TARTU ÜLIKOOL

Sotsiaalteaduste valdkond

Ühiskonnateaduste instituut

Infokorralduse õppekava

Liisa Asso

Põhikooliealiste arusaamad privaatsusest online mängukeskkondades

Lõputöö

Juhendaja: Maris Männiste, PhD

Tartu 2022

SISUKORD

SISSEJUHATUS

Lapsed veedavad päevas keskmiselt kaks kuni kolm tundi digitaalses maailmas, kuid uuringute järgi kasvab see aeg iga aastaga (Smahel jt, 2020). Lastele on internetis toimetamiseks jäänud üsna vabad käed, kuna ainult 14% 9-12-aastaste laste vanematest kontrollivad enda laste tegevusi võrgus (Livingstone jt, 2018). Tartu Ülikooli teadlaste poolt läbi viidud uuring tõi välja, et kui vaadata üldiselt mida lapsed internetis teevad, siis esikohal oli videote vaatamine, muusika kuulamine ja online mängude mängimine (Sukk ja Soo, 2018). Ka 2021.aastal läbi viidud ySKILLS'i küsitlusuuring leidis, et online mängud on laste seas väga populaarsed ning lausa 63% lastest mängib neid internetis igapäevaselt (Kalmus jt, 2022).

Online mängude (keskkond, kus mängijad on võrgu kaudu ühenduses) populaarsus on aasta-aastalt kasvanud (Shi jt, 2019). Online mänge on võimalik mängida läbi erinevate mängukeskkondade ning seadmete, nii üksi, kui mitmekesi. Online mängud on tihti realistliku ja keeruka graafikaga, seetõttu on nad kasutaja jaoks atraktiivsed ning tänu sellele üha rohkem kasutajaid nendest lummatud ongi (Sanders jt, 2010). Kuna nõudlus on suur ja olenemata vanusest meeldivad virtuaalmängud kõigile (Russell jt, 2018), siis on videomängude turg saanud maailma juhtivamaks meelelahutustööstuseks (Kröger jt, 2021). Suurimaks sihtrühmaks videomängude mängimisel on lapsed (Russel jt, 2018), neil on võimalik virtuaalmaailmas luua erinevaid graafilisi kujutisi, mida saab kasutada teistega suhtlemiseks ning mängimiseks nii, et teine kasutaja tema päris identiteeti ei tea (Chen, 2015). Mängides ei pea kasutaja esinema enda nime ja näoga vaid saab luua endale sobiva avatari (Williams jt, 2019) ning seeläbi on lastel võimalus käituda viisil ja öelda asju, mida tavapäraselt ei teeks ega ütleks (Makarova ja Makarova, 2019).

Online mängud asuvad erinevatel tehnilistel mänguplatvormidel. Mõned mänguplatvormid on nii suured, et päevas külastavad neid miljonid kasutajad. See annab mänguplatvormidele võimaluse koguda suurel hulgal mängijate andmeid, näiteks andmeid kasutaja asukoha, biomeetriliste andmete, emotsioonide, oskuste, huvide, tarbimisharjumuste, isikuomaduste, makseandmete ning isegi privaatselt edastatud sõnumite kohta (Russel jt, 2018; Kröger jt, 2021). Tihti analüüsivad

mängutootjad ka mängijate käitumist ja sellest saadud andmeid (Rubio-Manzano ja Trivino, 2016), nendeks andmeteks võivad sõltuvalt mängu tüübist olla näiteks hiireklikid, südame löögisagedus ja žestituvastus (Russel jt, 2018; Kröger jt, 2021). Mainitud andmeid saab kasutada mängude kohandamiseks, vigade avastamiseks, pettuste tuvastamiseks, kuid neid saab kasutada ka vähem õilsamate eesmärkide saavutamiseks, näiteks teadmisi mängija psühholoogiliste omaduste ja haavatavuste kohta saab ära kasutada selleks, et mõjutada mängijat nii, et ta ostaks tasulist sisu (Macenaite ja Kosta, 2017; Yannakakis ja Togelius, 2018; Kröger jt, 2021). Tasulise sisu soetamise juures võib tekkida aga oht, et makseandmed võivad sattuda valedesse kätesse ning see võib kaasa tuua suuri rahalisi kaotusi (Smahel jt, 2020). Eriti haavatavas seisus on lapsed, keda on lihtsam mõjutada ja kes tavaliselt ei süvene sellesse, mis peitub reklaami taga.

Eelnevale lisaks tuleb välja tuua, et lapsed jätavad online mänge mängides mänguplatvormidele suurel hulgal enda kohta käivat teavet. Mänguplatvormidele maha jäänud teave võib olla väga detailne ning seetõttu on oht, et laste andmeid võidakse kuritarvitada identiteedivarguse läbi (Martinovic jt, 2014), või näiteks jälgitakse last tema enda teadmata (Smahel jt, 2020). Juhul, kui lapsed sisestavad enda isiklike andmeid mänguplatvormidele võib juhtuda, et need lekivad ning satuvad kellegi kätte, kellel pole head kavatsused (Smahel jt, 2020). Need lekkinud andmed võivad lapsi tulevikus mõjutada (Berman ja Albright, 2017), online suhtlus salvestatakse, see on püsiv, otsitav ning kopeeritav, seega võib piinlik võrgusuhtlus välja tulla alles aastate pärast (Vallejo jt, 2021). Seega varitsevad mänguplatvormidel lapsi erinevad ohud, millest nad ei pruugi teadlikud olla.

Laste isiklikke andmeid kasutatakse ärilistel eesmärkidel, kuna lapsed ei saa aru, mida tähendab isikuandmete töötlemine ning kui laps on huvitatud mõne mängu mängimisest, siis ei süvene nad oluliselt sellesse, millele nad nõusoleku annavad (Stoilova jt, 2020). Seega „kauplevad“ lapsed mänguplatvormidel enese teadmata oma isikuandmetega midagi ise vastu saamata (Russell jt, 2018). Probleemiks on ka asjaolu, et mängude juures on hoiatused, millisele vanusegrupile need sobivad ning mängutootjad toovad välja, et mängus võib esineda vägivalda, kuid puuduvad hoiatused privaatsusega seotud riskide kohta (Martinovic jt, 2014). Mängude osas puudub samasugune regulatsioon nagu on kehtestatud teistele digiteenustele, näiteks otsingumootoritele, tutvumisrakendustele või sotsiaalmeedia platvormidele (Kröger jt, 2021). Lisaks on probleemiks ka see, et osadel mänguplatvormidel puuduvad vanusepiirangud (Kröger jt, 2021). Kui mänguplatvorm on vanusepiirangu ka kehtestanud siis paljud lapsed lähevad sellest piirangust mööda (Martinovic jt, 2014). Tihti esinetakse mänguplatvormil vanemana ning sisestatakse selline

vanus, mis mänguplatvormile ligipääsu võimaldab (Martinovic jt, 2014). Võib eeldada, et kui lapsed oleksid mänguplatvormidel olevatest ohtudest teadlikud, siis ei sooviks nad piirangutest mööda hiilida.

Eestis on varem uuritud laste käitumist sotsiaalmeedias ning kuidas sealne keskkond võiks mõjutada laste privaatsust ja turvalisust (Lorenz jt, 2017). Vaher-Torni (2019) uuris enda magistritöös seda, millised seaduslikud õigused on lastel enda privaatsusele, kui nad kasutavad sotsiaalmeedia platvorme. Eesti laste internetikasutamisega seonduvat privaatsust on uuritud ka 2020. aastal, kus leiti, et sotsiaalmeedias toimetades on paljud lapsed erinevate privaatsusriskidega kokku puutunud (Smahel jt, 2020). Privaatsuse aspekti on puudutatud ka 2018. aasta uuringus, kus kirjeldatakse sotsiaalmeedia riske laste privaatsusele ning vaadeldakse laste privaatsusõigust kontekstis, kus lapsevanem last läbi erinevate rakenduste jälgib (Anniste jt, 2018).

Seega on tähelepanu pööratud sellele, mida lapsed teevad sotsiaalmeedias üldiselt, kuid online mängukeskkondade kasutamise mõju laste privaatsusele ei ole laialdaselt käsitletud. Maailmas seevastu on probleemile tähelepanu pööratud. Näiteks on uuritud, kuidas mänguplatvormid peavad kinni eraelu puutumatuse reeglitest ja privaatsusest ning kuidas tehnoloogia võib mõjutada lapsmängijaid (Russel jt, 2018). Probleemile on tähelepanu pööratud ka 2021. aastal läbi viidud uuringus, mis käsitles mänguplatvormide privaatsusaspekte ning seda, et platvormidel toimuv andmete kogumine on seadustega reguleerimata (Kröger jt, 2021).

Eelnevast lähtuvalt oli töö eesmärgiks teada saada, kui teadlikud on teise kooliastme õpilased ohtudest privaatsusele, kui nad mängivad online keskkondades. Lisaks oli soov teada saada, milliseid meetmeid võtavad lapsed ise kasutusele, et oma privaatsust mänguplatvormidel kaitsta. Olukorra kaardistamine on oluline, et lapsevanemad ja haridusasutused oskaksid vajadusel rohkem tähelepanu suunata ennetustööle ja laste teadlikkuse tõstmisele.

Järgnev töö koosneb neljast osast. Esimeses osas kirjeldan andmestumise mõju isikuandmete kogumisele, kasutamisele ning säilitamisele, selgitan privaatsusega seonduvat ning seda, miks on oluline privaatsust kaitsta. Peatüki lõpus toon välja uurimisprobleemi ning püstitatud uurimisküsimused. Teises osas tutvustan meetodit ja valimit. Kirjeldan seda, kuidas valim moodustus, kuidas kogusin andmeid ja kuidas neid andmeid analüüsisin. Kolmandas osas toon välja tulemused ning neljandas osas toon välja olulisemad järeldused, mis tuginevad teooriaosale ning tulemustele.

Selle töö valmimise juures on mulle suureks toeks olnud minu juhendaja Maris Männiste, keda soovin tänada sujuva koostöö, toetuse ning abi eest. Lisaks soovin tänada intervjueeritavaid, kelle panus töö valmimisse oli väga oluline. Ning lisaks tänaksin enda perekonda kannatlikkuse eest, kuna järgnev töö valmis koos veedetava aja arvelt.

2 TEOREETILISED JA EMPIIRILISED LÄHTEKOHAD

Teooria peatükis kirjeldan, kuidas mõjutab andmestumine isikuandmeid ning nende kogumist. Selgitan privaatsuse olemust ning sellega seonduvaid mõisteid, lisaks kirjeldan, kuidas lapsed privaatsuse mõistest aru saavad. Peatüki lõpetuseks toon välja põhjused, miks on oluline privaatsust kaitsta ning millised võivad olla tagajärjed, kui seda ei tee.

2.1 Andmestumise mõju isikuandmete kogumisele, kasutamisele ning säilitamisele

Virtuaalmängud on kasvav trend, online mänge ei kasutata mitte ainult lõbustuse eesmärgil, vaid ka õppimiseks (Yannakakis ja Togelius, 2018), seega võivad online mängud lapsi ümbritseda nii koolis, kui ka kodus. Online mänguks nimetatakse mängu, mis hõlmab võrgu kaudu ühendatud mängijaid, võrk võib olla traadiga (traadiga ühendus saadetakse enamasti kaabliga) või traadita (traadita ühendus saadakse enamasti läbi Bluetoothi, WiFi või mobiilse andmeside) (Chen, 2015). Online videomängud sisaldavad erinevaid funktsioone. Ühe sellise funktsioonina saab välja tuua mängusisese vestlusakna, mis hõlbustab või aitab mängijatel omavahel sotsiaalselt suhelda (Arbeau, 2020). Mängud asuvad erinevatel tehnilistel mänguplatvormidel. Mänguplatvorm on süsteem, mis on spetsiaalselt kirjutatud mängutarkvara käivitamiseks (Law Insider, i.a). Mänguplatvormid saavad olla näiteks mobiilseadmetes, arvutites, mängukonsoolides ning need jagunevad veebipõhisteks ning veebist sõltumatuteks (Arbeau, 2020). Mänguplatvormi osad lahendused on võimelised mängutoiminguid tootjale edastama ning edastatud teave ei sõltu kasutaja asukohast, kasutatavast seadmest ja ühenduse tüübist (Chen, 2015).

Erinevad mänguplatvormid salvestavad, hävitavad ja töötlevad kasutajate isikuandmeid (Li jt, 2019). Isikuandmeteks loetakse andmeid, mille järgi on võimalik inimene tuvastada ning

isikuandmete töötlemiseks toiminguid isikuandmetega (Justiitsministeerium, i.a). Isikuandmed liigituvad (Andmekaitse Inspektsiooni…, 2019):

- tavalisteks isikuandmeteks - andmed, mille kaudu on võimalik inimest tuvastada (näiteks nimi, asukohateave, isikukood);
- tundlikeks isikuandmeteks - andmed, mille avaldamine võib inimese elu ja tervise ohtu seada, või mille kaudu on võimalik inimese identiteeti varastada (näiteks krediitkaardi andmed, kriminaal- ja väärteomenetlusega seoses kogutud andmed, asukohatuvastuse andmed);
- eriliiki isikuandmeteks - isikuandmed, mille kaudu on võimalik tuvastada inimese rassilist või etnilist päritolu, tema poliitilisi vaateid ning tema tuvastamiseks kasutatavaid biomeetrilisi andmeid.

Eristatakse ka digitaalseid isikuandmeid, mida saab omakorda liigitada järgnevalt (Pangrazio ja Selwyn, 2019):

- andmed, mida kasutajad seadmetele/süsteemidele annavad - näiteks teave enesejälgimise kohta, sotsiaalmeedia andmed, e-kirjad ja videod;
- andmed (nimetatakse ka suurandmeteks), mida seadmed/süsteemid kasutajatelt hangivad- andmed, mida kogutakse seadmekasutusest, veebiotsingutest, need andmed edastatakse näiteks mänguplatvormide tarkvaraarenduseks ja andmete analüüsiks;
- andmed, mida seadmed/süsteemid kasutajate nimel töötlevad- eesmärgiks on muuta isik tuvastatavaks, kasutatakse pigem süsteemiprotsessides, üksikud kasutajad nendega tavaliselt kokku ei puutu.

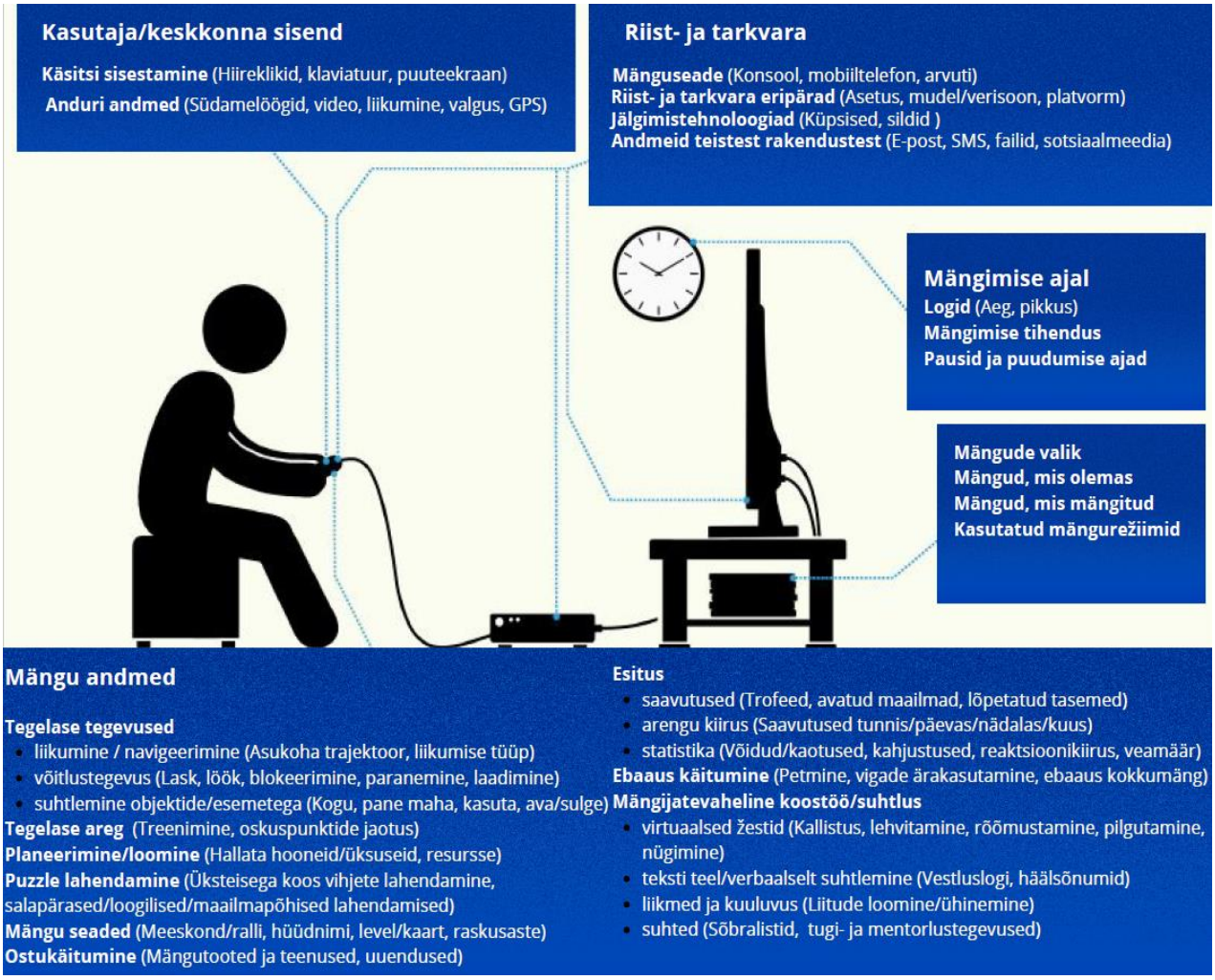
Mõiste suurandmed tuleneb sellest, et iga päev toodetakse inimeste poolt suurtes kogustes andmeid, näiteks tehakse Google kaudu päevas umbes 1 miljardit päringut, Facebookis üle 800 miljoni uuenduse ja Youtube'is vaadatakse päevas üle 4 miljardi video (Abdel-Basset jt, 2018). Nende külastuste ja päringutega jätavad kasutajad endast maha andmejäljed, mida nimetatakse ka „digitaalseks jalajäljeks“ (Hepp ja Breiter, 2018; Pangrazio ja Selwyn, 2019). Arusaam, kuidas andmevood muutuvad digitaalseks jalajäljeks on lastele, nagu ka enamikule täiskasvanutele liiga keeruline (Muhammad jt, 2017; Vervier jt, 2017; Stoilova jt, 2020).

Tänapäeval on üsna võimatu endast digitaalseid jälgi mitte maha jätta, seega on andmestumise mõju meile igapäevane (Masso jt, 2019). Andmestumine tähendab seega, et meie igapäevategevused jätavad läbi infotehnoloogiliste vahendite maha suurel hulgal andmeid (Harrik, 2021). Inimtegevuse käigus loodud andmed analüüsitakse, luuakse informatsiooniks ning need andmed saavad endale uue väärtuse (Masso jt, 2019). Andmestumise kontekstis räägitakse aina enam ka lapsepõlve andmestumisest, mis tähendab, et lastest luuakse digitaalsed jalajäljed isegi ennem nende sündimist (näiteks jagades ultrahelivõtet sotsiaalmeedias) (Siibak, 2019; Stoilova jt, 2020). Tihti postitavad lapsevanemad lastest pilte ning kasutavad laste jälgimiseks erinevaid rakendusi ja tehnikalahendusi, et olla kindel, et lapsega on kõik korras, kuid nende kasutamise juures on oht, et keegi ei tea, mis saab nendest kogutud andmetest edasi ja kuidas ja kes neid andmeid kasutab (Saar jt, 2019). Kui lapsed suuremaks kasvavad hakkavad nad ise endast andmejälgi maha jätma, näiteks läbi online mängude ja sotsiaalmeedia (Mascheroni, 2020).

Kuna andmehulgad võivad olla väga suured, siis otsitakse alati paremaid ja kiiremaid võimalusi nende töötlemiseks, vahel kasutatakse selleks ka tehisintellektide abi (Yannakakis ja Togelius, 2018). Tehisintellekti on määratletud, kui süsteemi võimet õigesti toimida ning väliseid andmeid tõlgendada, nendest andmetest õppida ja neid teadmisi selleks kasutada, et saavutada konkreetseid eesmärke ja ülesandeid (Kaplan ja Haenlein, 2019). Tehisintellekti abil on loodud mänguplatvormidel näiteks mittemängijatest tegelaskujud, kellega mängijal võidelda tuleb (Yannakakis ja Togelius, 2018). Tehisintellektidele lisaks kasutatakse andmete töötlemiseks ja kättesaamiseks ka algoritme, mis on juhiste komplektid ülesande täitmiseks, mis toodavad antud sisendist väljundit (Doneda ja Almeida, 2016). Algoritmid toimivad põhimõttel, et alguses leitakse andmete vahel seosed ning seejärel toob süsteem andmete analüüsimise käigus välja asjakohased kriteeriumid, mida saab vajadusel töödelda (Andmekaitse Inspektsioon, 2017). Nimetatud lahendused hoiavad mängutootjate aega ja ressursse kokku, kuna andmete kiireks ja tõhusamaks töötlemiseks kasutatakse tehnoloogiliste vahendite abi.

Mõningad mänguplatvormid annavad kogutud isikuandmetele ligipääsu ka kolmandate osapoolte rakendustele (Russell jt, 2018; Kröger jt, 2021). Näiteks mänguplatvorm Nintendo 3DS toetab oma süsteemis teisi rakendusi, läbi mängkonsooli saab kasutaja Netflixi lehega tutvuda, platvorm aga annab Netflixile võimaluse kasutaja andmeid töödelda (Russell jt, 2018). See näide ilmestab seda, et tihti edastatakse reklaamplatvormidele ja seotud partneritele suurel hulgal isiklikke ja tundlikke andmeid (Sanders, 2016; Russel jt, 2018). Kuna võrguvideomängud võivad toota palju rohkem andmeid, kui teised interneti põhised rakendused, teenused ja sotsiaalmeediaplatvormid,

siis on loogiline, et kolmandad osapooled soovivad mänguplatvormidega koostööd teha ja nendest andmetest osa saada (Kröger jt, 2021). Mänguplatvormidel kogutavatest andmetest annab ülevaate joonis 1, kus on välja toodud detailsemalt, milliseid andmeid mänguplatvormid koguvad ning mis tegurid võivad andmete kogumist mõjutada. Näiteks kogutakse mängimise ajal mängude logisid ning mängija tegevusi mängu ajal (hiireklikid, saavutused, suhtlus).



Joonis 1. Andmetüüpide klassifikatsioon, mida videomängud tavaliselt koguvad (Allikas: Kröger jt, 2021:4 (allika põhjal minu poolt eesti keelde tõlgitud))

Kuna lapsed (eriti teismelised) on täiskasvanutega võrreldes emotsionaalsemad ja impulsiivsemad, siis ei pruugi nad teadvustada oma virtuaalkäitumise pikaajalisi tagajärgi (Macenaite ja Kosta, 2017). Näiteks mõistavad lapsed seda, kuidas nende tegevustest erinevatel saitidel ja mänguplatvormidel jääb maha jälg, kuid nad ei tea mis need maha jäänud andmed täpsemalt on ja kuhu need edasi liiguvad (Stoilova jt, 2020). Veebiturundajad kasutavad seda ära, nad koguvad

isikuandmeid ja nende andmete põhjal pakuvad lastele reklaame, mis on kohandatud laste individuaalse profiili ja käitumise järgi (Macenaite ja Kosta, 2017; Yannakakis ja Togelius, 2018). Just sellised personaalsed reklaamid on need, mis on laste jaoks huvipakkuvad ja ligitõmbavad.

On leitud, et lapsed suudavad mõista seda, kuidas toimub andmete jagamine siis, kui näiteks lapsevanem laeb temast pildi sotsiaalmeediasse, kuid neil on keerulisem mõista, kuidas toimub isikuandmete kogumine kaubanduslikus kontekstis (Stoilova jt, 2020). Et vältida laste isikuandmete väärkasutamist on näiteks sotsiaalmeedia platvormidel kehtestatud vanusepiirangud- Facebookil on miinimum vanuseks 13 aastat, WhatsAppil 16+, Twitteril 13+ (Livingstone, 2018), aga osadel mänguplatvormidel sellised vanusepiirangud puuduvad (Kröger jt, 2021). Kui ka vanusepiirangud on seatud, siis kipuvad noored tihti mängukeskkondades esinema vanemana, kui nad tegelikult on, nad teevad seda selleks, et ligi pääseda soovitud mängusaidile (Martinovic jt, 2014).

Eelneva põhjal saab välja tuua, et andmestumine on suur osa laste elust. Andmestumise tagajärjel jäävad lastest veebikeskkonda ja mänguplatvormidele maha suurel hulgal erinevaid andmeid. Andmete jagamine ja kogumine toimub läbi erinevate seadmete ning keskkondade ning tihti ei saa lapsed isegi aru, et endast andmejäljed maha jätavad. Probleemiks on ka see, et lastel on keeruline mõista, kuidas toimub andmete kogumine kaubanduslikul eesmärgil. Veebiturundajad kasutavad seda teadmatust ära ning kasutavad kogutud andmeid ärilistel eesmärkidel, näiteks pakkudes analüüsitud andmete põhjal kasutajatele tasulist sisu. Lisaks jagavad veebiturundajad kogutud andmeid ka kolmandate osapooltega.

2.2 Privaatsus online keskkondades

Tihti on laste jaoks üllatuseks, et erinevate platvormide külastamisel koguvad need külastajate (isiku)andmeid (Livingstone jt, 2019; Stoilova jt, 2020). Privaatsusena mõistetakse üksikisikute, rühmade või intitutsioonide õigust saada teavet selle osas, millist indiviidi kohta käivat informatsiooni kellegi teisega jagatakse (Stoilova jt, 2020). Lisaks on puudutatud isikul õigus teada kuidas, millal ja kui suures ulatuses seda informatsiooni kogutakse, säilitatakse ja kasutatakse (Murumaa-Mengel jt, 2014; Beke jt, 2018). Seega, kui ettevõtted soovivad austada tarbijate privaatsust, peaksid nad seda tegema läbipaistvalt ning selgitama, millist teavet nad

koguvad, kuidas nad seda säilitavad ja millistel eesmärkidel nad seda kasutada plaanivad (Beke jt, 2018). Lisaks peaks tarbijal olemas olema võimalus kontrollida enda kohta kogutud andmeid ning andmete kogumisest loobuda või keelduda (Beke jt, 2018). Andmete töötlemise põhimõtteid reguleerib Eestis isikuandmete kaitse üldmäärus (GDPR), milles on muuhulgas sätestatud, millised on isikuandmete töötlemise põhimõtted, kirjeldatakse kes on vastutav ja volitatud töötleja ning millised on andmesubjekti õigused (Isikuandmete…, 2016).

Enamik mänguplatvorme pakub oma teenust tasuta, kuid nende teenustele juurdepääsu võimaldamiseks peavad kasutajad nõustuma eelseadistatud tingimuste paketiga ja privaatsussätetega (Scneble jt, 2021). Privaatsussätted töötavad põhimõttel, et iga külastaja peab külastavale lehele andma nõusoleku selleks, kas ja kuidas tema isikuandmeid võib töödelda ning teistega jagada (Isikuandmete kaitse…, 2007). Privaatsussätetest peab andmete vastutav töötleja välja tooma andmete töötlemise eesmärgid, isikuandmete kirjelduse, mida töödeldakse, isikud, kellele isikuandmeid avaldatakse, tähtajad, kui kaua andmeid säilitatakse ning turvameetmed, kuidas andmeid kaitstakse (Andmekaitse Inspektsioon, 2019). On oluline, et inimene, kes privaatsussätteid ja kasutustingimusi kinnitab, saaks aru, mida organisatsioon tema andmetega teeb (Andmekaitse Inspektsioon, 2017). Nimetatud kasutustingimused ja privaatsussätted on sageli aga pikad ja kirjutatud keerulises õiguskeeles ja seega on paljudel raske aru saada, mida seal täpselt öelda soovitakse (Scneble jt, 2021). Seega, kui juba täiskasvanutel on keeruline mõista, mida kasutustingimused ja privaatsussätted täpselt endas sisaldavad, siis on see laste jaoks veelgi keerulisem.

Uuringutega on leitud, et kui laps külastab mõnda saiti ja seal palutakse neil kinnitada lehe kasutamiseks lehe tingimused, privaatsussätted, küpsised ja isikuandmete kogumise teave, siis ei pruugi nad teadlikud olla, et nende kinnitamine ei ole kohustuslik ja neid on võimalik muuta (Stoilova jt, 2020). Kui lapsed on ka teadlikud, et nimetatud tingimusi ja sätteid on võimalik muuta, siis otsustavad paljud seda mitte teha (Livingstone jt, 2019). Seega jääb küsitavaks, kas kasutajad – eriti lapsed ja noored täiskasvanud – mõistavad tõesti tingimusi ja on teadlikud võrgustikuga liitumise tagajärgedest (Scneble jt, 2021). Lastele seostuvad privaatsusriskide tekitajatena pigem inimesed, näiteks häkkerid, kes võrgukeskkonda sisse murravad (Stoilova, 2020). EU Kids Online 2020 uuringust selgus, et peaaegu pooled (46%) Eesti lastest on olnud võrgusuhtluses kellegagi, keda nad kunagi silmast silma kohanud ei ole ning paljud lapsed (39%) olid kokku puutunud kahjulike veebisaitidega (Smahel jt, 2020). Seega on üsna reaalne, et veebikeskkonnas toimetades

puutuvad lapsed erinevate ohtudega kokku. Enamik lapsi, kes on kokku puutunud negatiivse võrgukogemusega otsivad abi enamasti sõpradelt või vanematelt (Smahel jt, 2020).

Et lapsed oskaksid erinevaid privaatsusega seonduvaid riske märgata ja nendega iseseisvalt toime tulla on oluline, et neil oleks head teadmised digitaalsest kirjaoskusest ning digipädevustest (Stoilova, 2020). Digipädevusi ja- oskusi defineeritakse ySKILLS'i uuringus, kui teadmiste ja oskuste kombinatsiooni, mis aitavad kasutada info- ja kommunikatsioonitehnoloogiat nii, et see oleks võimalikult kasulik (Kalmus jt, 2022). Digipädevuste juures on oluline, et lapsed teaksid kuidas enda privaatsust kaitsta. Mõistet "privaatsuse kaitse", kasutatakse peamiselt seoses tundliku teabega (nt. pangakonto andmed), mida võidakse väärkasutada identiteedivarguse ja kellegi teisena esinemise kaudu (andmeid kogutakse tavaliselt ilma nõusolekuta või teadliku nõusolekuta) (Martinovic jt, 2014). Privaatsuse kaitsmiseks saab veebis kasutada mitut identiteeti, jääda anonüümseks või esitada sootuks valikulist infot, kuna inimesel on õigus otsustada selle üle, kes ja mil määral teda puudutavale informatsioonile juurdepääsu saab ja kuidas seda kasutada võib (Murumaa-Mengel jt, 2014).

Eelneva põhjal saab välja tuua, et kui külastatakse mõnda uut veebilehte või mänguplatvormi, siis annab leht märku, et külastaja peab kinnitama kasutustingimused ning privaatsussätted. Tihti on need aga pikad ning keeruliselt sõnastatud ning seega on veebilehte või mänguplatvormi külastajal raske aru saada, mida seal täpsemalt öelda soovitakse. Kui juba täiskasvanutel on keeruline nende sisu mõista, siis laste jaoks on see veelgi keerulisem. Lisaks on leitud, et kui lapsed külastavad mõnda platvormi, siis nad kardavad pigem seda, et keegi inimene võib neile veebikeskkonnas halba teha. Laste jaoks on keeruline mõista, et külastatav platvorm ise võib nende andmeid kuidagi kuritarvitada.

2.3 Privaatsuse kaitsmise olulisus

Inimeste jaoks on privaatsus tänasel digiajastul väga oluline (Kokolakis, 2015). Kuid iga kord, kui keegi loob võrguteenuse juurdepääsuks uue konto, mis nõuab näiteks nime, sünniaega ja elukohta, siis on inimesed harjunud väga lihtsalt seda teavet andma, vastutasuks teenuse eest, mida nad soovivad (Vallejo jt, 2018). Sellist privaatsushoiakute ja privaatsuskäitumise vastuolu nimetatakse privaatsusparadoksiks (Kokolakis, 2015; Beke jt, 2018). Enamus mänguplatvorme toimivad

samuti põhimõttel, et enne mängimist tuleks kasutajal konto luua. Tegemist on tundlike andmetega ning tavaliselt lapsed ei süvene sellesse, et nad jagavad enda privaatseid andmeid, mida kolmandad osapooled võivad kuritarvitada. Näiteks, kui laps sisestab enda isikuandmed mänguplatvormile ja ta ei ole veendunud selles, et neid andmeid õigesti käsitletakse, siis võib juhtuda, et isikuandmed võivad lekkida (Vellejo jt, 2018). Isikuandmete lekkeid on tihti ka meedia kajastatud. Näiteks oli aastal 2021 suur andmeleke, kus turvanõrkust ära kasutades laadis küberkurjategija alla 300 000 eestlase isikukoodid, nimed ning fotod, andmeleke oli Riigi Infosüsteemi Ameti pihta, mis peaks Eestis meie kõigi isikuandmeid kaitsma (Lees, 2021).

Kui lapsed külastavad mänguplatvorme, mis ei ole usaldusväärsed, siis on neil suur võimalus enda seadmesse saada viirus, või nuhkvara, mis hakkab kasutaja isikuandmeid väärkasutama (Smahel jt, 2020). Nii viirused kui ka nuhkvara toimivad põhimõttel, et arvutisse laetakse kasutaja teadmata programme, mis hakkavad kasutaja tundlikku informatsiooni koguma, et seda hiljem kasutaja vastu kasutada (Aluoja, i.a). Veel üks oht, mida kasutaja vastu kasutada saab on raha väljapetmine. Erinevad mänguplatvormid julgustavad lapsi tasulist sisu ostma, kuid sisestatud makseandmeid võidakse kuritarvitada ning ebaseaduslikult kasutada (Smahel jt, 2020). Online mängude juures tuleb tihti ette ka seda, et lapsed liituvad häkkimisfoorumitega, et hankida mängude modifikatsioone, läbi selle saavad küberkurjategijad lastega ühendust ja nende andmetele ligipääsu (Livingstone jt, 2017). Lisaks võivad kurjategijad julgustada lapsi, et nad enda digioskustega osaleksid ebaseaduslikus võrgutegevuses (Livingstone jt, 2017), või suunavad kurjategijad lapsi, et nad aitaksid võimaldada ligipääsu enda vanemate andmetele (Oja, 2017).

Lisaks eelnevale on üheks riskiks laste privaatsusele ka see, kui seadmed jälgivad asukohti nende enese teadmata (Smahel jt, 2020). Asukoha privaatsus on inimese võimalus liikuda avalikus ruumis ootusega, et nende asukoht pole kellelegi teada, või seda ei salvestata salaja hilisemaks kasutamiseks (Liu, 2018). Informatsiooniline privaatsus tähendab, et inimesel on endal õigus otsustada selle üle, kes infokeskkonnas tema teabele juurdepääsu saab ja kuidas ta seda kasutada võib (Murumaa-Mengel jt, 2014). On kindlaks tehtud, et kui lapsed on jälgimisest teadlikud, siis nad ei soovi seda ja suhtuvad sellese tõsiselt (Stoilova jt, 2020). Asukohaandmeid on oluline kaitsta, kuna nende lekkimise kaudu on võimalik tuvastada isiku elukohta ning liikumisharjumusi (Liu, 2018). Kui sellised andmed satuksid kurjategijate kätte, siis ei ole neil raske tuvastada seda, millal inimesed kodus on ja milline oleks hea aeg selleks, et enda kuritegelikud plaanid ellu viia.

Lapsed ei mõista, et tihti võivad nad jätta endast maha privaatset teavet, mis võivad neid mõjutada ka täiskasvanueas. See võib toimuda viisil, kui lapsed räägivad võrgu kaudu kellegagi, vestlusest jääb maha jälg mis on püsiv ja kopeeritav ning võimatu on kontrollida, kes sellele vestlusele ligi pääseb (Vallejo jt, 2018). Seega on oluline, et lapsed oleksid teadlikud sellest, kuidas nende online käitumine võib neid hiljem tulevikus mõjutada. Keskkondade külastamisega võivad kaasneda mitmed erinevad riskid, nendeks võivad olla erinevad pahavara programmid või ka küberkurjategijad, kes laste teadmatust ära kasutada proovivad. On oluline, et kasutajad ei külastaks kontrollimata keskkondi ning süveneksid hoolikalt sellesse, kuhu ja milliseid andmeid nad sisestavad.

Eelneva põhjal saab välja tuua, et privaatsust on oluline kaitsta, kuna andmete lekkimise tagajärjel võivad küberkurjategijad tundlikele andmetele ligipääsu saada. Neid tundlikke andmeid saab kasutada selleks, et näiteks tekitada rahalist kahju või varastada identiteet. Kogutud andmed ei pruugi lapsi kohe mõjutada, vaid alles aastate pärast. Tavaliselt ei mõelda riskide peale ja sisestatakse konto loomisel enda andmed siiski kuna soovitakse ligi pääseda pakutavale teenusele.

2.4 Uurimisprobleem

Lähtuvalt eelnevast oli töö eesmärgiks teada saada, kui teadlikud on teise kooliastme õpilased ohtudest privaatsusele kui nad mängivad online keskkondades. Lisaks oli soov teada saada, milliseid meetmeid võtavad lapsed ise kasutusele, et oma privaatsust mänguplatvormidel kaitsta. Nimetatud teema oli oluline selleks, et lapsevanemad ja haridusasutused oskaksid vajadusel rohkem tähelepanu suunata ennetusööle ja laste teadlikkuse tõstmisele.

Eesmärgi saavutamiseks püstitasin järgmised uurimisküsimused:

- Milliseid online mänguplatvorme lapsed eelistavad?
- Kuidas lapsed mõistavad privaatsuse tähendust online mängukeskkondades?
- Millised ohte näevad lapsed enda privaatsusele online mänge mängides?
- Milliseid meetmeid lapsed ise kasutusele võtavad, et enda privaatsust online-keskkondades mängides kaitsta?

3 MEETOD JA VALIM

Kasutasin enda töös kvalitatiivset lähenemist. Käsitletavaks teemaks oli teise kooliastme õpilaste privaatsus online mängukeskkondades, viisin lastega läbi poolstruktureeritud intervjuud, mida kirjeldan täpsemalt andmete kogumise all. Läbi intervjuude sain kaardistada laste arvamusi käsitletava teema osas. Järgnevates peatükkides toon välja, mille järgi valimi moodustasin, kuidas andmeid kogusin ning kuidas saadud andmeid analüüsisin.

3.1 Valimi moodustamine

Soovisin välja selgitada laste arvamusi, hoiakuid ning kogemusi seoses online mängude privaatsusega, seega valisin valimi sihtrühmaks ühe Lõuna-Eesti põhikooli 6.a, 6.b ja 6.c klassi õpilased. Valimisse kuulus 10 last, kes olid 12-13-aastased.

Määrus „Põhikooli riiklik õppekava“ kirjeldab milline on erinevate kooliastmete õppekava, nimetatud määruse lisa nr 10 sätestab valikõppeaine „informaatika“ õpiväljundid teisele kooliastmele (4-6 klass), õppekava läbinud õpilane peaks oskama kaitsta enda virtuaalselt identiteeti ja enda kohta käivat tundlikku informatsiooni (Põhikooli…, 2011). Valitud kooli õppekava sisaldab valikõppeainena informaatikat, seega sobisid nimetatud kooli õpilased sihtrühmaks.

Kuuenda klassi õpilased on nimetatud ainet läbinud ning õppekava järgi võis eeldada, et õpilastel peaksid olema teadmised internetis valitsevatest ohtudest ja sellest, kuidas neid ohte vältida. Väidet kinnitas ka valitud põhikooli lehel olev õppekava lisa, mis kirjeldab, et informaatika aine läbinu oskab inforuumi kriitiliselt hinnata. Lisaks on valitud kooli õppe- ja kasvatuseesmärkide all kirjeldatud, et informaatikaõpetusega taotletakse seda, et õpilane teadvustaks ja oskaks vältida info- ja kommunikatsioonitehnoloogia kasutamisel tekkivaid ohte isikuandmetele ja turvalisusele.

Konsulteerisin kooliga ning koostasin lastevanematele allkirjastamiseks nõusolekuvormid, mille kaudu sain nõusolekud laste osalemiseks intervjuudes (Lisa 1).

3.2 Andmete kogumine

Kvalitatiivse lähenemise tunnuseks on see, et tulemusi väljendatakse pigem selgituse ja kirjelduste abil, mitte numbriliselt ega statistiliste mudelite kaudu (Gerring, 2017). Seega valisin andmete kogumiseks poolstruktureeritud intervjuud, mille puhul küsitlejal on intervjuukava (Lisa 2) küsimustega. Küsimused intervjuu kava jaoks sain kirjeldatud teooriast. Teooriaosast tulenesid probleemid, mis on mängukeskkondade ja privaatsusega seotud. Tänu eelnevalt koostatud intervjuu kavale sain vestluse jaoks ette valmistuda. Jagasin planeeritavad vestlusteemad plokkideks, et mul oleks endal lihtsam vestluse kulgu jälgida. Esimesse teemaplokki planeerisin ka sissejuhatavad küsimused, et lapsed saaksid vestlusesse sisse elada. Viisin vestlused läbi Zoom keskkonnas. Valisin selle lahenduse kuna selle eeliseks oli mugavus, paindlikkus ning asjaolu, et omavahel suhtlemiseks ei mängi asukoht rolli (Archibald jt, 2019).

Poolstruktureeritud intervjuu puhul oli minu jaoks oluline, et saaksin dialoogi ajal vajadusel küsimuste järjekorda muuta. Vestluste käigus tuli mitmel korral see vajadus kasuks, kuna ma ei soovinud intervjueeritava mõtteid katkestada. Kui tekkis vajadus küsimuste järjekorda muuta, siis tänu intervjuu kavale omasin head ülevaadet sellest, millised teemad on veel käsitlemata. Mitu korda tekkis ka tarvidus esitada täiendavaid küsimusi, et intervjueeritavate vastuseid kinnitada ja olla kindel, et sain vastusest õigesti aru. Kuigi küsimused olid kõikidele intervjueeritavatele samad, siis ei antud neile ette vastusevariante vaid neil oli võimalus vastata oma sõnadega. Evans (2017) on välja toonud, et intervjuu juures on üheks oluliseks faktoriks see, et dialoog oleks loomulik ja meenutaks igapäevast vestlust. Minu jaoks oli oluline, et lapsed ennast mugavalt tunneksid. Vestlus ei oleks tohtinud näida ülekuulamisena, kuna see oleks võinud neutraalsete andmete saamist otseselt mõjutada. Enne vestluse algust tutvustasin intervjueeritavatele ka võimalust, et nad võivad igal hetkel vestluse katkestada, või kui nad ei soovi mõnele küsimusele vastata, siis nad annaksid sellest mulle kindlasti teada.

Poolstruktureeritud meetodi puhul nägin kitsakohana seda, et intervjueerija võib vastajatele mõju avaldada nii, et see mõjutab lõpptulemust (Brymann ja Bell, 2011). Püüdsin jääda võimalikult

neutraalseks ning mitte enda oleku ega küsimustega vastajat suunata. Adams (2015) on intervjuude negatiivse küljena välja toonud asjaolu, et suuremate rühmade uurimisel ei oleks see ajalist faktorid arvesse võttes otstarbekas. Kuna minu valimisse kuulus 10 õpilast, siis oli selles osas risk maandatud ning suutsin mõistliku aja jooksul kõik intervjuud läbi viia. Intervjueerimise ühe võimaliku riskina tuuakse teaduskirjanduses välja veel, et mõni inimene võib anda selliseid vastuseid, mida ta eeldab, et temalt oodatakse ja mis tegelikult ei kajasta tema isiklikku vaadet (Brymann ja Bell, 2011). Üritasin probleemi vältida sellega, et võimalikult mitmekülgsete küsimustega veenduda selles, et jagatud mõtted tõepoolest peegeldaksid vastaja arvamust.

3.3 Andmete analüüs

Andmete analüüsiks kasutasin kvalitatiivset sisuanalüüsi, mis on mõeldud suuremate tekstihulkade kitsendamiseks ning saadud info üldistamiseks (Mayring, 2019). Kvalitatiivne sisuanalüüs on paindlik, selle sisu on tekstipõhine ja tugine numbritel ning seda on võimalik muuta ja täiendada (Kalmus jt, 2015). Minu jaoks oli see lähenemine ainuõige, kuna töö tugines kasutajate kogemustel, numbrite kaudu oleks raske edasi anda laste hoiakuid ja arvamusi.

Selle valiku miinuseks võib olla see, et erinevate materjalide täpne vastandamine ei ole võimalik, lisaks on välja toodud, et töö autor ei pruugi tulemusi täiesti objektiivselt tõlgendada vaid võib püstitada hoopis endale meelepärase hüpoteesi (Kalmus jt, 2015). Üritasin mitte luua eelarvamusi ja kogutud andmeid võimalikult adekvaatselt tõlgendada. Lähtusin sellest, et intervjuude tulemused annavad püstitatud küsimustele vastused.

Transkribeerisin kõik vestlused läbi Tallina Tehnikaülikooli loodud veebipõhise kõnetuvastusprogrammi (Tallinna Tehnikaülikool, i.a). Andmete analüüsiks tuli transkribeeritud andmed kodeerida, kasutasin selleks Microsoft Wordi programmi. Iga vestluse salvestasin eraldi faili. Kuna süsteem oli mõningate intervjuude osas andmed osaliselt välja jätnud (tõenäoliselt kehva helikvaliteedi ning halva diktsiooni tõttu), siis pidin kõik intervjuud läbi kuulama ja faili omapoolseid parandusi tegema. Kodeerimisel kasutasin kategooriate loomisel manuaalset lahendust. See tähendab, et jagasin failis iga vestluse osas teemad kategooriateks, lähtusin palju intervjuu kavast. Välja kujunes 4 põhilist kategooriat, milleks oli sissejuhatav osa, mängudega seonduv, privaatsusega seonduv ning andmete kogumine. Kasutasin teemade eristamiseks

Microsoft Wordi tekstimarkeri abi, mis tähendab, et värvisin samade teemaplokkide küsimused ja vastused sama värvi. See oli heaks abimeheks, kuna mõningate intervjuude puhul pidin küsimuste järjekorda vastavalt vestluse sisule muutma. Seejärel tõin kategooriatest välja enda töö jaoks olulised teadmised, mille põhjal sain tulemusi esitada.

Intervjuudes osalenud laste isikuandmete kaitsmiseks ei ole töös nende nimesid välja toodud, nimed on asendatud pseudonüümidega (näiteks Intervjueeritav 1).

4 TULEMUSED

Peatükis kirjeldan seda, milliste tulemusteni läbi viidud intervjuude põhjal jõudsin. Esmalt toon välja selle, milliseid mänguplatvorme lapsed eelistavad, milliseid andmeid mänguplatvormid nende arvates koguvad ning kuidas lapsed mõistavad privaatsuse tähendust online mängukeskkondades. Seejärel kirjeldan, milliste ohtudega võivad lapsed online mänge mängides kokku puutuda. Peatüki lõpetuseks toon välja selle, mis meetmeid lapsed ise kasutavad, et enda privaatsust online-keskkondades mängides kaitsta ning kui palju on lapsed mänguplatvormidel tutvunud kasutustingimuste ning privaatsussätetega.

4.1 Laste eelistused online mänguplatvormide osas

Intervjuudest selgus, et keskmine aeg, mis intervjueeritud lapsed päevas internetis veedavad, jääb umbes kolme ja poole tunni juurde. Nimetatud kolmest ja poolest tunnist kulub intervjueeritavatel keskmiselt online mängude peale umbes kaks ja pool tundi. Online mängudest ülejäänud aeg kulub nende endi sõnul erinevatele sotsiaalmeedia ning meelelahutus platvormidele, nagu näiteks TikTok, Snapchat ja Youtube.

Kõik intervjueeritavad tõid välja, et neile meeldib niisama internetis toimetada eelkõige üksi, kuid online mänge mängida meeldib neile siiski kellegagi koos. Mängimiseks eelistatakse kasutada peamiselt telefoni või arvutit, ainult üks intervjueeritav või välja, et enamasti kasutab ta mängimiseks konsooli nimega Xbox. Mängukonsoolidest toodi välja veel PlayStation, mida kasutakse vahetevahel, lisaks arvutile ja telefonile. Intervjuudest selgus, et enamik lapsi eelistavad mängimiseks mänguplatvormi nimega Roblox. Robloxile lisaks nimetati veel mänguplatvorme Minecraft, Fortnite, Steam ja EpicGames, mida külastatakse aeg-ajalt.

Kõikides intervjuudes toodi välja, et enne, kui üldse mängima saab asuda, peab looma platvormile konto. Konto loomisel nõuab platvorm tavaliselt kasutajanime, e-posti aadressi, telefoninumbrit, vanust ning parooli. Tasuliste mängude soetamise puhul nõuab süsteem ka krediitkaardi andmeid. Kasutajanime juures toodi välja, et tavaliselt ei sisestata kasutajanimeks enda pärisnime vaid luuakse mingi varjunimi, mis konto loomise hetkel kõnetab või seostatakse kasutajanimi hoopis hüüdnimega. Varjunimesid eelistakse seetõttu, et siis ei ole intervjueeritud laste arvates võimalik loodud profiili nendega kokku viia.

Intervjuudest selgus ka see, et konto loomisel on mõned mänguplatvormid seadnud kasutajatele vanusepiirangu. Selgus, et paljud lapsed on selle piirangu möödasaamiseks enda vanust valetanud, või nad oleksid valmis seda tegema, kui nad platvormi kasutamiseks piisavalt vanad ei ole.

> *Intervjueeritav 2: „Ma oleksin arvatavasti sellest kõrvale viilinud ja pannud ikkagi vanema kuupäeva, et ma oleksin ikkagi vanem, sest muidu ta ei lase mind sisse sinna.“*

Intervjuude analüüs näitas, et mänguplatvorme valides eelistavad lapsed mänge, mis on nende huvidega seotud. Intervjueeritute jaoks on oluline, et mängud oleksid pigem tasuta kättesaadavad, kui tasulised, mis on arvestades intervjueeritud laste vanust ka igati mõistetav. Mängude eest tasumine eeldaks nende jaoks ligipääsu maksevahendile, mida kõigil olla ei pruugi. Lisaks tõid intervjueeritud lapsed välja olulise aspektina mänguplatvormi turvalisuse, mis nende jaoks seostus andmete lekkimisega.

> *Intervjueeritav 9: „Et noh, et seal oleks palju tasuta mänge. /.../ No, et seal oleks hea turvalisus, et minu isiklikud andmed välja ei antaks.“*

Eelnevalt välja toodu põhjal saab öelda, et intervjueeritud laste jaoks on mänguplatvormid olulised, kuna umbes 2/3 internetis veedetud ajast kulub neil endi sõnul online mängude peale. Online mängude mängimiseks kasutatakse peamiselt telefoni ja arvutit, aeg-ajal ka erinevaid mängukonsoole. Intervjueeritavad kirjeldasid, et mängukeskkondi valides lähtuvad nad enda huvidest ning sõprade soovitustest. Intervjuudest selgus, et laste jaoks on oluline, et mänguplatvormidel olevad mängud oleksid tasuta kättesaadavad. Lisaks mainisid intervjueeritavad ka seda, et nende jaoks on oluline, et mänguplatvorm, kus nad toimetavad, oleks turvaline.

4.2 Andmete kogumine mänguplatvormidel ning kuidas lapsed mõistavad privaatsuse tähendust online mängukeskkondades

Soovisin teada, milliseid andmeid külastatavad mängusaidid võiksid intervjueeritavatelt nende arvates koguda. Toodi välja, et saidid koguvad tõenäoliselt paroole, intervjueeritavate vanust, e-posti aadressi ning seda, mis mängu nad parajasti mängivad, ehk kõike seda, mida nad mänguplatvormile konto loomisel sisestavad. Uurides, miks mängusaidid soovivad neid andmeid koguda, seostati andmete kogumist positiivsena. Toodi välja, et tõenäoliselt koguvad mängusaidid mängija kohta selleks andmeid, et veenduda, et isik, kes kontole sisse logis oled ikka sina ning seeläbi aitavad mänguplatvormid mängija andmeid kaitsta. E-posti aadressi puhul täpsustati, et mõne mänguplatvormi puhul pole selle sisestamine kohustuslik, kuid selle täiendusega saab enda konto turvalisemaks muuta. Mängusaidid saavad e-posti teel mängijat teavitada sellest, kui kontol toimub kahtlane tegevus või keegi võõras üritab kontole sisse logida.

> *Intervjueeritav 2: „Et kas, kas see, kes mängib olen ikka mina, võib-olla keegi teine on minu konto pealt sisse saanud ja siis ta mängib seal minu asjadega.“*

Paar intervjueeritud last oskasid andmete kogumise juures välja tuua ka kaubandusliku konteksti. Mainiti, et tõenäoliselt koguvad mänguplatvormid andmeid mängija huvide ja eelistuste kohta selleks, et raha teenimise eesmärgil tasulisi mängusiseseid asju pakkuda. Toodi välja, et tihti kasutavad mänguplatvormid selleks just eelnevalt mainitud e-posti. Juhul, kui mängija sisestab platvormile enda e-posti konto, siis hakkab platvorm meili peale reklaame saatma. Reklaamimise eesmärgil töötab intervjueeritavate sõnul ka platvorm ise, ehk kogutakse mängija eelistusi ning seeläbi soovitab platvorm juba tasulisi mänge, mida lapsed osta saaksid.

> *Intervjueeritav 5: „No nad ilmselt koguvad infot, mis mind huvitab, ehk siis nad saaksite reklaame selle kohta nagu natukene minu huvikohasemaks teha. /.../ Et nad saaks rohkem asju pakkuma, mida ma saaks osta, et nad saaks raha teha.“*

Suurem osa intervjueeritud lastest tõid küll välja, et tõenäoliselt kogub mänguplatvorm nende eelistusi mängude osas, kuid nad ei seostanud seda kaubandusliku kontekstiga, vaid nad tõid välja, et seeläbi pakub mäng neile järgmisi sarnaseid mänge. Selline eelistuste kaardistamine oli mõne

intervjueeritava jaoks kohati arusaamatu ning neile tundus, et mänguplatvorm surub neile pigem enda eelistusi peale. Teistele intervjueeritavatele pigem vastupidiselt meeldis, et mänguplatvorm eelnevate mängude põhjal teisi mänge soovitab. Toodi välja, et tänu sellele ei pea ta kasutaja ise uusi mänge otsima.

Intervjuude analüüsist selgus ka see, et suurem osa intervjueeritutest andmete sisestamises probleemi ei näinud. Toodi välja, et erinevate andmete sisestamine sobib neile seetõttu, et mänguplatvorm loob neile seeläbi turvalise keskkonna. Intervjueeritud lapsed selgitasid, et kui neil ka mingisugune kahtlus andmete sisestamise osas tekib saavad nad kas vanemate või sõprade käest uurida, miks neid andmeid vaja on.

> *Intervjueeritav 9: „No see pole väga hull, see on nagu iseenesest noh, reklaamimise ja turvalisuse põhjustel. Ja minu arust on see okei.“*

Mõni intervjueeritav mainis, et muretseb selle üle, mis andmete sisestamine endaga kaasa tuua võib kuid sellest hoolimata sisestatakse nõutavad andmed ikkagi, kuna mänguplatvormil saavutatu on laste jaoks oluline. Mängus saavutatu (kogutud virtuaalraha, vallutatud maailmad, soetatud virtuaalsed tööriistad jne- autori kommentaar) olulisust rõhutati mitmel korral. Samas ei olnud intervjueeritud laste jaoks lõpuni selge, miks konto loomisel andmete sisestamine üldse vajalik on ning miks ei võiks mänguplatvormil mängida ilma kontot loomata.

> *Intervjueeritav 3: „Ühest otsast on see nagu hea, et siis nagu see, mida sa oled saavutanud, seal, see ei kao ära. /.../*

Andmete kogumise jätkuks soovisin välja selgitada, mida tähendab intervjueeritud laste jaoks privaatsus. Intervjuudest selgus, et intervjueeritud laste jaoks tähendab privaatsus seda, et keegi võõras ei pääse nende andmetele ligi ning nad ise ei jaga enda andmeid võõrastega. Andmetena, mida lapsed privaatseks peavad ja teistega jagada ei sooviks toodi välja näiteks vanus, nimi, asukoht, IP-aadress, elukoht ja ka kool, kus nad õpivad. Privaatsust seostati ka isikliku ruumiga, kuhu ei tohiks teised tulla ja mis annab sulle õiguse seal teha asju, mida teised ei näe. Toodi veel välja, et privaatsus tähendab seda, et keegi ei saaks kellegi teise nime alt mänguplatvormil mängida. Ehk privaatsust seostati otseselt ka mänguplatvormiga.

Intervjueeritav 5: „Minu jaoks privaatsus tähendab seda, et keegi ei saaks minu nime alt siis mängida ja igasuguseid asju teha.“

Paludes välja tuua isiklikud andmed, siis need mõningal määral erinesid nendest andmetest, mida lapsed privaatseteks andmeteks pidasid. Isiklike andmetena toodi välja andmed, mis on otseselt seotud mänguplatvormidega, näiteks mängus saavutatu.

Eelneva kokkuvõttena saab välja tuua, et intervjueeritavate jaoks tähendab privaatsus seda, et keegi kolmas isik ei pääseks nende andmetele ligi. Lisaks toodi välja, et ka ise ei tohiks enda andmeid kellelegi võõrale jagada. Isiklike andmetena näevad intervjueeritavad andmeid, mille nad erinevatele platvormidele maha jätavad, näiteks sisestatud paroolid ja mängus saavutatu.

Enamus intervjueeritavatest seostavad mänguplatvormidel erinevate andmete kogumist pigem positiivsena. Nende arvates aitavad mänguplatvormid kogutud andmete abil mängija kontot turvalisena hoida. Näiteks annab mänguplatvorm e-posti teel märku, kui keegi võõras üritab kontole ligi pääseda. Ainult paar intervjueeritavat oskasid välja tuua andmete kogumise juures kaubandusliku konteksti, mis tähendab, et tõenäoliselt koguvad mänguplatvormid andmeid selleks, et suunata kasutajat tasulist sisu ostma. Siiski ei ole intervjueeritavate jaoks probleemiks mänguplatvormidele erinevate andmete sisestamine kuna mängus saavutatud tulemused on nende jaoks olulised.

4.3 Ohud privaatsusele online mänge mängides

Kui konto loodud ja mänguplatvormil toimetatakse, siis seal mängides suhtlevad intervjueeritud lapsed tavaliselt enda sõprade, trennikaaslaste või koolikaaslastega. Suhtlemiseks tuttavatega kasutatakse online mängukeskkonna kõrval Messengeri, Snapchati või Discordi. Neid lahendusi eelistatakse seetõttu, et mängplatvormid ei võimalda mängimise ajal üksteisele helistada ja videokõnet teha. Messengeri ja Discordi eelisena toodi välja ka asjaolu, et neid on võimalik tasuta kasutada. Enamus intervjueeritavad mängivad mänguplatvormidel võõrastega ning kasutavad omavahel suhtlemiseks platvormisisest vestlusakent. Võõrastega suhtlus toimub tavaliselt inglise keeles, kuna mänguplatvormidel on palju välismaalasi. Mingisuguseid probleeme intervjueeritavatel endil võõrastega suhtlemisel ei ole siiani ette tulnud.

Intervjueeritav 2: /.../ „nagu päriselu saad elada seal ja siis räägime erinevatest asjadest, kõik inglise keeles, sest et muidu ei saa keegi aru eesti keeles.“

Kuigi intervjueeritavad ise ei olnud võõrastega kokkupuutel negatiivset kogemust saanud, oskasid nad välja tuua enda lähedaste ja sõprade seast kogemusi, mis ei lõppenud väga hästi. Näiteks tõi üks intervjueeritav välja, et tema sõbra kontole said pahade kavatsustega inimesed ligipääsu ja seetõttu jäi sõber enda kontost ilma.

Teine intervjueeritav jagas kogemust, mis juhtus tema õega. Nimelt meeldis intervjueeritava õele tihti võõrastega mänguplatvormil nimega Roblox mängida. Kahjuks pääsesid selle tõttu küberkurjategijad intervjueeritava õe kontole ligi, kaaperdasid selle ja suutsid tekitada 100 euro väärtuses rahalise kahju. Lapsevanem oli varasemalt lapse kontole tasulisi asju soetanud ja seetõttu olid krediitkaardi andmed hilisemaks kasutamiseks kontole salvestatud. Kannatanud ei olekski kohe osanud kahju märganud, aga küberkurjategijad üritasid kaaperdatud konto kaudu veel erinevaid oste teha. Kuna rakendus nimega Google Play andis kannatanutele märku, et rahaline limiit on ületatud said nad aru, et konto on võõrastes kätes. Nad küll blokeerisid konto ära, kuid raha ei õnnestunud neil tagasi saada.

Intervjueeritav 8: „Minul ei ole niimoodi juhtunud. Õel on juhtunud /.../ Seal on mõned häkkerid/.../ mu õde oli nendega nagu sõber. Ja ma arvan, et ühele häkkerile ta ei meeldinud ja siis ta läks ja häkkis mu õe konto ära ja ostis 100 euroga Rublukse (virtuaalne raha Robloxi mängus) /.../ ema oli ostnud tema konto peale Rublukse ja need andmed jäid sinna sisse ja sai tänu sellele osta. /.../ ta raiskas sada euri ära onju, tal oli vaja kinnitust, et neid juurde osta. Nii, sest sa saad ju ainult sada eurot kuus maksta Play poest, siis ta küsib, kinnitust. /.../ Ta tahtis nagu spämmata, nii kaua, kuni mu emal poleks enam raha olnud. Nii ise aga, aga sellepärast, et Play pood ei luba, seal on niimoodi, et sada euri iga kuu ja siis pead panema verificationi (kinnituskoodi), et sa pole mingi , kes üritab lihtsalt raha raisata. /.../ Ei, ta ei jaganud parooli, õde lihtsalt ärkas järgmine päev üles ja läks Robloxi mängima, aga ta nägi, et Robloxi account (konto) oli välja logitud. Nii ta läks sisse, tagasi logima, aga tal oli see accounti parool kinni läinud, ta ei saanud enam enda vana parooli sisse panna, sest häkker, seal on settingud (seaded), mis tähendab seda, et sa saad vahetada seal parooli ära, see häkker oli selle parooli ära vahetanud niimoodi, et see inimene ei saaks sinna enam ligi. /.../ Need on häkkerid. On olemas Robloxis selline mäng

nagu Kahood, seal on väga palju häkkereid, seal on niimoodi, et igast serverist võid sa leida ühe häkkeri.

Uurisin lastelt ka seda, milliseid tegevusi mänguplatvormidel teha ei saa. Toodi välja, et mängus sees ei saa teistele kasutajatele halba teha sellega, et nendelt mängusiseseid asju ära võtta. Kuna intervjueeritavate jaoks on oluline, et mängud oleks tasuta, siis toodi välja, et mõnel platvormil ei saa kõiki mänge tasuta mängida. Intervjuude analüüsist selgus ka, et intervjueeritavate seas populaarsel mänguplatvormil Roblox ei saa mängijad vestlusaknas üksteisele mõningaid sõnu ja numbreid öelda. Uurides, millised need sõnad ja numbrid täpselt on sain vastuseks, et vestlus blokeerib ära ropud sõnad ning numbrid ja asendab need # märgiga.

Intervjueeritav 7: „Need on ropud, ropud, sõnad lihtsalt. /.../ Ta lihtsalt nagu blokib selle ära, et ta paneb nagu need hashtag märgid sinna peale, et seda ei ole näha.“

Intervjueeritud lapsed selgitasid, et numbrite hägustamine toimub sellepärast, et süsteem kaitseb nii laste andmeid. Mänguplatvorm ei luba intervjueeritavate sõnul numbreid sisestada, kuna seostab neid sellega, et laps üritab kellelegi võõrale enda telefoninumbrit või isikukoodi saata. Väidetavalt pidi selline numbrite ja sõnade hägustamine toimuma ainult alla 13-aastastele. Ehk konto loomisel tuvastab süsteem selle, mis vanuses on laps ning vastavalt sellele on paika pandud mänguplatvormi sisesed reeglid.

Vestlustest selgus, et enamus intervjueeritutest näevad privaatsusele ohtu pigem teistes inimestes, kes mänguplatvormidel samaaegselt mängivad. Intervjueeritavad kirjeldasid, et enda privaatsust saab online mängudes kaitsta nii, et sa ei räägi võõrastele enda isiklikke asju ning ei anna välja enda andmeid. Privaatsuse kaitsmiseks toodi välja veel võimalus, kui sa varjad kaasmängijate eest enda identiteeti. Ehk sa ei esine mänguplatvormidel enda nime ja näoga, vaid esined kellegi teisena. Kellegi teisena esinemise jätkuks mainiti ka varikontode kasutamist. Ehk, kui luua mingisugune varikonto, kuhu sisestada väljamõeldud andmed, siis peaks see takistama seda, et mängija kohta midagi teada saab. Tuli välja, et vältimaks seda, et enda igapäevast e-posti kontot kusagile sisestada, siis varikontode tarbeks loovad lapsed uue e-posti konto ja seovad selle pigem mängusaidiga.

Intervjuueritav 6: „Näiteks ei panegi enda andmeid päris sinna, et keegi ei saa asukohta väga palju teada. /.../ teebki mingi suvaga mingi konto, mitte nagu enda emailiga, vaid

panete näiteks suvalise Gmaili. Ja siis paned selle sinna hoopis, et siis ei saa sinu kohta keegi midagi teada.“

Eelneva põhjal saab öelda, et intervjueeritavad on mänguplatvormidel suheldes väga aktiivsed. Mängides suheldakse nii sõprade tuttavate, kui ka võõrastega. Võõrastega suhtlemisel kaasnevad ka ohud. Nimelt oskasid intervjueeritud lapsed välja tuua näiteid, mis nende sõprade või perekonnaliikmetega juhtunud on. Üks laps kirjeldas detailselt, kuidas küberkurjategijad tekitasid tema emale suure rahalise kahju.

Vestlustest selgus veel, et enamus intervjueeritavatest näevad privaatsusele ohtu pigem teistes inimestes, kes mänguplatvormidel samaaegselt mängivad. Uurides, kuidas saaks enda privaatsust online mängudes kaitsta, kirjeldasid intervjueeritavad, et enda privaatsust saab kaitsta sellega, kui ei räägi võõrastele enda isiklikke asju ega jaga kellegagi enda andmeid. Lisaks toodi välja, et enda privaatsuse kaitsmiseks luuakse tihti ka varikontosid. Või luuakse mängimise tarbeks uus e-posti aadress, mis seotakse mänguplatvormil loodud kontoga.

4.4 Meetmed mida lapsed rakendavad, et enda privaatsust online mängukeskkondades kaitsta

Järgnevalt soovisin välja selgitada seda, mida saaksid intervjueeritavad ise selleks teha, et online mängude mängimine nende jaoks turvaline ja ohutu oleks. Mõned intervjueeritavad tõid välja, et turvalisemaks ja ohutuks saaks enda jaoks mängimist läbi selle muuta, kui sisestad mänguplatvormile endast võimalikult vähe andmeid ning ei jaga neid kolmandate osapooltega. Lisaks toodi välja, et kindlasti peaks vältima enda isiklike andmete jagamist võõrastega, ei tohiks kellelegi öelda enda parooli, isikukoodi ja e-posti aadressi.

Intervjueeritav 3: „Ei jaga mitte mingisugust isikuandmed, isiklikke asju. Gmaili aadress, parool, isikukoodidega, mitte mingisuguseid sarnaseid andmeid. /.../“

Intervjuudes toodi veel välja, et mõistlikum on võõrastest ja tundmatutest lehtedest eemale hoida. Uurides intervjueeritavatelt seda, kuidas nad hindavad, milline külastatud leht on turvaline tõid

nad välja, et usaldavad veebibrauseri poolseid teavitusi selle kohta, kas leht on usaldusväärne. Sattudes võõrale ja kahtlasele lehele, annab brauser intervjueeritavate kogemuste põhjal sellest märku. Intervjuudest selgus, et lapsed oleksid huvitatud sellest, et ise kahtlaseid lehti tuvastada. Hetkel neil endil sellised teadmised puuduvad, kuidas eristada turvalisi lehti ebaturvalistest. Seega oleksid lapsed huvitatud sellest, kuidas enda digipädevusi suurendada.

> *Intervjueeritav 4: „Ma tegelikult täpselt ei tea ka kuidas neid turvalisi lehti eristada.“*

Mängude ja mängukeskkondade valimisel toodi välja, et hinnatakse väga ka kaasmängijate arvamust. Näiteks mänguplatvormidel on igal külastajal võimalik platvormi siseseid mänge hinnata ning arvustada, lapsed lähtuvad turvalisuse hindamisel nendest arvustustest. Lisaks kaasmängijate arvamusele peetakse oluliseks ka sõprade arvamusi ja kogemusi. Kui mõnel sõbral on mängusaidiga halb kogemus olnud, siis seda mänguplatvormi pigem välditakse.

> *Intervjueeritav 6: „Vaatan enne küsin sõprade käest, näiteks, et kas nad on mänginud seda mängu, et kas nad teavad, et kas seal võib olla midagi, kas neil on midagi juhtunud.“*

Erinevatest programmidest, millega privaatsust kaitsta saab mainiti Google Block Assistent'i, VPN'i ning Google Family Link'i. Uurides, kellelt intervjueeritavad lapsed privaatsusega seonduvatel teemadel informatsiooni saavad, tõid nad välja, et koolis informaatika tunnis on sellest räägitud. Mis puudutas seda, millal viimati koolis privaatsusega seonduvatel teemadel räägiti, läksid arvamused lahku. Mõned lapsed mainisid, et koolis räägiti neile viimati privaatsusega seonduvatel teemadel aasta aega tagasi. Teised tõid välja, et sellistel teemadel räägiti algklassides. Vestlustest selgus, et kui koolis on privaatsusega seonduvatel teemadel vesteldud, siis on see olnud pigem pealiskaudselt.

> *Intervjueeritav 7: „Eelmine aasta võib-olla siis, kui meil oli. /.../ See oli selline nagu tagasihoidlikum pigem.“*

Enamustel intervjueeritud lastel on ka lapsevanemad teadmisi andnud, kuidas enda privaatsust kaitsta. Mitme lapsega vesteldes selgus, et ka internet on koht, kus privaatsusega seonduvatel teemadel informatsiooni saadakse, näiteks YouTube'i videotest.

Privaatsuse kaitsmise jätkuks soovisin välja selgitada, kas intervjueeritavad on tutvunud tingimustega, mida mängusait palub neil ennem nõustumist lugeda ja kui nad on neid tingimusi lugenud, siis mis neil sellest meelde on jäänud. Intervjueeritavad mainisid, et kasutustingimused asusid kohe mängu pealehel ning enne mängima hakkamist pidid nad need kinnitama. Kõik intervjueeritavad olid vähemalt korra mängusaidil kasutustingimustega tutvunud. Paarile intervjueeritavale oli meelde jäänud, et seal kirjeldatakse seda, et mängija annab mänguplatvormile õigusi nende andmeid koguda ning küsib ka seda, et kas mängija võimaldab platvormile ligipääsu enda fotodele, meediale ja failidele. Teistele olid meelde jäänud reeglid, mis puudutasid otseselt mängimist, näiteks et mängimiseks tuleb konto luua, mängus olles ei tohi öelda rassistlike ja solvavaid sõnu teiste kaasmängijate kohta ning enda informatsiooni ei tohiks kaasmängijatega jagada. Juhul, kui mängusiseste reeglite vastu eksitakse on mänguplatvormil õigus mängija konto mingiks ajaks sulgeda.

> *Intervjueeritav 3: „Et ja nagu sa ei tohi nagu öelda mingeid rassistlikke või midagi solvavaid sõnu, sest muidu sul võidaks konto panna seitsmeks päevaks lukku, kolmekümne üheks päevaks lukku või, nagu üldse ära kustutada see konto. Siis ei tohtinud avaldada mingi mitte mingisugust isiklikku infot ja oli siis need mängureeglid, mida ei tohtinud, nagu, kui keegi teine nagu tekib siis teda ei tohi kohe ära tappa, sest selles võis ka nagu nagu nii-öelda mängusisese süüdistuse saada /.../.“*

Mitu intervjueeritud last mainisid, et kasutustingimused on mänguplatvormidel inglisekeelsed ja vahel ei saa nad aru, mida seal täpselt kirjutatakse. Mõned intervjueeritud lastest olid nende tõlkimiseks kasutanud näiteks ka Google Translate abi.

Mängusaidi tingimustega tutvumise jätkuks uurisin intervjueeritavatelt seda, kas nad on teadlikud sellest, mis tähendavad privaatsussätted ning kas nad on proovinud neid mõnel külastatud saidil ka muuta. Enamus lastest ütlesid, et nad ei tea, mis on privaatsussätted ja seega ei oskaks nad neid ka muuta. Ainult üks laps mainis, et privaatsussätted on privaatsusseaded, mida on võimalik muuta.

Privaatsusega seonduva juures soovisin veel teada, millised on teadmised ja oskused online mängude privaatsusega seoses, mille osas intervjueeritavad sooviksid paremaid teadmisi. Toodi välja, et paremaid teadmisi soovitakse sellest, kuidas enda privaatust üldiselt kaitsta saaks. Näiteks, kuidas takistada seda, et keegi teine sinu andmetele ligi ei saaks, ja milline võiks olla tugev parool,

mis aitaks enda kontot võõraste eest kaitsta. Lisaks sooviti teada, mida privaatsussätted endast kujutavad ning kuidas oleks neid võimalik muuta. Kasutustingimuste osas mainiti, et paremad teadmised võiksid olla sellest, kuidas neid paremini tõlkida saaks. Mainiti isegi seda, et soovitakse teadmisi, kuidas enda IP-aadressi kaitsta saaks.

> *Intervjueeritav 5: /.../"võib-olla natukene enda IP kohta , et rohkem teada saada, kuidas seda kaitsta."*

Eelneva põhjal saab öelda, et intervjueeritavate sõnul saab enda jaoks mängimist turvalisemaks ja ohutuks läbi selle muuta, kui sisestada mänguplatvormile endast võimalikult vähe andmeid. Lisaks ei tohiks enda andmeid kolmandatele osapooltega jagada. Mainiti veel seda, et tundmatutest ja kahtlastest lehtedest tuleks eemale hoida. Samas toodi välja, et teadmised usaldusväärsete lehtede hindamisel ei ole piisavalt head ning lehtede hindamisel tuginetakse pigem kaasmängijate ning sõprade kogemustele.

Intervjueeritavad tõid välja, et privaatsusega seonduvatel teemadel on neile koolis pigem põgusalt räägitud. Lisaks selgus, et enamus lapsi ei tea, mis on privaatsussätted ning nad ei oskaks neid ka muuta. Küll aga on nad tutvunud kasutustingimustega, sest need asuvad tavaliselt mängu pealehel. Kasutustingimused on nende jaoks aga tihti keerulised ning nende tõlkimise osas sooviksid lapsed paremaid teadmisi.

5 JÄRELDUSED JA DISKUSSIOON

Järgnevas peatükis esitan järeldused tuginedes intervjuudest saadud tulemustele ning arutlen nende üle seostades need varasema kirjandusega. Järelduste juures toon välja uurimisküsimuste vastused, mis lähtuvalt teemast olid järgnevad:

- Milliseid online mänguplatvorme lapsed eelistavad?
- Kuidas lapsed mõistavad privaatsuse tähendust online mängukeskkondades?
- Millised ohte näevad lapsed enda privaatsusele online mänge mängides?
- Milliseid meetmeid lapsed ise kasutusele võtavad, et enda privaatsust online-keskkondades mängides kaitsta?

5.1 Järeldused ja arutelu

Oma töös soovisin välja selgitada, kui teadlikud on teise kooliastme õpilased ohtudest privaatsusele, kui nad mängivad online keskkondades. Lisaks oli soov teada saada, milliseid meetmeid võtavad lapsed ise kasutusele, et oma privaatsust mänguplatvormidel kaitsta.

Intervjuude analüüs näitas, et lapsed eelistavad mänguplatvorme, mis on turvalised. Lisaks on mänguplatvormide valiku üheks kriteeriumiks ka mängude tasuta kättesaadavus. Kuna paljudel lastel puudub ligipääs maksevahenditele, siis on see tulemus ka mõistetav. Online mänguplatvormidelt otsitakse pigem mänge, mis on intervjueeritavate huvidega seotud. Enamus intervjueeritavatest tõi välja, et mänguplatvorm nimega Roblox on see, mida külastatakse kõige tihedamini.

Intervjuude analüüsist selgus, et enamus mänguplatvorme soovib, et kasutaja looks mängukeskkonda konto. Konto loomisel küsitakse enamasti ka mängijate vanust. On leitud, et kui mänguplatvormidele on seatud vanusepiirangud, siis kipuvad noored tihti mängukeskkondades

esinema vanemana, kui nad tegelikult on, nad teevad seda selleks, et ligi pääseda soovitud mängusaidile (Martinovic jt, 2014). Ka minu intervjuude analüüs tõi välja, et enamik intervjueeritavatest olid mänguplatvormidega liitudes vanemana esinenud. Või nad oleksid valmis seda tegema, kui mänguplatvorm, mida nad külastada soovivad on seadnud vanusepiirangu. Mingisuguseid riske intervjueeritavad endi sõnul selles ei näe. Intervjuude analüüsi põhjal saab öelda, et vanusepiirangud on siiski seatud põhjusega. Näiteks populaarne mänguplatvorm Roblox ei luba intervjueeritavate sõnul alla 13-aastastel lastel läbi vestlusakna teistele numbreid ja mõningaid sõnu kirjutada. See aitab ära hoida riski, kus lapsed jagavad võõrastele enda telefoninumbrit või isikukoodi.

Mänguplatvormidel toimetades on intervjueeritud laste jaoks privaatsus väga oluline. Intervjueeritavatega vesteldes selgus, et nende jaoks tähendab privaatsus, et keegi võõras ei pääse nende andmetele ligi ning nad ise ei jaga enda andmeid võõrastega. Privaatsust seostati ka isikliku ruumiga, kuhu ei tohiks teised tulla ja mis annab seal õiguse teha asju, mida teised ei näe. Andmetena, mida lapsed privaatseks peavad ja teistega jagada ei sooviks toodi välja näiteks vanus, nimi, asukoht, IP-aadress, elukoht ja kool. Lastega vesteldes selgus, et isiklikud andmed erinesid mõningal määral nendest andmetest, mida lapsed privaatseteks andmeteks pidasid. Isiklike andmetena toodi välja andmed, mis on otseselt seotud mänguplatvormidega, näiteks mängus saavutatu.

Nagu ka intervjuude analüüs näitas, siis on inimeste jaoks on privaatsus tänasel digiajastul väga oluline (Kokolakis, 2015). Kuid iga kord, kui keegi loob võrguteenuse juurdepääsuks uue konto, mis nõuab näiteks nime, sünniaega, elukohta, siis on inimesed harjunud väga lihtsalt seda teavet andma, vastutasuks teenuse eest, mida nad soovivad (Vallejo jt, 2018). Intervjueeritud laste arvates peaks enda ohutuse tagamiseks mänguplatvormile sisestama endast võimalikult vähe andmeid. Samas tõid lapsed välja, et kui konto loomisel tuleb enda kohta andmeid sisestada, siis suurem osa intervjueeritavatest andmete sisestamises probleemi ei näinud. Intervjueeritud lapsed leidsid, et andmete sisestamine loob neile hoopis turvalisema mängukeskkonna. Seega võib öelda, et laste jaoks seostus oma andmete jagamine mängukeskkonnas pigem turvalisusega, mitte aga privaatsusega või sellega seotud probleemidega.

Erinevate (isiku)andmete jagamine ning kogumine on see, mis saab privaatsust otseselt mõjutada. Külastades erinevaid mänguplatvorme jätavad lapsed endast maha palju andmeid. Nendeks andmeteks võivad olla näiteks hiireklikid või mängus saavutatud tulemused (Russel jt, 2018;

Kröger jt, 2021). Nimetatud andmeid analüüsitakse ning sellest analüüsist saadud tulemusi kasutatakse selleks, et mõjutada mängijat nii, et ta ostaks tasulist sisu (Macenaite ja Kosta, 2017; Yannakakis ja Togelius, 2018; Kröger jt, 2021). Tavaliselt kasutatakse mõjutusvahendina reklaame, mis on kohandatud selle järgi, mis mängijale võiks kõige rohkem huvi pakkuda (Macenaite ja Kosta, 2017; Yannakakis ja Togelius, 2018). Enamus intervjueeritavatest mõistsid, et platvormidel kuvatavad reklaamid on just neile kohandatud kuid nad ei seostanud seda kaubandusliku eesmärgiga. Intervjueeritavad tõid hoopis välja, et reklaamide abil pakub mänguplatvorm mängijale mänge, mida nad mängida võiksid. Ainult paar intervjueeritavat oskasid välja tuua, et tõenäoliselt kogub mänguplatvorm mängija andmeid selleks, et koguda teavet mängija huvide ja eelistuste kohta, et siis juba sellele tuginedes tasulist sisu pakkuda. Kui lapsed otsustavad mänguplatvormidelt tasulist sisu osta siis võib tekkida oht, et sisestatud makseandmeid võidakse kuritarvitada ning ebaseaduslikult kasutada (Smahel jt, 2020). See oht on üsna reaalne, kuna intervjueeritavad tõid välja ka sellekohased näiteid. Üks intervjueeritav kirjeldas väga detailselt seda, kuidas tema õe konto kaaperdamine tõi lapsevanemale kaasa 100-eurose rahalise kaotuse. Seega on andmete ebaseaduslik kasutamine väga reaalne oht.

Andmete ebaseaduslik kasutamine saab juhtuda kuna lastel on keeruline mõista seda, kuidas toimub isikuandmete kogumine kaubanduslikus kontekstis (Stoilova jt, 2020). Stoilova ja kaasautorid (2020) on välja toonud, et lastele seostuvad privaatsusriskide tekitajatena pigem inimesed, näiteks häkkerid, kes su kontole ligi pääseda üritavad. Intervjuude analüüsist saadud tulemused kinnitasid seda väidet. Nimelt tõid intervjueeritud lapsed korduvalt välja seda, et nende jaoks oleks probleemiks see, kui keegi pääseks nende kontole ligi ning seetõttu kaotaksid nad kõik mängus saavutatu. Intervjueeritavad ei maininud kordagi seda, et mänguplatvorm ise võiks nende privaatsusele ohtu kujutada.

Et lapsed oskaksid privaatsusega seonduvaid riske paremini märgata on oluline, et õppeasutused selgitaksid lastele seda, kuidas eraettevõtted andmetega toimetavad ning millised võimalused ja ohud erinevate veebikülastustega kaasnevad. Lisaks on oluline, et lapsed teaksid kuidas ja miks enda isikuandmeid internetiavarustes kaitsma peaks. Intervjuudest selgus, et enamus lapsi ei mäleta seda, millal neile viimati koolis privaatsusega seonduvatel teemadel räägiti ning ülejäänud tõid välja, et neile sellel teemal koolis räägitud, kuid põgusalt. Nagu valimi koostamise juures välja tõin, on valitud kooli õppekavas kirjas, et läbitud informaatika tund peaks lastele andma teadmised sellest, kuidas inforuumi kriitiliselt hinnata. Lisaks on valitud kooli õppe- ja kasvatuseesmärkide all kirjeldatud, et informaatikaõpetusega taotletakse seda, et õpilane teadvustaks ja oskaks vältida

info- ja kommunikatsioonitehnoloogia kasutamisel tekkivaid ohte isikuandmetele ja turvalisusele. Seega on õppeasutuste kohustus lastele selgitada, millised riskid võivad erinevate veebilehtede ning mänguplatvormide külastamisega kaasneda.

Lisaks lasub minu arvamuse kohaselt ka mänguplatvormidel kohustus paremini välja tuua, millised privaatsusega seonduvad riskid neil platvormidel valitsevad. On leitud, et mängude juures on hoiatused, millisele vanusegrupile need sobivad ning mängutootjad toovad välja, et mängus võib esineda vägivalda, kuid puuduvad hoiatused privaatsusega seotud riskide kohta (Martinovic jt, 2014). On oluline, et inimene, kes privaatsussätteid ja kasutustingimusi kinnitab, saaks aru, mida organisatsioon tema andmetega teeb (Andmekaitse Inspektsioon, 2017). Kahjuks selgus aga intervjuudest, et enamus lastest ei tea, mis privaatsussätted on ning seetõttu ei oskaks nad neid ka muuta. Kui lapsed ei oska mõista, mis on privaatsussätted, siis tähendab see tõenäoliselt seda, et need ei ole laste jaoks piisavalt nähtavad või ei ole neile sellel teemal varasemalt räägitud. Seda tõendab ka asjaolu, et enamus lapsi on vähemalt korra lugenud mänguplatvormidel olevaid kasutustingimusi, kuid privaatsussätted on nende jaoks võõrad. Lisaks on probleemiks see, et kasutustingimused ja privaatsussätted on sageli pikad ja kirjutatud keerulises õiguskeeles ja seega on paljudel raske aru saada, mida seal täpselt öelda soovitakse (Schneble jt, 2021). Seda kinnitasid ka lapsed, keda intervjueerisin. Kuna kõik lapsed olid kasutustingimustega vähemalt korra tutvunud, siis tõid nad välja, et vahel on raske aru saada, mis seal kirjas on. Märkimisväärne on aga see, et lapsed ise soovivad nendest aru saada ja nad on kasutanud kasutustingimuste tõlkimiseks isegi Google Translate'i abi.

Intervjuudest selgus, et lastel on olemas mõningad teadmised sellest, kuidas vältida kuritegelike kavatsusega isikuid, kuid neil puuduvad teadmised, kuidas enda privaatsust mängusaitides nii kaitsta, et nende andmed ei jõuaks nende enda teadmata kolmandate osapoolteni. On leitud, et enamik lapsi, kes on kokku puutunud negatiivse võrgukogemusega otsivad abi enamasti sõpradelt või vanematelt (Smahel jt, 2020). Ka vestlustest selgus, et probleemide korral pöörduvad lapsed tavaliselt enda vanemate või sõprade poole. Et lapsed oskaksid erinevaid privaatsusega seonduvaid riske märgata ja nendega iseseisvalt toime tulla on oluline, et neil oleks head teadmised digitaalsest kirjaoskusest (Stoilova, 2020). Kui laste teadmised digitaalsest kirjaoskusest on head, siis suure tõenäosusega oskavad nad erinevate probleemidega ka iseseisvalt toime tulla.

Iseseivalt hakkama saamise soovi kinnitas see, et intervjueeritud lapsed tõid korduvalt välja, et neil on olemas huvi teada saada, miks nad mänguplatvormidele üldse enda andmeid sisestama

peavad ning kuhu need sisestatud andmed edasi liiguvad. Toodi välja, et paremaid teadmisi soovitakse sellest, kuidas enda privaatsust mänguplatvormidel kaitsta saaks ning kuidas vältida seda, et keegi pahade kavatsustega isik ei pääseks isiklikele andmetele ligi. Lisaks mainiti vestluse ajal isegi seda, et soovitakse paremaid teadmisi, kuidas enda IP-aadressi kaitsta ja kuidas saaks paremini tõlkida kasutustingimusi, et need oleksid arusaadavad. Seega on laste huvi, kuidas enda privaatsust ja andmeid internetis ja mängukeskkondades olles kaitsta, väga suur. Oluline on laste digitaalset kirjaoskust kasvatada ning teha seda võimalikult selgelt ja neile arusaadavalt.

KOKKUVÕTE

Laste seas on online mängud üha populaarsemaks saanud, kuid nendes keskkondades tuleb tihti ette, et mänguplatvormid rikuvad kasutajate privaatsust. Maailmas on online mängude privaatsuse teemale tähelepanu pööratud, Eestis minule teadaolevalt mitte. Eestis on uuritud ainult privaatsuse aspekti, mis puudutab sotsiaalmeediat üldiselt. Seega oli minu sooviks teada saada, mida tähendab teise kooliastme õpilaste jaoks privaatsus, milliseid ohte nad mänguplatvormidel enda privaatsusele näevad ning milliseid meetmeid nad ise kasutusele võtavad, et enda privaatsust online-keskkondades kaitsta.

Püstitasin lähtuvalt teemast küsimused, mis olid järgnevad:

- Milliseid online mänguplatvorme lapsed eelistavad?
- Kuidas lapsed mõistavad privaatsuse tähendust online mängukeskkondades?
- Millised ohte näevad lapsed enda privaatsusele online mänge mängides?
- Milliseid meetmeid lapsed ise kasutusele võtavad, et enda privaatsust online-keskkondades mängides kaitsta?

Kirjeldasin läbi teooriaosa olulisemaid mõisteid. Tulemuste saamiseks viisin läbi kümme poolstruktureeritud intervjuud lastega, kelle vanus oli 12- kuni 13aastat. Vestlused toimusid Zoom keskkonnas. Saadud tulemusi analüüsisin läbi kvalitatiivse sisuanalüüsi.

Intervjuude analüüs näitas, et lapsed eelistavad mänguplatvorme, mis on nende jaoks turvalised. Lisaks on mänguplatvormide valiku üheks kriteeriumiks ka mängude tasuta kättesaadavus. Online mänguplatvormidelt otsitakse pigem mänge, mis on intervjueeritavate huvidega seotud.

Privaatsuse osas selgitasid lapsed, et nende jaoks tähendab privaatsus seda, et keegi võõras ei pääse nende andmetele ligi ning nad ise ei jaga enda andmeid võõrastega. Privaatsust seostati ka isikliku ruumiga, kuhu ei tohiks teised tulla ja mis annab seal õiguse teha asju, mida teised ei näe.

Üldiselt peavad lapsed mänguplatvorme üsna turvaliseks ning nende jaoks ei ole sinna erinevate andmete sisestamine probleemiks. Laste arvates koguvad mänguplatvormid nende andmeid selleks, et aidata kontot turvalisena hoida. Küll aga luuakse tihti mänguplatvormidele varikontosid, et enda õigeid andmeid mitte sisestada. Vestlustest selgus, et lapsed näevad mänguplatvormidel ohte pigem teistes kasutajates, seetõttu on nad ka väga valvsad ja ettevaatlikud võõrastega suhtlemisel, kuna nad kardavad, et keegi võib nende konto kaaperdada. Lisaks kardavad lapsed, et kui nad enda kontot piisavalt hästi ei kaitse, siis võidakse ilma jääda mängus saavutatud tulemustest.

Lapsed ise soovivad aru saada, mida mänguplatvorm neile pakub. Kõik intervjueeritavad mainisid, et nad on vähemalt korra mänguplatvormil olevate kasutustingimustega tutvunud. Kuna privaatsussätted ei ole laste jaoks nähtaval koha, siis ei osanud enamus intervjueeritavatest öelda, mis need on ja kuidas need mängija andmeid kaitsta saaksid.

On oluline, et mänguplatvormid teeksid privaatsusega seonduva teabe lastele paremini nähtavaks. Lisaks on oluline, et kasutustingimused ja privaatsussätted oleksid mängijate jaoks arusaadavas keeles. Kahjuks on need tihti aga võõrkeelsed ning keerulises õiguskeeles, millest lastele on väga raske aru saada. Kindlasti peaksid ka koolid privaatsusega seonduvatel teemadel rohkem teavitustööd tegema ning seda lastele arusaadavalt ja lihtsalt. Tänapäeval on väga oluline, et lapsed oskaksid lehtedel näiteks privaatsussätteid muuta ning nad teaksid, miks on nende muutmine vajalik. Läbi viidud intervjuud kinnitasid, et lastel endil on privaatsusega seonduvate teemade vastu huvi väga suur, seega peaks neile soovitud teadmised ka võimaldama.

SUMMARY

Primary school students perceptions of privacy in online gaming environments

Online games have become increasingly popular for children. But in these environments, gaming platforms often violate users privacy. The issue of the privacy of online games has received attention in the world, in Estonia, as far as I know, not. We've only looked at the privacy aspect of social media in general. So I wanted to find out what privacy means to children, what kind of privacy threats they see on gaming platforms and what measures they take to protect their own privacy when playing online.

Based on the topic, I asked the following questions:

- Which online play platforms do children prefer?
- How do children understand the meaning of privacy in oline environments?
- What threats do children see to their privacy when playing online games?
- What measures do children take to protect their privacy when playing online?

To obtain the results, I conducted ten semi-structured interviews with children aged 12-13. The conversations took place in Zoom. I analyzed the obtained results through a qualitative content analysis.

The analysis of the interviews showed that children prefer gaming platforms that are safe for them. In addition, one of the criteria for choosing gaming platforms is that the games would be available for free.

Children explained about privacy that for them, privacy means that no one else has access to their data and they do not share their data with strangers. Privacy was also associated with a personal

space that others should not come in and that gives them the right to do things that others cannot see.

In general, children think that gaming platforms are quite secure and they have no probleem entering different data there. Children believe that gaming platforms collect their data to secure their accounts.. However, to avoid entering personal information, children often create shadow accounts. Conversations have shown that children tend to see other users as threats on gaming platforms, so they are also very vigilant and cautious when dealing with strangers, as they fear that someone may hijack their account. Children also fear that if they do not protect their account well enough, they may lose the results of the game.

The children want to understand what the gaming platform offers them. All children mentioned that they have read the terms of use on the gaming platform at least once. As the privacy settings are not in a visible place, most of the interviewees could not say what privacy settings are and how privacy settings could protect the player's data.

It is important that gaming platforms make privacy information more visible to children and that the terms of use and privacy policy are in a language that players can understand. Unfortunately, they are often in a complex legal language that is very difficult for children to understand. Certainly, schools should also talk more about privacy issues. Nowadays, it is very important that children know how to change the privacy settings, and that they know why it is necessary to change them. The interviews confirmed that the children are very interested in these topics, so they should be provided with the desired knowledge.

KASUTATUD KIRJANDUS

1. Abdel-Basset, M., Mohamed, M., Smarandache, F., ja Chang, V. (2018). Neutrosophic Association Rule Mining Algorithm for Big Data Analysis. *Symmetry, 10(4),* 1-19. Kasutatud 04.12.2021, https://www.mdpi.com/2073-8994/10/4/106
2. Adams, W. C. (2015). Conducting semi-structured interviews. *Handbook of practical program evaluation, 4,* 492-505. Kasutatud 04.11.2021, https://books.google.ee/books?hl=en&lr=&id=zntNhoO6gCUC&oi=fnd&pg=PA365&dq=semistructured+interviewing&ots=UogqA_fQRU&sig=hdrHJg3VQosbb8kY_jwKuCLotxw&redir_esc=y#v=onepage&q=semi-structured%20interviewing&f=false
3. Aluoja, L. (ia.). Digihügieen. Kasutatud 05.01.2021, https://courses.cs.ut.ee/t/digiopik/Digih%c3%bcgieen/Tund2
4. Andmekaitse Inspektsioon. (2017). *Suurandmed ja privaatsus*. Juhendmaterjal organisatsioonidele. Kasutatud 16.03.2022, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiEgrShtcr2AhWXvYsKHaq_BLkQFnoECA0QAQ&url=https%3A%2F%2Fwww.aki.ee%2Fsites%2Fdefault%2Ffiles%2Fdokumendid%2Fsuurandmed_ja_privaatsus.pdf&usg=AOvVaw2D2Ns76BGJKS3dt9LIwiGJ
5. Andmekaitse Inspektsiooni koduleht. (2019). *Isikuandmete liigitus*. Kasutatud 19.02.2022, https://www.aki.ee/et/eraelu-kaitse/isikuandmed-ja-tootlemine/isikuandmete-liigitus
6. Andmekaitse Inspektsiooni koduleht. (2019). *Isikuandmete töötleja üldjuhendi veebitekst.* Kasutatud 02.03.2022, https://www.aki.ee/et/isikuandmete-tootleja-uldjuhendi-veebitekst#peat%C3%BCkk4.4
7. Anniste, K., Biin, H., Osila, L., Koppel, K., ja Aaben, L. (2018). *Lapse õiguste ja vanemluse uuring 2018.* Kasutatud 08.10.2021, https://webcache.googleusercontent.com/search?q=cache:HUz1nNdCwVkJ:https://www.sm.ee/sites/default/files/lovu_lopparuanne_final_1.11.18.pdf+&cd=10&hl=et&ct=clnk&gl=ee&client=firefox-b-e
8. Arbeau, K., Thorpe, C., Stinson, M., Budlong, B., ja Wolff, J. (2020). The meaning of the experience of being an online video game player. *Computers in Human Behavior Reports,*

2, 1-6. Kasutatud 07.10.2021, https://www.sciencedirect.com/science/article/pii/S2451958820300130

9. Archibald, M.M., Ambagtsheer, R.C., Casey, M.G., ja Lawless, M. (2019). Using Zoom Videoconferencing for Qualitative Data Collection: Perceptions and Experiences of Researchers and Participants. *International Journal of Qualitative Methods, 18,* 1-8. Kasutatud 20.02.2022, https://www.proquest.com/docview/2405672296?pq-origsite=gscholar&fromopenview=true
10. Beke, F.T., Eggers, F., ja Verhoef, P.C. (2018). Consumer Informational Privacy: Current Knowledge and Research Directions. *Foundations and Trends in Marketing, 11(1),* 1–71. doi: 10.1561/1700000057
11. Berman, G., Albright, K. (2017). *Children and the Data Cycle: Rights and Ethics in a Big Data World.* Kasutatud 20.02.2022, https://arxiv.org/abs/1710.06881
12. Bryman, A., ja Bell, E. (2011). Business research methods. Kasutatud 03.11.2021, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjl-Zu_zIr0AhU5CRAIHcqrCIwQFnoECAMQAQ&url=https%3A%2F%2Fwww.uwcentre.ac.cn%2Fhaut%2Fwp-content%2Fuploads%2F2018%2F11%2FAlan_Bryman_Emma_Bell_Business_Research_Methodsb-ok.cc.pdf&usg=AOvVaw2mKAe12KUuKxXYkMSPlpNN
13. Chen, T.T. (2015). Online Games. *Computers in Entertainment, 11(4),* 1-26. Kasutatud 25.09.2021, https://www.researchgate.net/publication/273520045_Online_Games
14. Doneda, D., Almeida A.F, V., What Is Algorithm Governance. *IEEE Internet Computing, 20(4),* 60-63. Kasutatud 16.03.2022, https://www.researchgate.net/publication/305801954_What_Is_Algorithm_Governance
15. Evans, C. (2017). Analysing Semi-Structured Interviews Using Thematic Analysis: Exploring Voluntary Civic Participation Among Adults. *SAGE Publications Limited.* Kasutatud 04.11.2021, https://wiserd.ac.uk/sites/default/files/documents/Overview_1.pdf
16. Gerring, J. (2017). Qualitative Methods. *Annual Review of Political Science, 20,* 15-36. Kasutatud 21.11.2021, https://www.annualreviews.org/doi/abs/10.1146/annurev-polisci-092415-024158
17. Harrik, A. (2021). Meediauurija: laste andmed võivad jõuda suurfirmadeni juba enne nende sündi. Kasutatud 13.02.2021, https://novaator.err.ee/1608449861/meediauurija-laste-andmed-voivad-jouda-suurfirmadeni-juba-enne-nende-sundi

18. Hepp, A., ja Breiter, A. (2018). The Complexity of Datafication: Putting Digital Traces in Context. A. Hepp (toim), A, Breiter (toim), U. Hasebrink (toim), *Communicative Figurations* (lk 387-405). Saksamaa: Palgrave Macmillan
19. Justiitsministeeriumi koduleht. (i.a). Kasutatud 30.11.2021, https://www.just.ee/ministeerium-uudised-ja-kontakt/isikuandmete-tootlemine
20. Kalmus, V., Masso, A., ja Linno, M. (2015). *Sotsiaalse analüüsi meetodite ja metodoloogia õpibaas:* Kvalitatiivne sisuanalüüs. Kasutatud 04.11.2021, https://samm.ut.ee/kvalitatiivnesisuanalyys
21. Kalmus, V., Opermann, S., Tikerperi, M.-L. (2022). Eesti õpilaste digipädevus: ülevaade ySKILLS'i küsitlusuuringu 1. laine tulemustest. KU Leuven, Leuven: ySKILLS.
22. Kaplan, A., ja Haenlein, M. (2019). Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. *Business Horizons, 62(1),* 15–25. Kasutatud 16.03.2022, https://www.sciencedirect.com/science/article/pii/S0007681318301393?casa_token=x8pZdjizxaYAAAAA:ZCXkUPG-WAUnErLeV4X7kzPAm4HIzEoMmdoUfQ0Sh0LTpsTVxt-I6QUGwd8KokuUEZVgvwARexw
23. Kennedy, H., Oman, S., Taylor, M., Bates, J., ja Steedman, R. (2020). *Public understanding and perceptions of data practices: a review of existing research.* Kasutatud 22.09.2021, https://livingwithdata.org/current-research/
24. Kokolakis, S. (2017). Privacy attitudes and priv. acy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64,* 122-134. Kasutatud 17.02.2022, https://www.sciencedirect.com/science/article/pii/S0167404815001017?casa_token=yLyaUzlQWKkAAAAA:0Z0xuR3rbMnELX87hgjzoj9TawNPHlDqhXeMqqtgmzdvcKHAPLgtWr308n3vgBkpjqoZYbWeMaI
25. Kröger, J.L., Raschke, P., Campbell, J.P., ja Ullrich, S. (2021). *Surveilling the Gamers: Privacy Impacts of the Video Game Industry.* Kasutatud 25.09.2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3881279
26. Kumar, P., Vitak, J., Chetty, M., Clegg, T-L., Yang, J., McNally, B., ja Bonsignore, E. (2018). Co-Designing Online Privacy-Related Games and Stories with Children. *Proceedings of the 17th ACM Conference on Interaction Design and Children,* 67-79. Kasutatud 04.12.2021, https://dl.acm.org/doi/abs/10.1145/3202185.3202735?casa_token=DaDprFV4EJ8AAAA

A:l5SbL26ts8b1XYum1Xnl6Mlo9EJg6jPPJ4lPGwdy-fybJB2D_vyI-5XMkQEfaR3fX1Dx4te1y7qU6g

27. Law Insider kodulehekülg. (i.a). Kasutatud 07.10.2021, https://www.lawinsider.com/dictionary/game-platform
28. Lees, M. (2021). Ligi 300 000 inimese dokumendifoto, nimi ja isikukood sattusid häkkeri kätte. *Tartu Postimees*, 29. juuli. Kasutatud 15.12.2021, https://majandus.postimees.ee/7303029/ligi-300-000-inimese-dokumendifoto-nimi-ja-isikukood-sattusid-hakkeri-katte
29. Li, F., Li, H., Niu, B., ja Chen, J. (2019). Privacy Computing: Concept, Computing Framework, and Future Development Trends. *Engineering. 5(6),* 1179-1192. Kasutatud 07.10.2021, https://www.sciencedirect.com/science/article/pii/S2095809919308240
30. Liu, B., Zhou, W., Zhu, T., Gao, L., ja Xiang, Y. (2018). Location privacy and its applications: A systematic study. IEEE access, 6, 17606-17624. Kasutatud 05.01.2022, https://ieeexplore.ieee.org/abstract/document/8329504
31. Livingstone, S. (2018). Children: a special case for privacy?. *Intermedia, 46(2),* 18-23. Kasutatud 30.11.2021, http://eprints.lse.ac.uk/89706/
32. Livingstone, S., Blum-Ross, A., ja Zhang, D. (2018). What do parents think, and do, about their children's online privacy? Parenting for a Digital Future: Survey Report 3. Kasutatud 04.12.2021, http://eprints.lse.ac.uk/87954/
33. Livingstone, S., Davidson, J., Bryce, J., Batool, S., Haughton, C., ja Nandi, A. (2017). Children's online activities, risks and safety: a literature review by the UKCCIS evidence group. Kasutatud 15.12.2021, https://scholar.google.com/citations?view_op=view_citation&hl=en&user=vPvN_lgAAAAJ&cstart=100&pagesize=100&citation_for_view=vPvN_lgAAAAJ:ybfzIt2tCtgC
34. Livingstone, S., Stoilova, M., ja Nandagiri, R. (2019). Children's data and privacy online: growing up in a digital age: an evidence review. Kasutatud 17.01.2021, http://eprints.lse.ac.uk/101283/
35. Lorenz, B., Kikkas, K., Sõmer, T., Osula, K., ja Veldre, A. (2017). *Küberpähkli 2017 uuringu kokkuvõttes.* Kasutatud 08.10.2021, https://docs.google.com/document/d/18aBcXcDVC2uGMLsUFiky1wG0Vtr84JTTkI0PvCf3sVI/edit
36. Macenaite, M., ja Kosta, E. (2017). Consent for processing children's personal data in the EU: following in US footsteps?. *Information & Communications Technology Law, 26(2),*

146-197. Kasutatud 04.12.2021, https://www.tandfonline.com/doi/full/10.1080/13600834.2017.1321096

37. Makarova, E.A., ja Makarova, E.L. (2019). Aggressive Behavior in Online Games and Cybervictimization of Teenagers and Adolescents. *International Electronic Journal of Elementary Educattion, 12(2),* 157-165. Kasutatud 18.10.2021, https://eric.ed.gov/?id=EJ1240214
38. Martinovic, D., Ralevich, V., McDougall, J., ja Perklin, M. (2014). *"You are what you play": Breaching privacy and identifying users in online gaming.* Kasutatud 21.09.2021, https://ieeexplore.ieee.org/document/6890921
39. MaruVR koduleht. (i.a). Kasutatud 29.01.2022, https://maruvr.ee/virtuaalreaalsus-virtual-reality-miks-see-vajalik-ja-kuidas-seda-kasutada/
40. Mascheroni, G. (2020). Datafied childhoods: Contextualising datafication in everyday life Current. *Sociology Review, 68(6),* 798-813. Kasutatud 13.02.2022, https://journals.sagepub.com/doi/full/10.1177/0011392118807534?casa_token=OEcXP8JPzakAAAAA%3AjvxUXNkpINXIAP7_WLvQMoUBHurFhWPBsGj1IXBAvdaGljRfFC-3C-DDboMXR7TkhOPQAV2CyqFDedA
41. Masso, A., Tiidenber, K., ja Siibak, A. (2019). Kuidas uurida andmestunud ühiskonda?. *Sirp*, 26.07.2019. Kasutatud 13.02.2022, https://sirp.ee/s1-artiklid/c21-teadus/kuidas-uurida-andmestunud-uhiskonda/
42. Mayring, P. (2019). Qualitative Content Analysis: Demarcation, Varieties, Development. *Forum Qualitative Sozialforschung Social Research, 20.* Kasutatud 21.11.2021, https://www.qualitative-research.net/index.php/fqs/article/download/3343/4557?inline=1
43. Muhammad, S.S., Dey, B.L., ja Weerakkody, V. (2017). Analysis of Factors that Influence Customers' Willingness to Leave Big Data Digital Footprints on Social Media: A Systematic Review of Literature. *Information Systems Frontiers, 20,* 559-576. Kasutatud 13.02.2022, https://link.springer.com/article/10.1007/s10796-017-9802-y
44. Murumaa-Mengel, M., Pruulmann-Vengerfeld, P., ja Laas-Mikko, K. (2014). *PRIVAATSUSÕIGUS INIMÕIGUSENA JA IGAPÄEVATEHNOLOOGIAD.* Uuringu teoreetilised ja empiirilised lähtealused. Kasutatud 07.10.2021, https://www.humanrightsestonia.ee/wp/wp-content/uploads/2014/11/EST-Uuringu-III-osa-Uuringu-teoreetilised-ja-empiirilised-l%C3%A4htealused.pdf
45. Oja, T. (2017). Küberturvaekspert: lapsed võivad netikurjategijad juhatada oma vanemate andmeteni. *Pealinn*, 01. veebruar. Kasutatud 15.12.2021,

https://pealinn.ee/2017/02/01/kuberturvaekspert-lapsed-voivad-netikurjategijad-juhatada-oma-vanemate-andmeteni/

46. Pangrazio. L., ja Selwyn, N. (2019). 'Personal data literacies': A critical literacies approach to enhancing understandings of personal digital data. *New Media & Society, 21(2),* 420-437. Kasutatud 04.12.2021, https://journals.sagepub.com/doi/full/10.1177/1461444818799523?casa_token=CoGoxDmZ8hYAAAAA%3ACKsh4nyF4KX1zON_bC9vgSY_3o9qra4gzJ7_am1nGdC2zex8zHkbaPl7QDYUWWnzeMpfRvLTCsjoMA
47. Põhikooli riiklik õppekava (06.01.2011). *Riigi Teataja.* Kasutatud 02.11.2021, https://www.riigiteataja.ee/akt/123042021010?leiaKehtiv
48. Isikuandmete kaitse seadus. (2007). *Isikuandmete kaitse seadus/uudis.* Kasutatud 02.03.2022, https://www.riigiteataja.ee/oigusuudised/eelvaadeSeadusUudis/303
49. Isikuandmete kaitse üldmäärus. (2016). *Euroopa Liidu Teataja I.* Kasutatud 04.04.2022, https://gdprinfo.eu/et
50. Rubio-Manzano. C., ja Trivino, G. (2016). Improving player experience in Computer Games by using players' behavior analysis and linguistic descriptions. *International Journal of Human-Computer Studies, 95,* 27-38. Kasutatud 18.10.2021, https://www.sciencedirect.com/science/article/abs/pii/S1071581916300763?casa_token=Fa4xr5idZHwAAAAA:BM3B5fYw-LiSNClj-BQvRVKHjapSQTNYl170h-5XN-e7OlLgzBMLjUtYgGJba42CKICBVddcmvs
51. Russel, C.N., Reidenberg, J.R., ja Moon, S. (2018). Privacy in Gaming. *Fordham Intellectual Property, Media and Entertainment Law Journal, 29(1), 61-180.* Kasutatud 22.09.2021, https://heinonline.org/HOL/P?h=hein.journals/frdipm29&i=70
52. Saar, S., Himma, M., ja Kooli, R. (2019). Digivahendid suurendavad lapsevanemate ärevust. Kasutatud 13.02.2022, https://novaator.err.ee/994957/digivahendid-suurendavad-lapsevanemate-arevust
53. Sanders, B. G. (2016). *Opportunities and Risks in Online Gaming Environments.* Kasutatud 23.09.2021, https://pearl.plymouth.ac.uk/handle/10026.1/8083
54. Sanders, B., Dowland, P., Atkinson, S., Zahra, D., Furnell, S., ja Papadaki, M. (2010). *Online Addiction: A Cultural Comparison of Privacy Risks in Online Gaming Environments.* Kasutatud 09.10.2021, https://www.researchgate.net/publication/220884165_Online_addiction_Privacy_risks_in_online_gaming_environments

55. Scneble, C.O., Favaretto, M., Elger, B.S., Shaw, D.M. (2021). Social Media Terms and Conditions and Informed Consent From Children: Ethical Analysis. *JMIR pediatrics and parenting, 4(2).* Kasutatud 02.03.2022, https://pediatrics.jmir.org/2021/2/e22281/
56. Shi, J., Renwick, R., Turner, N.E, ja Kirshk, B. (2019). Understanding the lives of problem gamers: The meaning, purpose, and influences of video gaming. *Computers in Human Behavior, 97,* 291-303. Kasutatud 18.10.2021, https://www.sciencedirect.com/science/article/pii/S0747563219301153
57. Siibak, A. (2019). Digiühiskonnas andmestunud laps. *Ajakiri Märka Last,* 05.02.2019. Kasutatud 13.02.2022, https://ajakiri.lastekaitseliit.ee/2019/02/05/digiuhiskonnas-andmestunud-laps/
58. Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Olafsson, K., Livingstone, S., ja Hasebrink, U. (2020). EU Kids Online 2020. *Survey results from 19 countries.* Kasutatud 08.10.2021, https://www.lse.ac.uk/media-and-communications/research/research-projects/eu-kids-online/eu-kids-online-2020
59. Stoilova, M., Livingstone, S., ja Nandagiri, R. (2020). Digital by Default: Children's Capacity to Understand and Manage Online Data and Privacy. *Media and Communication, 8(4),* 197- 207. Kasutatud 23.09.2021, http://eprints.lse.ac.uk/id/eprint/107114
60. Sukk, M., ja Soo, K. (2018). *EU Kids Online'i Eesti 2018. aasta uuringu esialgsed tulemused.Kalmus, V., Kurvits, R., Siibak, A. (toim). Tartu: Tartu Ülikool, ühiskonnateaduste instituut.* Kasutatud, 24.09.2021, https://sisu.ut.ee/euko/avaleht
61. Tallinna Tehnikaülikool. (i.a). *Veebipõhine kõnetuvastus.* Kasutatud 20.02.2022, http://bark.phon.ioc.ee/webtrans/
62. Vaher-Torni, S. (2019). *Laste privaatsusõiguste tagamine sotsiaalmeedias.* Magistritöö. Kasutatud 24.09.2021, https://digikogu.taltech.ee/en/Download/b23bb262-7dd6-4374-adba-4bed6e771b14
63. Vallejo, M.G, Munoz, G.E., ja Rosales, J.H. (2018). Kids and Parents Privacy Exposure in the Internet of Things: How to Protect Personal Information?. *Computación y Sistemas, 22(4),* 1191–1205. Kasutatud 15.12.2021, http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1405-55462018000401191
64. Vervier, L., Zeissig, E., Lidynia, C., ja Ziefle, M. (2017). Perceptions of Digital Footprints and the Value of Privacy. *InIoTBDS,* 80-91. Kasutatud 13.02.2022, https://pdfs.semanticscholar.org/6ab9/c92d968d6b588ab264f750fe33beac704c8f.pdf

65. Williams, M., Nurse, J.R.C., ja Creese, S. (2019). (Smart)Watch Out! encouraging privacy-protective behavior through interactive games. *International Journal of Human-Computer Studies, 132,* 121-137. Kasutatud 18.10.2021, https://www.sciencedirect.com/science/article/pii/S1071581918301587?casa_token=j2eihZxETL8AAAAA:Saeol0Yw8wm6XNDbz5wqFFuf71QR3iUF6ygdi6qsewRUordG1PdoqZl0KaMS6d-xSs4bO7FnkgA
66. Yannakakis, G.N., ja Togelius, J. (2018). *Artificial Intelligence and games.* Saksamaa: Springer Nature

LISAD
Lisa 1 Nõusoleku vorm

LASTE PRIVAATSUS ONLINE MÄNGUKESKKONDADES

Lugupeetud lapsevanem!

Minu nimi on Liisa Asso ning õpin Tartu Ülikoolis, infokorralduse erialal. Olen koostamas lõputööd, mille teemaks on „Laste privaatsus online mängukeskkondades“, juhendajaks Maris Männiste.

Palun nõusolekut Teie lapsel osaleda uuringus, mille käigus soovin välja selgitada, kui teadlikud on lapsed ohtudest privaatsusele, kui nad mängivad online keskkondades, ning milliseid meetmeid võtavad nad ise kasutusele, et oma privaatsust kaitsta. Töö jaoks on oluline kaardistada laste hoiakuid ja teadmisi nimetatud teema osas.

Uuringu käigus intervjueerin [redacted] õpilasi. Kogutud informatsiooni kasutatakse teadustööks ega jagata kolmandate osapooltega. Intervjuudes välja toodud informatsioon on lõputöös üldistatud ning esitatud anonüümsel kujul. Intervjuude transkriptsioone hoian turvaliselt, need on kättesaadavad ainult mulle ning töö juhendajale. Intervjuu toimub Zoom keskkonnas, ning see on hilisema töö lihtsustamiseks salvestatud. Salvestised kustutan kohe peale intervjuu transkribeerimist. Intervjuul osalemiseks sobiva aja lepin iga lapsega individuaalselt kokku.

Kui otsustate osaleda, siis hindan Teie lapse panust valmivasse töösse. Nõusoleku korral on vajalik, et täidaksite alloleva vormi ning edastaksite selle mulle e-posti teel [redacted].

Kinnitus

Kinnitan, et olen informeeritud ülalmainitud uuringust ja ma olen teadlik läbiviidava teadustöö eesmärgist ja andmekogumise metoodikast ja kinnitan oma nõusolekut selles osalemises (digi)allkirjaga. Allkirjastatud nõusoleku vormi võib edastada e-mailile [redacted].

Küsimuste korral võtke palun ühendust e-maili [redacted] või telefoni teel [redacted]

Lugupidamisega

Liisa Asso

LAPSEVANEMA NÕUSOLEKU VORM

Õpilase nimi ……..

Lapsevanema nimi …….

- Nõustumisel valige „Jah“, keeldumise korral valige „Ei“.

Nõustun, et minu laps osaleb uuringus, mille teemaks on „Laste privaatsus online mängukeskkondades“.

☐ ☐

Jah **Ei**

Mind on informeeritud nimetatud uuringust ja seega olen ma teadlik planeeritava töö eesmärgist ja metoodikast.

☐ ☐

Jah **Ei**

Nõustun, et salvestatud intervjuudest kogutud andmeid kasutatakse ainult nimetatud uuringu tarbeks.

☐ ☐

Jah **Ei**

Olen teadlik, et minu lapsel on igal hetkel võimalus uuringus osalemisest loobuda, ning sellega ei kaasne mingeid tagajärgi.

☐ ☐

Jah **Ei**

Lapsevanema allkiri ……

Kuupäev ……...

E-post või muu kontakt, mille kaudu oleks võimalik vestluseks sobiv aeg kokku leppida ……...

Lisa 2 Intervjuu kava

Minu nimi on Liisa Asso ning õpin Tartu Ülikoolis, infokorralduse erialal. Olen koostamas lõputööd, mille teemaks on „Laste privaatsus online mängukeskkondades“.

Soovin välja selgitada, kui teadlikud on lapsed ohtudest privaatsusele, kui nad mängivad online keskkondades ning milliseid meetmeid võtavad nad ise kasutusele, et oma privaatsust kaitsta. Töö jaoks on oluline kaardistada laste hoiakuid ja teadmisi nimetatud teema osas.

Kogutud informatsiooni kasutan teadustööks ega jaga seda kolmandate osapooltega. Intervjuudes välja toodud informatsioon on lõputöös üldistatud, ning esitatud anonüümsel kujul, seega pole siin räägitud juttu võimalik sinuga kokku viia. Intervjuude aluseks on lastevanemate kirjalikud nõusolekud.

Intervjuus osalemine on vabatahtlik, kui sa tunned, et sa ei soovi mõnele küsimusele vastata, siis palun anna sellest teada. Lisaks on sul võimalus intervjuu katkestada igal hetkel, kui sa seda soovid.

Teemaplokk	Küsimus
Sissejuhatav osa	Kui palju veedad sina tavaliselt internetis aega? Mis sa arvad, kuhu sul läheb kõige rohkem aega?
	Mis on tegevused, mida sulle kõige meelsamini meeldib internetis teha?
	Mida sa peamiselt internetis käimiseks kasutad – nutitelefoni, arvutit või mõnda muud seadet?
	On sul olemas oma isiklik arvuti või nutitelefon, mida selleks kasutada saad?
	Meeldib sulle internetis pigem üksi toimetada või kellegiga koos?
	Mida sulle meeldib üksi pigem teha ja mida teistega koos? Miks?

	Selgitan online mängu olemust, et lapsed saaksid aru, mis on online mäng.
Mängudega seonduv	Kui suure osa päevast sa kulutad online mängude peale?
	Milliseid seadmeid kasutad sa online mängude mängimiseks?
	Milliseid mängukonsoole sa mängimiseks kasutad?
	Milliseid mängusaite sa veebis mängimiseks kasutad?
	Mida sa jälgid mängusaiti valides? /Mis on sinu jaoks oluline mängusaiti valides?
	Milliseid andmeid mängusaidid sinult küsivad? Mis sa sellest arvad?
	Millised andmed on kohustuslikud, mis sul sisestada tuleb?
	Kuidas sa enda jaoks sobivaima kasutajanime leiad?
	Milliseid varjunimesid kasutad sa mängusaitidel? /Mille järgi selle valid?
	Suhtled sa vahel nende kasutajatega, kellega mängid ka väljaspool mängusaite?
	Mis kanalit suhtlemiseks kasutate?
	Miks just selline eelistus?
	Oled sa sattunud mängima ka kellegiga, keda sa koolist või trennist ei tea ja kes elab üldse kusagil teises riigis?
	Kuidas see kogemus on olnud?
	Milliseid tegevusi ei saa mänguplatvormidel teha? Miks?

Privaatsusega seonduv	Mida tähendab sinu jaoks privaatsus, kirjelda seda enda sõnadega?
	Kuidas enda privaatsust online mängudes kaitsta? Kelle käest sa selles osas infot saanud oled?
	Kui palju Teile räägitakse koolis privaatsusega seonduvatel teemadel?
	Millal viimane selline tund/ülevaade oli/tehti?
	Oled sa tutvunud tingimustega, mida mängusait palub ennem nõustumist lugeda?
	Mis sul sellest meelde jäänud on?
	Mis on privaatsussätted? Kas oled proovinud mõnikord saidil, mida külastad, privaatsussätteid muuta?
	Millises kohas asuvad privaatsussätted ja kasutustingimused online mängusaitidel?
	Millised on teadmised ja oskused online mängude privaatsusega seoses, mille osas sa sooviksid paremaid teadmisi?
Andmete kogumine	Mis sa arvad, milliseid andmeid need külastavavad mängusaidid sinu kohta koguvad?
	Mis sa sellest arvad, et need mängusaidid sinu kohta selliseid andmeid koguvad?
	Milliseid andmeid sa ei sooviks mängusaitidele enda kohta jagada aga sa pead selleks et mängida?
	Mis sa teed selleks, et sa ei peaks neid andmeid jagama? Mida täpsemalt?

	Mida saaksid sina teha selleks, et online mängude mängimine sinu jaoks ohutu oleks?
	Kuidas sa tuvastad, milline külastatud leht pole turvaline?
	Millised küsimused sul tekkisid seoses andmete kogumisega online mängukeskkondades?
Lõpetamine	Milliseid teemasid ma veel käsitlenud ei ole?
	Mille osas tekkisid küsimused?

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, Liisa Asso

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose „Põhikooliealiste arusaamad privaatsusest online mängukeskkondades“, mille juhendaja on Maris Männiste, 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.

Liisa Asso

20.05.2022