas, kus enda tegevusi hakatakse piirama, püüdes käituda vastavalt tajutud ühiskondlikele normidele. Samuti analüüsin, kas hoiakud riigipoolse jälgimise suhtes on seotud inimeste privaatsuskäitumisega veebis.

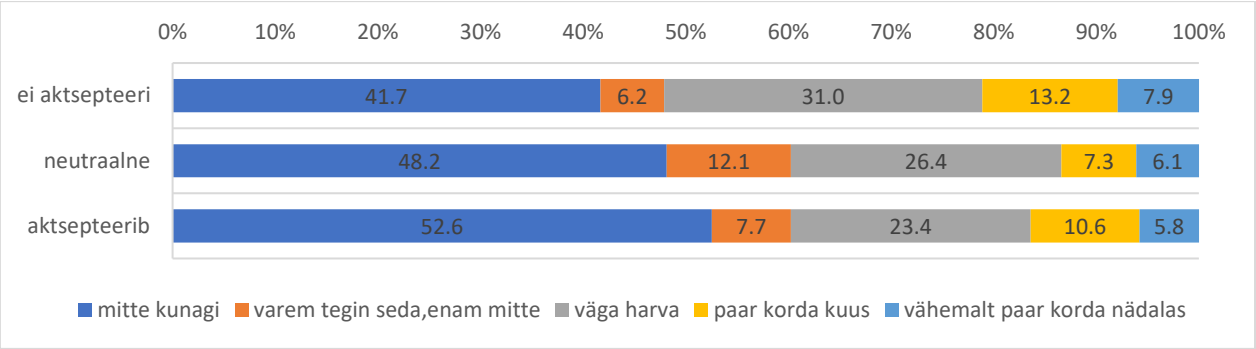
4.3.1 Internetiosalus

Risttabelite põhjal tehtud analüüsist selgus, et peaaegu ükski vaadeldavatest internetitegevustest polnud seotud riigipoolse digijälgimise aktsepteeritavusega. Nende tegevuste hulka kuulusid

piltide üleslaadimine, videote üleslaadimine, iseenda kohta info jagamine sotsiaalmeedias (nt Facebook, Twitter, Snapchat), meediauudiste jagamine sotsiaalmeedias, uudiste või artiklite kommenteerimine portaalides või sotsiaalvõrgustikes, foorumites sõnavõtmine (postitamine või kommenteerimine, nt Facebooki gruppides, Delfi foorumites, Perekoolis) ning liitumine mõne kampaania või protestiga või petitsioonile allkirja andmine. Seega pole oluline, kas ollakse jälgimise poolt, vastu või neutraalsete hoiakutega, nimetatud tegevusi tehakse ühtemoodi ning nende tegevuste suhtes ei ilmnenud enesetsensuuri, mis oleks seotud vastumeelsusega riigipoolse digijälgimise suhtes nagu võis algselt teooria põhjal eeldada.

Oli aga üks tunnus, mis kujunes statistiliselt oluliseks ning selleks tegevuseks on *muusika, filmide ja programmide allalaadimine või jagamine, nt Apple'i poest, Bittorrent'ist* vms (Crameri $V=0{,}106$, $p<0{,}01$). Tegemist on ainukese tegevusega vastajatele etteantud nimekirjas, mis võib viidata ka ebaseaduslikule tegevusele, juhul kui filmide, muusika või programmide allalaadimine on toimunud piraatluse teel. Tulemustest selgub üllatuslikult, et need, kes aktsepteerivad jälgimist rohkem, laadivad vähem internetist sisu alla, kui need, kes riigipoolset jälgimist ei aktsepteeri (vt Joonis 9).

Kuna väidete analüüsist selgus, et vanem põlvkond on aktsepteerivam riigipoolse digijälgimise suhtes ja tegemist on sihtrühmaga, kelle interneti tegevuste hulka kuigi tihti ehk ei kuulu filmide, muusika või programmide allalaadimine, siis otsustasin tulemuste paremaks tõlgendamiseks vaadata antud tunnuseid eraldi ka põlvkondade lõikes. Selgus, et vanemaealistest polnud muusika, filmide või programmide allalaadimise või jagamisega kokku puutunud ligi 70% sihtrühmast, nooremaealistest vaid 27%. Kui võtta kokku need, kes on tegevust teinud vähemalt paar korda kuus, selgub, et vanemas põlvkonnas on neid riigipoolset jälgimist aktsepteerijate hulgas 11% ja mitte-aktsepteerijate hulgas 8%, nooremas põlvkonnas on osakaalud vastupidised – mitte-aktsepteerijatest on vähemalt paar korda kuus midagi alla laadinud 29%, aktsepteerijate hulgas on sama näitaja 24%. Põlvkondade analüüsi tulemusena selgus siiski, et noorte põlvkonnas statistiline olulisus puudub, see-eest vanemas põlvkonnas on vastuste jaotuses olulised erinevused (Crameri $V=0{,}144$, $p=0{,}02$). Seega tundub Joonisel 9 nähtav tulemus olevat ikkagi mõjutatud rohkem vanuserühmast kui riigipoolse jälgimise aktsepteeritavusest.



Joonis 9. Muusika, filmide, programmide allalaadimine või jagamine (nt Apple'i poest, Bittorrent'ist) olenevalt hoiakutest riigipoolse digijälgimise suhtes

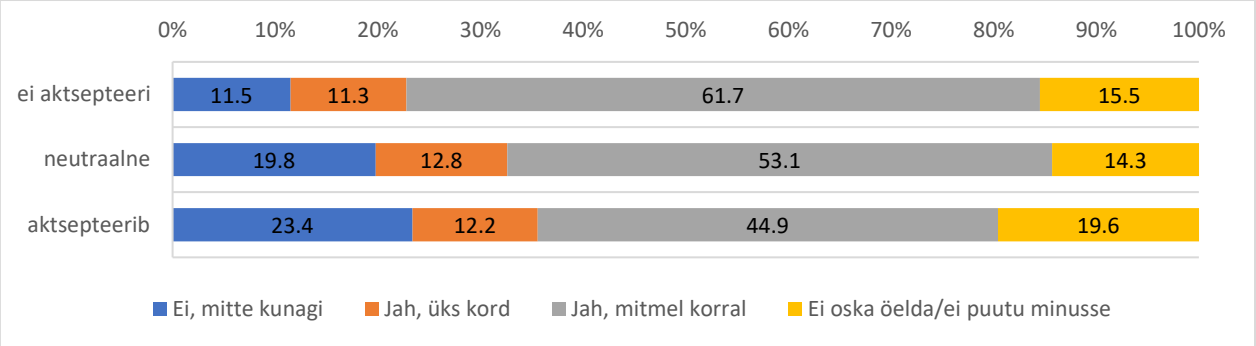
4.3.2 Privaatsuskäitumine veebis

Järgnevalt analüüsin, kas riigipoolse digijälgimise tolereerimine võiks olla seotud inimeste privaatsuskäitumisega internetis. Selle välja selgitamiseks vaatasin kolme privaatsusega seotud tegevust lähemalt.

Reeglite ja tingimuste lugemine enne uue äpi (ehk rakenduse) või veebikeskkonna kasutamist ei ole Eestis seotud sellega, kuivõrd aktsepteeritakse riigipoolset digijälgimist. Üldisemaid numbreid vaadates näeme, et 18% vastas, et pole kunagi reegleid ja tingimusi enne uue rakenduse kasutamist lugenud, 19% on ühe korra lugenud ning ligi 50% on mitmel korral lugenud. Võrdluseks välja tuues olid Rootsi osakaalud suhteliselt sarnased, kuid kui väidete analüüsist nähtus, et Portugali vastajad olid oluliselt enam digijälgimise vastu ja varasemate uurimuste järgi on portugallased oluliselt enam mures oma privaatsuse ja andmete üle, siis kasutustingimuste lugemine pole nii levinud praktika kui Eestis ja Rootsis – 29% vastajatest pole kunagi lugenud, 46% on ühe korra lugenud ja mitmel korral on lugenud 24%. Mõnevõrra võib selline olukord viidata privaatsuse paradoksile, kus küll tuntakse suurt muret oma andmete üle, kuid samal ajal nõustutakse enam rakenduste reeglite ja tingimustega, neid kõigepealt läbi lugemata.

Privaatsussätete muutmine sotsiaalvõrgustikus, et piirata kolmandatel osapooltel enda andmete kasutamist, on aga Eesti vastajate põhjal oluliselt seotud hoiakutega riigipoolse digijälgimise suhtes (Crameri V = 0,110, $p<0,01$). Need, kes aktsepteerivad enam riigipoolset digijälgimist, on muutnud privaatsussätteid vähem ja jälgimist mitte-aktsepteerijad oluliselt enam. Jälgimist pooldavate seas on 45% muutnud sätteid mitmel korral, mitte-pooldajate seas aga 62% (vt Joonis 10). Vaadates tunnust põlvkonna lõikes, selgub taaskord, et vanuserühm võib siin suurt rolli mängida. Kui noorte seas statistiliselt olulised erinevused gruppide vahel puuduvad ning keskmiselt ligi 80% neist on vastanud, et on muutnud privaatsussätteid mitmel korral, siis

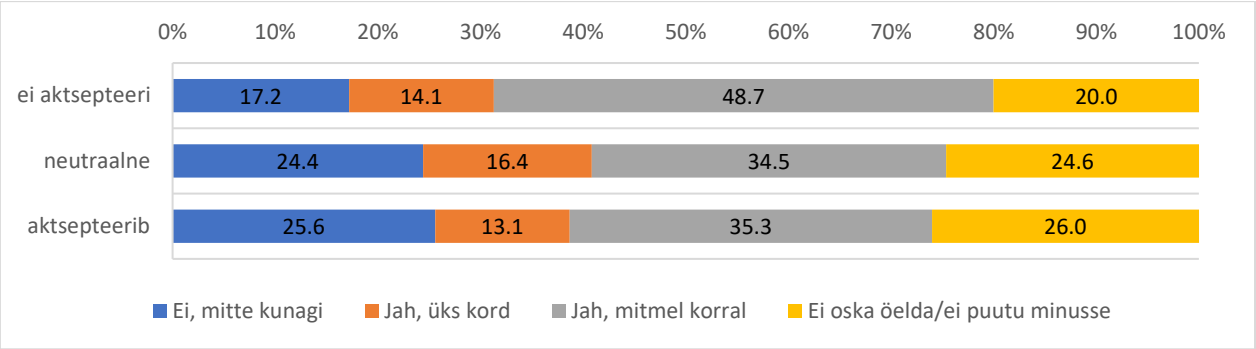
vanemaealiste puhul on oluliselt enam neid, kes pole seda mitte kunagi teinud või kes ei oska öelda. Oluliseks teguriks võivad siinkohal olla digioskused, mis vanemas vanuserühmas on tunduvalt madalamad (Crameri V=0,507, p<0,01), ning seega on tõenäoliselt privaatsussätete muutmine jäänud suuresti oskuste taha. Edasine lisavaade andmetesse näitab, et kui teha sarnane risttabel nagu Joonisel 10, kuid mitte kõigi vastajate seas, vaid ainult nende seas, kelle digioskused on vähemalt keskmisel tasemel, jääb kehtima ikkagi seos, kus jälgimist mitte-aktsepteerijad on oluliselt enam mitmel korral privaatsussätteid muutnud (Crameri V=0,111, p<0,01).



Joonis 10. Privaatsussätete muutmine mõnes sotsiaalvõrgustikus, et piirata enda andmete kasutamist sõltuvalt hoiakutest riigipoolse digijälgimise suhtes

Viimase privaatsust puudutava tegevusena uurisin seda, *kas ollakse kunagi loobutud mõne veebilehe või äpi kasutamisest, kuna ei soovitud, et neid seal jälgitakse* (Crameri V = 0,102, p<0,01). 25,6% jälgimise aktsepteerijatest pole kunagi selletõttu loobunud mõne veebilehe või rakenduse kasutamisest. Mitte-aktsepteerijate seas oli sama näitaja 17,2% ning oluliselt suurem oli ka nende osakaal, kes on mitmel korral loobunud mõne veebilehe või rakenduse kasutamisest (vt Joonis 11).

Kui eelneva kahe küsimuse puhul võisid rolli mängida vanemaealiste väiksemad digioskused ning seega võis madalam privaatsuskäitumine olla tingitud ka teadmiste puudumisest, siis eeldaks, et veebilehe või äpi kasutamisest loobumine nii konkreetseid teadmisi ja oskusi ei vaja (kui, siis võib-olla rakenduse eemaldamise oskused oma seadmest). Heites taaskord pilgu põlvkondade-vahelistele erinevustele, on seekord märgata mõlemas vanuserühmas sarnast mustrit – aktsepteerijad on vähem loobunud mõne veebilehe või rakenduse kasutamisest ning mitte-aktsepteerijad on oluliselt enam seda mitmeid kordi teinud. Kui võtta jällegi aluseks vaid digioskustega kasutajate tulemused, jääb oluline seos endiselt kehtima (Crameri V=0,102, p<0,01) ning riigipoolset jälgimist mitte-aktsepteerijad on enam loobunud mõne rakenduse kasutamisest, et hoiduda seal teostatavast jälgimisest.



Joonis 11. Loobunud mõne veebilehe või äpi kasutamisest, kuna ei soovinud, et neid seal jälgitakse sõltuvalt hoiakutest riigipoolse digijälgimise suhtes

5 JÄRELDUSED JA DISKUSSIOON

Käesolevas magistritöös sõnastasin viis peamist uurimisküsimust, millega soovisin uurida, milline on üldine aktsepteeritavus riigipoolse digijälgimise suhtes Eestis, millistel eesmärkidel on aktsepteerimine suurem ning millised taustatunnused võiksid aidata prognoosida kuulumist jälgimise aktsepteerijate, mitte-aktsepteerijate ja neutraalsemate hoiakutega gruppi. Et tulemusi paremini kontekstualiseerida ja tõlgendada, võrdlesin Eesti digijälgimise aktsepteerimist ka kahe võrdlusriigi – Rootsi ja Portugaliga. Lisaks uurisin ka seda, kas suhtumine riigipoolsesse digijälgimisse võiks olla seotud internetiosaluse ning privaatsuskäitumisega veebis.

5.1 Üldine sallivus riigipoolse digijälgimise suhtes

Üldise riigipoolse digijälgimise kohta võis varasemale teooriale tuginedes oletada, et Eestis jääb see pigem neutraalsele tasemele. Samuti oli oodata, et võrdlusriikidega kõrvutades sarnaneb Eesti oma tulemustega Rootsile ning mõlemad riigid on jälgimise suhtes aktsepteerivamad võrreldes Portugali vastajatega.

Hüpoteesid pidasid paika ning analüüsi käigus selgus, et Eesti vastajad on tõesti pigem keskmise sallivusega riigipoolse digijälgimise suhtes. See tähendab, et suurem osa vastustes jäi skaala keskmise vastusevariandi ümber ega kaldunud konkreetselt ei ühe ega teise äärmuse suunas. Ühe võimalusena võib seda põhjendada privaatsuse olulisuse ja murega oma andmete kontrolli ning riigipoolse jälgimise üle, mis eestlaste (ja ka rootslaste) puhul on küllaltki madal nii Eurobaromeetri (Euroopa Komisjon, 2011; 2015) kui ka magistritöös kasutatavate andmete alusel. Seega on neutraalsed või aktsepteerivamad hoiakud ootuspärased. Vähesel määral mure tundmine võib aga omakorda olla põhjustatud mitmest asjaolust, mida ma oma töö raames otseselt ei käsitlenud, kuid mida saaks võimalike põhjustena välja tuua. Näiteks võib usaldus andmeid haldavate institutsioonide vastu olla kõrge, mistõttu muretsetakse vähem andmejälgimise üle. Lisaks võib rolli mängida inimeste vähene teadlikkus sellest, kui palju, milliseid andmeid ja millistel eesmärkidel üldse kogutakse. Kolmanda võimaliku põhjendusena võiks välja tuua ka selle, et inimesed võivad subjektiivselt hinnata enda interneti- ja privaatsussätete kasutamise oskuseid kõrgelt ning seetõttu tunnevad, et omavadki suurt kontrolli oma andmete üle ega tunne muret (Humphreys, 2011; Gandy, 1989). Eesti vastajate seas oli kõige enam neutraalse hoiakuga inimesi, mis võibki viidata pigem asjaolule, et inimestel puudub informatsioon ja teadlikkus riigipoolse jälgimise toimimisest ning seetõttu ei omata kindlat poolt või vastu seisukohta. Kuna magistritöö analüüsi aluseks olev andmestik ei võimaldanud otseselt uurida, milline on inimeste

teadlikkus riigipoolsest jälgimisest, oleks tegu kindlasti olulise teguriga, mille seoseid selles teemavaldkonnas edaspidi täpsemalt uurida.

Rääkides digiühiskonnast, siis on Eestit vaieldamatult ka mujal maailmas tunnustatud kui ühte kõige eesrindlikumat digiriiki. See on üks aspekt, mille poolest oleme rahvusvaheliselt tuntud ja selle maine hoidmiseks ning e-teenuste kasutamise propageerimiseks tehakse pidevalt tööd ja investeeringuid. Selline e-Eesti ülistamine võibki seega suunata kodanikke enam kasutama erinevaid e-lahendusi. Kui Männiste ja Masso (2018) tõid välja, et usaldus organisatsiooni vastu võib olla seotud sellega, kuivõrd vastuvõtlikud ollakse mõne uue tehnoloogia kasutuselevõtu suhtes, siis võimalik, et seos on ka vastupidine. See tähendab, et pidev tehnoloogia ülistamine ja reklaamimine kui midagi, mille poolest oleme teistest paremad ja arenenumad, võib mõjutada meie suhtumist ka riigi organisatsioonidesse ning kasvatab just läbi nende tehnoloogiate usaldust riigiasutuste vastu.

Kui vaadata veel riikidevahelisi erisusi riigipoolse digijälgimise üldises aktsepteeritavuses, siis selgub, et Eesti vastajate hoiakud kattusid enamjaolt Rootsi vastajate hoiakutega – tunnuse *sallivus riigipoolse digijälgimise suhtes* keskmised väärtused olid: Eestis 1,84, Rootsis 1,85 ning Portugalis kõige madalam 1,70. Seega nähtub, et Portugali vastajad olid oluliselt vähem sallivad riigipoolse digijälgimise suhtes võrreldes Eesti ja Rootsiga, kes sarnase tulemusega on jälgimise suhtes tunduvalt leplikumad. Portugali vastajate seas olid ka põlvkonniti kõige väiksemad erinevused, samas kui Eesti ja Rootsi tulemusi iseloomustavad oluliselt suuremad käärid põlvkondade vahel ning vanem põlvkond on oluliselt aktsepteerivam riigipoolse jälgimise suhtes kui noorem põlvkond.

Kuigi Eesti sarnaneb ajaloolise tausta mõttes ehk pigem Portugalile, omades autoritaarse riigikorra kogemusi, jagab Eesti Rootsiga sarnasemaid väärtushinnanguid, mida saab seletada näiteks läbi kuulumise individualistlike vaadetega ühiskondade hulka, kus muuhulgas kaldutakse enam aktsepteerima ka enda üle teostatavat jälgimist (Dinev jt, 2005). Kalmus jt (2022) on tõlgendanud selliseid tulemusi ka ajalooliste mõjutuste valguses, kus Eesti vanem põlvkond usaldab oma taasiseseisvunud riiki, kuna see vastandub radikaalselt Nõukogude Liidule ning selle usalduse mõjul aktsepteerib ka enam jälgimist. Kuigi OECD (2023) andmete järgi oli Portugali usaldus riigiorganisatsioonide vastu üsna kõrge, selgus magistritöö analüüsist, et usaldus oli siiski Eesti ja Rootsiga võrreldes madalam, millest tulenevalt võidakse suhtuda negatiivsemalt erinevatesse jälgimistehnoloogiatesse (Pavone ja Esposti, 2010). Kalmus jt (2022) selgitavad Portugali madalamat usaldust tajutava haavatavusega valitsuse ja majanduslike huvide suhtes ning samuti

läbi struktuurse teabepuuduse Portugali ühiskonnas, mida ilmestab asjaolu, et mida vähem teadmisi omatakse institutsiooni kohta, seda madalam on ka usaldus.

5.2 Millistel eesmärkidel teostatav riigipoolne digijälgimine on aktsepteeritav?

Hinnates erinevaid eesmärke, mis võiksid avaldada mõju digijälgimise aktsepteeritavusele, püstitasin algselt hüpoteesi, et riigipoolne digijälgimine on aktsepteeritavam, kui sellel on konkreetne eesmärk ning eelkõige tolereeritakse jälgimist nendel juhtudel, kus oht ühiskonnale on suurem ja tajutavam. Eesmärkide uurimisel võrdlesin Eesti tulemusi jällegi Rootsi ja Portugali tulemustega.

Ka siinkohal pidasid hüpoteesid paika ning risttabelite kaudu analüüsitud viie väite põhjal, millest üks väide oli toodud ilma igasuguse jälgimise eesmärgita ning ülejäänud nelja väite puhul oli jälgimist põhjendatud, saab öelda, et inimesed on jälgimisele vastuvõtlikumad, kui selleks on olemas konkreetne vajadus. Samuti leidis kinnitust, et nendel juhtudel, mis kannavad endas suuremat ja tajutavamat ohtu ühiskonnale, on riigipoolne jälgimine aktsepteeritavam, mis ühtib ka varasema teadmisega (Davis ja Silver, 2004; Ziller ja Helbling, 2021).

Analüüsitulemustest selgus, et inimeste jaoks on riigipoolne digijälgimine kõige aktsepteeritavam juhul, kui sellega ennetatakse terrorirünnakuid. Terrorirünnakute puhul on tegemist reaalse ohuga inimeludele ning kuigi analüüsitavates riikides ei ole terrorirünnakud kuigi sagedased nähtused, jõuavad meedia vahendusel uudised mujalt maailmast meie kõigini. Näiteks Euroopa Liidus tehti 2020. aastal 57 terrorikatset ja see number hõlmab nii lõppenud, ebaõnnestunud kui ka nurjunud katseid (Terrorism ELis: terrorirünnakud…, 2021). Vigastatute arv oli 54 ning surmasid 21, mis on kahekordne kasv võrreldes 2019. aastaga (Terrorism ELis: terrorirünnakud…, 2021). Et sellist ohtu enda riigis ennetada, on ka inimesed aktsepteerivamad riigipoolse suurema jälgimise suhtes, eesmärgiga tagada turvalisem ühiskond.

Väidete seas aktsepteeriti jälgimist kõige vähem juhul, kui polnud selgelt välja toodud jälgimise põhjust. Nagu ka varasematest uurimustest on selgunud, toimub vahetustehingu teooria järgi privaatsuse ja turvalisuse tehing ikkagi inimeste läbimõeldud kaalutlustel (Wester ja Giesecke, 2019) ning jälgimise aktsepteerimiseks peavad riigiasutused olema läbipaistvad oma eesmärkidest rääkides. Siiski mõnevõrra üllatas, et väite puhul, kus polnud jälgimise põhjendust ette antud (*mind ei häiri, et riigivõimu asutustel on juurdepääs minu andmetele sotsiaalmeedias)*, oli sellega täiesti või üldiselt nõus küllaltki suur osa Eesti vastajatest – 42,2% (võrdluseks aktsepteeris riigipoolset digijälgimist terrorirünnakute ennetamise eesmärgil 65,7% Eesti vastajatest). Valdavalt tekitab

suure osakaalu jällegi vanem põlvkond, noorem põlvkond nii aktsepteeriv sellise jälgimise suhtes siiski ei olnud. Taaskord võib seda tõlgendada kas vanemaealiste suurema riigiasutuste usaldamise või ka madalama aktiivsusega sotsiaalmeedias, sest kui sotsiaalmeedia kasutus on madal või ei kasutata üldse, ei tunta tõenäoliselt ka nii suurt muret selle üle, kas riigil on ligipääs andmetele või mitte.

Rääkides sellest, et jälgimine on aktsepteeritavam juhul, kui jälgimise põhjus on parasjagu aktuaalne ja toimub eesmärgiga ennetada või leevendada mõnda otsest ohtu ühiskonnas, oli üheks huvipakkuvamaks analüüsi osaks väide *Riigivõimu asutustel on õigus jälgida kodanikke digitaalselt (nt droonide, äppide, mobiil-positsioneeringu abil), et ennetada haiguste levikut*. Arvestades, et analüüsi aluseks oleva projekti küsitlustöö toimus 2020. aasta sügisel ning Covid-19 pandeemia keskmes, on tegu väga asjakohase väitega, saamaks teada, millised olid inimeste hoiakud riigipoolse jälgimise suhtes ajal, mil oldi tavapärasest tunduvalt enam teadlikud, et nende üle teostatakse pidevat jälgimist riigi poolt. On teada, et inimeste valmisolek aktsepteerida enda üle teostatavat jälgimist sõltub ka jälgimismeetoditest (Wester ja Giesecke, 2019; Wright ja Watson, 2013) ning Covid-19 tõi endaga kaasa uusi jälgimisviise, mis sisaldasid enam asukoha- ja terviseandmete jälgimist (Chiusi jt, 2020).

Väidet analüüsides selgus, et tegu oli tõepoolest kõige vastuolulisema väitega. Vaadates keskmiseid väärtuseid, on gruppide vahelised erinevused selle väite puhul kõige suuremad. Ootuspäraselt on noored rohkem sellise jälgimise vastu kui vanem põlvkond. Kuigi pandeemia alguses oli olukord kõigi jaoks ärev ning haiguse kohta teati väga vähe, oli siiski teada, et vanemaealised ja terviseprobleemidega inimesed kuuluvad suurema tõenäosusega riskirühma, mis võis panna nad oluliselt enam muretsema nakatumise pärast ning seega aktsepteerima uusi jälgimismeetodeid tõkestamaks haiguse edasist levikut. Noored ja tervemad vastajad, kes on tõenäoliselt ka liikuvamad, tunnetasid ehk sellises jälgimises, mis kogus nende liikumisandmeid ning ka piiras oluliselt igapäevategevusi (erinevate kehtestatud liikumiskeeldude tõttu), suuremat probleemi. Lisaks põlvkondlikele erisustele, oli gruppide vahelisi erinevusi Eesti andmetes märgata ka haridustasemes, kus kõrgharidusega vastajad olid oluliselt enam valmis aktsepteerima riigipoolset digijälgimist eesmärgiga ennetada viiruse levikut ning kõrgharituseta vastajad suhtusid taolisesse jälgimisse suurema kriitikaga.

Teema edasiarendusena võiks aga kriitilisemalt küsida, kas valmisolek mõne suure ohu korral jälgimist enam aktsepteerida on ka tegelikult õigustatud ning kas sellest on ka reaalselt kasu kodanike turvalisuse suurendamisel, milles on kahelnud näiteks Schneier (2003). Võimalik, et

kodanike üle käib pidev jälgimine, mida küll põhjendatakse terrori- või mõne muu ohu ennetamisega, kuid tegelikult on vastu saadav kaitse näiline. Meil lihtsalt pole võimalik kuidagi kontrollida, kas sellel põhjendusel on ka tegelikult alust või toimib see kõigest inimeste rahustamistegevusena.

5.3 Riigipoolse digijälgimise aktsepteeritavust positiivselt mõjutavad tegurid

Enne analüüsi eeldasin, et riigipoolse digijälgimise aktsepteerimine Eestis on seotud põlvkonna, soo, rahvuse, kõrghariduse olemasolu, usaldusega riigiorganisatsioonide vastu, tugeva riigi pooldamise, demokraatia/sõnavabaduse pooldamise, korporatsioonide poolse digijälgimise tolereerimise, riigipoolse jälgimise kogemuste, privaatsuse olulisuse, murega oma andmete kontrolli üle ja privaatsusesse sekkumise kogemustega.

Suures osas pidas eeldus paika, kuid rahvus, kõrghariduse olemasolu ning üllataval kombel ka riigipoolse jälgimise kogemused ei aita prognoosida riigipoolsesse digijälgimisse suhtumist ehk nendel tunnustel puudus statistiliselt oluline seos sõltuva tunnusega.

Vaadates, millised taustatunnused regressioonanalüüsi põhjal riigipoolse digijälgimise aktsepteerimist positiivselt mõjutasid, tõusis esile tunnus *usaldus riigiorganisatsioonide vastu* ning mida suurem on usaldus, seda enam suhtutakse riigipoolsesse digijälgimisse kas neutraalselt või aktsepteerivalt ning kuulutakse väiksema tõenäosusega mitte-aktsepteerijate hulka. Samuti sai juba mainitud, et *põlvkondade* lõikes on jälgimise suhtes aktsepteerivamad vanemaealised võrreldes noorema põlvkonnaga. Noored, kes on digioskuste ja veebis tehtavate tegevuste osas mitmekülgsemad, tajuvad tõenäoliselt enam enda üle teostatavat digijälgimist kui vanem põlvkond, kelle internetis tehtavad tegevused ja oskused ei küüni üldjuhul samale tasemele. Vaid küsimuses, kas riigivõimu asutustel on õigus jälgida internetisuhtlust terrorirünnakute ennetamiseks, on põlvkonnad ühel meelel ning vanuserühm ei mängi rolli. *Soolises* võrdluses olid naised jälgimise suhtes veidi leplikumad kui mehed, kuuludes tõenäolisemalt neutraalsete hulka kui mitte-aktsepteerijate hulka.

Üllatav tulemus oli, et kui rahvus ei ole üldise riigipoolse digijälgimise aktsepteerimise prognoosimisel oluline tunnus, siis binaarsest logilistiliselt regressioonanalüüsist, mis sai põhianalüüsile lisaks kõikide viie väite kohta teostatud (vt LISA 3), selgus, et rahvuse tunnus on väga oluline väite *Mind ei häiri, et riigivõimu asutustel on juurdepääs minu andmetele sotsiaalmeedias* juures. Tegemist on väitega, millel pole konkreetset jälgimise põhjendust toodud. Kui algne eeldus oli, et muust rahvusest vastajad on Eestis pigem rohkem riigipoolse digijälgimise

vastu kui eestlased, siis selle väite puhul olid tegelikud tulemused vastupidised ja muust rahvusest vastajad nõustusid väitega oluliselt enam. Analüüsis kasutatud kvantitatiivsete andmete põhjal on sellisele tulemusele kahjuks küllaltki keeruline seletust pakkuda, kuid millele tasub antud väite juures kindlasti tähelepanu pöörata, on küsimuse sõnastus. Kui kõikide ülejäänud väidete puhul uuriti vastajate nõustumist, kas riigivõimu asutustel on nende meelest õigus teatud eesmärkidel jälgida oma kodanikke, siis esimese väite puhul, kus polnud konkreetset eesmärki mainitud, küsiti hoopis seda, kuivõrd riigivõimu asutuste ligipääs nende sotsiaalmeedia andmetele neid häirib. Seega on selle ühe väite esitlusviis erinev ning küsimus, kuivõrd miski häirib, on suuresti tunnetuslik, sest sõna „häirimine“ võib tähendada vastajatele väga erinevaid asju. Enamik muust rahvusest vastajaid valisid küsitlusankeedi täitmiseks venekeelse versiooni ning sõna „häirima“ võib erinevatesse keeltesse tõlgituna omandada erinevaid tähendusvarjundeid ja mõjutada seeläbi ka tulemusi.

Riigipoolse jälgimise aktsepteeritavus on seotud positiivselt ka *tugeva riigi pooldamise* ning *eraettevõtete-poolse digijälgimise aktsepteerimisega*. Tugeva riigi pooldajad leiavad, et riik toimib nende vajadustest lähtuvalt ning õigustavad seega enam erinevaid tegevusi, usus, et see toob ühiskonnale tervikuna kasu (Pavone ja Esposti, 2010). Seega tulemus, kus tugevama riigi suurem pooldamine tähendab riigipoolse digijälgimise kõrgemat aktsepteerimist, on küllaltki ootuspärane. Eraettevõtete-poolset digijälgimist aktsepteeritakse üldjuhul mingi konkreetse kasu saamise eesmärgil (näiteks, et kasutada vastutasuks mõnda rakendust tasuta vms; Humphreys 2011) ning sellest tulenevalt on andmejälgimine muutunud inimeste jaoks sotsiaalseks normiks (Young ja Quan-Haase, 2013). Võimalik, et inimesed, kes peavad korporatiivset andmejälgimist tavapäraseks, aktsepteerivad enam ka riigipoolset digijälgimist, kuna see toimub veelgi varjatumalt. Kui eraettevõtete-poolset digijälgimist on kergem märgata näiteks läbi suunatud reklaamide, siis riigipoolne jälgimine toimub automaatselt ning mitte-tajutavalt (Whitaker, 1999). Seetõttu ei pruugi inimestel tekkida sellise jälgimise osas suuremat vastumeelsust, sest lihtsalt ei teadvustada sellega kaasnevaid võimalikke ohte ja tagajärgi. Sellise sotsiaalse normi väljakujunemine, kus institutsionaalset jälgimist aktsepteeritakse lihtsalt seetõttu, et sellest ei ole pääsu kasutamaks erinevaid igapäevategevusi lihtsustavaid rakendusi, võib tähendada, et selle paratamatu olemus ei motiveeri inimesi põhjalikumalt uurima, mis sellise andmekogumise taga tegelikult peituda võib. Ning institutsioonide läbipaistmatu tegevus võib seega tegelikult rikkuda inimeste privaatsust ja kodanikuõigusi ning olla ohuks liberaalsele demokraatiale (Wilton, 2017).

5.4 Riigipoolse digijälgimise aktsepteeritavust negatiivselt mõjutavad tegurid

Analüüsitud tunnustest saab välja tuua veel mõned olulised seosed, mis on pigem negatiivse iseloomuga. Negatiivselt on riigipoolse digijälgimisega seotud näiteks privaatsuse olulisus, mure enda isiklike andmete kontrolli üle, demokraatia pooldamine ning privaatsusesse sekkumise kogemused.

Privaatsuse olulisus kujunes oluliseks tunnuseks kõigi viie väite puhul ja on oluline tegur prognoosimaks seega ka üldist suhtumist riigipoolsesse digijälgimisse. Ootuspäraselt väheneb jälgimise aktsepteerimine privaatsuse olulisuse kasvamisega. Kuna riigipoolse jälgimise peamiseks eesmärgiks peetakse turvalisuse suurendamist ning selle teostamiseks toimub põhiline vahetustehing kodanike privaatsuse arvelt (Pavone & Esposti, 2010), on privaatsuse olulisus antud küsimuse juures oodatult niivõrd tugeva seosega.

Nagu ka juba mainitud, on eestlaste mure oma andmete üle suhteliselt madal. Tunnus *mure enda isiklike andmete kontrolli üle* kujunes küll oluliseks regressioonmudelis, mille sõltuvaks tunnuseks oli riigipoolse digijälgimise sallivus koondtunnusena, kuid kui vaadata jällegi samade taustatunnustega viie väite kohta eraldi teostatud regressioonanalüüse (vt LISA 3), siis selgub, et ühegi väite puhul ei ilmnenud statistiliselt olulisi seoseid. Ka koondtunnusega läbiviidud regressioonanalüüsis oli seos võrdlemisi nõrk – mure kasvades väheneb tõenäosus kuuluda jälgimist aktsepteerijate asemel hoopis mitte-aktsepteerijate hulka 1% võrra. Võimalik, et tulemused viitavad ka taaskord inimeste teadmatusele riigipoolse jälgimise toimimisest ja selle tagajärgedest. Kuna seos on küllaltki nõrk, tähendab see seda, et ka need vastajad, kes tunnetavad suurt muret isiklike andmete kontrolli üle, ei tunneta tegelikult eriti probleemina seda, et riigivõimu asutused omavad ligipääsu nende sotsiaalmeedia- või muudele digiandmetele. Tõenäoliselt on nendel, kes tunnevad andmete kontrolli üle enam muret, suurem kartus siiski eraettevõtete, häkkerite jt ees, kelle puhul on teada rohkem juhtumeid isiklike andmete ärakasutamise kohta. Ka riigiasutustes on ette tulnud andmelekkeid, mis on arvatavasti mõjunud negatiivselt nende usaldusväärsusele kodanike tundlike andmete kaitsmisel, kuid üldiselt on selliseid skandaale siiski vähem olnud.

Demokraatlike väärtuste pooldamine prognoosib kuulumist kas riigipoolset jälgimist aktsepteerijate või mitte-aktsepteerijate hulka ehk mida suurem demokraatlike väärtuste pooldaja ollakse, seda enam kuulutakse mitte-aktsepteerijate hulka ning ei kuuluta aktsepteerijate ja neutraalsete hoiakutega gruppi. Jällegi on tegu loogilise tulemusega, kuna ka varasema kirjanduse põhjal (nt Hadjimatheou, 2013) on viidatud asjaolule, et jälgimistegevuse ja autoritaarsuse vahel

võib esineda kausaalne seos, mistõttu võib riigipoolne jälgimistegevus kujutada ohtu liberaalsetele demokraatlikele ühiskondadele.

Privaatsusesse sekkumise kogemused on samuti seotud sellega, kuidas suhtutakse riigipoolsesse jälgimisse, ning mida enam on olnud riive kogemusi, seda ettevaatlikumad ollakse ka jälgimise suhtes ja kuulutakse aktsepteerijate asemel hoopis mitte-aktsepteerijate hulka. Isiklikud kogemused ja oskused end kaitsta privaatsusesse sekkumise eest aitavad tunduvalt enam tajuda enda üle teostatavat jälgimist (Tanner, 2015), mistõttu ongi eeldatav, et privaatsuse riivega kokkupuutunute seas on jälgimine vastumeelsem.

Negatiivse suhtumisega riigipoolsesse digijälgimisse on Eestis ka noorem *põlvkond*, mida juba eelnevalt tõlgendasin.

5.5 Riigipoolse digijälgimise aktsepteeritavuse seos internetiosaluse ja privaatsuskäitumisega

Saades ülevaate riigipoolse digijälgimise aktsepteeritavuse kohta, huvitas mind ka see, kas ja kuidas on omavahel seotud äsja uuritud hoiakud ja tegelik käitumine veebis. Seega uurisin analüüsi käigus ka eeldust, et internetiosalus ja privaatsuskäitumine on seotud riigipoolse jälgimise aktsepteeritavusega. Teooria põhjal võis oletada, et mida sallivam ollakse riigipoolse jälgimise suhtes, seda vabamalt tehakse erinevaid toiminguid internetis, kuid rakendatakse oluliselt vähem privaatsusmeetmeid.

Hüpotees otseselt paika ei pidanud ning suhtumine riigipoolsesse digijälgimisse ei ole üldjuhul seotud Eesti inimeste internetikäitumisega. Mõningal määral võib siiski täheldada aktiivsemat privaatsusstrateegiate kasutamist, kui suhtutakse vastumeelsemalt riigipoolsesse digijälgimisse. Kuigi oli kahtlus, et sellised tulemused privaatsussätete kasutamise kohta võivad suuresti olla mõjutatud vanusest, sest vanemaealised vastajad väljendasid oluliselt suuremat nõustumist riigipoolse digijälgimisega, kuid nende digioskused ja teadmised privaatsusstrateegiate rakendamisest võivad jääda madalamale tasemele võrreldes noortega, kes on tunduvalt vastumeelsemad riigipoolse jälgimise suhtes, siis tegelikult jäid olulised seosed kehtima ka juhul, kui analüüs sai tehtud ainult nende seas, kelle digioskused olid vähemalt keskmisel tasemel.

Internetiosalust puudutava analüüsi kokkuvõtteks saab öelda, et suhtumine riigipoolsesse digijälgimisse ei mõju otseselt jahutavalt internetiosalusele ning internetikasutajad ei piira selle tõttu oma veebis tehtavaid tegevusi. Kuna varasemad uurimused on täheldanud, et inimesed tajuvad ilmselt rohkem korporatsioonide- kui riigipoolset jälgimist (Humphreys, 2011), siis

tulemuste paremaks tõlgendamiseks analüüsisin andmestiku peal põgusalt kõigi tegevuste seotust ka korporatsioonide-poolse digijälgimise aktsepteerimisega. Saadud tulemused olidki vastupidised – statistiliselt olulised seosed olid olemas peaaegu kõigi tegevustega ning seda suunas, kus korporatsioonide-poolse jälgimise mitte-aktsepteerijad osalesid loetletud internetitegevustes oluliselt vähem kui need, kes sellist jälgimist aktsepteerivad. See võibki viidata asjaolule, et riigipoolset digijälgimist ei tajuta nii hästi või kui tajutakse, siis ei tunnetata sellises jälgimises ohtu, mida võib teatud mõttes võtta ka positiivselt, kuna see näitab, et inimesed, kes on teadlikud riigipoolsest andmejälgimisest, ei tunneta, et peaksid piirama oma internetitegevusi või näiteks kartma oma arvamust veebikeskkondades avaldada.

5.6 Meetodikriitika

Magistritöös kasutatud andmestik andis hea võimaluse sisse vaadata teemasse, mis käsitles inimeste hoiakuid riigiasutuste poolt teostatava digitaalse jälgimise suhtes. Kuna olukorda pole Eesti andmete põhjal varem teadaolevalt kuigi palju uuritud, on tegemist olulise panusega antud teemavaldkonda. Töö metoodikas esines ka piiranguid, mida järgnevalt lühidalt käsitlen.

Esiteks ei saa töö tulemusi laiendada kogu elanikkonna peale, sest moodustatud valim kaasas küsitlusse vaid internetikasutajad ning valimi moodustamise aluseks oli peamiselt kaks põlvkonda. Seega pole andmestiku valim hetkel esinduslik ühegi kaasatud riigi elanikkonna suhtes.

Töö analüüsi osas kasutasin ka originaaltunnustest tuletatud koondtunnused, mille sisereliaabluse kontrollis ilmnes, et tunnuse *tugeva riigi pooldamine* näitajad ei olnud nii head kui teistel koondtunnustel. Analüüsi tulemused olid tunnuse lõikes siiski loogilised ja kasutatavad. Kaks küsimust, mille põhjal sai antud koondtunnus tuletatud, võisid olla vastajate jaoks mõnevõrra eksitavad ning põhjustada seetõttu ka madalamat reliaablust.

Lisaks selgus varasemast teooriast ja uurimustest veel üks väga oluline tunnus antud teema juures, mida oleks soovinud kaasata ka enda analüüsi ning mis oleks eelduste kohaselt aidanud oluliselt seletada riigipoolse digijälgimise aktsepteerimist. Selleks tunnuseks on *riigipoolse jälgimise tajumine*. Kahjuks ei võimaldanud andmestik lähemalt uurida, kas, kuidas ja mil määral inimesed tegelikult tajuvad riigipoolse jälgimise toimumist, kuid teemavaldkonna seisukohalt oleks tegemist olulise teguriga, mida edasiarendusena uutes teemakohastes töödes kindlasti lähemalt uurida.

KOKKUVÕTE

Magistritöö eesmärgiks oli anda ülevaade, milline on riigipoolse digijälgimise aktsepteeritavus Eestis ning mil määral võib see olla seotud inimeste internetiosaluse ja privaatsuskäitumisega. Tuginedes projekti „Sotsiaalmeedia jälgimine ja autoritarismikogemused“ (Bolin, Kalmus jt, 2023) andmetele, uurisin, milline on üldine sallivus riigipoolse digijälgimise suhtes, millised jälgimise põhjused on inimestele aktsepteeritavamad, millest võiksid need hoiakud sõltuda ning kas suhtumine jälgimisse võib olla seotud ka internetikäitumisega. Samuti huvitas, kuidas eristuvad Eesti andmed võrdlusriikide Rootsi ja Portugali andmetest, kes olid projekti kaasatud vastavalt oma ajaloolisele taustale. Analüüs koosnes kirjeldavast statistikast, kasutades risttabeleid ja keskmiste võrdlust, ning multinomiaalsest regressioonanalüüsist.

Tulemustest selgus, et üldine sallivus riigipoolse digijälgimise suhtes jääb Eestis pigem neutraalseks või kaldub veidi rohkem aktsepteerimise poole, kuid väga olulist rolli mängib vanus, kus noorem põlvkond on oluliselt vastumeelsem jälgimise suhtes ning vanem põlvkond tunduvalt pooldavam. Eesti vastajate arvamused ühtisid suurel määral Rootsi vastajate omadega ning erinesid oluliselt Portugali tulemustest, kus aktsepteeriti riigiasutuste poolset digijälgimist tunduvalt vähem. Lisaks selgus, et inimesed aktsepteerivad tõenäolisemalt riigipoolset digijälgimist, kui selle vajadus on põhjendatud ning samuti on oluline jälgimise põhjuseks oleva probleemi tõsidus ja ohtlikkus. Analüüsi käigus kujunes kõige aktsepteeritavamaks jälgimise põhjuseks terrorirünnakute ennetamine.

Uurides erinevate taustatunnuste seoseid riigipoolsele digijälgimisele, saab järeldada, et aktsepteerimine on suurem vanemas põlvkonnas, riigiasutusi rohkem usaldavate inimeste seas, nn tugeva riigi pooldajate seas ning nende seas, kes aktsepteerivad ka eraettevõtete-poolset digijälgimist. Sooliselt selgus, et naised on meestega võrreldes rohkem neutraalsema suhtumisega ning mehed kuuluvad suurema tõenäosusega jälgimist mitte-aktsepteerivasse gruppi. Negatiivselt mõjutavad riigipoolse digijälgimisega aktsepteerimist privaatsuse olulisus, demokraatia pooldamine ja mure enda isiklike andmete kontrolli üle. Analüüsi kaasatud taustatunnustest puudus statistiline olulisus rahvusel, kõrghariduse olemasolul ning huvitaval kombel ka varasema riigipoolse jälgimise kogemusel.

Suhtumine riigipoolsesse digijälgimisse ei olnud seotud internetiosalusega, mis tähendab, et jälgimise poolt või vastu hoiakud ei mõjutanud internetis tehtavate tegevuste sagedust. Privaatsuskäitumine veebis võib mõningal määral olla seotud riigipoolse jälgimise aktsepteeritavusega ning suurem vastumeelsus jälgimisele suurendab privaatsuskäitumist, kuid

töös saadud tulemused võisid tuleneda suuresti vanuselistest iseärasustest – vanemaealiste suuremast jälgimise aktsepteerimisest, madalamast internetiosalusest, väiksematest digioskustest ja privaatsusstrateegiate rakendamise oskustest.

Käesolev magistritöö andis seega ülevaate hoiakutest riigipoolse digijälgimise suhtes, kuid kuna töö aluseks oleva projekti andmed andsid infot vaid internetikasutajate ja kahe põlvkonna seisukohtade osas, oleks töö edasiarendusena huvitav teostada analüüs kogu elanikkonna suhtes esindusliku valimi peal, et saada täpsemat ülevaadet olukorrast. Samuti oleks asjakohane uurida hoiakute seotust reaalse riigipoolse jälgimise tajumise ehk teadlikkusega, mida töös kasutatav andmestik ei võimaldanud hetkel uurida.

SUMMARY

Acceptance of State Surveillance and its Relations with Internet Behaviour

The aim of this master's thesis was to provide an overview of the extent to which digital state surveillance is accepted in Estonia and whether it is related to people's online participation and privacy behaviour. Analysis is based on the data of the project "Social Media Surveillance and Experiences of Authoritarianism" (Bolin, Kalmus et al, 2023). I was also interested in comparing how the Estonian data differed from the data of the reference countries Sweden and Portugal, which were included in the project due to their different historical backgrounds. The analysis consisted of descriptive statistics through cross-tabulations and comparison of means, and multinomial regression analysis.

The results showed that general tolerance towards digital state surveillance in Estonia remains rather neutral or leans a little more towards acceptance, but the age group plays a very important role, where the younger generation is significantly more averse to surveillance and the older generation is much more in favor. The opinions of the Estonian respondents largely coincided with those of the Swedish respondents and differed significantly from the results of Portugal, where digital surveillance by state authorities was much less accepted. In addition, it turned out that people are more likely to accept digital state surveillance if its need is justified, and the seriousness and danger of the problem that is the reason for the surveillance is also an important factor. The analysis revealed that the most acceptable reason for surveillance was the prevention of terrorist attacks.

By examining the relationships with various background characteristics on the Estonian sample, it can be concluded that acceptance of state surveillance is greater in the older generation, among people who trust state institutions more, among supporters of the strong state, and among those who also accept digital surveillance by private corporations. In terms of gender, it turned out that women have a more neutral attitude compared to men, and men are more likely to belong to the group that does not accept surveillance. Acceptance of digital state surveillance is negatively influenced by the importance of privacy, support for democracy and concern about control of one's personal data. Among the background characteristics included in the analysis, there was no statistically significant relation with ethnicity, (higher) education and, interestingly, the previous experience of state surveillance.

Attitudes towards digital state surveillance were not related to online participation, which means that attitudes for or against surveillance did not affect the frequency of activities performed on the Internet. Online privacy behaviour may to some extent be related to the acceptance of state surveillance, where a greater aversion to surveillance increases privacy behaviour, but the results obtained in the study may have been largely due to age characteristics - older people's greater acceptance of surveillance, less active online participation, lower digital skills and lower knowledge of implementing privacy strategies.

This master's thesis thus gave an overview of the attitudes towards digital state surveillance, but since the project’s data reflects only the views of internet users and two generations, it would be interesting as a further development of the work to perform an analysis on a representative sample of the entire population in order to get a more accurate overview of the situation. It would also be appropriate to study the connection of state surveillance attitudes with the perception or awareness of state surveillance, which the dataset used in this master’s thesis did not enable to study.

KASUTATUD KIRJANDUS

Amoore, L. (2006). Biometric borders: Governing mobilities in the war on terror. Political Geography 25(3), 336-351. http://dx.doi.org/10.1016/j.polgeo.2006.02.001

Andrejevic, M. (2007). iSpy. Surveillance and power in the interactive era. Lawrence: The University Press of Kansas.

Barnes, S.B. (2006). A privacy paradox: Social networking in the United States. First Monday, 11(9). https://doi.org/10.5210/fm.v11i9.1394

Barriga, A.C., Martins, A.F., Simoes, M.J. ja Faustino, D. (2020). The COVID-19 pandemic: Yet another catalyst for governmental mass surveillance? Social Sciences & Humanities Open, 2(1). https://doi.org/10.1016/j.ssaho.2020.100096

Bauman, Z. ja Lyon, D. (2012). Liquid surveillance: A conversation. Cambridge/Malden: Polity Press.

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D. ja Walker, R.B. (2014). After Snowden: Rethinking the impact of surveillance. International Political Sociology, 8(2), 121–144. https://doi.org/10.1111/ips.12048

Bentham, J. (1791). Panopticon: Or, the inspection-house. Containing the idea of a new principle of construction applicable to any sort of establishment, in which persons of any description are to be kept under inspection, etc. Dublin: Thomas Byrne.

Bolin, G., Kalmus, V., Figueiras, R. ja Björklund, E. (2023). Social media surveillance and authoritarianism. Final report. Södertörn University.

Brown, I. (2015). Social media surveillance. R. Mansell, P.H. Ang, C. Steinfield jt (toim), The International Encyclopedia of Digital Communication and Society (lk 1117-1123). Hoboken, NJ: Wiley. https://doi.org/10.1002/9781118767771.wbiedcs122

Budak, J. ja Rajh, E. (2018). Citizens' online surveillance concerns in Croatia. Surveillance & Society, 16(3), 347–361. https://doi.org/10.24908/ss.v16i3.6907

Budak, J., Rajh, E. ja Anić, I-D. (2015). Privacy concern in Western Balkan countries: Developing a typology of citizens. Journal of Balkan and Near Eastern Studies, 17(1), 29–48. https://doi.org/10.1080/19448953.2014.990278

Büchi, M., Festic, N. ja Latzer, M. (2022). The chilling effects of digital dataveillance: A theoretical model and an empirical research agenda. Big Data & Society, 9(1), 1-14. https://doi.org/10.1177/20539517211065368

Büchi, M., Fosch-Villaronga, E., Lutz, C., Tamò-Larrieux, A., Velidi, S. ja Viljoen, S. (2020). The chilling effects of algorithmic profiling: Mapping the issues. Computer Law & Security Review, 36. https://doi.org/10.1016/j.clsr.2019.105367

Büscher, M., Perng, S.-Y. ja Liegl, M. (2015). Privacy, security, liberty: ICT in crises. International Journal of Information Systems for Crisis Response and Management, 6(4), 72–92. https://doi.org/10.4018/ijiscram.2014100106

Cadwalladr, C. ja Graham-Harrison, E. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian, 17. märts. Kasutatud 02.03.2023. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Chen, H., Beaudoin, C.E. ja Hong, T. (2016). Protecting oneself online: The effects of negative privacy experiences on privacy protective behaviors. Journalism & Mass Communication Quarterly, 93(2), 409–429. https://doi.org/10.1177/1077699016640

Chiusi, F., Fischer, S. ja Spielkamp, M. (2020). Automated decision-making systems in the COVID-19 pandemic: A European perspective. Special issue of the automating society report 2020. AlgorithmWatch. Kasutatud 13.03.2023, https://algorithmwatch.org/automating-society-2020-covid19/

Davis, D.W. ja Silver, B.D. (2004). Civil liberties vs. security: Public opinion in the context of the terrorist attacks on America. American Journal of Political Science, 48(1), 28–46. https://doi.org/10.2307/1519895

Dinev, T., Bellotto, M., Hart, P., Colautti, C., Russo, V. ja Serra, I. (2005). Internet users' privacy concerns and attitudes towards government surveillance-An exploratory study of cross-cultural

differences between Italy and the United States. BLED 2005 Proceedings, 30. Kasutatud 14.02.2023, http://aisel.aisnet.org/bled2005/30

Dinev, T., Hart, P. ja Mullen, M.R. (2008). Internet privacy concerns and beliefs about government surveillance – An empirical investigation. The Journal of Strategic Information Systems, 17(3), 214-233. https://doi.org/10.1016/j.jsis.2007.09.002

Eck, K. ja Hatz, S. (2020). State surveillance and the COVID-19 crisis. Journal of Human Rights, 19(5), pages 603-612. https://doi.org/10.1080/14754835.2020.1816163

ERR (2020). Statistikaamet hakkab viiruse leviku piiramiseks inimeste liikumist jälgima. ERR uudisteportaal, 24. märts. Kasutatud 12.03.2022, https://www.err.ee/1068185/statistikaamet-hakkab-viiruse-leviku-piiramiseks-inimeste-liikumist-jalgima

ERR (2022). Uuring: inimeste usaldus riigikogu ja valitsuse vastu kasvas. ERR uudisteportaal, 29. detsember. Kasutatud 26.03.2023, https://www.err.ee/1608833854/uuring-inimeste-usaldus-riigikogu-ja-valitsuse-vastu-kasvas

Euroopa Komisjon (2011). Eurobaromeetri eriuuring nr 359 raport: Suhtumine andmekaitsesse ja elektroonilisse identiteeti Euroopa Liidus. Kasutatud 22.03.2023, https://joinup.ec.europa.eu/collection/eidentity-and-esignature/document/eu-attitudes-data-protection-and-electronic-identity-european-union

Euroopa Komisjon (2015). Eurobaromeetri eriuuring nr 431 raport: Andmekaitse. Kasutatud 22.03.2023, https://europa.eu/eurobarometer/surveys/detail/2075

Flyverbom, M., Deibert, R., ja Matten, D. (2017). The governance of digital technology, big data, and the internet: New roles and responsibilities for business. Business & Society, 58(1), 1-17. https://doi.org/10.1177/0007650317727540

Foucault, M. (1977). Discipline and punish: The birth of the prison. New York: Vintage Books.

Gandy Jr., O.H. (1989). The surveillance society: Information technology and bureaucratic social control. Journal of Communication, 39(3), 61–76. https://doi.org/10.1111/j.1460-2466.1989.tb01040.x

Gandy Jr., O.H. (1993). The panoptic sort: A political economy of personal information. Boulder: Westview.

Grayling, A.C. (2007). Are ID cards either philosophically or pragmatically justifiable? Prospect Magazine, 26.oktoober. Kasutatud 15.04.2023, https://www.prospectmagazine.co.uk/regulars/52042/graylings-question

Grenville, A. (2010). Shunning surveillance or welcoming the watcher? Exploring how people traverse the path of resistance. E. Zureik, L.L. Harling Stalker, E. Smith, D. Lyon, ja Y. E. Chan (toim), Surveillance, privacy and the globalization of personal information (lk 70–83). Montreal & Kingston, London, Ithaca: McGill-Queen's University Press.

Hadjimatheou, K. (2013). Ethics and surveillance in authoritarian and liberal states. Surveillance: Ethical issues, legal limitations, and efficiency collaborative project. Seventh Framework Programme. Kasutatud 05.01.2023, https://surveille.eui.eu/wp-content/uploads/sites/19/2015/04/D4.4-Ethics-and-surveillance-in-authoritarian-and-liberal-states.pdf

Hofstede Insights. (2023).Hofstede kultuuridimensioonide indeksite võrdlus. Kasutatud 26.03.2023, https://www.hofstede-insights.com/country-comparison/estonia,portugal,sweden/

Huddy, L., Feldman, S., Capelos, T. ja Provost, C. (2002). The consequences of terrorism: Disentangling the effects of personal and national threat. Political Psychology, 23 (3), 485-509. https://doi.org/10.1111/0162-895X.00295

Humphreys, L. (2011). Who's watching whom? A study of interactive technology and surveillance. Journal of Communication, 61(4), 575–595. https://doi.org/10.1111/j.1460-2466.2011.01570.x

in 't Veld, S. (2022). Draft report of investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware (2022/2077(INI). Euroopa Parlament. Kasutatud 06.05.2023. https://www.europarl.europa.eu/doceo/document/PEGA-PR-738492_EN.pdf

Ioannou, A. ja Tussyadiah, I. (2021). Privacy and surveillance attitudes during health crises: Acceptance of surveillance and privacy protection behaviours. Technology in Society, 67. https://doi.org/10.1016/j.techsoc.2021.101774

Kalmus, V., Bolin, G. ja Figueiras, R. (2022). Who is afraid of dataveillance? Attitudes toward online surveillance in a cross-cultural and generational perspective. New Media & Society, 1–23. https://doi.org/10.1177/14614448221134493

Kininmonth, J., Thompson, N., McGill, T. ja Bunn, A. (2018). Privacy concerns and acceptance of government surveillance in Australia. ACIS 2018 - 29th Australasian Conference on Information Systems. Kasutatud 27.03.2023, http://hdl.handle.net/20.500.11937/74937

Kirchgaessner, S. (2022). Israel blocked Ukraine from buying Pegasus spyware, fearing Russia's anger. The Guardian, 23. märts. Kasutatud 05.05.2023. https://www.theguardian.com/world/2022/mar/23/israel-ukraine-pegasus-spyware-russia

Koomen, M. (2021). The encryption debate in the European Union: 2021 update. International Encryption Brief. Carnegie Endowment for International Peace, 31. märts. Kasutatud 05.05.2023. https://carnegieendowment.org/2021/03/31/encryption-debate-in-european-union-2021-update-pub-84217

Kübarsepp, I. (2022). Vastuoluline plaan: Euroopa Liit tahab teha sõnumid politseile nähtavaks. Delfi Ärileht, 18. oktoober. Kasutatud 13.05.2023. https://arileht.delfi.ee/artikkel/120084444/vastuoluline-plaan-euroopa-liit-tahab-teha-sonumid-politseile-nahtavaks

Liive, R. (2020). AKI peadirektor Pille Lehis: mulle teeb muret Euroopa trend ja soov koroonaäppe arendada, Digigeenius portaal, 27. mai. Kasutatud 11.03.2022, https://digi.geenius.ee/rubriik/uudis/aki-peadirektor-pille-lehis-mulle-teeb-muret-euroopa-trend-ja-soov-koroonaappe-arendada/

Lührmann, A., Maerz, S., Grahn, S., Alizada, N., Gastaldi, L., Hellmeier, S., Hindle, G. ja Lindberg, S. (2020). Autocratization surges-resistance grows: Democracy report 2020. V-Dem Institute, 6. september. Kasutatud 15.02.2023, https://v-dem.net/documents/14/dr_2020_dqumD5e.pdf

Lyon, D. (2001). Surveillance society – monitoring everyday life. Buckingham: Open University Press.

Lyon, D. (2007). Surveillance studies: An Overview. Cambridge: Polity.

Lyon, D. (2015). Surveillance after Snowden. Cambridge/Malden: Polity Press.

Mannheim, K. (1928/1952). The problem of generations. Essays on the sociology of knowledge. London: Routledge & Keegan Paul, 276-320.

Manokha, I. (2018). Surveillance, panopticism, and self-discipline in the digital Age. Surveillance & Society, 16(2), 219–237. https://doi.org/10.24908/ss.v16i2.8346

Marx, G. (2005). Seeing hazily (but not darkly) through the lens: Some recent empirical studies of surveillance technologies. Law & Social Inquiry, 30(2), 339-399. https://doi.org/10.1111/j.1747-4469.2005.tb01016.x

Meyrowitz, J. (2007). Watching us being watched: State, corporate, and citizen surveillance. Sümpoosioni "The End of Television? Its Impact on the World (So Far)" ettekanne. Annenberg School for Communication, University of Pennsylvania, Philadelphia.

Michaelsen, A. ja Glasius, M. (2018). Authoritarian practices in the digital age. International Journal of Communication, 12, 3788–3794. Kasutatud 21.02.2023.

Monahan, T. (2010). Surveillance as governance: Social inequality and the pursuit of democratic surveillance. K.D. Haggerty, M.Samatas (toim), Surveillance and Democracy. London: Routledge-Cavendish.

Morozov, E. (2011). The net delusion: How not to liberate the world. London, UK: Allen Lane.

Männiste, M. ja Masso, A. (2018). The role of institutional trust in Estonians' privacy concerns. Studies of Transition States and Societis, 10(2), 22-39. https://doi.org/10.58036/stss.v10i2.676

Nam, T. (2019). What determines the acceptance of government surveillance? Examining the influence of information privacy correlates. The Social Science Journal, 56(4), 530–544. https://doi.org/10.1016/j.soscij.2018.10.001

Norberg, P.A., Horne, D.R. ja Horne, D.A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. Journal of Consumer Affairs, 41(1), 100-126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Nugin, R. ja Kalmus, V. (2018). Social generations and societal changes. P. Vihalemm, A. Masso ja S.Opermann (toim), The routledge international handbook of European social transformations. London: Routledge (lk 298−311).

OECD (2023). Trust in government (indicator). Kasutatud 11.03.2023, https://doi.org/10.1787/1de9675e-en

Preibusch, S. (2015). Privacy behaviors after Snowden. Communications of the ACM, 58(5), 48–55. https://doi.org/10.1145/2663341

Pavlou, P.A. (2011). State of the information privacy literature: Where are we now and where should we go? MIS Quarterly, 35(4), 977-988. https://doi.org/10.2307/41409969

Pavone, V. ja Degli-Esposti, S. (2010). Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security. Public Understanding of Science, 21(5), 556-572. https://doi.org/10.1177/0963662510376886

Pegg, D. ja Cutler, S. (2021). What is Pegasus spyware and how does it hack phones? The Guardian, 18. juuli. Kasutatud 09.05.2023. https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones

Penney, J.W. (2016). Chilling effects: Online surveillance and Wikipedia use. Berkeley Technology Law Journal 31(1), 117–182. Kasutatud 15.04.2023.

Raynes-Goldie, K. (2010). Aliases, creeping and wall cleaning: Understanding privacy in the age of Facebook. First Monday, 15(1). https://doi.org/10.5210/fm.v15i1.2775

Sandford, A. (2020). Hungary: „Critics silenced“ in social media arrests as EU debates Orban's powers. Euronews, 15. mai. Kasutatud 01.01.2023, https://www.euronews.com/my-europe/2020/05/14/hungary-critics-silenced-in-social-media-arrests-as-eu-debates-orban-s-powers

Schneier, B. (2003). Beyond fear. Thinking sensibly about security in an uncertain world. Copernicus Books.

Schneier, B. (2009). Beyond security theater. New Internatsionalist, 1. november. Kasutatud 06.05.2023. https://newint.org/features/2009/11/01/security

Smith, A. (2014). Half of online Americans don't know what a privacy policy is. Pew Research Center, 4. detsember. Kasutatud 02.04.2023, https://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is/

Solove, D.J. (2006). A taxonomy of privacy. University of Pennsylvania Law Review, 154(3), 477–560. https://doi.org/10.2307/40041279

Spence, K. (2005). World risk society and war against terror. Political Studies, 53(2), 284–302. https://doi.org/10.1111/j.1467-9248.2005.00529.x

Statistikaamet (2020). Liikuvusanalüüs, 2019–2020. Kasutatud 13.02.2023, https://www.stat.ee/et/avasta-statistikat/kiirstatistika/liikuvusanaluus-2019-2020

Stoycheff, E., Liu, J., Xu, K. ja Wibowo, K. (2018). Privacy and the panopticon: Online mass surveillance's deterrence and chilling effects. New Media & Society, 21(3), 602–619. https://doi.org/10.1177/1461444818801317

Svenonius, O. ja Björklund, F. (2018). Explaining attitudes to secret surveillance in post-communist societies. East European Politics, 34(2), 123-151. https://doi.org/10.1080/21599165.2018.1454314

Ziller, C. ja Helbling, M. (2021). Public support for state surveillance. European Journal of Political Research 60(4), 994-1006. https://doi.org/10.1111/1475-6765.12424

Zureik, E. ja Hindle, K. (2004). Governance, security and technology: The case of biometrics. Studies in Political Economy, 73(1), 113-137. https://doi.org/10.1080/19187033.2004.11675154

Tanner, A. (2015). How ads follow you from phone to desktop to tablet. MIT Technology Review, 1. juuli. Kasutatud 15.04.2023, https://www.technologyreview.com/2015/07/01/167251/how-ads-follow-you-from-phone-to-desktop-to-tablet/

Terrorism ELis: terrorirünnakud, surmad ja vahistamised 2020. aastal. (2021). Euroopa Parlament, 20. august. Kasutatud 30.03.2023, https://www.europarl.europa.eu/news/et/headlines/society/20210628STO07262/terrorism-elis-terrorirunnakud-surmad-ja-vahistamised-2020-aastal

Tooding, L.-M. (2015). Andmete analüüs ja tõlgendamine sotsiaalteadustes. Tartu: Tartu Ülikooli Kirjastus.

Trüdinger, E.-M. ja Steckermeier, L.C. (2017). Trusting and controlling? Political trust, information and acceptance of surveillance policies: The case of Germany. Government Information Quarterly, 34(3), 421–433. https://doi.org/10.1016/j.giq.2017.07.003

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. Bulletin of Science, Technology & Society, 28(1), 20-36. https://doi.org/10.1177/0270467607311484

Véliz, C. (2020). Privacy is power: Why and how you should take back control of your data. London, UK: Bantam Press.

Voge, C. (2022). EU's contempt for encryption puts all Europeans at risk. EURACTIV. 22, september. Kasutatud 05.05.2023. https://www.euractiv.com/section/digital/opinion/eus-contempt-for-encryption-puts-all-europeans-at-risk/

Walrave, M., Vanwesenbeeck, I., ja Heirman, W. (2012). Connecting and protecting? Comparing predictors of self-disclosure and privacy settings use between adolescents and adults. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 6(1), artikkel 3. https://doi.org/10.5817/CP2012-1-3

Watson, H., ja Wright, D. (2013). Report on existing surveys. Deliverable 7.1, PRISMS Project. Karlsruhe: Fraunhofer Institute for Systems and Innovation Research ISI. https://doi.org/10.24406/publica-fhg-299140

Wester, M. ja Giesecke, J. (2019). Accepting surveillance- An increased sense of security after terror strikes? Safety Science, 120, 383-387. https://doi.org/10.1016/j.ssci.2019.07.013

Whitaker, R. (1999). The end of privacy: How total surveillance is becoming a reality. New York: New Press.

Wilton, R. (2017). After Snowden – the evolving landscape of privacy and technology. Journal of Information, Communication and Ethics in Society, 15(3), 328-335. https://doi.org/10.1108/JICES-02-2017-0010

Wright, D. (2017). Privacy and trust at risk in surveillance societies. Euroopa Komisjon (toim), Trust at risk. Implications for EU policies and institutions (lk 48-68). Luxembourg: Publications Office of the European Union. Kasutatud 04.02.2023, https://op.europa.eu/en/publication-detail/-/publication/e512c11b-e922-11e6-ad7c-01aa75ed71a1

Young, A. L. ja Quan-Haase, A. (2013). Privacy protection strategies on Facebook: The Internet privacy paradox revisited. Information, Communication & Society, 16(4), 479-500. https://doi.org/10.1080/1369118X.2013.777757

LISA 1. Rootsi ja Portugali tunnuste kirjeldav statistika

Tabel 8. Sõltuvate tunnuste kirjeldav statistika Rootsi kohta

Tunnus	Vastanute arv	Keskmine	Standard-hälve	Min	Max	Vastamata
Sallivus riigipoolse digitaalse jälgimise suhtes	1094	1,85	1,42	0	4	0
1. väide: Mind ei häiri, et riigivõimu asutustel on juurdepääs minu andmetele sotsiaalmeedias	1041	2,28	0,95	1	4	53
2. väide: Riigivõimu asutustel on õigus jälgida kodanike internetisuhtlust, et ennetada terrorirünnakuid	1043	2,65	1,03	1	4	51
3. väide: Riigivõimu asutustel on õigus jälgida kodanike internetisuhtlust, et ennetada vägivaldseid proteste või tänavarahutusi	1033	2,48	1,02	1	4	61
4. väide: Riigivõimu asutustel on õigus jälgida kodanike internetisuhtlust, et ennetada välisriikide sekkumist (nt valimistesse);	1010	2,62	1,04	1	4	84
5. väide: Riigivõimu asutustel on õigus jälgida kodanikke digitaalselt (nt droonide, äppide, mobiil-positsioneeringu abil), et ennetada haiguste levikut.)	1010	2,44	1,04	1	4	84

Tabel 9. Sotsiaaldemograafiliste tunnuste sagedusjaotused Rootsi kohta

		Vastanute arv	Osakaal
Sugu	Mees	549	50,2%
	Naine	545	49,8%
Vanuserühm	Noorem põlvkond	553	50,5%
	Vanem põlvkond	541	49,5%
Kõrghariduse olemasolu	Ei	718	65,7%
	Jah	367	33,5%
	Vastamata	9	0,8%

Tabel 10. Sõltumatute tunnuste kirjeldav statistika Rootsi kohta

Tunnus	Vastanute arv	Keskmine	Standard-hälve	Min	Max	Vastamata
Usaldus riigiasutuste vastu	1094	2,12	1,23	0	4	0
Privaatsuse olulisus	1094	3,40	1,42	1	5	0
Riigipoolse jälgimise kogemus	1094	0,79	1,18	0	4	0
Mure andmete kontrolli üle*	906	2,46	0,70	1	4	188
Demokraatia pooldamine	1094	2,73	1,45	0	4	0

Tunnus	Vastanute arv	Keskmine	Standard-hälve	Min	Max	Vastamata
Tugeva riigi pooldamine	1094	1,84	1,43	0	4	0
Privaatsuse riive kogemused	1094	1,43	1,31	0	4	0
Sallivus korporatsioonide-poolse digijälgimise suhtes	1094	1,65	1,09	0	4	0

* Tunnus *mure andmete kontrolli üle* on originaaltunnus ja seetõttu on selles andmelünki (’vastamata/ei oska öelda’). Ülejäänud tunnused on arvutuslikult saadud koondtunnused, millel andmelüngad puuduvad.

Tabel 11. Internetis tehtavate tegevuste vastuste jaotused Rootsi kohta

	Mitte kunagi	Varem tegin seda, enam mitte	Väga harva	Paar korda kuus	Vähemalt paar korda nädalas
Piltide üleslaadimine	16,2%	3,8%	33,8%	24,7%	21,4%
Videote üleslaadimine	37,4%	6,0%	34,3%	12,2%	10,1%
Muusika, filmide, programmide allalaadimine või jagamine	56,6%	10,8%	16,2%	8,7%	7,6%
Iseenda kohta info jagamine sotsiaalmeedias	24,7%	6,8%	28,4%	19,0%	21,2%
Meediauudiste jagamine sotsiaalmeedias	36,5%	4,5%	30,3%	12,6%	16,0%
Uudiste või artiklite kommenteerimine portaalides/sotsiaalvõrgustikes	47,8%	4,5%	25,4%	8,8%	13,5%
Foorumites sõnavõtmine	30,4%	4,8%	29,1%	15,8%	19,9%
Liitumine mõne kampaania/protestiga/petitsioonile allkirja andmine	51,5%	4,0%	27,0%	9,3%	8,2%

Tabel 12. Privaatsuskäitumist puudutavate küsimuste vastuste jaotus Rootsi kohta

	Ei, mitte kunagi	Jah, üks kord	Jah, mitmel korral	Ei oska öelda/ei puutu minusse
Reeglite ja tingimuste lugemine enne uue rakenduse või veebikeskkonna kasutamist?	16,8%	21,1%	52,6%	9,5%
Privaatsussätete muutmine mõnes sotsiaalvõrgustikus, eesmärgiga piirata enda andmete kasutamist	25,0%	18,5%	42,5%	14,0%
Mõne veebilehe või äpi kasutamisest loobumine, kuna ei soovinud, et Teid seal jälgitakse	22,4%	18,6%	47,0%	12,0%

Tabel 13. Sõltuvate tunnuste kirjeldav statistika Portugali kohta

Tunnus	Vastanute arv	Keskmine	Standard-hälve	Min	Max	Vastamata
Sallivus riigipoolse digitaalse jälgimise suhtes	1044	1,48	1,34	0	4	0
1. väide: Mind ei häiri, et riigivõimu asutustel on juurdepääs minu andmetele sotsiaalmeedias	1025	1,96	0,94	1	4	19
2. väide: Riigivõimu asutustel on õigus jälgida kodanike internetisuhtlust, et ennetada terrorirünnakuid	1024	2,36	0,98	1	4	20
3. väide: Riigivõimu asutustel on õigus jälgida kodanike internetisuhtlust, et ennetada vägivaldseid proteste või tänavarahutusi	1021	2,19	0,94	1	4	23
4. väide: Riigivõimu asutustel on õigus jälgida kodanike internetisuhtlust, et ennetada välisriikide sekkumist (nt valimistesse);	1014	2,20	0,96	1	4	30
5. väide: Riigivõimu asutustel on õigus jälgida kodanikke digitaalselt (nt droonide, äppide, mobiil-positsioneeringu abil), et ennetada haiguste levikut.)	1016	2,35	1,03	1	4	28

Tabel 14. Sotsiaaldemograafiliste tunnuste sagedusjaotused Portugali kohta

		Vastanute arv	Osakaal
Sugu	Mees	557	53,4%
	Naine	408	39,1%
	Vastamata	49	7,6%
Vanuserühm	Noorem põlvkond	525	53,4%
	Vanem põlvkond	519	39,1%
Kõrghariduse olemasolu	Ei	475	45,5%
	Jah	561	53,7%
	Vastamata	8	0,8%

Tabel 15. Sõltumatute tunnuste kirjeldav statistika Portugali kohta

Tunnus	Vastanute arv	Keskmine	Standard-hälve	Min	Max	Vastamata
Usaldus riigiasutuste vastu	1044	1,70	1,14	0	4	0
Privaatsuse olulisus	1044	4,42	1,03	1	5	0
Riigipoolse jälgimise kogemus	1044	1,07	1,32	0	4	0
Mure andmete kontrolli üle*	894	2,98	0,67	1	4	150
Demokraatia pooldamine	1044	2,84	1,23	0	4	0

Tunnus	Vastanute arv	Keskmine	Standard-hälve	Min	Max	Vastamata
Tugeva riigi pooldamine	1044	1,92	1,25	0	4	0
Privaatsuse riive kogemused	1044	2,11	1,29	0	4	0
Sallivus korporatsioonide-poolse digijälgimise suhtes	1044	1,91	1,07	0	4	0

* Tunnus *mure andmete kontrolli üle* on originaaltunnus ja seetõttu on selles andmelünki (’vastamata/ei oska öelda’). Ülejäänud tunnused on arvutuslikult saadud koondtunnused, millel andmelüngad puuduvad.

Tabel 16. Internetis tehtavate tegevuste vastuste jaotused Portugali kohta

	Mitte kunagi	Varem tegin seda, enam mitte	Väga harva	Paar korda kuus	Vähemalt paar korda nädalas
Piltide üleslaadimine	10,7%	2,8%	25,1%	24,0%	37,5%
Videote üleslaadimine	21,7%	5,2%	30,9%	17,6%	24,6%
Muusika, filmide, programmide allalaadimine või jagamine	26,7%	11,3%	26,1%	18,3%	17,6%
Iseenda kohta info jagamine sotsiaalmeedias	16,2%	4,9%	31,3%	19,2%	28,4%
Meediauudiste jagamine sotsiaalmeedias	12,6%	4,9%	31,1%	19,7%	31,7%
Uudiste või artiklite kommenteerimine portaalides/sotsiaalvõrgustikes	20,4%	5,0%	30,1%	15,4%	29,2%
Foorumites sõnavõtmine	25,3%	7,6%	30,2%	13,6%	23,4%
Liitumine mõne kampaania/protestiga/petitsioonile allkirja andmine	21,3%	7,3%	46,1%	16,7%	8,6%

Tabel 17. Privaatsuskäitumist puudutavate küsimuste vastuste jaotus Portugali kohta

	Ei, mitte kunagi	Jah, üks kord	Jah, mitmel korral	Ei oska öelda/ei puutu minusse
Reeglite ja tingimuste lugemine enne uue rakenduse või veebikeskkonna kasutamist?	28,5%	45,5%	24,0%	1,9%
Privaatsussätete muutmine mõnes sotsiaalvõrgustikus, eesmärgiga piirata enda andmete kasutamist	22,6%	21,2%	52,3%	3,8%
Mõne veebilehe või äpi kasutamisest loobumine, kuna ei soovinud, et Teid seal jälgitakse	33,7%	14,6%	47,2%	4,6%

LISA 2. Koondtunnuste sisereliaabluse kontroll

Tabel 18. Koondtunnuste reliaabluskoefitsiendid

	Reliaablus-koefitsient
Sallivus riigipoolse digijälgimise suhtes	0.887*
Sallivus korporatsioonide-poolse digijälgimise suhtes	0.723*
Usaldus riigiasutuste vastu	0.860*
Privaatsuse olulisus	0.854*
Riigipoolse jälgimise kogemus	0.774**
Demokraatia pooldamine	0.633**
Tugeva riigi pooldamine	0.551**

* – Cronbachi α; ** – Spearman-Browni koefitsient (kahest küsimusest koosnevate koondtunnuste korral)

LISA 3. Binaarne logistiline regressioonanalüüs viie väite kohta

Tabel 19. Binaarse logistilise regressioonanalüüsi mudel (väide 1)

	Mind ei häiri, et riigivõimu asutustel on juurdepääs minu andmetele sotsiaalmeedias		
	Regressiooni-kordaja	Riskisuhe	p
(Intercept)	-0.239	0.787	-
Sugu (naine)	-0.121	0.886	-
Põlvkond (vanem)	0.593	1.810	***
Rahvus (muu rahvus)	0.690	1.993	***
Kõrghariduse olemasolu (jah)	0.130	1.139	-
Usaldus riigiasutuste vastu	0.270	1.309	***
Privaatsuse olulisus	-0.453	0.636	***
Mure privaatsuse ja andmete kontrolli üle	0.002	1.002	-
Privaatsusesse sekkumise kogemused	-0.324	0.724	***
Riigipoolse jälgimise kogemus	0.066	1.068	-
Demokraatia pooldamine	0.085	1.089	-
Tugeva riigi pooldamine	-0.115	0.892	-
Sallivus eraettevõtete digijälgimise suhtes	0.645	1.905	***

*p<0.1; **p<0.05, ***p<0.01
Usaldusnivoo 95%
Sõltuva tunnuse taustakategooria: ei nõustu väitega

Tabel 20. Binaarse logistilise regressioonanalüüsi mudel (väide 2)

	Riigivõimu asutustel on õigus jälgida kodanike internetisuhtlust, et ennetada terrorirünnakuid		
	Regressiooni-kordaja	Riskisuhe	p
(Intercept)	0.299	1.348	-
Sugu (naine)	0.183	1.201	-
Põlvkond (vanem)	0.282	1.326	-
Rahvus (muu rahvus)	0.364	1.439	-
Kõrghariduse olemasolu (jah)	-0.154	0.858	-
Usaldus riigiasutuste vastu	0.377	1.459	***
Privaatsuse olulisus	-0.233	0.792	***
Mure privaatsuse ja andmete kontrolli üle	0.004	1.004	-
Privaatsusesse sekkumise kogemused	-0.130	0.878	*
Riigipoolse jälgimise kogemus	0.027	1.028	-
Demokraatia pooldamine	-0.099	0.906	-
Tugeva riigi pooldamine	0.038	1.039	-
Sallivus eraettevõtete digijälgimise suhtes	0.352	1.422	***

*p<0.1; **p<0.05, ***p<0.01
Usaldusnivoo 95%
Sõltuva tunnuse taustakategooria: ei nõustu väitega

Tabel 21. Binaarse logistilise regressioonanalüüsi mudel (väide 3)

	Riigivõimu asutustel on õigus jälgida kodanike internetisuhtlust, et ennetada vägivaldseid proteste või tänavarahutusi		
	Regressiooni-kordaja	Riskisuhe	p
(Intercept)	-0.378	0.685	-
Sugu (naine)	0.282	1.325	*
Põlvkond (vanem)	0.624	1.866	***
Rahvus (muu rahvus)	0.138	1.148	-
Kõrghariduse olemasolu (jah)	-0.109	0.897	-
Usaldus riigiasutuste vastu	0.293	1.341	***
Privaatsuse olulisus	-0.132	0.876	**
Mure privaatsuse ja andmete kontrolli üle	-0.002	0.998	-
Privaatsusesse sekkumise kogemused	-0.121	0.886	*
Riigipoolse jälgimise kogemus	-0.015	0.985	-
Demokraatia pooldamine	-0.317	0.728	***
Tugeva riigi pooldamine	0.279	1.321	***
Sallivus eraettevõtete digijälgimise suhtes	0.339	1.404	***

*p<0.1; **p<0.05, ***p<0.01
Usaldusnivoo 95%
Sõltuva tunnuse taustakategooria: ei nõustu väitega

Tabel 22. Binaarse logistilise regressioonanalüüsi mudel (väide 4)

	Riigivõimu asutustel on õigus jälgida kodanike internetisuhtlust, et ennetada välisriikide sekkumist (nt valimistesse)		
	Regressiooni-kordaja	Riskisuhe	p
(Intercept)	-0.185	0.831	-
Sugu (naine)	0.225	1.252	-
Põlvkond (vanem)	0.603	1.827	***
Rahvus (muu rahvus)	0.070	1.073	-
Kõrghariduse olemasolu (jah)	-0.039	0.961	-
Usaldus riigiasutuste vastu	0.349	1.417	***
Privaatsuse olulisus	-0.178	0.837	***
Mure privaatsuse ja andmete kontrolli üle	-0.001	0.999	-
Privaatsusesse sekkumise kogemused	-0.108	0.897	-
Riigipoolse jälgimise kogemus	0.035	1.036	-
Demokraatia pooldamine	-0.170	0.844	**
Tugeva riigi pooldamine	0.158	1.172	**
Sallivus eraettevõtete digijälgimise suhtes	0.273	1.314	***

*p<0.1; **p<0.05, ***p<0.01
Usaldusnivoo 95%
Sõltuva tunnuse taustakategooria: ei nõustu väitega

Tabel 23. Binaarse logistilise regressioonanalüüsi mudel (väide 5)

	Riigivõimu asutustel on õigus jälgida kodanikke digitaalselt (nt droonide, äppide, mobiil-positsioneeringu abil), et ennetada haiguste levikut		
	Regressiooni-kordaja	Riskisuhe	p
(Intercept)	-0.758	0.469	*
Sugu (naine)	0.146	1.158	-
Põlvkond (vanem)	0.497	1.643	***
Rahvus (muu rahvus)	0.371	1.449	-
Kõrghariduse olemasolu (jah)	0.166	1.180	-
Usaldus riigiasutuste vastu	0.419	1.520	***
Privaatsuse olulisus	-0.169	0.845	***
Mure privaatsuse ja andmete kontrolli üle	0.001	1.001	-
Privaatsusesse sekkumise kogemused	-0.171	0.843	**
Riigipoolse jälgimise kogemus	0.069	1.072	-
Demokraatia pooldamine	-0.164	0.849	**
Tugeva riigi pooldamine	0.087	1.090	-
Sallivus eraettevõtete digijälgimise suhtes	0.375	1.454	***

*p<0.1; **p<0.05, ***p<0.01
Usaldusnivoo 95%
Sõltuva tunnuse taustakategooria: ei nõustu väitega

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, Kati Randma,

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose „Riigipoolse digijälgimise aktsepteeritavus ja seosed internetikäitumisega“, mille juhendaja on Veronika Kalmus, 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 4.0, 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.

Kati Randma

21.05.2023