

TARTU ÜLIKOOL
Sotsiaalteaduste valdkond
Ühiskonnateaduste instituut
Infokorralduse õppekava

Gajane Veeroja
Eesti üldhariduskoolide inglise keele õpetajate kogemus õpilaste andmetega e-
keskkondades
Lõputöö

Juhendaja: Katrin Kannukene, MA

Tartu 2023

SISUKORD

SISSEJUHATUS.....	3
1 TEOREETILISED JA EMPIIRILISED LÄHTEKOHAD	6
1.1 Andmestumine hariduses	6
1.2 Õpetajate teadmised ja kogemused andmekaitse, andme-eeetika ja privaatsusega	8
1.3 Õpilaste andmete privaatsuse kaitsmise olulisus.....	11
1.4 Uurimistöö eesmärk ja uurimisküsimused	13
2 MEETOD JA VALIM.....	14
2.1 Valimi moodustamine	14
2.2 Andmete kogumine	15
2.3 Andmete analüüs.....	16
3 TULEMUSED.....	18
3.1 E-keskkonnad ja nende valiku põhjused	18
3.2 Õpetajate tegevused õpilaste andmetega ja nende kaitsmiseks.....	21
3.3 Õpetajate teadmised ohtudest e-keskkondades ning andmekaitsest.....	23
4 JÄRELDUSED JA DISKUSSIOON	26
4.1 Järeldused ja diskussioon	26
4.2 Meetodi kriitika.....	33
KOKKUVÕTE.....	35
SUMMARY	37
KASUTATUD KIRJANDUS	39
LISAD	47
Lisa 1 Nõusoleku vorm	47
Lisa 2 Poolstruktureeritud intervjuu kava	48

SISSEJUHATUS

Andmete kasvav kättesaadavus koos võimsama töötlemisega loob uusi võimalusi ühiskonnaelu mõõtmiseks, salvestamiseks, kirjeldamiseks ja esitamiseks numbrites (Jarke ja Breiter, 2019: 1; Going..., 2019; Sarker, 2021: 1). Haridussektor on üks silmapaistvamaid andmetööstlusest mõjutatud valdkondi ning nende kogutavad ja töödeldud andmed on olulised ja mahult väga suured (Jarke ja Breiter, 2019: 1; Using data..., 2023).

Seda, et ka Eesti haridussektor on suuresti mõjutatud andmetööstlusest ja sellega kaasnevatest reeglitest, näitab kauaaegne ja laialdane andmete kogumine eri registritesse (Eesti Hariduse Infosüsteem, e-kool, Stuudium, rahvastikuregister, Haridussilm, Haridusportaal jne). Eesti Haridus- ja Teadusministeeriumi (edaspidi HTM) üldine eesmärk on tugevdada andmetel põhinevat otsuste tegemist hariduses läbi hariduse seiresüsteemi täiustamise, kuna andmete ja indikaatorite kasutamist on peetud Eesti hariduse 2035. aasta strateegia elluviimise oluliseks komponendiks (Enhancing..., 2021: 1).

Hiljutine pandeemia tõukas tagant hariduse digitaliseerimist kommertsharidustehnoloogia järsult suurenenud levikuga, mis on võimaldanud hariduses pidevat andmete genereerimist (Hillman, 2022: 122; Arantes ja Buchanan, 2022). Digiplatvormide roll haridusprotsessides on tähelepanu saanud kriitilistes platvormiuuringutes, infrastruktuuri- ning teaduse ja tehnoloogia uuringutes. (Robinson, 2022). Leitud on, et tehnoloogiliselt saavad kolmandatest osapooltest äriüksused koguda ja salvestada haridusandmeid oma serverites ja andmeladudes, mistõttu haridusasutused ei suuda andmete kasutamist kontrollida (Hillman, 2022: 122; Torchia, 2023) ning hariduspoliitika ei suuda tehnoloogiliste arengutega sammu pidada (Arantes ja Buchanan, 2022: 1).

Seega on selge, et haridustehnoloogia kasutamine on toonud kaasa töödeldavate õpiandmete plahvatusliku kasvu. Kuid õpetajate teadmised ja oskused haridusliku tehnoloogia osas on ebapiisavad (Mandinach ja Cotto, 2021; Arantes ja Buchanan, 2022). Õpetajad teevad tehnoloogiaga seonduvaid

otsuseid, teadmata, kuidas need mõjutavad seda, milliseid õpilaste andmeid kogutakse või avalikustatakse, kuidas andmeid salvestatakse ning kuidas andmeid tõlgendatakse ja õpilaste kohta otsuste tegemiseks kasutatakse (Mandinach ja Cotto, 2021; Using data..., 2023). .

Eesti õpetajad tunnistavad ka ise, et nende digioskused vajavad täiendamist, ehkki lausa 95% õpetajatest kasutavad õppetöös korrapäraselt digilahendusi (Haridus -ja Teadusministeerium, 2019). Kuigi digiõpe on olnud alates 2016. aastast õpetajate täiendõppes kesksel kohal (Education..., 2020: 14), tuleb Andmekaitse Inspeksiooni (edaspidi AKI) (2020) andmetel koolides sageli ette olukordi, kus töötajad ei tea, milline on õige käitumisviis ning seetõttu võib juhtuda, et õpilaste andmeid avaldatakse kas valesti (õpilase pilt kooli kodulehel ilma nõusoleku küsimiseta, kuhugi kaasatud või kuskilt eemaldatud õpilaste nimed suuremas grupivestluses jmt) või jäetakse vajalik info ilma mõjuva põhjuseta avaldamata.

Mitmed maailmas ja võib oletada, et ka Eestis populaarsemad e-keskkonnad kasutavad õpianalüütikat. Näiteks õpperakendused ja platvormid, mis selle abil pakuvad ülevaadet õpilaste õppimisest ja annavad õpilastele või õpetajatele soovitusi (Arantes, 2019). Õpianalüütika süsteemide eesmärk on analüüsida, millised tegurid ennustavad empiirilisel õpilaste tulemusi (Arantes, 2019; Rethinam, 2014). Eestis pole täpset statistikat, mil määral ning milliste tegevustega õpetajad, kas teadlikult või sellest ise aru saamata, taoliste süsteemidele andmestikku toodavad, toetavad või kasutavad.

Õpetajate suunamisel haridustehnoloogiat kasutavad põhikooli õpilased seisavad silmitsi mitmete küberturvalisuse ja privaatsusega seotud ohtudega (Chanenson jt, 2023) nagu nende isikut tuvastava teabe, biomeetriste andmete, akadeemilise teabe, geograafilise asukoha, veebibrauseri ajaloo, IP-aadresside, samuti õpilaste käitumis-, distsiplinaar- ja meditsiinilase teabe võimalik avaldamine (Understanding..., 2020; Gebhart, 2017: 27). Minu 10 aastane poeg peab õppetöös kasutama mitmeid erinevaid e-keskkondi ja tunnen muret, kuidas andmestumine võib teda mõjutada.

Arvestades, et suur osa õpetaja tööst on seotud õpilaste andmetega, on oluline, et õpetajad omaksid teadmisi privaatsusega seotud probleemide lahendamiseks, oleksid õpilaste andmete kogumise, kasutamise ja kaitsmise osas hästi informeeritud ning suudaksid toetada ka õpilaste teadlikkuse kasvu nende andmete kaitsmisel. On oluline küsida, milline on õpetajate kogemus õpilaste andmete kaitsmise ja privaatsusega e-keskkondades, et mõista paremini teema kitsaskohti, aga ka võimalusi. Suur osa vabavaralistest e-keskkondadest võimaldavad õpetada inglise keeles (E-õppe..., 2017) või inglise keelt, seega on inglise keele õpetajatel lai valik erinevate e-keskkondade vahel. Lisaks on

ingliseelsete õppematerjalidega kaasa tulevad e-keskkonnad juba aastaid kasutuses olnud (Pata ja Laanpere, 2009: 118), mistõttu võib oletada, et inglise keele õpetajatel on mitmekülgseid pikemaajalisi kogemusi e-keskkondadega.

Eelnevast lähtudes on töö eesmärgiks välja selgitada üldhariduskoolide inglise keele õpetajate teadlikkus isikuandmete kaitse põhimõtetest ja nende rakendamisest e-keskkondade valikul ja kasutamisel. Olukorra kaardistamine on oluline, sest õpetajate teadmised ja praktikad võivad mõjutada nende andmepõhiseid otsuseid ning edasi antavaid teadmisi ja seeläbi nende õpilaste elusid praegu ja tulevikus.

Lõputöö koosneb neljast osast. Esimeses osas kirjeldan andmetöötluse mõju haridussüsteemile, õpetajatele ja õpilastele, kirjutan õpetajate teadmistest ja kogemustest andmekaitse, privaatsuse, e-õppe platvormide ning õpianalüütikaga ja selgitan õpilaste andmete privaatsuse kaitsmise olulisust. Esimese osa lõpus toon välja uurimisprobleemi ning püstitatud uurimisküsimused. Lõputöö teises osas tutvustan meetodit ja valimit. Kirjeldan valimi moodustamist, andmete kogumist ja kogutud andmete analüüsimist. Kolmandas osas toon välja uurimistöö tulemused ning neljandas osas teen saadud tulemuste ja teooriosa põhjal olulisemad järeldused.

Tahan avaldada südamest tänu oma lõputöö juhendajale Katrin Kannukesele, asjatundliku juhendamise, kannatlikkuse ja vankumatu toetuse eest kogu lõputöö kirjutamisprotsessi vältel. Tänan ka intervjuueeritavaid, sest nende osaluse tõttu sai see töö võimalikuks. Lisaks tänan enda perekonda, eriti oma poega, kes innustasid mind igal sammul andma endast parima.

1 TEOREETILISED JA EMPIIRILISED LÄHTEKOHAD

Teooria peatükis kirjeldan erinevatele allikatele tuginedes andmetöötuse mõju haridussüsteemile, õpetajatele ja õpilastele; õpetajate teadmisi ja kogemusi andmekaitsest, privaatsusest, e-õppe platvormidest ning õpianalüütikast. Lisaks toon välja, miks on oluline õpilaste andmete privaatsust kaitsta ning millised on tagajärjed, kui seda ei tehta.

1.1 Andmestumine hariduses

Andmestumine (*datafication*) on protsess, mille käigus subjektid, objektid ja tavad muudetakse digitaalseteks andmeteks, mis on masinloetavad ja mõõdetavad, andmete koondamise ja analüüsimise eesmärgil (Southerton, 2020). Southerton (2020) ütleb, et tegemist on loogikaga, mis näeb maailmas asju kui andmeallikaid, mida korrelatsioonide jaoks "kaevandada" või müüa, ning millest on võimalik saada teadmisi inimkäitumise ja sotsiaalsete probleemide kohta. See laiaulatuslik andmejälgimise süsteem, üksikisikute tegevust ja suhtlust kajastavate andmete süstemaatiline jälgimine, võib tekitada pideva jälgimise tunde, mis võib takistada inimesi lubatud või isegi sotsiaalselt soovitatavast käitumisest (Büchi jt, 2022: 2) ning on ohuks inimeste privaatsusele (Connolly ja Fox, 2017: 1522).

Paljudes ühiskondades on digitaalne meedia muutunud kõige mugavamaks vahendiks igapäevastes toimingutes, näiteks teabe otsimine või ideede vahetamine (Büchi jt, 2022: 2). Lisaks aktiivsele sisu loomisele loob ainuüksi võrgus olemine püsivaid digitaalseid jälgi ja andmeid (Büchi jt, 2022: 2). Selliste andmete (kasutatava seadme-, asukoha-, logi-, konto-, tehingute jpm) kasvav kogumine ja analüüs (Dijck, 2014: 198) on automatiseeritud, pidev, odav ja läbipaistmatu.

Suurandmed on tööstuses ja akadeemilistes ringkondades trendikas termin (Shehab jt 2021: 25; Cao, 2017: 1). See on termin, mida kasutatakse, et kirjeldada suuri ja keerulisi andmekogumeid, mis oma suuruse tõttu nõuavad kogumiseks, analüüsimiseks, haldamiseks ja salvestamiseks keerukate algoritmide ja võimsate arvutussüsteemide olemasolu (Shehab jt 2021: 25; Abdel-Basset jt, 2018: 1). Andmeanalüütika viitab andmekogumite uurimise protsessile, et teha järeldusi neis sisalduva teabe kohta, sageli eesmärgiga parandada mingeid protsesse või teha otsuseid (Cao, 2017: 2; Hariri jt, 2019: 2; Abdel-Basset jt, 2018: 2). Andmeanalüütikat saab kasutada trendide tuvastamiseks, prognooside tegemiseks ja mustrite või kõrvalekallete tuvastamiseks suurtes andmekogumites (Cao, 2017: 14; Hariri jt, 2019: 2).

Suurandmete töötlustehnikate rakendamine õppimise parandamiseks on õpianalüütika (Clow, 2013: 684). Long ja Siemens (2011: 33) defineerivad õpianalüütikat kui õppija andmete analüüsimist ja esitlemist eesmärgiga mõista ja hallata õppimist ja õppimise keskkonda. Suurandmete algoritmiline analüüs toob kaasa algoritmilise kallutatuse, mis alles hiljuti pälvis haridustöötajate tähelepanu (Arantes, 2019). Algoritmilist kallutatust võib kirjeldada kui korduvat süsteemset viga analüüsis, millest on mõjutatud analüüsi tulemused ja selle pealt tehtavad otsused (Arantes, 2019). Kuivõrd suurandmete töötlustehnikaid rakendatakse ka õppimises, siis võib oletada, et algoritmiline kallutus esineb ka õpianalüütikas.

Andmetöötlus võib aidata haridusasutustel paremini mõista oma õpilaste vajadusi ja parandada oma teenuseid ning anda õpetajatele reaajas tagasisidet õpilaste soorituste ja edusammude kohta, võimaldades neil kiiresti sekkuda ja vastavalt vajadusele oma tegevust kohendada (Using data..., 2023). Negatiivse külje pealt võimaldab andmetöötlus erinevaid rikkumisi. Kuna töödeldakse nii palju andmeid, on tõenäoline, et need võivad sattuda pahatahtlikele osapooltele ja neid kasutatakse konfidentsiaalsele teabele juurdepääsu saamiseks. See võib kaasa tuua identiteedivargusi, juriidilisi tagajärgesid või muid kuritegusid, samuti kahjustada mainet (Macenaite ja Kosta, 2017: 146; Day jt, 2022: 3).

Day jt (2022: 1) sotsiaal-juriidiline analüüs, mis käsitleb lastelt koolis õpetamise ja õppimise eesmärgil kogutud andmeid, leidis, et kuigi andmete kogumist reguleerib valitsuse loodud raamistik, on mõned probleemsed erandid. Vajadus tervikliku haridusandmete haldamise järele – regulatsioon selle kohta, kes milliseid andmeid kogub, kuidas ja miks neid kasutatakse – kasvab jätkuvalt (Day, 2021). Haridusandmete kasutamise tavadele ei tehta eetilist kontrolli ja isiklikul tasandil pole õpilastel

nende tavade suhtes mingit sõnaõigust (Hillman, 2022: 123). Teisisõnu puudub ühtne ja sisuline järelevalve- ja andmehaldusraamistik, mis tagaks vastutustundliku andmete kasutamise üha digitaliseerivas haridussektoris (Day, 2021; Jim ja Chang, 2018). Õiguslikud raamistikud saavutavad andmete hallatavuse vaid osaliselt, kuna haridustehnoloogia ettevõtted jätkavad olemasolevate lünkade ärakasutamist (Palfrey jt, 2020: 1). Day jt (2022: 1) leidsid, et koolidel on vähe mehhanisme ja ebapiisavad teadmised või vahendid, et panna haridustehnoloogia pakkujad laste andmete töötlemise eest vastutama, samas on haridustehnoloogia pakkujatel seaduste tõlgendamisel märkimisväärne vabadus.

Eelneva põhjal võib väita, et andmestumine on suur osa haridussektorist. Andmestumise tagajärjel jäävad õpilastest e-keskkonnadesse maha püsivaid digitaalsed jäljed ja andmed ning haridusasutused ei suuda tagada nende andmete kaitsmist või neid andmeid hallata. Andmestumine võib hariduses olla probleemiks kuna see võib viia selleni, et otsuste tegemisel tuginetakse vaid andmetele, selle asemel, et keskenduda konkreetse õpilase vajadustele. Lisaks võib andmestumine põhjustada privaatsusprobleeme, kuna andmeid saab kasutada õpilaste profiileerimiseks ja teatud rühmade sihtimiseks. Seega on selge vajadus reguleeritud ja tervikliku haridusandmete haldamise järele.

1.2 Õpetajate teadmised ja kogemused andmekaitse, andme-eetika ja privaatsusega

Infoühiskonnas on andmekaitse väga olulisel kohal ning sellega puutuvad kokku peaaegu kõik asutused ja inimesed (Mäe, 2016). Üks eriti haavatav sihtgrupp andmekaitse vaatepunktist on lapsed ja noorukid (Day, 2022). Kuivõrd suur osa laste ja noorte ajast kulub õppetegevusele, siis võib eeldada, et haridusasutused ning nende töötajad, seal hulgas õpetajad, mängivad õpilaste andmete kaitsmisel olulist rolli. Õpetajad seisavad oma tööelus silmitsi märkimisväärse ja kasvava survega, sest nad kogevad aina suurenevat välist kontrolli selle üle, mida ja kuidas nad õpetavad (Stevenson, 2017: 537). AKI (2020) ütleb, et andmekaitse ei tohi saada õpetamisel takistuseks, kuid Student Privacy Compass (i.a) hinnangul mõjutavad hariduse andmestumise muudatused õpetajaid ainulaadselt ja just õpetajatel on õpilaste andmete privaatsuse kaitse tagamisel selge roll. Selle tõttu ei pea pedagoogid mitte ainult saama koolitust õpilaste privaatsusega seonduva seadusandluse teemal,

vaid ka mõistma, kuidas seaduste järgimine konkreetselt nende rollide suhtes kehtib ning kuidas kasutada õpilaste andmeid vastutustundlikult ja eetilisel (Student..., i.a.).

Õpetajate isikuandmete kaitse üldmäärusega (2016) (edaspidi IKÜM) seonduvad teadmised võttis üldisemalt Eestis vaatluse alla Küberpähkli uuring (Lorenz jt, 2020), kus viidi läbi ankeetküsitlus 13 136 õpilasega 4.-9. klassidest nii vene- kui eestikeelsetes õppekavades. Sellest selgus, et isikuandmetega toimetamise põhimõtteid ei tunne hästi ei õpilased ega õpetajad. Lorenz jt (2021) toovad näite sellest, kuidas õpilase parool avalikustatakse. Nimelt on juhtum, kus õpetaja kasutab õpilase kasutajanime ja parooli näitamist kui distsiplineerivat vahendit õpilase korrale kutsumiseks veebitunni ajal. Lorenz jt (2021) lahkavad seda juhtumit Õpetajate Lehes ning leiavad, et selline käitumine on vale eetiliselt (võimu kuritarvitamine), juriidiliselt (tundlike andmete avaldamine omaniku loata) ning ka tehnilises mõttes – kooli kontekstis võib ühe kasutaja andmete lekkimine seada ohtu kogu kooli infosüsteemi. Lisaks võib see tekitada küberkiusamise klassikaaslaste poolt, sest neil tekib võimalus erinevatesse süsteemidesse sisse logida teise õpilase andmetega, ka on selline käitumine halb eeskuju (Lorenz jt, 2021).

Teine näide (Lorenz jt, 2021) on liikumistund koos pereliikmetega, kus õpetaja soovib oma isiklikule e-posti aadressile pilte, videoid, liikumislogisid ja kirjeldusi. Lorenz jt (2021) toovad välja, et Eesti Vabariigi põhiseaduse § 26 sätestab, et igapähe on õigus perekonna- ja eraelu kaitsele ning ÜRO laste õiguste konventsiooni artikkel 16 sätestab, et mitte ühegi lapse eraellu, perekonnaellu ega kirjavahetusse ei või meelevaldselt ega ebaseaduslikult sekkuda, samuti ei tohi ebaseaduslikult rünnata lapse au ja head mainet. Lorenz jt (2021) leiavad et antud juhul tuleks koolil võtta pereliikmete nõusolek nende isikuandmete töötlemiseks ning jätkavad, et kui kodutööde käigus kogutud isikuandmed lekivad, tuleb haldustrahvi nõue koolile, mitte õpetajale.

E-keskkond on elektrooniline keskkond, kus on võimalik luua ja hallata nii õppesisu (nt õppematerjalid, harjutused) kui ka õppeprotsesse (nt kodutööd, juhendamine, hindamine) (AKI, 2017). AKI (2017), viis läbi uuringu, mille eesmärk oli saada ülevaade sellest, milliseid e-õppe keskkondi koolid kasutavad ning milline on isikuandmete töötlemise olukord ja õppeasutuste teadlikkus andmekaitse põhimõtetest ning nende rakendamisest e-õppe läbiviimisel. Antud seires keskenduti õppeasutustele, mitte õpetajatele, kes teemaga kõige otsesemalt kokku puutuvad, kuid see toetab asutuse osa vastutusest antud teemadel. AKI läbiviidud e-õppe keskkondade seire (2017) ütleb, et e-õppe vahendusel õppetegevuse osutaja peab arvestama võimalusega, et ta töötleb erinevaid

isikuandmeid ja on isikuandmete seaduse mõistes isikuandmete vastutav töötleja. Hariduse Infotehnoloogia Sihtasutus (edaspidi HITSA) sai aastal 2019 ülesandeks selgitada õpetajatele ja haridusasutuste juhtidele IKÜM-iga seonduvat (Kukk, 2019).

Lisaks andmekaitsele on oluline ka andme-eetika. Andme-eetika on eetika haru, mis hindab andmepraktikaid (nii struktureeritud kui ka struktureerimata andmete kogumist, genereerimist, analüüsimist ja levitamist), mis võivad inimesi ja ühiskonda negatiivselt mõjutada. See hõlmab õige ja vale käitumise kontseptsioonide käsitlemist ja soovitamist ning automatiseeritud/tehisintellekti (AI) ajendatud tegevuste ja otsuste läbipaistvust ja kaitstust seoses andmetega üldiselt ja eelkõige isikuandmetega (What Is..., 2022). Mandinach ja Cotto (2021) on oma artiklis USA näitel rõhutanud, kui oluline on andmete privaatsuse ja andme-eetika lisamine õpetajate ettevalmistusprogrammidesse.

Tammets ja Laanpere (2015) uurisid, kuidas Eestis välja töötatud õpianalüütika kontseptuaalne raamistik pöörab tähelepanu ka eetikale ja privaatsusele. Tammets ja Laanpere (2015: 239-240) uuring kinnitas, et eetika ja privaatsus olid Eestis suurimad kitsaskohad ning, et õppijad ja õpetajad eelistasid, et nende andmed oleksid kättesaadavad ühest portaalist. Uuringust (Tammets ja Laanpere, 2015: 240) selgus, et õppijaid tuleks andmete kogumisest ilmingimata teavitada ning üles kerkisid küsimused selle kohta, mis andmeid kogutakse, kellel on andmetele ligipääs, mida nende andmetega tehakse (mida ja miks analüüsitakse) ning kes ja mis kujul näevad analüüsitud andmeid.

Kuna andmed on kõikjal hariduspraktikas, on oluline, et õpetajad oleksid teadlikud eetilistest probleemidest ja tegeleksid nendega integreeritud lähenemisviisi kaudu, mis hõlmab andmete privaatsust ja andme-eetikat. Mandinach ja Cotto (2021) kirjutavad veel, et õpetajad peavad mõistma oma olulist rolli õpilaste kaitsmisel võimaliku kahju eest ning professionaalne areng on parim viis selle arusaama saavutamiseks. Nad lisavad, et privaatsuskultuuri loomine on kogu haridusringkonda hõlmav jõupingutus. Mandinach ja Cotto (2021) jõudsid järeldusele, et muutused tulevad hariduses aeglaselt ja isegi heade kavatsuste korral võib uute teemade, nagu andme-eetika või andmete privaatsus, tutvustamine olla väljakutse.

Eelneva põhjal saab välja tuua, et on oluline, et õpetajatel oleksid piisavad teadmised ja kogemused andmekaitsest, andme-eetikast ja privaatsusest, tagamaks õpilaste andmete turvalisus. Õpetajatel on kohustus mõista seadusi ja määrusi, mis reguleerivad andmete kogumist ja kasutamist, samuti nende otsuste eetilisi tagajärgi. Õpetajad peaksid olema teadlikud enda rollist õpilaste andmete privaatsuse kaitsmisel. See hõlmab endas ka võimalikke riskide teadmist, mis kaasnevad andmete jagamisega

kolmandate osapooltega. Tagades õpetajate koolitamise õpilaste andmete kaitsmise teemadel, saavad koolid tagada turvalise õpikeskkonna kõigile õpilastele.

1.3 Õpilaste andmete privaatsuse kaitsmise olulisus

Igal inimesel on õigus privaatsusele ning isikuandmete kaitsele (IKÜM, 2016) ning on täiesti mõisteta, miks isikuandmete privaatsus on inimestele oluline, arvestades, et tänapäeval on andmed vara, millega on võimalik inimest profileerida ning temaga manipuleerida (Valgjärv, 2021). Isikuandmed on mistahes andmed tuvastatud või tuvastatava füüsilise isiku kohta, sõltumata sellest, millisel kujul või millises vormis need andmed on (AKI, 2019). Alla 16-aastaste laste isikuandmed kuuluvad erikaitse alla (IKÜM, 2016). Eelkõige nõuab IKÜM vanema või eestkostja nõusoleku andmist mis tahes töötlemiseks, mis hõlmab laste andmeid (IKÜM, 2016). Isikuandmete töötlemine peab olema seaduslik, eesmärgipärane ja õppijale läbipaistev ning õppeasutus, kui isikuandmete vastutav töötleja, peab tagama andmete kaitseks organisatsioonilised, füüsilised ja infotehnilised turvameetmed (E-õppe..., 2017).

E-õppe keskkondade seire (E-õppe..., 2017) toob välja, et isikuandmeteks on näiteks õpikeskkonna kasutaja nimi, e-posti aadress ja kontaktandmed, samuti õppijaga seotud tegevused nagu õppematerjali läbimiseks ja omandamiseks kulunud aeg, õigete ja valede vastuste osakaal või õppeasutuse hinnang õppija tulemustele. Eriliiki isikuandmed on andmed, millest ilmneb rassiline või etniline päritolu, poliitilised vaated, usulised või filosoofilised veendumused või ametiühingusse kuulumine, füüsilise isiku füüsilise ja vaimse tervisega seotud isikuandmed, sealhulgas temale tervishoiuteenuste osutamist käsitlevad andmed, mis annavad teavet tema tervisliku seisundi kohta (IKÜM, 2016:119/6). Mis puutub koolidesse, siis School Education Gateway (2018) selgitab, et isikuandmete erikategooriasse kuuluvad õpilase biomeetrilised andmeid (nt sõrmejäljed, fotod), usuga seotud veendumused (nt õpilane ei soovi osaleda religioonitunnis), terviseandmeid (nt allergiad) ja toitumisalased nõudmised (mis võivad anda vihje nende tervise või usu kohta).

Andmete privaatsuse kaitsmine ei tähenda vaid teiste isikute takistamist üksikisiku kohta teabe saamisel. Andmete privaatsus seisneb tingimuste loomises, kus üksikisikud jagavad oma isikuandmeid, kuna nad usuvad, et teised neid andmeid kaitsevad ning see on eriti oluline hariduse

kontekstis, kus õpilastel on harva valida, kas jagada oma isikuandmeid oma õppeasutusega (Student..., 2021). Privaatsuse all võib pidada silmas privaatsust kui teiste eest varjamise õigust ning kontrolli isikliku informatsiooni üle (Solove, 2002: 1109). Student Privacy Compass (2021) kirjutab, et privaatsus, kui õigluse keskne komponent, kerkib sageli esile hariduse kontekstis ning et õpilaste andmete privaatsus viitab õpilaste andmete vastutustundlikule, eetilisele ja õiglasele kogumisele, kasutamisele, jagamisele ja kaitsmisele. Kuna õpilased – eriti nooremad lapsed – ei ole täielikult varustatud andmete kogumise ja kasutamise võimalike eeliste ja riskide kaalumiseks, vajavad nad spetsiaalset privaatsuse kaitset (Student..., 2021).

Arundel (2021) arvab, et aegunud seadused, riiklike reeglite rohkus ja tehniliste tööriistade arvu suurenemine raskendavad õpilaste isikuandmete kaitsmist. Kuigi andmete privaatsus ja andmeturve on omavahel tihedalt seotud, võib täiesti turvaline andmesüsteem ikkagi rikkuda üksikisiku privaatsust, kui organisatsiooni või süsteemi tavapäraste võimaluste piires tegutsevad volitatud kasutajad koguvad või kasutavad isikuandmeid varjatud, ootamatul, sobimatul või ebaõiglasel viisil (Student..., 2021).

Kuna koolid on aastast 2020 olnud mõjutatud COVID-19 pandeemiast (Student..., i.a.), on õpilaste andmete privaatsus ja andme-eetika muutunud palju teravamaks teemaks kui kunagi varem. Internetis õppimise käigus toodetakse andmeid õpilaste/õpetajate ja platvormide vahelise suhtluse kaudu ning enamikul juhtudel ei pruugi õpilased/õpetajad olla teadlikud oma isikuandmete kaitsmisest (Huang jt, 2020: 4). Student Privacy Compass (i.a) hinnangul võitlevad koolid jätkuvalt hariduses uue normaalsusega, kus tehnoloogia on tugevalt integreeritud ja klassiruumid liiguvad kiiresti isikliku ja virtuaalse vahel. Kui õpilaste privaatsus ei ole nõuetekohaselt kaitstud, on võimalikud tagajärjed õpilastele ja peredele tekitatud kahju, õiguslikud tagajärjed, nagu trahvid või kohtuasjad, ja avalike suhete katastroofid (Mandinach ja Cotto, 2021).

Eelneva põhjal saab välja tuua, et õpilaste andmete privaatsus on oluline, et tagada õpilaste turvalisus hariduskeskkonnas. Õpilaste andmete privaatsus võimaldab õpilastel kontrollida, kuidas õppeasutused nende andmeid jagavad ja kasutavad. See kaitseb õpilasi nende isikuandmete võimaliku väärkasutuse või ärakasutamise eest. Lisaks on õpilaste andmete privaatsuse kaitsmine oluline, et vältida õiguslikke tagajärgesid ning õpilaste lähedastele tekitatud kahju.

1.4 Uurimistöö eesmärk ja uurimisküsimused

Antud töös uurin õpetajate poolt õpilaste andmete jälgimise igapäevaseid aspekte e-keskkondades. Eesmärk on välja selgitada üldhariduskoolide inglise keele õpetajate teadlikkus isikuandme kaitse põhimõtetest ja nende rakendamisest e-keskkondades.

Lähtuvalt eesmärgist olen püstitanud järgmised uurimisküsimused:

1. Millest lähtub õpetajate kasutatavate e-keskkondade valik?
2. Kuidas tagavad õpetajad õpilaste andmete kaitsmise e-keskkondades?
3. Milliseid ohte õpilaste andmete privaatsusele e-keskkondades õpetajad teadvustavad?

2 MEETOD JA VALIM

Uurimistöö eesmärk on välja selgitada üldhariduskooli inglise keele õpetajate teadlikkus isikuandme kaitse põhimõtetest ja nende rakendamisest e-keskkondades. Eesmärgi saavutamiseks valisin kvalitatiivse uurimisviisi, mis annab võimaluse lähemalt tutvuda inimeste kogemuste ja arvamustega (Lagerspetz, 2017). Järgnevates peatükkides kirjeldan valimi moodustamist ning andmete kogumist ja kogutud andmete analüüsi.

2.1 Valimi moodustamine

Valimi moodustamise viisiks on sihipärane valim. Sihipärane valim on uuritavate tahtlik valimine, mis põhineb nende võimel selgitada konkreetset teemat, mõistet või nähtust (Robinson, 2014). Valimi moodustamisel võtsin arvesse uuritava asukohta, eriala, seda millises kooliastmes ja kui vanade õpilastega uuritav töötab ja kas ta kasutab ühe õpetamise vahendina e-keskkondasid. Valimi moodustavad inglise keele õpetajad oma pikaajalise kogemuse tõttu e-keskkondadega, sest ingliskeelsete õppematerjalidega tulevad kaasa mahukad välismaised õpikeskkonnad (Pata ja Laanpere, 2009:118) ning ingliskeelsete keskkondade valik on lai (E-õppe..., 2017). Uuringu valimisse kuulub kaheksa üldhariduskooli inglise keele õpetajat kuuest Tartu linna koolist. Mitme kooli näitel on valim erisugusem. Mitme kooli kaasamine tuleneb ka sellest, et ühest koolist ei saanud ma piisavalt intervjueeritavaid. Järgneva Tabel 1 andmed annavad intervjueeritavatest lühikese ülevaate:

Tabel 1. Intervjueeritavad

Isikud	Vanus Aastates	Sugu	Tööstaaž Aastates	Õpilaste vanus aastates	Haridustase
Intervjueeritav nr 1	43	N	18	10- 16	Magister
Intervjueeritav nr 2	29	N	5	10- 16	Magister
Intervjueeritav nr 3	39	N	10	8- 16	Magister
Intervjueeritav nr 4	25	N	5	10 -14	Magister
Intervjueeritav nr 5	26	N	4	10- 12	Magister
Intervjueeritav nr 6	30	N	4	9- 13	Magister
Intervjueeritav nr 7	30	N	6	7-12	Magister
Intervjueeritav nr 8	48	N	26	11-16	Magister

Töö toob inglise keele õpetajate näitel välja, millised probleemid on Eestis seotud e-keskkondade turvalisusega ja õpetajate rolliga selles. Õpetajatega võtsin ühendust e-posti teel. Saatsin kutse uuringus osalemiseks 96-le õpetajale ning sain kaheksa nõusolekut ja kaks keeldumist. E-posti teel palusin õpetajatel enne intervjuud vastata, milliseid inglise keele e-keskkondasid nad oma töös kasutavad. Selgitasin välja milliseid isikuandmeid nendes e-keskkonnas töödeldakse, kuidas mingis keskkonnas toimub kasutaja tuvastamine ja andmeedastus ning millised on keskkonna kasutustingimused. Mõnel juhul ei saanud ma vajalikku informatsiooni enne intervjuud, seega lähtusin teiste keskkondade kohta kogutud teadmistest.

2.2 Andmete kogumine

Andmete kogumise meetodiks valisin poolstruktureeritud individuaal-intervjuu. Poolstruktureeritud individuaal-intervjuu on oma olemuselt paika pandud vestlus, kus kasutatakse varem koostatud intervjuukava (Lepik jt, 2014). Eesmärk on minimaalselt suunata intervjueeritavat teemade käsitlemisel ja sõnastamisel ning anda intervjueeritavale võimalus teemade üle arutleda, lähtudes tema enda isiklikest kogemustest ja arvamustest (Lagerspetz, 2017).

Enamiku intervjuudest viisin läbi õpetajatega kooli ruumides kohtudes. Mulle oli oluline, et intervjuueeritava mugavuse huvides oleks temal võimalik valida aeg ja koht. Ühe intervjuu viisin läbi teises linnas, avalikus kohvikus. Veendusin, et minu ja intervjuueeritava vestlust ei oleks kuulda kolmandatele isikutele. Selleks valisin kohviku kõige eraldatuma osa ning teenindaja tulekul peatasin intervjuu. Tutvustasin enne intervjuu algust uuringu eesmäärke, orienteeruvat ajalist kestvust, uuringus osalemise konfidentsiaalsust, seda kuidas tulemusi kasutatakse ning küsisin luba intervjuu salvestamiseks (Lepik jt, 2014). Selgitasin ka seda kuidas andmeid hoiustatakse. Intervjuu käigus väljendasin enda kehakeele ja hääletooniga enda erapooletust õpetajate vastuste suhtes ning proovisin õpetajaid vastamise ajal mitte katkestada ega suunata. Intervjuud läbi viies jätsin vajadusel küsimusi vahele (kui sain vastuse mõne teise küsimuse juures) või küsisin täiendavaid küsimusi. Intervjuu lõpus andsin intervjuueeritavatele võimaluse lisada täiendavaid mõtteid, mille kohta ma oma küsimustes tähelepanu ei pööranud. Intervjuu lõpus tänasin kõiki osalejaid nende aja ja koostöö eest ning küsisin nõusoleku vajadusel saata täiendavaid küsimusi.

Intervjuudest tegin transkriptsioonid. Intervjuud transkribeerisin Tallina Tehnikäülikooli kõnetuvatusprogrammi abil (Olev ja Alumäe, 2022), mis paraku eeldas põhjalikku järel töötlemist, sest olenevalt intervjuueeritava diktsioonist ja kõnetempost olid tekstid väga erineva kvaliteediga ning vajasis parandamist. Kontroll tähendas, et kuulasin kõik intervjuud läbi ning parandasin samal ajal loodud tekstifaile. Intervjuudes osalejate isikuandmete kaitsmiseks on töös kasutatud nimede asemel pseudonüüme.

2.3 Andmete analüüs

Analüüsimeetodina kasutasin kvalitatiivsest sisuanalüüsi. Kvalitatiivne sisuanalüüs on tekstianalüüs, mis eeldab materjali mitmekordset hoolikat läbilugemist ning mis võimaldab jõuda kogutud andmetes esinevate mustrite, olulise ja ebaolulise eristamiseni alles analüüsi käigus (Lagerspetz, 2017). Kvalitatiivse sisuanalüüsi olemus on mõista teksti või muude andmeallikate tähendust, jagades need osadeks ja analüüsides nende vahelisi seoseid (Kalmus jt, 2015).

Andmete analüüsiks tuli tekstid kodeerida ning selleks kasutasin *QCAmap* tasuta veebilehte ning Microsoft Exceli programmi. Kodeerimisel lähtusin uurimisküsimustest. Esmalt lugesin tekstid tervikuna läbi ning mõtete korral tegin teksti sisse märkuseid. Seejärel lõin Excelis uurimisküsimuste alla kategooriad ja alamkategooriad. Kategooriad moodustasin induktiivsel meetodil ehk lähtuvalt tekstist, arvestades uurimisküsimusi ja teoreetilist tausta (Kalmus jt, 2015). Lugesin tekste korduvalt läbi ning iga lõigu, lause ja sõna puhul, mis seondus konkreetse uurimisküsimusega, märkisin ära, kas see sobib ühte või mitmesse kategooriasse või kas selle jaoks oleks vaja luua eraldi kategooria või muuta eelnevaid. Välja kujunes viis põhilist kategooriat: keskkondade kasutamisega seonduv, õpetajate eelistustega seonduv, andmetega seotud tegevused, õpetajate teadmised ning õpetajate kogemused. Kuna intervjuudes oli erisusi küsimuste järjekorra ja küsimuste sisu osas, siis märgistasin sama teemabloki küsimused ja vastused kindla värviga. Tuli ka ette, et üks vastus vastas mitmele teemale, sellisel juhul märgistasin selle mõlema värviga. Seejärel kirjutasin välja töö eesmärgist lähtuvalt olulise info, mille põhjal sain esitada tulemused.

Kuni õpingute lõpetamiseni antud erialal säilitan intervjuude helifaile ja pseudonüümitud transkriptsioone Tartu Ülikooli OneDrive pilveteenuses, millele on ligipääs minul ja minu juhendajal.

3 TULEMUSED

Siin peatükis annan ülevaate uuringu tulemustest - milliseid e-keskkondasid õpetajad õppetöös kasutavad ning miks, millised on õpetajate arusaamad privaatsusest ning mida peavad õpetajad e-keskkondadeks ohuks õpilaste andmetele. Toon välja milline on õpetajate kokkupuude andmekaitsega, millised on õpetajate tegevused õpilaste andmetega e-keskkonnas ning millised on õpetajate tegevused nende andmete kaitsmiseks.

3.1 E-keskkonnad ja nende valiku põhjused

Selgus, et kõik õpetajad kasutavad õppetöös mitmeid erinevaid e-keskkondi ning nad aduvad ka ise, et **keskkondade valik on väga lai**. Mõnedes koolides on need kooli poolt osaliselt kompenseeritud ning teistes kasutab õpetaja tasuta piirangutega versiooni. Oli ka neid õpetajaid, kes tasusid e-keskkonna eest ise. Intervjuude analüüs näitas, et **e-keskkondade valimisel on õpetajatel autonoomsus** ning kool neile selle kohta suuniseid ei anna, kuid mõnel juhul, kooli rahastuse olemasolul, eelistati rahastatud keskkondi. Õpetajate vastusest selgus, et e-keskkondade kasutamise sagedus tõusis pandeemia põhjustatud distantsõppe ajal ning mõned õpetajad, kes enne pandeemiat e-keskkondi õppetöös pigem ei kasutanud, kasutavad neid nüüd igapäevaselt.

Intervjueeritav nr 8: „Ma olen suht algaja, et distantsõpe oli see, mis, mis tegelikkuses tegi selle võimalikuks. Et ma ei olnud väga nende keskkondade kasutaja.“

Õpetajate seas populaarsemad e-keskkonnad olid *Quizlet, Quiziz, Kahoot, Youtube, Live Worksheets, Blooket* ja *Google* lahendused (*Drive, Docs, Meets*). Harvem kasutati *JeopardyLabs, LearningApps, Padlet, Canva, Mentimeter* jpt e-keskkondi. *Quizlet, Quiziz* ja *Kahoot* olid esikolmikus, sest keeleõppe

seisukohast oli õpetajate jaoks oluline just sõnavara õpetamine ning nendes keskkondades on seda õpetajate hinnangul kõige parem teha. Üks õpetaja ütles, et on ühinenud ühe grupiga, kus soovitatakse õpetööks erinevaid keskkondi. Õppematerjalidega kaasa tulevate e-keskkondadega kokkupuude oli kõigil õpetajatel, aga aktiivselt kasutati neid harva. Teksti analüüsist selgus, et viimase puhul võib põhjus olla selles, et nende sisu ei paku õpetajatele piisavalt suurt materjalide valikut ning need ei ole piisavalt paindlikud, et õpetaja saaks ise endale vajalikku sisu luua. Lisaks sõltus nende kasutamine sellest, kas need olid parasjagu kooli poolt rahastatud (iga õpilase kasutaja eest tuleb eraldi maksta). Selgus, et tihtipeale kasutatakse neid ka sõltuvalt õpilaste vanusegrupist.

Keskkonna valikut mõjutas see, et enamikes e-keskkondades **ei oleks vajalik konto loomine**, sest võis juhtuda, et noorematel õpilastel oli kodus iseseisev kasutamine keeruline, kui sisselogimise andmed ununesid. Mitmel puhul peab kasutajal keskkonnas toimetamiseks olema vähemalt nimi, mille järgi saab teda identifitseerida. Mõned õpetajaid lubasid ka hüüdnime kasutamist, kuid mitmed nõudsid, et **õpilane kasutaks enda päris nime**. Perekonnanime üldjuhul ei nõutud. Kui oli siiski vaja sisse logida, löid õpilased ise endale kasutajakonto ning suures osas kasutasid sisse logimiseks kooli poolt loodud e-posti aadressi. Vaid õppematerjalidega kaasas olevates e-keskkondades pidid õpetajad ise õpilasele kasutaja looma. Õpilaste võimalik ligipääsu piiratus ei saanud õpetajale keskkonna valikus määravaks faktoriks, sest enamikul õpilastel polnud vanuse või muude põhjustega - nt lapsevanema seatud piirangutega õpilase seadmes - seonduvaid takistusi. Lisaks selgus, et õpilased kasutavad kooli internetti, seega ei olnud takistuseks ka internetile ligipääsu puudumine õpilase individuaalses seadmes.

Mitmed õpetajad märkisid, et eelistavad kasutada neid keskkondi, kus on nõ elulised harjutused-ajalooliste sündmuste ja reaalsete isikute kohta. Õpetajate jaoks oli oluline ka see, et keskkond oleks ülesannete lahendamisel **lihtsalt kasutatav**. Selle faktori mõju vähendamiseks tutvuti vahel keskkonnaga esmalt koolis, tunni ajal, kus õpetaja sai ise juhendada, kuidas asju teha ning alles seejärel suunati õpilast iseseisvalt kodus tegutsema. Mitmed õpetajad tõid välja, et nende jaoks on oluline, et e-keskkond on õpilasele **lõbus, õpilased ei tunneks, et teevad tööd** ning keskkond aitaks kaasa läbitud **teemade paremale kinnistamisele**.

Mõned õpetajad olid rahul sellega, et keskkondade kasutamine **säästab aega**, sest ülesanded on juba valmis tehtud. Pigem eelistatakse neid keskkondi kus ülesandeid ei pea ise looma ning **ülesannete valik on piisavalt suur**.

Intervjueeritav 3: „Seal on niimoodi, et on keeletasemete järgi - on välja toodud erinevad grammatikaülesanded, kuulamisülesanded, lugemisülesanded ja ma saangi võtta näiteks, et ma ei tea, mul on üheksas klass, ma võtangi B üks seal ja on sellised päris elu nagu kuulamisasjad, päris elu tekstid artiklitest, et ta on selline väga hea.“

Üks õpetaja oli rahul keskkonnas olevate filtritega, mis **blokeerisid ebasobiliku sisu** nagu ebasünda kasutajanime kirjutamine või ebasünda emotikonide kasutamise. Reklaamide hulk või olemasolu ei mõjutanud otsust keskkonda kasutada, kuid intervjuu jooksul tõi mõni õpetaja välja seose turvalisuse ja reklaamide vahel ning nägi **õpilasel vastutust** sellekohane info õpetajani viia.

Intervjueeritav 3: „Hästi kriitiline, et kui sul juba hakkab viskama seal mingi liiga palju mingeid imelikke reklaame või asju, et siis kindlasti ka õpetajat teavitada, sellepärast, et väga paljud õpetajad ei mõtle selle peale, et kui turvaline see leheküljel tegelikult on või noh, ongi, et mis seal nagu võib nagu õpilastele näiteks pakkuda.“

Analüüsist tuli välja ka see, et on hea, kui keskkonda saab kasutada telefoni ja arvuti vaates. Õpetajate jaoks oli oluline, et keskkonnas **saab näha kas ja kui palju õpilane on ülesandeid läbinud**, et saada ülevaade tema õppeedukusest. Samas mõõnsid õpetajad, et ka ilma keskkonnata saavad nad aru, kas õpilasel läheb aines hästi või halvasti.

Eeltoodu põhjal võib öelda, et intervjueeritud õpetajate jaoks on e-keskkondade kasutamine õppetöös igapäevane tegevus. Õppetöös kasutatavate e-keskkondade valik on lai ja nende kasutus on reguleerimata – kool ega riik piiranguid ei sea, seega õpetajad lähtuvad oma eelistustest. Valitakse ennekõike keskkondi, kuhu ei pea sisse logima, mis on laste jaoks lõbusad ja lihtsad ning kus on suur valik ülesandeid kas juba eelnevalt valmis või õpetajal võimalik luua. Turvalisus ja reklaamid ei mängi olulist rolli, kuid siiski on õpilaste andemete turvalisus õpetajate jaoks olulise tähtsusega.

3.2 Õpetajate tegevused õpilaste andmetega ja nende kaitsmiseks

E-keskkondade kasutamise viis erines selle poolest, kuidas see jõudis õpilasteni. Mitmel juhul jagas õpetaja keskkonda visuaalse õppematerjalina ja projekteeris selle klassiruumi seinale, sidumata sellega õpilaste andmeid. Teistel juhtudel suunas õpetaja õpilased e-keskkonda nende enda individuaalse seadmega – nii tunni ajal kui ka peale kooli koduste ülesannete lahendamiseks. Oli ka neid õpetajaid, kes said õpilastele e-keskkondade kasutamiseks **võimaldada koolipoolseid seadmeid**. Mõned õpetajad eelistavad andmete kaitsmiseks, et õpilased kasutavadki just koolipoolset tehnikat. Kuigi vastustest tuli välja, et isegi koolipoolsete seadmete olemasolul eelistavad õpetajad mõnel juhul lasta õpilastel kasutada oma isiklikku seadet, sest enamasti on **koolipoolsete seadmete arv piiratud** ning neid ei saa alati õpetajatele sobival ajal kasutada.

Intervjueeritav nr 4: „Kui ma näiteks koolitahvli kasutan, et meil on koolis see ka võimalus. /.../ et siis me peame vaatama pingsalt tabelit, et kas mul on nüüd vaba auk, et kas ma saan nagu tahvli kasutada või mitte, või on, ma ei tea, keegi kaheksanda klassi oma juba võtnud need ära, et siis ma lasen nagu lastel telefonis ise teha.“

Õpetajad tõid välja, et õpilaste andmete kaitsmiseks teevad nad õpilastele **selgitustööd** – ohtudest rääkimine ja pidev rõhutamine, et nad oma andmeid võõrastega ei jagaks. Nõustamist tehakse nii ennetavalt, kui ka peal probleemi tekkimist. Märgitakse ära, et õpilased ei tohiks kasutada erinevates keskkondades **sama parooli** ning lisaks peaksid nad oma **parooli sagedamini vahetama**.

Intervjueeritav nr 7: „selles mõttes uuendada turvalised paroolid ja neid mitte jagada kellegagi. Mingis mõttes väga väikest õpilastega, on see väga raske, sest et need paroolid ei püsi meeles ja peavad olema kirjutatud üles kuigi see on noh, kõigi reeglite vastane. Kõike ei saa nagu selles mõttes reguleerida, selles mõttes mingi vanuseni oleks võib-olla hea kui vanemad nagu haldaksid seda kõike, aga see on jälle vanematele ka nii suure nagu lisakoormuse panemine.“

Üks õpetaja kutsus kooli õpilastega rääkima **veebikontsaabli**. Märgitakse ka ära selline keskkond nagu „Targalt Internetis“, millest on õpilastele räägitud. Eelmises alapeatükis sai märkitud, et kuigi mõned õpetajad lubavad õpilasel kasutada e-keskkonnas kasutajanime, siis teised nõuavad, et õpilane kasutaks oma pärisnime ja mõnel juhul ka **täisnime**. Kui vajalik on sisse logimine, siis suunavad õpetajad õpilast kasutama oma kooli e-posti aadressi. Üks õpetaja ütles, et on **vanemaid teavitanud** sellest, mis keskkondi ta õpilastega kasutab.

Palusin õpetajatel kirjeldada, mis toimingud neil e-keskkondades seoses õpilaste andmetega on. Mõne keskkonna puhul vastasid õpetajad, et nende töö on **luua õpilastele e-keskkonnas kasutaja konto** ning vajadusel abistada õpilast, kui parool ununeb. Mõned õpetajad ütlesid, et mitmes keskkonnas luuakse konto esimeses klassis ning õpetajal on kaust, keskkonnaväliselt, kus on **kõigi tema õpilaste kasutajatunnus ja parool**. Kõik õpetajad leidsid, et üldiselt on nende **tegevused õpilaste andmetega e-keskkonnas minimaalsed**. Üks õpetaja ütles, et tema ei lisa õpilaste kohta peale kasutajanime mingeid muid andmeid kuhugile keskkondadesse ja kui ta tahaks neid rohkem panna, siis ta **küsis lapsevanemate nõusolekut**. Osad õpetajad leidsid, et vastutus õpilaste andmete turvalisuse eest lasub õpilaste endi ja nende vanemate õlgadel.

Intervjuudest selgus, et mõnel juhul kasutasid õpetajad keskkonna võimalust **siduda töötulemusi konkreetse õpilasega**. Valdavad huviks olid erinevad - mõned soovisid hinnata õpilaste osalust aines või teemas, osad sooritustaset, teised saada sisendit õpilasega individuaalseteks arengu aruteludeks, märgiti ära ka võistlusmoment õpilaste endi vahel. Seoses huvi fookusega olid õpetajatel nimetatud tulemuste kontrollimiseks erinevad meetodid. Mitmel puhul jagas õpilane oma soorituse tulemusi ekraanipildina e-maili teel või füüsiliselt õpetajale näidates. Paljudel puhkudel lähtuti e-keskkonnas kuvatavast statistikast, mis võis lähtuvalt keskkonnast olla nähtav ainult õpetajale või ka ülejäänud klassile. Andmeid võis selliselt kätte saada kuni **määramatu ajani minevikus**. Üks õpetaja märkis, et peab andmed keskkonnast ise ära kustutama.

Intervjueeritav nr 4: „ Kui ma annan neile selle lahendamiseks midagi, siis see jääb nagu alatiseks sinna, nii kaua, kuni mina ära kustutan. “

Eeltoodust tulenevalt võib öelda, et õpetajate hinnangul ei mängi nende tegevus suurt rolli õpilaste andmete jõudmisel e-keskkonda ning olulisel määral pannakse vastutust õpilasele ja lapsevanemale. Nagu ka esimese uurimisküsimuse tulemustes selgus, siis eelistatakse kasutada keskkondi, kuhu õpilane ei pea sisse logima, kuid antud kontekstis liigitub see õpetajate tegevuste alla õpilaste andmete kaitsmiseks. Peamine tegevus õpilaste andmete kaitsmisel on teavitustöö andmete kaitsmise meetodite ja internetis valitsevate ohtude kohta. Õpetajate teadmised erinevates e-keskkondades õpilaste andmetega tehtavatest toimingutest (kasutamine, edastamine, hoiustamine jne) on minimaalsed.

3.3 Õpetajate teadmised ohtudest e-keskkondades ning andmekaitsest

Uurisin õpetajate käest, millised ohud nende arvates õpilasi *online* keskkondades varitsevad ning millised neist on olemas ka õppetöökas kasutatavates e-keskkondades. Põhilised ohud, mis *online* keskkondade kohta välja toodi, olid **eale mittesobiliku sisu peale sattumine**, endast **digitaalse jälje jätmine** (seda seostati mõnel juhul veebi küpsiste aktsepteerimisega), oma **andmete jagamine võõrastele** pahatahtlikke kavatsustega isikutele ning **kiusamise ohvriks langemine**. Õppetöökas kasutatavates keskkondades leiti, et ohuks on see, kui õpilane klikkab mõnele keskkonnas olevale **reklaamile**, mis võib viia ta **sobimatu sisu** juurde. Samuti peeti õppetöös ohuks, kui õpilane peab keskkonna kasutamiseks **sisse logima**. Seda seostati sellega, et kasutaja tegemise ja sisselogimise korral jääb õpilasest e-keskkonda rohkem andmeid.

Intervjueeritav 5: „Võib-olla ainult siis, kui sisse logimisega, et ikkagi siis ta salvestab, siis jäävad meiliaadressid ja kõik muud jäljed jäävad maha.“

Küsisin, et milliseid andmeid e-keskkonnad õpilase kohta koguvad ja mis eesmärgil. Mitmed õpetajad ei osanud sellele küsimusele vastata. Pakuti, et ehk kogutakse **statistikat keskkonna kasutussageduse kohta**. Järeldati, et kui külastab tihti, siis võimalik tagajärg on, et leht muutub tasuliseks. Samuti arvati, et keskkonnad koguvad statistikat selle kohta, milliseid ülesandeid õpilased lahendavad, et pakkuda rohkem sarnaseid ülesandeid ja oma **lehe sisu muuta vastavalt kasutajate vajadustele**. Õpetajad uskusid, et põhilised andmed, mis õpilase kohta kogutakse, on tema **e-posti aadress, kooli nimi, klass, päritolu riik, IP aadress, asukoht, õpilase saavutused/tulemused**. Osa õpetajaid arvas, et kui õpilane ei kasuta oma isiklikku seadet, vaid kooli poolt antut, siis ei saa õpilase isikut siduda tema külastatud e-keskkondadega – olenemata sellest, kas ta oma isikliku meilikontot vms kuskil kasutab. Leiti, et andmeid kogutakse suures osas reklaami jaoks, mida õpilastele saata.

Intervjueeritav 2: „Tõenäoliselt kogu see asi, mis meil igal pool toimub, et keegi kogub andmeid reklaamide jaoks, toodete jaoks, mida sulle, mis reklaame sulle saata, keegi kindlasti jälgib, aga seda, kes täpselt, kes, kes sellega tegeleb, seda mina öelda ei oska.“

Õpetajad **ei olnud end teadlikuks teinud** teemadel, milliseid andmeid mingis keskkonnas kogutakse (kasutaja sisestuse, ajakulu, kasutatava seadme, asukoha kohta jne), kes tegelikult kogub ja kuhu, kui

turvaliselt neid andmeid hoiustatakse ning kui kaua, kas ja kellele neid edasi saadetakse ning mille jaoks andmeid kasutatakse (üldine statistiline analüüs, kasutajapõhine analüüs jne).

Intervjueeritav 1: „No tegelikult ma ei ole päris kindel noh selles mõttes selle aasta jooksul, kui nad õpivad, kindlasti, aga, aga ma ei ole järgmisel aastal enam kontrollinud.“

Küll aga väljendati intervjuu jooksul nendel teemadel arutledes, et küsimustele mõeldes tõusis teadlikkus ohukohtadest ja sellega koos ka teema olulisus õpetajate silmis. Intervjuudest selgus, et mingil määral õpetajad siiski **teadvustavad enda rolli** õpilaste andmete kaitsmisel keskkonna valimisel.

Intervjueeritav nr 3: „On see ka õpetaja töö natuke nagu jälgida, et mis need lehed on, kui turvalised need on, ongi jälle, et kas ta peab sisse logima, miks mulle ei meeldigi väga palju kasutada neid, kus nad peavad sisse logima. et noh, ikkagi natuke kriitiliselt nagu läbi mõelda.“

Mis puutub andmekaitse, siis mitmed õpetajad ütlesid, et on andmekaitse kohta saanud teadmisi oma **erilaste õpingute käigus, mis oli mitme aasta eest**. Mainiti ka kooli poolt saadetavaid infokirjasid ja koolitusi kuid samas märgiti ära, et alati **ei saa koolitustest osa võtta**, sest samal ajal toimuvad tunnid. Mõned õpetajad ütlesid, et kooli poolt on õpilastele andmekaitsest rääkimiseks kutsutud kohale spetsialist. Spetsialist andis koolituse õpilastele alates kuuendast klassist. Samas kasutavad õpilased e-keskkondasid alates esimesest klassist.

Järgmisena soovisin välja selgitada, mida tähendab õpetajate jaoks privaatsus ja mis on neile selle tähtsus. Vastuseid analüüsid on selge, et läbivalt **peeti privaatsust oluliseks**. Üks õpetaja leidis, et privaatsus on see, et ta ei kommenteeri õpilase töid teiste õpilaste kuuldes. See oli läbiv joon, et peeti oluliseks **õpilase õppetulemuste privaatsuse kaitsmist**. Samas möönis mitu õpetajat, et nii mõneski e-keskkonnas on ülesannete tulemused teistele õpilastele näha. Õpetajad väljendasid mõistmist, et tänapäeval on privaatsuse mõiste laienenud digikeskkonda. Toodi näited privaatsuse rikkumise kohta, kui erinevad rakendused võtavad andmeid õpilase telefonist – kontaktid, pildid, kirj vahetus, pere ja asukoht. Vastati ka, et privaatsus on see, kui **ei jagata oma isikuandmeid**.

Intervjueeritav 4: „Privaatsus, kui me räägime näiteks sellest, et õpilane kasutab omaenda telefoni, siis need keskkonnad ei läheks nagu täielikult tuustima sinna.“

Ühe õpetaja õpilane oli sattunud olukorda, kus palus klassikaaslase abi ühe keskkonna parooli vahetamisel ning see klassikaaslane, olles saanud teada tema parooli, kuritarvitas neid andmeid **tellides tema nimel tasulisi mängu**. Teine juhtum leidis aset ühes õppetöös kasutatavas keskkonnas tunni ajal, kus tundi pääses virtuaalsel teel võõras isik, kellele üks õpilane oli jaganud keskkonna kutset. Kutset jaganud õpilane kannatas selle juhtumi tõttu **reaalset kahju** – kahandati tema käitumishinnet. Distsantsõppe ajal oli õpetaja hinnangul see probleem sagedasem, et **e-keskkonnas läbiviidavasse tundi sattusid võõrad isikud**. Intervjueeritav nr 1 rääkis kogemusest, kus õpilane, kes kasutas kooli poolt antud tahvlit, ei saanud õpetööks kasutatavast e-keskkonnast mingi tehnilise tõrke tõttu välja logida. Iga kord, kui ta üritas end keskkonnast välja logida, logis lehekülg ta uuesti sisse tagasi. Mõlemad õpetajad teadvustasid nende olukordade järgselt, kui oluline on e-keskkonnas õpilaste andmete kaitsmine ning millised võivad olla tagajärjed, kui seda ei tehta.

Kokkuvõtteks saab öelda, et õpetajate teadmised e-keskkondade ohtudest ja andmekaitsest on vähesed. Pole pigem osaletud koolitustel väljaspool oma tasemeõpinguid ega süvenetud temaatilistesse e-mailidesse. Ohuks peeti sobimatut sisu, isikuandmete jagamist, reklaami ja kiusamist. Andmetele peeti suureks ohuks just keskkonda kasutaja loomist ja sisselogimist. Õpetajad tunnistasid, et nad pigem ei oska vastata, mis eesmärgil andmeid kogutakse, aga pakkusid, et põhjus võib olla statistika tegemiseks, lehe parandamiseks ning suunatud reklaami saatmiseks. Privaatsust peeti oluliseks, kuid privaatsuse defineerimise asemel toodi rohkem välja, mis seda ohustab.

4 JÄRELDUSED JA DISKUSSIOON

Järgmises peatükis esitan oma järeldused intervjuudes arutletud teemade kohta ning analüüsin neid tuginedes teooria osas kasutatud kirjandusele. Järeldustes toon välja vastused uurimisküsimuste. Uurimisküsimused olid järgmised:

1. Millest lähtub õpetajate kasutatavate e-keskkondade valik?
2. Kuidas tagavad õpetajad õpilaste andmete kaitsmise e-keskkondades?
3. Milliseid ohte õpilaste andmete privaatsusele e-keskkondades õpetajad teadvustavad?

Peatüki lõpus kirjeldan valimi moodustamise, andmete kogumise ja kogutud andmete analüüsiks valitud meetodite eeliseid ja puuduseid.

4.1 Järeldused ja diskussioon

E-keskkonnad ja nende valiku põhjused

Intervjuude analüüsist selgus, et õpetajatel on autonoomsus e-keskkondade valikul ning eelistatakse e-keskkondi, mis on tasuta. Kuna kool üldiselt nende kasutamist rahaliselt ei toetanud, siis on selline tulemus loogiline. Siit tuleb välja aga probleemikoht, kus kogu valiku raskus ja andmete turvalisuse eest sisuline vastutus jääb õpetajale. Õpetajad vahetuvad ja nende teadmiste tasemed erinevad, kuna need on sõltuvuses rohkem iga õpetaja enda kogemustest kui kuskil õppekavas või õppeasutuses ettenähtud koolitustest. Seetõttu tundub ebapiisav, kui valitud vahendite sobilikkus sõltub vaid neist. Kuivõrd õpetaja pädevuses on planeerida ainekava tööd ja valida seda toetavad vahendid, siis võiks tal säilida võimalus soovi korral õppetöös kaasata e-keskkondi ning selle õiguse täielik piiramine, õpilaste andmete turvalisuse parandamiseks, ei tundu mõistlik. E-keskkondade kasutus võiks olla

reguleeritud kas riigi või õppeasutuste poolt – näiteks heakskiidetud ja kontrollitud keskkonnad, kirjalikud ajakohased nõuded uue keskkonna sobilikkuse hindamiseks ning tingimused, mida peab mingites kindlates keskkondades jälgima. Selliseid tegevusi saaks toetada just nendel teemadel töötav HITSA. Ka teooria osas olen märkinud, et haridustehnoloogia ettevõtted jätkavad pidevalt õiguslike raamistike olemasolevate lünkade ärakasutamist (Palfrey jt, 2020: 1) ja seetõttu oleks vaja ajakohast regulatsiooni nii riigi kui kooli tasemel – eriti kui muutused tulevad hariduses aeglaselt (Mandinach ja Cotto, 2021). AKI (2017) ja ka Lorenz jt (2021) töös nenditakse, et andmete kehva privaatsuse tagajärgede korral on enne õpetajat vastutav eelkõige õppeasutus.

Teine oluline kriteerium on keskkonnas olev sisu. Intervjuude analüüsist selgus, et eelistatakse lehti, kus on lai valik õppematerjale erinevas vanuses õpilastele. Ainega seonduva sisu võimalused tunduvad olevat olulisemad, kui sellega kaasnevate reklaamide sisud, kogus või kuvamispehmed (õpilase kasutusandmetel põhinev suunatud reklaam), mis väljendab teadmatust andme-eetika põhimõtetest. Tänapäeva veebilahendustes on reklaamid põhiliseks rahastusallikaks (Manjoo, 2018) ning nende alusel valitavate keskkondade täielik piiramine võib seada piirangud kasutatava sisu mitmekülgsusele. See omakorda võib vähendada e-keskkondade positiivset mõju õpitulemustele, mida õpetajad intervjuudes oluliseks pidasid. Reklaamide koguse piiramiseks on tarkvaralisi vahendeid (Cook, 2023) kuid iga õpilase isiklikku seadmesse need ei jõua. Õppeasutuse poolt võimaldatud seadmed, tarkvara litsentsid, nimekiri sobilikest vabavaradest või praktilised temaatilised töötoad tõstaksid turvalisust (Arundel, 2021), suurendades taolise tarkvara kasutust. Siinkohal oleks eeldus, et nimetatud andmete ajakohasust perioodiliselt kontrollitakse ja täiendatakse ja lahendused korralikult läbi mõeldakse. Praktiline õpe toetaks ka andme-eetika seisukohast andmete privaatsuse vajalikkusest arusaamist, et õpilased ei lubaks nii kergekäeliselt suunatud reklaamideks andmete kogumist.

Intervjuudest lähtus, et õpetajad eelistavad selgelt e-keskkondi, kus ei ole vaja kasutaja või konto loomist. Konto loomisega seostati intervjuudes ohtu õpilase andmetele. Büchi jt (2022: 2) leiavad, et ainuüksi võrgus viibimine loob püsiva digitaalse jalajälje ja andmed. Ilma sisse logimata saavad leheküljed koguda vaadeldavaid andmeid (*observed data*) - üksikisiku tegevuse salvestamisega, nt asukohaandmed mobiiltelefonide kasutamisel (Huang jt, 2020:12). Seega ei piisa andmete turvalisuse tagamiseks sisse logimise vältimisest.

Intervjuude tulemustest on näha, et isiklik nutiseade või ligipääs mõnele nutiseadmele on peaaegu kõigil õpilastel - vastasel juhul oleks nende õppetöö antud aines piiratud. Kui õpilased osakavad nutiseadmes kasutada õpetajate antud e-keskkondi, võib oletada, et seal kasutatakse ka muudest allikatest saadud e-lahendusi. Ainuüksi e-keskkondade ja nende valiku turvalisuse tõstmine seega on andmete kaitseks ebapiisav ja võiks mõelda erinevatele võimalustele õpilaste ja nende vanemate teadlikkuse kasvatamisele (Huang jt, 2020). Selle tulemusena saaks nad informeeritumalt iseseisvalt otsustada ja piirata, millal mingeid andmeid jagatakse ning mõistaks paremini selle otsuse mõjusid (Huang jt, 2020).

Edaspidised uuringud võiksid keskenduda nende tegurite uurimisele, mis mõjutavad õpetajate otsuseid kasutada konkreetseid e-keskkondi. See võib hõlmata õpetaja individuaalsete omaduste, (näiteks tema tehnoloogiaoskuste ja -kogemuse), aga ka kontekstuaalsete tegurite (ressursside kättesaadavus ja kooli tehnoloogiline infrastruktuur), uurimist. Lisaks peaks uurima, kuidas e-keskkondi kasutatakse õpilaste õppimise toetamiseks ja milliseid strateegiaid kasutavad õpetajad nende vahendite tõhusaks kasutamiseks. Oluline on ka paremini mõista, kuidas e-keskkondade kasutamine mõjutab õppe kvaliteeti ja õpilaste saavutusi.

Õpetajate tegevused õpilaste andmetega ja nende kaitsmiseks

Õpetajate vastustest selgus, et kui ei ole võimalik sisse logimist vältida, siis tehti kasutaja kooli poolt loodud e-posti aadressiga. Lisaks, kui e-keskkondades ei pea kasutajat looma, siis õpilased teevad seda omavoliliselt - kui nad soovivad koguda punkte ja oma saavutusi näha. E-keskkonnale mandaadi esitamisega (nt kasutajanimi või e-posti aadress ja parool) tõendavad õpilased oma identiteeti ning vähim, mida teha selle kaitsmiseks, on luua tugev parool (Huang jt, 2020:40). Õpetajad mainisid turvalisuse kaalutlustel erinevate paroolide kasutust ja perioodilist vahetamist, kuid mitte nende tugevust. Sellest võib oletada, et ka õpilaste arusaam sellel teemal võib olla puudulik ja vajaks parandamist. Lisaks, kuna turvalise interneti käitumisega seostatakse siiski kasutajakonto kustutamist (Wisniewski jt, 2015:2), võiks leida viise õpetajaid ja nende läbi ka õpilasi informeerida sellest, et kui kasutaja on tehtud ja tulemused ära nähtud, tuleks võimalusel see kasutajakonto kohe jälle ära kustutada.

Õpetajad leidsid, et nende poolne tegevus õpilaste andmetega e-keskkondades on minimaalne. Võis mõista, et see võrdus nende jaoks ka suurema turvalisusega, kuigi seal ei pruugi korrelatsiooni olla. Samas mõnsid mõned õpetajad, et olenevalt keskkonnast on neil võimalik näha õpilase läbitud

ülesandeid ja tehtud tööde tulemusi ning et nooremate õpilaste puhul valdab õpetaja õpilase kasutajatunnust ja parooli. Õpetajad ei tundu teadvustavat, millised õpilaste andmed just õpetajate endi otsuste ja tegevustega seonduvalt õpianalüütikas kasutatavad on ning seda teadmata on neil raske hinnata keskkonna kvaliteeti andme-eetika seisukohast või piirata oma tegevusi valitud keskkonnas sellest lähtuvalt. Eelnevast võib oletada, et õpetajad ei teadvusta enda rolli olulisust õpilaste andmete kaitsmisel. Mandinach ja Cotto (2021) kirjutavad, et õpetajad peavad mõistma oma kriitilist rolli õpilaste andmete privaatsuse kaitsmisel, vältimaks privaatsuse rikkumisega kaasnevaid võimalikke kahjusid ning, et selle saavutamiseks võiks nende õppekavasse olla lisatud andmekaitse.

Intervjuudest selgus, et õpilaste andmete kaitsmiseks eelistatud vahend on õpetajate jaoks teavitustöö, kuid oli näha, et õpetajate endi teadmised selles valdkonnas on puudulikud. Nagu eespool arutus ning ka tulemustes märgitud, siis õpetajad soovitasid näiteks erinevaid parooli ja nende perioodilist vahetamist. Erinevates keskkondades erinevate paroolide kasutamine on ka Huang jt (2020: 41) hinnangul üks andmete privaatsuse tagamise meetodeid ning nõrga parooli puhul soovitavad mingi perioodi tagant parooli vahetamist ka mitmed küberturvalisusest rääkivad artiklid (McAfee, 2022; Johnson, 2020; Kaspersky, i.a). Sellest hoolimata nende meetmete väärtus väheneb, kui õpetajal on – nagu intervjuudest nähtus - kaustad õpilaste kasutajaandmete ja paroolidega ning paroolide tugevusele tähelepanu ei pöörata. Ühest küljest on sel moel andmed ohus õpetaja enda tegevustega seoses, kuid teisalt, kui keegi pahatahtlik saab ligi õpetaja kaustadele, saab ta ühe ründega ligi ka kõigi tema õpilaste andmetele (Lorenz jt, 2021) Eelnevaid ohte silmas pidades tuleks siin sobivad erimeetmed leida (Student..., 2021) ning kindlasti võtta arvesse ka õpilaste erinevat vanust, sest esimese klassi laps tõenäoliselt ei mõista parooli ja andmete privaatsuse kontseptsiooni selliselt nagu kaheksanda klassi õpilane.

Erinevalt õpetajate väljendatud arvamustest, ei kaitse koolipoolse tehnika kasutamine õpilase andmete privaatsust, kui koolil puudub protsess uute veebipõhiste tööriistade kontrollimiseks (Arundel, 2021). Arundel (2021) sõnul, kontrollimaks, et e-keskkond ei seaks ohtu õpilaste isikuandmeid, tuleb kontrollida selle keskkonna kasutustingimusi ja veenduda, et veebisaidi omanikul pole halba mainet. Kuivõrd intervjuude analüüsist selgus, et õpetajad ja koolid, kus nad töötavad, ei kontrolli eelmainitud faktoreid, siis ei ole võimalik väita, et koolipoolse tehnika kasutamisel oleksid õpilaste andmed täiesti kaitstud võrreldes isikliku seadme kasutusega. Kirjeldatud eksiarvamus võib vastupidi viia hoopis petliku turvatundeni ja väljenduda tavapärasest isegi hooletumas andmete käitlemises. Lisaks ei tule

õpetaja vastusest kuidagi välja, et koolipoolse tehnika turvameetmetele oleks kuidagi omakorda nõuetele vastavuse kontrolli läbi viidud. See suurendab turberiski õpilase andmetele ja privaatsusele, kui turvameetmete realiseerijad kasutavad isikuandmeid varjatud, ootamatul, sobimatul või ebaõiglasel viisil (Student..., 2021).

Tulevased uuringud antud teemal võiksid keskenduda sellele, kuidas õpetajad õpilaste andmeid koguvad ja säilitavad ning kuidas nad neid juhendamiseks ja hindamiseks kasutavad. Lisaks võiks uurida, kuidas õpetajaid koolitatakse õpilaste andmeid kasutama ja kaitsma ning kuidas selline koolitus nende tegelikku praktikat mõjutab.

Õpetajate teadmised ohtudest e-keskkondades ning andmekaitsest

Peamisteks online keskkondades varitsevateks ohtudeks õpilastele peeti eale mittesobilikku sisu, endast digitaalse jälje jätmist, oma andmete jagamist võõrastele, kiusamise ohvriks langemist ja reklaami. Student Privacy Primer (2021) on avaldanud nimekirja peamiste ohtude ja kahjuga õpilastele nende andmete privaatsuse rikkumisel. Intervjuude analüüsist tulenevalt võib öelda, et peaaegu kõik õpetajad teadvustasid vähemalt ühte seal nimetatud riski, milleks oli sobimatu sisu. Vähem teadvustati kiusamise ohvriks langemist, reklaami ning üldist ohutust. Üldse ei teadvustatud võrdsusprobleemi, liigset jälgimist, püsivat kirjet ja võimaluste kaotamist. See ei pruugi tähendada, et õpetajad ei ole nendest tagajärgedest üldse teadlikud vaid on võimalik, et see ei ole teema, millele nad sagedasti mõtleavad. Samas võib oletada, et neid ei peetud nii oluliseks või tõenäoliseks, et oleks mainimist väärt.

Õpetajad ei olnud teadlikud, mida õpilaste andmetega erinevates keskkondades tehakse ning kelle poolt, kuidas ja kus neid säilitatakse või miks neid säilitatakse. Mitmed õpetajad ei teadnud, et koolis oleks teemakohaseid koolitusi üldse tehtud. Mõned õpetajad polnud osalenud koolide korraldatud koolitustel ebasobiva toimumisaja tõttu ning polnud lugenud ka kooli poolt saadetud teemakohaseid e-kirjasid. Kuivõrd õpilaste andmete kaitsmine on digitaalsel ajastul tähelepanu nõudev valdkond, siis on oluline, et kool, kui õpetaja tööandja, toetaks ja juhendaks õpetajaid antud teemal. Õpetajad peavad saama koolitust kehtivate õpilaste privaatsusseaduste kohta; mõistma, kuidas nende rollide puhul kehtib seaduste järgimine ning kasutama andmeid vastutustundlikult ja eetilisel viisil (Mandinach ja Cotto,

2021). Kool vajab sealjuures tuge riigilt, sest üldine laste eraelu puutumatus ja andmekaitse õiguste kandja on siiski riik (Day, 2022).

Sellest võib oletada, et koolituste arvu kasvamine ja õpetajatele seal osalemiseks sobivate tingimuste loomine toetaks olulisel määral õpetajate teadlikkuse kasvu. Õpetajate vastustest lähtus, et nad teevad otsuseid oma olemasolevate teadmiste alusel, seega e-keskkondade valik ja nende turvalise kasutuse oskus on otseses sõltuvuses nende teadmistest. AKI (2017) hinnangul peab isikuandmete töötlemine olema õppijale läbipaistev ning õppeasutus, kui isikuandmete vastutav töötleja, peab tagama andmete kaitseks organisatsioonilised, füüsilised ja infotehnilised turvameetmed. Võib järeldada, et kooli vastutus on tagada õpetajate vajalikud teadmised ja võimalused õpilaste andmete kaitsmiseks ning alustada võiks sellest, et õppetöös kasutatavad keskkonnad on kooli poolt kontrollitud ja heaks kiidetud.

Õpetajad arvasid, et erinevad e-keskkonnad koguvad õpilaste andmeid selleks, et koostada statistikat antud keskkonna kasutamissageduse ja lahendatud ülesannete/mängude tüüpide kohta - eesmärgiga parandada lehe sisu, muuta leht (osaliselt) tasuliseks või, et saata õpilasele reklaami. Kuna õpetajad kasutavad eelpool toodud keskkondasid õppetöös, siis võib järeldada, et neile ei seostunud õpilaste andmete kasutamine lehe sisu parandamiseks negatiivse tagajärjena. Negatiivse tagajärjena seostati lehe tasuliseks muutumist ning võib järeldada, et see tulenes asjaolust, et sellel oleks õpetajate tööle otsene tagajärg. Võib oletada, et kuna tänapäeva õpilased kooliväliselt kasutavad lisaks mitmeid e-lahendusi, siis õpetajatele tundub just selles võrdluses, et nende suunatud keskkondi ja nendega seonduvaid ohte on võrdluses märkimisväärselt vähem. Selline mõtteviis toetab arusaama, kus õpetaja ei tunne vastutust andmelekket tekkinud tagajärgede eest ega ka selle ennetamise osas.

Montgomery (2015: 771) kirjutab, et turunduse, andmete kogumise, jälgimise ja sihtimise toimingud on spetsiaalselt kohandatud noorukite arengu põhiaspektidele, võttes arvesse noorte vajadusi ja kasutades ära nende ainulaadset haavatavust. Noorukite emotsionaalse volatiilsuse ja impulsiivse käitumise tõttu on nad täiskasvanutest haavatavamad selliste tehnikate suhtes nagu reaalses pakkumine, asukoha sihtimine (eriti kui kasutaja on ostukoha lähedal) ja kohandatud dünaamilised loominguks reklaamid nende individuaalsele profiilile ja käitumismustritele (Montgomery, 2015: 771). On oluline märkida, et lapsed moodustavad kolmandiku internetikasutajatest, seega on vähe andmeid töötlevaid ettevõtteid, mis ei töötle ka laste andmeid (Day, 2022). Lapsed on haavatavamad

kui täiskasvanud ja nad ei mõista nende andmete kogumisega nõustumise pikaajalisi tagajärgi (Day, 2022).

Õpetajad arvasid, et andmed, mida kogutakse on e-posti aadress, kooli nimi, klass, päritolu riik, IP aadress, asukoht ja õpilase saavutused/tulemused. Tänapäeva digitaalse meedia keskkonnas suudab süsteem jälgida ja analüüsida ka käitumist, tegevust ja võrgusuhteid, mis toimuvad nii võrgus kui ka väljaspool seda (Montgomery, 2015: 773). Suur hulk kasutajaandmeid kaevandatakse ja salvestatakse nüüd regulaarselt käitumusliku sihtimise ladudesse ja muudesse andmebaasidesse ning neid kasutatakse veebipõhise sihtimise profiilide värskendamiseks (Montgomery, 2015: 773). Kogutud andmete hulka kuuluvad ka konteksti puutuvad või tehinguandmed ehk metaandmed. Sellised metaandmed annavad teistele kogutavatele andmetele tähenduse ja konteksti; näiteks teabel selle kohta, kui kaua kulus konkreetsel õpilasel veebiülesande täitmiseks, on rohkem tähendust, kui on teada kuupäev ja kellaaeg, millal õpilane tegevuse lõpetas, mitu katset õpilane tegi ja kui kaua õpilase hiir hõljus üksuse kohal (mis võib viidata otsustavusele) (Huang, 2020:27).

Huvitav oli ka asjaolu, et kuigi mitmed intervjuudes nimetatud keskkondadest kasutavad ennustavat analüütikat, siis õpetajad ei väljendanud märkimisväärset huvi selle tarbimise osas ja mitmel puhul isegi ei teadnud, kust seda otsida. Võib oletada, et kui õpetajad oleksid paremini kursis oma töövahendite võimalustega, tuleks neile sellega seonduvalt pähe ka rohkem ohte, mis võivad kaasas käia taoliste andmete kokku panemisega. Igal juhul on õpetajate vähese huvi tulemusena raske hinnata, mil moel on nende õpilased juba praegu mõjutatud töö teoreetilises osas mainitud algoritmilisest kallutatusest (Arantes, 2019) ning kas see mõju võib drastiliselt muutuda õpetajate teadlikkuse muutumisel. Kõik õpetajad väljendasid arusaama, et privaatsus üldiselt ja õpilaste andmete privaatsus on oluline teema ning tunnistasid, et sooviksid, et teaksid sellest teemast rohkem.

Kuigi vaid kahes intervjuus tulid välja juhtumid, kus õpilane oli kannatanud reaalselt kahju, või tal oli oma andmete turvalisusega konkreetne probleem, ei tähenda, et taolisi või sarnaseid juhtumeid pole ka teistel õpetajatel ette tulnud. Nagu teорияosas on märgitud, siis rahaline kahju ja maine kahju on põhilised andmete privaatsusega seotud riskid (Lorenz jt, 2020). Intervjueeritav nr 8 ja intervjueeritav nr 1, kes juhtumitest rääkisid, ja kelle hinnangul on andmete privaatsus ja turvalisus e-keskkondades hetkel väga päevakajaline ning oluline teema, on töötanud õpetajana 18-26 aastat. Võimalik, et avameelsus eelnimetatud juhtumite jagamisel ning kokkupuude erinevate taoliste olukordadega võib

olla seotud nende pikemaajalise kogemusega õpetajana. Taoliste probleemide aset leidmine võib olla sagedasem ning selle välja selgitamiseks tuleks teostada laiaulatuslikum uuring.

Antud valimi põhjal ei saa teha mingeid konkreetseid järeldusi õpetajate üldiste teadmiste kohta õpilaste andmete privaatsusest. Lisaks ei kuulunud valimisse ühtegi üle 50-aastast õpetajat (vt Tabel 1), mistõttu on võimatu teha järeldusi vanemate õpetajate teadmiste kohta õpilaste andmete privaatsusest.

Kuivõrd antud uuring keskendus keeleõppe valdkonna õpetajatele, siis see annab ühe võimalusena aluse edasisteks kvantitatiivse meetodiga uuringuteks, mis täpsustavad, mil määral antud probleemid laienevad ka ülejäänud valdkondade õpetajatele ja kui tihti. Tulevased uuringud antud teemal peaksid hindama olemasolevate andmekaitseprogrammide tõhusust koolides ja uurima õpilastele digitaalse ohutuse õpetamise parimaid tavasid. Arvan, et uurida tuleks ka seda, kuidas saaks õpetajaid andmekaitse osas paremini koolitada ning milline on selle koolituse mõju nende teadmistele e-keskkondade ohtudest.

4.2 Meetodi kriitika

Valimi moodustamise viisiks on sihipärane valim. Antud meetod võimaldas mul lähtuvalt uurimuse eesmärgist valida uuritavad vastavate kriteeriumite alusel nt asukoht ja valmidus osalema. Selline paindlikus lihtsustas minu jaoks intervjueeritavate leidmist. Valimisse kuulus kaheksa õpetajat ja kuigi väikese valimi puhul ei saa suuri võrdluseid ja üldistusi teha (Lagerspetz, 2017), oli võimalik vaadelda, kas on selgelt eristuvaid tulemusi, mille kehtivust suuremas valimis oleks põhjust täpsemalt uurida.

Andmete kogumise meetodiks valisin poolstruktureeritud individuaal-intervjuu. Poolstruktureeritud intervjuu sobis antud uuringu kvalitatiivse iseloomuga, sest soovisin uuringu tulemusi väljendada pigem selgituste ja kirjelduste abil, mitte numbriliselt, saada teada uuritavate arvamusi antud teemast ning avastada uut infot (Lagerspetz, 2017). Poolstruktureeritud intervjuu võimaldas küsimused varasemalt ette valmistada, kuid ma ei pidanud neid esitama ettenähtud järjekorras ja sõnastuses (Lepik jt, 2014) ning see andis mulle võimaluse küsida ka täpsustavaid küsimusi (Lagerspetz, 2017).

Intervjuu kava (Lisa 1) olemasolu tõttu oli lihtsam hoida töö fookust. Samuti sain selle olemasolu tõttu kindel olla, et olulised küsimused saavad küsitud ja intervjuu ei kaldu teemast kõrvale.

Selle meetodi oht on, et intervjueritav ja uurija jäävad oma rollidesse kinni ning vastused piirduvad loodud fassaadi näitamisega ning püüdliselt oletuslike vastustega (Lagerspetz, 2017), seega antud meetodi puhul võib olla keeruline olla kindel, millised on intervjueritava tõesed arvamused ning kogemused. Proovisin seda ohtu maandada küsides avatud küsimusi võimaldades õpetajatel teemasse sügavamale sisse minna ja esitades täpsustavaid küsimusi, väljendades sellega enda siirast huvi nende vastuste kohta ning lastes neil oma vastust täpsustada (Lepik jt, 2014). Lisaks sellel alustasin vestlust üldise info ja enda tutvustamisega, et õpetajad tunneksid end vabamalt. Rõhutasin, et tegemist ei ole teadmiste kontrolliga ning et ei ole valesid vastuseid.

Analüüsimeetodina kasutasin kvalitatiivset sisuanalüüsi. See analüüsi meetod võimaldas mul keskenduda teksti peamistele ja olulistele tähendustele, samas võimaldades analüüsida ka latentset sisu, mis tähendab, et tuleb võtta arvesse ridade vahele peidetud teksti, autori vihjeid, kavatsusi ja eesmärke (Kalmus jt, 2015). Antud meetod sobis mulle kõige paremini, sest soovisin arvesse võtta teksti konteksti, varjatud tähendusi ning samas eristada individuaalseid juhtumeid. Valisin andmete analüüsiks kvalitatiivse sisuanalüüsi, sest see on paindlik meetod, aitab tuvastada erinevaid vaatenurki, saada uurimisteedest igakülgselt arusaama ning see võimaldab avastada andmetest mustreid ja teemasid (Lagerspetz, 2017), mis võivad aidata kaasa edasistele küsimustele ja uuringutele. Lisaks soovisin, et mul oleks võimalik teha analüüsi avatult, mitte ettevalmistatud kategooriate abil, sest see andis mulle võimaluse leida tulemustest ka seda infot, mida ma ei osanud alguses otsida (Lagerspetz, 2017).

Selle meetodit kasutamise oht on, et autor ei suuda tulemusi täiesti objektiivselt tõlgendada ja teeb teksti analüüsides endale meelpäraseid järeldusi ning erinevaid tekste ei ole võimalik võrrelda samade kriteeriumite alusel. (Kalmus jt, 2015). Selle ohu maandamiseks üritasin teadlikult tõlgendada andmeid ilma eelarvamusteta ning lähtusin analüüsi koostamisel uurimisküsimustest, hoolega loodud kategooriatest ning liikusin läbi teksti rahulikus tempos.

KOKKUVÕTE

Õpetajad kasutavad õppetöös üha enam e-keskkondasid, kuid sellega kaasneb ka suur oht õpilaste andmete privaatsusele. Andmete privaatsusele ja just alaealiste andmete privaatsusele pööratakse üha suuremat tähelepanu nii Eestis kui ka mujal maailmas. Õpetajate rolli selles on paljudes riikides uuritud, kuid Eestis on uuritud üldiselt andmete privaatsuse aspekti. Minu eesmärk oli välja selgitada üldhariduskoolide inglise keele õpetajate teadlikkus isikuandme kaitse põhimõtetest ja nende rakendamisest e-keskkondades. Valisin inglise keele õpetajad, sest inglise keelsete e-keskkondade valik on väga lai. Tahtsin selgitada välja, milline on inglise keele õpetajate kogemus e-keskkondadega, mida nad teevad, et kaitsta õpilaste andmete privaatsust, milline on nende kokkupuude andmekaitsega ning milliseid ohte nad õpilaste andmetele teadvustavad.

Teemaga seotult püstitasin järgmised küsimused:

1. Millest lähtub õpetajate kasutatavate e-keskkondade valik?
2. Kuidas tagavad õpetajad õpilaste andmete kaitsmise e-keskkondades?
3. Milliseid ohte õpilaste andmete privaatsusele e-keskkondades õpetajad teadvustavad?

Oma töö teooriaosas olen kirjeldanud erinevaid teemat puudutavaid mõisteid. Uurimisküsimustele vastuste saamiseks viisin läbi kaheksa poolstruktureeritud intervjuud Tartu linna põhikoolides töötavate inglise keele õpetajatega. Intervjuud teostasin läbi silmast-silma kohtumiste. Saadud tulemuste analüüsiks kasutasin kvalitatiivse sisuanalüüsi meetodit.

Intervjuude analüüs näitas, et õpetajad kasutavad e-keskkondasid lähtuvalt nende sisust ja tasuta kättesaadavusest. Sisu puhul oli oluline, et see oleks mitmekülgne, kuid võimaldaks ka ise uusi materjale luua. Eelistati ka keskkondasid, kus pole vajalik kontot luua ning enamik õpetajaid lasi õpilasel kasutada keskkonda õpilase enda seadmes. Keskkonna turvalisus andmekaitse kontekstis ei mänginud keskkonna valikul rolli, kuid oli õpetajate jaoks siiski oluline.

Õpetajate hinnangul oli nende roll õpilaste andmete e-keskkonda sattumises minimaalne ning päädis mõnel juhul kasutajanime sisestamisega. Peamisteks ohtudeks e-keskkonnas pidasid õpetajad eale mittesobiliku sisu nägemist, reklaame ja oma andmete jagamist võõrastega. Õpetajate endi tegevus õpilaste andmete kaitsmiseks oli peamiselt teavitustöö andmete kaitsmise meetodite kohta ning keskkondade valik, mis ei nõudnud sisse logimist.

Õpetajad arvasid, et õpilaste andmeid kasutatakse peamiselt e-keskkonna statistikaks, sisu parandamiseks ja õpilasele reklaamide saatmiseks. Suurem osa õpetajaid ei olnud osalenud andmekaitseteemalistel koolitustel. Õpetajad pidasid privaatsust oluliseks. Privaatsuse mõiste defineerimise asemel, toodi näiteid, mis privaatsust ohustab.

Kokkuvõttes saan väita, et õpetajate tase õpilaste andmete privaatsuse kaitsmisel sõltub olemasolevatest teadmistest ja sellest tulenevalt ka õpetajate tegevused õpilaste andmete kaitseks. Teadvustatakse neid ohte, mida juba teatakse või osatakse oma teadmistest tuletada. E-keskkondade kasutus võiks olla reguleeritud eelistatult riigi või ka õppeasutuste poolt.

SUMMARY

The experience of English language teachers in Estonian general education schools with student data in e-environments

Teachers are increasingly using e-environments in their teaching, but this also poses a great risk to the privacy of students' data. More and more attention is being paid to data privacy, and especially to the privacy of minors, both in Estonia and in other parts of the world. The role of teachers in this has been studied in many countries, but in Estonia the aspect of data privacy has been studied in general. My goal was to find out the awareness of English language teachers in general education schools about the principles of personal data protection and their implementation in e-environments. I chose English language teachers because the selection of English language e-environments is very wide. I wanted to find out what is the experience of English language teachers with e-environments, what they do to protect the privacy of students' data, what is their exposure to data protection and what threats they perceive to students' data. Related to the topic, I posed the following questions:

1. What is the basis for the choice of e-environments used by teachers?
2. How do teachers ensure the protection of students' data in e-environments?
3. What threats to the privacy of students' data in e-environments are teachers aware of?

In the theory part of my work, I have described various concepts related to the topic. To get answers to the research questions, I conducted eight semi-structured interviews with English language teachers working in primary schools in the city of Tartu. I conducted the interviews through face-to-face meetings. I used the method of qualitative content analysis to analyze the obtained results.

The analysis of the interviews showed that teachers use e-environments based on their content and free availability. Regarding the content, it was important that it be versatile, but also allow you to

create new materials yourself. Environments where it is not necessary to create an account were also preferred, and most teachers let the student use the environment on the student's own device. Environmental security in the context of data protection did not play a role in the choice of environment but was still important to teachers.

According to the teachers, their role in getting students' data into the e-environment was minimal, and in some cases, it ended with entering a username. Teachers considered seeing inappropriate content, advertisements and sharing their data with strangers to be the main threats in the e-environment. The teachers' own actions to protect students' data were mainly outreach work on data protection methods and the selection of environments that did not require logging in.

Teachers believed that student data is mainly used for e-environment statistics, to improve content and to send advertisements to the student. The majority of teachers had not participated in training on data protection. Teachers considered privacy important. Instead of defining the concept of privacy, examples were given that threaten privacy.

In summary, I can say that the level of protection to privacy of students' data provided by the teachers, depends on their existing knowledge. In connection to that, so do the actions of teachers to protect students' data. Dangers that are already known or can be derived from one's knowledge, are made aware. The use of e-environments could preferably be regulated by the state or educational institutions.

KASUTATUD KIRJANDUS

Abdel-Basset, M., Mohamed, M., Smarandache, F. ja Chang, V. (2018). Neutrosophic Association Rule Mining Algorithm for Big Data Analysis. *Symmetry*, 10(4), 106.

<https://doi.org/10.3390/sym10040106>

Aldous Arantes, J. (2019). Equity Implications of Predictive Analytics in K-12 Classrooms.

Ubiquitous Learning: An International Journal, 12(2), 63–84.

<https://doi.org/10.18848/1835-9795/CGP/v12i02/63-84>

Andmekaitse ei tohi saada õpetamisel takistuseks. (2020). *Andmekaitse Inspeksioon*, 11. veebruar.

Kasutatud 26.11.2022, <https://www.aki.ee/et/uudised/andmekaitse-ei-tohi-saada-opetamisel-takistuseks>

Andmekaitse Inspeksiooni kodulehekülj. (2019). *Isikuandmete liigitus*. Kasutatud 15.11.2022,

<https://www.aki.ee/et/eraelu-kaitse/isikuandmed-ja-tootlemine/isikuandmete-liigitus>

Arantes, J. ja Buchanan, R. (2022). Educational data advocates: Emerging forms of teacher agency in postdigital classrooms. *Learning, Media and Technology*, 0(0), 1–21.

<https://doi.org/10.1080/17439884.2022.2087084>

Arundel, K. (2021). Why student data remains at risk—And what educators are doing to protect it.

Kasutatud 22.10.2022, <https://www.k12dive.com/news/why-student-data-remains-at-risk-and-what-educators-are-doing-to-protect-it/611462/>

- Büchi, M., Festic, N. ja Latzer, M. (2022). The Chilling Effects of Digital Dataveillance: A Theoretical Model and an Empirical Research Agenda. *Big Data & Society*, 9(1), <https://doi.org/10.1177/205395172111065368>
- Cao, L. (2017) Data Science: A Comprehensive Overview. *ACM Computing Surveys*, 50(3), <https://doi.org/10.1145/3076253>
- Chanenson, J., Sloane, B., Rajan, N., Morril, A., Chee, J., Huang, D.Y. ja Chetty, M. (2023). Uncovering Privacy and Security Challenges In K-12 Schools. *Conference on Human Factors in Computing Systems*, 592, 1-28. <https://doi.org/10.1145/3544548.3580777>
- Clow, D. (2013). An overview of learning analytics. *Teaching in Higher Education*, 18(6), 683–695. <https://doi.org/10.1080/13562517.2013.827653>
- Connolly, R. ja Fox, G. (2017). *Dataveillance and Information Privacy Concerns*: <https://doi.org/10.4018/978-1-5225-0983-7.ch063>
- Cook, S. (2023). The best free ad blockers for Chrome, Firefox, and Safari. Comparitech. Kasutatud 05.05.2023, <https://www.comparitech.com/blog/vpn-privacy/best-free-ad-blockers/>
- Day, E. (2021). Governance of data for children's learning in UK state schools. *Digital Futures Commission, 5Rights Foundation*. Kasutatud 31.12.2022, <https://digitalfuturescommission.org.uk/wp-content/uploads/2021/06/Governance-of-data-for-children-learning-Final.pdf>
- Day, E. (2022). Data governance for children: An emerging priority area for privacy professionals | *UNICEF Office of Global Insight & Policy*. Kasutatud 26.11.2022, <https://www.unicef.org/globalinsight/stories/data-governance-children-emerging-priority-area-privacy-professionals>

- Day, E., Pothong, K., Atabey, A. ja Livingstone, S. (2022). Who controls children's education data? A socio-legal analysis of the UK governance regimes for schools and EdTech. *Learning, Media and Technology*, 0(0), 1–15. <https://doi.org/10.1080/17439884.2022.2152838>
- Dijck, J. van. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society*, 12(2), 197–208. <https://doi.org/10.24908/ss.v12i2.4776>
- E-õppe keskkondade seire kokkuvõte. (2017) *Andmekaitse Inspeksioon*. Kasutatud 15.11.2022, https://www.aki.ee/sites/default/files/seired/e-oppe_keskkondade_seire_kokkuvote.pdf
- Enhancing data informed strategic governance in education in Estonia (2021). OECD Education Policy Perspectives, No. 47, OECD Publishing, Paris, <https://doi.org/10.1787/11495e02-en>.
- Gebhart, G. (2017). Spying on Students: School-Issued Devices and Student Privacy. Kasutatud 10.04.2023, <https://www.eff.org/wp/school-issued-devices-and-student-privacy>
- Griffith, E. (i.a). Stop Changing Your (Strong, Unique) Passwords So Much. Kasutatud 08.04.2023, <https://www.pcmag.com/opinions/stop-changing-your-strong-unique-passwords-so-much>
- Haridus- ja Teadusministeerium. (2019). *Haridus- ja Teadusministeeriumi valdkondade 2018.a arengukavade täitmise analüüs*. Kasutatud 04.12.2022, <http://www.digar.ee/id/nlib-digar:408589>
- Hariri, R. H., Fredericks, E. M. ja Bowers, K. M. (2019). Uncertainty in big data analytics: Survey, opportunities, and challenges. *Journal of Big Data*, 6(1), 44. <https://doi.org/10.1186/s40537-019-0206-3>
- Hillman, V. (2022). Bringing in the technological, ethical, educational and social-structural for a new education data governance. *Learning, Media and Technology*, 0(0), 1–16. <https://doi.org/10.1080/17439884.2022.2052313>

- How Often Should You Change Your Passwords? (2022). *McAfee*. Kasutatud 08.04.2023,
<https://www.mcafee.com/learn/how-often-should-you-change-your-passwords/>
- How often should you change your passwords? (i.a) Kaspersky. Kasutatud 08.04.2023,
<https://www.kaspersky.com/resource-center/preemptive-safety/how-often-password-change>
- Huang, R.H., Liu, D.J., Zhu, L.X., Chen, H.Y., Yang, J.F., Tlili, A., Fang, H.G. ja Wang, S.F.
(2020). *Personal Data and Privacy Protection in Online Learning: Guidance for Students, Teachers and Parents*. Beijing: Smart Learning Institute of Beijing Normal University.
- Inspektsioonist (2020). *Andmekaitse Inspektsioon*, 29. juuni. Kasutatud 30.12.2022,
<https://www.aki.ee/et/inspektsioon-kontaktid/inspektsioonist>
- Isikuandmete kaitse üldmäärus (GDPR). (2016). Kasutatud 24.10.2022, <https://gdprinfo.eu/et>
- Jarke, J. ja Breiter, A. (2019). Editorial: The datafication of education. *Learning, Media and Technology*, 44(1), 1–6. <https://doi.org/10.1080/17439884.2019.1573833>
- Jim, C. K. ja Chang, H.-C. (2018). The current state of data governance in higher education. *Proceedings of the Association for Information Science and Technology*, 55(1), 198–206.
<https://doi.org/10.1002/pra2.2018.14505501022>
- Johnson, D. (i.a). How often you should change your passwords, according to cybersecurity experts. Kasutatud 08.04.2023, <https://www.businessinsider.com/guides/tech/how-often-should-i-change-my-password>
- Kalmus, V., Masso, A. ja Linno, M. (2015), *Sotsiaalse analüüsi meetodite ja metodoloogia õpibaas*. Kasutatud 10.04.2023, <https://samm.ut.ee/kvalitatiivne-sisuanalyys>
- Kukk, K. (2019). HITSA õppematerjalid on haridusasutustele toeks isikuandmete töötlemisel. *Märka Last*. Kasutatud 26.11.2022, <https://ajakiri.lastekaitseliit.ee/2019/02/07/hitsa-oppematerjalid-on-haridusasutustele-toeks-isikuandmete-tootlemisel>

- Lagerspetz, M. (2017) Ühiskonna uurimise meetodid. Sissejuhatus ja väljajuhatus. TLÜ Kirjastus, Tallinn 2017.
- Lepik, K., Harro-Loit, H., Kello, K., Linno, M., Selg, M. ja Strömpl, J. (2014). Intervjuu. Kasutatud 26.11.2022, <https://samm.ut.ee/intervjuu>
- Long, P. ja Siemens, G. (2011). Penetrating the Fog: Analytics in Learning and Education. Kasutatud 30.12.2022, <https://er.educause.edu/articles/2011/9/penetrating-the-fog-analytics-in-learning-and-education>
- Lorenz, B., Eomäe, T., Kirna, C., Poudel, D., Saks, H., Talisainen, A., Mikli, A. ja Kits, R. (2020). KüberPähkel. Kasutatud 26.11.2022, https://drive.google.com/file/d/1B-nSO_4-B2zsoWP0IO1o-HCvi462xANC/view?usp=embed_facebook
- Lorenz, B., Kikkas, K., Baum, A. ja Metsäär, T. (2021). Kitsaskohti andmekaitse rakendamisel koolides. *Õpetajate Leht*, 31. märts. Kasutatud 26.11.2022, <https://opleht.ee/2021/03/kitsaskohti-andmekaitse-rakendamisel-koolides/>
- Lühike GDPRi juhised koolidele ja õpetajatele. (2018). School Education Gateway, *Euroopa koolihariduse veebiplatvorm*. Kasutatud 26.11.2022, <https://www.schooleducationgateway.eu/et/pub/resources/tutorials/brief-gdpr-guide-for-schools.htm>
- 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. <https://doi.org/10.1080/13600834.2017.1321096>
- Mandinach, E. B. ja Cotto, J. (2021). The Case for Including Data Privacy and Data Ethics in Educator Preparation Programs. *Student Privacy Compass*, 5. oktoober. Kasutatud 26.11.2022, <https://studentprivacycompass.org/resource/case-data-privacy-ethics/>

- Manjoo, F. (2018). As Ad Business Booms, 'Traditional' Internet Falls by Wayside. *The New York Times*, 31. jaanuar. Kasutatud 15.05.2023,
<https://www.nytimes.com/2018/01/31/technology/internet-advertising-business.html>
- Montgomery, K. C. (2015). Youth and surveillance in the Facebook era: Policy interventions and social implications. *Telecommunications Policy*, 39(9), 771–786.
<https://doi.org/10.1016/j.telpol.2014.12.006>
- Mäe, M. (2016). Andmekaitse pomm tiksu8b. *Ärileht*, 4. märts. Kasutatud 26.11.2022,
<https://www.aripaev.ee/arvamused/2016/03/08/andmekaitse-pomm-tiksub>
- Olev, A. ja Alumäe, T. (2022) Estonian Speech Recognition and Transcription Editing Service, *Baltic J. Modern Computing*, Vol. 10 (2022), No. 3, pp. 409–421
<https://doi.org/10.22364/bjmc.2022.10.3.14>
- Palfrey, Q., Good, N., Ghamrawi, L., Monge, W. ja Boag, W. (2020). Privacy Considerations as Schools and Parents Expand Utilization of Ed Tech Apps During the COVID-19 Pandemic. Kasutatud 31.12.2022, <https://digitalwatchdog.org/wp-content/uploads/2020/09/IDAC-Ed-Tech-Report-912020.pdf>
- Pata, K. ja Laanpere, M. (2009). Haridustehnoloogia käsiraamat. Kasutatud 08.04.2023,
https://opikeskkonnad.files.wordpress.com/2016/09/tiigriope_haridustehnoloogia_kasiraamat.pdf
- Education Policy Outlook Estonia (Poliitikaülevaade Eesti kohta). (2020) OECD Kasutatud 04.12.2022, <https://www.oecd.org/education/policy-outlook/country-profile-Estonia-2020.pdf>
- Rethinam, B. V. (2014). Predictive Analytics in K-12: Advantages, Limitations & Implementation - .Kasutatud 14.01.2023, <https://thejournal.com/articles/2014/06/12/predictive-analytics-in-k-12-advantages-limitations-implementation.aspx>

- Robinson, R.S. (2014). Purposive Sampling. In: Michalos, A.C. (eds) *Encyclopedia of Quality of Life and Well-Being Research*. Springer, Dordrecht. https://doi.org/10.1007/978-94-007-0753-5_2337
- Robinson, B. (2022). Governance on, with, behind, and beyond the Discord platform: A study of platform practices in an informal learning context. *Learning, Media and Technology*, 0(0), 1–14. <https://doi.org/10.1080/17439884.2022.2052312>
- Sarker, I. H. (2021). Machine Learning: Algorithms, Real-World Applications and Research Directions. *SN Computer Science*, 2(3), 160. <https://doi.org/10.1007/s42979-021-00592-x>
- Shehab, N., Badawy, M. ja Arafat, H. (2021). Big Data Analytics and Preprocessing. A. E. Hassanien & A. Darwish (Toim), *Machine Learning and Big Data Analytics Paradigms: Analysis, Applications and Challenges* (lk 25–43). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-59338-4_2
- Solove, D. J. (2002). Conceptualizing Privacy. *California Law Review*, 90(4), 1087–1155. <https://doi.org/10.2307/3481326>
- Southerton, C. (2020). Datafication. L. A. Schintler ja C. L. McNeely (Toim), *Encyclopedia of Big Data* (lk 1–4). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-32001-4_332-1
- Stevenson, H. (2017). The “Datafication” of Teaching: Can Teachers Speak Back to the Numbers? *Peabody Journal of Education*, 92(4), 537–557. <https://doi.org/10.1080/0161956X.2017.1349492>
- Student Data Privacy and Data Ethics Scenarios. (i.a.). Kasutatud 26.11.2022, <https://studentprivacycompass.org/scenarios/>
- Student Privacy Primer. (i.a.). *Student Privacy Compass*. Kasutatud 27.11.2022, <https://studentprivacycompass.org/resource/student-privacy-primer/>

- Tammets, K. ja Laanpere, M. (2015). Conceptual framework for learning analytics and its feasibility in the Estonian context. *Eesti Haridusteaduste Ajakiri. Estonian Journal of Education*, 3(2), 216–246. <https://doi.org/10.12697/eha.2015.3.2.08>
- Torchia, R. (2023). What Is Third-Party Risk, and What Do Schools Need to Know? Kasutatud 10.04.2023, <https://edtechmagazine.com/k12/article/2023/02/what-third-party-risk-and-what-do-schools-need-know-perfcon>
- Understanding Child Data Privacy for Distance Learning. (2020). IEEE Innovation at Work. Kasutatud 23.10.2022, <https://innovationatwork.ieee.org/understanding-child-data-privacy-for-distance-learning/>
- Using data to improve the quality of education. (2022) *Unesco IIEP Learning Portal*, 22. märts. Kasutatud 10.04.2023, <https://learningportal.iiep.unesco.org/en/issue-briefs/monitor-learning/using-data-to-improve-the-quality-of-education>
- Valgjärv, M. (2021). Andmekaitse- miks ja kellele? *Õpetajate Leht*, 23. aprill. Kasutatud 07.10.2022, <https://opleht.ee/2021/04/andmekaitse-miks-ja-kellele/>
- What Is Data Ethics? (i.a.). Cognizant. Kasutatud 26.11.2022, <https://www.cognizant.com/us/en/glossary/data-ethics>
- Wisniewski, P., Jia, H., Xu, H., Rosson, M. B. ja Carroll, J. M. (2015). „Preventative“ vs. „Reactive“: How Parental Mediation Influences Teens’ Social Media Privacy Behaviors. *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, 302–316. Vancouver BC Canada: ACM. <https://doi.org/10.1145/2675133.2675293>

LISAD

Lisa 1 Nõusoleku vorm

Koostan lõputööd teemal „Inglise keele õpetajate kogemused ja arvamused õpilaste andmetega e-keskkonnas“. Uuringu käigus kogutud informatsiooni kasutatakse teadustöökse ega jagata kolmandate osapooltega. Intervjuudes välja toodud informatsioon on lõputöös üldistatud ning esitatud anonüümsel kujul. Intervjuu salvestatakse ning intervjuude transkriptsioonid on kättesaadavad ainult minule ning minu töö juhendajale. Nõusolekut saab igal ajal tagasi võtta vastavalt isikuandmete kaitse üldmääruse artikkel 7 lõikele 3. Nõusoleku tagasivõtmine ei mõjuta enne tagasivõtmist nõusoleku alusel toimunud töötlemise seaduslikkust.

Lisa 2 Poolstruktureeritud intervjuu kava

Sissejuhatus	Tere! Olen väga tänulik, et leidsite aega intervjuu tegemiseks. Kinnitan, et minu esitatud küsimustele ei ole õigeid ega valesid vastuseid, vaid olulised on Teie enda seisukohad. Võite ka igal hetkel vastamisest keelduda. Kas võime sinatada?
Milliseid keskkondasid kasutavad?	<p>Millis e- keskkondasid oled hiljuti kasutanud? Millist kõige rohkem kasutad? Rääkige sellest lähemalt. Selgita täpsemalt, mida seal tegema peab?</p> <ol style="list-style-type: none"> 1) <i>Millised on võimalused?</i> 2) <i>Mida peate teie tegema?</i> 3) <i>Mida õpilased teevad?</i> <p>Mis andmeid ise õpilase kohta sisestate? Mis on olnud Teie ülesanded ja tegevused seoses õpilaste andmetega? Millised on õpilase õigused seal keskkonnas? Millised on õpetaja õigused seal keskkonnas? Milliseid andmeid õpilase kohta seal keskkonnas on? Millised isikuandmed? Millised eriliigilised?</p>
Mida nad saavad teha õpilaste andmete kaitsmiseks/mida teevad?	<p>Millised on e-keskkonna kasutamise tingimused? Mis piirangud on õpilaste andmete vaatamisel? Mis õigused on õpilaste andmete vaatamisel? Mida näed õpilase kohta X keskkonnas? Mida näed tema õppimise kohta X keskkonnas? Milliseid järeltusi saad teha tema kohta? Kes veel õpilase andmeid näeb? Milliseid andmeid õpilased üksteise kohta näevad? Milliseid õpilaste andmeid see keskkond kogub? Kes õpilase andmeid seal töötleb? Mis nende andmetega võib juhtuda? Mis ohustab õpilasi online keskkondades? Millised nendest ohtudest esinevad ka õpetöös kasutatavates keskkondades? Kuidas on reguleeritud õpilaste andmete kaitsmine? Mida teete, et õpilase andmed oleksid kaitstud? Mida saaksite veel teha? Mida õpilased ise saaksid teha, et nende andmed oleksid kaitstud?</p>
Mida nad teavad?	<p>Mis on X keskkonna miinused andmekaitse kontekstis? Mis on X keskkonna plussid andmekaitse kontekstis? Kuidas mõista privaatsust? Kus on sulle räägitud andmekaitsest? Kus on sulle räägitud õpilaste andmete kaitsest? Millisel isikuandmete kaitse teemalisel koolitusel oled osalenud? Kui pika perioodi kohta on võimalik õpilase andmeid näha? Kui kaua neid andmeid on võimalik näha?</p>

	Mis eesmärgil neid alles hoitakse?
Lõpetuseks	Mida soovite veel lisada selle teemaga seoses, mille kohta ma ei küsinud? Kui mul tekivad lisaküsimused, kas ma saan teiega veel ühendust võtta? Tänan veelkord, et olite valmis minu küsimustele vastama.

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, Gajane Veeroja,

1. Annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose „nimi“, mille juhendaja on Katrin Kannukene, 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 Commons'i litsentsiga CC BY NC ND 4.0, mis lubab autorile viidates teost reprodutseerida, levitada ja üldsusele suunata ning keelab luua tuletatud teost ja kasutada teost ärieesmärgil, kuni autoriõiguse kehtivuse lõppemiseni.

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

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

Gajane Veeroja

21.05.2023