TARTU ÜLIKOOL

Sotsiaalteaduste valdkond

Ühiskonnateaduste instituut

Infokorralduse õppekava

Tõnu Mandel

Telefonikasutaja salajaseks jälgimiseks mõeldud rakenduste sihtrühmad ja nendele suunatud sõnumid

Lõputöö

Juhendaja: Maris Männiste, MA

Tartu 2020

SISUKORD

SISSEJUHATUS 3
1 KIRJANDUSE ÜLEVAADE 5
1.1 Jälgimine 5
1.2 Nuhkvara (ing k *spyware*) 8
1.3 Jälgimist võimaldavate rakenduste võimekus 10
1.4 Privaatsus ja andmetele juurdepääs 13
1.5 Jälgimist reguleeriv seadusandlus Eesti Vabariigis 14
2 VALIM JA MEETOD 18
2.1 Valim 18
2.2 Uurimismeetod 21
3 TULEMUSED JA JÄRELDUSED 22
3.1 Nuhkrakenduste sihtrühmad 22
3.2 Peamised teenuse turundamiseks kasutatavad sõnumid 25
3.2.1 Sõnumid lastevanematele 26
3.2.2 Sõnumid tööandjatele 37
4 ARUTELU 47
KOKKUVÕTE 50
SUMMARY 52
KASUTATUD KIRJANDUS 54

SISSEJUHATUS

Mida aeg edasi, seda rohkem inimesed kasutavad oma elus erinevaid teenuseid ja tehnilisi lahendusi – rakendused, nutitelefonid, tahvlid (Penwarden, 2014). Mitmed rakendustest on aga lisaks enda põhifunktsiooni täitmisele seadistatud kasutaja tegevusi jälgima ja privaatseid andmeid koguma. Teenused, mille puhul kasutaja ise nõustub kasutustingimustega, annavad talle tegelikult võimaluse tutvuda ka sellega, milliseid andmeid tema kohta kogutakse. Teenuste puhul, mida keegi teine kasutab selleks, et varjatult või salaja andmeid koguda, kasutaja seda teha ei saa ning väga tihti ei ole inimene protsessist enne teadlik, kui nende andmete põhjalt tekib näiteks konflikt või tehakse tööandja poolt ka inimese jaoks kahjulik otsus.

Interneti vahendusel on väga kergesti võimalik leida ettevõtteid, kes pakuvad teenuseid/rakendusi, mis võimaldavad salajast andmete kogumist või –jälgimise teenust (Freed jt, 2018). Tasu eest pakutakse kolmandale osapoolele, kelleks aina enam võib olla eraisik, võimalust jälgida teist isikut, viimase teadmata (Gillman, 2019). Kui varasema käsitluse kohaselt on isikud olnud jälgimise objektiks mingi üksuse poolt, siis Lyon (2018) väidab, et jälgimine on midagi milles me ise aktiivselt ja tihti innukalt osaleme.

Salajase jälgimise rakenduse teenusepakkujate sõnumid sihtrühmadele on vähe uuritud teema teadusartiklites. Suurele osale ühiskonnast on veel teadmata, millised on peamised sihtrühmad, kelleni teenusepakkujad püüavad jõuda. Samuti puudub selgus, milliste teemadega tahetakse sihtrühma kuuluvaid inimesi mõjutada teenust kasutama. Teema aktuaalsus seisneb veel selleski, et jälgimisega seotud äppide kasutusaktiivsus on tõusuteel, näiteks koroona viiruse puhul (Jones, 2020; Packham, 2020). Seega parem mõistmine jälgimisega seonduvatest rakendustest on oluline.

Lõputöö eesmärk on kaardistada ning analüüsida sõnumeid, mille kaudu konkreetseid teenuseid turustatakse ja lähtudes püstitatud eesmärgist, otsin vastuseid järgmistele uurimisküsimustele:

1. Millistele sihtrühmadele eelkõige on suunatud telefonikasutaja salajaseks jälgimiseks mõeldud rakendused?
2. Milliseid sõnumeid kasutatakse, et rakendust sihtrühmadele turundada?

Lõputöö jaguneb neljaks peatükiks. Esimeses peatükis annan ülevaate teoreetilistest ja empiirilistest lähtekohtadest, mis aitavad töö tulemusi paremini mõista. Teises peatükis esitan ülevaate kasutatud valimist ja uurimismetoodika kirjelduse. Kolmandas peatükis presenteerin uurimise käigus kogutud tulemusi, samuti annan ülevaate tehtud järeldustest. Neljas peatükk on arutelu, kus diskuteerin üldisemalt tulemuste üle.

1 KIRJANDUSE ÜLEVAADE

Selles peatükis selgitan mõistet nuhkvara ja annan ülevaate jälgimist võimaldavate rakenduste olemusest. Samuti annan ülevaate privaatsuse ja jälgimise mõiste erinevatest käsitlustest ning Eesti Vabariigi õigusruumis kehtivatest varjatud jälgimisega seotud regulatsioonidest.

1.1 Jälgimine

Jälgimine on mitmeti mõistetav. Inglise keelses erialases teadustöös eristatakse jälgimise kohta kolme erinevat mõistet: *tracking* – jälgimine, järgimine; *surveillance* – seire, valve; *monitoring* – jälgimine, seiret tegema (EKI, 2019). Esimese termini puhul leiavad osad autorid (Gabriels, 2016; Simpson, 2014), et tegemist on informatsiooni kogumisega ja subjekti liikumise jälgimisega. McQuade ja Danielson (2019) selgitavad jälgimist (ing k *monitoring*) kui terminit, mis viitab inimeste, kohtade, asjade või protsesside süsteemsele, pidevale ja aktiivsele või passiivsele vaatlusele. Täpsustusena lisab Nolan (2018), et tegemist on ärilistel põhjustel või seadusega lubatud toimingute tegemisega ning enamik seireid pole salajased ja neid saab jälgida. Seire (ing k *surveillance*) on jälgimise (ing k *monitoring*) sihtvorm, mida tavaliselt viiakse läbi konkreetsete andmete või tõendite saamiseks ja toimub ilma isiku teadmata (nt andmeid kogutakse rakendustest) (Nolan, 2018). Tänapäevase seire ühisteks tunnusteks loetakse, et andmed on hõlpsasti kvantifitseeritavad, hästi jälgitavad, tõenäoliselt omavad majandusliku - rahaliselt mõõdetavat dimensiooni – ja on hangitud distantsilt (Lyon, 2018). Salajase jälgimise puhul on samuti oluline mõiste luuramine (ing k *spying*), mis definitsiooni kohaselt on (ise märkamatuks jääda püüdes) kedagi või midagi (usaldamatult) jälgima, varitsema, kellelgi või millelgi silma peal hoidma (EKI, 2020).

David Lyon (2018) nendib, et jälgimine on igapäevane elu tõsiasi. Seda kasutatakse turvalisuse või mugavuse suurendamise vahendina ning mõnikord kasutatakse seda nauditava või rahustava võimalusena. Selliseid võimalusi, mida pakuvad praegu süsteemid või seadmed jälgimiseks, ei ole kunagi varem olnud.

ÜRO Uimastite ja Kuritegevuse Büroo[1] (edaspidi UNODC) (2009) on jaganud enda raportis jälgimise võimalused lähtudes funktsioonipõhistest võimekustest (vt Tabel 1).

Tabel 1 Funktsioonipõhised jälgimise võimalused.

Audio jälgimine	**Visuaalne jälgimine**	**Jälitamisseire**	**Andmejälgimine**
Telefoni pealtkuulamine	Varjatud videovalve seadmed	Globaalne positsioneerimissüsteem (GPS)/transpondrid[2]	Arvuti/internet (nuhkvara/küpsised[3])
Kõne IP-protokolli kaudu (VoIP)	Autosisesed videosüsteemid	Mobiiltelefonid	Blackberries[4]/ mobiiltelefonid
Pealtkuulamise seadmed (saladiktofonid ruumides)	Kehaga kantavad videoseadmed	Raadiosageduslikud identifitseerimise seadmed (RFID)	Klahvivajutuse jälgimine
	Termopildistamine/ ette suunatud infrapunakaamerad (FLIR)	Biomeetriline infotehnoloogia (võrkkesta skaneerimine lennujaamades jne)	
	Sisevõrgu kaamera (CCTV)		

(Allikas: UNODC, 2009)

Jälgimine on jagatud UNODC poolt neljaks suuremaks rühmaks: audio-, visuaalne-, andmejälgimine ja jälitamisseire. Alajaotustest ilmneb, et kõikide gruppide ühiseks nimetajaks on tehnoloogia rakendamine jälgimise teostamiseks. Informatsiooni ja andmete kogumiseks kasutatakse erinevaid abivahendeid, mis varieeruvad füüsilistest seadmetest spetsiaalselt loodud tarkvarani. Neid abivahendeid nimetatakse valvetehnoloogiateks (ing k *surveillance technology*), mille all liigituvad alates droonidest kuni telefoni pealtkuulamise seadmeteni erinevad tehnoloogilised lahendused (Cayford ja Pieters, 2018). Samas märgivad Cayford ja Pieters (2018), et luureametnikud mõistavad valvetehnoloogiate all peamiselt sideandmetega tegelevaid süsteeme (telefoni kõnede, e-kirjad jne monitoorimist). Veelgi detailsemaks minnes sõnastab Ünver (2018) jälgimise ühe eriharu digitaalse seire (ing k *digital surveillance*), kui reaalajas ja retrospektiivis veebijalajälje vaatamise, töötlemise ja katalogiseerimise toiminguna nende osalejate tahte ja/või

[1] United Nations Office on Drugs and Crime ehk UNODC.
[2] Seade raadiosignaali vastuvõtmiseks ja erineva signaali automaatseks edastamiseks. https://www.skybrary.aero/index.php/Transponder
[3] ISO/IEC 27032: HTTP-serveri ja brauseri vahel vahetatavad andmed olekuteabe talletuseks kliendi poolel ja selle võtuks hiljem serveril kasutamiseks, kusjuures brauser võib olla kliendiks või serveriks. Saab kasutada ka kasutaja eelistusi jälgiva ja privaatsust rikkuva nuhkvarana. https://akit.cyber.ee/term/565-cookie-1
[4] Nutitelefon. https://blackberrymobile.com/emea/

teadmiste vastu, kellele sellised andmed kuuluvad. Lyon väitis 2007. aastal, et digitaalsed seadmed suurendavad ainult jälgimisvõimet või aitavad mõnikord edendada teatud tüüpi järelevalvet või muudavad selle olemust (Lyon, 2007).

Suurbritannia salateenistus MI5 (2019) sõnastab enda jälgimistegevuse teabe kogumiseks ning rakendab seda huvipakkuvate organisatsioonide ja nende võtmeisikute, infrastruktuuri, kavatsuste, plaanide ja võimaluste kohta teabe saamiseks.

Peamisteks tehnikateks luureandmete kogumisel on:

- varjatud inimluure allikad ehk „agendid". Agendid on inimesed, kes on võimelised andma salajast teavet uurimise eesmärgi kohta. Agendid ei ole MI5 töötajad;
- suunatud seire (ing k *directed surveillance*), näiteks sihtmärkide järgimine ja/või vaatlemine;
- side pealtkuulamine, näiteks e-kirjade või telefonikõnede jälgimine;
- sideandmed (sealhulgas hulgikommunikatsiooni andmete (ing k *bulk communications data*) kasutamine); teave side kohta. Näiteks „kuidas ja millal" need on loodud, mida tavaliselt hangitakse sideteenuse pakkujatelt;
- massiivsed isikuandmed. Andmekogumid, mis sisaldavad teavet paljude inimeste kohta ja millele pääseb sihipäraselt juurde huvipakkuva teema tuvastamiseks või selle kohta teabe leidmiseks;
- jälitustegevus (ing k *intrusive surveillance*), näiteks pealtkuulamisseadmete panemine kellegi koju või autosse;
- seadmete jälgimine, näiteks varjatud juurdepääs arvutitele või muudele seadmetele (MI5, 2019).

Eespoolt loetletud tehnikate rakendamine viitab sellele, et potentsiaalse kogutava informatsiooni hulk ei ole väike. See toob meid veel ühe olulise termini juurde, milleks on suurandmed. Suurandmete (ing k *Big Data*)[5] iseloomustamiseks kasutatakse suurt mahtu, kiirust ja mitmekesisust. See pakub aga huvi järjest suurenevale osalejate ringile alates avalikust sektorist (valitsusasutused, julgeolekuagentuurid) kuni erasektorini (interneti ettevõtjad, tervishoiuteenuse pakkujad). Andmeid nähakse väärtusliku kaubana nii rahas kui ka vahendina teiste juhtimiseks või

[5] Suurandmed (ing k *Big data*) defineeritakse kui suured ja keerulised andmekogumid, mida on olemasolevate infotehnoloogiliste rakendustega keeruline analüüsida. Suurandmete puhul on tegu suurte andmemahtudega, mis on heterogeensed ehk mitmekesised (andmed kogutakse mitmest allikast ja nad esinevad erineval kujul, sh videosalvestused, e-kirjad, tekst, numbrid jne) ning mida kogutakse ja analüüsitakse reaalajas (või võimalikult selle lähedal). (Eljas-Taal, Veerpalu ja Romanainen, 2017)

isegi kontrollimiseks. (Lyon, 2018) Väga hea näitena toob siin kohal Wil Chivers (2019) sotsiaalmeediaettevõtted ja internetiteenuse pakkujad, kellel on privilegeeritud juurdepääs meie digitaalsetele tehingutele ja kes regulaarselt koguvad ning muudavad need andmed rahaks. Sarnasele järeldusele on samuti jõudnud teisedki autorid (Zaia, 2019; Young, 2012), et elanikkonda jälgivad nii riik, ametkonnad (sh jõustruktuurid) kui ka korporatsioonid, nagu Google ja Apple, kuna andmed on muutunud uueks valuutaks.

Duke (2019) märgib, et seoses andmete salvestamise ja levitamise ning seiretehnoloogiate odavamaks ja hõlpsamini kättesaadavaks muutumisega on tavalised inimesed hakanud jälgimispraktikaid rakendama. Samuti sotsiaalmeedia jälgimises osalejad õpivad suurte organisatsioonide strateegiatest ja vastupidi (Lyon, 2018). Jälgimisega seoses saame rääkida sellistest mõistest nagu omnoptikon ja panoptikon. Omnoptikoni kirjeldab Rosen (2004) kui ühisvalvet, mis käib kaasa uue meedia ajastuga - toimub pidev üksteise jälgimine, samal ajal teadmata, kes ja millal keda jälgib. Vidili jt (2010) nimetavad omnoptikoni sotsiaalse järelevalve horisontaalseks vaateks – paljud jälgivad paljusid, mis on omane näiteks sotsiaalmeediale. Panoptikoni puhul mõistetakse tänapäeva ühiskonna raamistikus seda, kui vähesed jälgivad paljusid (McCullagh, 2005). Vidili jt (2010) nimetab seda järelevalve vertikaalseks vaateks, mis on omane ettevõtlusele, jõustruktuuridele jne.

Olenevalt kontekstist võib jälgimise tähendus varieeruda. Tänapäeva ühine nimetaja on siiski tehnoloogiliste vahendite kasutamine jälgimise või siis seire teostamiseks. Laiemas pildis formuleerib tänapäevas jälgimise kontseptsiooni siiski kõige paremini David Lyon enda raamatus „The Culture of Surveillance“. Lyon (2018) leiab, et Suure Venna idee – üksainus üksus, kes meid jälgib ja kontrollib, pole enam 21. sajandi jälgimiseks sobiv metafoor. Selle asemel väidab ta, et jälgimine pole asi, mida tehakse lihtsalt meile, vaid ka asi, milles me ise aktiivselt ja sageli entusiastlikult osaleme.

1.2 Nuhkvara (ing k *spyware*)

Arvutisüsteemide arenguga on käsikäes käinud samuti pahavara areng. Pahavara eesmärgiks on arvutisüsteemi kahjustamine omaniku teadmata ja/või nõusolekuta (Saad, Serageldin ja Salama, 2015). Mobiilsete seadmete puhul, nagu nutitelefonid, jagavad Saad jt (2015) pahavara kaheks suuremaks tüübiks. Üheks neist on troojalased ja viirused. Teise grupi moodustavad nuhkvara ja robotvõrk (ing k *botnet*). Saracino (2018) koos enda kolleegidega jagas pahavara kuueks erinevaks

klassiks: nuhkvara, SMS-trooja, installeerija, robotvõrk, juurkratt (ing k *rootkit*) ja lunavara. Selline klassifikatsioon saadi käitumusliku analüüsi tulemusena. Mina oma töös keskendun nuhkvarale ning teisi pahavara klasse ei analüüsi.

Andmekaitse ja infoturbe leksikon (2020) sõnastab pahavara (ing k *badware*) olemuse kui kasutaja seadmesse installeeritud soovimatut tarkvara, mis ei ole mõeldud kahjustamiseks. Näidetena tuuakse nuhkvara ja reklaamvara. Kuna pahavara võib häirida ja rikkuda privaatsust, siis tegemist on ikkagi ühe kahjurvara (ing k *malware*) liigiga. Nuhkvara määratletakse petuprogrammina või selle moodulina, mis kogub seadme omaniku või kasutaja tundlikke andmeid ja saadab need kolmandale poolele. Nendeks andmeteks võivad olla paroolid, krediitkaardinumbrid, omaniku poolt külastatavad veebilehed, kasutatavad programmid jne. (AKIT, 2020; Federal Trade Commission, 2005)

Nii Garrie (2007) kui ka Saracino (2018) koos oma kolleegidega toovad enda töös välja, et nuhkvara on tavaliselt kasutaja seadmesse installeeritud rakendus ja paigaldatud ilma kasutaja teadmata. Selle abil ei saa mitte ainult jälgida kasutajate tegevusi veebis, vaid samuti jälgida kõike mida kasutaja teeb enda seadmega ja seda infot edastada välisele üksusele ehk seadmele, mida kasutatakse jälgimiseks (GAO, 2016).

Mercaldo ja Saracino (2018) nuhkvara definitsioonis on olemas samad aspektid nagu eelnevatel uurijatel. Lisaks täpsustatakse, et mobiilseadmetelt kogutaks isiklikke andmeid ja need saadetakse välisele serverile kasutaja nõusolekuta. Isiklikeks andmeteks loetletakse IMEI[6] ja IMSI[7], telefoni kontakte, sõnumeid, sotsiaalse võrgustiku konto kasutaja andmeid ja asukoha määramist.

Eelnevaid määratlusi ja selgitusi nuhkvara kohta võtab väga lühidalt ning konkreetselt kokku ISO standard. ISO/IEC 27032 kohaselt on nuhkvara petutarkvara, mis kogub arvutikasutajailt privaatset või konfidentsiaalset teavet, sealhulgas tundlikku teavet (ISO, 2018).

Nuhkvara käsitletakse samuti, kui katuse terminit, mille alla kuuluvad erinevad tehnoloogiad, nii legaalsed kui ka illegaalsed (Garrie, Blakley ja Armstrong, 2007). Freed jt (2018) käsitluse kohaselt kuuluvad nn „legaalse nuhkvara“ klassifikatsiooni alla kahesuguse kasutusega rakendused. Sinna kuuluvad näiteks: vargusvastased jälgimisrakendused, vanemliku kontrolli rakendused ja hädaabirakendused.

[6] Rahvusvaheline mobiilseadme identifikaator (Ing k *International Mobile Equipment Identity*). https://akit.cyber.ee/term/3137-imei-number
[7] Rahvusvaheline mobiilabonendi identifikaator (Ing k *International Mobile Subscriber Identity*). https://akit.cyber.ee/term/2017-imsi-number

Selliseid rakendusi, mille esialgne funktsioon on legitiimne, kuid soovi korral saab kasutada nuhkvarana – nimetatakse kahesuguse kasutusega äppideks (Chatterjee jt, 2018; Freed jt, 2018). Chatterjee jt (2018) märgivad, et mõnede pealtnäha heatahtlikke äppe nagu näiteks „*Find My Friends*“ või teised perekonna jälgimise rakendused (nt *Life360, Verizon Smart Family*), saab ära kasutada inimeste varjatud jälgimiseks. Nende algne eesmärk on heasoovlik, kuid pahatahtliku eesmärgiga isik võib rakenduse võimalusi ära kasutades seadmele distantsilt ligi pääseda ning omandada informatsiooni seadmest teise kasutaja teadmata. Seega ei saa nuhkvara puhul rääkida ainult kui pahavaralistest tarkvarast või rakendusest.

Üldjuhul on nuhkvara teenuse tellijateks olnud riikide valitused ja korrakaitse organid (Harkin, Molnar ja Vowles, 2019). Enda raamatus „The Culture of Surveillance“ märgib Lyon (2018), et lisaks politseile ning luureagentuuridele tegelevad jälgimisega samuti korporatsioonid. Sellistest suurettevõtetest toob Schneier (2013) näidetena esile Facebook-i, Google-i ja Amazon-i. Tänapäeval on aga turg laienenud ning nuhkvara müüakse turvatootena, mis on tavaliselt suunatud ettevõtetele, lapsevanematele ja lähedastele partneritele (Harkin, Molnar ja Vowles, 2019).

Põhjused, miks keegi nuhkvara teenust tarbib, sõltuvad suuresti sihtrühmast. Dr. Katleen Gabriels (2016) loetleb mõningaid põhjuseid, miks keegi võiks nuhkvara kasutada. Ühe näitena toob Gabriels (2016) lahutatud vanemad, kus üks osapooltest luurab enda eks partneri järele veendumaks, kas teine täidab enda vanemlikke kohustusi. Motiivideks võivad niisamuti olla tööandjate soov jälgida enda töötajate tegevusi (Lyon, 2018; Weston, 2015), vanemate soov kontrollida enda laste käitumist ja elukaaslastel veenduda oma partneri truuduses (Gabriels, 2016; Harkin, Molnar ja Vowles, 2019). Ameerika Ühendriikide valitsuse vastutusameti (GAO, 2016) raport leiab enda uurimuses, et enamus jälgimisrakendustest on teadlikult turustatud inimestele, kes soovivad luurata enda elukaaslaste, laste või töötajate järele.

Kokkuvõttes võib öelda, et nuhkvara eesmärgiks on koguda kasutaja enda kui ka tema tegevuste kohta andmeid. Kogutud informatsioon saadetakse välisele üksusele, milleks võib olla mõni server või siis seadmele, mida kasutatakse jälgimiseks.

1.3 Jälgimist võimaldavate rakenduste võimekus

Krüptograaf Bruce Schneier on öelnud, et me elame jälgimise kuldajal (Tanriverdi, 2015). Internetis lühikese otsimise tulemusena võib avastada mitmeid erinevaid ettevõtteid, kes pakuvad nutiseadme või arvuti salajase jälgimise teenust. Jälgimist võimaldavaid rakendusi leiab nii veebis

otsingut tehes kui ka äpi poodidest. (Freed jt, 2018) Nimekiri erinevatest teenustest, mida nuhkvara pakub, on laia ampluaaga, võimaldades:

- jälgida telefoni kõnesid ja sõnumeid;
- ligipääsu suhtlusportaalides peetud vestlustele ja multimeediale;
- asukoha jälgimist;
- lugeda e-kirja vahetust;
- monitoorida kasutaja tegevusi veebis;
- salvestada telefoni kõnesid;
- lülitada sisse telefoni mikrofoni ja/või kaamerat;
- vaadata pilte, videosid ja kalendrisse tehtud märkmeid;
- kaugkontrolli jälgitava seadme üle;
- erinevate rapordite ja teadete saamist;
- kasutaja tuge jälgijale.
  (Garrie, Blakley ja Armstrong, 2007; Highster Mobile, 2019; Hoverwatch, 2019; mSpy, 2019; SpyFone, 2019; Spyera, 2019; SpyMyFone, 2019; Spyzie, 2019; XNSPY, 2019).

Liialduseta võib öelda, et firmade poolt pakutav nuhkvara võimaldab jälgida igat liigutust, mis nutiseadmega tehakse. Osad ettevõtjad võimaldavad rakendust kasutada tasuta prooviversioonina enne kui potentsiaalne klient teenuse sisse ostab (mSpy, 2019; SpyFone, 2019). Enamus teenusepakkujatest sellist võimalust ei võimalda ning toote tarbimise eest tuleb koheselt tasuda. Olenevalt firmast on välja töötatud teenuse paketid, mida saab tellida. Soovides suuremale andmehulgale ligi pääseda, tuleb endale soetada kõrgemast hinnaklassist teenuse pakett, mis seda võimaldab. Odavamad lahendused pakuvad piiratud teenuste hulka ja sellest tulenevalt puudub täielik ülevaade informatsiooni vahetusest, mis toimub sihtseadmes. Lisaks teenuste põhistele pakkumistele on turul olemas tooted lähtuvalt sihtseadmes kasutuses oleva tarkvarast. Eraldi eksisteerivad rakendused Androidi ja iOS operatsioonisüsteemil tegutsevatele seadmetele.

Enne nuhkrakenduse ostmist tuleb aga arvestada teatud eeltingimustega, mis peavad olema täidetud, et teenust saaks kasutada.

- Rakenduse installeerimiseks peab olema juurdepääs sihtseadmele.
- Veenduma, et rakendus ühilduks nutitelefoniga, mida tahetakse jälgida.
- Interneti ühendus (Wifi või mobiilandmeside).
  (Gillman, 2018)

Erinevad spioonirakendused kasutavad erinevat terminoloogiat, kuid nende tööpõhimõte on sarnane. Esmalt tuleb installeerida nuhkvara valitud telefoni, sisestada litsentsi võti ja lasta rakendusel teha enda tööd. Seejärel saab jälgida nuhkrakendusega nakatatud seadmega tehtavaid tegevusi kasutades siis arvutit või mõnda nutivahendit (vt Kuvatõmmis 1) (Gillman, 2019).

Kuvatõmmis 1 Nuhkrakenduse kasutusele võtmine (Allikas: Gillman, 2019)

Lähtuvalt operatsioonisüsteemide eripärast on rakenduste installeerimine erinev. Mõlema platvormi puhul on siiski esmatähtis ligipääs seadmele (nutitelefon, tahvelarvuti). Android tarkvara korral on vaja vaid nuhkvara paigaldada, mis ei nõua erilisi oskusi. Apple toodete puhul, mis kasutavad iOS operatsioonisüsteemi, on tarvis enne installeerimist teha lahtimurdmine (ing k *jailbreaking*). Lahtimurdmine lubab kasutada seadmes tarkvara, milleks Apple ei anna luba. Juurimist (ing k *rooting*) ehk volitamatult ülemkasutaja õiguste omandamist läheb vaja vaid juhul kui tahetakse kasutada rakenduse lisafunktsioone. (Eterovic-Soric jt, 2017) Loomulikult on võimalik soetada rakendus, mis ei nõua eraldi lahtimurdmist ja juurimist (Highster Mobile, 2019; Spyzie, 2019; XNSPY, 2019).

Pärast installeerimist jääb nuhkvara rakendus kasutaja eest varjatuks (Eterovic-Soric jt, 2017; Garrie, Blakley ja Armstrong, 2007). Nuhkvara töötab taustal ilma kasutaja teadmata. Nüüd on võimalik nutitelefoni tegevust eemalt jälgida, vajamata uuesti füüsilist juurdepääsu sihtseadmele. Kogu jälgitud andmestik kogutakse ja salvestatakse pilve ning sellele pääseb ligi veebipõhise portaali kaudu. (Gillman, 2019)

Jälgimist võimaldavate rakenduste teenuste nimistu on vägagi laiapõhjaline. Kasutamine on tarbijate jaoks tehtud võimalikult lihtsaks. Piisab vaid spioontarkvara alla laadimisest, soovitud seadmesse installeerimisest ja juba saabki nuhkrakendust kasutama hakata. Loomulikult tuleb enne toode teenuse pakkujalt osta, kuigi mõned ettevõtted pakuvad tasuta proovi varianti. Samuti tasub eelnevalt läbi mõelda võimalikud eeltingimused, mis võivad teenuse tarbimisel takistavaks teguriks saada. Näiteks kui telefonile puudu ligipääs, siis on keeruline spioonrakendust installeerida.

1.4 Privaatsus ja andmetele juurdepääs

Privaatsuse päritoluks peetakse Rooma õigusest tulenevat *actio iniuriarum*-it (ld. k), mille eesmärgiks oli kaitsta inimese füüsilist puutumatust ja kaitsta tema väärikust ja mainet (Periñán, 2012). Oxfordi ülikooli sõnastik määratleb privaatsust, kui seisundit, kus teised inimesed ei häiri või ei jälgi isikut (Lexico, 2019). David Solove (2002) laiendab teemat ning toob välja kuus privaatsuse eri aspekti:

1. õigus olla rahule jäetud;
2. piiratud ligipääs endale – võime kaitsta end teiste soovimatu juurdepääsu eest;
3. salastatus - teatud asjade varjamine teiste eest;
4. kontroll isikliku informatsiooni üle - võime kontrollida enda kohta käiva teabe üle;
5. isiksus - oma isiksuse, individuaalsuse ja väärikuse kaitse;
6. intiimsus - kontroll oma intiimsuhete või eluaspektide üle või eluaspekte.

Seoses tehnoloogia arenguga pakuvad Friedewald jt (2013) seitse privaatsuse tüüpi: isiku eraelu puutumatus (ing k *privacy of the person*), käitumise ja tegevuse privaatsus (ing k *privacy of behaviour and action*), isikliku suhtluse privaatsus (ing k *privacy of communication*), andmete ja pildi privaatsus (ing k *privacy of data and image*), mõtete ja tunnete privaatsus (ing k *privacy of thoughts and feelings*), asukoha ja ruumi privaatsus (ing k *privacy of location and space*) ning ühingu privaatsus (ing k *privacy of association*), sealhulgas grupi privaatsus (ing k *group privacy*).

Nagu näha, siis privaatsust võib tajuda, vaadelda mitmest erinevast küljest. Privaatsust võib jagada ka konstitutsionaalseks- ja informatsiooniliseks privaatsuseks. Esimese all peetakse silmas vabadust võtta otsuseid vastu ilma teiste vahele segamiseta teemades, mida loetakse intiimseks ja personaalseks. Teise puhul saame rääkida indiviidi kontrollist oma teabele juurdepääsu üle (van den Hoven jt, 2018). See hõlmab endas isiku kohta kogutud, salvestatud ja jagatud andmeid (Murumaa-Mengel, Pruulmann-Vengerfeld ja Laas-Mikko, 2014).

Kontrolli idee näib olevat kõikehõlmav, kuid tänapäeva kontekstis rõhutatakse isiku õigust otsustada andmetele juurdepääsu ulatust, kellele anda ligipääs teda puudutavale informatsioonile ja nende andmete kasutamiseks (Moore, 2008; Rössler, 2005). Murumaa-Mengel jt (2014) lisavad, et samuti sisaldab see kontrolli informatsiooni kasutamise õiguste üle.

Enda privaatsuse ja andmete juurdepääsu kaitsmiseks on vastuvõetud mitmed õigusaktid ja Eesti õigussüsteemi lahutamatuks osaks on rahvusvahelise õiguse[8] üldtunnustatud põhimõtted. 2018. aasta 25. mail jõustus Euroopa Parlamendi ja Nõukogu määrus füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus ehk IKÜM) (Euroopa Parlament; Euroopa Liidu Nõukogu, 2016). Määrus annab seadusliku aluse olla unustatud. See tähendab seda, et võib nõuda andmete kustutamist, kui töötlemiseks pole õigustust või andmed ei ole enam asjakohased. Selle nõude peale tuleb andmed kustutada. Inimesel peab olema võimalik enda isikuandmetele ligi pääseda ja neid endaga kaasa võtta. Samuti võib vabalt oma andmeid eri andmetöötlejate vahel liigutada. Juhul kui isiku andmeid töödeldakse, siis tuleb talle töötleja poolt selgitada, kuidas, milliseid andmeid ja millistel eesmärkidel kasutatakse. Sama regulatsiooni (2016) kohaselt, nagu isikul on õigus nõuda andmete töötlemist, on ka määruse kohaselt töötlejal õigus keelduda nende töötlemisest.

Eesti Vabariigi põhiseaduse (1992) § 26 sätestab, et igaühel on õigus perekonna- ja eraelu puutumatusele. Paragrahvis sõnastatakse selgelt, et riigiasutused, kohalikud omavalitsused ja nende ametiisikud ei tohi kellegi perekonna- ega eraellu sekkuda. Eranditena on välja toodud: „…seaduses sätestatud juhtudel ja korras tervise, kõlbluse, avaliku korra või teiste inimeste õiguste ja vabaduste kaitseks, kuriteo tõkestamiseks või kurjategija tabamiseks.“.

Kokkuvõtvalt võib nentida, et privaatsust saab ja annabki erinevalt tõlgendada. Sarnasele järeldusele on jõudnud samuti Regan (2000), et inimesed võivad tunnetada privaatsust erinevalt. Palju loeb kontekst ning ajaline raamistik, sest ühiskonna arenguga on muutuses samuti arusaam privaatsusest. Selleks, et inimestel oleks õigus enda privaatsusele ja võimalus seda vajadusel kaitsta, on vastu võetud erinevaid seadusandlikke regulatsioone. Eesti Vabariigi kodaniku jaoks on kindlasti enda privaatsuse kaitsmisel oluline tugisammas põhiseaduse § 26. Laiemas Euroopa kontekstis on samuti vägagi määrava tähtsusega IKÜM.

1.5 Jälgimist reguleeriv seadusandlus Eesti Vabariigis

Inimeste jälgimine nende enda teadmata ja nõusolekuta tõstatab esile probleeme nii seadusandlikus võtmes kui ka eetilises aspektis. Eesti Vabariigi põhiseadus (1992) § 43 sätestab: „Igaühel on õigus tema poolt või temale posti, telegraafi, telefoni või muul üldkasutataval teel

[8] PS § 3 Riigivõimu teostatakse üksnes põhiseaduse ja sellega kooskõlas olevate seaduste alusel. Rahvusvahelise õiguse üldtunnustatud põhimõtted ja normid on Eesti õigussüsteemi lahutamatu osa.

edastatavate sõnumite saladusele. Erandeid võib kohtu loal teha kuriteo tõkestamiseks või kriminaalmenetluses tõe väljaselgitamiseks seadusega sätestatud juhtudel ja korras.“.

Põhiseaduse § 43 kaitseb isikute sõnumisaladust, kuid samas on loetletud erandid, mille puhul on lubatud sõnumisaladust rikkuda. Enda artiklis selgitab Anu Baum (2016), et erandite all ei ole mõeldud teada saamiseks kellega teine pool suhtleb ja millest nad omavahel räägivad. Erandiks ei loeta isegi Põhiseaduse mõttes vanemliku kontrolli teostamise vajadust kui õigustust sõnumisaladuse rikkumiseks (Baum, 2016). Samas põhiseaduse kommetaaris (Laos ja Sepp, 2017) tuuakse välja Riigikohtu kriminaalkolleegiumi otsus[9], et kaitsealasse ei kuulu saadetud ja andmekandjale salvestatud sõnumid, mis on saatja või saaja valduses.

Julgeolekuasutuste seaduse (2019) § 21^1, mille mõju laieneb Kaitsepolitseiametile (KAPO) ja Välisluureametile (VLA), on täpsustatud, et teabe kogumisel ja töötlemisel võib julgeolekuasutus piirata andmesubjekti õigusi. Varjatud teabe kogumise meetodid ja vahendid kehtestab aga asjaomane minister oma määrusega (JAS, 2019). Samuti omab varjatud jälgimise õigust politsei. Kriminaalmenetluse seadustik (2019) § 126^7 reguleerib politsei salajast pealtkuulamist või –vaatamist. Oluliseks aspektiks on nõue, et jälitustegevuseks peab olema eeluurimiskohtuniku luba, mis antakse kaheks kuuks ning seda võib kohtunik pikendada kahe kuu kaupa. Erandiks on siin puhul KAPO ja VLA. Seadusest tulenevalt on asutuste ülesanne iseseisvalt teabehanke käigus hangitud info alusel ennetada julgeolekuohte. Sellisel korral ei loeta seadusest tulenevat volitusnormi jälitustegevuseks, vaid teabehankeks ning kohtuniku käest luba ei küsita. (Heldna, 2016)

Kriminaalmenetluse seadustikus (2019) kui ka julgeolekuasutuste seaduses (2019) on kirjas paragrahv, millega on asutustele pandud kohustus teavitada pärast varjatud jälgimise lõppemist isikut, kelle suhtes jälgimist teostati. Teavitus peab endas hõlmama salajase jälgimise asjaolusid, aega ja liiki. Seda ei pea aga tegema, kui see ohustab eesmärki, mille tõttu alustati tegevust (JAS, 2019) või kui see:

- kahjustab oluliselt kriminaalmenetlust;
- kahjustab oluliselt teise isiku seadusega tagatud õigusi ja vabadusi või seab teise isiku ohtu;
- seab ohtu jälitusasutuse meetodite, taktika, jälitustoimingu tegemisel kasutatava vahendi või politseiagendi, variisiku või salajasele koostööle kaasatud isiku koostöö salajasuse (KrMS, 2019).

[9] RKKKo 30.06.2014, 3-1-1-14-14, p-d 816 ja 817

Eraviisiline jälitustegevus liigitub karistusõiguse (Sootak, 2016) kohaselt vabadusvastaseks süüteoks[10] (Riigi Teataja, 2015). Karistusseadustiku § 137 sätestab kriminaalkorras karistava teona eraviisilise jälitustegevuse isiku poolt, kellel puudub selleks seaduslik õigus, eesmärgiga koguda teise isiku kohta andmeid. Juhul kui ebaseaduslikku salajast jälitustegevust viis läbi isik, kes seadusest tulenevalt omab õigust jälitustegevuseks, siis seda reguleerib § 315 – ebaseaduslik jälitustegevus ja teabe varjatud kogumine (KarS, 2019).

Inimeste jälgimist selgitab Baum (2016) kui: „korduvat või pikemaajalist varjatud visuaalset vaatlemist kas vahetult või tehniliste vahendite abil, sõnumite salajast pealtkuulamist või läbivaatamist, sõltumata sõnumite edastamise, läbivaatamise või pealtkuulamise viisist ning asjade või inimeste kohta andmeid sisaldavate andmekogude salajast läbivaatamist“.

Oluline aspekt karistusseadustiku § 137 puhul on eesmärk koguda andmeid. Kui jälgimisrakendust kasutada vaid kolmanda isiku sõnumite lugemiseks ning neid ei salvestata ega koguta, siis pole tegemist eraviisilise jälitustegevusega (Baum, 2016). Siin kohal aga ei tohi unustada, et sõnumisaladus on eraldi kaitstud ning selle rikkumine on karistusseadustiku (2019) § 156 kriminaalkorras karistatav.

Sõnumisaladuse rikkumise korral on ette nähtud sanktsioonina rahaline karistus. Juhul kui sõnumile pääseti ligi oma ametiseisundit kuritarvitades, siis see on raskendav asjaolu ning karistatakse rahalise karistusega või kuni üheaastase vangistusega. Eraviisiline jälitustegevus on raskem süütegu ja maksimaalne karistusmäär on kuni kolmeaastane vangistus (KarS, 2019).

Veel ühe aspektina tuleb kindlasti nuhkvara kasutamisel võtta arvesse, et rakendus on vaja jälgitava isiku seadmesse installeerida, mis samuti on karistatav. See on hõlmatud karistusseadustiku § 217, mille kohaselt arvutisüsteemile ebaseadusliku juurdepääsu hankimise eest kaitsevahendi kõrvaldamise või vältimise teel võib teo toimepanijat oodata rahaline karistus või kuni kolmeaastane vangistus (KarS, 2019). Arvutisüsteemide all mõistetakse kriminaalõiguses seadet või seadmete gruppi, millest vähemalt üks täidab automaatse andmetöötluse funktsiooni, mis tähendab seda, et sinna alla kuuluvad nii nutitelefonid kui ka tahvelarvutid (Baum, 2016; Kukrus, 2004).

Seadusandlikust poolest on varjatud jälgimise õigus antud vaid jõustruktuuridele ning nendelgi peab olema vastavasisuline luba kohtu poolt, erandiks vaid KAPO ja VLA teatud tingimustel.

[10] RKKKo 3-1-1-93-15, 3-1-1-5-09, 3-1-1-158-05 ja 3-1-1-124-04.

Seega kasutaja salajaseks jälgimiseks mõeldud rakenduse rakendamine on Eestis eraviisiliseks jälitustegevuseks ebaseaduslik ning kriminaalkorras karistatav.

2 VALIM JA MEETOD

Käesolev peatükk on jagatud kaheks osaks. Esimeses osas kirjeldan valimi moodustumist ning teises osas annan ülevaate kasutatud meetodist.

Lõputöö eesmärk on kaardistada ning analüüsida sõnumeid, mille kaudu konkreetseid teenuseid turustatakse ja lähtudes püstitatud eesmärgist, otsin vastuseid järgmistele uurimisküsimustele:

1. Millistele sihtrühmadele on suunatud telefonikasutaja salajaseks jälgimiseks mõeldud rakendused?
2. Milliseid sõnumeid kasutatakse, et rakendust sihtrühmadele turustada?

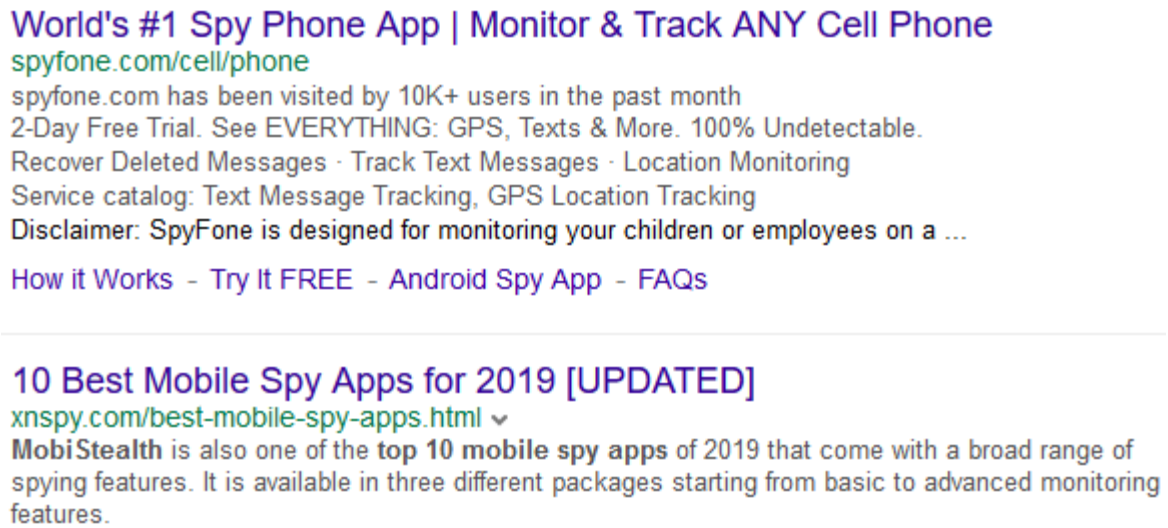
2.1 Valim

Uuringu jaoks valisin välja neli erinevat teenust, mis turustavad nuhkvara rakendust. Selle valimi moodustamiseks viisin läbi turuanalüüsi, selgitamaks välja millised nuhkvara rakendused on kõige enam otsitavad ja kasutatavad. Selle tarbeks kasutasin veebiotsingutes terminit „nuhkvara“ ning tuvastasin nuhkvara müüjad, kelle esinemissagedus otsingumootorites on kõrge. Eeldasin, et kõige edukamad nuhkvara müüjad on turul need, kes saavad otsingumootori täiustatud optimeerimisest (SEO)[11] kõige rohkem kasu. Analüüsi jaoks kasutasin kolme erinevat otsingumootorit: Google, Bing ja Yahoo. Kõigis kolmes erinevas otsingu keskkonnas kasutasin täpselt samu inglise keelseid otsisõnu: „*spyware*“, „*spyware apps*“, „*tracking apps*“, „*phone surveillance apps*“ ja „*top spyware apps*“.

Kasutades otsingusõna „*top spyware apps*“, andis otsingumootor vastetena mitmeid erinevaid veebilehti, kuhu on koondatud erinevad nuhkvara loendid (vt Kuvatõmmis 2). Nende nimekirjade eesmärgiks on võrrelda erinevaid rakendusi ning anda võimalikele huvilistele ülevaade nuhkvara võimalustest ja piirangutest (vt Kuvatõmmis 3). Taolisi ülevaateid saab näha näiteks lehtedelt: www.bestphonespy.com, www.bestcellphonespyapps.com ja www.thetruthspy.com. Lisaks võib

[11] Kodulehe otsingumootoritele optimeerimine (ing k *search engine optimization* ehk SEO) on moodus kodulehe leitavuse, külastatavuse ja usalduse suurendamiseks otsingumootorites (Veebikoda, 2017).

nende loendite eesmärgiks olla potentsiaalsete kasutajate meelitamine konkreetsete teenusepakkujate poole. Mõningate loendite puhul on tegemist nuhkvara tootva ettevõtte enda reklaamistrateegiaga (vt Kuvatõmmis 3) (Harkin, Molnar ja Vowles, 2019; XNSPY, 2019).



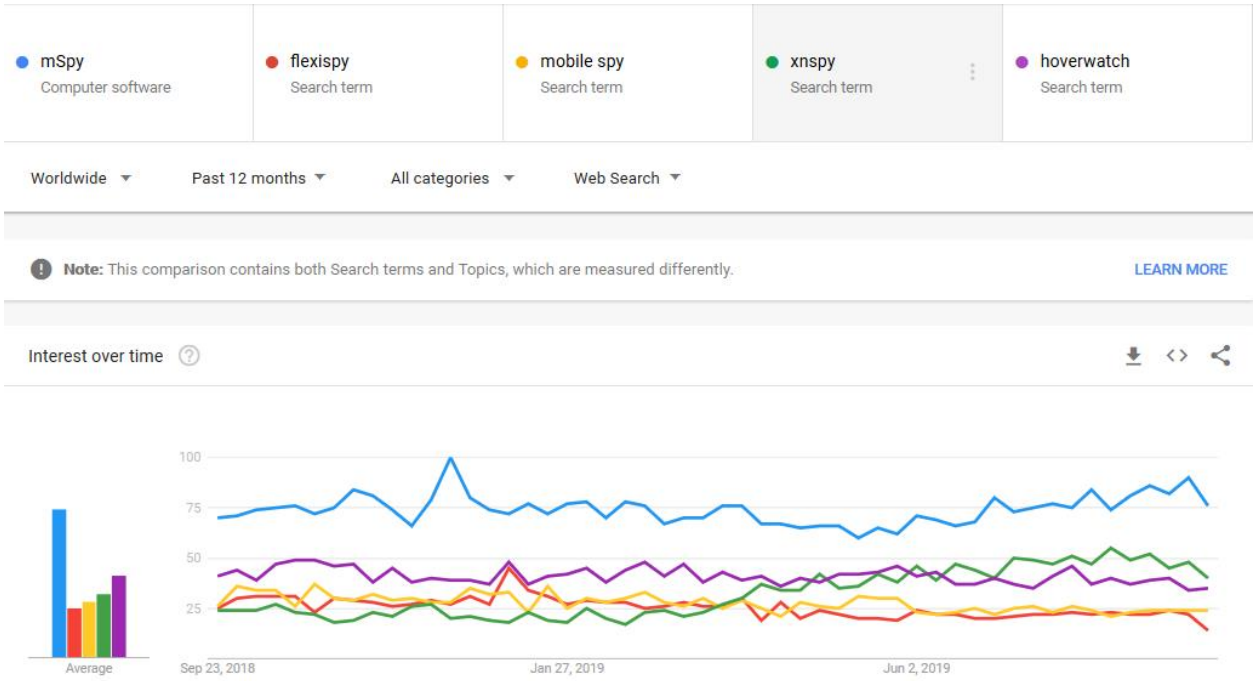
Kuvatõmmis 2 Erinevad soovitus nimekirjad parimatest nuhkvara rakendustest. Yahoo otsingumootoris teostatud otsing „*top spyware apps*“ 15.09.2019.

	1	2	3	4	5	6	7	8	9	10
Apps	XNSPY	Trackmyfone	Spyzie	Mobistealth	ispyoo	Stealth-Genie	mSpy	MobileSpy Agent	AppMia	Highster Mobile
Rating	9.8	9	8	7.8	7.5	7.3	7	6.9	6.7	6
Features										
Android OS Support	4.0 to 8.0	4.0 to 8.0	4.0 to 8.0	7.0 to 9.1	6.0 to 11.0	4 and above	7.0 to 11.0	4.0 to 7.1.2	1.0 and above	N/A
iOS Support	6.0 to 11.2.5	6.0 to 11.2.5	6.0 to 11	N/A	N/A	7 and above	Does not support iOS	2.0 to 6.0	9.0.x and above	6.0 to 11
Call Recording	✓	✗	✗	✗	✓	✗	✗	✗	✓	✗
Surround Recording	✓	✗	✗	✓	✓	✗	✗	✗	✓	✗
Geofencing	✓	✗	✓	✗	✗	✓	✓	✗	✗	✗
Remote Control	✓	✓	✗	✗	✗	✓	✓	✗	✓	✓
Watchlist alert	✓	✓	✗	✗	✗	✗	✓	✗	✗	✗
Internet Browsing	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Kuvatõmmis 3 Nuhkvara rakenduste võrdlus tabel XNSPY kodulehel (Allikas: XNSPY, 2019).

Kasutades otsingumootorite tulemusi ja võttes arvesse enam esinenud nuhkrakendused, mida võis leida soovituslikest nimekirjadest, koostasin esialgse nimekirja saadaolevatest nuhkvara rakendustest. Lähtuvalt esinemise sagedusest erinevate otsingusõnade lõikes kui ka kogu teostatud otsingute koondina valisin välja kümme kõige sagedamini esinenud nuhkvara rakendust.

Seejärel kasutasin Google tööriista „*Google trends*“, mis võimaldab kasutajatel teha võrdlevaid päringuid teemade ja nende otsimise sageduse kohta. Algsest nimekirjast väljavalitud kümnest rakendusest valisin omakorda välja viis kõige sagedamini otsitud salajase jälgimise rakendust (vt Kuvatõmmis 4).



Kuvatõmmis 4 Nuhkvara rakenduse otsingusagedused ajavahemikus 23.09.2018 - 21.09.2019. (Allikas: Google Trends, 2019)

Viiest kõige enam otsitud salajase jälgimise rakendustest arvasin omakorda välja rakenduse FlexiSpy. Seda põhjusel, et viirusetõrje programm andis hoiatuse rakenduse kodulehe kohta, kui potentsiaalse pahavara rünnaku lähtekohana. Seetõttu kasutan enda lõputöö uurimuses nelja salajase jälgimise rakendust, milleks on:

1. mSpy
2. Mobile spy
3. XNSPY
4. Hoverwatch

2.2 Uurimismeetod

Lõputöös olen kasutanud andmete analüüsimiseks läbikäimismeetodit (ing k *walkthrough method*). Esimese etapina tutvusin kõigi nelja teenusepakkuja kodulehtedega süvitsi. Kuna läbikäimismeetod uurib kontseptsioone, mida rakendus edastab tegevuste kohta, mida see peaks pakkuma, toetama või võimaldama (Light, 2014; Light ja McGrath, 2010; Light, Fletcher ja Adam, 2008; Papacharissi, 2009), siis lähtuvalt lõputöö eesmärgist ning püstitatud uurimisküsimustest keskendusingi sihtrühmade ja nendele suunatud sõnumite leidmisele teenusepakkujate veebilehtedelt.

Leitud sõnumite süstematiseerimiseks ja sihtrühmade põhiseks kategoriseerimiseks kasutasin MS Excel keskkonda. Peale esialgset kategooriatesse jagamist kordasin korrastamise protsessi. Selle tulemusena suutsin andmed jagada sihtrühmade alla erinevatesse sõnumi rühmadesse.

Järgnevalt alustasin sõnumite analüüsimist ehk detailsema ülevaate saamiseks teenuse pakkujate sõnumite osas, kasutasin võrdlevat analüüsi. Light jt (2018) kirjeldavad seda meetodi mõistes kui rakenduse visiooni, toimimismudeli ja juhtimise uurimist, mis võimaldab mõista, kuidas rakenduse kujundajad, arendajad, välja andjad ja omanikud loodavad, et kasutajad saavad selle rakenduse ja integreerivad selle enda tehnoloogia kasutamise tavadesse. Light jt (2018) märgivad, et läbikäimismeetodi puudusi saab lahendada erinevate meetodite ja andmeallikate kombineerimise teel. Antud juhul puudus vajadus kombineerida erinevaid meetodeid, sest selliste lahenduste uurimine nõuab uusi meetodeid ning see sobis seda tüüpi tekstide analüüsiks kõige paremini.

3 TULEMUSED JA JÄRELDUSED

Selles peatükis annan ülevaate uurimistulemustest ja nende järeldustest. Tulemused ja järeldused on jagatud kaheks peatükiks, milles teine peatükk on omakorda jagatud kaheks alampeatükiks. Esimene peatükk annab ülevaate sihtrühmadest, kellele on sõnumid suunatud. Teine peatükk koos alampeatükkidega keskendub sõnumitele, mis on sihtrühmadele suunatud.

3.1 Nuhkrakenduste sihtrühmad

Lõputöös uurisin nelja erinevat nuhkrakendust, mis on vabalt kätte saadavad kõigile internetis. Analüüsi keskmeks võtsin rakenduste kodulehed, et tuvastada millistele sihtrühmadele on suunatud telefonide salajaseks jälgimiseks mõeldud rakendus. Analüüsi tulemusena ilmnes kaks sihtrühma, kelle jälgimiseks soovitatakse salajase jälgimise rakendust kasutada (vt Tabel 2).

Tabel 2 Sihtrühmad, kelle luuramiseks on rakendus mõeldud.

	Selgesõnaline soovitus kasutada tarkvara **laste** jälgimiseks?	Selgesõnaline soovitus kasutada tarkvara **töötajate** jälgimiseks?
mSpy	Jah	Jah
Hoverwatch	Jah	Jah
XNSPY	Jah	Jah
Mobile Spy	Jah	Jah

(Autori poolt koostatud seisuga 03.03.2020)

Paralleelselt nende sihtrühmadega, keda soovitatakse jälgida, joonistus välja kaks peamist sihtrühma, kelle turundus oli suunatud – lapsevanemad ja tööandjad. Toetudes varasematele uuringutele võis eeldada, et spioonrakendust soovitatakse kasutada elukaaslastel enda partnerite jälgimiseks (Chatterjee jt, 2018; Freed jt, 2018; Harkin, Molnar ja Vowles, 2019), kuid käesoleva uuringu tulemused seda väidet ei toeta. Ainukesena tõi selle võimaluse esile XNSPY teenusepakkuja ametliku blogi postituses (Kido, 2017) (vt Kuvatõmmis 5).

Kuvatõmmis 5 Blogipostitus XNSPY kodulehelt. 13.03.2020 (Allikas: Kido, 2017)

XNSPY blogipostitus on tehtud 24.09.2017. Ühtegi hiljem lisatud viidet elukaaslase või partneri järele luuramiseks ei olnud võimalik tuvastada. Samas Harkin jt (2019) töös on olemas 2018. aasta veebruaris tehtud kuvatõmme mSpy kodulehelt, kus selgelt viidatakse abikaasadele, kui ühele sihtgrupile keda võiks jälgida. Sellest saab järeldada, et rakendusi turundavad ettevõtted on teinud millalgi 2018 – 2019 aastal olulise muudatuse selles osas, kellele loodud teenust turundada. Võib oletada, et tegemist on mõne seadusandlikust muudatusest tuleneva fookuse muudatusega, kuna rakenduste pakutavate teenuste hulk võimaldab totaalset andmete kontrolli. Seega pole välistatud, et laste ja töötajate jälgimine on seaduse poole peal veel piisavalt hall ala, kus saab toimetada, kuid partnerite/elukaaslaste oma on nüüdseks paremini reguleeritud. Sellest lähtuvalt on teenusepakkujad end järelikult distantseerinud sõnumitest, mis viitavad võimalusele nuhkida enda abikaasa või partneri järele, kuna see võib kaasa tuua võimalikke probleeme. Võimatu pole samuti seos 2018. aastal jõustunud IKÜM-ga (Euroopa Parlament; Euroopa Liidu Nõukogu, 2016), mis viis teenusepakkujad sellise muutuseni.

Töötajate ja laste järele soovitavad luurata eranditult kõik teenusepakkujad. Olenevalt ettevõttest on suunatud sõnumite põhiline rõhk orienteeritud pigem ühe kindla sihtrühma jälgimisele. mSpy

on rakenduse reklaamimisel kuvanud eelkõige kui vanemliku kontrolli rakendus (ing k *parental control app*) (vt Kuvatõmmis 6). Hoverwatchi ja Mobile Spy (vt Kuvatõmmis 7) puhul on fookus jaotunud aga pigem võrdselt mõlema sihtrühma vahel ehk puudub selge eelistus lapsevanemate ja tööandjate vahel. XNSPY kodulehe sisu keskendub pigem aga lastevanematele kui olulisele võimalikule teenuse kasutajale.

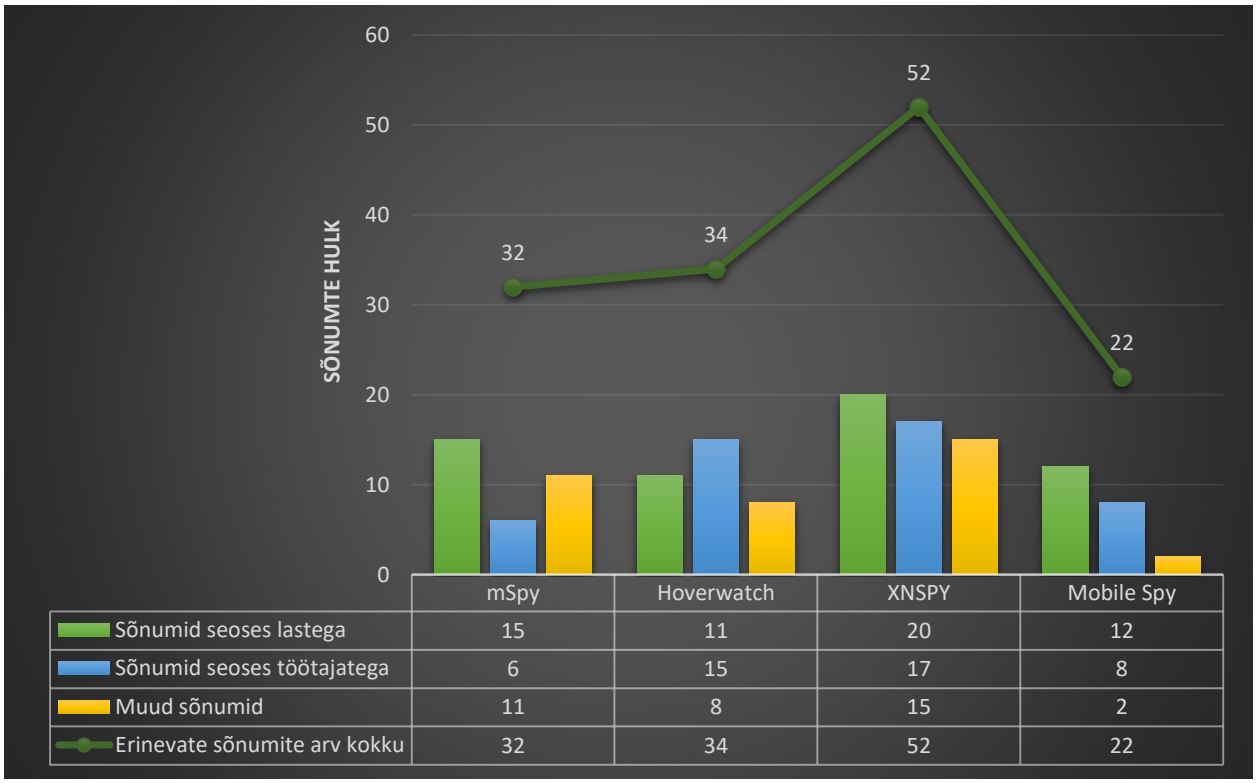
Kuvatõmmis 6 mSpy turundus sõnum nende kodulehe esiküljel. 12.03.2020

Kuvatõmmis 7 Mobile Spy turundus sõnum nende kodulehe esiküljelt. 13.03.2020

Kui lastega seoses on kõik rakendused enda sõnumid suunanud lastevanematele, siis XNSPY on seda ringi veelgi laiendanud. Nimelt on nende üheks sihtrühmaks haridusasutused/koolid, kellele soovitatakse võtta nende rakendus kasutusse, et jälgida koolis õppivaid lapsi. Selle all mõeldakse siiski kooli enda nutivahendeid, kuhu vastav tarkvara soovitatakse koolidel installeerida.

3.2 Peamised teenuse turundamiseks kasutatavad sõnumid

Sõnumid, millega sihtrühma poole pöördutakse, et enda toodet müüa, varieeruvad. Põhiliseks läbivaks teemaks on turvalisus pakkumine erinevates aspektides. Olenevalt sellest kas lähenetakse lapsevanemale või tööandjale, sõltub ka rõhuasetus. Eelkõige tuginetakse sõnumite puhul teenuse positiivsete külgedele ja sellele, et kasusaajateks ei ole mitte ainult rakenduse kasutajad vaid samuti need keda hakatakse jälgima. Oluline osa on sõnumitel, mis toonitavad psühholoogilisi vajadusi nagu kontrolli omamine ning turvatunne.



	mSpy	Hoverwatch	XNSPY	Mobile Spy
Sõnumid seoses lastega	15	11	20	12
Sõnumid seoses töötajatega	6	15	17	8
Muud sõnumid	11	8	15	2
Erinevate sõnumite arv kokku	32	34	52	22

Joonis 1 Sihtrühmadele suunatud sõnumite hulk. (Autori poolt koostatud seisuga 13.03.2020)

Koondarve võrreldes (vt Joonis 1) ilmneb XNSPY märgatav ülekaal erinevate suunatud sõnumite hulgas, mis ületab Mobile Spy omi kahekordselt. mSpy ja Hoverwatchi-ga võrreldes on ülekaal poolteisekordne. See annab hea ülevaate selle kohta kui hästi on ettevõte läbi mõelnud enda poolse kommunikatsiooni. Kui palju on panustatud selle jaoks, et tekitada erinevate sihtrühmade tarbeks võimalikult suur erinevate sõnumitega kandepind, et seeläbi võita endale kliente. Samuti ilmneb see sõnumite kirjapildis, kus mängitakse sõnastusega. Paralleelselt leiavad kasutust terminid jälgima (ing k *monitor*)(vt Kuvatõmmis 6 ja Kuvatõmmis 7) ja luurama (ing k *spy*).

> *Kui olete kunagi mõelnud, kuidas luurata tekstisõnumeid, kui vaatate oma lapsi või töötajaid, kes pidevalt midagi telefonis kirjutavad, kuid te ei teadnud, mida teha, siis nüüd on teil lahendus.*[12] (Hoverwatch, 2020)
>
> *Kui jälgite oma lapse või töötajate mobiiltelefone, on väga oluline uurida ka nende kalendrikirjeid, sest see võib aidata teil valmistuda järgmisteks toiminguteks.* (XNSPY, 2020)

Esimeses näites kasutatakse terminit luurama (ing k …*how to spy on text messages*…), samas teise näite puhul jälgima (ing k *…are monitoring your…*). Sellised näited on ühiseks tunnusjooneks kõigi nelja rakenduse puhul. Siin juures on oluline tähele panna, et taoline ristkasutus toimub vaid sõnumite puhul. Otseselt keegi ennast spioonrakendusena ei reklaami, kuigi osade teenusepakettide puhul öeldakse, et tegemist on luuramiseks mõeldud tarkvaraga (ing k *spy software*). Sellest hoolimata saame rääkida teadlikust soovitusest luurata nii töötajate kui ka laste järele. Üheks põhjuseks miks terminitega nn „mängitakse“ võib olla soov end teha nähtavaks. Nähtavaks just erinevatele otsingumootoritele, et võimalike päringute korral just nende koduleht ilmneks otsingutulemustes ja seda maksimaalselt kõrgel positsioonil.

Sõnumite teiseks läbivaks jooneks on see, et nad jäävad enamasti väga üldiseks. XNSPY toob oma sõnumis näitena, et näed töötaja kalendrit. Kuid ei täpsusta, milleks see on tööandja jaoks vajalik? Viidatakse võimalusele, kuid samas ei osutata, mis on selle otsene kasu. Taoline mall on pidev kõikide sihtrühmade ja sõnumite korral. Tuuakse esile võimalus, kuid puudub selgitus või mõni muu viide, miks see on oluline või vajalik.

3.2.1 Sõnumid lastevanematele

On täiesti loomulik, et lapsevanem tahab kaitsta enda last kõigi ohtude eest, mis maailmas varitsevad. Üheks ohuallikaks on kindlasti arengud ning sündmused (nt seksuaalkurjategijad, küberkuritegevus), mis leiavad aset kübermaailmas ja jõuavad lapseni läbi nutiseadme. Selle tõdemuseni on samuti jõudnud ettevõtted, kes pakuvad lapsevanematele võimalust ning vahendit, kuidas enda järeltulijat viidatud ohtude eest kaitsta. Lapse kaitsmine erinevate ohtude eest ongi suur ühine nimetaja, millest saab lapsevanematele suunatud sõnumite puhul rääkida. Loetletakse erinevaid ohuallikaid ning seeläbi sisendatakse, et lapse järgi luuramine on igati õigustatud tegevus. Mõnede suunatud sõnumite puhul toovad teenusepakkujad välja konkreetsed

[12] Autori tõlge inglise keelest eesti keelde. Järgnevalt kogu töö ulatuses on kaldkirjas ja taandega esitatud lõputöö autori tõlge.

sõnumirakenduste nimed ehk juba antakse kasutajale viide, et nende spioonrakenduse funktsioone on võimalik kasutada suhtlusplatvormi mingisuguste teenuste puhul.

> *Kik-i sugused sõnumirakendused ohustavad alaealiseid lapsi, kuna seal võivad nad kokku puutuda* ***küberkiusamisega****,* ***veebikiskjatega****,* ***petturitega*** *jne. Kasutades mSpy Kik Messengeri jälgijat, saate oma lapse tekste jälgida ja alati aimugi saada. mis su laps seal teeb. Välista võimalus, et sinu laps suhtleks veebikiskjatega, küberkiusajatega ja muude vägivallatsejatega, kes võivad teie lapsele kahju teha, tagades juurdepääsu oma laste Kik-sõnumitele.* (mSpy, 2020)

Lastevanematele suunatud sõnumite puhul joonistus välja neli suuremat rühma: kuritegevus, lapse kasvatamine, suhted ja kontroll (vt Tabel 3). Tulemuste grupeerimisel võtsin arvesse kriteeriumit, et sõnumit projekteeriti lapsevanematele kui ühte kindlat põhjust, miks peaks kasutama nutiseadme salajase jälgimise rakendust.

Tabel 3 Sõnumid, põhjendused miks peaks lapsevanem kasutama salajase jälgimise rakendus lapse nutiseadmes.

		mSpy	Hoverwatch	XNSPY	Mobile Spy
Kuritegevus	Netipervod	x		x	x
	Netikiusamine	x	x	x	x
	Seaduse rikkumise tõkestamine	x		x	x
	Identiteedi vargus	x		x	
	Küberkurjategijad	x			
	Sekstimine (ing k *Sexting*)	x		x	x
Lapse kasvatamine	Lapse psühholoogilise tervise kaitsmine			x	x
	Halb lapse arengule	x	x	x	
	Küberhügieeni juurutamine			x	
	Parema digitaalse keskkonna loomine			x	
Suhted	Heade suhete hoidmine lastega		x	x	
	Sotsiaalne isolatsioon	x			
Kontroll	Kaitsta last veebi sisu eest	x	x	x	x
	Turvatunne (asukoha teadmine)	x	x	x	
	Vastutustundlik vanemlik kontroll	x	x	x	
	Lapsed ei taju veebiohte, sina tajud	x	x	x	x
	Meelerahu	x	x	x	x
	Teadmisvajadus/ info nälg/ õigus teada	x	x	x	x
	Sensitiivse info lekke tõkestamine		x	x	
	Kontroll seadmete üle - mõjutusvahend			x	x
	Aja raiskamine	x	x	x	x
	Liiklusohutuse tagamine			x	x

(Autori poolt koostatud seisuga 14.03.2020)

Täiesti tavaline praktika näitab erinevate sõnumite ristkasutamist, et põhjendada, õigustada või näitlikustada edastatavat sõnumit. Fundamentaalne aluspind kõikide eraldiseisvate sõnumite puhul on kaitsmine ja võimalike ohtude ennetamine. Olgu selleks kas nähtavate või nähtamatute ohtude eest. Ainus sõnum, mis seda ühist kaitsmise platvormi teistega ei jaga on kontrolli rühma kuuluv

sõnum – „Kontroll seadmete üle – mõjutusvahend“. Järgnevalt toon Tabelis 3 viidatud kategooriate kaupa välja peamised sõnumid, mida teenusepakkujad kasutavad.

3.2.1.1 Kuritegevus

Kuritegevuse kategooria alla klassifitseerisin alamsõnumid nagu: netipervod, netikiusamine, seaduse rikkumise tõkestamine, identiteedi vargus, küberkurjategijad ja sekstimine (ing k *sexting*). Sõnumite analüüsis ilmnes, et kuritegevuse sõnumit peavad oluliseks teemaks kõik rakendused, välja arvatud Hoverwatch. Hoverwatch mainib ainsa asjana netikiusamist ja võimalust seda tõkestada. Küberkiusamise puhul märgivad teenusepakkujad, et lapsed ei ole altid enda vanemaid sellest probleemist teavitama. XNSPY väidab, et vaid 10% lastest räägivad enda vanematele, et nad on langenud netikiusamise ohvriks ning sellest vaid 1/5 teeb avalduse politseisse. mSpy, XNSPY ja Mobile Spy toovad veel juurde eraldi netipervode ohu ning võimaluse tõkestada lapsel seaduse rikkumisi. Netipervode all peetakse silmas veebi keskkonnas tegutsevaid pedofiile, ahistajaid (Freienthal, 2018). Seaduse rikkumise tõkestamise puhul toob mSpy näite, et kui sinu lapse telefonis on olemas video, millel on selgelt kujutatud alaealise seksuaalseid tegusid või alastust, siis võib sellise video omamise eest mobiilseadmes saada kriminaalsüüdistuse. Seda isegi juhul, kui sinu lapsel ei olnud midagi video tegemisega pistmist ja see lihtsalt saadeti talle. Sellest hoolimata võivad lapsed seista silmitsi raskete ja püsivate tagajärgedega nagu näiteks seksuaalkurjategijate registrisse sattumine. Samuti võib see probleeme tekitada lapsevanemale, sest seadme tegelik kasutaja ei ole üheselt tuvastatav. Alaealise lapse puhul on elementaarne, et nutitelefon ja selle teenusepakett on vanema nimel. Seega võib öelda, et sõnumiga rõhutakse lapsevanemate vastutustundele ning sellele, et ilma nende kontrollita võib saada lapsest ohver või kurjategija. Seaduse rikkumise sõnumi puhul tuuakse tegelikult näiteks sõnumit sekstimine[13] (ing k *sexting*), mida esitatakse aga samuti iseseisva sõnumina.

> *Alaealiste pornograafilise (lapsporno) sisu jagamine või alla laadimine on kuritegu ning ja lapsevanemana on teie kohustus kontrollida oma laste isiklikes mobiilseadmetes olevaid videosid.* (XNSPY, 2020)

Kõik valimis olnud rakendused peale Hoverwatch-i toovad selle välja eraldi ohuna, mille eest peab enda lapsi kaitsma. Kuna ükski tegevus ega oht ei ole täiesti eraldiseisev vaid tihedalt teistega alati mingit moodi seotud, siis sekstimine võib kaasa tuua kiusamise, eriti küberkiusamise. Isegi kui poolalasti või alasti pilte jagatakse kinnises keskkonnas, siis need isikud, kelle kätte pildid satuvad,

[13] Varjamatult seksuaalse või pornograafilise iseloomuga sõnumite ja (enese)fotode saatmine andme- või mobiilside vahenditega (AKIT, 2020)

võivad neid kasutada pildi saatja alandamiseks, edasi saatmiseks või avaldamiseks veebis. Seksuaalse sisu jagamine võib viia püsiva väljapressimiseni ja kahjustada isiku enda väärikust ja mainet kui ka oma perekonna mainet. See omakorda ei pruugi piirduda vaid veebikeskkonnaga või internetis toimuva küberkiusamisega, vaid võib edasi areneda füüsiliseks (seksuaalseks) väärkohtlemiseks, mis leiab aset „päris maailmas“. Hillepi ja Pärnametsa (2020) laste ja noorte seksuaalse väärkohtlemise hoiakute ja kogemuste uuringusse kaasatud spetsialistid jagavad seda sama arvamust: „Virtuaalmaailmas lapsed ei saa aru, kui nad teevad alasti pilte, saadavad teistele ja siis salvestavad telefonidesse, see on kõik kuritegu. Ja samamoodi, et nad ei julge rääkida vanematele, et keegi ähvardab, pressib välja need pildid või soovib a’la kokku saada. Nad ei taju, et Instagramis, Snapchatis või mujal mingi pedofiil või ma ei tea, mis haige inimene salvestab need intiimsisuga videod ja levitab edasi. Et see on suur probleem. Et lapsed istuvad kodus, neil on turvaline oma nelja seina vahel ja tagajärgedele nad ei mõtle.” Samuti toob mSpy enda väite tõestamiseks välja statistikat, et tegemist on probleemiga, mida ei tohi eirata. Samas puuduvad igasugused viited, kus kohast on võetud nende poolses reklaamis välja toodud statistilised andmed.

> *Sekstimine on laste seas levinud probleem, kuna enam kui 30% teismelistest jagab endast alasti või poolalasti fotosid või saadab seksuaalse sisuga sõnumeid. Mitte kõik lapsed pole teadlikud tagajärgedest, mis hõlmavad nii tervise- kui ka juriidilisi probleeme. Pole kahtlustki, et lapsed ei peaks sellist tüüpi käitumisega kokku puutuma.* (mSpy, 2020)

Sukk ja Soo (2018, lk 38) viitavad EU Kids Online’i Eesti 2018. aasta uuringu esialgsed tulemustes, et sekstimisega on Eestis 11-17-aastatest lastest viimase aasta jooksul kokku puutunud 11% küsitletust. Seksuaalse sisuga sõnumeid saadakse lastele tunduvalt rohkem, kui neid lapsed ise saadavad. Küsitluses (EU Kids Online, 2018) osalenud 763-st lapsest 23 on kokku puutunud seksisõnumite saatmisega. Samal ajal selliste sõnumite saajateks on 13–14-aastastest lastest olnud ainult 7% ja 15–17-aastaste laste seas on see näitaja 20%. Seega Eestis tehtud uuring (EU Kids Online, 2018) ei kattu mitte kuidagi mSpy poolt esitatud statistilise väitega, et tegemist oleks laialt levinud probleemiga. Samas on sekstimine ainult üks väärkohtlemise liikidest internetis. 2020 aastal Eesti Vabariigis läbiviidud laste ja noorte seksuaalse väärkohtlemise hoiakute ja kogemuste uuringust selgub, et minimaalselt ühel korral vähemalt ühte seksuaalse väärkohtlemise liiki oli kogenud internetis viimase 12 kuu jooksul 45% 16–26-aastastest noortest (N=558) (Hillep ja Pärnamets, 2020).

mSpy ja XNSPY hoiatavad vanemaid lisaks veel identiteedivarguse eest, mis võib nende lapsi tabada. Kui XNSPY kasutab seda kui lihtsalt ühe märksõnana, siis mSpy mainib eraldi ohuna küberkurjategijaid.

> *Kahjuks mõtlevad lapsed harva isikliku teabe jagamise tagajärgedele. Sellepärast satuvad nad kergesti identiteedivarguste ohvriks. Laste naiivsuse ärakasutamiseks võivad küberkurjategijad hõlpsalt meelitada lapsi oma lõksu pettuseteatega, näiteks: „Ma leidsin koos teiega naljaka foto. Vaata". Seda tehakse eesmärgiga varastada teie lapse isiklikke andmeid, nt paroole.* (XNSPY, 2020)

Lapsele loodud kontod võivad olla seotud vanema kontoga, sest osad keskkonnad võimaldavad erinevaid kasutaja profiile luua või siis ühe kasutaja alla teha mitu erinevat kasutajakontot (nt Netflix). Ühesküljest see võimaldab näilist kontrolli laste tegevuste üle ja lihtsustab veebifunktsioonide haldamist. Samas see muudab aga lapsed küberkurjategijate jaoks atraktiivsemaks sihtmärgiks, kuna läbi nende on võimalik jõuda vanemate andmeteni. Kätte saadud andmeid saab kasutada näiteks identiteedivarguseks või krediitkaardi pettusteks.

3.2.1.2 Lapse kasvatamine

Lapse kasvatamise kategooria alla liigitasin neli sõnumite gruppi: lapse psühholoogilise tervise kaitsmine, halb mõju lapse arengule, küberhügieeni juurutamine ja parema digitaalse keskkonna loomine. Nendele kõigile neljale aspektile on ainukesena tähelepanu pööranud XNSPY. mSpy ja Hoverwatch juhivad tähelepanu, et telefoni installeeritud rakenduste kasutamine võib mõjuda halvasti lapse arengule. Nenditakse, et on olemas rakendused, mis soodustavad arengut, kuid eksisteerivad samuti vastupidise toimega äpid. Siin juures ei tooda ühtegi konkreetset näidet. Sõnum, mis hoiatab arengut pärssiva toime eest on seostud lapse õpingute ja hakkama saamisega koolis.

> *Pidev tekstisõnumite saatmine ja telefonis mängimine võivad mõjutada teie laste haridust, kuna nende tähelepanu on pidevalt häiritud ega suuda õpingutele korralikult keskenduda*. (Hoverwatch, 2020)

Juhul kui lapsevanemal puudub kindel ülevaade, mis nutiseadmes toimub, siis põhinedes analüüsitud sõnumitele võib järeldada lapse arengus seisakut, kui mitte öelda lapse taandarengut. Teise külje pealt võib oletada, et õppimisega seotud sõnumid hoopis püüavad rõhutada vanemate soovile ja tahtele toetada lapse edukust. Mobile Spy koos XNSPY-ga juhivad lastevanemate

tähelepanu veel eraldi sellele, et areneva lapse tervist, seal hulgas psühholoogilist tervist on vaja kaitsta.

XNSPY väidab, et lapse telefonis toimuval pideva kontrolli peal hoides saab kodus juurutada parema küberhügieeni. Olles kogu aeg kursis, mida sinu järglane toimetab nutiseadmes, saab vanem teda juhendada ja õpetada, kuidas ohutult veebi avarustes käituda. Pidev lapse jälgimine võib samas viia ülevoolava kontrollini, mida tuntakse kui ka helikopter vanemlusena (Tigasson, 2018). Mis puudutab parema digitaalse keskkonna loomist, siis selle kohta sõnab XNSPY: „*When you spy on FB messenger, you provide a better digital space to your kids*“. Sõnum esitab küll positiivse tooni, kuid jääb arusaamatuks, kuidas see peaks reaalselt toimima, sest seda mõtet ei ole rohkem lahti seletatud. Võib järeldada, et teenusepakkujad rõhuvad oma sõnumites sellele, et lapsi jälgides loome turvalisema digitaalse keskkonna. Pöördvõrdelise tulemina pole aga välistatud, et lapsed õpivad paremini oma digitaalset jalajälge peitma.

3.2.1.3 Vanemate suhted lastega

Kategooria, mis käsitleb vanemate suhteid enda lastega – selle alla liigitasin kaks sõnumite gruppi: heade suhete hoidmine lastega ja sotsiaalne isolatsioon. Suhete kategoorias on teenusepakkujad eelkõige silmas pidanud lapsevanema ja lapse omavahelist läbisaamist. Mõnede laiendatud sõnumite osas räägitakse üleüldisest sotsiaalsest suhtlusoskusest ning normaalsest toimetulekust ühiskonnas, kus on vajalik inimestega lävida. Sõnumid väidavad, et lapse salajase jälgimisega saab tagada, et lapsevanemad saavad hoida häid suhteid enda lastega. Hoverwatch-i sõnul aitab nähtamatu tarkvara omamine kõige täpsemat informatsiooni saada, täpsustamata millisele informatsioonile viidatakse ja seeläbi päästa oma suhted lastega.

> *Nähtamatu tarkvara omamine aitab teil saada kõige täpsemat teavet ja päästa oma suhted lastega, kuna nad ei pruugi olla üleliia õnnelikud, kui teavad, et saate nende mobiiltelefoniga seotud tegevust jälgida.* (Hoverwatch, 2020)

Samuti lisatakse, et lapsed ei pruugi olla liiga õnnelikud teades, et vanemad saavad mobiiltelefoniga seotud tegevust jälgida. Olenevalt lapse vanusest võib tekkida usalduse küsimus. Kui väikelaps ei pruugi endale teadvustada rakenduse kasutamise eesmärke ja iseloomu, siis vanemate laste puhul võib esile kerkida lapse poolne tõlgendus, et vanemad ei usalda teda. Saab oletada, et rakendust soovitatakse installeerida sihttelefoni laste teadmata. Samuti võib väita, et rakenduste pakkujad siiski juhivad kasutaja tähelepanu sellele, et teenuse kasutamisel võib olla mingi konkreetne negatiivne mõju ning see ei pruugi teisele poolele sobida. Samuti on leitud, et lapsed kipuvad oma halba käitumist varjama ning valetama selle kohta (Marx ja Steeves, 2010).

XNSPY soovitab ühe enda teenuse puhul just vastupidist – öelda lastele, et selline rakendus on telefoni paigaldatud, mis jälgib kõiki tegevusi. Sõnumist lähtudes võib pakkuda, et selline lähenemine peaks kindlustama, et laps enam kunagi ei valetaks vanemale ja seeläbi tagama justkui paremad vanema-lapse suhted. See järeldus põhineb eeldusel, et kui isik, käesoleval juhul laps, teab et teda jälgitakse siis käitub ta paremini. Samas kui sellise jälgimisega ära harjuda, siis võib ära kaduda algne tugevnenud enesedistsipliin. Paralleele saab siin kohal tuua turvakaameratega. Näiteks kaameratega me tihti enam ei pane neid tähelegi. Teame, et need on olemas, aga otseselt seeläbi oma tegevust kontrollida ei pruugi. Klahvilogija teenuse tutvustamisel samas öeldakse, et tegemist on turvalise ja varjatud teenusega, mis pole pealetükkiv, seega laps ei tunne end ebamugavalt kui teenus tema telefonis töötab. Järelikult selle teenuse puhul ei pruugi laps isegi teada, et igat tema klahvivajutus on vanematele nähtav.

Ohuna lapse suhtlus oskusele märgib mSpy sotsiaalset isolatsiooni, mis võib tekkida, kui vanemad otsustavaid samme ei astu, kuidas nende laps telefoni kasutab. Selle tõestuseks toob mSpy näite, milles viitab teaduslikule uuringule. Läbi selle võtte kasutatakse turundamiseks viiteid, mis võivad teenusekasutaja jaoks tähendada, et sellistel praktikatel võib olla ka teaduslik põhi all.

> *Psühholoogid on tõestanud, et lastel, kes veedavad kogu aja ekraanidel, on raskusi näost näkku suhtlemisega. Kui ekraan on saatja ja saaja vahel, tunnevad lapsed end mugavamalt ja avatumalt. Kuid tegelikult viib see võimetuseni näidata oma tegelikke emotsioone ja suhelda inimestega igapäevaelus*. (mSpy, 2020)

Laste nutitelefonide jälgimise mõju vanemate ja laste omavahelistele suhetele on tõenäoliselt sõltuvuses laste vanusest. Väiksemad lapsed usutavasti tolereerivad vanemlikku järelvalvet rohkem, kuid seda arvatavasti võiksid teha teismelised. Põhjus peitub tõenäoliselt selles, kuidas erinevas vanuses lapsed tajuvad vanemate poolset kontrolli ja jälgimist.

3.2.1.4 Kontroll

Kontrolli blokk moodustab pea poole kõikidest suunatud sõnumitest. Selles valdkonnas selekteerisin välja üksteist erinevat sõnumit. Rakenduste lähtuvalt on kontrolli sõnumite hulk arvuliselt kaetud erinevalt: XNSPY – 10, Hoverwatch – 8, mSpy – 7, Mobile Spy – 7. Peamised sõnumid selle kategooria all on:

- kaitsta last veebi sisu eest;
- turvatunne (asukoha teadmine);
- vastutustundlik vanemlik kontroll;

- lapsed ei taju veebiohte, sina tajud;
- meelerahu;
- teadmisvajadus/info nälg/õigus teada;
- sensitiivse info lekke tõkestamine;
- kontroll seadmete üle – mõjutusvahend;
- aja raiskamine;
- liiklusohutuse tagamine.

Esmane mida rõhutatakse on see, et lapsevanem peab kaitsma enda järeltulijat veebi sisu eest. Olgu selleks siis vägivald, pornograafia või rassism. Soovimatu materjali eest saab kaitsta vaid juhul kui omatakse kontrolli seadme üle. See viib meid aga teise argumendi juurde, et lapsed ei taju veebiohte, kuid täiskasvanud tajuvad.

> *Mõned lapsed on naiivsed ja võivad suhelda võõrastega, mis võib olla äärmiselt ohtlik.* (Hoverwatch, 2020)

Kuna erinevad sõnumid on omavahel seotud ning toetavad teineteist, siis kogu sihtseadme kontrollimine annab lapsevanemale meelerahu. See narratiiv on suuremal või vähemal määral valimis esindatud salajast jälgimist võimaldavate rakenduste poolt esile tõstetud. Kõige otsesemalt on see toodud mSpy kodulehel: „*for your peace of mind*“, ehk sinu meelerahu jaoks. Lisaks tuuakse mSpy, Hoverwatch-i ja XNSPY puhul välja, et lapse telefoni jälgimine on tegelikult vastutustundlik vanemlik kontroll. Juhul kui sa hoolid enda lapsest, siis sa ju ometi hoiad tema tegemistel silma peal? Nende sõnumite puhul mängitakse ühelt poolt laste isikuomadustega ja teiselt poolt nii öelda „hea“ lapsevanema kuvandiga.

> *Laialdane järelevalvesüsteem on vastutustundliku vanemliku kontrolli jaoks hädavajalik.* (mSpy, 2020)

Vastutustundliku vanemliku kontrolli alaliigiks võiks nimetada lapsevanemate enda turvatunde ehk lapsevanemaks olemisega kaasnevaks vajaduseks, teadmaks järeltulija reaalset asukohta. Kuna see on aga otseselt seotud geo aediku funktsiooniga[14], siis käsitlen seda eraldi liigina. Ainsana ei märgi seda sõnumit Mobile Spy, kuigi see funktsionaalsus on neil olemas (Mandel, 2020). Teiste rakenduste sõnumid on aga turvatunde loomisel näiteks sellised:

[14] Geo aedik (ing k *geofence*) on objekti raadiuse määramise tehnoloogia. Sellega on võimalik tekitada virtuaalseid geograafilisi piire reaalsete asukohtade ümber. Nendesse digitaalselt loodud, kindla raadiusega perimeetriga aladesse, kas sattudes või väljudes käivitub kasutaja nutiseadmes konkreetsed tegevused. (Prii, 2018; Regio, 2019)

> *Teie lapse asukoht reaalses maailmas peaks olema teile olulisem kui kunagi varem, kuna tänapäeval on lastel väga suur oht langeda väärkohtlemise ohvriks.* (XNSPY, 2020)

> *Tänapäeval on lapsevanematele üks kriitilisemaid väljakutseid laste ohutuse ja tervise tagamine. MSpy abil saate luua turvalised tsoonid kodu, lapse kooli ja muude asukohtade ümber ning saada teateid, kui teie laps neist lahkub. Turvaliste tsoonide seadmine on kasulik, et kaitsta teie last ohtlike või kaugemate linnapiirkondade külastamise eest.* (mSpy, 2020)

Eelneva kahte sõnumit analüüsides võib täheldada viidet, et lapse asukohta teades saab vanem ära hoida väärkohtlemise. Samuti soovitavad sõnumid tekitada füüsilised liikumispiirangud, mille kaudu justkui saaks teatud negatiivseid mõjusid elimineerida. Nagu teistegi sõnumite puhul jääb siingi mõte üldiseks ega anna täpseid juhiseid või lahendusi. Samas Hoverwatch on võtnud geolokatsiooni teenuse ja turvatunde asemel serveerinud sõnumit ühe teise nurga alt.

> *…tegelikult oma töö tegemise või õppimise asemel sihttelefonile raisatud. Kui kõned tunduvad kahtlased, saate geograafilise asukoha funktsiooni abil kindlaks teha, kus helistati.* (Hoverwatch, 2020)

Eelmine näide ilmestab veel ühte aspekti, miks vanemad peaksid salaja jälgima laste nutitelefonide kasutust – aja raiskamine. Olgu selleks siis erinevad mängud, sotsiaalmeedia platvormid või siis liigne helistamine nagu Hoverwatch väidab.

> *Pidev sõnumite saatmine ja telefonis mängimine võivad mõjutada teie laste haridust, kuna nende tähelepanu on pidevalt hajunud ja nad ei suuda õpingutele korralikult keskenduda.* (Hoverwatch, 2020)

Kuidas sundida lapsi enda koolitöid korrektselt ja õigeaegselt tegema, mitte aga telefonis kulutama kuulub kasvatamise osa juurde. Võtteid on selleks erinevaid, kuid ka siin on ettevõtted tabanud soodsa võimaluse kasvatada enda klientide arvu. XNSPY ja Mobile Spy toovad vanematele sõnumi, et salajase jälgimise rakendust saab kasutada ka kui mõjutusvahendit. Juhul kui lapsed ei tee nagu vanemad nõuavad, siis saab telefonis olevaid rakendusi kinni panna või telefon lukustada.

> *Kas vajate võlukeppi, mis võiks julgustada teie lapsi öösel magama ja päeva jooksul kõvasti õppima? XNSPY on kaasaegne lahendus, mis pole vähem kui maagia, kui tegemist on mobiiltelefonide kasutamise vahendamisega. XNSPY abil saate ajutiselt oma laste Android-seadmetes olevad rakendused blokeerida, kuni nad on oma kodutööd, majapidamistööd ja muud olulised ülesanded teinud.* (XNSPY, 2020)

Selle sõnumi puhul on tegemist jõupositsioonilt lähenemisega. Samuti eeldab selline lähenemine, et lapsed on teadlikud, et nende telefoni on paigaldatud selline rakendus. Tühjad ähvardused on viljatud ning domineeriva positsiooni säilitamine nõuab, kas väga veenvat esinemist või demonstratsiooni enda üleoleku kohta. Rakenduste blokeerimise kontekstis tähendab see seda, et lapsi teavitatakse taolise võimekuse olemasolust või siis reaalselt pannaksegi midagi lukku.

Hoverwatch ja XNSPY jagavad ühist sõnum vanematele, et nende rakenduse kasutamisel on võimalik takistada sensitiivse informatsiooni lekkimist. Seda siis lapse enda kohta, kui ka pere puudutavaid andmeid. XNSPY toob selle probleemsõnumi esile Skype-i näites.

> *Lastel on Skype-is võimalik jagada enda tundlikke andmeid eakaaslaste ja anonüümsete inimestega, kuna Skype rakendus kasutab mitmekesiseid sõnumi-, helistamis- ja multimeedia jagamis võimalusi.* (XNSPY, 2020)

Hoverwatch jääb enda näite puhul üldisemaks ega piirdu vaid ühe kindla rakendusega. See viitab just sellele, et jälgimise puhul ei piisa vaid kindlate rakenduste monitoorimisest. Vajalik on saada maksimaalne ülevaade sihttelefonis toimuvast. Kõik neli rakendust rõhutavad, et lapsevanematel on õigustatud teadmisvajadus selle kohta, mida nende lapsed telefonis teevad. Viidatakse samuti sellele, et nõnda saab enda uudishimu rahuldada. Kuigi Eesti Vabariigi Põhiseaduse mõttes ei ole sõnumisaladuse rikkumine õigustatud vanemliku kontrolli rakendamiseks (Baum, 2016), mida teenusepakkujate sõnumite puhul saab nimetada õigustatud teadmisvajaduseks. Samas hüpoteetiliselt võiks lapsevanemal olla kuni lapse teatud vanuse või küpsusastme saavutamiseni õigus omada ülevaadet teabest, mis on kaitstud sõnumisaladusega.

> *Üks asi on seista oma lapse kohal arvuti taga ja jälgida tema Interneti kasutamist, kuid kui nad kannavad oma mobiiltelefoni endaga kaasas, siis kuidas teada, et nad ei vaata ebasobivaid veebilehti, kui te ei vaata? Mobile Spy on ideaalne lahendus. Selle abil näete oma lapse mobiiltelefoni kogu Interneti-tegevust, teadmaks milliseid veebilehti nad külastavad.* (Mobile Spy, 2020)

Lisaks kogu lapse suhtluse kontrollimisele ja enda teadmisvajaduse rahuldamisele pakutakse vanematele võimalust tagada rakenduse lapse telefoni paigaldamise kaudu ka liiklusohutust. Sellega saab tagada mitte ainult lapse ohutust vaid samuti kaasliiklejate turvalisust ning vara kaitset.

> *Sõnumite saatmine sõidu ajal on veel üks oht, millega teie laps silmitsi seisab. XNSPY abil saate jälgida oma laste mobiiltelefonide tekstisõnumeid ja isegi lukustada nende seadmed sõidu ajal.* (XNSPY, 2020)

Peamise tuumiku sõnumitest, mis käivad laste kohta on suunatud sellele, et lapsevanem kasutaks rakendust tööriistana kaitsmaks enda järeltulijaid ja ennetamaks võimalike ohtude teket. Teine läbiv foon on kontroll kõige üle mida laps teeb. Olgu selleks kontroll selle üle kellega ta suhtleb tekstisõnumite ja helistamise vahendusel või milliseid veebilehti külastab, videoid saab ja saadab ning kus kohas reaalajas viibib. Samuti ei pruugi lapsed olla piisavalt elukogenud ja targad, et hoiduda erinevatest ohtudest, mis veebikeskkonnas neid varitseda võivad. Põhjustest miks üks vanem peaks nii käituma varieerub alates sellest, et lapsed võivad varjata ja valetada, kuni selleni et läbi täieliku vanemliku kontrolli on tagatud lapse igakülgne heaolu.

3.2.2 Sõnumid tööandjatele

Teiseks grupiks, kes on salajase jälgimise rakenduse müüjate kõrgendatud tähelepanu alla sattunud, on tööandjad. Rakenduste loojad on ettevõtjate jaoks loonud mitmeid erinevaid sõnumeid, millega nende poole pöörduda, neid mõjutada (vt Tabel 4). Suunatud sõnumitega on põhjalikumalt teemale lähenenud XNSPY ja Hoverwatch. Mobile Spy ja mSpy on tööandjatele, kui potentsiaalsetele klientidele vähem tähelepanu pööranud. Seetõttu leiab nende kodulehtedelt poole vähem erinevaid sõnumeid, millega on otseselt pöördutud tööandjate poole.

Tabel 4 Sõnumid, põhjendused miks peaks tööandja kasutama salajase jälgimise rakendus töötaja nutiseadmes.

		mSpy	Hoverwatch	XNSPY	Mobile Spy
Produktiivsus	Töö produktiivsuse tõstmine		x	x	
	Ettevõtte edukuse tõstmine		x	x	
	Motivatsiooni tõstmine		x	x	
	Tööaja jälgimine		x	x	
	Töötaja asukoha jälgimine	x	x	x	x
	Raha kokkuhoid			x	x
Turvalisus	Ettevõtte maine kaitsmine			x	
	Ettevõtte turvalisuse tagamine	x	x	x	x
	Informatsiooni lekete kõrvaldamine/ vältimine	x	x	x	x
	Andmevarguste tõkestamine	x	x	x	x
	Meelerahu	x		x	x
	Töötajate lojaalsuse kontrollimine		x	x	
	Teadmisvajadus/ info nälg/ õigus teada	x	x	x	x
Suhted	Tööline ei tea, mis on talle tegelikult hea		x		
	Heade tööalaste suhete hoidmine		x		
Telefonikasutuse piiramine isiklikuks tarbeks	Aja raiskamise tõkestamine		x	x	
	Tööajast porno vaatamise elimineerimine		x	x	
	Telefonide eesmärgi pärane kasutamine (ametialaseks kasutamiseks)		x	x	x
	Tööalase kiusamise tõkestamine			x	

(Autori poolt koostatud seisuga 14.03.2020)

Põhjustest miks tööandjatele suunatud sõnumite hulk on väiksem võib peituda seaduslikus regulatsioonis (nt andmekaitse). Kui eraelus on jälgimisega seotud „mänguruum“ suurem, siis töötajate jälgimine on komplitseeritum. Samuti on see seadusandlikult paremini reguleeritud. Lisaks on täiskasvanud paremini informeeritud enda õigustest. Väga suures ja üldistavas raamis on tööandjatele seatud sõnumid otseselt või kaudsemalt seotud ettevõtte kaitsmisega ja töötajate kontrollimisega. Teenusepakkujad ei täpsusta ettevõtte kaitsmise narratiivi kasutades, et mis kaitset vajab. Põhjus taolises umbmäärasuses võib asetseda selles, et olenevalt firmast ja selle juhtides, kaitset vajav objekt ei pruugi olla üks ja see sama. Jättes aga sõnumi piisavalt üldistava saavad erinevat perspektiivi omavad ettevõtjad sõnumiga sellest hoolimata samastuda. Olgu siis kaitsmist nõutavaks esemeks ettevõtte varad, ressurss, intellektuaalne omand või midagi muud. Järgnevalt toon Tabelis 4 viidatud kategooriate kaupa välja peamised sõnumid, mida teenusepakkujad kasutavad.

3.2.2.1 Produktiivsus

Produktiivsuse kategooria alla grupeerisin kuus erinevat sõnumite rühma: töö produktiivsuse tõstmine, ettevõtte edukuse tõstmine, motivatsiooni tõstmine, tööaja jälgimine, töötaja asukoha jälgimine ja raha kokkuhoid. Mobile Spy toob all olevas näites välja, et ettevõtte juhtimine ja käigus hoidmine on kulu. Mida väiksemad on jooksvad kulutused, selle võrra jääb rohkem raha üle mida investeerida või kasumina välja võtta. Seega ühe sõnumina tullakse tööandjate juurde sellega, et kontrollides töötajatele kätte jagatud töötelefone on võimalik raha kokku koida. Seda siis kas piirates nende kõnede hulka või reaalajas jälgida, kus nad ametiautodega viibivad. Viimane sobiks transpordisektoris tegutsevatele firmadele.

> *Tööandjad annavad need telefonid oma töötajatele ainult tööks. Kas teie ettevõte maksab iga kuu töötaja mobiiltelefoni kasutamise eest tohutult palju? Kuidas te teate, kas teie töötajad kasutavad ettevõtte telefone ettenähtud tööks? Kas nad kasutavad oma ettevõtte sõidukeid töö eesmärgil?* (Mobile Spy, 2020)

Üheks võimaluseks kasumi suurendamiseks on kulutuste kärpimine, siis teine võimalus selleks on tootlikkuse/produktiivsuse tõstmine. Sõnumite vaatevinklist saame eristada kahte erinevat lähenemist: töötajate produktiivsuse tõstmine ja ettevõtte edukuse tõstmine.

> *Töötajate mobiiltelefonide jälgimislahendus, mis ei ole pealetükkiv, annab neile ruumi segamatult töötada. Mobiiltelefonide jälgimine on mõeldud tootlikkuse tõstmiseks, mitte selle hävitajaks. Töötajate kaugjälgimise vajaduste jaoks valige ainult XNSPY ja tehke oma ettevõte uhkeks!* (XNSPY, 2020)

> *Skype on sageli kasutatav vestlus- ja videokõnede tarkvara, mis on kontorites eriti kuulus tänu oma kättesaadavusele peaaegu kõigis mobiilsidesüsteemides. Ettevõtted, kes ei suuda edukalt lahutada töötajate tööd ja töövälise tegevusi, kannatavad lõpuks tootlikkuse langusega.* (XNSPY, 2020)

> *Kui teate, kuidas tekstisõnumeid luurata ja töötajate tegevust jälgida, pole see enam probleem, mis võib teie ettevõtte edu mõjutada.* (Hoverwatch, 2020)

Rakenduse poolt esitatud sõnumid ei anna ettevõtjatele ühtegi kindlat tegevuskava või suunist, kuidas peaks töötajate jälgimine nende teenuse vahendusel tõstma firmade tootlikust/edukust. XNSPY viitab küll töö ja tööväliste tegevuste lahus hoidmisele, kuid sõnumi kontekstis kasutatav Skype näide ei tee sõnumit selgemaks ega paremini mõistetavaks. Võib oletada, et ettevõtte juhile püütakse kuvada arusaam, et töö tarbeks ettenähtud Skype rakendust ei kasutata tööga seotud kõnedeks vaid isiklikuks tarbeks. Omades aga täielikku kontrolli, mida suhtlusplatvormis vahendusel tehakse, saaks töötajaid korrale kutsuda. Teoreetiliselt võib nende sõnumite puhul pakkuda, et teenusepakkujad püüavad just sellise loogika alusel sisendada tööandjatele, et nõnda on võimalik tõsta töötajate produktiivsust ja seeläbi ettevõtte edukust. Tööaega kasutatakse töö tegemiseks ning ei kulutata kõrvaliste tegevuste peale. Kolmanda komponendina tootlikkuse suurendamise osas toovad Hoverwatch ja XNSPY esile motivatsiooni tõstmise.

> *Suureks motivatsiooniks on rohkem vaeva näha, kui teate, et teie iga tegevust jälgitakse ja võrreldakse seda teiste töötajatega. Kuni te ei kehtesta oma töötajatele hullumeelseid reegleid, on kõigil hea meel (välja arvatud loodrid ja muiduleivasööjad) selle rakenduse installimisel kõigi ettevõtte mobiilseadmetesse.* (Hoverwatch, 2020)

Motivatsiooni näite puhul saame väita, et sõnum soovitab tekitada kollektiivis võistlus momendi. Selle tulemiks peaks ideaalis olema töötajate vaheline konkurents, mis suurendab tööliste motivatsiooni enda tööd veelgi paremini teha. Jääb küsitavaks kui efektiivselt selline süsteem iseseisvalt toimiks. Oletuslikult peaks juures olema stiimulite pakett, mis premeerib tublimaid teenistujaid ning samuti läheb vaja väga selgeid meetmeid nende jaoks, kes ei ole motiveeritud. Jääb vaieldavaks, kui tõhus selline motiveerimine võib osutuda, kui igat sinu tegevust jälgitakse. Inimeste privaatsuse vajadused on erinevad ning seda tunnetatakse enda jaoks erinevalt (Regan, 2000). Oma rolli mängib siin juures kindlasti see, millises valdkonnas tegutsetakse ning milliseid andmeid töödeldakse. Näiteks avalikus sektoris töötavate julgeoleku valdkonna ametnike arvuti kasutamisel jälgitakse igat kui viimast liigutust. Põhjust selleks on kuna küberturvalisuse spetsialistid ütlevad, et turvaketi kõige nõrgem lüli on inimesed, mitte tehnoloogia (Alashe, 2019;

Matthews, 2017; Mitnick, 2003). Ära ei tohi unustada siinjuures seda, et kui ühes valdkonnas on taoline jälgimine vajalik ning aktsepteeritud, siis see kindlasti ei pea olema teistes tööstusharudes. Pealegi jääb küsitavaks ikkagi kuidas telefoni kasutamist ning selle sisu jälgimine motivatsiooni tõstab. Tegemist on vaid ühe töövahendiga ning kui töötajal endal puudub selge võrdlusmoment, siis muutub selle otstarbekus küsimärgi alla.

Teistsuguse mõõtme toob sisse töötaja asukoha jälgimine, kasutades salajast jälgimise rakendust. Võimalus enda töötaja asukohta reaalajas vaadata on teenus, mis leiab sõnumites tunduvalt täpsemaid soovitusi kasutuseks, kui teised teenused.

> *Saate teada enda töötaja hetkeasukoha üksikasjalikul kaardil ja kontrollida tema marsruudi ajalugu kindla ajavahemiku jooksul, saate alati teada, kus nad konkreetsel hetkel asuvad. Eriti nende kohta, kes on sageli teel. Ettevõtteomanikuna on teil täielik õigus teada, kuidas nad oma tööaega veedavad!* (mSpy, 2020)

> *See (rakendus) jälgib kõigi teie kontoris asuvate inimeste täpset asukohta, nii et näete, kui palju aega kõnealune isik veedab lõunapausideks või muudeks tegevusteks.* (Hoverwatch, 2020)

Tööliste asukoha jälgimist käsitlevate sõnumite puhul on väga märkimisväärne mSpy sõnum, kus rõhutatakse, et jälgimise alla kuulub just tööaeg. See viitab sellele, et tööväline aeg ei tohiks jälgimise alla kuuluda. Teiste teenusepakkujate puhul see aspekt nii selgesõnaliselt ei väljendu.

mSpy näide kirjeldab eelkõige transpordi sektorit hõlmavat teenuse rakendust. Näiteks kaugsõidu autojuhtide puhul saab ülemus kontrollida, kas alluvad peavad kinni seadusega sätestatud töö- ja puhkeaja seadusest, järgivad etteantud marsruuti ega tee juhuslikke kõrvaltöid.

Üheks potentsiaalseks rakenduseks soovitatakse enda teenus hankida selleks, et pidada tööaja arvestust. Kontrollida efektiivsemalt, et töötajad teeksid töö ajal tööd, mitte ei tegeleks kõrvaliste asjadega. Olgu siis selleks liigne aja veetmine suitsunurgas või pikale venitatud lõunapausid. Lisaks sellele saab registreerida tööle saabumise ja sealt lahkumise aja, mille alusel saab pidada tööaja arvestust ning lähtuvalt sellest arvutada inimese palga.

3.2.2.2 Turvalisus

Produktiivsuse kõrval on järgmiseks suuremaks blokiks turvalisuse temaatika, mis on teenusepakkujate sõnumite üheks kandvaks teemaks. Sinna alla kuuluvad alamteemad nagu: ettevõtte maine kaitsmine, ettevõtte turvalisuse tagamine, andmevarguste tõestamine,

informatsiooni lekete kõrvaldamine/vältimine, töötajate lojaalsuse kontrollimine, meelerahu ja teadmisvajadus/ info nälg/ õigus teada.

> *Kas teie töötajad saadavad ettevõttele kuuluvat vara? Kas nad kustutavad oma telefonilogid? See ei loe, sest tarkvara ei sõltu telefoni sisemisest logimissüsteemist.* (Mobile Spy, 2020)
>
> *Töötajatega seoses saate teada, kas nad lekitavad teie ettevõttele kuuluvat konfidentsiaalset teavet.* (Hoverwatch, 2020)

Töötajaid kujutatakse antud sõnumites kui potentsiaalsed riski allikad, kes võivad firma reeta, müües konkurentidele praeguse tööandja ärisaladusi. Nende sõnumitega tekitatakse usaldamatust enda alluvate suhtes ning soodustatakse teatud paranoiat, meelitades nõnda ettevõtte juhte kahtlustama ja kontrollima enda töötajate igat tegevust. Kahtlemata on enda ettevõtte sisese informatsiooni kaitsmine oluline aspekt, millele tuleb mõelda. Tööstuslik spionaaž on läbi aegade toimunud ning praegune ajastu ei ole erandiks. Erinevate turvasüsteemide (tulemüürid, autentimine jne) rakendamine ja integreerimine erinevatesse protsessidesse tagavad enamasti selle, et keegi ei pääse väljast poolt sisse andmetele ligi. Olenevalt süsteemist peaksid need samuti tagama selle, et keegi informatsiooni välja poole ei levita. Samas organisatsiooni sees tegutsev isik on tuttav kehtestatud meetmetega ja võib leida turvaaugu, mida saab ära kasutada ja ettevõttele kahju tekitada. Värvika näitena siinkohal on analoogiks Edward Snowden-i juhtum[15].

> *Klientidele, kes kaitsevad oma ärisaladusi ja intellektuaalset omandit töötajaid rõhumata; jõustada eeskirju jälgides, mitte filtreerides ega keelates.* (Hoverwatch, 2020)
>
> *Kasutades Androidi XNSPY spioonirakendust, saate teada, kas teie töötajad plaanivad teie vastu vandenõud. Samamoodi saate teada ka seda, millised töötajad on teile tõeliselt lojaalsed.* (XNSPY, 2020)

Lisaks usaldamatusele on üheks komponendiks teadmatus. Kui tööandja ei tea, mida töötajad teevad, siis puudub ka teadmine kas ollakse lojaalsed või mitte. Sellisel juhul võib salajase jälgimise rakendus muutuda üheks tööriistaks mida saab rakendada firma juhtimiseks, kuna ettevõtte juhtimine kindlasti nõuab teadmisi ja julgust võtta vastu otsuseid. Samuti võib see tagada teatud meelerahu tööandajale. Seda on mSpy kohe otsese sõnumina esile toonud: „*for your peace of mind*“ ehk teie meelerahu jaoks.

[15] Lekitas informatsiooni NSA ja CIA ülisalajase jälgimisprogrammi PRISM kohta.

> *Selles kõrilõikajalikus ärimaailmas ei saa te teha otsuseid, mis põhinevad oletustel, millega teie töötajad kogu päeva vältel tegelevad, välja arvatud juhul, kui kasutate XNSPY-d ja jälgite kogu päeva jooksul nende tegelikke ja digitaalseid tegevusi. Ettevõtete omanikud saavad mitu litsentsi korraga ostes raha kokku hoida ja saada kasu paljudest suurepärastest jälgimisfunktsioonidest.* (XNSPY, 2020)

Seoses suurenenud informatsiooni hulgaga, millele juhil on juurdepääs, võimaldab paremini korraldada enda otsuste vastuvõtmise protsessi. Ühelt poolt pakub XNSPY oma sõnumiga, et konkurentide ees on võimalik edu saavutada (vt *kõrilõikajalikus ärimaailmas*), kui jälgida enda töötajaid. Samas analüüsides seda sõnumit tekitab küsimust fraas: „*jälgite kogu päeva jooksul nende tegelikke ja digitaalseid tegevusi*“. See eeldab töötajate tegelike tegevuste jälgimist digitaalsete kõrval. Järelikult võib eeldada, et taoline kombineeritud andmestik annab tööandjale alles selge pildi sellest, mida töötaja tegelikult teeb. Ettevõtte juhtimine on siiski päris ajakulukas tegevus, seega kogu enda fookuse suunamine töötajate jälgimisele ei tundu optimaalne ega ratsionaalne. Erisusena võiks sellisesse raami sobida pigem spetsiaalne osakond, mis ongi loodud puhtalt enda töötajate jälgimiseks. Ajaloolises narratiivist võiks paralleelina tuua näideteks KGB ja Gestaapo.

Ähmaste piiridega on veel teised sõnumid, mida salajaseks jälgimiseks mõeldud rakendused tööandjatele edastavad. „Teadmisvajadus/ info nälg/ õigus teada“ valdkonna alla liigituvad sõnumid ei piirdu vaid ettevõtte huvidega seotud info jälgimisest. Seal on otsesed viited inimeste eraelu puudutavate andmete jälgimisele.

> *Kui olete mures, et teie töötaja kasutab mobiiltelefoni sobimatult, on Mobile Spy just teie jaoks. SMS, Facebook ja muud tekstisõnumid on muutunud populaarseks viisiks inimeste omavaheliseks suhtlemiseks. Mida nad seal kirjutavad? Suitsetamine, uimastid või sekstimine? Kas nad on seal, kus nad peaksid olema? Kas teie töötajad paljastavad konfidentsiaalset teavet? Teil on õigus teada.* (Mobile Spy, 2020)

> *Inimesed planeerivad suurema osa sündmustest oma nutitelefonides olevatesse kalendritesse. Kui teil on vaja teada, mida teie töötajad kavatsevad teha ning kuhu minna, on see kalendri jälgimise funktsioon teile väga kasulik. Saate vaadata kõiki kasutaja sisestatud meeldetuletusi ja saada ülevaate tema igapäevastest tegevustest. Rakendus annab koos SMS-ide ja häälkõnede jälgimisega kogu vajaliku teabe.* (Hoverwatch, 2020)

Nagu näidetest näha, siis sõnumitega soovitatakse jälgida mida töötaja teeb, kellega suhtleb ja milline on selle suhtluse sisu. Peamine põhjus/põhjendus millele juhitakse tähelepanu on see, et

tööandjal on õigus teada. Pääsedes ligi kogu sellele andmestikule saab tööandja kindlasti midagi huvitavat teada ehk rõhutakse inimeste uudishimule.

3.2.2.3 Tööandjate suhted töötajatega

Sõnumite blokk tööandjate suhted töötajatega sisaldab endas kahte erinevat alamsõnumite kooslust, milleks on see, et tööline ei tea, mis on talle tegelikult hea ja heade tööalaste suhete hoidmine. Kuna juhtide vastuvõetud otsused ei pruugi alati olla koheselt arusaadavad alluvatele, sest nendel puudub sama infoväli, mida omab ettevõtja. Sellega osaliselt haakub Hoverwatch-i sõnum: „…*employees may not realize what is good for them*…“, ehk töötajad ei pruugi aru saada mis on neil hea. Sõnumiga viidatakse justkui sellele, et ettevõtja ongi nn „kõrgemal tasemel“ võrreldes töölisega. Taoline enesekindlus ja arvamus, et ülemad teavad kõige paremini, kuidas asjad käima peavad, võib hukatuslikuks saada. Juhid ei arvesta alluvatega ega nende arvamuste ja ettepanekutega. Olukorra progresseerudes muutub paratamatult firma sisekliima halvemaks. See võib lõpuks päädida kas tööliste lahkumisega või mõne muu negatiivse stsenaariumiga ettevõtte edukuse võtmes. Eeldusel, et ei muutu ülemate kindel arvamus, et nemad teavad kõike kõige paremini.

Sihttelefoni totaalne kontrollimine võib tõesti olla kasulik tööriist ülematele. Sõnumi analüüsi põhjal võib pakkuda, et töötajaid pigem ei teavitata taolisest jälgimisrakendusest, sest nad ei pruugi ju aru saada selle kasumlikkusest. Tulu või kahju saab aga peituda ülemate tegudes või tegemata jätmises seoses selle informatsiooniga, mida selle teenuse vahendusel omandatakse.

> *Nähtamatu tarkvara omamine aitab teil saada kõige täpsemat teavet ja päästa oma suhted töötajatega, kuna nad ei pruugi olla liiga õnnelikud, kui teavad, et saate nende mobiiltelefoniga seotud tegevust jälgitakse. Seetõttu on üsna kasulik kasutada nähtamatusrežiimi ja teada, et teie töötajad ei muudaks oma käitumist nutitelefonides oleva tarkvara tõttu.* (Hoverwatch, 2020)

Hoverwatch-i sõnum, mis puudutab suhete hoidmist viitab otsesele soovitusele varjata jälgimisrakenduse olemas olust sihttelefonides töötajate eest. See omakorda läheb aga täielikult vastuollu nende poolt edastatava motivatsiooni sõnumiga, mis just soovitab teavitada alluvaid spioonrakendusest. Võimalik seletus sellele võib asetseda faktis, et tahetakse enda sõnumites olla võimalikult eripalgeline ja seetõttu ei lasta end taolistest konfliktidest häirida. Samuti näitab see seda, et rakenduse müümisel on eetilised ja seadusandlikud piirid hägustatud.

3.2.2.4 Telefonikasutuse piiramine isiklikuks tarbeks

Sõnumite kategooria, mis käsitleb telefonikasutuse piiramist isiklikuks tarbeks hõlmab endas nelja erinevat sõnumite rühma:

- aja raiskamise tõkestamine;
- tööajast porno vaatamise elimineerimine;
- telefonide eesmärgi pärane kasutamine (ametialaseks kasutamiseks);
- tööalase kiusamise tõkestamine.

Väidetavalt kulutavad töötajad tunde, et külastada enda lemmik veebilehti või lihtsalt mängivad telefoniga töö ajast. Rõhutatakse teenuse osutajate poolt sõnumeid, et telefone tuleb kasutada eesmärgipäraselt, mitte isiklikuks tarbeks.

> *Pealegi, selle jälgija abil salvestatakse kõik telefonivestlused ja tekstisõnumid, seega töötajad ei kasuta ettevõtte telefone isiklikuks otstarbeks.* (XNSPY, 2020)

> *Peaaegu iga töötaja hakkab looderdama, kui tal on tunne, et ka nii saab. Kellelegi ei meeldi rasket vaeva näha, eriti kui keegi üle õla ei vaata.* (Hoverwatch, 2020)

Nagu XNSPY märgib enda sõnumis, et kui töötajad on teadlikud, mida installeeritud rakendus teeb, siis nad loobuvad sihttelefoni kasutamisest isiklikuks otstarbeks. Hoverwatch väidab enda sõnumiga, et töölised on juba enda loomu pooles laisad ega soovi töö tegemisse panustada. Ainus meede tööle sundimiseks on see, kui nad tunnevad, et keegi pidevalt neid jälgib. Salajase jälgimise rakendus oleks just kui virtuaalne kubjas, kes paneb töötajad pingutama.

Sõnum, mis eraldi käsitleb ajaraiskamine tööajast, on pornograafia vaatamine.

> *70 protsenti kogu pornograafia veebisaitide liiklusest tuleb tööajal. Ärge olge tööandja, kelle töötajad veedavad oma päeva tööl pornot vaadates*. (XNSPY, 2020)

Lähtuvalt pakutavatest teenustest, mida rakendaja müüjad pakuvad, siis pornograafia vaatamise takistamine on rakendatav läbi tõkestamise. Veebilehtede blokeerimise võimalust aga pakub vaid mSpy. Kuidas on mõeldud teistel teenuse pakkujatel tõkestamine realiseerida, jääb sõnumite analüüsis selgusetuks. Teine väga huvitav sõnum mida XNSPY on välja käinud, väidab et nende rakenduse kasutamisel saab võidelda tööl leviva kiusamise vastu.

> *XNSPY abil saate ka võidelda töökohal esineva kiusamise vastu, mis on silmapaistev probleem suhtlusvõrgustikurakenduste kasutamisel töötajate poolt.* (XNSPY, 2020)

Peamine märksõna mis läbivalt jookseb kõikides sõnumites on kontroll. Kontroll kõige üle, mis sihttelefonides toimub. Ülevaade sellest kus töötajad asuvad ja kuidas nad telefone kasutavad. Mõningad sõnumid soovitavad alluvaid teavitada, et selline jälgimise rakendus on paigaldatud. Ja läbi selle saavutada soovitud efekti. Teisel pool on aga sõnumid, mis soovitavad varjata seda ning kasutada rakendust pigem salajase andmekogujana ja luurata oma töötajate järele.

4 ARUTELU

Sõnumite ampluaa, mida teenusepakkujad esitavad sihtrühmadele, on märkimisväärselt laialdased. Uuringu tulemustest lähtuvalt saab väita, et kõige kesksem sõnum on kaitsmine. Kaitsmise teemat aga edastatakse peamiselt kontrolli võtmes, et jälgijal peab olema ülevaade kõigest mis sihtseadmes toimub ning läbi selle on tal võimalik teostada kellegi või millegi kaitset. Täpselt nagu Murumaa-Mengel jt (2014) enda uuringus märgivad, et kontrolli idee näib olevat kõike hõlmav, siis seda sama saab väita samuti nuhkvara rakenduste sõnumite puhul. Seda toetab näiteks rakenduste funktsioon jääda sihttelefoni kasutaja eest varjatuks (Eterovic-Soric jt, 2017; Garrie, Blakley ja Armstrong, 2007).

Uuringu käigus selgus, et teenusepakkujad kasutavad enda teenuse reklaamimiseks erinevaid märksõnu. Näiteks paralleelselt leiavad kasutust terminid jälgima (ing k *monitor*) ja luurama (ing k *spy*). Üheks põhjuseks miks terminitega nn „mängitakse“ võib olla soov end teha nähtavaks. See võib tõenäoliselt olla seotud kodulehe otsingumootoritele optimeerimisega, läbi mille suurendatakse kodulehe leitavust ja usaldust otsingumootorites (Veebikoda, 2017). Teise põhjusena võib olla teenusepakkuja soov laiendada enda toote sõnumit võimalikult suurele osale sihtrühmast. Motiivid salajase jälgimise rakenduse kasutamiseks ühes sihtrühmas tõenäoliselt varieeruvad. Näiteks üks tööandja tahab seda kasutada töötajate liikumisteede monitoorimiseks kontoris, et parandada kabineti arhitektuuri (tõsta pidevat koostööd tegevate alluvate töökohad üksteise lähemale). Teine tööandja tahab kasutada teenusepakkuja rakendust töötajate järele luuramiseks, et tabada alluv kes müüb konkurentidele asutusesiseseks kasutamiseks mõeldud informatsiooni. Lisaks erinevate märksõnadega varieerimisele teenusepakkujad ei täpsusta näiteks ettevõtte kaitsmise narratiivi kasutades, et mis kaitset vajab. Põhjus taolises umbmäärasuses võib asetseda selles, et olenevalt firmast ja selle juhtides, kaitset vajav objekt ei pruugi olla üks ja see sama. Jättes aga sõnumi piisavalt üldistava saavad erinevat perspektiivi omavad ettevõtjad sõnumiga sellest hoolimata samastuda. Olgu siis kaitsmist nõutavaks esemeks ettevõtte varad, ressurss, intellektuaalne omand või midagi muud. Täpselt samasuguse loogika alusel lähenetakse lapsevanemate sihtrühmale. Seega soovides mõlemale enda teenust müüa, tuleb enda sõnumeid vastavalt varieerida kliendi potentsiaalsetele ootustele ja soovidele.

Uuringu tulemustest leidsin, et salajase jälgimise rakenduse teenusepakkujate fookuses on kaks sihtrühma – lapsevanema ja tööandja. Vanematele soovitatakse nuhkrakendust kasutada laste jälgimiseks ning tööandjatel enda alluvate jälgimiseks. Toetudes varasematele uuringutele võis eeldada, et spioonrakendust soovitatakse kasutada elukaaslastel enda partnerite jälgimiseks (Chatterjee jt, 2018; Freed jt, 2018; Harkin, Molnar ja Vowles, 2019), kuid käesoleva uuringu tulemused seda väidet ei toeta. Seadusandlikust aspektist lähtuvalt on salajase jälgimise rakendus teenus, mis oma olemuselt eksisteerib nn „hallil alal". Jääb selgusetuks põhjus, miks teenusepakkujad on loobunud kasutamast sõnumeid, mis soovitavad rakendust kasutada elukaaslaste või partnerite jälgimiseks. Võimalik seos võib peituda 2018. aastal jõustunud IKÜM-ga (Euroopa Parlament; Euroopa Liidu Nõukogu, 2016).

Samas sõnumid laste ja töötajate jälgimiseks on jätkuvalt olemas. Eeldades, et ühe sihtgrupi kadumine fookusest on seotud seadusloomega. Sellest saab siis järeldada, et laste ja töötajate õiguskaitse pole piisav, kuigi Eesti Vabariigi põhiseadus (1992) § 43, mis kaitseb sõnumisaladust peaks selle välistama. Lisaks on igasugune varjatud ja ilma nõusolekuta jälgimine on kriminaalne ja karistatav. Juhul kui isik on nõusoleku andnud, siis võib ka ainult selle nõusoleku ulatuses andmeid koguda. Eestis kehtivad seadused, mis kaitsevad inimest salajase jälgimise eest on piisavalt üldised, et rakenduvad samuti digikeskkonna kontekstis. Sellest hoolimata eksisteerivad vabalt kättesaadavad teenused, mis võimaldavad aga just salajast jälgimist teostada tavalisel kodanikul. Sellisel juhul tekib küsimus ega käesolevad seadused ole liiga üldised, et teenuste müük, mis võimaldavad inimeste järele luurata, tundub olemagi lubatud.

Kindlasti vajab salajase jälgimise rakenduse kasutamine sügavamat analüüsi juriidilisest aspektist. Kui õiguspärane on nuhkrakendust kasutades inimeste järele luurata? Kas Eesti seadustes võib leida augu, mis lubavad rakendusi kasutada salaja, ilma sihttelefoni kasutaja nõusolekuta? Samuti võib seda teemat veelgi piiritleda ning uurida, milline õiguslik raamistik kohaldub taolise tegevuse puhul, kui subjektiks on alaealine laps. Teenuste vahendajad on samuti teadlikud, et nende tegevus toimub seadusandlikus mõistes nn „hallil ala". Milliseid meetmeid on nuhkrakenduse müügist tulu teenivad ettevõtted rakendanud, et kaitsta ennast võimalike juriidiliste probleemide ja kohtusse sattumise eest?

Teenusepakkujate suur tähelepanu on sõnumites koondunud selle ümber, et vanemad peavad jälgima ja kontrollima põhimõtteliselt kõike seda mida nende laps nutitelefonis teeb. Hoidma silma peal sellele kellega räägib, milliseid veebilehtesid vaatab, kui kaua aega kulutab nutiseadmele jne. Kindlasti on vajalik, et lapsevanem õpetab oma järeltulijat kõige selle osas, mis puudutab

tänapäevaseid seadmeid ja omab ülevaadet olukorrast. Seega lähtuvalt vanemlikust kasvatusest kui ka tulevaste suhete mõttes või isegi eetilisest aspektist mõeldes – on see siiski hea kui vanemad nii ulatuslikult lapsi jälgivad? Teatud maalt läheb piir ratsionaalse vanemliku kontrolli ja nn „helikopter vanemluse“ vahel. Samas Helberg (2018) leidis, et jälgimis äppide kasutamine laste peal ei toonud mingeid muutusi ega eripärasusi ning lapsevanemad pigem arvasid, et rakenduse mõju perekonnasisesele usaldusele on pigem positiivne.

KOKKUVÕTE

Minu lõputöö on kirjutatud teemal „Telefonikasutaja salajaseks jälgimiseks mõeldud rakenduste sihtrühmad ja nendele suunatud sõnumid“. Uuritav valdkond on oluline ja huvipakkuv, kuna tehnoloogia arenguga on muutunud andmete jagamine ja informatsioonile ligipääs hõlpsamaks. Sellest johtuvalt on aga muutunud isikliku informatsiooni kaitsmine üha keerulisemaks. Teemavaliku ajendiks oli seminaritöö raames teostatud uuring, mis käsitles telefonikasutaja salajaseks jälgimiseks mõeldud rakenduste võimekusi.

Lõputöö eesmärgiks oli selgitada välja sihtrühmad, kellele sõnumid on suunatud ning kaardistada ja analüüsida sõnumeid, mille kaudu konkreetseid teenuseid turustatakse. Uurimisküsimustele vastuse saamiseks kasutasin läbikäimismeetodit nelja salajase jälgimisrakenduse teenusepakkuja veebilehe analüüsimiseks.

Uuringu tulemustest selgus, et sihtrühmasid on kaks, kellele sõnumid on suunatud – lapsevanemad ja tööandjad. Teenusepakkujate sõnumid keskendusid sellele, et salajase jälgimise rakendust peaksid lapsevanemad kasutama enda laste peal ning tööandjad enda alluvate jälgimiseks. Erandina on XNSPY-l sõnumid haridusasutustele, soovitades enda rakenduse teenuseid kasutada koolis õpilaste jälgimiseks. Isoleeritud leiuna on XNSPY-l 2017.aastast viide spioonrakenduse kasutamise soovitusest elukaaslase jälgimiseks.

Suunatud sõnumite analüüsimisel selgus, et peamine fookus on seatud mõistega kaitsmine ja sekundaarsena joonistus välja kontrolli temaatika. Lastevanematele rihitud sõnumid kandsid pea eranditult narratiivi, et vanem peab kaitsma enda last erinevate võimalike ohtude eest. Väljund selle teostamiseks on aga kontrolli omamine lapse telefoni üle. Ettevõtjate puhul on kaitset vajavaks objektiks firma, mida siis peab kaitsma samuti erinevate ohtude eest. Üheks riskiks on firma töötajad ise või siis on nad vahendiks mõnele välisele ohuallikale. Tööandjate kontrolliga seotud sõnumid on tihedalt põimitud töötajate maksimaalse ekspluatatsiooniga firma hüvanguks.

Sõnumite kuvamisel on kõigi teenusepakkujate ühiseks jooneks erinevate sõnumite ristkasutamine, et põhjendada, õigustada või näitlikustada edastatavat sõnumit. Rõhutatakse

pidevale olukorrateadlikkuse vajalikkusele ja sellele, et salajase jälgimise rakenduse kasutamisel on kasusaajateks mitte ainult rakenduse kasutajad, vaid samuti need, keda hakatakse jälgima.

SUMMARY

My dissertation is written on the topic of "The Target Groups of Applications for Secret Monitoring of Telephone Users and the Messages Aimed at the Users". This field of study is important and interesting as technological developments have made it easier to share data and access information. As a result, the protection of personal information has become increasingly difficult. The choice of topic was motivated by a study conducted in connection to the seminary work, which dealt with the capabilities of applications intended for secret surveillance of telephone users.

The aim of the dissertation was to identify the target groups whom the messages are addressed to and to map and analyse the messages that are used to market the specific services. To answer the research questions, I used a walkthrough method to analyse the websites of four secret tracking service providers.

The results of the survey revealed that there are two target groups whom the messages are addressed to - parents and employers. The messages from the service providers focused on the fact that the covert surveillance application should be used by parents on their children and by employers to monitor their subordinates. As an exception, XNSPY has messages for educational institutions recommending the use of its own application services to monitor students at school. As an isolated finding, XNSPY has a reference from 2017 to the recommendation of using a spy application to monitor a spouse.

The analysis of targeted messages revealed that the main focus is on the concept of protection and, secondarily, on the topic of control. The messages lined up for the parents almost exclusively included the narrative that the parent must protect his or her child from various possible dangers. The way to do this, however, is to have control over the child's phone. In the case of entrepreneurs, the object in need of protection is the company, which must then also be protected from various threats. The company's employees themselves are one of the risks or they are a means to some external source of danger. Employer control messages are thoroughly entwined with the idea of maximum exploitation of the employees for the benefit of the company.

When displaying messages, the common feature of all service providers is the cross-use of different messages to justify or illustrate the message being transmitted. It is emphasized that there is a constant need for situational awareness and that the beneficiaries of a covert surveillance application are not only the users of the application, but also those who will be monitored.

KASUTATUD KIRJANDUS

Alashe, O. (2019). Are Humans Really “The Weakest Link” In The Cyber Security Chain? *Computer Business Review*. Kasutamise kuupäev: 11. 04 2020. a., allikas https://www.cbronline.com/opinion/are-humans-really

Andmekaitse ja infoturbe leksikon. (2020). Kasutamise kuupäev: 23. 08 2019. a., allikas Andmekaitse ja infoturbe leksikon: https://akit.cyber.ee/

Baum, A. (2016). Nuhkimisest….juriidiliselt. *Märka Last*. Kasutamise kuupäev: 26. 08 2019. a., allikas https://ajakiri.lastekaitseliit.ee/2016/02/12/nuhkimisest-juriidiliselt/

Cayford, M., & Pieters, W. (08. 03 2018. a.). The effectiveness of surveillance technology: What intelligence officials are saying. *The Information Society, 34*(2), 88-103. doi:https://doi.org/10.1080/01972243.2017.1414721

Chatterjee, R., Doerfler, P., Orgad, H., Havron, S., Palmer, J., Freed, D., . . . Ristenpart, T. (2018). The Spyware Used in Intimate Partner Violence. *Symposium on Security and Privacy* (lk 441-458). San Francisco: IEEE. doi:10.1109/SP.2018.00061

Chivers, W. (07. 09 2019. a.). Resisting Digital Surveillance Reform: The Arguments and Tactics of Communications Service Providers. *Surveillance & Society, 17*(3/4), 517-532. doi:https://doi.org/10.24908/ss.v17i3/4.10836

Duke, S. A. (07. 09 2019. a.). Database-Driven Empowering Surveillance: Definition and Assessment of Effectiveness. *Surveillance & Society, 17*(3/4), 499-516. doi:https://doi.org/10.24908/ss.v17i3/4.10877

Eesti Vabariigi põhiseadus. (28. 06 1992. a.). Allikas: Riigi Teataja: https://www.riigiteataja.ee/akt/633949?leiaKehtiv

EKI. (06. 11 2019. a.). *Eesti Keele Instituudi inglise-eesti sõnastik.* Allikas: http://portaal.eki.ee/dict/ies/

EKI. (22. 03 2020. a.). Allikas: Sõnaveeb, EKI ühendsõnastik 2020: https://sonaveeb.ee/search/unif/dlall/dsall/detail/luurama/1

Eljas-Taal, K., Veerpalu, A., & Romanainen, J. (2017). Kas andmetest kujuneb uus varaklass? *Pikksilm*, 13-24. Kasutamise kuupäev: 01. 11 2019. a., allikas https://www.riigikogu.ee/wpcms/wp-content/uploads/2017/11/02.06.Pikksilm_2-Kas-andmetest-kujuneb-uus-varaklass.pdf

Eterovic-Soric, B., Choo, K.-K. R., Ashman, H., & Mubarak, S. (2017). Stalking the stalkers – detecting anddeterring stalking behaviours using technology: A review. *Compuers & Security*, 278-289. Kasutamise kuupäev: 25. 08 2019. a., allikas https://www.academia.edu/34373172/Stalking_the_stalkers_detecting_and_deterring_stalking_behaviours_using_technology_A_review

Euroopa Parlament; Euroopa Liidu Nõukogu. (2016). *EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS (EL) 2016/679.* Kasutamise kuupäev: 29. 08 2019. a., allikas EUR-Lex: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32016R0679

Federal Trade Commission. (03 2005. a.). Monitoring Software on Your PC:Spyware, Adware, and Other Software. Allikas: https://www.ftc.gov/sites/default/files/documents/reports/spyware-workshop-monitoring-software-your-personal-computer-spyware-adware-and-other-software-report/050307spywarerpt.pdf

Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., & Dell, N. (2018). "A Stalker's Paradise":How Intimate Partner Abusers Exploit Technology. *The 2018 CHI Conference*, (lk 1-13). Montreal QC, Canada. doi:10.1145/3173574.3174241

Freienthal, T.-A. (2018). "Netipervertide" kuvand noorte seas: Eesti gümnasistide kogemused ja hinnangud. Allikas: http://dspace.ut.ee/handle/10062/60644?show=full

Friedewald, M., Finn, R. L., & Wright, D. (2013). Seven Types of Privacy. rmt: *European Data Protection: Coming of Age* (lk 3-32). Springer. doi:10.1007/978-94-007-5170-5_1

Gabriels, K. (2016). 'I keep a close watch on this child of mine': a moral critique of other-tracking apps. *Ethics and Information Technology, 18*(3), 175-184. doi:https://doi-org.ezproxy.utlib.ut.ee/10.1007/s10676-016-9405-1

GAO. (2016). *SMARTPHONE DATA: Information and Issues Regarding Surreptitious Tracking Apps That Can Facilitate Stalking.* U.S. Government Accountability Office. Kasutamise kuupäev: 26. 08 2019. a., allikas https://www.gao.gov/assets/680/676738.pdf

Garrie, D. B., Blakley, A. F., & Armstrong, M. J. (2007). The Legal Status of Spyware. *The Federal Communication Law Journal, 59*, 165-169. Allikas: http://www.fclj.org/wp-content/uploads/2013/01/11-GarrieFINAL.pdf

Gillman, J. (30. 05 2018. a.). *How to Install Cell Phone Spy Software.* Kasutamise kuupäev: 28. 08 2019. a., allikas BestPhoneSpy: https://www.bestphonespy.com/how-to-install-cell-phone-spy-software/

Gillman, J. (19. 08 2019. a.). *How Does Cell Phone Spy Software Work?* Kasutamise kuupäev: 25. 08 2019. a., allikas BestPhoneSpy: https://www.bestphonespy.com/how-does-cell-phone-spy-software-work/

Google Trends. (2019). Kasutamise kuupäev: 21. 09 2019. a., allikas https://trends.google.com/trends/explore?q=%2Fm%2F01117_ww,flexispy,mobile%20spy,xnspy,hoverwatch

Harkin, D., Molnar, A., & Vowles, E. (28. 01 2019. a.). The commodification of mobile phone surveillance: An analysis of the consumer spyware industry. *Crime, Media, Culture*. doi:10.1177/1741659018820562

Helberg, K. (2018). *Laste jälgimine erinevate äppide kaudu ning sellega seonduvad probleemid ja võimalused.* Lõputöö, Tartu Ülikool, Sotsiaalteaduste valdkond, Ühiskonnateaduste instituut, Infokorralduse õppekava, Tartu. Allikas: https://dspace.ut.ee/bitstream/handle/10062/60438/helberg_karl_2018.pdf?sequence=1&isAllowed=y

Heldna, E. (2016). Juridica. *Julgeolekuasutuste kogutud informatsiooni kasutamine kriminaalmenetluses ja jagamine uurimisasutustega*(10), 718-726. Allikas: https://www.juridica.ee/article.php?uri=2016_10_julgeolekuasutuste_kogutud_informatsiooni_kasutamine_kriminaalmenetluses_ja_jagamine_uurimis

Highster Mobile. (2019). Kasutamise kuupäev: 24. 08 2019. a., allikas Highster Mobile kodulehekülg: https://www.highstermobi.com/

Hillep, P., & Pärnamets, R. (2020). *Laste ja noorte seksuaalse väärkohtlemise hoiakute ja kogemuste uuring*. Justiitsministeerium. Kasutamise kuupäev: 2020, allikas https://www.just.ee/sites/www.just.ee/files/laste_ja_noorte_seksuaalse_vaarkohtlemise_uuring_2020_euk.pdf

Hoverwatch. (2019). Kasutamise kuupäev: 24. 08 2019. a., allikas Hoverwatch koduleheküIg: https://www.hoverwatch.com/

Hoverwatch. (2020). Allikas: Hoverwatch koduleht: www.hoverwatch.com

ISO. (2018). *ISO/IEC 27032:2012 Information technology -- Security techniques -- Guidelines for cybersecurity*. Kasutamise kuupäev: 23. 08 2019. a., allikas ISO.org: https://www.iso.org/standard/44375.html

Jones, K. (04. 05 2020. a.). The COVID-19 Impact on App Popularity. *Visual Capitalist*. Kasutamise kuupäev: 20. 05 2020. a., allikas https://www.visualcapitalist.com/covid-19-impact-on-app-popularity/

Julgeolekuasutuste seadus. (15. 03 2019. a.). Tallinn: Riigi Teataja. Kasutamise kuupäev: 11. 04 2019. a., allikas https://www.riigiteataja.ee/akt/113032019067?leiaKehtiv

Karistusseadustik. (31. 07 2019. a.). Tallinn: Riigi Teataja. Kasutamise kuupäev: 26. 08 2019. a., allikas https://www.riigiteataja.ee/akt/119032019030?leiaKehtiv

Kido, J. (24. 09 2017. a.). This Mobile Monitoring User Cleverly Uncovers a Cheating Boyfriend. XNSPY Official Blog. Kasutamise kuupäev: 13. 03 2020. a., allikas https://xnspy.com/blog/this-mobile-monitoring-user-cleverly-uncovers-a-cheating-boyfriend.html?fbclid=IwAR2oHfFF0-QajChuSjeoCEidZ5l4JjoX3dHj5L5sKYoESwMs1iORjrowPNs

Kriminaalmenetluse seadustik. (15. 03 2019. a.). Tallinn: Riigi Teataja. Kasutamise kuupäev: 21. 05 2019. a., allikas https://www.riigiteataja.ee/akt/113032019007?leiaKehtiv

Kukrus, A. (2004). Küberkuritegevuse tõkestamine infoühiskonnas. *Riigikogu Toimetised*, 101-109. Kasutamise kuupäev: 26. 08 2019. a., allikas https://rito.riigikogu.ee/wordpress/wp-content/uploads/2016/04/RiTo-9.pdf

Laos, S., & Sepp, H. (2017). *Paragrahv 43*. Allikas: Põhiseadus.ee: https://www.pohiseadus.ee/index.php?sid=1&ptid=48&p=43

Lexico. (2019). *British & World English*. Kasutamise kuupäev: 29. 08 2019. a., allikas Lexico.com: https://www.lexico.com/en/definition/privacy

Light, B. (2014). *Disconnecting with social networking sites.* United Kingdom: Palgrave Macmillan. doi:10.1057/9781137022479

Light, B., & McGrath, K. (2010). Ethics and social networking sites: A disclosive analysis of Facebook. *Information Technology & People, 23*(4), 290-311. doi:10.1108/09593841011087770

Light, B., Burgess, J., & Duguay, S. (01. 03 2018. a.). The walkthrough method: An approach to the study. *New Media & Society, 20*(3), 881-900. doi:https://doi.org/10.1177/1461444816675438

Light, B., Fletcher, G., & Adam, A. (2008). Gay men, Gaydar and the commodification of difference. *Information Technology & People, 21*(3), 300-314. Allikas: https://www.emerald.com/insight/content/doi/10.1108/09593840810896046/full/html

Lyon, D. (2007). *Surveillance Studies: An Overview.* Cambridge: Polity Press.

Lyon, D. (2018). *The Culture of Surveillance.* Cambridge: Polity Press.

Mandel, T. (2020). *Rakendused telefonikasutaja salajaseks jälgimiseks.* Seminaritöö, Tartu Ülikool, Sotsiaalteaduste valdkond, Ühiskonnateaduste instituut, Infokorralduse õppekava.

Marx, G. T., & Steeves, V. (06 2010. a.). From the Beginning: Children as Subjects and Agents of Surveillance. *Surveillance & Society, 7*(3), lk 192-230. doi:10.24908/ss.v7i3/4.4152

Matthews, E. D. (2017). Incoming: The Weakest Link in Security Chain Is People, Not Technology. *SIGNAL*. Kasutamise kuupäev: 11. 04 2020. a., allikas https://www.afcea.org/content/Article-incoming-weakest-link-security-chain-people-not-technology

McCullagh, K. (2005). Identity information: the tension between privacy and the societal benefits associated with biometric database surveillance. *20th BILETA Conference: Over-Commoditised; Over-Centralised; Over-Observed: the New Digital Legal World?* Belfast. Allikas: https://www.bileta.org.uk/wp-content/uploads/Identity-Information-The-Tension-Between-Privacy-and-the-Societal-Benefits-Associated-With-Biometric-Database-Surveillance.pdf

McQuade, S. C., & Danielson, P. (22. 10 2019. a.). *Monitoring and Surveillance.* Kasutamise kuupäev: 06. 11 2019. a., allikas Encyclopedia.com: https://www.encyclopedia.com/science/encyclopedias-almanacs-transcripts-and-maps/monitoring-and-surveillance

Mercaldo, F., & Saracino, A. (2018). Not so Crisp, Malware! Fuzzy Classification of Android Malware Classes. *International Conference on Fuzzy Systems* (lk 1). Rio de Janeiro: IEEE. doi:10.1109/FUZZ-IEEE.2018.8491521

MI5. (2019). *GATHERING INTELLIGENCE*. Kasutamise kuupäev: 08. 11 2019. a., allikas MI5 koduleht: https://www.mi5.gov.uk/gathering-intelligence

Mitnick, K. D. (2003). Are You the Weak Link? *Harvard Business Review*. Kasutamise kuupäev: 11. 04 2020. a., allikas https://hbr.org/2003/04/are-you-the-weak-link

Mobile Spy. (2020). Allikas: Mobile Spy koduleht: http://www.mobile-spy.com/index.html

Moore, A. (05. 09 2008. a.). Defining Privacy. *Journal of Social Philosophy, 3*(39), 411–428. doi: https://doi.org/10.1111/j.1467-9833.2008.00433.x

mSpy. (2019). Kasutamise kuupäev: 24. 08 2019. a., allikas mSpy koduleheküIg: https://www.mspy.com/

mSpy. (2020). Allikas: mSpy koduleheküIg: www.mspy.com

Murumaa-Mengel, M., Pruulmann-Vengerfeld, P., & Laas-Mikko, K. (2014). Privaatsusõigus inimõigusena ja igapäevatehnoloogiad. Kasutamise kuupäev: 29. 08 2019. a., allikas https://www.humanrightsestonia.ee/wp/wp-content/uploads/2014/11/EST-Uuringu-III-osa-Uuringu-teoreetilised-ja-empiirilised-l%C3%A4htealused.pdf

Nolan, C. (02. 05 2018. a.). Data Surveillance, Monitoring, and Spying: Personal Privacy in a Data-Gathering World. Kasutamise kuupäev: 06. 11 2019. a., allikas https://www.dataversity.net/data-surveillance-monitoring-spying-personal-privacy-data-gathering-world/#

Packham, C. (27. 04 2020. a.). More than two million Australians download COVID-19 app, testing expands. *Reuters*. Kasutamise kuupäev: 20. 05 2020. a., allikas https://www.reuters.com/article/us-health-coronavirus-australia/more-than-two-million-australians-download-covid-19-app-testing-expands-idUSKCN22902G

Papacharissi, Z. (2009). The virtual geographies of social networks: a comparative analysis of Facebook, LinkedIn and ASmallWorld. *11*(1-2), 199-220. doi:https://doi.org/10.1177/1461444808099577

Penwarden, R. (2014). The Rise Of The Smartphone. Allikas: fluidsurveys.com: https://fluidsurveys.com/wp-content/uploads/2014/11/The-Rise-Of-The-Smartphone.pdf

Periñán, B. (2012). The Origin of Privacy as a Legal Value: A Reflection on Roman and English Law. *American Journal of Legal History*, *52*(2), 183–201. doi:https://doi.org/10.1093/ajlh/52.2.183

Prii, R. (04. 09 2018. a.). *Mis on Geofence ja miks on see muutumas uueks trendiks?* Kasutamise kuupäev: 01. 10 2019. a., allikas Begin.ee: https://begin.ee/blog/geofence/

Regan, P. M. (2000). *Legislating Privacy: Technology, Social Values, and Public Policy.* Universty of North Carolina Press. Allikas: https://books.google.ee/books?id=KkPqCQAAQBAJ&printsec=frontcover&hl=et#v=onepage&q&f=false

Regio. (2019). *Asukohapõhised lahendused*. Kasutamise kuupäev: 30. 09 2019. a., allikas Regio: http://www.regio.ee/?op=body&id=259

Riigi Teataja. (2015). Kohtulahendite liigitus. Kasutamise kuupäev: 26. 08 2019. a., allikas https://www.riigiteataja.ee/kohtulahendite_liigitus.html?jaotus=juur.206106663.206106667.206109430.206109495.206109502.206109503&kokkuvotted=false&jaotusedVaikimisiAvatud=

Rosen, J. (2004). The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age. Kasutamise kuupäev: 12. 01 2020. a., allikas http://www.antoniocasella.eu/nume/rosen_2004.pdf

Rössler, B. (2005). *The Value of Privacy.* Polity Press.

Saad, M. H., Serageldin, A., & Salama, G. I. (2015). Android spyware disease and medication. *Second International Conference on Information Security and Cyber Forensics* (lk 120). Cape Town: IEEE. doi:10.1109/InfoSec.2015.7435516

Saracino, A., Martinelli, F., Sgandurra, D., & Dini, G. (2018). MADAM: Effective and Efficient Behavior-based Android Malware Detection and Prevention. *IEEE Transactions on Dependable and Secure Computing, 15*(1), 83 - 97. doi:10.1109/TDSC.2016.2536605

Schneier, B. (21. 10 2013. a.). The Trajectories of Government and Corporate Surveillance. Kasutamise kuupäev: 24. 10 2019. a., allikas https://www.schneier.com/blog/archives/2013/10/the_trajectorie.html

Simpson, B. (2014). Tracking children, constructing fear: GPS and the manufacture of family safety. *Information & Communications Technology Law, 23*(3), 273-285. doi:http://dx.doi.org/10.1080/13600834.2014.970377

Solove, D. J. (2002). Conceptualizing Privacy. *California Law Review, 90*(4), lk 1087-1155. doi:ttps://doi.org/10.15779/Z382H8Q

Sootak, J. (2016). Karistusõiguse üldosa terminitest ehk Elu seaduse fassaadi taga. *Õiguskeel*, 1-16. Allikas: https://www.just.ee/sites/www.just.ee/files/jaan_sootak._karistusoiguse_uldosa_terminitest_ehk_elu_seaduse_fassaadi_taga.pdf

Spyera. (2019). Kasutamise kuupäev: 24. 08 2019. a., allikas Spyera koduleheküIg: https://spyera.com/

SpyFone. (2019). Kasutamise kuupäev: 24. 08 2019. a., allikas SpyFone koduleheküIg: https://www.spyfone.com

SpyMyFone. (2019). Kasutamise kuupäev: 24. 08 2019. a., allikas SpyMyFone koduleheküIg: https://www.spymyfone.com/

Spyzie. (2019). Kasutamise kuupäev: 24. 08 2019. a., allikas Spyzie koduleheküIg: https://www.spyzie.com/

Sukk, M., & Soo, K. (2018). *EU Kids Online'i Eesti 2018. aasta uuringu esialgsed tulemused.* Tartu Ülikool, Ühiskonnateaduste instituut, Tartu. Kasutamise kuupäev: 01. 04 2020. a., allikas https://sisu.ut.ee/sites/default/files/euko/files/eu_kids_online_eesti_2018_raport.pdf

Zaia, M. (07. 09 2019. a.). Exploring Consciousness: The Online Community's Understanding of Mobile Technology Surveillance. *Surveillance & Society, 17*(3/4), 533-549. doi:https://doi.org/10.24908/ss.v17i3/4.11934

Tanriverdi, H. (2015). Dein Handy weiß alles über dich. *Süddeutsche Zeitung*. Kasutamise kuupäev: 02. 09 2019. a., allikas https://www.sueddeutsche.de/digital/verschluesselungs-experte-bruce-schneier-dein-handy-weiss-alles-ueber-dich-1.2397418

Tigasson, K.-R. (05. 12 2018. a.). Helikoptervanemad: emad ja isad, kelle hoolitsus lapsi lämmatab. *Eesti Ekspress*. Kasutamise kuupäev: 23. 05 2020. a., allikas https://ekspress.delfi.ee/kuum/helikoptervanemad-emad-ja-isad-kelle-hoolitsus-lapsi-lammatab?id=84638555

UNODC. (2009). Current practices in electronic surveillance in the investigation of serious and organized crime. New York. Kasutamise kuupäev: 06. 11 2019. a., allikas https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf

van den Hoven, J., Blaauw, M., Pieters, W., & Warnier, M. (2018). *Privacy and Information Technology*. Metaphysics Research Lab, Stanford University. Kasutamise kuupäev: 29. 08 2019. a., allikas https://plato.stanford.edu/archives/sum2018/entries/it-privacy/

Veebikoda. (2017). *Otsingumootoritele optimeerimine (SEO) – põhjalik selgitus.* Kasutamise kuupäev: 15. 09 2019. a., allikas Veebikoda: https://veebikoda.com/otsingumootoritele-optimeerimine/

Weston, M. (2015). Wearable surveillance – a step too far? *Strategic HR Review, 14*(6), 214-2019. doi:10.1108/SHR-09-2015-0072

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

Ünver, A. (2018). Politics of Digital Surveillance, National Security and Privacy. Kasutamise kuupäev: 06. 11 2019. a., allikas https://edam.org.tr/en/politics-of-digital-surveillance-national-security-and-privacy/

XNSPY. (2019). Kasutamise kuupäev: 24. 08 2019. a., allikas XNSPY koduleheküIg: https://xnspy.com/

XNSPY. (2020). Allikas: XNSPY koduleheküIg: www.xnspy.com

Young, N. (2012). *The Virtual Self: How Our Digital Lives Are Altering the World Around Us.* Toronto: McClelland & Stewart.

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, **Tõnu Mandel**,

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose
   „Telefonikasutaja salajaseks jälgimiseks mõeldud rakenduste sihtrühmad ja nendele suunatud sõnumid“,
   mille juhendaja on Maris Männiste, MA,

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

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

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

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

Tõnu Mandel
25.05.2020